Contents

4 Galois Theory

In this chapter we extend our analysis of field extensions by developing Galois theory, whose central idea is to relate the permutations of roots of polynomials (which has a natural group structure) to the structure of splitting fields. Galois theory and its applications, in particular, illustrate the power of using the action of one object (in this case, a group) on another object (in this case, a field) to reveal structural information about both. We will develop the fundamental theorem of Galois theory, which makes this relationship between groups and fields precise, and then apply it to study the structure of finite fields, cyclotomic fields, abelian extensions, and the roots of polynomials (including cubic and quartic equations), culminating in Abel's celebrated theorem on the insolvability by radicals of the general quintic equation. Our work will draw upon, and tie together, nearly all of the results we have developed previously about polynomials, field extensions, and groups.

4.1 Field Automorphisms and Galois Groups

- We begin by studying the collection of structure-preserving symmetries of a field K.

4.1.1 Field Automorphisms

- Definition: If K is a field, a (field) automorphism of K is a ring isomorphism of K with itself; explicitly, a field automorphism is a map $\sigma : K \to K$ that is a bijection and has $\sigma(x+y) = \sigma(x) + \sigma(y)$ and $\sigma(xy) = \sigma(x)\sigma(y)$ for all $x, y \in K$. The collection of all automorphisms of K is denoted $\mathrm{Aut}(K)$.
  - Example: For $K = \mathbb{C}$, the complex conjugation map $\sigma(a+bi) = a - bi$, for $a, b \in \mathbb{R}$, is an automorphism of K. It is clearly a bijection, and it is easy to verify that it also respects addition and multiplication.
  - Example: For $K = \mathbb{Q}(\sqrt{D})$ for squarefree D, the "conjugation map" $\sigma(a+b\sqrt{D}) = a - b\sqrt{D}$, for $a, b \in \mathbb{Q}$, is an automorphism of K. (Note that if $D < 0$ then this map is simply complex conjugation.)
  - Example: For $K = \mathbb{F}_{p^n}$ for a positive integer n, the pth-power Frobenius map $\sigma(x) = x^p$ for $x \in K$ is an automorphism of K. As we have previously mentioned, σ respects addition and multiplication and is injective, hence (since K is finite) it is a bijection.
  - Based on our understanding of groups as collections of symmetries, we would expect $\mathrm{Aut}(K)$ to be a group under function composition, and indeed it is: the operation is well-defined (since the composition of two automorphisms is an automorphism), the operation is associative (since function composition is associative), there is an identity element (namely, the identity map), and every element has an inverse (namely, the inverse function, which is also an automorphism).
- Given a map from K to K, it is not hard to check whether it is an automorphism, but *a priori* it is not obvious how to construct automorphisms of K, nor how to compute the automorphism group $\mathrm{Aut}(K)$.
  - As a first step we observe that any automorphism of K must fix 0 and 1 (i.e., map 0 and 1 to themselves), and hence by a trivial induction must fix the prime subfield of K.
  - In particular, this immediately tells us that $\mathrm{Aut}(\mathbb{Q})$ and $\mathrm{Aut}(\mathbb{F}_p)$ are both the trivial group.
  - To extend this further, it will be useful to generalize our analysis to automorphisms that preserve field extensions:
- Definition: If K/F is a field extension, we define $\mathrm{Aut}(K/F)$ to be the set of automorphisms of K fixing F (i.e., the collection of $\sigma \in \mathrm{Aut}(K)$ such that $\sigma(a) = a$ for every $a \in F$).
  - We can see that $\mathrm{Aut}(K/F)$ is a subgroup of $\mathrm{Aut}(K)$: the identity map on K is clearly an element of $\mathrm{Aut}(K/F)$, and if $\sigma, \tau \in \mathrm{Aut}(K/F)$ then $\sigma\tau^{-1}$ is also in $\mathrm{Aut}(K/F)$ since $\sigma\tau^{-1}(a) = \sigma(\tau^{-1}(a)) = \sigma(a) = a$ for all $a \in F$.
  - By our observations above, $\mathrm{Aut}(K) = \mathrm{Aut}(K/K')$ where K' is the prime subfield of K; thus, we may freely pass between speaking about automorphisms of K and automorphisms of K/K'.
- Notice that if $\sigma \in \mathrm{Aut}(K/F)$, then $\sigma(v+w) = \sigma(v) + \sigma(w)$ and $\sigma(\alpha v) = \alpha\sigma(v)$ for any $v, w \in K$ and $\alpha \in F$: this means that σ is an F-vector space isomorphism from K to itself.
  - In particular, we may completely specify σ by its values on a basis for K/F.
  - In fact, since σ also respects multiplication in K, it is enough to specify the value of σ on a set of generators for K/F as a field extension.
  - Of course, we cannot specify these values arbitrarily (for example, we cannot map any of the nonzero generators to 0). Even avoiding such trivial difficulties, other problems can arise.
  - For example, if $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$, the choices $\sigma(\sqrt{2}) = \sqrt{3}$ and $\sigma(\sqrt{3}) = \sqrt{2}$ do extend to a linear transformation from K to K (where we also set $\sigma(1) = 1$ and $\sigma(\sqrt{6}) = \sigma(\sqrt{2})\sigma(\sqrt{3}) = \sqrt{6}$, and extend to all of K by $\mathbb{Q}$-linearity). However, the resulting map is not a field automorphism, because $\sigma(\sqrt{2}\cdot\sqrt{2}) = 2$ but $\sigma(\sqrt{2}) \cdot \sigma(\sqrt{2}) = 3$.
  - We would like determine exactly what choices will extend to an actual automorphism of the extension.

- As suggested by the example above, because $\sigma \in \mathrm{Aut}(K/F)$ preserves addition and multiplication along with all elements of F, it will also preserve any algebraic relations between the generators that can be written using coefficients of F.
- In many cases, we can use this observation to compute all possible automorphisms:

- Example: Find all automorphisms of $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$.
  - By the discussion above, an automorphism σ of $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is completely determined by the value $\sigma(\sqrt{2})$. Explicitly, we would have $\sigma(a+b\sqrt{2}) = \sigma(a) + \sigma(b)\sigma(\sqrt{2}) = a + b \cdot \sigma(\sqrt{2})$, for $a, b \in \mathbb{Q}$.
  - Furthermore, since $(\sqrt{2})^2 - 2 = 0$, applying σ to both sides yields $0 = \sigma(0) = \sigma[(\sqrt{2})^2 - 2] = \sigma(\sqrt{2}^2) - \sigma(2) = \sigma(\sqrt{2})^2 - 2$.
  - This means that $\sigma(\sqrt{2})^2 = 2$, and thus there are only two possibilities for $\sigma(\sqrt{2})$, namely $\sigma(\sqrt{2}) = \sqrt{2}$ and $\sigma(\sqrt{2}) = -\sqrt{2}$.
  - But each of these choices does in fact extend to an automorphism of $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$: the choice $\sigma(\sqrt{2}) = \sqrt{2}$ is satisfied by the identity automorphism, while the choice $\sigma(\sqrt{2}) = -\sqrt{2}$ is satisfied by the conjugation automorphism.
  - We conclude that $|\mathrm{Aut}(K/\mathbb{Q})| = 2$, and so the automorphism group must be cyclic and isomorphic to $\mathbb{Z}/2\mathbb{Z}$.
  - Indeed, if τ represents the conjugation automorphism, we can see that τ^2 is the identity (as dictated by the structure of the group).
  - Remark: If D is a squarefree integer, the same arguments with D in place of 2 show that for $K = \mathbb{Q}(\sqrt{D})$, the automorphism group $\mathrm{Aut}(K/\mathbb{Q})$ also has order 2 and is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

- Example: Find all automorphisms of $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$.
  - As above, an automorphism σ of $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is completely determined by the value $\sigma(\sqrt[3]{2})$.
  - Since $(\sqrt[3]{2})^3 - 2 = 0$, applying σ to both sides yields $\sigma(\sqrt[3]{2})^3 - 2 = 0$, and so $\sigma(\sqrt[3]{2})$ is a root of the polynomial $x^3 - 2$.
  - However, the other two roots of this polynomial (inside $\mathbb{C}$) are $\sqrt[3]{2} \cdot \zeta_3$ and $\sqrt[3]{2} \cdot \zeta_3^2$ for ζ_3 a primitive 3rd root of unity. These elements are not in $\mathbb{Q}(\sqrt[3]{2})$, since they are not real.
  - Therefore, the only possibility is to have $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$, and then σ is simply the identity map. Thus, $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ is the trivial group.
  - Remark: If K is either of $\mathbb{Q}(\sqrt[3]{2} \cdot \zeta_3)$ or $\mathbb{Q}(\sqrt[3]{2} \cdot \zeta_3^2)$, then $\mathrm{Aut}(K/\mathbb{Q})$ is also the trivial group. This follows by the same argument, since the polynomial $x^3 - 2$ only has one root in K.

4.1.2 Computing Automorphisms

- By formalizing the arguments given in the examples above, we can compute the automorphisms of any simple algebraic extension. We will first establish a lemma that will be useful for constructing isomorphisms:

- Lemma (Lifting Isomorphisms): Let $\varphi : E \to F$ be an isomorphism of fields. If α is algebraic over E with minimal polynomial $p(x) = a_0 + a_1 x + \cdots + a_n x^n \in E[x]$, and β is algebraic over F with minimal polynomial $q(x) = \varphi(a_0) + \varphi(a_1)x + \cdots + \varphi(a_n)x^n \in F[x]$, then there is a unique isomorphism $\tilde{\varphi} : E(\alpha) \to F(\beta)$ extending φ (i.e., such that $\tilde{\varphi}|_E = \varphi$) and such that $\varphi(\alpha) = \beta$.
  - Note that we essentially proved this result in the course of establishing the uniqueness of splitting fields.
  - Proof: Note that $[E(\alpha) : E] = n$ with an explicit basis $\{1, \alpha, \alpha^2, \ldots, \alpha^n\}$, and similarly $[F(\beta) : F] = n$ with basis $\{1, \beta, \beta^2, \ldots, \beta^n\}$.
  - Then any isomorphism $\tilde{\varphi}$ extending φ with $\tilde{\varphi}(\alpha)$ must have $\tilde{\varphi}(c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}) = \varphi(c_0) + \varphi(c_1)\beta + \cdots + \varphi(c_{n-1})\beta^{n-1}$ for $c_i \in E$, so there is at most one possible map $\tilde{\varphi}$.
  - On the other hand, one may verify that this map $\tilde{\varphi}$ (which is well defined) does indeed respect addition and multiplication, and has an inverse map $\tilde{\varphi}^{-1}(d_0 + d_1\beta + \cdots + d_{n-1}\beta^{n-1}) = \varphi^{-1}(d_0) + \varphi^{-1}(d_1)\alpha + \cdots + \varphi^{-1}(d_{n-1})\alpha^{n-1}$, so $\tilde{\varphi}$ is in fact an isomorphism.

- Theorem (Automorphisms of Simple Algebraic Extensions): Suppose α is algebraic over F with minimal polynomial $m(x)$, and $K = F(\alpha)$: then for any $\sigma \in \mathrm{Aut}(K/F)$, $\sigma(\alpha)$ is also a root of $m(x)$ in K. Conversely, if β is any other root of $m(x)$ in K, then there exists a unique automorphism $\tau \in \mathrm{Aut}(K/F)$ with $\tau(\alpha) = \beta$. Hence $|\mathrm{Aut}(K/F)|$ is equal to the number of roots of $m(x)$ in K, and is (in particular) finite and at most $[K : F]$.
    - Proof: Suppose that $m(x) = a_n x^n + \cdots + a_1 x + a_0$ with the $a_i \in F$. Note that $\sigma(a_i) = a_i$ since σ fixes F.
    - Then $m(\sigma(\alpha)) = a_n\sigma(\alpha)^n + \cdots + a_1\sigma(\alpha) + a_0 = \sigma(a_n\alpha^n) + \cdots + \sigma(a_1\alpha) + \sigma(a_0) = \sigma(a_n\alpha^n + \cdots + a_1\alpha + a_0) = \sigma(0) = 0$ and so $\sigma(\alpha)$ is also a root of $m(x)$.
    - For the second statement, suppose β is another root of $m(x)$ in K. If we apply the isomorphism lifting lemma with $E = F$ (so that the isomorphism φ is the identity map), then we see that there is a unique isomorphism $\tau : F(\alpha) \to F(\beta)$ such that $\tau(\alpha) = \beta$. Since $F(\alpha) = K = F(\beta)$, the map τ is an automorphism of K.
    - We then have a bijection between roots of $m(x)$ in K and $\mathrm{Aut}(K/F)$, and since $m(x)$ has degree $[K : F]$, we conclude that $|\mathrm{Aut}(K/F)| \leq [K : F]$.
- Using this characterization, we can compute all the automorphisms of a simple algebraic extension, and then (at least in principle) we may determine the structure of the automorphism group:
- Example: Identify the elements and group structure of $\mathrm{Aut}(\mathbb{Q}(\sqrt{2} + \sqrt{3})/\mathbb{Q})$.
    - As we have previously computed, $\sqrt{2} + \sqrt{3}$ is a root of the polynomial $m(x) = x^4 - 10x^2 + 1$, and since $K = \mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ has degree 4 over $\mathbb{Q}$, we see $m(x)$ is irreducible.
    - By applying the quadratic formula twice, we can see that the four roots of $m(x)$ are $\pm\sqrt{2} \pm \sqrt{3}$, all of which are in K. Hence there are 4 automorphisms of $K/\mathbb{Q}$, obtained by mapping $\sqrt{2}+\sqrt{3}$ to any one of the other four roots of $m(x)$.
    - We could, if desired, compute the actions of these four automorphisms just from their behavior on $\sqrt{2} + \sqrt{3}$.
    - Clearly, the map sending $\sqrt{2} + \sqrt{3}$ to itself will extend to the identity automorphism.
    - Also, the map σ with $\sigma(\sqrt{2} + \sqrt{3}) = -\sqrt{2} + \sqrt{3}$ has $\sigma(5 + 2\sqrt{6}) = \sigma((\sqrt{2} + \sqrt{3})^2) = \sigma(\sqrt{2} + \sqrt{3})^2 = (\sqrt{2}-\sqrt{3})^2 = 5-2\sqrt{6}$, and $\sigma(11\sqrt{2}+9\sqrt{3}) = \sigma((\sqrt{2}+\sqrt{3})^3) = \sigma(\sqrt{2}+\sqrt{3})^3 = (\sqrt{2}-\sqrt{3})^3 = 11\sqrt{2}-9\sqrt{3}$.
    - So since σ fixes $\mathbb{Q}$, by taking appropriate linear combinations we can conclude that $\sigma(\sqrt{2}) = \sqrt{2}$, $\sigma(\sqrt{3}) = -\sqrt{3}$, and $\sigma(\sqrt{6}) = -\sqrt{6}$. Thus σ is the map with $\sigma(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}$ for $a, b, c, d \in \mathbb{Q}$.
    - In a similar way, we can see that the map τ with $\tau(\sqrt{2}+\sqrt{3}) = \sqrt{2}-\sqrt{3}$ has $\tau(\sqrt{2}) = \sqrt{2}$, $\tau(\sqrt{3}) = -\sqrt{3}$, and thus τ is the map with $\tau(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}$ for $a, b, c, d \in \mathbb{Q}$.
    - We can then immediately compute that $\sigma\tau$ is the map with $\sigma\tau(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) = a-b\sqrt{2}-c\sqrt{3}+d\sqrt{6}$ for $a, b, c, d \in \mathbb{Q}$.
    - Notice then that σ^2, τ^2, and $(\sigma\tau)^2$ are each the identity map, and also that $\tau\sigma = \sigma\tau$.
    - Then we immediately see that $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \{e, \sigma, \tau, \sigma\tau\}$ is isomorphic to the Klein 4-group.
- The procedure in the example above only applies to simple extensions, and in any case it seems likely that it might be easier to analyze the automorphisms of $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ using the simpler generators $\sqrt{2}$ and $\sqrt{3}$.
    - We know that any automorphism of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ must map $\sqrt{2}$ to $\pm\sqrt{2}$ and must also map $\sqrt{3}$ to $\pm\sqrt{3}$, and since $\sqrt{2}$ and $\sqrt{3}$ generate the field, these choices completely determine the automorphism.
    - But since these two choices yield at most 4 possible automorphisms, and there actually are 4 automorphisms from our calculations above, all 4 possible choices must in fact extend to automorphisms.
    - We can see that the automorphism mapping $\sqrt{2} \mapsto \sqrt{2}$ and $\sqrt{3} \mapsto \sqrt{3}$ is the identity map.
    - If we let σ be the automorphism mapping $\sqrt{2} \mapsto -\sqrt{2}$ and $\sqrt{3} \mapsto \sqrt{3}$, then we can see that $\sigma(\sqrt{6}) = \sigma(\sqrt{2})\sigma(\sqrt{3}) = -\sqrt{6}$, and so explicitly σ is the map we found above with $\sigma(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}$ for $a, b, c, d \in \mathbb{Q}$.

- Likewise, if we let τ be the automorphism mapping $\sqrt{2} \mapsto \sqrt{2}$ and $\sqrt{3} \mapsto -\sqrt{3}$, then we can see that $\tau(\sqrt{6}) = \tau(\sqrt{2})\tau(\sqrt{3}) = -\sqrt{6}$, and so τ is the map we identified above with $\tau(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}$ for $a, b, c, d \in \mathbb{Q}$. We can then immediately determine the group structure by composing σ and τ as we did above.

- Notice that our computation of the automorphisms in the second version of the example relied on the knowledge that there were actually 4 automorphisms of the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$.
  - We could, alternatively, have constructed these automorphisms explicitly via the isomorphism lifting lemma on simple extensions.
  - To construct σ, first observe that $x^2 - 2$ is the minimal polynomial of both $\sqrt{2}$ and $-\sqrt{2}$ over $\mathbb{Q}(\sqrt{3})$, since $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{3})] = 2$.
  - Then by the isomorphism lifting lemma applied to the identity map on $\mathbb{Q}(\sqrt{3})$, there is an automorphism σ of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ with $\mathbb{Q}(-\sqrt{2}, \sqrt{3})$ that fixes $\mathbb{Q}(\sqrt{3})$ and maps $\sqrt{2}$ to $-\sqrt{2}$. This automorphism then has $\sigma(\sqrt{2}) = -\sqrt{2}$ and $\sigma(\sqrt{3}) = \sqrt{3}$, so it extends to the automorphism we identified above.
  - In a similar way, we can construct τ by observing that $x^2 - 3$ is the minimal polynomial of both $\sqrt{3}$ and $-\sqrt{3}$ over $\mathbb{Q}(\sqrt{2})$, and so there is an automorphism τ of $\mathbb{Q}(-\sqrt{2}, \sqrt{3})$ that fixes $\mathbb{Q}(\sqrt{2})$ and maps $\sqrt{3}$ to $-\sqrt{3}$.
  - We can also construct $\sigma\tau$ by lifting the conjugation automorphism on $\mathbb{Q}(\sqrt{3})$: explicitly, $x^2 - 2$ is the minimal polynomial of both $\sqrt{2}$ over $\mathbb{Q}(\sqrt{3})$ and of $-\sqrt{2}$ over $\mathbb{Q}(-\sqrt{3})$. Then there is an automorphism of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ that extends the conjugation automorphism on $\mathbb{Q}(\sqrt{3})$ (sending $\sqrt{3}$ to $-\sqrt{3}$) to $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ that maps $\sqrt{2}$ to $-\sqrt{2}$.

- We can use a similar procedure to the one we gave for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ to construct automorphisms of other composite extensions by lifting isomorphisms of appropriate subfields.
  - For example, if $K = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$, then there is an isomorphism of $E = \mathbb{Q}(\sqrt[3]{2})$ with $E' = \mathbb{Q}(\sqrt[3]{2} \cdot \zeta_3)$ that maps $\sqrt[3]{2}$ to $\sqrt[3]{2} \cdot \zeta_3$.
  - Since the minimal polynomial of ζ_3 over both E and E' has degree 2 (since ζ_3 is a root of the quadratic polynomial $x^2 - x + 1$ and ζ_3 is not in E or E'), we can then lift this isomorphism to obtain an automorphism σ of K with $\sigma(\zeta_3) = \zeta_3$ and $\sigma(\sqrt[3]{2}) = \sqrt[3]{2} \cdot \zeta_3$.
  - We can write out the full action of σ on K using the $\mathbb{Q}$-basis $\{1, \sqrt[3]{2}, \sqrt[3]{4}, \zeta_3, \sqrt[3]{2}\zeta_3, \sqrt[3]{4}\zeta_3\}$: since $\sigma(1) = 1$, $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}\zeta_3$, $\sigma(\sqrt[3]{4}) = \sqrt[3]{4}\zeta_3^2$, $\sigma(\zeta_3) = \zeta_3$, $\sigma(\sqrt[3]{2}\zeta_3) = \sqrt[3]{2}\zeta_3^2$, and $\sigma(\sqrt[3]{4}\zeta_3) = \sqrt[3]{4}\zeta_3^3 = \sqrt[3]{4}$.
  - Then $\sigma(c_1 + c_2\sqrt[3]{2} + c_3\sqrt[3]{4} + c_4\zeta_3 + c_5\sqrt[3]{2}\zeta_3 + c_6\sqrt[3]{4}\zeta_3) = c_1 + c_2\sqrt[3]{2}\zeta_3 + c_3\sqrt[3]{4}\zeta_3^2 + c_4\zeta_3 + c_5\sqrt[3]{2}\zeta_3^2 + c_6\sqrt[3]{4}$ for arbitrary constants $c_i \in \mathbb{Q}$.
  - Observe (in particular) how unpleasant it would be to verify that σ is actually an automorphism of K using only this latter description!

- It is not immediately obvious, however, that every automorphism of an arbitrary finite-degree extension actually arises in this fashion.
  - Suppose that K/F is a finite-degree extension: as we have shown, $K = F(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_1, \ldots, \alpha_n \in K$ that are algebraic over F.
  - Since each automorphism σ of K/F is determined by its values on $\alpha_1, \ldots, \alpha_n$, and $\sigma(\alpha_i)$ must be a root of the minimal polynomial of α_i, we see that there are only finitely many automorphisms of K/F, and so $\mathrm{Aut}(K/F)$ is a finite group.
  - If $\beta_1, \beta_2, \ldots, \beta_n$ are other roots of the minimal polynomials of the α_i in K, we might attempt to use the isomorphism lifting lemma to construct an automorphism of K that maps α_i to β_i for each i.
  - But this is not always possible: for example, consider the field $K = \mathbb{Q}(\sqrt[4]{2}, \sqrt{2})$. If we take $\alpha_1 = \sqrt[4]{2}$ and $\beta_1 = -\sqrt[4]{2}$, with $\alpha_2 = \sqrt{2}$ and $\beta_2 = -\sqrt{2}$, then each β_i is a root of the corresponding minimal polynomial of α_i over $\mathbb{Q}$.
  - However, there is no automorphism τ of K that maps α_1 to β_1 and α_2 to β_2, because we would have $\tau(\sqrt{2}) = \tau(\alpha_2) = \beta_2 = -\sqrt{2}$, but also $\tau(\sqrt{2}) = \tau(\alpha_1^2) = \beta_1^2 = \sqrt{2}$.

- The issue here is that there is an algebraic relation between the generators of this field (namely, $\sqrt{2} = (\sqrt[4]{2})^2$) that must also be respected by the automorphism, so we cannot make our choices arbitrarily.
- There is also another related difficulty in this example, namely, that some isomorphisms of subfields cannot be lifted to the full field.
- For example, the conjugation map $\sigma : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ sending $\sqrt{2}$ to $-\sqrt{2}$ cannot be lifted to an automorphism of K, because there is no possible value of $\tilde{\sigma}(\sqrt[4]{2})$: its square would necessarily be $-\sqrt{2}$, but there is no such element in K.
- On the other hand, there is such an element (namely, $\sqrt[4]{2} \cdot i$) in the splitting field $\mathbb{Q}(\sqrt[4]{2}, i)$. This suggests that working with splitting fields may solve this particular problem, and in fact, we have already shown that for splitting fields, we can always lift isomorphisms on appropriate subfields to the full splitting field.

4.1.3 Automorphisms of Splitting Fields, Galois Groups

- We now consider automorphisms of splitting fields. We will first establish a useful fact about roots of polynomials in splitting fields:
- Theorem (Normality of Splitting Fields): If K is a splitting field over F and $p(x) \in F[x]$ is irreducible, if $p(x)$ has a root in K then $p(x)$ splits completely in K (i.e., all roots of $p(x)$ are in K).
  - Proof: Suppose that K is the splitting field of the polynomial $q(x) \in F[x]$ having roots $r_1, \ldots, r_n$: then $K = F(r_1, \ldots, r_n)$.
  - Suppose also that $p(x)$ has a root $\alpha \in K$, and let β be any other root of $p(x)$ (in some splitting field).
  - By the isomorphism lifting lemma, there is an isomorphism $\sigma : F(\alpha) \to F(\beta)$ fixing F and with $\sigma(\alpha) = \beta$.
  - Then $K(\beta) = F(r_1, \ldots, r_n, \beta) = F(\beta)(r_1, \ldots, r_n)$, so $K(\beta)$ is a splitting field for $q(x)$ over $F(\beta)$. Also, since $\alpha \in K$, we see that K is a splitting field for $q(x)$ over $F(\alpha)$.
  - Then by the isomorphism lifting lemma for splitting fields[1], the isomorphism $\sigma : F(\alpha) \to F(\beta)$ extends to an isomorphism of the respective splitting fields K and $K(\beta)$ fixing F.
  - In particular we see that $[K : F] = [K(\beta) : F]$, but since both of these extensions are finite-degree, we conclude $K(\beta) = K$, and thus $\beta \in K$. Since β was an arbitrary root of p, all roots of p are in K.
- The property of splitting fields described above arises often enough that we will give it a name:
- Definition: The extension K/F is normal if for any irreducible $p(x) \in F[x]$, if $p(x)$ has a root in K then $p(x)$ splits completely in K.
- Now we can compute the size of $\mathrm{Aut}(K/F)$ when K is a splitting field over F:
- Theorem (Automorphisms of Splitting Fields): If K is a splitting field over F, then $|\mathrm{Aut}(K/F)| \leq [K : F]$ with equality if and only if K/F is separable (i.e., when K is the splitting field of a separable polynomial over F).
  - Proof: We will show a slightly stronger result via result by induction on $n = [K : F]$.
  - Suppose that $\varphi : E \to F$ is a given field isomorphism, and K is the splitting field of the polynomial $q_E(x)$ over E. If $q_F(x)$ denotes the polynomial obtained by applying φ to the coefficients of $q_E(x)$, let L be the splitting field of $q_F(x)$ over F.
  - We have previously shown (in the course of showing that splitting fields are unique) that K is isomorphic to L via a map that extends φ. We will show that the number of such isomorphisms $\sigma : K \to L$ is at most $[K : F]$, with equality if and only if K/F is separable. The desired result then follows upon setting $E = F$ and φ to be the identity map.
  - The base case $n = 1$ is trivial, since then $K = E$, $L = F$, and so the only possible map $\sigma : K \to L$ extending φ is φ itself.

[1] Recall that if $\varphi : E \to F$ is an isomorphism of fields with $p(x) = a_0 + a_1 x + \cdots + a_n x^n \in E[x]$, and we set $q(x) = \varphi(a_0) + \varphi(a_1)x + \cdots + \varphi(a_n)x^n \in F[x]$, then if K/E is a splitting field for p and L/F is a splitting field for q, the isomorphism φ extends to an isomorphism $\tau : K \to L$ (i.e., with $\tau|_E = \varphi$).

- For the inductive step, suppose $n \geq 2$ and let $p_E(x)$ be any irreducible factor of $q_E(x)$ of degree greater than 1 having a root α, which is in K by hypothesis. Set $p_F(x)$ to be the polynomial obtained by applying $\varphi$to the coefficients of $p_E(x)$.
- If σ is any isomorphism from K to L, then $\sigma(\alpha)$ is some root β_i of $p_F(x)$, which is in L. By the isomorphism lifting lemma, the number of such isomorphisms $\tau_i : E(\alpha) \to F(\beta_i)$ is equal to the number of roots β_i of $p_F(x)$, which is at most $[F(\beta) : F] = \deg(p_F) = \deg(p_E) = [E(\alpha) : E]$, with equality precisely when $p_E(x)$ is separable.
- Now we apply the inductive hypothesis to each of the possible maps $\tau_i : E(\alpha) \to F(\beta_i)$, since K is a splitting field (of q_E) over $E(\alpha)$ and L is a splitting field (of q_F) over $F(\beta_i)$, to see that the number of isomorphisms $\sigma : K \to L$ extending τ_i is at most $[K : E(\alpha)]$ with equality precisely when $q_E(x)$ is separable.
- Summing over all of the maps τ_i, we see that the total number of isomorphisms $\sigma : K \to L$ extending $\varphi : E \to F$ is at most $[E(\alpha) : E] \cdot [K : E(\alpha)] = [K : E]$, with equality if and only if $q_E(x)$ is separable (since this implies $p_E(x)$ is also separable).

- We can see that splitting fields of separable polynomials have the property that the number of automorphisms is equal to the extension degree. Such fields play a pivotal role in studying finite-degree extensions:

- Definition: If K/F is a finite-degree extension, we say that K is a Galois extension of F (or that K is Galois over F) if $|\mathrm{Aut}(K/F)| = [K : F]$. If K/F is a Galois extension, we will refer to the automorphism group $\mathrm{Aut}(K/F)$ as the Galois group of K/F, and denote it as $\mathrm{Gal}(K/F)$.

  - Some authors refer to the automorphism group of any extension as a Galois group. We only refer to Galois groups for extensions that have the "maximal possible" number of automorphisms as a way of emphasizing the important properties of these extensions.
  - Our result above shows that if K is a splitting field of a separable polynomial over F, then K/F is Galois. We will later show that the converse of this statement is also true, namely that $|\mathrm{Aut}(K/F)| \leq [K : F]$ for all finite-degree extensions, and that equality holds if and only if K/F is a splitting field of a separable polynomial.
  - The requirement that the polynomial be separable is necessary: for example, suppose $F = \mathbb{F}_2(t)$ and K is the splitting field of the irreducible polynomial $p(x) = x^2 - t$. Then $K = F(t^{1/2})$, and $p(x) = (x - t^{1/2})^2$ in K: then any automorphism σ of K/F is determined by the value of $\sigma(t^{1/2})$. But since $\sigma(t^{1/2})$ must map to a root of $p(x)$, there is only one choice, namely $\sigma(t^{1/2}) = t^{1/2}$. Hence $\mathrm{Aut}(K/F)$ is the trivial group, even though $[K : F] = 2$.

- In many cases, we can explicitly compute Galois groups of splitting fields by analyzing the behavior of generators of the extension:

- Example: Find the Galois group of the splitting field of $p(x) = x^3 - 2$ over $\mathbb{Q}$.

  - We have seen that the splitting field of $x^3 - 2$ over $\mathbb{Q}$ is $K = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$.
  - To compute the elements of this group we can try to identify the automorphisms explicitly based on their actions on the generators $\sqrt[3]{2}$ and ζ_3.
  - Since the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is $x^3 - 2$, any automorphism of $K/\mathbb{Q}$ must send $\sqrt[3]{2}$ to one of the three roots $\sqrt[3]{2}$, $\sqrt[3]{2}\zeta_3$, and $\sqrt[3]{2}\zeta_3^2$.
  - Likewise, since the minimal polynomial of ζ_3 over $\mathbb{Q}$ is $x^2 - x + 1$, any automorphism of $K/\mathbb{Q}$ must send ζ_3 to one of the two roots ζ_3, ζ_3^2.
  - Thus, there are at most 6 possible automorphisms of $K/\mathbb{Q}$. But because $[K : \mathbb{Q}] = 6$ and K is the splitting field of a separable polynomial, we know $\mathrm{Gal}(K/\mathbb{Q})$ is a group of order 6, and therefore all 6 of the possible choices must actually extend to automorphisms.
  - For example, one automorphism is the map σ with $\sigma(\sqrt[3]{2}, \zeta_3) = (\sqrt[3]{2}\zeta_3, \zeta_3)$. By choosing a basis for $K/\mathbb{Q}$ we can describe this map completely explicitly as $\sigma(c_1 + c_2\sqrt[3]{2} + c_3\sqrt[3]{4} + c_4\zeta_3 + c_5\sqrt[3]{2}\zeta_3 + c_6\sqrt[3]{4}\zeta_3) = c_1 + c_2\sqrt[3]{2}\zeta_3 + c_3\sqrt[3]{4}\zeta_3^2 + c_4\zeta_3 + c_5\sqrt[3]{2}\zeta_3^2 + c_6\sqrt[3]{4}$.
  - Another automorphism is the map τ with $\tau(\sqrt[3]{2}, \zeta_3) = (\sqrt[3]{2}, \zeta_3^2)$.

- We can then see that σ^2 is the map with $\sigma^2(\sqrt[3]{2}, \zeta_3) = (\sqrt[3]{2}\zeta_3^2, \zeta_3)$, and that σ^3 is the identity.
- Likewise, τ^2 is the identity, while $\sigma\tau$ is the map with $\sigma\tau(\sqrt[3]{2}, \zeta_3) = \sigma(\sqrt[3]{2}, \zeta_3^2) = (\sqrt[3]{2}\zeta_3, \zeta_3^2)$, and $\tau\sigma$ is the map with $\tau\sigma(\sqrt[3]{2}, \zeta_3) = \tau(\sqrt[3]{2}\zeta_3, \zeta_3) = (\sqrt[3]{2}\zeta_3^2, \zeta_3^2)$.
- We can see in particular that $\sigma\tau \neq \tau\sigma$ in this case, so by our classification of groups of order 6, we see that the Galois group must be isomorphic to $D_{2\cdot 3}$. Indeed, one can check that $\tau\sigma^2 = \sigma\tau$, meaning that σ plays the role of the element $r \in D_{2\cdot 3}$ while τ plays the role of s.

- In the example above, we could (more easily) have identified that $G \cong S_3$ by observing that G permutes the roots of the polynomial $x^3 - 2$, which generate $K/\mathbb{Q}$.
  - Since any automorphism is uniquely determined by its action on generators, and only the identity map fixes all of the generators, we obtain an injective homomorphism from G into S_3. But since $|G| = 6$ as we noted above, this map is necessarily an isomorphism, and we can identify the elements of G explicitly by the corresponding permutation on the roots of $x^3 - 2$.
  - In fact, this will work in general: if K/F is the splitting field of the polynomial $p(x)$ with roots $r_1, r_2, \ldots, r_n$, then any element of the Galois group will act as a permutation on these roots, and conversely, any element of $\mathrm{Gal}(K/F)$ is characterized by the associated permutation inside S_n (if we fix a labeling of the roots).
  - In the example above, if we label the roots $\{\sqrt[3]{2}, \sqrt[3]{2}\zeta_3, \sqrt[3]{2}\zeta_3^2\}$ as $\{1, 2, 3\}$, then σ corresponds to the permutation $(1\,2\,3)$ while τ corresponds to the permutation $(2\,3)$.
  - In general, the Galois group will not be all of S_n: for example, as we saw earlier, the Galois group of the field $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, which is the splitting field for $p(x) = (x^2 - 2)(x^2 - 3)$, only has 4 elements.

- Example: Find the Galois group of the splitting field of $p(x) = x^4 - 3$ over $\mathbb{Q}$.
  - The roots of this polynomial are $3^{1/4} \cdot i^k$ for $0 \leq k \leq 3$, and so the splitting field is $K = \mathbb{Q}(3^{1/4}, i)$, which has degree 8 over $\mathbb{Q}$ by similar arguments to those we have given.
  - Each automorphism of $K/\mathbb{Q}$ must map $3^{1/4}$ to one of the 4 roots of $x^4 - 3$, and must map i to one of the 2 roots of $x^2 + 1$.
  - Thus, since we know there are 8 automorphisms of $K/\mathbb{Q}$, all 8 choices must actually yield automorphisms.
  - One such automorphism is the map σ with $\sigma(3^{1/4}, i) = (3^{1/4}i,\ i)$, and another is the complex conjugation map τ with $\tau(3^{1/4}, i) = (3^{1/4}, -i)$.
  - We can then see that σ has order 4, τ has order 2, and $\sigma\tau = \tau\sigma^3$: hence the Galois group is isomorphic to the dihedral group $D_{2\cdot 4}$ of order 7, with σ corresponding to r and τ corresponding to s.
  - If we label the four roots$\{3^{1/4}, 3^{1/4}i, -3^{1/4}, -3^{1/4}i\}$ of $p(x)$ as $\{1, 2, 3, 4\}$, then σ corresponds to the permutation $(1\,2\,3\,4)$ and τ corresponds to the permutation $(2\,4)$.

- We can also analyze prime cyclotomic extensions and finite field extensions (we will return to these examples later in more depth):

- Example: If p is a prime, find the Galois group of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$.
  - As we have discussed, $K = \mathbb{Q}(\zeta_p)$ has degree $p - 1$ over $\mathbb{Q}$, and is the splitting field of the cyclotomic polynomial $\Phi_p(x) = \dfrac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$ whose roots are $\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}$. Thus, $\mathrm{Gal}(K/\mathbb{Q})$ has order $p - 1$.
  - Furthermore, any element $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ is determined by the value $\sigma(\zeta_p)$, which must be ζ_p^k for some integer k with $1 \leq k \leq p - 1$. Since there are at most $p - 1$ such maps, all of them must actually give rise to automorphisms.
  - Hence $\mathrm{Gal}(K/\mathbb{Q}) = \{\sigma_1, \sigma_2, \ldots, \sigma_{p-1}\}$ where $\sigma_a(\zeta_p) = \zeta_p^a$.
  - We can then compute $\sigma_a\sigma_b(\zeta_p) = \sigma_a(\zeta_p^b) = \zeta_p^{ab}$. Thus we see that $\sigma_a\sigma_b = \sigma_{ab}$, where we view the subscript modulo p. Hence the group structure of $\mathrm{Gal}(K/\mathbb{Q})$ is the same as the structure of the nonzero elements of $\mathbb{Z}/p\mathbb{Z}$ under multiplication.
  - Explicitly, this says that the map $\varphi : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathrm{Gal}(K/\mathbb{Q})$ given by $\varphi(a) = \sigma_a$ is an isomorphism.

- Since $(\mathbb{Z}/p\mathbb{Z})^\times$ is the multiplicative group of the field $\mathbb{F}_p$, which is a cyclic group, we conclude that $\mathrm{Gal}(K/\mathbb{Q})$ is a cyclic group of order $p-1$.

- Example: If p is a prime, find the Galois group of $\mathbb{F}_{p^n}/\mathbb{F}_p$.
  - We have previously shown that $K = \mathbb{F}_{p^n}$ is the splitting field of the separable polynomial $x^{p^n} - x$ over $\mathbb{F}_p$, and so the Galois group has order $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$.
  - We have also shown that the Frobenius map $\varphi : K \to K$ given by $\varphi(a) = a^p$ is an automorphism of K.
  - We can compute $\varphi^2(a) = \varphi(a^p) = a^{p^2}$, $\varphi^3(a) = \varphi(\varphi^2(a)) = \varphi(a^{p^2}) = a^{p^3}$, and in general $\varphi^k(a) = a^{p^k}$.
  - In particular, since every element of $\mathbb{F}_{p^n}$ is a root of $x^{p^n} - x$, we see that $\varphi^n(a) = a^{p^n} = a$ for every a, and so φ^n is the identity.
  - On the other hand, φ^k for $k < n$ cannot be the identity, since $\varphi^k(a) = a$ is the same as the polynomial equation $a^{p^k} - a = 0$, which can have at most $p^k < p^n$ roots in K.
  - Hence φ has order n in $\mathrm{Gal}(K/\mathbb{F}_p)$, but since $|\mathrm{Gal}(K/\mathbb{F}_p)| = n$, this means that $\mathrm{Gal}(K/\mathbb{F}_p)$ is cyclic and generated by φ.

4.1.4 Fixed Fields

- If K/F is a field extension, the automorphism group $\mathrm{Aut}(K/F)$ acts on elements on K.
  - If $\sigma \in \mathrm{Aut}(K/F)$ is a particular automorphism, consider the set of all elements of K stabilized by σ: it is a subset of K containing F (since all elements of F are fixed by σ) and is closed under subtraction and division, since if x, y are both fixed by σ then so are $x - y$ and x/y (the latter when $y \neq 0$).
  - Thus, the elements stabilized by σ is a subfield of K containing F, which we will call the fixed field of σ. In general, if E is a field with $F \subseteq E \subseteq K$, we call E an intermediate field of K/F.
  - Example: For $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$, if σ is the automorphism with $\sigma(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}$ for $a, b, c, d \in \mathbb{Q}$, then the elements of K fixed by σ are those of the form $a + c\sqrt{3}$. Thus the fixed field of σ is the subfield $\mathbb{Q}(\sqrt{3})$.
  - Example: For $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$, if $\sigma\tau$ is the automorphism with $\sigma\tau(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6}$ for $a, b, c, d \in \mathbb{Q}$, then the elements of K fixed by σ are those of the form $a + d\sqrt{6}$. Thus the fixed field of $\sigma\tau$ is the subfield $\mathbb{Q}(\sqrt{6})$.
  - Example: For $K = \mathbb{Q}(2^{1/4})/\mathbb{Q}$, if σ is the automorphism with $\sigma(2^{1/4}) = -2^{1/4}$, then $\sigma(a + b2^{1/4} + c\sqrt{2} + d2^{3/4}) = a - b2^{1/4} + c\sqrt{2} - d2^{3/4}$, then the elements of K fixed by σ are those of the form $a + c\sqrt{2}$. Thus the fixed field of σ is the subfield $\mathbb{Q}(\sqrt{2})$.

- More generally, we can consider subfields fixed by a collection of automorphisms:

- Definition: If K/F is a field extension and S is a set of automorphisms of K/F, then the fixed field of S is the subfield of K fixed by all automorphisms in S.
  - Note that the fixed field of S is the intersection of the fixed fields of all automorphisms in S, each of which is a subfield of K containing F, and so the fixed field of S is indeed a field (justifying the name).
  - Example: For $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$, if σ is the automorphism with $\sigma(\sqrt{2}, \sqrt{3}) = (-\sqrt{2}, \sqrt{3})$ and τ is the automorphism with $\tau(\sqrt{2}, \sqrt{3}) = (\sqrt{2}, -\sqrt{3})$, then the only elements of K fixed by both σ and τ are rational numbers, so the corresponding fixed field is $\mathbb{Q}$.
  - Notice that if σ and τ both fix the subfield E, then so do $\sigma\tau$ and σ^{-1}. Thus, since the identity also fixes E, we see that the collection of automorphisms fixing E is a subgroup of $\mathrm{Aut}(K/F)$.
  - It is then easy to see that the fixed field of S is the same as the fixed field of $\langle S \rangle$, the subgroup of $\mathrm{Aut}(K/F)$ generated by S. We may therefore restrict our focus to fixed fields of subgroups of $\mathrm{Aut}(K/F)$.
  - Example: For $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$, if σ is the automorphism with $\sigma(\sqrt{2}, \sqrt{3}) = (-\sqrt{2}, \sqrt{3})$ and τ is the automorphism with $\tau(\sqrt{2}, \sqrt{3}) = (\sqrt{2}, -\sqrt{3})$, then by our calculations above, the fixed fields of the possible subgroups $\{e\}$, $\langle\sigma\rangle$, $\langle\tau\rangle$, $\langle\sigma\tau\rangle$, and $\langle\sigma, \tau\rangle$ of $\mathrm{Aut}(K/\mathbb{Q})$ are $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{6})$, and $\mathbb{Q}$ respectively.

- Example: For $K = \mathbb{Q}(2^{1/4})/\mathbb{Q}$, if σ is the automorphism with $\sigma(2^{1/4}) = -2^{1/4}$ then the fixed fields of the possible subgroups $\{e\}$ and $\langle\sigma\rangle$ of $\mathrm{Aut}(K/\mathbb{Q})$ are $\mathbb{Q}(2^{1/4})$ and $\mathbb{Q}(\sqrt{2})$. Notice in particular that $\mathbb{Q}$ is not the fixed field of any subgroup of K, since the only nontrivial automorphism σ in $\mathrm{Aut}(K/\mathbb{Q})$ fixes all of $\mathbb{Q}(\sqrt{2})$.

- In more complicated examples, computing fixed fields ultimately reduces to solving a system of linear equations.
  - Explicitly, each automorphism of K/F acts as a linear transformation on K as an F-vector space.
  - If we fix a basis for K/F, determining the elements fixed by a linear transformation (or collection of linear transformations) is the same as solving the corresponding system of linear equations in the coefficients of the basis elements.
  - Thus, computing the fixed field of a subgroup is equivalent to solving a (possibly large) system of linear equations over F.
  - By our remarks above, the fixed field of a subgroup is the same as the fixed field for a set of its generators, so when actually computing fixed fields explicitly, we only need to solve the equations associated with the generators of the desired subgroup.

- Example: For $K = \mathbb{Q}(2^{1/3}, \zeta_3)/\mathbb{Q}$, find the fixed field of the subgroup $\langle\varphi\rangle$, where φ is the automorphism with $\varphi(2^{1/3}, \zeta_3) = (2^{1/3}\zeta_3, \zeta_3^2)$,
  - If we use the explicit basis $\{1, 2^{1/3}, 4^{1/3}, \zeta_3, 2^{1/3}\zeta_3, 4^{1/3}\zeta_3\}$ for K, then we can compute $\varphi(a + b2^{1/3} + c4^{1/3} + d\zeta_3 + e2^{1/3}\zeta_3 + f4^{1/3}\zeta_3) = a + b2^{1/3}\zeta_3 + c4^{1/3}\zeta_3^2 + d\zeta_3^2 + e2^{1/3} + f4^{1/3}\zeta_3$ for $a, b, c, d, e, f \in \mathbb{Q}$.
  - Since $\zeta_3^2 = -1 - \zeta_3$, rewriting in terms of the original basis yields $\varphi(a + b2^{1/3} + c4^{1/3} + d\zeta_3 + e2^{1/3}\zeta_3 + f4^{1/3}\zeta_3) = (a - d) + e2^{1/3} - c4^{1/3} - d\zeta_3 + b2^{1/3}\zeta_3 + (f - c)4^{1/3}\zeta_3$.
  - Hence the elements of the fixed field are the elements with $a = a - d$, $b = e$, $c = -c$, $d = -d$, $e = b$, and $f = f - c$.
  - These conditions reduce to $d = 0$, $c = 0$, and $b = e$, so the fixed field is the elements of the form $a + b(2^{1/3} + 2^{1/3}\zeta_3) + f(4^{1/3}\zeta_3) = a - b2^{1/3}\zeta_3^2 + f4^{1/3}\zeta_3$, which is the field $\mathbb{Q}(2^{1/3}\zeta_3^2)$.

- We can also invert this procedure and consider the collection of automorphisms in $\mathrm{Aut}(K/F)$ that fix a particular intermediate field E of K/F, which will simply be[2] the group $\mathrm{Aut}(K/E)$:
  - Example: For $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$, if E is the subfield $\mathbb{Q}(\sqrt{3})$, then there are two automorphisms of $K/\mathbb{Q}$ that fix E, namely the identity map and the automorphism τ with $\tau(\sqrt{2}, \sqrt{3}) = (-\sqrt{2}, \sqrt{3})$.
  - Example: For $K = \mathbb{Q}(2^{1/3}, \zeta_3)/\mathbb{Q}$, if E is the subfield $\mathbb{Q}(\zeta_3)$, then the subgroup of $\mathrm{Aut}(K/\mathbb{Q})$ fixing E is $\langle\sigma\rangle$, where σ is the automorphism with $\sigma(2^{1/3}, \zeta_3) = (2^{1/3}\zeta_3, \zeta_3)$. To see this observe that σ does fix E, hence so does $\langle\sigma\rangle$, and each of the other automorphisms of K map ζ_3 to ζ_3^2 hence do not fix E.
  - Example: For $K = \mathbb{Q}(2^{1/4})/\mathbb{Q}$, if E is the subfield $\mathbb{Q}(\sqrt{2})$, then the subgroup of $\mathrm{Aut}(K/\mathbb{Q})$ fixing E is all of $\mathrm{Aut}(K/\mathbb{Q})$. If $E = \mathbb{Q}$, then the subgroup of $\mathrm{Aut}(K/\mathbb{Q})$ fixing E is also all of $\mathrm{Aut}(K/\mathbb{Q})$.

- We now have two operations that relate subgroups of $\mathrm{Aut}(K/F)$ to intermediate fields of K/F: to a subgroup we associate its corresponding fixed field, and to an intermediate field we associate the subgroup stabilizing it.
  - Observe that each of these operations is inclusion-reversing.
  - Explicitly, if E_1 and E_2 are two intermediate fields of K/F with $E_1 \subseteq E_2$, then $\mathrm{Aut}(K/E_2) \subseteq \mathrm{Aut}(K/E_1)$, since any automorphism that fixes E_2 automatically fixes the subfield E_1 as well.
  - In the other direction, if H_1 and H_2 are subgroups of $\mathrm{Aut}(K/F)$ with $H_1 \subseteq H_2$, then the corresponding fixed fields F_1 and F_2 have $F_2 \subseteq F_1$, since any automorphism in H_1 (i.e., fixing F_1) by assumption is also in H_2 (i.e., fixes F_2).

- It is natural to ask how these maps relate to one another (and in particular, whether they are inverses).

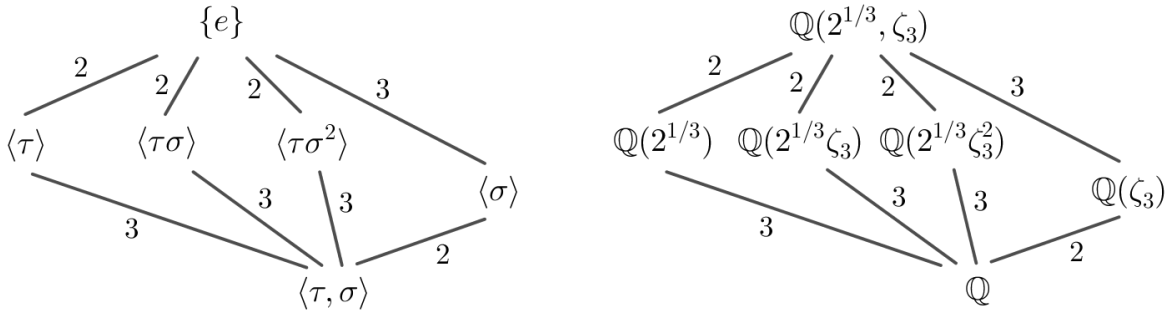
[2] Note that this is also the stabilizer of E under the group action of $\mathrm{Aut}(K/F)$ on subsets of K.

- ◦ Example: For $\mathbb{Q}(\sqrt{2},\sqrt{3})$, the fixed fields of the possible subgroups $\{e\}$, $\langle\sigma\rangle$, $\langle\tau\rangle$, $\langle\sigma\tau\rangle$, and $\langle\sigma,\tau\rangle$ of $\mathrm{Aut}(K/\mathbb{Q})$ are $\mathbb{Q}(\sqrt{2},\sqrt{3})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{6})$, and $\mathbb{Q}$ respectively. Inversely, the automorphism groups $\mathrm{Aut}(K/E)$ for each of the subfields $\mathbb{Q}(\sqrt{2},\sqrt{3})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{6})$, and $\mathbb{Q}$ are $\{e\}$, $\langle\sigma\rangle$, $\langle\tau\rangle$, $\langle\sigma\tau\rangle$, and $\langle\sigma,\tau\rangle$ respectively. Thus, the two maps are inverses for $\mathbb{Q}(\sqrt{2},\sqrt{3})$, at least for all of the subfields we have listed (we will later show that these are in fact all of the subfields of K).
- ◦ Example: For $K=\mathbb{Q}(2^{1/4})/\mathbb{Q}$, the fixed fields of the subgroups $\{e\}$ and $\langle\sigma\rangle$ of $\mathrm{Aut}(K/\mathbb{Q})$ are $\mathbb{Q}(2^{1/4})$ and $\mathbb{Q}(\sqrt{2})$ respectively. Inversely, the automorphism groups $\mathrm{Aut}(K/E)$ for each of the intermediate fields $\mathbb{Q}(2^{1/4})$, $\mathbb{Q}(\sqrt{2})$, and $\mathbb{Q}$ are $\{e\}$, $\langle\sigma\rangle$, and $\langle\sigma\rangle$ respectively. Here, the two maps are not inverses: although the fixed field map on subgroups is injective, the subfields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}$ both have automorphism group $\langle\sigma\rangle$.
- ◦ Example: For $K=\mathbb{Q}(2^{1/3})/\mathbb{Q}$, the fixed field of $\mathrm{Aut}(K/\mathbb{Q})$, which is the trivial group, is $\mathbb{Q}(2^{1/3})$. The corresponding automorphism groups for both intermediate fields $\mathbb{Q}(2^{1/3})$ and $\mathbb{Q}$ are the full automorphism group.
- ◦ Note that the field in the first example was a Galois extension (i.e., a splitting field of a separable polynomial), while the fields in the second and third examples were not. In those two examples, $\mathrm{Aut}(K/\mathbb{Q})$ did not have "enough automorphisms" to ensure that the fixed field of $\mathrm{Aut}(K/\mathbb{Q})$ is actually $\mathbb{Q}$ rather than a larger subfield.

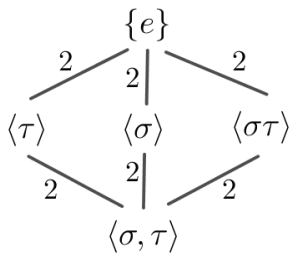
- Our goal in the next section is to show that these two maps are in fact inverses when the extension K/F is Galois, and to elucidate the associated "Galois correspondence" between subgroups of $\mathrm{Gal}(K/F)$ and intermediate fields of K/F in that case.

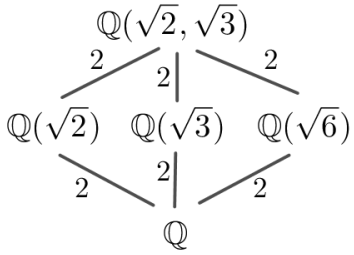
4.2 The Fundamental Theorem of Galois Theory

- As we have described, when K/F is a Galois extension there appears to be a natural inclusion-reversing correspondence between subgroups of the automorphism group $\mathrm{Gal}(K/F)$ and intermediate fields E of K/F.
  - ◦ For $K=\mathbb{Q}(2^{1/3},\zeta_3)/\mathbb{Q}$, with the automorphisms $\sigma(2^{1/3},\zeta_3)=(2^{1/3}\zeta_3,\zeta_3)$ and $\tau(2^{1/3},\zeta_3)=(2^{1/3},\zeta_3^2)$ we have previously described, the fixed fields of the subgroups $\{e\}$, $\langle\tau\rangle$, $\langle\tau\sigma\rangle$, $\langle\tau\sigma^2\rangle$, $\langle\sigma\rangle$, and $\langle\tau,\sigma\rangle$ are respectively $\mathbb{Q}(2^{1/3},\zeta_3)$, $\mathbb{Q}(2^{1/3})$, $\mathbb{Q}(2^{1/3}\zeta_3)$, $\mathbb{Q}(2^{1/3}\zeta_3^2)$, $\mathbb{Q}(\zeta_3)$, and $\mathbb{Q}$. Conversely, the automorphism groups $\mathrm{Aut}(K/E)$ fixing those six intermediate fields are precisely those subgroups of $\mathrm{Gal}(K/\mathbb{Q})$ in that order.
  - ◦ This correspondence is particularly obvious when comparing subgroup and subfield diagrams: here are the corresponding subgroup and subfield diagrams for $\mathbb{Q}(2^{1/3},\zeta_3)/\mathbb{Q}$ (where we have also labeled the diagrams with the relative extension degrees and subgroup indices and drawn the subgroup diagram upside-down):



  - ◦ For another example, if we take $K=\mathbb{Q}(\sqrt{2},\sqrt{3})$ with the automorphisms $\sigma(\sqrt{2},\sqrt{3})=(-\sqrt{2},\sqrt{3})$ and $\tau(\sqrt{2},\sqrt{3})=(\sqrt{2},-\sqrt{3})$, then the fixed fields of the subgroups $\{e\}$, $\langle\sigma\rangle$, $\langle\tau\rangle$, $\langle\sigma\tau\rangle$, and $\langle\sigma,\tau\rangle$ are $\mathbb{Q}(\sqrt{2},\sqrt{3})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{6})$, and $\mathbb{Q}$ respectively. Conversely, the automorphism groups $\mathrm{Aut}(K/E)$ fixing those five intermediate fields are precisely those subgroups of $\mathrm{Gal}(K/\mathbb{Q})$ in that order, yielding the correspondences of the subgroup and subfield diagrams:





- We will also remark that for $\mathbb{Q}(2^{1/3}, \zeta_3)/\mathbb{Q}$, there are three subfields that are Galois over $\mathbb{Q}$, namely $\mathbb{Q}(2^{1/3}, \zeta_3)$, $\mathbb{Q}(\zeta_3)$, and $\mathbb{Q}$. The corresponding subgroups are $\{e\}$, $\langle\sigma\rangle$, and $\langle\sigma, \tau\rangle$, and these are precisely the normal subgroups of $\mathrm{Gal}(\mathbb{Q}(2^{1/3}, \zeta_3)/\mathbb{Q})$. On the other hand, for $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$, all of the subfields are Galois over $\mathbb{Q}$, and all of the corresponding subgroups are normal.

- Our goal in this section is to describe some characterizations of Galois extensions, and then show that all of these properties will hold for arbitrary (finite-degree) Galois extensions K/F:

- Theorem (Characterizations of Galois Extensions): If K/F is a field extension, the following are equivalent:

  1. K/F is Galois, which is to say, it has finite degree and $|\mathrm{Aut}(K/F)| = [K : F]$.
  2. K/F is the splitting field of some separable polynomial in $F[x]$.
  3. F is the fixed field of $\mathrm{Aut}(K/F)$.
  4. K/F is a normal, finite, and separable extension. (Equivalently: $[K : F]$ is finite, and if $p(x)$ is irreducible in $F[x]$ but has a root in K, then $p(x)$ splits completely with distinct roots over K.)

- Theorem (Fundamental Theorem of Galois Theory): Let K/F be a Galois extension and let $G = \mathrm{Gal}(K/F)$. Then there is an inclusion-reversing bijection between intermediate fields E of K/F and subgroups H of G, given by associating a subgroup H to its fixed field E. Under this correspondence, if the subgroup H corresponds to the field E, then

  1. Subgroup indices correspond to extension degrees, so that $[K : E] = |H|$ and $[E : F] = |G : H|$.
  2. The extension K/E is always Galois, with Galois group H.
  3. If $\overline{F}$ is a fixed algebraic closure of F, then the embeddings of E into F are in bijection with the left cosets of H in G.
  4. The extension E/F is Galois if and only if H is a normal subgroup of G, and in such a case, $\mathrm{Gal}(E/F)$ is isomorphic to G/H.
  5. Intersections of subgroups correspond to joins of fields, and joins of subgroups correspond to intersections of fields: $H_1 \cap H_2$ corresponds to E_1E_2, while $\langle H_1, H_2\rangle$ corresponds to $E_1 \cap E_2$.
  6. The lattice of subgroups of G is the same as the lattice of intermediate fields of K/F turned upside-down.

4.2.1 Characterizations of Galois Extensions

- We will first establish the characterization of Galois extensions given above. First we show that distinct automorphisms are linearly independent as functions:

- Proposition (Independence of Automorphisms): If $\sigma_1, \sigma_2, \ldots, \sigma_n$ are distinct embeddings of a field K into a field L, then they are linearly independent as functions on K. In particular, distinct automorphisms of K are linearly independent as functions.

  - Proof: We show the result by induction on n. The base case $n = 1$ is trivial, since any embedding of a field is nonzero (since it is injective).
  - Now suppose that $n > 1$ and let $\sigma_1, \sigma_2, \ldots, \sigma_n$ be distinct automorphisms with a dependence relation $a_1\sigma_1 + a_2\sigma_2 + \cdots + a_n\sigma_n = 0$ with the $a_i \in L$: explicitly, this means that for any $x \in K$ we have $a_1\sigma_1(x) + a_2\sigma_2(x) + \cdots + a_n\sigma_n(x) = 0$.

- Since $\sigma_1 \neq \sigma_2$, there exists $y \in K$ such that $\sigma_1(y) \neq \sigma_2(y)$, where we note that $y \neq 0$.
- By the dependence relation, we see $a_1\sigma_1(xy) + a_2\sigma_2(xy) + \cdots + a_n\sigma_n(xy) = 0$, so that $a_1\sigma_1(x)\sigma_1(y) + a_2\sigma_2(x)\sigma_2(y) + \cdots + a_n\sigma_n(x)\sigma_n(y) = 0$.
- By taking a linear combination of this equation with the original dependence, we may cancel the leading coefficient to obtain the dependence $a_2\sigma_2(x)[\sigma_1(y) - \sigma_2(y)] + \cdots + a_n\sigma_n(x)[\sigma_1(y) - \sigma_n(y)] = 0$ for all x.
- By the inductive hypothesis, all of the coefficients $a_i[\sigma_1(y) - \sigma_i(y)]$ must then be zero, so in particular $a_2[\sigma_1(y) - \sigma_2(y)] = 0$. Since $\sigma_1(y) \neq \sigma_2(y)$ this implies $a_2 = 0$.
- But then the original dependence relation becomes $a_1\sigma_1(x) + a_3\sigma_3(x) + \cdots + a_n\sigma_n(x) = 0$, so again by the inductive hypothesis, all of the remaining a_i are zero.
- Thus, $\sigma_1, \sigma_2, \ldots, \sigma_n$ are linearly independent as functions on K, as claimed.

- We can use the independence of automorphisms to compute the degree of the field fixed by a subgroup of $\mathrm{Gal}(K/F)$:

- Theorem (Degree of Fixed Fields): Suppose K/F is a finite-degree field extension and H is a subgroup of $\mathrm{Aut}(K/F)$. If E is the fixed field of H, then $[K : E] = |H|$.

  - Proof: Suppose $H = \{\sigma_1, \sigma_2, \ldots, \sigma_h\}$, and also that $[K : E] = d$. Let $v_1, v_2, \ldots, v_d$ be a basis for K/E.
  - First we will show that if $d < h$, then the automorphisms $\sigma_1, \ldots, \sigma_h$ are linearly independent (which will contradict the proposition above).
  - So suppose $n < h$. Then by standard properties of systems of linear equations, the homogeneous system of n equations in h variables

$$\begin{aligned} \sigma_1(v_1)x_1 + \sigma_2(v_1)x_2 + \cdots + \sigma_h(v_1)x_h &= 0 \\ \sigma_1(v_2)x_1 + \sigma_2(v_2)x_2 + \cdots + \sigma_h(v_2)x_h &= 0 \\ &\vdots \quad \vdots \quad \vdots \\ \sigma_1(v_d)x_1 + \sigma_2(v_d)x_2 + \cdots + \sigma_h(v_d)x_h &= 0 \end{aligned}$$

    over K has a nonzero solution $(x_1, x_2, \ldots, x_h) = (c_1, c_2, \ldots, c_h)$ for $c_i \in K$.
  - Then for any $a_1, a_2, \ldots, a_d \in F$, adding a_i times the ith equation above yields the relation

$$[a_1\sigma_1(v_1) + a_2\sigma_1(v_2) + \cdots + a_d\sigma_1(v_d)]c_1 + \cdots + [a_1\sigma_h(v_1) + a_2\sigma_h(v_2) + \cdots + a_d\sigma_h(v_d)]c_h = 0$$

    and since the σ_i fix each of the constants a_i, if we write $w = a_1v_1 + a_2v_2 + \cdots + a_dv_d$, this says that

$$\sigma_1(w)c_1 + \sigma_2(w)c_2 + \cdots + \sigma_h(w)c_h = 0.$$

  - But since the a_i are arbitrary elements of F and the v_i are a basis for K/E, we see that the relation above holds for every $w \in K$, meaning that it is a linear dependence of the σ_j.
  - But this is impossible by the previous proposition, so we must have $h \leq d$. Now we will show $h = d$, so suppose instead that $h < d$, and let $v_1, v_2, \ldots, v_{h+1}$ be F-linearly independent elements of K.
  - Now consider the solutions $(x_1, x_2, \ldots, x_{h+1}) = (\alpha_1, \ldots, \alpha_{h+1})$ to the following homogeneous system:

$$\begin{aligned} \sigma_1(v_1)x_1 + \sigma_1(v_2)x_2 + \cdots + \sigma_1(v_{h+1})x_{h+1} &= 0 \\ \sigma_2(v_1)x_1 + \sigma_2(v_2)x_2 + \cdots + \sigma_2(v_{h+1})x_{h+1} &= 0 \\ &\vdots \quad \vdots \quad \vdots \\ \sigma_h(v_1)x_h + \sigma_h(v_2)x_2 + \cdots + \sigma_h(v_{h+1})x_{h+1} &= 0. \end{aligned}$$

    Since there are more variables than equations, there is at least one nonzero solution $(\alpha_1, \ldots, \alpha_{n+1})$ in K.
  - Now we will exploit the group action of the σ_i to show that the existence of a nonzero solution in K implies the existence of a nonzero solution with all the $\alpha_i \in E$, which will then contradict the linear independence of the v_i: if all the α_i are in E then they are fixed by all the σ_j, so the first equation of the system would give an F-linear dependence of the x_i over K, contrary to assumption.

- So suppose $(\alpha_1, \ldots, \alpha_{h+1})$ is a nonzero solution to the system. We show by induction on k that there is a solution to the system with k elements in E.
- For the base case $k = 1$, choose any nonzero α_i and rescale the solution so that $\alpha_i = 1$.
- For the inductive step, suppose (after relabeling and rescaling if necessary) that $\alpha_1, \ldots, \alpha_k$ are in E with $\alpha_k = 1$. If all the α_i are in E we are done, so assume $\alpha_{k+1} \notin E$. Then the system is

$$\begin{aligned}
\sigma_1(v_1\alpha_1 + \cdots + v_{k-1}\alpha_{k-1}) + \sigma_1(v_k) + \sigma_1(v_{k+1})\alpha_{k+1} + \cdots + \sigma_1(v_{h+1})\alpha_{h+1} &= 0 \\
\sigma_2(v_1\alpha_1 + \cdots + v_{k-1}\alpha_{k-1}) + \sigma_2(v_k) + \sigma_2(v_{k+1})\alpha_{k+1} + \cdots + \sigma_2(v_{h+1})\alpha_{h+1} &= 0 \\
&\vdots \quad \vdots \quad \vdots \\
\sigma_h(v_1\alpha_1 + \cdots + v_{k-1}\alpha_{k-1}) + \sigma_h(v_k) + \sigma_h(v_{k+1})\alpha_{k+1} + \cdots + \sigma_h(v_{h+1})\alpha_{h+1} &= 0.
\end{aligned}$$

- Now since $\alpha_{k+1} \notin E$, by the assumption that E is the fixed field of H, there is some $\tau \in H$ with $\tau(\alpha_{k+1}) \neq \alpha_{k+1}$. If we apply τ to each of the equations above, then because H is a group, the elements $\{\sigma_1, \ldots, \sigma_h\}$ are merely permuted by left-multiplication by τ. If we permute the equations back into their original order, we obtain the following system:

$$\begin{aligned}
\sigma_1(v_1\alpha_1 + \cdots + v_{k-1}\alpha_{k-1}) + \sigma_1(v_k) + \sigma_1(v_{k+1})\tau(\alpha_{k+1}) + \cdots + \sigma_1(v_{h+1})\tau(\alpha_{h+1}) &= 0 \\
\sigma_2(v_1\alpha_1 + \cdots + v_{k-1}\alpha_{k-1}) + \sigma_2(v_k) + \sigma_2(v_{k+1})\tau(\alpha_{k+1}) + \cdots + \sigma_2(v_{h+1})\tau(\alpha_{h+1}) &= 0 \\
&\vdots \quad \vdots \quad \vdots \\
\sigma_h(v_1\alpha_1 + \cdots + v_{k-1}\alpha_{k-1}) + \sigma_h(v_k) + \sigma_h(v_{k+1})\tau(\alpha_{k+1}) + \cdots + \sigma_h(v_{h+1})\tau(\alpha_{h+1}) &= 0.
\end{aligned}$$

- Now subtract this system from the original one: this yields

$$\begin{aligned}
\sigma_1(v_{k+1})[\alpha_{k+1} - \tau(\alpha_{k+1})] + \cdots + \sigma_1(v_{h+1})[\alpha_{h+1} - \tau(\alpha_{h+1})] &= 0 \\
\sigma_2(v_{k+1})[\alpha_{k+1} - \tau(\alpha_{k+1})] + \cdots + \sigma_2(v_{h+1})[\alpha_{h+1} - \tau(\alpha_{h+1})] &= 0 \\
&\vdots \quad \vdots \quad \vdots \\
\sigma_h(v_{k+1})[\alpha_{k+1} - \tau(\alpha_{k+1})] + \cdots + \sigma_h(v_{h+1})[\alpha_{h+1} - \tau(\alpha_{h+1})] &= 0.
\end{aligned}$$

  and so we obtain a new solution to the system, namely $(0, 0, \ldots, 0, \alpha_{k+1} - \tau(\alpha_{k+1}), \ldots, \alpha_{h+1} - \tau(\alpha_{h+1}))$, which is nonzero since $\alpha_{k+1} - \tau(\alpha_{k+1}) \neq 0$, and which has at least k entries in E.
- Hence by induction, we obtain a solution which has all its entries in E. But then this would contradict the assumption that the v_i are linearly independent, which is impossible. Thus we must have $n = h$, meaning that $[K : E] = |H|$.

- Now we may establish the characterizations of Galois extensions described earlier:
- Theorem (Characterizations of Galois Extensions): If K/F is a field extension, the following are equivalent:

1. K/F is Galois, which is to say, it has finite degree and $|\mathrm{Aut}(K/F)| = [K : F]$.
2. K/F is the splitting field of some separable polynomial in $F[x]$.
3. F is the fixed field of $\mathrm{Aut}(K/F)$.
4. K/F is a normal, finite, and separable extension. (Equivalently: $[K : F]$ is finite, and if $p(x)$ is irreducible in $F[x]$ but has a root in K, then $p(x)$ splits completely with distinct roots over K.)

- Proof: We have previously shown that (2) implies (1) and that (2) implies (4).
- (4) implies (2): If K/F is a finite-degree extension then $K = F(\alpha_1, \ldots, \alpha_n)$ for some α_i algebraic over F. If $m_i(x)$ is the minimal polynomial of α_i, then since K/F is separable, each of the m_i is separable, and since K/F is normal, each of the other roots of the m_i is in K. Now let $m(x)$ be the least common multiple of the m_i: then m is separable and all of its roots are in K and generate K/F, so K/F is the splitting field of $m(x)$.
- (1) is equivalent to (3): If E is the fixed field of $\mathrm{Aut}(K/F)$, then by our theorem on the degrees of fixed fields, $|\mathrm{Aut}(K/F)| = [K : E] = [K : F]/[E : F]$. Thus $|\mathrm{Aut}(K/F)| = [K : F]$ if and only if $[E : F] = 1$, which is to say, if and only if F is the fixed field of $\mathrm{Aut}(K/F)$.

- (1) implies (4): Suppose K/F is Galois: then K/F is finite and separable. Now suppose that $p(x) \in F[x]$ is irreducible and has a root $\alpha \in K$. Let $\text{Gal}(K/F) = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ and consider the values $\sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_n(\alpha)$. By reordering, assuming that $\sigma_1(\alpha), \ldots, \sigma_k(\alpha)$ are distinct and that the others are duplicates.
- Now consider the polynomial $q(x) = (x - \sigma_1(\alpha))(x - \sigma_2(\alpha)) \cdots (x - \sigma_k(\alpha)) \in K[x]$. Notice that $q(x)$ is separable by the hypothesis that $\sigma_1(\alpha), \ldots, \sigma_k(\alpha)$ are distinct, and that α is among the $\sigma_i(\alpha)$ since the identity map is an automorphism
- For each $\tau \in \text{Gal}(K/F)$, notice that τ permutes the values $\sigma_1(\alpha), \ldots, \sigma_k(\alpha)$, and therefore it fixes each of the coefficients of $q(x)$, since these are symmetric functions in $\sigma_1(\alpha), \ldots, \sigma_k(\alpha)$.
- Since K/F is Galois and (1) implies (3) by the above, the fact that every coefficient of $q(x)$ is fixed by every element of $\text{Gal}(K/F)$ implies that they are all in F, so in fact $q(x) \in F[x]$.
- Then $q(x)$ is a polynomial in $F[x]$ having α as a root, so it is divisible by the minimal polynomial $p(x)$ of α.
- On the other hand, since α is a root of $p(x) \in F[x]$, the elements $\sigma_1(\alpha), \ldots, \sigma_k(\alpha)$ are all roots of $p(x)$ as well, so $q(x)$ divides $p(x)$. Hence in fact $p(x) = q(x)$, whence the roots of $p(x)$ are all in K. Thus K/F is normal, so we are done.

- In the proof above, the elements $\sigma(\alpha)$ for $\sigma \in \text{Gal}(K/F)$ played a crucial role, and they will show up very often:

- Definition: If K/F is a Galois extension and $\alpha \in K$, the elements $\sigma(\alpha)$ for $\sigma \in \text{Gal}(K/F)$ are called (Galois) conjugates of α over F. If E is an intermediate field of K/F, the field $\sigma(E) = \{\sigma(\alpha) : \alpha \in E\}$ is called a (Galois) conjugate field of E over F.

- We will show later that if the subfield E corresponds to the subgroup H of $\text{Gal}(K/F)$, then the Galois conjugate field $\sigma(E)$ corresponds to the conjugate subgroup $\sigma H \sigma^{-1}$ (thus justifying the use of the same word "conjugate" in this context).
- Example: For $\mathbb{Q}(2^{1/3}, \zeta_3)/\mathbb{Q}$, the Galois conjugates of $2^{1/3}$ are $2^{1/3}$, $2^{1/3}\zeta_3$, and $2^{1/3}\zeta_3^2$, while the Galois conjugates of $2^{1/3} + \zeta_3$ are $2^{1/3} + \zeta_3$, $2^{1/3}\zeta_3 + \zeta_3$, $2^{1/3}\zeta_3^2 + \zeta_3$, $2^{1/3} + \zeta_3^2$, $2^{1/3}\zeta_3 + \zeta_3^2$, and $2^{1/3}\zeta_3^2 + \zeta_3^2$.
- The proof we gave above showed, along the way, that the Galois conjugates of α over F are the roots of the minimal polynomial of α over F. (Roughly speaking, Galois conjugates are "algebraically indistinguishable" over F, the indistinguishability being provided by the automorphism σ.)
- In particular, if we have an explicit description of the Galois group's action on K/F, then we can easily find the minimal polynomial of an arbitrary element of K (and its degree) by computing its Galois conjugates.
- Example: The Galois conjugates of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$ are $\sqrt{2} + \sqrt{3}$, $\sqrt{2} - \sqrt{3}$, $-\sqrt{2} + \sqrt{3}$, and $-\sqrt{2} - \sqrt{3}$. Thus, the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$ has degree 4, and is given explicitly by $p(x) = (x - \sqrt{2} - \sqrt{3})(x - \sqrt{2} + \sqrt{3})(x + \sqrt{2} - \sqrt{3})(x + \sqrt{2} + \sqrt{3}) = x^4 - 10x^2 + 1$.

4.2.2 Proof of the Fundamental Theorem

- We have now developed enough to prove the fundamental theorem of Galois theory:

- Theorem (Fundamental Theorem of Galois Theory): Let K/F be a Galois extension and let $G = \text{Gal}(K/F)$. Then there is an inclusion-reversing bijection between intermediate fields E of K/F and subgroups H of G, given by associating a subgroup H to its fixed field E. Under this correspondence, if the subgroup H corresponds to the field E, then

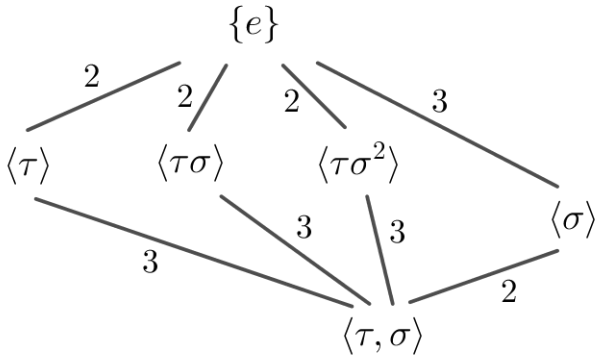
1. Subgroup indices correspond to extension degrees, so that $[K : E] = |H|$ and $[E : F] = |G : H|$.
2. The extension K/E is always Galois, with Galois group H.
3. For any $\sigma \in G$, the subfield $\sigma(E)$ corresponds to the subgroup $\sigma H \sigma^{-1}$.
4. The extension E/F is Galois if and only if H is a normal subgroup of G, and in such a case, $\text{Gal}(E/F)$ is isomorphic to G/H.

5. Intersections of subgroups correspond to joins of fields, and joins of subgroups correspond to intersections of fields: $H_1 \cap H_2$ corresponds to E_1E_2, while $\langle H_1, H_2\rangle$ corresponds to $E_1 \cap E_2$.
6. The lattice of subgroups of G is the same as the lattice of intermediate fields of K/F turned upside-down.

- We will establish several of the calculation parts first before showing that correspondence maps are actually inverses of one another.
- Proof (1): Suppose that H is a subgroup of G and let E be the fixed field of H. By definition E is fixed by every element of H, so H is contained in $\mathrm{Aut}(K/E)$ so in particular $|H| \leq |\mathrm{Aut}(K/E)|$.
- But we also know that $|\mathrm{Aut}(K/E)| \leq [K : E] = |H|$ from our previous results, so we must in fact have $|H| = |\mathrm{Aut}(K/E)| = [K : E]$.
- For the other statement we have seen that F is the fixed field of $\mathrm{Gal}(K/F)$, and so $[K : F] = |G|$. Then dividing this relation by the one above immediately yields $[E : F] = |G : H|$, by the definition of the index of a subgroup and the degree tower formula.
- Proof (2): Suppose that H is a subgroup of G and let E be the fixed field of H. As calculated above, we have $|H| = |\mathrm{Aut}(K/E)| = [K : E]$, so K/E is Galois. Furthermore, since everything is finite this forces $H = \mathrm{Aut}(K/E) = \mathrm{Gal}(K/E)$ as claimed.
- Proof (0): For surjectivity of the fixed field map, suppose E is an intermediate field. As we have shown above, K/E is Galois with Galois group $\mathrm{Aut}(K/E)$. But by our characterization of Galois extensions, this means E is the fixed field of the subgroup $\mathrm{Aut}(K/E)$ of G.
- For injectivity, suppose that H_1 and H_2 are subgroups of G with respective fixed fields E_1 and E_2. If $E_1 = E_2$, then E_1 is fixed by H_2, so since $\mathrm{Aut}(K/E_1) = H_1$ from (2) above, this means $H_2 \leq H_1$. Conversely, since E_2 is fixed by H_1, then by the same argument we have $H_1 \leq H_2$, so $H_1 = H_2$.
- Finally, the correspondences are inverse to one another because the automorphisms fixing E are precisely $\mathrm{Aut}(K/E)$, again by the above.
- Proof (3): Suppose that the subgroup corresponding to $\sigma(E)$ is H'. For $\sigma \in G$ observe that for any $\alpha \in E$ and $h \in H$, we have $(\sigma h \sigma^{-1})(\sigma(\alpha)) = \sigma(h(\sigma^{-1}(\sigma(\alpha)))) = \sigma(h(\alpha)) = \sigma(\alpha)$ since h fixes α by assumption. This means that every element of $\sigma H \sigma^{-1}$ fixes $\sigma(E)$, and so $\sigma H \sigma^{-1} \leq H'$.
- Since E/F and $\sigma(E)/F$ are isomorphic (via σ), we have $[E : F] = [\sigma(E) : F]$, whence $[K : E] = [K : \sigma(E)]$, and then by (1) we see that $\left|\sigma H \sigma^{-1}\right| = |H| = |H'|$. Since both groups are finite we therefore have $\sigma H \sigma^{-1} = H'$ as claimed.
- Proof (4): First observe that the statement that $\sigma(E) = E$ for all $\sigma \in G$ is equivalent to saying that E is normal (since for any $\alpha \in E$, the Galois conjugates $\sigma(\alpha) \in E$ are the other roots of the minimal polynomial of α, so E is normal precisely when all $\sigma(\alpha)$ are also in E). Then since K/F is Galois, it is finite-degree and separable, so E/F is also finite-degree and separable.
- Then since the Galois correspondence is a bijection, we see that $\sigma(E) = E$ for all $\sigma \in G$ if and only if $\sigma H \sigma^{-1} = H$ for all $\sigma \in G$. Hence E is Galois over F if and only if H is normal in G, as claimed.
- If H is normal in G, then we may view a left coset σH as acting on E via $(\sigma H) \cdot E = \sigma(E)$. It is easy to see that this action is well-defined and faithful, and since $|\mathrm{Gal}(E/F)| = |G : H|$ from (1), the corresponding association of σH with the automorphism σ of E yields an isomorphism of $\mathrm{Gal}(E/F)$ with the quotient group G/H.
- Proof (5): Suppose that H_1 and H_2 are subgroups of G with respective fixed fields E_1 and E_2. Then any element in $H_1 \cap H_2$ fixes both E_1 and E_2 hence fixes everything in E_1E_2 (since the elements of the composite field are rational functions of elements of E_1 and E_2). Conversely any automorphism fixing E_1E_2 must in particular fix both E_1 and E_2 hence be contained in $H_1 \cap H_2$. Thus, $H_1 \cap H_2$ corresponds to E_1E_2.
- Likewise, $E_1 \cap E_2$ is fixed by any element in H_1 or H_2, hence also by any word in such elements, so $\langle H_1, H_2\rangle$ fixes $E_1 \cap E_2$. Inversely, if σ is any automorphism that does not fix $E_1 \cap E_2$, then for any $h \in H_1 \cup H_2$ we see that σh also does not fix $E_1 \cap E_2$, so by an easy induction argument on the word length, we see that σ cannot be written as a word in $\langle H_1, H_2\rangle$. Thus, $\langle H_1, H_2\rangle$ corresponds to $E_1 \cap E_2$.
- Proof (6): This follows immediately from (1), (5), and the fact that the Galois correspondence is inclusion-reversing.

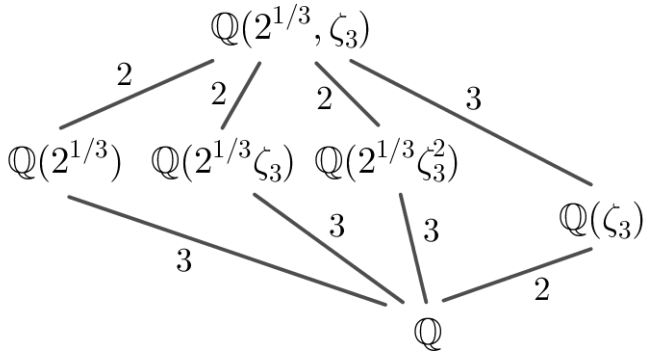
4.2.3 Examples of the Fundamental Theorem

- We may use the fundamental theorem of Galois theory to extract quite a lot of new information about field extensions.
  - First, if K/F is Galois, then subgroups of the Galois group correspond to intermediate fields, so in particular we can find all of the intermediate fields of K/F by computing the fixed field for each subgroup (note that we have previously described how to reduce the computation of fixed fields to solving a system of linear equations). Then we can draw the full subfield lattice for K/F using only the subgroup lattice of $\mathrm{Gal}(K/F)$.
  - More generally, even if K/F is not Galois, if it is finite-degree and separable then we know $K = F(\alpha_1, \ldots, \alpha_n)$ for some algebraic α_i whose minimal polynomials are separable. Then the splitting field of the lcm of these minimal polynomials $\hat{K}$ is Galois over K: then as above we can find all of the intermediate fields of $\hat{K}/F$, which will in particular identify all of the intermediate fields of K/F.
  - Also, as we described earlier, we can use the Galois action to compute Galois conjugates of elements, which will give us information about minimal polynomials.
- Example: Identify all of the intermediate fields of $\mathbb{Q}(2^{1/3}, \zeta_3)/\mathbb{Q}$ and then draw the subfield lattice.
  - We have done all of these calculations in various pieces already, but let us describe how to do them more systematically using the fundamental theorem.
  - We know that $K = \mathbb{Q}(2^{1/3}, \zeta_3)/\mathbb{Q}$ is Galois since it is the splitting field of $x^3 - 2$ over $\mathbb{Q}$, and so we know that $|\mathrm{Gal}(K/\mathbb{Q})| = 6$. Any automorphism must map $2^{1/3}$ to one of its Galois conjugates $2^{1/3}$, $2^{1/3}\zeta_3$, $2^{1/3}\zeta_3^2$ and likewise must map ζ_3 to one of its Galois conjugates ζ_3, ζ_3^2.
  - Since there are only six possibilities we conclude that all six yield automorphisms of $K/\mathbb{Q}$.
  - With $\sigma(2^{1/3}, \zeta_3) = (2^{1/3}\zeta_3, \zeta_3)$ and $\tau(2^{1/3}, \zeta_3) = (2^{1/3}, \zeta_3^2)$, we can verify (as previously) that $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to $D_{2\cdot 3}$ with σ behaving as r and τ behaving as s, and also isomorphic to S_3 via the permutation action on $\{2^{1/3}, 2^{1/3}\zeta_3, 2^{1/3}\zeta_3^2\}$ with σ behaving as $(1\,2\,3)$ and τ behaving as $(2\,3)$.
  - From our knowledge of the dihedral group, we know it has subgroups $\{e\}$, $\langle\tau\rangle$, $\langle\tau\sigma\rangle$, $\langle\tau\sigma^2\rangle$, $\langle\sigma\rangle$, and $\langle\sigma, \tau\rangle$, and can draw the corresponding lattice:

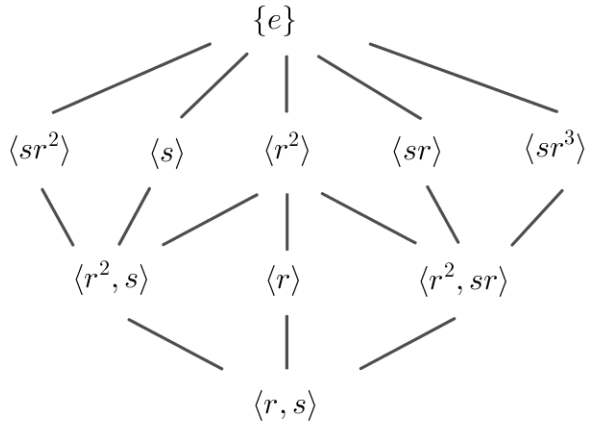


  - The fixed field of $\{e\}$ is K, while the fixed field of $\langle\sigma, \tau\rangle = \mathrm{Gal}(K/\mathbb{Q})$ is $\mathbb{Q}$ by condition (3) of the characterization of Galois extensions.
  - For the other fixed fields we can either compute the action explicitly on a basis (which is straightforward, if tedious) or try to identify elements of K that might generate some of these fields, and then exploit the Galois action.
  - For example, observe that σ stabilizes ζ_3, and since the fixed field corresponding to σ must have degree 2 over $\mathbb{Q}$, it must be equal to $\mathbb{Q}(\zeta_3)$. Notice that $\langle\sigma\rangle$ is normal in the Galois group, and indeed $\mathbb{Q}(\zeta_3)$ is Galois over $\mathbb{Q}$.
  - Likewise, we can see that τ stabilizes $2^{1/3}$, and since the fixed field of τ must have degree 3 over $\mathbb{Q}$, it must be equal to $\mathbb{Q}(2^{1/3})$.

- Since the subgroup $\langle\tau\rangle$ is not normal, we can compute other fixed fields by conjugating it (via part (3) of the fundamental theorem): for example, $\sigma\langle\tau\rangle\sigma^{-1} = \langle\tau\sigma\rangle$ stabilizes $\sigma(\mathbb{Q}(2^{1/3})) = \mathbb{Q}(2^{1/3}\zeta_3)$, and $\sigma^2\langle\tau\rangle\sigma^{-2} = \langle\tau\sigma^2\rangle$ stabilizes $\sigma^2(\mathbb{Q}(2^{1/3})) = \mathbb{Q}(2^{1/3}\zeta_3^2)$.
- We can then assemble all of this information into the full subfield lattice:

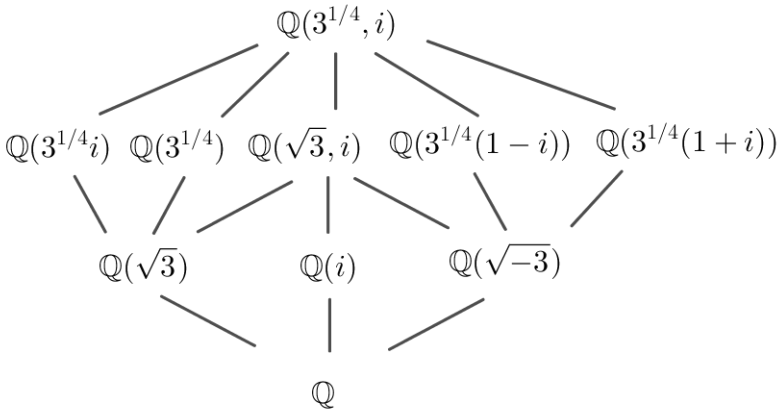


- Example: Identify all of the intermediate fields of $\mathbb{Q}(3^{1/4}, i)$ and then draw the subfield lattice.
  - We know that $K = \mathbb{Q}(3^{1/4}, i)/\mathbb{Q}$ is Galois since it is the splitting field of $x^4 - 3$ over $\mathbb{Q}$, and so we know that $|\mathrm{Gal}(K/\mathbb{Q})| = 8$. Any automorphism must map $3^{1/4}$ to one of its Galois conjugates $3^{1/4}$, $3^{1/4}i$, $-3^{1/4}$, $-3^{1/4}i$, and likewise must map i to one of its Galois conjugates i, $-i$.
  - Since there are only eight possibilities we conclude that all eight yield automorphisms of $K/\mathbb{Q}$.
  - With the automorphisms $r(3^{1/4}, i) = (3^{1/4}i, i)$ and $s(3^{1/4}, i) = (3^{1/4}, -i)$, we can verify (as previously) that $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to $D_{2\cdot 4}$.
  - From our knowledge of the dihedral group, we know it has subgroups $\{e\}$, $\langle s\rangle$, $\langle sr\rangle$, $\langle sr^2\rangle$, $\langle sr^3\rangle$, $\langle r^2\rangle$, $\langle r\rangle$, $\langle r^2, s\rangle$, $\langle r^2, sr\rangle$, and $\langle r, s\rangle$, and can draw the corresponding lattice:

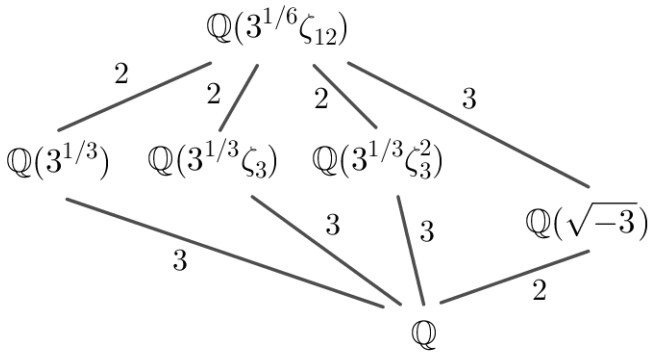


  - The fixed field of $\{e\}$ is K, while the fixed field of $\langle r, s\rangle = \mathrm{Gal}(K/\mathbb{Q})$ is $\mathbb{Q}$ by condition (3) of the characterization of Galois extensions.
  - For the other fixed fields, observe that r stabilizes i, and since the fixed field of $\langle r\rangle$ has degree 2 over $\mathbb{Q}$, it must be $\mathbb{Q}(i)$. Also r^2 stabilizes $\sqrt{3}$ and i, so the fixed field of $\langle r^2\rangle$ must be $\mathbb{Q}(\sqrt{3}, i)$.
  - Likewise, s stabilizes $3^{1/4}$ so the fixed field of $\langle s\rangle$ must be $\mathbb{Q}(3^{1/4})$ since it has degree 4 over $\mathbb{Q}$. Then since $r\langle s\rangle r^{-1} = \langle sr^2\rangle$ the fixed field of $\langle sr^2\rangle$ is $s(\mathbb{Q}(3^{1/4})) = \mathbb{Q}(3^{1/4}i)$.
  - Since $\sqrt{3}$ is stabilized by r^2 and s, and the fixed field $\langle r^2, s\rangle$ has degree 2 over $\mathbb{Q}$, it is $\mathbb{Q}(\sqrt{3})$.
  - Likewise, since $\sqrt{-3} = i\sqrt{3}$ is stabilized by r^2 and sr, and the fixed field $\langle r^2, sr\rangle$ has degree 2 over $\mathbb{Q}$, it is $\mathbb{Q}(\sqrt{-3})$.
  - It remains to find the fixed field of $\langle sr\rangle$ and $\langle sr^3\rangle$; since these are conjugate, it is enough to find one of them.

- For sr, we can compute explicitly that sr stabilizes $3^{1/4}(1-i)$ (this element can be found by writing out an explicit basis and evaluating the action of sr on it) but that no other nonidentity automorphism fixes it, so it does not lie in any proper subfield of the fixed field of sr. Thus the fixed field of sr is $\mathbb{Q}(3^{1/4}(1-i))$.
- Then since $r\langle sr\rangle r^{-1} = \langle sr^3\rangle$, the fixed field of $\langle sr^3\rangle$ is $r[\mathbb{Q}(3^{1/4}(1-i))] = \mathbb{Q}(3^{1/4}(1+i))$. So the full subfield lattice is as follows:



- Example: Find the splitting field K of $p(x) = x^6 + 3$ over $\mathbb{Q}$ and identify all of its subfields.
  - If we write $\alpha = (-3)^{1/6} = 3^{1/6}e^{i\pi/12}$, we can see that the roots of $p(x)$ are $\alpha \cdot \zeta_6^k$ for $0 \le k \le 5$, where $\zeta_6 = e^{2\pi i/6} = \frac{1}{2} + i\frac{\sqrt{3}}{2}$ is a primitive 6th root of unity.
  - Thus, $K = \mathbb{Q}(\alpha, \zeta_6)$, which is the composite of the fields $\mathbb{Q}(\alpha)$, which has degree 6 over $\mathbb{Q}$ by Eisenstein's criterion, and the field $\mathbb{Q}(\zeta_6)$, which has degree 2 over $\mathbb{Q}$.
  - Any automorphism of $K/\mathbb{Q}$ then must map α to one of its six Galois conjugates over $\mathbb{Q}$, namely $\alpha \cdot \zeta_6^k$ for $0 \le k \le 5$, and must also map ζ_6 to one of its two Galois conjugates over $\mathbb{Q}$, namely ζ_6, $\zeta_6^5 = \overline{\zeta_6}$.
  - It would then seem that we have 12 automorphisms of $K/\mathbb{Q}$, and that $[K : \mathbb{Q}]$ is equal to 12.
  - But in fact, this is not the case: note that $\alpha^3 = \sqrt{3}e^{i\pi/4} = i\sqrt{3}$, and therefore $2\zeta_6 - 1 = i\sqrt{3} = \alpha^3$, meaning that $\zeta_6 \in \mathbb{Q}(\alpha)$.
  - Therefore in fact $K = \mathbb{Q}(\alpha)$ so $[K : \mathbb{Q}] = 6$, not 12, and the automorphisms (of which there are 6) are determined solely by their action on α.
  - If σ is the automorphism with $\sigma(\alpha) = \alpha\zeta_6$, then $\sigma(\sqrt{-3}) = \sigma(\alpha^3) = \alpha^3\zeta_6^3 = -\sqrt{-3}$, and thus $\sigma(\zeta_6) = \zeta_6^5$. Hence $\sigma^2(\alpha) = \sigma(\alpha)\sigma(\zeta_6) = \alpha$, so σ has order 2.
  - Likewise, if τ is the automorphism with $\tau(\alpha) = \alpha\zeta_6^2$, then $\tau(\sqrt{-3}) = \tau(\alpha^3) = \alpha^3\zeta_6^6 = \sqrt{-3}$ and thus $\tau(\zeta_6) = \zeta_6$. Hence $\tau^3(\alpha) = \alpha\zeta_6^6 = \alpha$, so τ has order 3.
  - We can then compute $\tau\sigma(\alpha) = \tau(\alpha\zeta_6) = \alpha\zeta_6^3$, while $\sigma\tau(\alpha) = \sigma(\alpha\zeta_6^2) = \alpha\zeta_6^5$: thus $\sigma\tau \ne \tau\sigma$.
  - Hence $\mathrm{Gal}(K/\mathbb{Q})$ is non-abelian, so must be isomorphic to the dihedral group $D_{2\cdot 3}$, with σ playing the role of s and τ playing the role of r.
  - We can then compute fixed fields: by the fundamental theorem of Galois theory, the fixed field of τ is the unique subfield of $\mathbb{Q}(\alpha)$ of degree, so it must be $\mathbb{Q}(\sqrt{-3})$.
  - Likewise, there are three Galois-conjugate subfields of degree 3: since $\alpha^2/\zeta_6 = 3^{1/3} \in K$, this means one of them is $\mathbb{Q}(3^{1/3})$. We can compute $\sigma(3^{1/3}) = \sigma(\alpha^2/\zeta_6) = \alpha^2\zeta_6^3 = -\alpha^2$, and so σ fixes $\mathbb{Q}(3^{1/3})$.
  - Since the Galois conjugates of $3^{1/3}$ over $\mathbb{Q}$ are $3^{1/3}\zeta_3$ and $3^{1/3}\zeta_3^2$ the other fixed fields are $\mathbb{Q}(3^{1/3}\zeta_3)$ (the fixed field of $\langle\sigma\tau\rangle$) and $\mathbb{Q}(3^{1/3}\zeta_3)$ (the fixed field of $\langle\sigma\tau^2\rangle$). The full subfield diagram is then as follows:



4.3 Applications of Galois Theory

- In this section we apply the fundamental theorem of Galois theory to study the structure of a number of different classes of field extensions: finite fields, simple extensions, composite extensions, and cyclotomic extensions.

4.3.1 Finite Fields and Irreducible Polynomials in $\mathbb{F}_p[x]$

- Let p be a prime and n be a positive integer. As we have discussed, there is a unique (up to isomorphism) finite field $\mathbb{F}_{p^n}$ with p^n elements, and it is the splitting field of the separable polynomial $x^{p^n} - x$ over $\mathbb{F}_p$.
    - We have also shown that the Galois group $G = \text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is cyclic of order n and is generated by the Frobenius automorphism $\varphi_{(n)} : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ with $\varphi_{(n)}(x) = x^p$.
    - Then from our knowledge of cyclic groups, we see that the subgroups of G are of the form $\langle \varphi^d \rangle$ for the divisors d of n. Because G is abelian, all of these subgroups are normal, so the corresponding fixed fields are all Galois.
    - Since $\varphi_{(n)}^d(x) = x^{p^d}$, the fixed field of φ^d is the set of solutions to the equation $x^{p^d} - x = 0$ inside $\mathbb{F}_{p^n}$: this means that the fixed field is the splitting field of $x^{p^d} - x$, which is the field $\mathbb{F}_{p^d}$.
    - Thus, by the fundamental theorem of Galois theory, we conclude that the subfields of $\mathbb{F}_{p^n}$ are the fields $\mathbb{F}_{p^d}$ for d dividing n.
    - Furthermore, the Galois group $\text{Gal}(\mathbb{F}_{p^d}/\mathbb{F}_p)$ is generated by the image of $\varphi_{(n)}$ inside the quotient group $G/\langle \varphi^d \rangle$. Note that this map is simply the pth power map on elements, which is the map $\varphi_{(d)} : \mathbb{F}_{p^d} \to \mathbb{F}_{p^d}$. (In other words, the restriction of the Frobenius map from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^d}$ yields the Frobenius map on $\mathbb{F}_{p^d}$.)
- We can also use these observations to prove a useful result on irreducible polynomials over $\mathbb{F}_p$:
- Theorem (Factorization of $x^{p^n} - x$ in $\mathbb{F}_p[x]$): For any prime p and any positive integer n, the polynomial $x^{p^n} - x$ factors in $\mathbb{F}_p[x]$ as the product of all monic irreducible polynomials over $\mathbb{F}_p$ of degree dividing n.
    - Proof: Let $q(x) = x^{p^n} - x$. As we have noted previously, $q(x)$ is separable and its roots are the elements of $\mathbb{F}_{p^n}$.
    - If $f(x)$ is any monic irreducible factor of $x^{p^n} - x$, then $\mathbb{F}_p[x]/f(x)$ is a subfield of $\mathbb{F}_{p^n}$, hence must be equal to $\mathbb{F}_{p^d}$ for some d dividing n. Since $\deg(f) = d$ this means the degree of g divides n.
    - Conversely, if $f(x)$ is a monic irreducible polynomial over $\mathbb{F}_p$ of degree d dividing n, then $\mathbb{F}_p[x]/(f(x))$ is a finite field with p^d elements: hence it is (isomorphic to) $\mathbb{F}_{p^d}$.
    - Then any root α of $f(x)$ is contained in $\mathbb{F}_{p^d}$ hence lies in $\mathbb{F}_{p^n}$ and is thus a root of $q(x)$. Since $f(x)$ is separable (since it is irreducible over a finite field) this means $f(x)$ divides $q(x)$.
    - Thus, the irreducible factors of $x^{p^n} - x$ are precisely the monic irreducible polynomials over $\mathbb{F}_p$ of degree dividing n, and since no factor can be repeated, $x^{p^n} - x$ must simply be their product.

- We can use the factorization above above to give an exact count of the monic irreducible polynomials in $\mathbb{F}_p[x]$:
  - Let $f_p(n)$ be the number of monic irreducible polynomials of exact degree n in $\mathbb{F}_p[x]$.
  - The theorem says that $p^n = \sum_{d|n} d f_p(d)$, since both sides count the total degree of the product of all irreducible polynomials of degree dividing n. Using this recursion, we can compute the first few values:

n	1	2	3	4	5	6	7	8
$f_p(n)$	p	$\frac{1}{2}(p^2-p)$	$\frac{1}{3}(p^3-p)$	$\frac{1}{4}(p^4-p^2)$	$\frac{1}{5}(p^5-p)$	$\frac{1}{6}(p^6-p^3-p^2+p)$	$\frac{1}{7}(p^7-p)$	$\frac{1}{8}(p^8-p^4)$

  - For example, we see that there are $(3^7-3)/7 = 312$ monic irreducible polynomials of degree 7 over $\mathbb{F}_3$.
- In fact, we can use the recursion to write down a general formula:
- Definition: The Möbius function is defined as $\mu(n) = \begin{cases} 0 & \text{if } n \text{ is divisible by the square of any prime} \\ (-1)^k & \text{if } n \text{ is the product of } k \text{ distinct primes} \end{cases}$. In particular, $\mu(1) = 1$.
- Proposition (Möbius Inversion): If $f(n)$ is any sequence satisfying a recursive relation of the form $g(n) = \sum_{d|n} f(d)$, for some function $g(n)$, then $f(n) = \sum_{d|n} \mu(d) g(n/d)$.
  - Proof: First, consider the sum $\sum_{d|n} \mu(d)$: we claim it is equal to 1 if $n = 1$ and 0 if $n \neq 0$.
  - To see this, if $n = p_1^{a_1} \cdots p_k^{a_k}$, the only terms that will contribute to the sum $\sum_{d|n} \mu(d)$ are those values of $d = p_1^{b_1} \cdots p_k^{b_k}$ where each b_i is 0 or 1. If $k > 0$, then half of these 2^k terms will have $\mu(d) = 1$ and the other half will have $\mu(d) = -1$, so the sum is zero. Otherwise, $k = 0$ means that $n = 1$, in which case the sum is clearly 1.
  - Now we prove the desired result by (strong) induction. It clearly holds for $n = 1$, so now suppose the result holds for all $k < n$.
  - Then $\sum_{d|n} \mu(d) g(n/d) = \sum_{d|n} \mu(d) \sum_{d'|(n/d)} f(d') = \sum_{dd'|n} \mu(d) f(d') = \sum_{d'|n} f(d') \sum_{d|(n/d')} \mu(d)$ by induction and reordering the sum.
  - But the last sum is simply $f(n)$, because $\sum_{d|(n/d')} \mu(d)$ is zero unless n/d' is equal to 1.
- By applying Möbius inversion to $f_p(n)$, we immediately obtain the following:
- Corollary: The number of monic irreducible polynomials of degree n in $\mathbb{F}_p[x]$ is $f_p(n) = \frac{1}{n} \sum_{d|n} p^{n/d} \mu(d)$.
  - Example: The number of monic irreducible polynomials of degree 18 in $\mathbb{F}_2[x]$ is $\frac{1}{18}(2^{18} - 2^9 - 2^6 + 2^3) = 14532$.
  - From this corollary, we see that $f_p(n) = \frac{1}{n} p^n + O(p^{n/2})$, where the "big-$O$" notation means that the error is of size bounded above by a constant times $p^{n/2}$ as $n \to \infty$.
- We will note that any of these irreducible polynomials $f(x)$ of degree n yields gives a model for $\mathbb{F}_{p^n}$, namely as $\mathbb{F}_p[x]/(f(x))$.
  - If f_1 and f_2 are both irreducible of degree n, then $F_1 = \mathbb{F}_p[x]/(f_1(x))$ and $F_2 = \mathbb{F}_p[y]/(f_2(y))$ are both isomorphic to $\mathbb{F}_{p^n}$.
  - To compute an isomorphism between them, we simply observe that $f_1(x)$ splits completely over F_2, and if $\alpha(y)$ represents any root, then the map sending $\overline{x}$ in F_1 to $\alpha(y)$ in F_2 extends to an isomorphism of F_1 with F_2. (In other words, we map a root x of f_1 in F_1 to a root $\alpha(y)$ of f_1 in F_2.)
  - In practice, it can be rather cumbersome to compute the roots by hand, although there do exist efficient factorization algorithms over finite fields, one of which is known as Berlekamp's algorithm.
- Example: Compute an explicit isomorphism of the field $\mathbb{F}_3[x]/(x^3+2x+1)$ with the field $\mathbb{F}_3[y]/(y^3+y^2+2)$.
  - Note that both x^3+2x+1 and y^3+y^2+2 are irreducible over $\mathbb{F}_3$ because they are degree-3 and have no roots in $\mathbb{F}_3$.

- To compute an isomorphism, we search for a root of x^3+2x+1 in $\mathbb{F}_3[y]/(y^3+y^2+2)$.
- Checking the various possibilities eventually reveals that $2y^2+2y$ is a root of x^3+2x+1, and therefore the map $\varphi : \mathbb{F}_3[x]/(x^3+2x+1) \to \mathbb{F}_3[y]/(y^3+y^2+2)$ with $\varphi(x) = 2y^2+2y$ is such an isomorphism.

- As a final remark, we will observe that the simple structure of finite field extensions also yields a nice description of the algebraic closure $\overline{\mathbb{F}_p}$.
  - Explicitly, if $\alpha \in \overline{\mathbb{F}_p}$ then α (being algebraic over $\mathbb{F}_p$) is contained in a finite-degree extension of $\mathbb{F}_p$, namely, one of the fields $\mathbb{F}_{p^n}$.
  - But notice that the fields $\mathbb{F}_{p^n}$ for $n \geq 1$ are partially ordered under inclusion, and that any two of them are contained in another (namely, $\mathbb{F}_{p^n}$ and $\mathbb{F}_{p^m}$ are both contained in $\mathbb{F}_{p^{mn}}$).
  - Thus, the union of these fields (technically, the colimit) is well defined, and by the above, it contains every element α algebraic over $\mathbb{F}_p$, meaning that it is the algebraic closure. Symbolically, $\overline{\mathbb{F}_p} = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$.
  - Furthermore, since the Frobenius maps on the various $\mathbb{F}_{p^n}$ are all consistent under restriction, we see that they extend to a Frobenius map $\varphi : \overline{\mathbb{F}_p} \to \overline{\mathbb{F}_p}$ on the algebraic closure, defined explicitly via $\varphi(x) = x^p$.
  - Note that φ has infinite order as an element of $\mathrm{Aut}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$, but one may show in fact that $\mathrm{Aut}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ is uncountably infinite[3] (and thus φ is not a generator, since the cyclic subgroup it generates is only countably infinite).

4.3.2 Simple Extensions and the Primitive Element Theorem

- We can use the fundamental theorem of Galois theory to determine (in a large number of cases) when an arbitrary finite-degree extension K/F is simple, which is to say, when $K = F(\alpha)$ for some $\alpha \in K$. The easiest case is when F is finite:

- Proposition (Finite Fields are Simple): Suppose K/F is a finite-degree extension and F is finite. Then K is a simple extension of F.
  - Proof: If K/F has finite degree and F is finite, then K is also finite. As we have shown, the multiplicative group $K^\times$ of any finite field is cyclic. If α is any generator, then every nonzero element of K is a power of α, and thus in particular $F(\alpha) = F[\alpha] = K$.

- Next we prove a characterization of simple extensions in terms of their subfields:

- Proposition (Simple Extensions and Subfields): Suppose K/F is a finite-degree extension. Then $K = F(\alpha)$ for some $\alpha \in K$ if and only if K/F has finitely many intermediate fields.
  - Proof: If F is finite then the result follows immediately from the previous proposition, so now assume F is infinite.
  - First suppose $K = F(\alpha)$ is a simple extension and suppose E is an intermediate field of K/F.
  - Let $m(x) \in F[x]$ be the minimal polynomial for α over F and $p(x) \in E[x]$ be the minimal polynomial for α over E, and note that $p(x)$ divides $m(x)$ in $E[x]$.
  - If we let E' be the field generated over F by the coefficients of $p(x)$, then clearly $E' \subseteq E$, and the minimal polynomial for α over E' is also $p(x)$. But since $[K:E] = \deg p = [K:E']$, this means $E' = E$.
  - We conclude that E is generated over F by the coefficients of some monic polynomial dividing $m(x)$ in $F[x]$. Since there are only finitely many such factors (explicitly, there are at most 2^n such factors where n is the number of roots of $m(x)$), there are finitely many such subfields.

[3] More explicitly, since $\overline{\mathbb{F}_p} = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$, the automorphism group $\mathrm{Aut}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ is determined by its actions on each of the fields $\mathbb{F}_{p^n}$. The action on each of these fields must be as an automorphism, and so elements of $\mathrm{Aut}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ can be thought of as sequences of automorphisms $(\sigma_1, \sigma_2, \sigma_3, \dots)$ where σ_i is an automorphism of $\mathbb{F}_{p^i}$ for each $i \geq 1$. These automorphisms must be chosen consistently: for any $d|n$, the restriction of σ_n to $\mathbb{F}_{p^d}$ must equal σ_d. Conversely, if all of these choices are made consistently, then because $\overline{\mathbb{F}_p} = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$, the sequence $(\sigma_1, \sigma_2, \sigma_3, \dots)$ does yield an automorphism of $\overline{\mathbb{F}_p}/\mathbb{F}_p$. The resulting sequences of consistent automorphisms $(\sigma_1, \sigma_2, \sigma_3, \dots)$ are an example of a general construction called an inverse limit; in this case, we have shown that $\mathrm{Aut}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ is isomorphic to the inverse limit $\varprojlim_n (\mathbb{Z}/n\mathbb{Z})$, which is an uncountably infinite group called $\hat{\mathbb{Z}}$.

- For the converse, suppose K/F has finite degree and finitely many intermediate fields. Then $K = F(\alpha_1, \ldots, \alpha_n)$ for some algebraic $\alpha_i \in K$, so it suffices to show that $F(\beta, \gamma)$ is a simple extension for any algebraic β, γ, since then the result for K follows immediately by induction.
- To show this, consider the subfields $F(\beta + x\gamma)$ for $x \in F$: since F is infinite by hypothesis and there are only finitely many intermediate fields of K/F, there must exist distinct $x, y \in F$ such that $F(\beta + x\gamma) = F(\beta + y\gamma)$. Call this field E.
- Then $E \subseteq F(\beta, \gamma)$, and since E contains $\beta + x\gamma$ and $\beta + y\gamma$ it also contains $(x - y)\gamma$ and thus γ since $x - y$ is a nonzero element of F. Then E clearly also contains $\beta = (\beta + x\gamma) - x\gamma$, and so $E = F(\beta, \gamma)$.
- We conclude that $E = F(\beta + x\gamma)$ is a simple extension of F, so we are done.

- Using the Galois correspondence, we can then see immediately that a finite-degree Galois extension has finitely many intermediate subfields, since these are in bijection with subgroups of the Galois group (which is a finite group), and is therefore simple. We may extend this result to any separable extension:

- Theorem (Primitive Element Theorem): If K/F is a finite-degree separable extension, then $K = F(\alpha)$ for some $\alpha \in K$. In particular, any finite-degree extension of characteristic-0 fields is a simple extension.

  - In general, an element α generating the extension K/F is called a primitive element for K/F.
  - Proof: If K/F is a finite-degree separable extension, then $K = F(\alpha_1, \ldots, \alpha_n)$ for some algebraic $\alpha_1, \ldots, \alpha_n$. Let the minimal polynomial of α_i over F be $m_i(x)$, and define $m(x)$ to be the least common multiple of the polynomials $m_i(x)$.
  - Then $m(x)$ cannot have any repeated roots, since by definition of the least common multiple this would require one of the m_i to have a repeated root, so $m(x)$ is separable. Let L be its splitting field over F: then L contains each of $\alpha_1, \ldots, \alpha_n$, hence contains K, and L/F is a Galois extension.
  - By the fundamental theorem of Galois theory, the intermediate fields of L/F are in bijection with the subgroups of $\mathrm{Gal}(L/F)$. Since $\mathrm{Gal}(L/F)$ is a finite group, it has finitely many subgroups, and so there are finitely many intermediate fields of L/F.
  - Since K is a subfield of L/F, this means there are finitely many intermediate fields of K/F also. By the previous result, this means K/F is a simple extension, as claimed.
  - The second statement follows immediately, since every extension of characteristic-0 fields is separable.

- As indicated by the results above, if K/F has finite degree with $K = F(\alpha_1, \ldots, \alpha_n)$ and F is infinite, then we may always construct a primitive element as an F-linear combination of the generators $\alpha_1, \ldots, \alpha_n$.

  - If in addition K/F is Galois, then to verify that $\beta \in K$ is a primitive element, we need only check that it is not fixed by any element of the Galois group $\mathrm{Gal}(K/F)$, since then it cannot be an element of any proper subfield of K/F.
  - More generally, to determine whether an element β of a non-Galois separable extension K/F is a generator, we may compute all of its Galois conjugates (inside a Galois extension $L/K/F$): if the number of distinct Galois conjugates is equal to the degree $[K : F]$, then β will generate K/F.

- Example: If p is a prime, find a primitive element for the Galois extension $\mathbb{Q}(3^{1/p}, \zeta_p)/\mathbb{Q}$.

  - Note that $\mathbb{Q}(3^{1/p}, \zeta_p)$ is the splitting field of the Eisenstein-irreducible polynomial $x^p - 3$ over $\mathbb{Q}$, and is also the composite of the fields $\mathbb{Q}(3^{1/p})$ and $\mathbb{Q}(\zeta_p)$, which have degrees p and $p - 1$ over $\mathbb{Q}$. Thus, $[K : \mathbb{Q}] = p(p - 1)$.
  - Any element of the Galois group must map $3^{1/p}$ to one of its p Galois conjugates $3^{1/p}, 3^{1/p}\zeta_p, \ldots, 3^{1/p}\zeta_p^{p-1}$ over $\mathbb{Q}$, and must also map ζ_p to one of its $p - 1$ Galois conjugates $\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}$ over $\mathbb{Q}$.
  - Since this yields at most $p(p - 1)$ choices, each must actually extend to an automorphism of $K/\mathbb{Q}$.
  - To compute a primitive element, let us try the easiest nontrivial linear combination of the generators, namely $\alpha = 3^{1/p} + \zeta_p$.
  - We can see that applying all of the automorphisms in the Galois group to α yield the $p(p - 1)$ elements $3^{1/p}\zeta_p^a + \zeta_p^b$ for $a \in \{0, 1, \ldots, p - 1\}$ and $b \in \{1, 2, \ldots, p - 1\}$.
  - Since no automorphism fixes α, we conclude that $\alpha = \boxed{3^{1/p} + \zeta_p}$ is a primitive element for $K/\mathbb{Q}$.

- We will also remark that there do exist non-separable finite-degree extensions that are not simple.
  - For example, consider the fields $K = \mathbb{F}_p(x^p, y^p)$ and $L = \mathbb{F}_p(x, y)$, where x and y are indeterminates.
  - Then $[L : K] = [L : F(x^p, y)] \cdot [F(x^p, y) : F(x^p, y^p)] = p \cdot p = p^2$.
  - On the other hand, there is no primitive element for L/K, because the pth power of every element of L lies in K: taking pth powers does not affect elements in $\mathbb{F}_p$ and respects addition and multiplication, so the result of taking the pth power of a rational function in L is simply to replace x with x^p and y with y^p.
  - Therefore, every element of L satisfies a polynomial of degree p with coefficients in K. In particular, there does not exist any element α in L with $[K(\alpha) : K] = p^2$, and so L/K is not a simple extension. (In fact, this argument works if $\mathbb{F}_p$ is replaced with any field of characteristic p.)
  - One may also explicitly compute an infinite family[4] of intermediate subfields, namely, $K(x + y^{1+np})$ for positive integers n. The existence of infinitely many intermediate fields again implies that L/K cannot be a simple extension.
  - We also remark that this example is essentially the simplest possible, since a non-simple extension must be inseparable (hence its degree can be reduced to a power of p) and every extension of degree p is simple (since it is generated by any element of K not in F): thus a non-simple field extension of minimal degree must be an inseparable extension of degree p^2 over a field of characteristic p.

4.3.3 Composite Extensions

- Next we consider the question of computing Galois groups of composite extensions. The main result in this direction is as follows:
- Proposition ("Sliding-Up" Galois Extensions): Suppose K/F is a Galois extension and L/F is any extension. Then the extension KL/L is Galois, and its Galois group is isomorphic to the subgroup $\mathrm{Gal}(K/K \cap L)$ of $\mathrm{Gal}(K/F)$.
  - Proof: By our characterization of Galois extensions, K is the splitting field of a separable polynomial $p(x)$ over F: explicitly, $K = F(r_1, r_2, \ldots, r_n)$ where the r_i are the roots of $p(x)$ in K.
  - Then KL is the splitting field of $p(x)$ over L, since $KL = L(r_1, r_2, \ldots, r_n)$, and so KL/L is Galois.
  - Now suppose σ is any automorphism of KL/L: observe that the restriction $\sigma|_K$ of σ to K is an automorphism of K, since $\sigma|_K(K)$ is a Galois conjugate field of K, hence must equal K since K/F is Galois.
  - Hence we obtain a well-defined map $\varphi : \mathrm{Gal}(KL/L) \to \mathrm{Gal}(K/F)$ given by restricting an automorphism of KL/L to K/F. This map is trivially a homomorphism, and its kernel consists of the automorphisms of KL fixing both L and K, but the only such map is the identity.
  - To compute the image, observe that every element in $\mathrm{im}(\varphi)$ must fix the elements of L inside K, hence $\mathrm{im}(\varphi) \leq \mathrm{Gal}(K/K \cap L)$.
  - Now let E be the fixed field of $\mathrm{im}(\varphi)$: then the observation above shows that E contains $K \cap L$.
  - Also, notice that EL is fixed by $\mathrm{Gal}(KL/L)$, since any $\sigma \in \mathrm{Gal}(KL/L)$ fixes L and its restriction to K fixes E (by definition).
  - Thus, by the fundamental theorem of Galois theory, we see that $EL = L$, and hence $E \subseteq L$. Since $E \subseteq K$ this means $E \subseteq K \cap L$, and so we must have $E = K \cap L$.
  - Hence again by the fundamental theorem of Galois theory, we conclude that $\mathrm{im}(\varphi) = \mathrm{Gal}(K/E) = \mathrm{Gal}(K/K \cap L)$.
- As a corollary, we obtain a useful formula for the degree of a composite extension where at least one of the fields is Galois:

[4] Explicitly, each of these fields is a degree-p extension of K (since $x + y^{1+ap} \notin K$ but as noted earlier its pth power is in K) but they are all distinct: the composite of $K(x + y^{1+ap})$ and $K(x + y^{1+bp})$ contains the difference $y(y^{ap} - y^{bp})$ and hence y (since the second term is in K), and hence also x. This means the composite field is $K(x, y) = L$, but since $[L : K] = p^2$ this means the original fields could not have been equal.

- Corollary (Degree of Composite): Suppose K/F is a Galois extension and L/F is any finite-degree extension. Then $[KL:F] = \dfrac{[K:F]\cdot[L:F]}{[K\cap L:F]}$.
  - Proof: From the above result, we know that $\mathrm{Gal}(KL/L) \cong \mathrm{Gal}(K/K\cap L)$, and therefore by the fundamental theorem of Galois theory, $[KL:L] = [K:K\cap L]$.
  - Then $[KL:F] = [KL:L]\cdot[L:F] = [K:K\cap L]\cdot[L:F] = \dfrac{[K:F]\cdot[L:F]}{[K\cap L:F]}$, as claimed.
- We may also say more about the Galois group of the composite of two Galois extensions:
- Proposition (Galois Groups of Composites): If K_1/F and K_2/F are Galois, then K_1K_2/F is also Galois and its Galois group is isomorphic to the subgroup of $\mathrm{Gal}(K_1/F)\times\mathrm{Gal}(K_2/F)$ consisting of elements whose restrictions to $K_1\cap K_2$ are equal. In particular, if $K_1\cap K_2 = F$, then $\mathrm{Gal}(K_1K_2/F) \cong \mathrm{Gal}(K_1/F)\times\mathrm{Gal}(K_2/F)$.
  - Proof: If K_1 and K_2 are Galois over F then they are splitting fields of some separable polynomials $p_1(x)$ and $p_2(x)$.
  - Then the composite field K_1K_2 is the splitting field of the least common multiple of $p_1(x)$ and $p_2(x)$, which as we have previously noted is also separable. Hence K_1K_2/F is also Galois.
  - To compute the Galois group, observe that the action of any automorphism on K_1K_2/F is completely determined by its actions on K_1/F and K_2/F (since the elements of K_1 and K_2 generate K_1K_2), and so we have a homomorphism $\varphi : \mathrm{Gal}(K_1K_2)/F \to \mathrm{Gal}(K_1/F)\times\mathrm{Gal}(K_2/F)$ given by $\varphi(\sigma) = (\sigma_{K_1}, \sigma_{K_2})$.
  - This map φ is clearly injective, since any automorphism fixing both K_1 and K_2 fixes K_1K_2.
  - To compute $\mathrm{im}(\varphi)$, first observe that $\mathrm{im}(\varphi)$ is certainly contained in the subgroup H of $\mathrm{Gal}(K_1/F)\times\mathrm{Gal}(K_2/F)$ consisting of elements whose restrictions to $K_1\cap K_2$ are equal.
  - Furthermore, notice that for any fixed $\tau\in\mathrm{Gal}(K_2/F)$, there are $|\mathrm{Gal}(K_1/K_1\cap K_2)|$ automorphisms $\sigma\in\mathrm{Gal}(K_1/F)$ such that $\sigma|_{K_1\cap K_2} = \tau|_{K_1\cap K_2}$, and so $|H| = |\mathrm{Gal}(K_2/F)|\cdot|\mathrm{Gal}(K_1/K_1\cap K_2)| = [K_2:F]\cdot[K_1:K_1\cap K_2]$.
  - On the other hand, by the sliding-up proposition, we know that $\mathrm{Gal}(K_1K_2/K_2)\cong\mathrm{Gal}(K_1/K_1\cap K_2)$ and thus $[K_1K_2:K_2] = [K_1:K_1\cap K_2]$. Hence $|\mathrm{im}(\varphi)| = |\mathrm{Gal}(K_1K_2)/F| = [K_1K_2:F] = [K_1K_2:K_2]\cdot[K_2:F] = [K_1:K_1\cap K_2]\cdot[K_2:F]$.
  - Thus we see that $|H| = |\mathrm{im}(\varphi)|$, and so they must be equal, as claimed.
  - The second statement follows immediately, since if $K_1\cap K_2 = F$ then every element (σ,τ) in the direct product has $\sigma|_{K_1\cap K_2} = \tau|_{K_1\cap K_2}$.
- In cases where we can compute $K_1\cap K_2$, this allows us to determine Galois groups for composite fields explicitly:
- Example: Find the degree of $\mathbb{Q}(2^{1/3}, 3^{1/2}, \zeta_3)/\mathbb{Q}$ and describe its Galois group.
  - Observe that $L = \mathbb{Q}(2^{1/3}, 3^{1/2}, \zeta_3)$ is the composite of the Galois extensions $K_1 = \mathbb{Q}(2^{1/3}, \zeta_3)$ and $K_2 = \mathbb{Q}(3^{1/2})$.
  - Now observe that K_1 has a unique quadratic subfield, namely $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$, which is not equal to K_2. Hence we have $K_1\cap K_2 = \mathbb{Q}$.
  - Then by the degree formula we have $[K_1K_2:\mathbb{Q}] = \dfrac{[K_1:\mathbb{Q}]\cdot[K_2:\mathbb{Q}]}{[K_1\cap K_2:\mathbb{Q}]} = \boxed{12}$, and the Galois group is simply the direct product $\mathrm{Gal}(K_1/\mathbb{Q})\times\mathrm{Gal}(K_2/\mathbb{Q}) \cong \boxed{S_3\times(\mathbb{Z}/2\mathbb{Z})}$.
- Example: Find the degree of $\mathbb{Q}(2^{1/3}, 3^{1/3}, \zeta_3)/\mathbb{Q}$ and describe its Galois group.
  - Observe that $L = \mathbb{Q}(2^{1/3}, 3^{1/3}, \zeta_3)$ is the composite of the Galois extensions $K_1 = \mathbb{Q}(2^{1/3}, \zeta_3)$ and $K_2 = \mathbb{Q}(3^{1/3}, \zeta_3)$.
  - Then $K_1\cap K_2$ certainly contains $\mathbb{Q}(\zeta_3)$ and is contained in K_1, so since $[K_1:\mathbb{Q}(\zeta_3)] = 3$ we must have either $K_1\cap K_2 = K_1$ or $K_1\cap K_2 = \mathbb{Q}(\zeta_3)$.

- If $K_1 \cap K_2 = K_1$ then we would also have $K_1 \cap K_2 = K_2$ by degree considerations, and then K_1 would equal K_2. But this is not possible, because it would imply that $3^{1/3} \in \mathbb{Q}(2^{1/3})$, which is not true[5].
- Hence $K_1 \cap K_2 = \mathbb{Q}(\zeta_3)$, and so by the degree formula we see that $[K_1K_2 : \mathbb{Q}] = \dfrac{[K_1 : \mathbb{Q}] \cdot [K_2 : \mathbb{Q}]}{[K_1 \cap K_2 : \mathbb{Q}]} = \dfrac{6 \cdot 6}{2} = \boxed{18}$.
- The Galois group is then the order-18 subgroup of $\mathrm{Gal}(K_1/\mathbb{Q}) \times \mathrm{Gal}(K_2/\mathbb{Q}) = S_3 \times S_3$ of pairs (σ, τ) where $\sigma|_{\mathbb{Q}(\zeta_3)} = \tau|_{\mathbb{Q}(\zeta_3)}$.
- Explicitly, these are the maps with $\varphi(2^{1/3}, 3^{1/3}, \zeta_3) = (2^{1/3}\zeta_3^a,\ 3^{1/3}\zeta_3^b,\ \zeta_3^c)$ where $a \in \{0, 1, 2\}$, $b \in \{0, 1, 2\}$, and $c \in \{1, 2\}$. It is easy to see that every element in the Galois group must be of this form, and conversely since $|\mathrm{Gal}(K_1K_2/\mathbb{Q})| = 18$, each of these 18 choices does extend to an actual automorphism.

4.3.4 Cyclotomic Extensions

- We now turn our attention to studying cyclotomic extensions. Our first goal is to compute the degree and the Galois group of the cyclotomic extension $\mathbb{Q}(\zeta_n)$ for an arbitrary positive integer n, but to do this we require some preliminary facts about the nth roots of unity.
  - As we have observed previously, the group $\mu_n = \{1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}\}$ of nth roots of unity is cyclic of order n and generated by ζ_n. We have an explicit isomorphism of μ_n with $\mathbb{Z}/n\mathbb{Z}$ given by associating ζ_n^k with $\overline{k}$.
  - From properties of order, we see that the order of ζ_n^k is $n/\gcd(n, k)$, so in particular ζ_n^k has order n precisely when k is relatively prime to n (equivalently, when k is a unit modulo n).
  - If ζ is an nth root of unity of order n, we call it a <u>primitive</u> nth root of unity: by the above remarks, the number of primitive nth roots of unity is $|(\mathbb{Z}/n\mathbb{Z})^\times|$. This number is an important quantity that often shows up in number theory:

- <u>Definition</u>: If n is a positive integer, the <u>Euler φ-function</u> $\varphi(n)$, also sometimes called the <u>Euler totient function</u>, is the number of units in $\mathbb{Z}/n\mathbb{Z}$. Equivalently, $\varphi(n)$ is the number of positive integers k with $1 \le k \le n$ that are relatively prime to n.
  - <u>Example</u>: We have $\varphi(6) = 2$ since there are 2 units modulo 6, namely $\overline{1}$ and $\overline{5}$.

- We can give an explicit formula for the value of $\varphi(n)$:

- <u>Proposition</u> (Value of $\varphi(n)$): If p is a prime, then $\varphi(p^k) = p^k - p^{k-1}$, and for any relatively prime integers a and b we also have $\varphi(ab) = \varphi(a)\varphi(b)$. Thus, if n has prime factorization $n = \prod_i p_i^{a_i}$, we have $\varphi(n) = \prod_i p_i^{a_i - 1}(p_i - 1) = n \cdot \prod_i (1 - 1/p_i)$.
  - <u>Proof</u>: If p is a prime, then $\varphi(p^k) = p^k - p^{k-1}$, since the integers with $1 \le k \le p^k$ not relatively prime to p^k are simply the multiples of p, of which there are p^{k-1}.
  - For the second statement, we first observe that if a and b are relatively prime positive integers, then there is a ring isomorphism of $\mathbb{Z}/ab\mathbb{Z}$ with $(\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z})$ given by $\psi(k \bmod ab) = (k \bmod a, k \bmod b)$.
  - It is easy to see that ψ is a group isomorphism since it respects addition and is injective (hence surjective because the domain and target both have size ab), and since it also respects multiplication it is a ring isomorphism.
  - Then since the rings $\mathbb{Z}/ab\mathbb{Z}$ and $(\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z})$ are isomorphic, their corresponding unit groups $(\mathbb{Z}/ab\mathbb{Z})^\times$ and $(\mathbb{Z}/a\mathbb{Z})^\times \times (\mathbb{Z}/b\mathbb{Z})^\times$ are also isomorphic.
  - Comparing cardinalities shows that $\varphi(ab) = \varphi(a)\varphi(b)$ for any relatively prime integers a and b.
  - For the last statement, we simply write n as a product of prime powers and then apply the two results we have just established to conclude that $\varphi(n) = \prod_i p_i^{a_i - 1}(p_i - 1)$. The second formula follows by pulling out a factor of $p_i^{a_i}$ from each term.

[5] This is intuitively obvious, but for completeness, it follows by observing that any element σ of the Galois group has the property that $\sigma(3^{1/3})/3^{1/3}$ is a 3rd root of unity, and then noting that the only elements $z \in \mathbb{Q}(2^{1/3})$ with $\sigma(z)/z$ equal to a third root of unity for all $\sigma \in \mathrm{Gal}(K_1/\mathbb{Q})$ are rational multiples of $\{1, 2^{1/3}, 4^{1/3}\}$, and $3^{1/3}$ is not equal to any of these.

- Definition: The nth cyclotomic polynomial $\Phi_n(x)$ is the monic polynomial of degree $\varphi(n)$ whose roots are the primitive nth roots of unity: $\Phi_n(x) = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} (x - \zeta_n^k)$.
  - Observe that the roots of $x^n - 1$ are all of the nth roots of unity, so if we group together all of the primitive dth roots of unity for each $d|n$, we see that $x^n - 1 = \prod_{d|n} \Phi_d(x)$. (Computing the degree of both sides also establishes the identity $n = \sum_{d|n} \varphi(d)$ for the Euler φ-function.)
  - This yields a recursion that we can use to compute $\Phi_n(x)$: for example, $x^6 - 1 = \Phi_6(x)\Phi_3(x)\Phi_2(x)\Phi_1(x)$, so $\Phi_6(x) = \dfrac{x^6 - 1}{(x^2 + x + 1)(x + 1)(x - 1)} = x^2 - x + 1$.
  - Furthermore, using this recursion we can see by induction on n that $\Phi_n(x)$ will always have integer coefficients. Explicitly: the base case $n = 1$ is trivial, and for the inductive step, observe that $\prod_{d|n, d<n} \Phi_d(x)$ is monic, has integer coefficients, and divides $x^n - 1$ in $\mathbb{Q}(\zeta_n)[x]$: hence it divides $x^n - 1$ in $\mathbb{Q}[x]$ since both polynomials have coefficients in $\mathbb{Q}$. Then by Gauss's lemma, $\prod_{d|n, d<n} \Phi_d(x)$ divides $x^n - 1$ in $\mathbb{Z}[x]$, so the quotient $\Phi_n(x)$ has integer coefficients.
- We have previously shown that if p is prime, then $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible over $\mathbb{Q}$. We now extend this result to all of the polynomials $\Phi_n(x)$:
- Theorem (Irreducibility of Cyclotomic Polynomials): For any positive integer n, the cyclotomic polynomial $\Phi_n(x)$ is irreducible over $\mathbb{Q}$, and therefore $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.
  - Proof: Suppose that we have an irreducible monic factor of $\Phi_n(x)$ in $\mathbb{Q}[x]$. By Gauss's lemma, this yields a factorization $\Phi_n(x) = f(x)g(x)$ where $f(x), g(x) \in \mathbb{Z}[x]$ are monic and $f(x)$ is irreducible.
  - Let ω be a primitive nth root of unity that is a root of f, and let p be any prime not dividing n. Since f is irreducible, this means f is the minimal polynomial of ω.
  - By properties of order, we see that ω^p is also a primitive nth root of unity, hence is a root of either f or of g.
  - Suppose ω^p is a root of g, so that $g(\omega^p) = 0$. This means ω is a root of $g(x^p)$, and so since f is the minimal polynomial of ω, it must divide $g(x^p)$: say $f(x)h(x) = g(x^p)$ for some $h(x) \in \mathbb{Z}[x]$.
  - Now view this equation in $\mathbb{F}_p$ (i.e., modulo p): this yields $\overline{f}(x)\overline{h}(x) = \overline{g}(x^p) = \overline{g}(x)^p$. Thus by unique factorization in $\mathbb{F}_p[x]$, we see that $\overline{f}(x)$ and $\overline{g}(x)$ have a nontrivial common factor in $\mathbb{F}_p[x]$.
  - Then since $\Phi_n(x) = f(x)g(x)$, reducing modulo p yields $\overline{\Phi_n}(x) = \overline{f}(x)\overline{g}(x)$ and so $\overline{\Phi_n}(x)$ would have a repeated factor, hence so would $x^n - 1$. But this is a contradiction because since $x^n - 1$ is separable in $\mathbb{F}_p[x]$ (its derivative is nx^{n-1}, which is relatively prime to $x^n - 1$ because p does not divide n).
  - Hence we conclude that ω^p is not a root of g, so it must be a root of f. Since this holds for every root ω of f, we see that for any $a = p_1 p_2 \cdots p_k$ that is relatively prime to n, then $\omega^a = ((\omega^{p_1})^{p_2})^{\cdots p_n}$ is a root of f.
  - But this means every primitive nth root of unity is a root of f, and so $\Phi_n = f$ is irreducible as claimed.
  - The second statement follows immediately, because $\Phi_n(x)$ is then the minimal polynomial of ζ_n, so $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg(\Phi_n) = \varphi(n)$.
- We can now easily compute the Galois group of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$:
- Theorem (Galois Group of $\mathbb{Q}(\zeta_n)$): The extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois with Galois group isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$. Explicitly, the elements of the Galois group are the automorphisms σ_a for $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ acting via $\sigma_a(\zeta_n) = \zeta_n^a$.
  - Proof: Since $K = \mathbb{Q}(\zeta_n)$ is the splitting field of $x^n - 1$ (or $\Phi_n(x)$) over $\mathbb{Q}$ it is Galois, and $|\mathrm{Gal}(K/\mathbb{Q})| = [K : \mathbb{Q}] = \varphi(n)$.
  - Furthermore, any automorphism σ must map ζ_n to one of its Galois conjugates over $\mathbb{Q}$, which are the roots of $\Phi_n(x)$: explicitly, these are the $\varphi(n)$ values ζ_n^a for a relatively prime to n.
  - Since there are in fact $\varphi(n)$ possible automorphisms, each of these choices must extend to an automorphism of $K/\mathbb{Q}$.

- Hence the elements of the Galois group are the maps σ_a as claimed. Since $\sigma_a(\sigma_b(\zeta_n)) = \sigma_a(\zeta_n^b) = \zeta_n^{ab}$, the composition of automorphisms is the same as multiplication of the indices in $(\mathbb{Z}/n\mathbb{Z})^\times$, and since this association is a bijection, the Galois group is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$.

- By using the structure of the Galois group we can in principle compute all of the subfields of $\mathbb{Q}(\zeta_n)$. In practice, however, this tends to be computationally difficult when the subgroup structure of $(\mathbb{Z}/n\mathbb{Z})^\times$ is complicated.

  - The simplest case occurs when $n = p$ is prime, in which case (as we have shown already) the Galois group $G \cong (\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $p-1$. Let σ be a generator of the Galois group, with $\sigma(\zeta_p) = \zeta_p^a$ where a is a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$.
  - Then by the Galois correspondence, the subfields of $\mathbb{Q}(\zeta_p)$ are the fixed fields of σ^d for the divisors d of $p-1$.
  - We may compute an explicit generator for each of these fixed fields by exploiting the action of the Galois group on the basis $\{\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}\}$ for $\mathbb{Q}(\zeta_p)/\mathbb{Q}$. (Note that this set is obtained from the standard basis $\{1, \zeta_p, \ldots, \zeta_p^{p-2}\}$ using the relation $\zeta_p^{p-1} + \zeta_p^{p-2} + \cdots + \zeta_p + 1 = 0$ from the minimal polynomial of ζ_p.)
  - Since all of these basis elements are Galois conjugates, the action of any element of the Galois group permutes them.
  - Now for any subgroup H of G, define the element $\alpha_H = \sum_{\sigma \in H} \sigma(\zeta_p)$: we claim that α_H is a generator for the fixed field of H.
  - To see this, observe first that if $\tau \in H$, then $\tau(\alpha_H) = \alpha_H$ because τ merely permutes the elements $\sigma(\zeta_p)$ for $\sigma \in H$.
  - Conversely, because the elements $\sigma(\zeta_p)$ for $\sigma \in G$ form a basis, if $\tau \in G$ has $\tau(\alpha_H) = \alpha_H$ then $\tau(\zeta_p)$ must equal $\sigma(\zeta_p)$ for some $\sigma \in H$. But then $\tau\sigma^{-1}$ acts as the identity on ζ_p and hence on all of $\mathbb{Q}(\zeta_p)$, so it must be the identity element: thus, $\tau = \sigma \in H$.
  - We conclude that the automorphisms fixing α_H are precisely the elements of H, and so $\mathbb{Q}(\alpha_H)$ is the fixed field of H.

- Example: Find generators for each of the subfields of $\mathbb{Q}(\zeta_7)$.

  - We know that $G = \mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/7\mathbb{Z})^\times$. By trial and error we can see that $\overline{3}$ has order 6 in $(\mathbb{Z}/7\mathbb{Z})^\times$, so it is a generator. The corresponding automorphism generating G is the map σ with $\sigma(\zeta_7) = \zeta_7^3$.
  - The subgroups of G are then $\langle\sigma\rangle = \{e, \sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5\}$, $\langle\sigma^2\rangle = \{e, \sigma^2, \sigma^4\}$, $\langle\sigma^3\rangle = \{e, \sigma^3\}$, and $\langle\sigma^6\rangle = \{e\}$.
  - A generator of the fixed field of $\langle\sigma\rangle$ is given by $\zeta_7 + \sigma(\zeta_7) + \sigma^2(\zeta_7) + \sigma^3(\zeta_7) + \sigma^4(\zeta_7) + \sigma^5(\zeta_7) = \zeta_7 + \zeta_7^3 + \zeta_7^2 + \zeta_7^6 + \zeta_7^4 + \zeta_7^5$.
  - Similarly, the fixed field of $\langle\sigma^2\rangle$ is generated by $\zeta_7 + \sigma^2(\zeta_7) + \sigma^4(\zeta_7) = \zeta_7 + \zeta_7^2 + \zeta_7^4$, while the fixed field of $\langle\sigma^3\rangle$ is generated by $\zeta_7 + \sigma^3(\zeta_7) = \zeta_7 + \zeta_7^6$.
  - We can also use the Galois action to compute the minimal polynomials of each of these elements, since we may compute all of these elements' Galois conjugates.
  - For example, the element $\zeta_7 + \zeta_7^2 + \zeta_7^4$ has one other Galois conjugate inside $\mathbb{Q}(\zeta_7)$, namely $\zeta_7^3 + \zeta_7^5 + \zeta_7^6$. Then their common minimal polynomial is $m(x) = [x - (\zeta_7 + \zeta_7^2 + \zeta_7^4)] \cdot [x - (\zeta_7^3 + \zeta_7^5 + \zeta_7^6)] = x^2 + x + 2$, as follows from multiplying out and simplifying the coefficients. Solving the quadratic yields an explicit formula $\zeta_7 + \zeta_7^2 + \zeta_7^4 = \dfrac{-1 - \sqrt{-7}}{2}$, and thus the corresponding fixed field $\mathbb{Q}(\zeta_7 + \zeta_7^2 + \zeta_7^4) = \mathbb{Q}(\sqrt{-7})$.
  - Similarly, the element $\zeta_7 + \zeta_7^6 = 2\cos(2\pi/7)$ has two other Galois conjugates, namely $\zeta_7^2 + \zeta_7^5 = 2\cos(4\pi/7)$ and $\zeta_7^3 + \zeta_7^4 = 2\cos(6\pi/7)$. Their common minimal polynomial is $m(x) = [x - (\zeta_7 + \zeta_7^6)] \cdot [x - (\zeta_7^2 + \zeta_7^5)][x - (\zeta_7^3 + \zeta_7^4)] = x^3 + x^2 - 2x - 1$. Thus, our analysis implies that the Galois group of this polynomial is cyclic of order 3.

- For other n, we can perform similar computations, although there is not usually as convenient a basis available[6]. We can simplify some of these computations by writing $\mathbb{Q}(\zeta_n)$ as a composite of smaller cyclotomic fields:

[6] In general, the primitive nth roots of unity form a basis for $\mathbb{Q}(\zeta_n)$ precisely when n is squarefree.

- Proposition (Composites of Cyclotomic Extensions): If a and b are relatively prime integers, then the composite of $\mathbb{Q}(\zeta_a)$ and $\mathbb{Q}(\zeta_b)$ is $\mathbb{Q}(\zeta_{ab})$, the intersection is $\mathbb{Q}$, and $\mathrm{Gal}(\mathbb{Q}(\zeta_{ab})/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_a)/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_b)/\mathbb{Q})$. In particular, if the prime factorization of n is $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, then $\mathbb{Q}(\zeta_n)$ is the composite of the fields $\mathbb{Q}(\zeta_{p_i^{a_i}})$ for $1 \leq i \leq k$, and $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_{p_1^{a_1}})/\mathbb{Q}) \times \cdots \times \mathrm{Gal}(\mathbb{Q}(\zeta_{p_k^{a_k}})/\mathbb{Q})$.
    - Proof: Observe that $\zeta_{ab}^b = \zeta_a$ and $\zeta_{ab}^a = \zeta_b$, so both ζ_a and ζ_b are in $\mathbb{Q}(\zeta_{ab})$: thus, the composite field is contained in $\mathbb{Q}(\zeta_{ab})$.
    - Also, since a and b are relatively prime, there exist integers s and t with $sa + tb = 1$. Then $\zeta_b^s \cdot \zeta_a^t = \zeta_{ab}^{as+bt} = \zeta_{ab}$, and so ζ_{ab} is contained in the composite field of $\mathbb{Q}(\zeta_a)$ and $\mathbb{Q}(\zeta_b)$. Hence the composite field is $\mathbb{Q}(\zeta_{ab})$.
    - Then since $[\mathbb{Q}(\zeta_{ab}) : \mathbb{Q}] = \varphi(ab) = \varphi(a)\varphi(b) = [\mathbb{Q}(\zeta_a) : \mathbb{Q}] \cdot [\mathbb{Q}(\zeta_b) : \mathbb{Q}]$, by the formula for the degree of a composite extension we must have $[\mathbb{Q}(\zeta_a) \cap \mathbb{Q}(\zeta_b) : \mathbb{Q}] = 1$ so $\mathbb{Q}(\zeta_a) \cap \mathbb{Q}(\zeta_b) = \mathbb{Q}$.
    - The statement about the Galois group of $\mathbb{Q}(\zeta_{ab})/\mathbb{Q}$ follows immediately from our result on the Galois group of a composite of Galois extensions. The second statement then follows by a trivial induction by breaking n into the individual prime power factors.
    - Remark: More generally, by replacing $sa + tb = 1$ with $sa + tb = \gcd(a, b)$, one may adapt the proof above to show that for any a and b, the composite of $\mathbb{Q}(\zeta_a)$ and $\mathbb{Q}(\zeta_b)$ is $\mathbb{Q}(\zeta_{\mathrm{lcm}(a,b)})$ and the intersection is $\mathbb{Q}(\zeta_{\gcd(a,b)})$.
- By using this decomposition of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, we can show that every abelian group appears as a Galois group over $\mathbb{Q}$:
- Theorem (Abelian Galois Groups over $\mathbb{Q}$): If G is an abelian group, then there exists an extension $K/\mathbb{Q}$ with Galois group isomorphic to G.
    - Proof: By the classification of finite abelian groups, G is isomorphic to a direct product of cyclic groups, say as $G \cong (\mathbb{Z}/m_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_k\mathbb{Z})$.
    - By a theorem of Dirichlet[7], for any positive integer m there exist infinitely many primes congruent to 1 modulo m. In particular, we may choose distinct primes p_i such that $p_i \equiv 1 \bmod m_i$ for each i.
    - Then since m_i divides $|\mathrm{Gal}(\mathbb{Q}(\zeta_{p_i})/\mathbb{Q}| = p_i - 1$ and $\mathrm{Gal}(\mathbb{Q}(\zeta_{p_i})/\mathbb{Q}$ is cyclic, there exists a subgroup of index m_i.
    - If K_i represents the corresponding fixed field, then $K_i/\mathbb{Q}$ is Galois (since $\mathrm{Gal}(\mathbb{Q}(\zeta_{p_i})/\mathbb{Q}$ is abelian, so every subgroup is normal) and by the fundamental theorem of Galois theory we see that its Galois group is cyclic of order m_i.
    - By our results above, since the p_i are distinct primes, the intersection of any two of the fields $\mathbb{Q}(\zeta_{p_i})$ is $\mathbb{Q}$, so the same holds for the fields K_i.
    - Hence by our results on Galois groups of composites, we see that the Galois group of $K = K_1 K_2 \cdots K_k$ over $\mathbb{Q}$ is isomorphic to $\mathrm{Gal}(K_1/\mathbb{Q}) \times \mathrm{Gal}(K_2/\mathbb{Q}) \times \cdots \times \mathrm{Gal}(K_k/\mathbb{Q}) \cong (\mathbb{Z}/m_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_k\mathbb{Z}) \cong G$, as desired.
- Perhaps surprisingly, the converse of this theorem is also true (although much harder to prove):
- Theorem (Kronecker-Weber): If $K/\mathbb{Q}$ is a Galois extension with abelian Galois group, then K is contained in a cyclotomic extension of $\mathbb{Q}$.
    - This theorem was originally stated and mostly proven by Kronecker in the 1850s (his argument contained gaps in the case where the Galois group had order a power of 2), and Weber gave another proof in the 1880s (which also contained some gaps).

[7] More generally, if a is relatively prime to m, Dirichlet's theorem on primes in arithmetic progression says that there exist infinitely many primes congruent to a modulo m. For the case with $a = 1$ that we used here, we can outline a proof using cyclotomic polynomials: first, for any nonconstant polynomial in $\mathbb{Z}[x]$ with constant term ± 1, since n divides $p(n) - p(0)$ for any n, we see that there are infinitely many different primes dividing at least one of $p(1)$, $p(2)$, $p(3)$, ... Applying this result for $p(x)$ equal to the mth cyclotomic polynomial, we see that there are infinitely many different primes dividing at least one of $\Phi_m(1)$, $\Phi_m(2)$, ... Then one can show that if p does not divide m and $\Phi_m(k) \equiv 0 \bmod p$, then k is relatively prime to p and has order m in $(\mathbb{Z}/p\mathbb{Z})^\times$, which in turn implies $p \equiv 1 \bmod m$.

- In general, if $\mathrm{Gal}(K/F)$ is abelian, we say that K/F is an abelian extension. Since abelian groups are (in a sense) the least complicated finite groups, abelian extensions tend to be particularly well-behaved (for example, all of their intermediate fields are Galois).
- The problem of understanding the structure of all abelian extensions of other finite-degree extensions of $\mathbb{Q}$ falls under the branch of number theory known as class field theory, which generalizes and combines many threads from classical number theory, and has in turn been generalized and extended in other ways.

- For general finite groups G, it is still an open problem whether G is the Galois group of some extension $K/\mathbb{Q}$.
  - The problem of computing which groups occur as Galois groups over $\mathbb{Q}$, or more generally over an arbitrary field F, is known as the inverse Galois problem.

- As a final remark, we note that it is also possible to apply some of these results to study the roots of unity over an arbitrary field F.
  - Since the polynomials $\Phi_n(x)$ are monic and have integer coefficients, the primitive nth roots of unity will still be the roots of $\Phi_n(x)$, although $\Phi_n(x)$ may no longer be irreducible or separable over F.
  - In general, if ζ_n is any primitive nth root of unity, then $F(\zeta_n)/F$ is the splitting field of $\Phi_n(x)$ and if $\Phi_n(x)$ is separable, it will be Galois with cyclic Galois group.

4.3.5 Constructible Numbers and Regular Polygons

- Using the fundamental theorem of Galois theory, we can also give another characterization of constructible numbers, which will serve as a prototype for our work later on solvability in radicals:

- Theorem (Constructible Numbers): The number $\alpha \in \mathbb{C}$ is constructible over $\mathbb{Q}$ if and only if the Galois group of its minimal polynomial over $\mathbb{Q}$ has order a power of 2.
  - Proof: Suppose the minimal polynomial α over $\mathbb{Q}$ is $m(x)$. Let K be the splitting field of $m(x)$ over $\mathbb{Q}$ and suppose $\mathrm{Gal}(K/\mathbb{Q}) = G$.
  - If α is constructible, we have a tower of quadratic extensions $\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_d$ with $[K_{i+1} : K_i] = 2$ and $\alpha \in K_d$.
  - If L is any Galois extension of $\mathbb{Q}$ containing K_d, then $KL/\mathbb{Q}$ is also Galois. For any $\sigma \in \mathrm{Gal}(KL/\mathbb{Q})$, we have a tower of quadratic extensions $\mathbb{Q} = \sigma(K_0) \subseteq \sigma(K_1) \subseteq \cdots \subseteq \sigma(K_d)$ with $[\sigma(K_{i+1}) : \sigma(K_i)] = 2$ and $\sigma(\alpha) \in K_d$.
  - Thus, all Galois conjugates of α over $\mathbb{Q}$ are constructible. It is then an easy induction to see that if $\alpha_1, \ldots, \alpha_n$ are the roots of $m(x)$, then $[\mathbb{Q}(\alpha_1, \ldots, \alpha_k) : \mathbb{Q}(\alpha_1, \ldots, \alpha_{k-1})]$ is a power of 2 for each k, and hence $|G| = [K : \mathbb{Q}] = [\mathbb{Q}(\alpha_1, \ldots, \alpha_n) : \mathbb{Q}]$ is also a power of 2, as claimed.
  - For the converse, suppose $|G| = 2^n$. We first show by induction on n that there exists a chain of subgroups $G = G_0 \geq G_1 \geq \cdots \geq G_n = \{e\}$ such that $[G_i : G_{i+1}]$ has order 2 for each i.
  - The base case $n = 1$ is trivial, since we have the obvious chain $G = G_0 \geq G_1 = \{e\}$.
  - For the inductive step, we recall that there is at least one nonidentity element of G in the center $Z(G)$ of G. By taking an appropriate power we may assume $z \in Z(G)$ has order 2: then the subgroup $\langle z \rangle$ has order 2 and is normal in G.
  - The quotient group $\overline{G} = G/\langle z \rangle$ therefore has order 2^{n-1} so by the inductive hypothesis it has a chain of subgroups $\overline{G} = \overline{G_0} \geq \overline{G_1} \geq \cdots \geq \overline{G_{n-1}} = \{\overline{e}\}$ where $[\overline{G_i} : \overline{G_{i+1}}] = 2$ for each i.
  - Then by the fourth isomorphism theorem, we may lift each of the $\overline{G_i}$ to a subgroup G_i of G containing $\langle z \rangle$ with $G_i/G_{i+1} \cong \overline{G_i}/\overline{G_{i+1}}$.
  - We then have a chain of subgroups $G = G_0 \geq G_1 \geq \cdots \geq G_{n-1} = \langle z \rangle \geq G_n = \{e\}$ with $[G_i : G_{i+1}] = 2$ for each i, as required.
  - Finally, apply the fundamental theorem of Galois theory to this chain of subgroups: we obtain a chain of subfields $\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = K$ with $[K_{i+1} : K_i] = 2$ for each i. Since $\alpha \in K$, this shows α lies in a tower of quadratic extensions and is therefore constructible, as claimed.

- As an immediate application we can characterize the constructible regular n-gons:
- Corollary (Constructible n-gons): The regular n-gon is constructible by straightedge and compass if and only if $\varphi(n)$ is a power of 2, if and only if n is a power of 2 times a product of distinct primes of the form $2^{2^k}+1$ for some integer k.
    - Proof: As we showed, the regular n-gon is constructible if and only if $\cos(2\pi/n)$ is constructible, and it is easy to see that since $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n + \zeta_n^{-1})] = 2$, that $\cos(2\pi/n)$ is constructible if and only if ζ_n is constructible.
    - Then since $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is a Galois extension with Galois group $(\mathbb{Z}/n\mathbb{Z})^\times$ of order $\varphi(n)$, the result above shows that ζ_n is constructible precisely when $\varphi(n)$ is a power of 2.
    - The second statement follows by considering the prime factorization $n = p_1^{a_1} \cdots p_k^{a_k}$ of n: since $\varphi(n) = \varphi(p_1^{a_1}) \cdots \varphi(p_k^{a_k})$ we see $\varphi(p_i^{a_i}) = p_i^{a_i - 1}(p_i - 1)$ must be a power of 2, which requires either $p_i = 2$ or $a_i = 1$ and $p_i - 1$ to be a power of 2.
    - In the latter case (requiring $p = 2^k + 1$) then if k has an odd prime factor d then $2^k + 1$ is divisible by $2^d + 1$ and is therefore not prime. Hence the only primes of this form are $2^{2^k} + 1$ for some integer k, as claimed.
    - Remark: The primes of the form $p_n = 2^{2^n} + 1$ are called Fermat primes. Fermat conjectured that all of these numbers were prime based on the fact that $p_0 = 3$, $p_1 = 5$, $p_2 = 17$, and $p_3 = 65537$ are prime; however, p_4 was shown to be composite by Euler. The numbers p_5 through p_{32} have subsequently been proven composite, and it is now unknown whether there are any other Fermat primes at all!

4.4 Galois Groups of Polynomials

- If K/F is a Galois extension and we have an explicit description of the action of $\mathrm{Gal}(K/F)$ on the elements of K, we have described in detail how to use the fundamental theorem of Galois theory to compute intermediate fields and minimal polynomials of elements.
    - However, all of this discussion presupposes our ability to compute the Galois group and its action on K.
    - If K is described only as the splitting field of a polynomial $p(x) \in F[x]$, it is not generally obvious how to determine the Galois group nor even how to compute the degree K/F.
    - Our goal in this section is to describe methods for computing Galois groups of general polynomials (recall that the Galois group of $p(x)$ over F is simply the Galois group of the splitting field).
    - Since this can become quite difficult when the degree of the polynomial is large, we will focus primarily on polynomials of small degree.
- As we have previously observed, if $p(x) \in F[x]$ is a separable polynomial of degree n with splitting field K, then any $\sigma \in \mathrm{Gal}(K/F)$ is completely determined by its permutation of the roots of p.
    - If we fix an ordering of the roots, then we obtain an injective homomorphism from $\mathrm{Gal}(K/F)$ into the symmetric group S_n, and so we may view the Galois group interchangeably with its image in S_n.
    - For example, for $p(x) = (x^2-2)(x^2-3)(x^2-6)$ over $\mathbb{Q}$, the splitting field is $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ with Galois group generated by the automorphisms σ and τ with $\sigma(\sqrt{2}, \sqrt{3}) = (-\sqrt{2}, \sqrt{3})$ and $\tau(\sqrt{2}, \sqrt{3}) = (\sqrt{2}, -\sqrt{3})$.
    - If we label the six roots $\{\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}, \sqrt{6}, -\sqrt{6}\}$ as $\{1, 2, 3, 4, 5, 6\}$, then σ corresponds to the permutation $(1\,2)(5\,6)$, τ corresponds to the permutation $(3\,4)(5\,6)$, and $\sigma\tau$ corresponds to the permutation $(1\,2)(3\,4)$.
- We also observe that automorphisms must act as permutations on the roots of the irreducible factors of $p(x)$.
    - Thus, we may study the action of each element of $\mathrm{Gal}(K/F)$ on the roots of each irreducible factor of $p(x)$ separately.
    - If $q(x)$ is an irreducible factor of $p(x)$ of degree m, then as we have shown, the roots of $q(x)$ are all Galois conjugates.

- Thus, the Galois group permutes the roots of $q(x)$ transitively, meaning that for any roots α, β of $q(x)$, there is some $\sigma \in \mathrm{Gal}(K/F)$ with $\sigma(\alpha) = \beta$.
- In particular, if $p(x)$ is itself irreducible, then $\mathrm{Gal}(K/F)$ must be a transitive subgroup of S_n. This information reduces (rather substantially) the number of possibilities.

4.4.1 Symmetric Functions

- We first analyze the Galois group of a "generic" polynomial, which requires studying the relationship between the coefficients of a polynomial and its roots.
  - If $p(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_0$ is monic and has roots $x_1, x_2, \ldots, x_n$, then $p(t) = (t-x_1)(t-x_2)\cdots(t-x_n)$.
  - Expanding out and comparing coefficients shows that $a_{n-1} = -(x_1 + x_2 + \cdots + x_n)$, $a_{n-2} = x_1x_2 + x_1x_3 + \cdots + x_1x_n + x_2x_3 + \cdots + x_{n-1}x_n$, ... , and $a_0 = (-1)^n x_1 x_2 \cdots x_n$.
  - The functions of the x_i appearing in the coefficients are symmetric functions in the roots:
- Definition: If $x_1, \ldots, x_n$ are fixed indeterminates, then for $1 \leq k \leq n$, the kth elementary symmetric function s_k in $x_1, \ldots, x_n$ is given by the sum of all products of the x_i taken k at a time. Explicitly, we have

$$\begin{aligned} s_1 &= x_1 + x_2 + x_3 + \cdots + x_n \\ s_2 &= x_1x_2 + x_1x_3 + \cdots + x_1x_n + x_2x_3 + \cdots + x_{n-1}x_n \\ s_3 &= x_1x_2x_3 + \cdots + x_{n-2}x_{n-1}x_n \\ &\vdots \quad \vdots \quad \vdots \\ s_n &= x_1x_2x_3\cdots x_n \end{aligned}$$

  - From the discussion above, we see that if $p(t)$ is monic and has roots $x_1, x_2, \ldots, x_n$, then $p(t) = (t - x_1)(t - x_2)\cdots(t - x_n) = t^n - s_1t^{n-1} + s_2t^{n-2} + \cdots + (-1)^n s_n$.
- If F is any field, this means that the field $F(x_1, x_2, \ldots, x_n)$ is a Galois extension of $F(s_1, s_2, \ldots, s_n)$, since it is the splitting field of the polynomial $p(t) = t^n - s_1t^{n-1} + s_2t^{n-2} + \cdots + (-1)^n s_n$. Our first goal is to determine the Galois group of this extension:
- Proposition (Generic Galois Group): The field $F(x_1, x_2, \ldots, x_n)$ is a Galois extension of $F(s_1, s_2, \ldots, s_n)$ whose degree is $n!$ and whose Galois group is isomorphic to S_n. Explicitly, the isomorphism is provided by the group action of S_n on $F(x_1, x_2, \ldots, x_n)$ via index permutation.
  - Proof: As noted above, the extension is Galois because it is the splitting field of the polynomial $p(t) = t^n - s_1t^{n-1} + s_2t^{n-2} + \cdots + (-1)^n s_n$. Let G be the Galois group.
  - As we have discussed previously, S_n acts on $F[x_1, \ldots, x_n]$ via index permutation, with the action given by $\sigma \cdot p(x_1, \ldots, x_n) = p(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$. It is easy to see that this action is also well-defined on rational functions.
  - Furthermore, each of the elementary symmetric functions $s_1, s_2, \ldots, s_n$ is invariant under any permutation of the variable indices, so $F(s_1, s_2, \ldots, s_n)$ is fixed under this action, and therefore is an automorphism of $F(x_1, x_2, \ldots, x_n)/F(s_1, s_2, \ldots, s_n)$.
  - This means S_n is (isomorphic to) a subgroup of G, since the only permutation map fixing $F(x_1, x_2, \ldots, x_n)$ is the identity permutation.
  - In particular, we see $|G| \geq |S_n| = n!$, and therefore $[F(x_1, x_2, \ldots, x_n) : F(s_1, s_2, \ldots, s_n)] = |G| \geq n!$.
  - On the other hand, because $F(x_1, x_2, \ldots, x_n)$ is the splitting field of the degree-n polynomial $p(t)$ over $F(s_1, s_2, \ldots, s_n)$, we see that $[F(x_1, x_2, \ldots, x_n) : F(s_1, s_2, \ldots, s_n)] \leq n!$ by our bounds on the degree of a splitting field.
  - Therefore, we must have equality, so $[F(x_1, x_2, \ldots, x_n) : F(s_1, s_2, \ldots, s_n)] = n!$.
  - Then $|G| = n! = |S_n|$, and the elements of G are precisely the automorphisms induced by index permutations, so that $G \cong S_n$.

- As a corollary, we obtain the following classical result about symmetric functions:
- Corollary (Symmetric Functions): If $p(x_1, x_2, \ldots, x_n)$ is a rational function over a field F that is symmetric in the variables $x_1, x_2, \ldots, x_n$, then it is a rational function in the symmetric functions $s_1, s_2, \ldots, s_n$.
    - As an example, the function $p(x_1, x_2, x_3) = x_1^3 + x_2^3 + x_3^3$ is symmetric in x_1, x_2, and x_3, and indeed one can verify that $p(x_1, x_2, x_3) = s_1^3 - 3s_1s_2 + 3s_3$.
    - Proof: Let $L = F(x_1, x_2, \ldots, x_n)$ and $K = F(s_1, s_2, \ldots, s_n)$. If $p(x_1, x_2, \ldots, x_n)$ is a rational function that is symmetric in $x_1, x_2, \ldots, x_n$, then it lies in the fixed field of $G = \text{Gal}(L/K)$.
    - But by our characterization of Galois extensions, the fixed field of G is simply the base field: thus, p is an element of K, meaning that it is a rational function in $s_1, s_2, \ldots, s_n$.
    - Remark: If $p(x_1, x_2, \ldots, x_n)$ is a polynomial that is symmetric in the x_i, then in fact one can show that p is necessarily a polynomial function of the elementary symmetric functions.
- Our results above, loosely speaking, say that the Galois group of a "generic" degree-n polynomial is S_n, in the sense that if the s_i are indeterminates, then the Galois group of $p(t) = t^n - s_1t^{n-1} + \cdots + (-1)^n s_n$ is isomorphic to S_n.
    - However, by itself, this result does not actually give any information about the Galois group for any specific values of the parameters s_i.
    - We would like to be able to "specialize" the choices of the s_i by setting them equal to specific elements of the field F. However, choosing values for the s_i may introduce algebraic relations between them that shrink the size of the Galois group.
    - Over a finite field, for example, no matter what values we choose for the coefficients, the Galois group will always be cyclic (since every extension of finite fields is Galois with cyclic Galois group), so for $n \geq 3$ we will always obtain some "collapsing" of the Galois group structure from S_n.
    - Over $\mathbb{Q}$ (or more generally finite extensions of $\mathbb{Q}$), however, a theorem of Hilbert known as Hilbert's irreducibility theorem gives a sufficient condition for specializations not to collapse, in the sense that the Galois group of the specialization will be isomorphic to the Galois group of the original "generic" family.
    - In particular, by applying Hilbert's irreducibility theorem to the extension $F(x_1, x_2, \ldots, x_n)/F(s_1, s_2, \ldots, s_n)$, one may deduce that "most" specializations of the s_i at elements of $\mathbb{Q}$ will yield a polynomial with Galois group S_n.

4.4.2 Discriminants of Polynomials

- If F is a field of characteristic not equal to 2, then we may find the roots of a degree-2 polynomial in $F[x]$ via the usual procedure of completing the square.
    - Explicitly, if $p(t) = at^2 + bt + c$, then $p(t) = 0$ is equivalent to $a(t + b/(2a))^2 + (c - b^2/(4a)) = 0$, and then rearranging and extracting the square root yields the usual quadratic formula $t = \dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$.
    - The nature of the roots is closely tied to the value of the discriminant $D = b^2 - 4ac$: for example, the polynomial has a repeated root (i.e., is inseparable) precisely when $D = 0$, and the roots generate the extension $F(\sqrt{D})$, which has special properties when D is a perfect square.
    - In terms of the roots r_1 and r_2 themselves, we can see that when $p(t)$ is monic, $D = (r_1 - r_2)^2$.
- We can generalize the idea of a discriminant to an arbitrary polynomial:
- Definition: If $x_1, x_2, \ldots, x_n$ are arbitrary, we define the discriminant $\Delta(x_1, \ldots, x_n)$ as the product $\prod_{i=1}^{n} \prod_{j=i+1}^{n} (x_i - x_j)^2 = \prod_{i<j} (x_i - x_j)^2$, and we define the discriminant $\Delta(p)$ of the polynomial p with roots $r_1, \ldots, r_n$ (including multiplicities) to be $\Delta(r_1, \ldots, r_n)$.
    - When the terms are clear from context, we will often write the discriminant merely as Δ.
    - Note that $\Delta(x_1, \ldots, x_n)$ is a symmetric polynomial in the x_i, and is thus an element of $F[s_1, \ldots, s_n]$.

- In particular, this means that $\Delta(p)$ is a polynomial function in the coefficients of p. However, since the total degree of Δ in the x_i is $n(n-1)$, for large n the resulting expressions will be quite complicated.
- Even for the degree-3 polynomial $p(t) = t^3+at^2+bt+c$, the formula is $\Delta = -27c^2+18abc-4b^3-4a^3c+a^2b^2$.

- We have also encountered the discriminant in our analysis of the alternating group A_n.
  - Specifically, we showed that the square root of the discriminant $\sqrt{\Delta} = \prod_{i<j}(x_i - x_j)$ has the property that $\sigma(\sqrt{\Delta}) = \sqrt{\Delta}$ for $\sigma \in A_n$, and $\sigma(\sqrt{\Delta}) = -\sqrt{\Delta}$ for $\sigma \notin A_n$.
  - If the characteristic of F is not equal to 2, this means $\sqrt{\Delta}$ is not fixed by all of S_n, but its square is: thus, $\sqrt{\Delta}$ generates a degree-2 extension of $F(s_1, s_2, \ldots, s_n)$.
  - Since $[S_n : A_n] = 2$, by the fundamental theorem of Galois theory, we conclude that $\sqrt{\Delta}$ generates the fixed field of A_n.

- By applying this to specific polynomials, we obtain the following very useful fact:

- Proposition (A_n and Discriminants): If F is a field of characteristic not 2, and $p(x) \in F[x]$ is any separable polynomial, then the Galois group of $p(x)$ is a subgroup of A_n if and only if $\sqrt{\Delta(p)} \in F$.
  - Proof: As we remarked above, $\Delta = \Delta(p)$ is symmetric in the roots of p and is therefore fixed by every element of the Galois group G of p.
  - If we fix an ordering of the roots $r_1, \ldots, r_n$ of p, then $\sqrt{\Delta(p)} = \prod_{i<j}(r_i - r_j)$ is an element of the splitting field K.
  - Then if σ is any element of the Galois group, we see that $\sigma(\sqrt{\Delta}) = \epsilon(\sigma) \cdot \sqrt{\Delta}$, where $\epsilon(\sigma)$ is the sign of the permutation that σ induces on the roots.
  - Since the characteristic of F is not 2 (so that $\sqrt{\Delta} \neq -\sqrt{\Delta}$) we see that σ fixes $\sqrt{\Delta}$ if and only if $\sigma \in A_n$.
  - Thus, the Galois group is a subgroup of A_n if and only if every element of the Galois group fixes $\sqrt{\Delta}$, which is in turn equivalent to saying that $\sqrt{\Delta} \in F$.

4.4.3 Cubic Polynomials

- We now study degree-3 polynomials using the tools we have developed so far.
  - If $f(t) \in F[t]$ is a reducible degree-3 polynomial, everything reduces to the case of lower degree.
  - If $f(t)$ factors either as a product of 3 degree-1 terms, then the splitting field of f is F and the Galois group is trivial.
  - If $f(t)$ factors as a product of a degree-1 term and an irreducible degree-2 term, then the splitting field of p is a quadratic extension of F (obtained by solving the quadratic equation) and the Galois group is $\mathbb{Z}/2\mathbb{Z}$.

- The interesting case is for an irreducible polynomial, so suppose $f(t) = t^3 - a_1t^2 + a_2t - a_3$ is an irreducible cubic polynomial in $F[t]$ with splitting field K.
  - If f has roots $\beta_1, \beta_2, \beta_3$, then since $a_1 = s_1$ is the sum of the roots, we have $\beta_3 = a_1 - \beta_1 - \beta_2$. Thus, $K = F(\beta_1, \beta_2, \beta_3) = F(\beta_1, \beta_2)$.
  - We therefore have a tower of extensions $F \subset F(\beta_1) \subseteq F(\beta_1, \beta_2) = K$, where $[F(\beta_1) : F] = 3$ and $[K : F(\beta_1)] \leq 2$.
  - Since p is irreducible, the Galois group of f is a transitive subgroup of S_3. It is easy to see that there are only two such subgroups, namely S_3 and A_3, and from our discussion above, we can tell these cases apart by looking at the discriminant (as long as the characteristic of F is not 2).
  - When the Galois group is A_3, this means that if α is any root of f in K, then $K = F(\alpha)$. (In particular, the other roots of f will be polynomials in α.) Furthermore, there are no proper nontrivial intermediate fields of K/F since A_3 has no nontrivial proper subgroups.

- When the Galois group is S_3, there are nontrivial proper subgroups, which (by the Galois correspondence) correspond to intermediate fields: specifically, there is the quadratic subfield of K fixed by A_3 (which by our discussion is generated by the square root of the discriminant), and also the three cubic subfields of K each fixed by a transposition (each of which will be generated by one of the three roots of f).

- We summarize these observations in the following proposition:

- Proposition (Galois Groups of Cubics): If F is a field of characteristic not equal to 2 and $f(t) = t^3 - a_1t^2 + a_2t - a_3$ is an irreducible cubic polynomial in $F[t]$, then the Galois group of p is either A_3 or S_3, and it is A_3 precisely when the discriminant $\Delta(p) = -27a_3^2 + 18a_1a_2a_3 - 4a_2^3 - 4a_1^3a_3 + a_1^2a_2^2$ is a square in F.

  - Proof: As noted above, if f is irreducible then the Galois group is a transitive subgroup of S_3, hence is either S_3 or A_3. By our results on discriminants, it is A_3 precisely when the discriminant is a square in F.
  - To compute the formula for the discriminant, if the characteristic of F is not 3, we may make a change of variables $y = t - a_1/3$ and then analyze the polynomial $g(y) = y^3 + py + q$ where $p = a_2 - a_1^3/3$ and $q = (-2/27)a_1^3 + a_1a_2/3 - a_3$ are F-rational polynomials in the original coefficients.
  - Since the roots of g are translates of the roots of f, the discriminants of f and g are the same (since the discriminant only involves the pairwise differences of the roots).
  - Since $\Delta(g)$ is a symmetric polynomial of homogeneous degree 6 (i.e., every term has degree 6) in its roots r_1, r_2, r_3, it is a polynomial in s_1, s_2, s_3, and since $s_1 = 0$ we may ignore it. Since s_2 is homogeneous of degree 2 and s_3 is homogeneous of degree 3, we must have $\Delta(g) = c_1 \cdot s_2^3 + c_2 \cdot s_3^2$ since these are the only homogeneous polynomials in s_1, s_2, s_3 of degree 6.
  - We may compute c_1 and c_2 by picking values for r_1, r_2, r_3 and then comparing the value of $\Delta(s)$ to $c_1 \cdot s_2^3 + c_2 \cdot s_3^2$. Choosing, for example, $(r_1, r_2, r_3) = (-1, 0, 1)$ and $(-2, 1, 1)$ leads to the equations $4 = c_1(-1)^3 + c_2(0)$ and $0 = c_1(-3)^3 + c_2(-2)^2$, whence $c_1 = -4$ and $c_2 = -27$.
  - Hence $\Delta(f) = \Delta(g) = -4p^3 - 27q^2$, and then plugging back in for a_1, a_2, a_3 and simplifying eventually yields the given formula (which one may verify is also correct in characteristic 3).

- The technique employed in the proof above, of making a change of variables to simplify the form of the cubic equation, is very useful and will allow us to reduce (sometimes, greatly) the amount of computation required in examples.

- Example: Find the Galois group of $f(t) = t^3 - 3t + 1$ over $\mathbb{Q}$ and identify all subfields of its splitting field.

  - This cubic is irreducible over $\mathbb{Q}$ since it has no roots by the rational root test.
  - Using the formula from the (proof of) the proposition, we see that $\Delta(f) = 4 \cdot 3^3 - 27 = 81$. Since this is a perfect square in $\mathbb{Q}$, the Galois group is $\boxed{A_3}$.
  - Since the splitting field has degree 3, its only subfields are itself and $\mathbb{Q}$.
  - After some effort, one may show that if α is a root of f then so is $\alpha^2 - 2$. Hence, if α is one root of f, then the others are $\alpha^2 - 2$ and $(\alpha^2 - 2)^2 - 2 = -\alpha^2 - \alpha - 2$.

- Example: Find the Galois group of $f(t) = t^3 + t + 1$ over $\mathbb{Q}$ and identify all subfields of its splitting field.

  - This cubic is is irreducible over $\mathbb{Q}$ since it has no roots by the rational root test.
  - Using the formula from the (proof of) the proposition, we see that $\Delta(f) = -4 \cdot 1^3 - 27 = -31$. Since this is not a perfect square in $\mathbb{Q}$, the Galois group is $\boxed{S_3}$.
  - By the fundamental theorem of Galois theory, there is a unique quadratic subfield of the splitting field, namely $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{-31})$.
  - There are also three conjugate degree-3 subfields, namely, $\mathbb{Q}(\beta_1)$, $\mathbb{Q}(\beta_2)$, and $\mathbb{Q}(\beta_3)$ where $\beta_1, \beta_2, \beta_3$ are the three roots of f.
  - Another way of seeing that the Galois group must be S_3 is that by calculus, the polynomial has one real root and two (necessarily) complex-conjugate roots. Therefore, complex conjugation is an element of the Galois group that transposes two of the roots (hence has order 2), so the Galois group must be S_3.

- Although we have computed the Galois group of an arbitrary cubic, the results do not actually give us an explicit description of the fields of interest, since we do not have formulas for the roots.
  - The problem of finding a general formula for the roots of a cubic equation was considered by the ancient Egyptians and Greeks (one aspect of which was the attempt to construct cube roots using straightedge and compass, as we have previously discussed), and also by a number of later mathematicians.
  - Ultimately, the story of how the cubic formula was eventually publicized is rather convoluted, and we will briefly summarize it.
  - Minimal progress was made on solving the cubic until the early 1500s, when del Ferro discovered a method for solving cubics of the form $t^3 + pt = q$. However, due to the nature of Renaissance patronage, he did not publicize his method, but only taught it to his student Fior.
  - In 1535, Fior in turn challenged another scholar, Niccolo Fontana (nicknamed Tartaglia due to a physical deformity), who eventually (re)discovered the solution to the cubic, and (again, as was normal at the time) kept it a secret.
  - Eventually, Gerolamo Cardano (an avid astrologer and gambler who at one time was one of the most well-regarded physicians in Europe, who was eventually jailed for heresy and then pardoned by the Pope) was able, after repeated entreaties and vows never to reveal Tartaglia's method, to coax Tartaglia into revealing it.
  - Cardano was then able to extend Tartaglia's method to solve the general cubic equation, and eventually took a student, Ludovico Ferrari, who was able to extend Cardano's techniques to solve degree-4 equations. Cardano and Ferrari eventually discovered that del Ferro had solved the cubic prior to Tartaglia's discovery of the solution, and published his generalization in 1545, giving credit to del Ferro, Fior, and Tartaglia. (Despite receiving proper attribution, Tartaglia nonetheless felt betrayed by Cardano, despite the fact that del Ferro had developed the technique prior to Tartaglia.)
- We will present a solution of the cubic similar to Cardano's (and presumably, also to Tartaglia's).
- Theorem (Cardano's Formulas): If the characteristic of F is not 2 or 3, and the polynomial $g(t) = t^3 + pt + q$ is irreducible and separable over F, then for $A = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$ and $B = \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$ with cube roots chosen so that $AB = -p/3$, the three roots of g are $A + B$, $\zeta_3 A + \zeta_3^2 B$, and $\zeta_3^2 A + \zeta_3 B$, where $\zeta_3 = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$ is a primitive 3rd root of unity over F.
  - Proof: From the algebraic identity $(x+y)^3 - 3xy(x+y) = x^3 + y^3$, we can see that if we take $x + y = t$, $3xy = -p$, and $x^3 + y^3 = -q$, then the identity becomes $t^3 + pt + q = 0$.
  - The equation $3xy = -p$ implies $y = -p/(3x)$, and then $x^3 + y^3 = -q$ becomes $x^3 - p^3/(27x^3) = -q$, whence $x^6 + qx^3 - \frac{p^3}{27} = 0$. (Note that we need the characteristic not to be 3, in order to divide by 27.)
  - This is a quadratic in x^3, so solving yields $x^3 = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$ and then $y^3 = -q - x^3 = -\frac{q}{2} \mp \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$. (Note that we are using the fact the characteristic is not 2 to invoke the quadratic formula here.)
  - Since we may interchange x and y, let us assume $x^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$ and $y^3 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$.
  - Then there are three possible values for x, namely $x = \zeta_3^k \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$, and since we must also have $3xy = p$, any choice of x yields a unique value for y, namely $y = \zeta_3^{2k} \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$.
  - Thus, we obtain the claimed solutions $t = \zeta_3^k \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \zeta_3^{2k} \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$ for $k \in \{0, 1, 2\}$.
- Example: Find the roots of the cubic $f(t) = t^3 + t + 1$ over $\mathbb{Q}$.

- By Cardano's formulas, we compute $A = \sqrt[3]{-\frac{1}{2} + \sqrt{\frac{31}{108}}}$ and $B = \sqrt[3]{-\frac{1}{2} + \sqrt{\frac{31}{108}}}$.
- Thus, the three roots of f are $A + B$, $\zeta_3 A + \zeta_3^2 B$, and $\zeta_3^2 A + \zeta_3 B$.

- Example: Find the roots of the cubic $f(t) = t^3 - 3t + 1$ over $\mathbb{Q}$.
  - By Cardano's formulas, we compute $A = \sqrt[3]{-\frac{1}{2} + \sqrt{-\frac{3}{4}}}$ and $B = \sqrt[3]{-\frac{1}{2} - \sqrt{-\frac{3}{4}}}$.
  - Thus, the three roots of f are $A + B$, $\zeta_3 A + \zeta_3^2 B$, and $\zeta_3^2 A + \zeta_3 B$.
  - For this polynomial we can compute more explicit descriptions of the roots, since the term under the cube root for A is $-\frac{1}{2} + \frac{\sqrt{-3}}{2} = \zeta_3$, while the term under the cube root for B is ζ_3^2.
  - Then we have $A = \sqrt[3]{\zeta_3} = \zeta_9$ while $B = \zeta_9^8$ (note that we must choose the cube roots so that $AB = 1$).
  - Hence the roots are in fact $A + B = \zeta_9 + \zeta_9^8 = 2\cos(2\pi/9)$, $\zeta_3 A + \zeta_3^2 B = \zeta_9^4 + \zeta_9^5 = 2\cos(8\pi/9)$, and $\zeta_3^2 A + \zeta_3 B = \zeta_9^7 + \zeta_9^2 = 2\cos(4\pi/9)$.

- In the second example above, notice that all of the original expressions for the roots from Cardano's formulas involved complex numbers, even though all of the roots are real.
  - In fact, this will always be the case when the polynomial has three real roots: if all three roots are real, then $\sqrt{\Delta}$ is also clearly real (since it is a polynomial in the roots), and so Δ is a nonnegative real number.
  - But in Cardano's formulas, we have $A = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} = \sqrt[3]{-\frac{q}{2} + \sqrt{-\Delta}}$, and likewise B also involves $\sqrt{-\Delta}$.
  - On the other hand, if the polynomial has two complex-conjugate roots, then in fact Δ will always be negative: to see this, suppose the roots are $x + iy$, $x - iy$, w with x, y, w real.
  - Then $\sqrt{\Delta} = (2iy)(x+iy-w)(x-iy-w) = (2iy)[(x-w)^2+y^2]$ is purely imaginary, and so Δ is negative.
  - As a coda to the tortuous history of the cubic, we will remark that it is this perplexing appearance of square roots of negative numbers in the formulas for real solutions to cubic equations that led to the initial development of complex numbers in mathematics.
  - To illustrate, for the cubic $p(t) = t^3 - 15 - 4$, Cardano's formulas give $A = \sqrt[3]{2 + \sqrt{-121}}$ and $B = \sqrt[3]{-2 + \sqrt{-121}}$, even though one may verify that the three roots of this cubic are the real numbers 4 and $-2 \pm \sqrt{3}$.
  - To resolve this difficulty, Bombelli in 1572 observed that one may formally compute $(2 \pm \sqrt{-1})^3 = \pm 2 + \sqrt{-121}$, and so one may take $A = 2 + \sqrt{-1}$ and $B = 2 - \sqrt{-1}$ to obtain the correct root $A + B = 4$.
  - It turns out to be impossible to give general formulas involving only real radicals for the solutions of irreducible cubics with $\Delta < 0$, and so resolving this difficulty could only be achieved by working with non-real numbers.

4.4.4 Quartic Polynomials

- We may use similar techniques to analyze degree-4 polynomials, although because S_4 has many more subgroups than S_3, there are numerous possible Galois groups.
  - As before, if the polynomial is reducible then we may reduce to lower-degree cases, so assume that the polynomial $f(t) = t^4 - a_1 t^3 + a_2 t^2 - a_3 t + a_4$ is an irreducible quartic polynomial in $F[t]$ with splitting field K.
  - As in the cubic case, if $\beta_1, \beta_2, \beta_3, \beta_4$ are the roots of f, then $\beta_4 = a_1 - \beta_1 - \beta_2 - \beta_3$ and so $K = F(\beta_1, \beta_2, \beta_3)$.
  - In this case we obtain a tower of extensions $F \subset F(\beta_1) \subseteq F(\beta_1, \beta_2) \subseteq F(\beta_1, \beta_2, \beta_3) = K$, where $[F(\beta_1) : F] = 4$, $[F(\beta_1, \beta_2) : F(\beta_1)] \leq 3$, and $[K : F(\beta_1, \beta_2)] \leq 2$.

- By making a substitution $y = t - a_1/4$, as with the cubic, we may equivalently analyze the polynomial $g(y) = y^4 + py^2 + qy + r$, which will have the same Galois group and discriminant as f.
- A brief search will reveal that there are five possible isomorphism classes for the Galois group of g as transitive subgroups of S_4, namely, S_4, A_4, $D_{2\cdot 4}$, C_4 (the cyclic group of order 4), and V_4 (the Klein 4-group). As explicit permutation groups, one can write $D_{2\cdot 4} = \langle (1\,2\,3\,4),\, (1\,3)\rangle$, $C_4 = \langle (1\,2\,3\,4)\rangle$, and $V_4 = \langle (1\,2)(3\,4),\, (1\,3)(2\,4)\rangle$.
- By using the discriminant we can distinguish some possibilities: if the discriminant is a square, then the Galois group is a subgroup of A_4, and it is easy to see that there are two such subgroups: A_4 and V_4. If the discriminant is not a square, then the Galois group is one of the others: S_4, $D_{2\cdot 4}$, and C_4.

- To differentiate further between these possibilities, we may study other functions of the roots that are not fixed by all the elements in S_4.
  - As first described by Lagrange, one method is to consider the elements $\theta_1 = (\beta_1 + \beta_2)(\beta_3 + \beta_4)$, $\theta_2 = (\beta_1 + \beta_3)(\beta_2 + \beta_4)$, and $\theta_3 = (\beta_1 + \beta_4)(\beta_2 + \beta_3)$.
  - These elements are permuted by S_4, and the stabilizer of each individual element is a dihedral subgroup of S_4: for example, θ_2 is stabilized by the dihedral subgroup $\langle (1\,2\,3\,4),\, (1\,3)\rangle$ we wrote earlier, while the others are stabilized by appropriate conjugate subgroups. The stabilizer of all three elements is the Klein-four group V_4.
  - Since θ_1, θ_2, θ_3 are permuted by S_4, their elementary symmetric functions are fixed by S_4, and so the cubic polynomial whose roots are $\theta_1, \theta_2, \theta_3$ is fixed by the entire Galois group, so its coefficients lie in F.[8]
  - We may then compute $\theta_1+\theta_2+\theta_3 = 2s_2$, $\theta_1\theta_2+\theta_1\theta_3+\theta_2\theta_3 = s_1s_3+s_2^2-4s_4$, and $\theta_1\theta_2\theta_3 = s_1^2s_2s_3-s_1^2s_4-s_3^2$.
  - Since $s_1 = 0$, this means that $\theta_1, \theta_2, \theta_3$ are the three roots of the polynomial $h(z) = z^3 - 2pz^2 + (p^2 - 4r)z + q^2$, which is called the <u>resolvent cubic</u> of $g(y)$.
  - Very conveniently, the discriminant of this cubic is the same as the discriminant of the quartic, since $(\theta_1 - \theta_2)^2 = (\beta_1 - \beta_4)^2(\beta_2 - \beta_3)^2$ and likewise for the other two squared differences. (In particular, we see that the elements θ_i are distinct as long as the β_i are.)
  - If we can find the factorization of the resolvent cubic over F, then this will yield information about whether the elements θ_i are in F, which in turn gives information about the possible elements in the Galois group.

- <u>Theorem</u> (Galois Groups of Quartics): Suppose F has characteristic not 2 or 3, and let $f(y) = y^4+py^2+qy+r$ be an irreducible separable quartic over F with associated resolvent cubic $g(z) = z^3 - 2pz^2 + (p^2 - 4r)z + q^2$ and discriminant $\Delta = \Delta(f) = \Delta(g)$. Then the Galois group of f is one of S_4, A_4, $D_{2\cdot 4} \cong \langle (1\,2\,3\,4),\, (1\,3)\rangle$, $C_4 \cong \langle (1\,2\,3\,4)\rangle$, and $V_4 = \langle (1\,2)(3\,4),\, (1\,3)(2\,4)\rangle$. More specifically:
  1. The Galois group is V_4 if and only if Δ is a square in F and the resolvent cubic splits completely over F.
  2. The Galois group is A_4 if and only if Δ is a square in F and the resolvent cubic has no roots in F.
  3. The Galois group is S_4 if and only if Δ is not a square in F and the resolvent cubic has no roots in F.
  4. The Galois group is C_4 if and only if Δ is not a square in F, the resolvent cubic has exactly one root r' in F, and the polynomials $x^2 + r'$ and $x^2 + (r' - p)x + r$ both split over $F(\sqrt{\Delta})$.
  5. The Galois group is $D_{2\cdot 4}$ if and only if Δ is not a square in F, the resolvent cubic has exactly one root in F, and at least one of the polynomials $x^2 + r'$ and $x^2 + (r' - p)x + r$ is irreducible over $F(\sqrt{\Delta})$.

  - <u>Remark</u>: The condition differentiating C_4 and $D_{2\cdot 4}$ is a result due to Kappe and Warren from 1989. There is a more classical condition (specifically, whether $f(y)$ splits over $F(\sqrt{\Delta})$) that is harder to check that can also tell these groups apart.

[8] If one has the idea of trying to construct a cubic polynomial with coefficients in F whose roots $\theta_1, \theta_2, \theta_3$ are functions of $\beta_1, \beta_2, \beta_3, \beta_4$, then since $\theta_1, \theta_2, \theta_3$ would be Galois conjugates, the stabilizer of any one of them would necessarily be a subgroup of S_4 of index 3 (i.e., of order 8) and the only such subgroups of S_4 are dihedral groups of order 8. If one chooses a specific one of these dihedral subgroups, say $\langle (1\,2\,3\,4),\, (1\,3)\rangle$, then the corresponding element θ must be a function of $\beta_1, \beta_2, \beta_3, \beta_4$ that is fixed by both generators but not by all of S_4. There is no such function of degree 1, but there are essentially two choices of degree 2 given by $\theta = (\beta_1 + \beta_3)(\beta_2 + \beta_4)$ and $\theta = \beta_1\beta_3 + \beta_2\beta_4$.

- Implicit in our characterization is the fact that no other scenarios (e.g., Δ being a square and the resolvent cubic having exactly one root in F) can occur.
- We will also remark that the most efficient way to compute the discriminant Δ is to use the formula for the discriminant of the cubic $g(z)$.
- Proof: As we have shown above, if $\beta_1, \beta_2, \beta_3, \beta_4$ are the roots of $f(y)$, then the roots of the resolvent cubic $g(z)$ are $\theta_1 = (\beta_1 + \beta_2)(\beta_3 + \beta_4)$, $\theta_2 = (\beta_1 + \beta_3)(\beta_2 + \beta_4)$, and $\theta_3 = (\beta_1 + \beta_4)(\beta_2 + \beta_3)$, and that $\Delta(p) = \Delta(g)$.
- As we have also noted, up to conjugacy the only transitive subgroups of S_4 are S_4, A_4, $D_{2\cdot 4}$, C_4, and V_4, so the Galois group G must be one of these.
- First suppose that Δ is a square: then the Galois group is one of A_4 and V_4.
- If the resolvent cubic has all its roots in F, then all three of the θ_i are in F, meaning that they are fixed by G. Since the only elements of S_4 fixing each of $\theta_1, \theta_2, \theta_3$ are the elements of the Klein 4-group V_4, this means $G \subseteq V_4$, hence $G = V_4$
- If the resolvent cubic does not have all its roots in F, then the only possibility is to have $G = A_4$. In this case, none of the θ_i is fixed by all of G (since the stabilizer of any given θ_i is a dihedral group of order 8), and so none of them lies in F.
- Now suppose Δ is not a square: then the Galois group is one of S_4, $D_{2\cdot 4}$, and C_4.
- If the resolvent cubic has no roots in F and $\Delta(g)$ is not a square, the Galois group of the resolvent cubic is S_3: thus, the degree $[K : F]$ is divisible by 6, meaning that $|G|$ is divisible by 6. The only possibility here is that $G = S_4$.
- It is not possible for the resolvent cubic to split completely over F, since then the Galois group would stabilize each of the θ_i hence be contained in V_4.
- Thus, the only remaining case is that the resolvent cubic factors over F as the product of a degree-1 and an irreducible degree-2 polynomial (i.e., it has exactly one root in F), and in this case the Galois group is either $D_{2\cdot 4}$ or C_4.
- To distinguish between these, notice that $F(\sqrt{\Delta})$ is the fixed field of $G \cap A_4$ by the fundamental theorem of Galois theory.
- Now let r' be the root of g in F and assume that G contains the 4-cycle $(1\,2\,3\,4)$, so that it is either $C_4 = \langle (1\,2\,3\,4) \rangle$ or $D_{2\cdot 4} = \langle (1\,3), (1\,2\,3\,4) \rangle$: then $r' = (\beta_1 + \beta_3)(\beta_2 + \beta_4)$ since this is the only θ_i fixed by $(1\,2\,3\,4)$.
- If the Galois group is C_4 then the unique quadratic subfield of K/F is $F(\sqrt{\Delta})$, and is also the fixed field of the subgroup $\langle (1\,3)(2\,4) \rangle$. Then the roots of the two polynomials $(x-(\beta_1+\beta_3))(x-(\beta_2+\beta_4)) = x^2+r'$ and $(x - \beta_1\beta_3)(x - \beta_2\beta_4) = x^2 + (r' - p) + r$ are both fixed by this subgroup, and hence lie in $F(\sqrt{\Delta})$. In other words, these polynomials both split over $F(\sqrt{\Delta})$.
- If the Galois group is $D_{2\cdot 4}$ then $F(\beta_1) = F(\beta_3)$ is the fixed field of $\langle (2\,4) \rangle$ and $F(\sqrt{\Delta})$ is the fixed field of $\langle (1\,2)(3\,4), (1\,3)(2\,4) \rangle$, since the given elements are fixed by the indicated subgroups (the latter because it lies inside A_4) and the fields have the correct degrees.
- Now consider the two polynomials $(x-(\beta_1+\beta_3))(x-(\beta_2+\beta_4))$ and $(x-\beta_1\beta_3)(x-\beta_2\beta_4)$: we claim that at least one is irreducible over $F(\sqrt{\Delta})$. Otherwise, both $\beta_1+\beta_3$ and $\beta_1\beta_3$ would be elements of $F(\sqrt{\Delta})$, and then $F(\sqrt{\Delta})$ would be a subfield of $F(\beta_1) = F(\beta_3)$. But this cannot occur because the fixing subgroup of $F(\sqrt{\Delta})$, namely $\langle (1\,2)(3\,4), (1\,3)(2\,4) \rangle$, does not contain the fixing subgroup of $F(\beta_1) = F(\beta_3)$, namely $\langle (2\,4) \rangle$.
- Thus, if the Galois group is $D_{2\cdot 4}$, at least one of the polynomials $(x - (\beta_1 + \beta_3))(x - (\beta_2 + \beta_4)) = x^2 + r'$ and $(x - \beta_1\beta_3)(x - \beta_2\beta_4) = x^2 + (r' - p) + r$ is irreducible over $F(\sqrt{\Delta})$. The converse conditions are then immediate since these cases are disjoint.

- Example: Find the Galois group of $f(y) = y^4 - 2$ over $\mathbb{Q}$.
  - This polynomial is irreducible by Eisenstein, and its resolvent cubic is $g(z) = z^3 + 8z$ with discriminant $\Delta = -4 \cdot 8^3 = -2048$.
  - Since the discriminant is not a square and the resolvent cubic factors as $g(z) = z(z^2 + 8)$ we see that the Galois group is either C_4 or $D_{2\cdot 4}$.

- To determine which of these it is, we see that the root of $g(z)$ is $r' = 0$, so we must test the reducibility of $x^2 + r' = x^2$ and $x^2 + (r' - p)x + r = x^2 - 2$ over $\mathbb{Q}(\sqrt{-2048}) = \mathbb{Q}(\sqrt{-2})$.
- Although the first polynomial is reducible, the second is irreducible over $\mathbb{Q}(\sqrt{-2})$. Hence the Galois group is the dihedral group $\boxed{D_{2\cdot 4}}$ of order 8 (as we have shown previously by computing the action explicitly on the splitting field).

- Example: Find the Galois group of $f(y) = y^4 + 8y + 12$ over $\mathbb{Q}$.
  - One may verify by direct calculation that f is irreducible (it has no roots by the rational root test, and also does not factor as the product of two integral quadratics).
  - Then the resolvent cubic is $g(z) = z^3 - 48z + 64$, with discriminant $\Delta = -4(-48)^3 - 27(64)^2 = 2^{14} \cdot 3^3 - 3^3 \cdot 2^{12} = 2^{12} \cdot 3^4$.
  - Since the discriminant is a square, and the resolvent cubic has no rational roots (again via the rational root test), by our criterion we conclude that the Galois group is $\boxed{A_4}$.

- Example: Find the Galois group of $f(y) = y^4 + 2y - 2$ over $\mathbb{Q}$.
  - This polynomial is irreducible by Eisenstein, and its resolvent cubic is $g(z) = z^3 + 8z + 4$ with discriminant $\Delta = -4 \cdot 8^3 - 27 \cdot 4^2 = -2^4 \cdot 5 \cdot 31$.
  - Since the discriminant is not a square, and the resolvent cubic has no rational roots (via the rational root test), by our criterion we conclude that the Galois group is $\boxed{S_4}$.

- Example: Find the Galois group of $f(y) = y^4 - 14y^2 + 9$ over $\mathbb{Q}$.
  - One may verify by direct calculation that f is irreducible (it has no roots by the rational root test, and also does not factor as the product of two integral quadratics).
  - Then the resolvent cubic is $g(z) = z^3 + 28z^2 + 160z = z(z + 8)(z + 2)$, with discriminant $\Delta = 2^{14} \cdot 3^2 \cdot 5^2$.
  - Since the discriminant is a square, and the resolvent cubic splits completely over $\mathbb{Q}$, by our criterion we conclude that the Galois group is $\boxed{V_4}$.
  - In this case, we may compute the roots explicitly using the quadratic formula to solve for y^2 and then compute and simplify the square root: eventually, we can see that the roots are $\pm\sqrt{2} \pm \sqrt{5}$.

- Example: Find the Galois group of $f(y) = y^4 + 5y + 5$ over $\mathbb{Q}$.
  - This polynomial is irreducible by Eisenstein, and its resolvent cubic is $g(z) = z^3 - 20z + 25$ with discriminant $\Delta = -4 \cdot (-20)^3 - 27 \cdot 25^2 = 5^3 \cdot 11^2$. Note that the resolvent cubic factors as $(z + 5)(z^2 - 20z + 25)$.
  - Since the discriminant is not a square, and the resolvent cubic has a root, the Galois group is either C_4 or $D_{2\cdot 4}$.
  - To determine which of these it is, we see that the root of $g(z)$ is $r' = -5$, so we must test the reducibility of $x^2 + r' = x^2 - 5$ and $x^2 + (r' - p)x + r = x^2 - 10x + 5$ over $\mathbb{Q}(\sqrt{5^3 \cdot 11^2}) = \mathbb{Q}(\sqrt{5})$.
  - These quadratics both factor over $\mathbb{Q}(\sqrt{5})$ since their roots are $\pm\sqrt{5}$ and $5 \pm 2\sqrt{5}$. Hence the Galois group is $\boxed{C_4}$.

- By exploiting the resolvent cubic, we can extend Cardano's formulas to solve the general quartic as well.
  - Explicitly, by Cardano's formulas, we may compute the solutions $\theta_1, \theta_2, \theta_3$ of the resolvent cubic.
  - To find the roots $\beta_1, \beta_2, \beta_3, \beta_4$ of the original quartic, we must then solve the system $\theta_1 = (\beta_1 + \beta_2)(\beta_3 + \beta_4)$, $\theta_2 = (\beta_1 + \beta_3)(\beta_2 + \beta_4)$, and $\theta_3 = (\beta_1 + \beta_4)(\beta_2 + \beta_3)$.
  - However, since $\beta_1 + \beta_2 + \beta_3 + \beta_4 = 0$, we see that $\theta_1 = -(\beta_1 + \beta_2)^2$, $\theta_2 = -(\beta_1 + \beta_3)^2$, and $\theta_3 = -(\beta_2 + \beta_3)^2$.
  - Taking the square roots then yields $\beta_1 + \beta_2 = \pm\sqrt{-\theta_1}$, $\beta_1 + \beta_3 = \pm\sqrt{-\theta_2}$, and $\beta_2 + \beta_3 = \pm\sqrt{-\theta_3}$.
  - The square roots are not independent, however, since we must also satisfy the relation $(\beta_1 + \beta_2)(\beta_1 + \beta_3)(\beta_2 + \beta_3) = -q$, so the choice of any two determines the third. We may then easily compute $\beta_1, \beta_2, \beta_3$ from the linear equations above, and then $\beta_4 = -\beta_1 - \beta_2 - \beta_3$.

- In practice, the solutions obtained by this technique are sufficiently complicated that they are not especially useful (other than as a demonstration of the existence of a general formula for the roots).
- For example, for the quartic $g(y) = y^4 + 2y - 2$ with resolvent cubic $h(z) = z^3 + 8z + 4$, Cardano's formulas yield $A = \sqrt[3]{-2 + \sqrt{\frac{620}{27}}}$ and $B = \sqrt[3]{-2 - \sqrt{\frac{620}{27}}}$, with both cube roots real for concreteness.
- Then the three roots of g are $A + B$, $\zeta_3 A + \zeta_3^2 B$, and $\zeta_3^2 A + \zeta_3 B$, so we obtain an explicit root of f as $\frac{1}{2}\sqrt{\sqrt[3]{-2 + \sqrt{\frac{620}{27}}} + \sqrt[3]{-2 - \sqrt{\frac{620}{27}}}} + \frac{1}{2}\sqrt{\zeta_3 \sqrt[3]{-2 + \sqrt{\frac{620}{27}}} + \zeta_3^2 \sqrt[3]{-2 - \sqrt{\frac{620}{27}}}} - \frac{1}{2}\sqrt{\zeta_3^2 \sqrt[3]{-2 + \sqrt{\frac{620}{27}}} + \zeta_3 \sqrt[3]{-2 - \sqrt{\frac{620}{27}}}}$.
- One may verify that this value is approximately $0.34845 - 1.24753i$, which is indeed one of the roots of f (as can be estimated numerically, e.g., via Newton's method).

4.4.5 Computing Galois Groups over $\mathbb{Q}$

- We would like to extend our work on the Galois groups of cubic and quartic polynomials to higher degree.
  - Unfortunately, there is a substantial computational obstruction to doing this, namely that we require a description of the transitive subgroups of S_n in order to analyze the possible Galois groups of an irreducible polynomial.
  - When n is large or has many prime factors, there are very many transitive subgroups of S_n (since, for example, any subgroup containing an n-cycle is automatically transitive) and there is no obvious method for cataloguing them.
  - Assuming that we do have a list of all of the transitive subgroups of S_n, and have verified that a polynomial $f(t) \in F[t]$ is irreducible, then the Galois group of f must be one of the groups on our list.
  - If we can somehow glean enough information about the permutations in this subgroup, in principle we should be able to determine the Galois group exactly.
- If F is a subfield of $\mathbb{R}$, one simple way we can obtain information is by looking at the action of complex conjugation on the roots of f.
  - Since the roots of f necessarily come in complex conjugate pairs, complex conjugation will act as a product of k 2-cycles, where k is the number of conjugate pairs of roots.
  - In some cases this is enough to show that the Galois group must actually be S_n.
- Example: Show that the Galois group of $f(t) = t^5 - 4t + 2$ over $\mathbb{Q}$ is S_5.
  - Since $f(-2) = -14$, $f(0) = 2$, $f(1) = -1$, and $f(2) = 18$, the intermediate value theorem implies that f has at least 3 real roots.
  - On the other hand, since $f'(t) = 5t^4 - 4$, we see that there are two values at which $f'(t) = 0$ (namely $t = \pm\sqrt[4]{4/5}$) and therefore by Rolle's theorem f can have at most 3 real roots. (Alternatively, one could apply Descartes' rule of signs to see that f has at most 3 real roots.)
  - Hence f has exactly 3 real roots, and thus also has 2 complex-conjugate roots.
  - Then complex conjugation is an element of the Galois group that acts as a transposition.
  - Furthermore, since f is irreducible by Eisenstein's criterion, any root generates an extension of degree 5 over $\mathbb{Q}$.
  - Thus by the fundamental theorem of Galois theory, the Galois group must have order divisible by 5, so by Cauchy's theorem, it must contain an element of order 5. But the only elements of order 5 in S_5 are 5-cycles, so G contains a 5-cycle.
  - By relabeling we may assume the transposition is $(1\,2)$, and then by taking an appropriate power of the 5-cycle we may assume that 2 follows 1 in its cycle decomposition, and then by relabeling we may assume it is $(1\,2\,3\,4\,5)$.
  - It is then straightforward to see that these elements generate S_5, and so we must have $G = S_5$.

- We may obtain additional information about the cycle structures of elements in the Galois group by appealing to the following theorem from algebraic number theory:
- Theorem (Dedekind-Frobenius): If $f(t) \in \mathbb{Z}[t]$ is irreducible with Galois group G over $\mathbb{Q}$, then for any prime p not dividing the discriminant $\Delta(f)$, if the mod-p reduction of $f(t)$ factors over $\mathbb{F}_p$ as a product of terms having degrees $k_1, k_2, \ldots, k_d$, then G contains a permutation having a cycle decomposition of lengths $k_1, k_2, \ldots, k_d$.
    - There is a more general result about factorizations of ideals in certain rings due to Dedekind that contains this fact as a special case.
    - Using this theorem, we may therefore determine cycle types for elements of the Galois group by factoring $f(t)$ modulo p for many primes p.
    - Furthermore, it follows from another theorem of algebraic number theory (the Chebotarev density theorem) that the asymptotic proportion of primes for which $f(t)$ factors into terms of degrees $k_1, k_2, \ldots, k_d$ is proportional to the number of permutations in G with cycle type $k_1, k_2, \ldots, k_d$.
    - By computing the factorization of $f(t)$ modulo p for a reasonably large number of primes p and tallying the results, one may therefore identify an optimal candidate for the Galois group by comparing the proportions of cycle types observed to the proportion of cycle types in the possible transitive subgroups of S_n.
- We will now list the transitive subgroups of S_n for some smaller values of n (along with the distribution of cycle types):
    - There is a standard labeling of the transitive subgroups of S_n due to Conway, Hulpke, and McKay, which we include with the tables. We also remark that many subgroups have (isomorphic) conjugates inside S_n, and the list of generators is only one possibility among many.
    - For degree 5, there are 5 transitive subgroups of S_5, with generators and cycle types as follows:

#	Order	Name	Generators	1	2	2,2	3	2,3	4	5
5T1	5	C_5	(1 2 3 4 5)	1						4
5T2	10	$D_{2\cdot 5}$	(1 2 3 4 5), (1 5)(2 4)	1		5				4
5T3	20	F_{20}	(1 2 3 4 5), (1 2 4 3)	1		5			10	4
5T4	60	A_5	(1 2 3), (3 4 5)	1		15	20			24
5T5	120	S_5	(1 2 3 4 5), (1 2)	1	10	15	20	20	30	24

    - For degree 6, there are 16 transitive subgroups of S_6, with generators and cycle types as follows:

#	Order	Name	Generators	1	2	2,2	2,3	2,4	2,2,2	3	3,3	4	5	6
6T1	6	C_6	(1 2 3 4 5 6)	1					1		2			2
6T2	6	S_3	(1 3 5)(2 4 6), (1 4)(2 3)(5 6)	1					3		2			
6T3	12	$S_3 \times C_2$	(1 2 3 4 5 6), (1 4)(2 3)(5 6)	1		3			4		2			2
6T4	12	A_4	(1 4)(2 5), (1 3 5)(2 4 6)	1		3					8			
6T5	18	F_{18}	(2 4 6), (1 4)(2 5)(3 6)	1					3	4	4			6
6T6	24	$A_4 \times C_2$	(3 6), (1 3 5)(2 4 6)	1	3	3			1		8			8
6T7	24	S_4 (a)	(1 4)(2 5), (1 3 5)(2 4 6), (1 5)(2 4)	1		9		6			8			
6T8	24	S_4 (b)	(1 4)(2 5), (1 3 5)(2 4 6), (1 5)(2 4)(3 6)	1		3			6		8	6		
6T9	36	$S_3 \times S_3$	(2 4 6), (1 5)(2 4), (1 4)(2 5)(3 6)	1		9			6	4	4			12
6T10	36	F_{36}	(2 4 6), (1 5)(2 4), (1 4 5 2)(3 6)	1		9		18		4	4			
6T11	48	$S_4 \times C_2$	(3 6), (1 3 5)(2 4 6), (1 5)(2 4)	1	3	9		6	7		8	6		8
6T12	60	A_5	(1 2 3 4 6), (1 4)(5 6)	1		15					20		24	
6T13	72	$F_{36} \rtimes C_2$	(2 4 6), (2 4), (1 4)(2 5)(3 6)	1	6	9	12	18	6	4	4			12
6T14	120	S_5	(1 2 3 4 6), (1 2)(3 4)(5 6)	1		15			10		20	30	24	20
6T15	360	A_6	(1 2)(3 4 5 6), (1 2 3)	1		45		90		40	40		144	
6T16	720	S_6	(1 2 3 4 5 6), (1 2)	1	15	45	120	90	15	40	40	90	144	120

    - For degree 7, there are 7 transitive subgroups of S_7, with generators and some cycle types as follows (for any cycle type not listed, S_7 is the only transitive subgroup containing it):

#	Order	Name	Generators	1	2,2	2,4	2,2,2	2,2,3	3	3,3	5	6	7
7T1	7	C_7	(1 2 3 4 5 6 7)	1									6
7T2	14	$D_{2\cdot 7}$	(1 2 3 4 5 6 7), (2 7)(3 6)(4 5)	1			7						6
7T3	21	F_{21}	(1 2 3 4 5 6 7), (1 2 4)(3 6 5)	1						14			6
7T4	42	F_{42}	(1 2 3 4 5 6 7), (1 3 2 6 4 5)	1			7			14		14	6
7T5	168	$PSL_2(\mathbb{F}_7)$	(1 2 3 4 5 6 7), (1 2)(3 6)	1	21	42				56			48
7T6	2520	A_7	(3 4 5 6 7), (1 2 3)	1	105	630		210	70	280	504		720
7T7	5040	S_7	(1 2 3 4 5 6 7), (1 2)	1	105	630	105	210	70	280	504	840	720

- For degree 8, there are 50 transitive subgroups of S_8. We will not list these, although we will mention that there are two subgroups of order 96 (specifically, groups 8T32 and 8T33) that have the same collection of cycle types appearing with the same frequencies.
- Here are the numbers[9] of transitive subgroups of S_n for the values of n up through 23:

n	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
# Transitive Subgroups	34	45	8	301	9	63	104	1954	10	983	8	1117	164	59	7

- We can use these tables to compute probable Galois groups for irreducible polynomials of degree ≤ 7 by computing the factorization of the polynomial modulo primes not dividing its discriminant and listing the corresponding cycles that must appear in its Galois group. (We may also check whether the discriminant is a square, which will tell us whether G is a subgroup of A_n.)
- Example: Determine the probable Galois group of $f(t) = t^5 - t^2 - 2t - 3$.
  - We can compute that this polynomial has discriminant $\Delta = 17^2 \cdot 29^2$, so its Galois group is a subgroup of A_5.
  - Computing the factorization of $f(t)$ modulo p for the 100 smallest primes excluding 17 and 29 yields the following cycles:

Factorization Type	1	2	2,2	3	2,3	4	5
# Appearances	1		20	30			49

  - The only transitive subgroup contained in A_5 having these cycle types is A_5 itself, so in fact we have proven that the Galois group of this polynomial is A_5.
  - Note that the distribution of the factorization types matches fairly closely with the distribution of cycle types in A_5, as should be expected.
- Example: Determine the probable Galois group of $f(t) = t^5 - 5t^2 - 3$.
  - We can compute that this polynomial has discriminant $3^2 \cdot 5^6$, so its Galois group is a subgroup of A_5.
  - Computing the factorization of $f(t)$ modulo p for the 100 smallest primes excluding 3 and 5 yields the following cycles:

Factorization Type	1	2	2,2	3	2,3	4	5
# Appearances	8		54				38

  - The only transitive subgroups contained in A_5 having these cycle types are $D_{2\cdot 5}$ and A_5.
  - Since $D_{2\cdot 5}$ has no 3-cycles (in contrast to S_6, 1/3 of whose elements are 3-cycles) we would expect no factorizations to have a 3-cycle if the Galois group were $D_{2\cdot 5}$, while we would expect about 1/3 of them to have a 3-cycle if the Galois group were A_5.
  - Since no 3-cycles appear in the computed factorizations, it seems overwhelmingly likely that the Galois group is $D_{2\cdot 5}$.
- Example: Determine the probable Galois group of $f(t) = t^6 - t^5 - t^2 + t + 1$.
  - This polynomial has discriminant $-3^3 \cdot 433$, so its Galois group is not a subgroup of A_6.

[9] This information courtesy of John Jones' database of transitive groups at https://hobbes.la.asu.edu/Groups/ .

- Computing the factorization of $f(t)$ modulo p for the 100 smallest primes excluding 3 and 433 yields the following cycles:

Factorization Type	1	2	2,2	2,3	2,4	2,2,2	3	3,3	4	5	6
# Appearances	1	4	14	17	29	6	8	3			18

- There are only two transitive subgroups that contain cycles of each of these types: the subgroup 6T13 of order 72 and the subgroup 6T16 (which is S_6).
- Since 6T16 has no 4-cycles or 5-cycles (in contrast to S_6, roughly $1/3$ of whose elements are 4-cycles or 5-cycles), and no 4-cycles or 5-cycles appear in the computed factorizations, it seems overwhelmingly likely that the Galois group is 6T13.

- Example: Determine the probable Galois group of $f(t) = t^7 - 7t + 3$.
  - We can compute that this polynomial has discriminant $3^8 \cdot 7^8$, so its Galois group is a subgroup of A_7.
  - Computing the factorization of $f(t)$ modulo p for the 100 smallest primes excluding 3 and 7 yields the following cycles:

Factorization Type	1	2,2	2,4	2,2,2	2,2,3	3	3,3	5	6	7
# Appearances		15	32				32			21

  - There are only two transitive subgroups contained in A_7 that contain cycles of each of these types, namely $PSL_2(\mathbb{F}_7)$ and A_7.
  - As above, since the observed factorization types match the cycles of $PSL_2(\mathbb{F}_7)$ very closely (in contrast to A_7, which also has 3-cycles, 2,2,3-cycles, and 5-cycles), the probable Galois group is $PSL_2(\mathbb{F}_7)$.

- Once a candidate for the Galois group has been identified, it is then possible to construct resolvent polynomials (similar to the resolvent cubic we used for the quartic) and then use information about their roots and factorizations to eliminate all of the other possible Galois groups.
  - For example, to establish that a particular polynomial of degree 5 has Galois group $D_{2\cdot 5} = \langle (1\,2\,3\,4\,5), (1\,5)(2\,4) \rangle$ requires eliminating the possibility that the Galois group is $A_5 = \langle (1\,2\,3), (3\,4\,5) \rangle$.
  - One way to do this is to compute the resolvent polynomial whose roots are the S_5-permutations of $\beta_1\beta_2 + \beta_2\beta_3 + \beta_3\beta_4 + \beta_4\beta_5 + \beta_5\beta_1$, which in this case has degree 12 (since there are 11 other possible results of permuting the indices, such as $\beta_1\beta_3 + \beta_2\beta_4 + \beta_3\beta_5 + \beta_4\beta_1 + \beta_5\beta_2$). This will differentiate between $D_{2\cdot 5}$ and A_5 since $D_{2\cdot 5}$ fixes several of these elements (so the resolvent polynomial will have a rational root) but A_5 does not.
  - Notice that, unlike the case of the resolvent cubic for the quartic, the resolvent polynomial for $D_{2\cdot 5}$ has degree 12, which much larger than the degree of the original quintic polynomial. (This is a typical phenomenon when $n \geq 5$.)

4.4.6 Solvability in Radicals

- We have described ways to compute Galois groups for polynomials of moderate degree, and a natural followup is to try to find "formulas in radicals", similar to the cubic and quartic formulas, for the roots of these polynomials.
  - Explicitly, we consider a formula in radicals to be one that is constructed via some combination of field operations (addition, subtraction, multiplication, division) and extraction of nth roots.
  - In order to do this, we need to study field extensions obtained by adjoining nth roots of elements.

- Definition: If F is a field, the extension field K/F is a simple radical extension of K if $K = F(\beta)$ for some β with $\beta^n \in F$ for some n.
  - For any $a \in F$ we will write $a^{1/n}$ to denote an arbitrary choice of a root β of the polynomial $x^n - a$ in an algebraic closure of F.
  - Observe that for an arbitrary F, the extension $F(a^{1/n})$ will not be Galois in general: its normal closure will be the splitting field of $x^n - a$ over F, which is only equal to $F(a^{1/n})$ when $F(a^{1/n})$ contains the nth roots of unity.

- In particular, if F itself contains the nth roots of unity, then $F(a^{1/n})$ will automatically be Galois over F for any $a \in F$, as long as $x^n - a$ is separable (which occurs precisely when n is not divisible by the characteristic of F and $a \neq 0$).
- In this case, any automorphism $\sigma \in \mathrm{Gal}(F(a^{1/n})/F)$ is uniquely determined by the value of $\sigma(a^{1/n}) = a^{1/n}\zeta$ for some nth root of unity ζ.
- We may then essentially compute the Galois group $\mathrm{Gal}(F(a^{1/n})/F)$, which turns out always to be cyclic.

- Theorem (Simple Radical Extensions): Let F be a field of characteristic not dividing n that contains the nth roots of unity. Then for any $a \in F^\times$, the field $F(a^{1/n})/F$ is Galois and its Galois group is cyclic of order dividing n. Conversely, any cyclic Galois extension K/F of order dividing n has the form $K = F(a^{1/n})$ for some $a \in F$.
  - Proof: First suppose $a \in F^\times$. If F contains the nth roots of unity, then $F(a^{1/n})$ is the splitting field of $x^n - a$ over F. Since $\mathrm{char}(F)$ does not divide n and $a \neq 0$, $x^n - a$ is separable, and so $F(a^{1/n})/F$ is Galois.
  - If $G = \mathrm{Gal}(F(a^{1/n})/F)$, then for any $\sigma \in G$ we have $\sigma(a^{1/n}) = a^{1/n}\zeta_{(\sigma)}$ for some nth root of unity $\zeta_{(\sigma)}$.
  - We therefore have a map $\varphi : G \to \mu_n$ from G to the cyclic group μ_n of nth roots of unity by setting $\varphi(\sigma) = \zeta_{(\sigma)} = \sigma(a^{1/n})/a^{1/n}$.
  - Then $\varphi(\sigma\tau) = \sigma(\tau(a^{1/n}))/a^{1/n} = \sigma(a^{1/n}\zeta_{(\tau)})/a^{1/n} = \sigma(a^{1/n})\zeta_{(\tau)}/a^{1/n} = \zeta_{(\sigma)}\zeta_{(\tau)} = \varphi(\sigma)\varphi(\tau)$ for any $\sigma, \tau \in G$, so φ is a group homomorphism.
  - Furthermore, $\ker\varphi$ consists of the automorphisms fixing $a^{1/n}$, hence is trivial. Thus, by the first isomorphism theorem, we see that φ yields an isomorphism of G with its image inside μ_n. Since $\mathrm{im}\,\varphi$ is a subgroup of μ_n, it is cyclic of order dividing n as claimed.
  - For the converse, suppose K/F is cyclic Galois of order dividing n, where F contains the nth roots of unity and $\mathrm{char}(F)$ does not divide n.
  - Let σ be a generator of $G = \mathrm{Gal}(K/F)$ and ζ be a primitive nth root of unity.
  - Then because the automorphisms $1, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ are linearly independent, there exists an element $\alpha \in K$ such that the element $\beta = \alpha + \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) + \cdots + \zeta^{n-1}\sigma^{n-1}(\alpha)$ is nonzero.
  - We can then compute $\zeta\sigma(\beta) = \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) + \cdots + \zeta^{n-1}\sigma^{n-1}(\alpha) + \zeta^n\sigma^n(\alpha) = \beta$, since both ζ and σ have order dividing n.
  - This implies $\sigma(\beta) = \zeta^{-1}\beta$, and so iterating this yields $\sigma^k(\beta) = \zeta^{-k}\beta$. In particular, since $\beta \neq 0$ we see that β is not fixed by any nonidentity element of G, and so $K = F(\beta)$.
  - Finally, we have $\sigma(\beta^n) = \zeta^{-n}\beta^n = \beta^n$ so β^n is fixed by σ hence by all of G, and thus $\beta^n = a$ is an element of F. This means $K = F(a^{1/n})$ for some $a \in F$, as claimed.
  - Remark: The element β is called a Lagrange resolvent, and its construction can be motivated by looking for an element of K with the property that $\sigma(\beta) = \zeta^{-1}\beta$: writing $\beta = \alpha + c_1\sigma(\alpha) + \cdots + c_n\sigma^{n-1}(\alpha)$, and then computing the coefficients c_i.

- Now that we have characterized the extensions obtained by adjoining nth roots of individual elements, we can give a precise definition for solving an equation in radicals:

- Definition: If $\alpha \in F$, we say α can be expressed in radicals of α is an element of some tower of simple radical extensions, namely, if there exist extensions $F = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_d = K$ such that $\alpha \in K$ and K_{i+1}/K_i is a simple radical extension for each i, and we say K/F is a root extension. We also say a polynomial $f(x) \in F[x]$ is solvable in radicals if each of its roots can be expressed in radicals.
  - Example: Any constructible number can be expressed in radicals, since (as we proved) the constructible numbers are those which are contained in some tower of quadratic extensions.
  - Example: The algebraic number $\sqrt[3]{2 + 7\sqrt{2 + \sqrt{5}} - 8\sqrt[9]{17}}$ can be expressed in radicals over $\mathbb{Q}$.
  - Example: Any root of unity can be expressed in radicals, since by definition any nth root of unity is an nth root of 1.

- It is straightforward to see that the composite of two root extensions of F is also a root extension of F: explicitly, if $F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_d = K$ and $F = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_k = L$ are two towers of simple radical extensions, then so is $F = K_0L_0 \subseteq K_1L_0 \subseteq K_2L_0 \subseteq \cdots \subseteq K_dL_0 \subseteq K_dL_1 \subseteq \cdots \subseteq K_dL_k = KL$.
- In particular, the set of all elements in the algebraic closure $\overline{F}$ that can be expressed in radicals is a subfield of $\overline{F}$. Also, if α can be expressed in radicals and $\sigma(\alpha)$ is any Galois conjugate, then $\sigma(\alpha)$ can also be expressed in radicals, because $F = K_0 \subseteq \sigma(K_1) \subseteq \cdots \subseteq \sigma(K_d) = \sigma(K)$ is also a tower of simple radical extensions.

- We would like to characterize the elements $\alpha \in \overline{F}$ that can be expressed in radicals, which (by our observation about Galois conjugates) is equivalent to characterizing the polynomials in $F[x]$ that are solvable in radicals.
  - We would like to be able to give a statement requiring information only about the minimal polynomial of α, but in order to do this we first need to see that α is contained in a Galois root extension.

- Proposition (Elements Expressible in Radicals): If α can be expressed in radicals over F, then α is contained in a root extension L having a tower $F = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_k = L$ where L is Galois over F and each intermediate extension L_{i+1}/L_i is Galois with cyclic Galois group.
  - Proof: Suppose α can be expressed in radicals over F. Then by our observation above, all Galois conjugates $\sigma(\alpha)$ can also be expressed in radicals over F, and so the splitting field K of the minimal polynomial of α is a root extension of F.
  - This means that there is a tower of simple radical extensions $F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_d = K$, where K_{i+1}/K_i is obtained by extracting an n_ith root.
  - If we let E be the field obtained by adjoining all n_ith roots of unity to F, then E/F is a simple radical extension of F, since it is obtained by adjoining a root of the polynomial $x^{n_1n_2\cdots n_{d-1}} - 1$.
  - Now consider the tower $F \subseteq E = EK_0 \subseteq EK_1 \subseteq \cdots \subseteq EK_d = EK$. Each extension EK_{i+1}/EK_i is a simple radical extension obtained by extracting an n_ith root of unity, and since all of these roots of unity are in E (hence in EK_i), by our characterization of simple radical extensions, these extensions are all Galois with cyclic Galois group.
  - Now just set $L_1 = E$ and $L_{i+1} = EK_i$ for $i \geq 1$, with $L = EK$. Then L is Galois over F (since it is the composite of two Galois extensions E/F and K/F) and each extension L_{i+1}/L_i is Galois with cyclic Galois group, as required.

- By applying the fundamental theorem of Galois theory to the tower constructed above, we obtain a condition on the Galois group of L/F.
  - Explicitly, if G_i is the subgroup of $G = \mathrm{Gal}(L/F)$ associated to the intermediate extension L_i, then we obtain a chain of subgroups $G = G_0 \geq G_1 \geq \cdots \geq G_k = \{e\}$ such that G_{i+1} is normal in G_i and the quotient group G_i/G_{i+1} is cyclic for each i.

- Definition: A finite group G is solvable if there exists a chain of subgroups $G = G_0 \geq G_1 \geq \cdots \geq G_k = \{e\}$ such that G_{i+1} is normal in G_i and the quotient group G_i/G_{i+1} is cyclic for each $0 \leq i \leq k-1$.
  - We emphasize that G_{i+1} is only required to be a normal subgroup of the previous subgroup G_i, and does not have to be a normal subgroup of G itself.
  - Example: Any finite abelian group is solvable, since every finite abelian group is a direct product of cyclic groups.
  - Example: The dihedral group $D_{2\cdot n}$ is solvable, since the subgroup $G_1 = \langle r \rangle$ is cyclic and the quotient group $D_{2\cdot n}/G_1$ is also cyclic (it has order 2 and is generated by $\overline{s}$).
  - Example: The symmetric group S_4 is solvable, via the chain $S_4 \geq A_4 \geq V_4 \geq \langle (1\,2)(3\,4) \rangle \geq \{e\}$, where $V_4 = \langle (1\,2)(3\,4), (1\,3)(2\,4) \rangle$. Note that V_4 is normal in A_4 since it is in fact normal in S_4, and each successive quotient is cyclic because it has prime order (either 2 or 3).

- Here are some of the fundamental properties of solvable groups:

- Proposition (Properties of Solvable Groups): Let G be a group.

1. If G is solvable, then any subgroup H is solvable and any quotient group G/N is solvable.
   - Proof: Suppose G is solvable with a chain $G = G_0 \geq G_1 \geq \cdots \geq G_k = \{e\}$ such that G_{i+1} is normal in G_i and G_i/G_{i+1} is cyclic.
   - If H is a subgroup of G, let $H_i = G_i \cap H$ for each i. Then $H_{i+1} = H_i \cap G_{i+1}$, so by the second isomorphism theorem, we see that H_{i+1} is normal in H_i and $H_i/H_{i+1} = H_i/(H_i \cap G_{i+1}) \cong H_i G_{i+1}/G_{i+1}$.
   - But since $H_i G_{i+1}$ is a subgroup of G_i, the latter is a subgroup of G_i/G_{i+1} and hence cyclic. Hence we obtain a chain $H = H_0 \geq H_1 \geq \cdots \geq H_k = \{e\}$ such that H_{i+1} is normal in H_i and H_i/H_{i+1} is cyclic, so H is solvable.
   - If N is a normal subgroup of G, let $\overline{G_i} = G_i/(G_i \cap N) \cong G_i N/N$ be the image of G_i in G/N.
   - Then by the second and third isomorphism theorems, $(G_i N/N)/(G_{i+1}N/N) \cong G_i N/G_{i+1}N$, and the latter is isomorphic to a quotient of G_i/G_{i+1} by the second isomorphism theorem, hence is cyclic.
   - Hence the chain $G/N = \overline{G_0} \geq \overline{G_1} \geq \cdots \geq \overline{G_k} = \{\overline{e}\}$ has the property that $\overline{G_{i+1}}$ is normal in $\overline{G_i}$ and $\overline{G_i}/\overline{G_{i+1}}$ is cyclic, so G/N is solvable.
2. If N is a normal subgroup of G such that N and G/N are solvable, then G is solvable.
   - Proof: Suppose that N has a chain $N = N_0 \geq N_1 \geq \cdots \geq N_d = \{e\}$ and G/N has a chain $G/N = \overline{G_0} \geq \overline{G_1} \geq \cdots \geq \overline{G_k} = \{\overline{e}\}$.
   - Then by the fourth isomorphism theorem we may lift each of the $\overline{G_i}$ to a subgroup G_i of G containing N with $G_i/G_{i+1} \cong \overline{G_i}/\overline{G_{i+1}}$.
   - Then the chain $G = G_0 \geq G_1 \geq \cdots \geq G_k = N = N_0 \geq N_1 \geq \cdots \geq N_d = \{e\}$ shows G is solvable.
3. G is solvable if and only if G has a chain of subgroups $G = G_0 \geq G_1 \geq \cdots \geq G_k = \{e\}$ such that G_{i+1} is normal in G_i and the quotient group G_i/G_{i+1} is abelian.
   - We note that this is often taken as the definition of a solvable group, rather than the one we gave where successive quotients are cyclic.
   - Proof: If G is solvable then it clearly has such a chain (since cyclic groups are abelian).
   - For the converse, we induct on k. The base case $k = 1$ is trivial since abelian groups are solvable as noted above. For the inductive step, suppose we have a chain $G = G_0 \geq G_1 \geq \cdots \geq G_k = \{e\}$ such that G_{i+1} is normal in G_i and the quotient group G_i/G_{i+1} is abelian.
   - Then G_1 is solvable by the inductive hypothesis, and G/G_1 is also solvable (since it is abelian). Hence by (2), G is solvable.

- From our results above, we see that if $f(x)$ is solvable in radicals, then each of its roots is contained in a Galois extension L/F whose Galois group $\mathrm{Gal}(L/F)$ is solvable.
  - The Galois group of $f(x)$ is $\mathrm{Gal}(K/F)$ where K is the splitting field for f. Since this is a quotient group of $\mathrm{Gal}(L/F)$ and quotient groups of solvable groups are solvable, $\mathrm{Gal}(K/F)$ is solvable.
  - Our central result is that the converse is true also.

- Theorem (Solvability in Radicals): Let F be a field and $f(x) \in F[x]$ be a polynomial of degree n, where the characteristic of F does not divide $n!$ (in particular, if F has characteristic 0). Then $f(x)$ is solvable in radicals if and only if the Galois group of f is a solvable group.
  - This result (at least for $F = \mathbb{Q}$) is essentially due to Galois, and was the historical motivation for Galois' development of Galois theory.
  - Proof: Note that any irreducible factor of f has degree at most n, hence dividing $n!$, so all irreducible factors of f are separable. By replacing f with the least common multiple of its irreducible factors (which does not change the roots), we may therefore assume f is separable.
  - Now suppose f is solvable in radicals, and let K be the splitting field of f, with $G = \mathrm{Gal}(K/F)$.
  - If α is any root of f, then α is expressible in radicals, and so by our proposition, there exists a Galois extension L_α/F containing α such that $\mathrm{Gal}(L_\alpha/F)$ is solvable.
  - Then the composite L of all the L_α over all roots α of f is also Galois over F, and its Galois group is a subgroup of the direct product of the $\mathrm{Gal}(L_\alpha/F)$ by our results on Galois groups of composite extensions.
  - Since the direct product of solvable groups is solvable, and subgroups of solvable groups are solvable, this means the Galois group of L/F is solvable.

- Since L contains all roots of f, it contains K, and so by the fundamental theorem of Galois theory $G = \mathrm{Gal}(K/F)$ is a quotient of $\mathrm{Gal}(L/F)$. Thus G is a quotient of a solvable group, hence is solvable.
- For the converse, suppose G is solvable and has a chain $G = G_0 \geq G_1 \geq \cdots \geq G_k = \{e\}$ such that G_{i+1} is normal in G_i and G_i/G_{i+1} is cyclic of order n_i.
- By the fundamental theorem of Galois theory, the corresponding fixed fields $F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_k = K$ such that K_{i+1}/K_i is Galois with cyclic Galois group of order n_i.
- If we let E be the extension of F containing all of the n_ith roots of unity for each i, then E/F is Galois and a simple radical extension (as we have noted).
- Then EK_{i+1}/EK_i is also Galois with cyclic Galois group of order dividing n_i by the "sliding-up" property of the Galois extension K_{i+1}/K_i. Then since E contains the n_ith roots of unity, we conclude that EK_{i+1}/EK_i is a simple radical extension.
- This means $F \subseteq E \subseteq EK_1 \subseteq EK_2 \subseteq \cdots \subseteq EK_k = EK$ is a tower of simple radical extensions containing all the roots of f, and so f is solvable in radicals as claimed.

- By the theorem above, we may immediately determine whether a polynomial is solvable in radicals by checking whether its Galois group is solvable. In particular we obtain the famed Abel-Ruffini theorem on the insolvability of the general quintic:
- Corollary (Abel-Ruffini Theorem): The groups A_n and S_n are not solvable for $n \geq 5$, and therefore the general equation of degree n is not solvable in radicals for any $n \geq 5$.
  - Proof: For $n \geq 5$ the group A_n is simple and therefore not solvable: it has no nontrivial proper normal subgroups, so the only possibilities for the first subgroup G_1 in a chain would be $G_1 = A_n$ or $G_1 = \{e\}$, neither of which will work.
  - Then S_n is also cannot be solvable, since subgroups of solvable groups are solvable. The second part follows immediately from our result that the Galois group of the general equation of degree n is S_n.
- We can also give specific examples of polynomials that are not solvable in radicals using the methods we have described previously for computing Galois groups.
  - For example, as we noted earlier, the polynomial $f(t) = t^5 - 4t + 2$ has Galois group S_5 over $\mathbb{Q}$, and is therefore not solvable in radicals.
  - Likewise, we also showed (by analyzing factorizations over $\mathbb{F}_p$) that the polynomial $f(t) = t^5 - t^2 - 2t - 3$ has Galois group A_5 over $\mathbb{Q}$, hence also is not solvable in radicals.
- For polynomials whose Galois group is solvable, there do exist formulas in radicals for the roots. We briefly outline the situation for $n = 5$, where (it is not hard to see) C_5, $D_{2\cdot 5}$, and F_{20} are all solvable.
  - Since each of C_5, $D_{2\cdot 5}$, and F_{20} is contained in F_{20}, an irreducible quintic is solvable in radicals precisely when its Galois group is a subgroup of F_{20}.
  - As detailed in a 1991 paper of D. Dummit, this may in turn be determined by determining whether an associated resolvent polynomial for F_{20} (of degree 6) has a rational root, and if so, one may give explicit formulas in radicals for the roots of the quintic.
  - For the quintic $f(x) = x^5 + px + q$ in particular, the resolvent sextic is $f_{20}(x) = x^6 + 8px^5 + 40p^2x^4 + 160p^3x^3 + 400p^4x^2 + (512p^5 - 3125q^4)x + (256p^6 - 9375pq^4)$, and the quintic $f(x)$ is solvable in radicals if and only if the resolvent sextic has a rational root.
  - Example: For $f(x) = x^5 + 120x - 1344$ of discriminant $\Delta = 2^{11} \cdot 3^4 \cdot 5^6$, the resolvent sextic has a rational root $x = 1440$, and therefore f is solvable. Since the discriminant is not a square, its Galois group is not contained in A_5, and must therefore be F_{20}.

Well, you're at the end of my handout. Hope it was helpful.