Math 5111 (Algebra 1)

Lecture #19 of 24 $\sim$ November 16th, 2020

Galois Groups and Fixed Fields

- Automorphisms of Splitting Fields
- Galois Groups
- Fixed Fields
- The Fundamental Theorem of Galois Theory

This material represents §4.1.3-4.1.4 from the course notes.

Field Automorphisms

Last time, we introduced automorphisms of a field extension K/F (ring isomorphisms of K with itself that fix F) and characterized automorphisms of simple extensions:

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 $\tau(\alpha) = \beta$.
Therefore, $|\mathrm{Aut}(K/F)|$ is equal to the number of roots of $m(x)$ in K, and is (in particular) finite and at most $[K : F]$.

Today, we will extend these results to study automorphism of splitting fields.

Isomorphism Lifting Lemma

We will also use the isomorphism lifting lemma a number of times, so here is a reminder of what it says:

Lemma (Lifting Isomorphisms)

Let $\varphi : E \to F$ be an isomorphism of fields. If α is algebraic over E with minimal polynomial $p(x) = a_0 + a_1x + \cdots + a_nx^n \in E[x]$, 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 $\varphi(\alpha) = \beta$.

By iteratively applying this result, we can lift the isomorphism φ (or $\tilde{\varphi}$) to an isomorphism of the splitting field of p over E with the splitting field of q over F.

Automorphisms of Splitting Fields, I

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).

This 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.

The content of the theorem is that splitting fields are normal.

Automorphisms of Splitting Fields, II

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 $F(\alpha)$.

Automorphisms of Splitting Fields, III

Proof (continued):

- By the isomorphism lifting lemma for splitting fields, 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, since isomorphisms preserve extension degrees, this means $[K : F] = [K(\beta) : F]$.
- But since both of these extensions are finite-degree, we must have $K(\beta) = K$, and thus $\beta \in K$.
- Since β was an arbitrary root of p, all roots of p are in K. This means K is normal, as claimed.

Automorphisms of Splitting Fields, IV

Now we can compute $\#\mathrm{Aut}(K/F)$ when K is a splitting field:

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).

Automorphisms of Splitting Fields, V

We will actually show a slightly stronger 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.
- Take $q_F(x)$ to be the polynomial obtained by applying φ to the coefficients of $q_E(x)$ and let L be the splitting field of $q_F(x)$ over F.
- By using the isomorphism lifting lemma, we showed 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.

Automorphisms of Splitting Fields, V

Proof:

- We induct on $n = [K : F]$. 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.
- 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 φ to the coefficients of $p_E(x)$. Then 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.

Automorphisms of Splitting Fields, VI

Proof (continued):

- 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 $F(\beta_i)$.
- This tells us 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).

Automorphisms of Splitting Fields, VII

Splitting fields of separable polynomials 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 if $|\mathrm{Aut}(K/F)| = [K : F]$.

If K/F is a Galois extension, we will refer to $\mathrm{Aut}(K/F)$ 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.

Automorphisms of Splitting Fields, VIII

Our theorem from two slides ago 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 $[K : F] = 2$.

Automorphisms of Splitting Fields, IX

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

- Specifically, if we can write down a nice set of generators for a splitting field, then to compute elements of the Galois group, we just have to identify the automorphisms based on their actions on the generators.
- In some cases, just knowing the order of the Galois group (which by our theorem is equal to the degree of the splitting field, when it is separable) is enough to characterize all the possible automorphisms.

Automorphisms of Splitting Fields, IX

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 $K = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$.
- So let's try to write down some automorphisms 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 $K/\mathbb{Q}$.

Automorphisms of Splitting Fields, IX

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

- But because $[K : \mathbb{Q}] = 6$ and K is separable, we know $\mathrm{Gal}(K/\mathbb{Q})$ is a group of order 6.
- Thus, all 6 possible choices $\sqrt[3]{2} \mapsto \{\sqrt[3]{2}, \sqrt[3]{2}\zeta_3, \sqrt[3]{2}\zeta_3^2\}$, $\zeta_3 \mapsto \{\zeta_3, \zeta_3^2\}$ must actually extend to automorphisms.
- One automorphism σ has $\sigma(\sqrt[3]{2}, \zeta_3) = (\sqrt[3]{2}\zeta_3, \zeta_3)$.
- Another automorphism τ has $\tau(\sqrt[3]{2}, \zeta_3) = (\sqrt[3]{2}, \zeta_3^2)$.
- Then $\sigma\tau$ has $\sigma\tau(\sqrt[3]{2}, \zeta_3) = \sigma(\sqrt[3]{2}, \zeta_3^2) = (\sqrt[3]{2}\zeta_3, \zeta_3^2)$, whereas $\tau\sigma$ has $\tau\sigma(\sqrt[3]{2}, \zeta_3) = \tau(\sqrt[3]{2}\zeta_3, \zeta_3) = (\sqrt[3]{2}\zeta_3^2, \zeta_3^2)$.
- Since $\sigma\tau \neq \tau\sigma$ here, so by our classification of groups of order 6, we see that the Galois group must be isomorphic to $D_{2\cdot 3}$.

Automorphisms of Splitting Fields, X

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

- With the automorphisms σ with $\sigma(\sqrt[3]{2}, \zeta_3) = (\sqrt[3]{2}\zeta_3, \zeta_3)$ and τ with $\tau(\sqrt[3]{2}, \zeta_3) = (\sqrt[3]{2}, \zeta_3^2)$, we can check that $\sigma^3 = \tau^2 = e$, while $\tau\sigma^2 = \sigma\tau$.
- Thus, σ plays the role of the element $r \in D_{2\cdot 3}$ while τ plays the role of s.
- Another way we could have identified the Galois group G was to observe that G permutes the roots of the polynomial $x^3 - 2$.
- Since these roots generate the splitting field $K/\mathbb{Q}$, the group action is faithful, and so we get an embedding of G as a subgroup of S_3. But since $\#G = 6$, in fact $G \cong S_3$.

Automorphisms of Splitting Fields, X

In fact, this last observation holds 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. 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, 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 $(2\,3)$.

Although in that example the Galois group was all of S_3, in general Galois groups can be proper subgroups of S_n.

- For example, as we saw last time, 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.
- If we label the roots $\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}$ as $\{1, 2, 3, 4\}$ then the possible permutations are e, $(1\,2)$, $(3\,4)$, and $(1\,2)(3\,4)$.

Automorphisms of Splitting Fields, XI

Example: Find the order of the Galois group of the splitting field of $p(x) = x^4 - 3$ over $\mathbb{Q}$.

Automorphisms of Splitting Fields, XI

Example: Find the order of 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.
- Since the polynomial is trivially separable since it is irreducible and in characteristic 0, the order of the Galois group is 8.
- 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.

Automorphisms of Splitting Fields, XII

Example: Find the Galois group of the splitting field of $p(x) = x^4 - 3$ over $\mathbb{Q}$.

Automorphisms of Splitting Fields, XII

Example: Find the Galois group of the splitting field of $p(x) = x^4 - 3$ over $\mathbb{Q}$.

- One automorphism σ has $\sigma(3^{1/4}, i) = (3^{1/4}i,\ i)$, and another map τ has $\tau(3^{1/4}, i) = (3^{1/4}, -i)$.
- We can then see σ has order 4, τ has order 2, and $\sigma\tau = \tau\sigma^3$.
- Thus, the Galois group is isomorphic to the dihedral group $D_{2\cdot 4}$ of order 8, with σ acting as r and τ acting as 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 $(2\,4)$.
- In fact, we could have identified the Galois group structure purely using the fact that it is a subgroup of S_4 of order 8: it is then a Sylow 2-subgroup of S_4, and as we have previously shown, the Sylow 2-subgroups of S_4 are dihedral of order 8.

Automorphisms of Splitting Fields, XIII

Example: If p is a prime, find the Galois group of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$.

Automorphisms of Splitting Fields, XIII

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 ζ_p, ζ_p^2, ... , ζ_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 $\sigma_a(\zeta_p) = \zeta_p^a$.

Automorphisms of Splitting Fields, XIV

Example: If p is a prime, find the Galois group of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$.

- We have $\mathrm{Gal}(K/\mathbb{Q}) = \{\sigma_1, \sigma_2, \ldots, \sigma_{p-1}\}$ 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 $p-1$.
- If you like, you can also recognize this action as the automorphism *group* of the cyclic group of pth roots of unity.

Automorphisms of Splitting Fields, XV

Example: If p is a prime, find the Galois group of $\mathbb{F}_{p^n}/\mathbb{F}_p$.

Automorphisms of Splitting Fields, XV

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 then 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, 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 $\mathrm{Gal}(K/\mathbb{F}_p)$. Thus, $\mathrm{Gal}(K/\mathbb{F}_p)$ is cyclic and generated by the Frobenius map φ.

Fixed Fields, I

We will now exploit more of the group-action structure of the automorphism group of an extension K/F.

Fixed Fields, I

We will now exploit more of the group-action structure of the automorphism group of an extension K/F.

- If $\sigma \in \mathrm{Aut}(K/F)$ is a particular automorphism, consider the set of all elements of K stabilized by σ.
- This 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. We call this subfield the fixed field of σ.
- The fixed field of σ is an intermediate field of the extension K/F, meaning that it is a field that lies between K and F.

Fixed Fields, II

Examples:

1. Suppose that $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$.
   - 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 $\mathbb{Q}(\sqrt{3})$.
   - If τ is the automorphism with $\tau(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}$, then the elements of K fixed by τ are those of the form $a + b\sqrt{2}$. Thus, the fixed field of τ is the subfield $\mathbb{Q}(\sqrt{2})$.
   - The elements fixed by $\sigma\tau$ are those of the form $a + d\sqrt{6}$. Thus the fixed field of $\sigma\tau$ is the subfield $\mathbb{Q}(\sqrt{6})$.

Fixed Fields, III

Examples:

2. Suppose $K = \mathbb{Q}(2^{1/4})/\mathbb{Q}$.
   - If σ is the automorphism with $\sigma(2^{1/4}) = -2^{1/4}$, then $\sigma(a + b2^{1/4} + c\sqrt{2} + d2^{3/4}) = a - b2^{1/4} + c\sqrt{2} - d2^{3/4}$.
   - This means that 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 $\mathbb{Q}(\sqrt{2})$.
   - The only other automorphism of this field extension is the trivial automorphism. Its fixed field is $\mathbb{Q}(2^{1/4})$.

Fixed Fields, IV

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.

- The fixed field of each automorphism is a subfield of K containing F. Thus, the fixed field of S is indeed a field (justifying the name).

Fixed Fields, V

Examples:

3. Suppose $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$.
   - As before let σ be the automorphism with $\sigma(\sqrt{2}, \sqrt{3}) = (-\sqrt{2}, \sqrt{3})$ and τ be the automorphism with $\tau(\sqrt{2}, \sqrt{3}) = (\sqrt{2}, -\sqrt{3})$.
   - Then the fixed field of the set $\{\sigma, \tau\}$ is the intersection $\mathbb{Q}(\sqrt{3}) \cap \mathbb{Q}(\sqrt{2}) = \mathbb{Q}$: the only elements of K fixed by both σ and τ are rational numbers.
   - In the same way, the fixed field of $\{\tau, \sigma\tau\}$ is $\mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(\sqrt{6}) = \mathbb{Q}$, and the fixed field of $\{\sigma, \sigma\tau\}$ is also $\mathbb{Q}$.

Fixed Fields, VI

In fact, we really only need to concern ourselves with fixed fields of subgroups of $G = \mathrm{Aut}(K/F)$.

- Specifically, 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 $\mathrm{Aut}(K/F)$, since we do not lose any information by doing so.

Fixed Fields, VII

Examples:

4. Suppose once again that $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$.
   - Take σ, τ as before with $\sigma(\sqrt{2}, \sqrt{3}) = (-\sqrt{2}, \sqrt{3})$ and $\tau(\sqrt{2}, \sqrt{3}) = (\sqrt{2}, -\sqrt{3})$.
   - By our calculations earlier, 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.

Fixed Fields, VIII

Examples:

5. Suppose $K = \mathbb{Q}(2^{1/4})/\mathbb{Q}$.
   - Take σ to be the automorphism with $\sigma(2^{1/4}) = -2^{1/4}$.
   - Then as we already calculated, 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 $\mathbb{Q}(\sqrt{2})$.

Fixed Fields, IX

In more complicated examples, computing fixed fields ultimately reduces to solving a system of linear equations[1].

- 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.
- Since the fixed field of a subgroup is the same as the fixed field for a set of its generators, when we actually compute fixed fields explicitly, we only need to solve the equations associated with the generators of the desired subgroup.

[1] This is pleasantly convenient, because linear algebra is the best.

Fixed Fields, X

Example: For $K = \mathbb{Q}(2^{1/3}, \zeta_3)/\mathbb{Q}$, find the fixed field E of the subgroup $\langle\varphi\rangle$, where φ acts via $\varphi(2^{1/3}, \zeta_3) = (2^{1/3}\zeta_3, \zeta_3^2)$,

- Let's use the basis $\{1, 2^{1/3}, 4^{1/3}, \zeta_3, 2^{1/3}\zeta_3, 4^{1/3}\zeta_3\}$ for K. Then $\varphi(a + b2^{1/3} + c4^{1/3} + d\zeta_3 + e2^{1/3}\zeta_3 + f4^{1/3}\zeta_3) = a + b2^{1/3}\zeta_3 + c4^{1/3}\zeta_3^2 + d\zeta_3^2 + e2^{1/3} + f4^{1/3}\zeta_3$ 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 E have $a = a - d$, $b = e$, $c = -c$, $d = -d$, $e = b$, and $f = f - c$.
- These reduce to $d = 0$, $c = 0$, and $b = e$, so E's elements are $a + b(2^{1/3} + 2^{1/3}\zeta_3) + f(4^{1/3}\zeta_3) = a - b2^{1/3}\zeta_3^2 + f4^{1/3}\zeta_3$.
- Thus, we see $E = \mathbb{Q}(2^{1/3}\zeta_3^2)$.

Fixed Fields, XI

Example: For $K = \mathbb{Q}(2^{1/3}, \zeta_3)/\mathbb{Q}$, find the fixed field E of the subgroup $\langle \psi \rangle$, where ψ acts via $\psi(2^{1/3}, \zeta_3) = (2^{1/3}, \zeta_3^2)$,

Fixed Fields, XI

Example: For $K = \mathbb{Q}(2^{1/3}, \zeta_3)/\mathbb{Q}$, find the fixed field E of the subgroup $\langle\psi\rangle$, where ψ acts via $\psi(2^{1/3}, \zeta_3) = (2^{1/3}, \zeta_3^2)$,

- Again use $\{1, 2^{1/3}, 4^{1/3}, \zeta_3, 2^{1/3}\zeta_3, 4^{1/3}\zeta_3\}$ for K. Then $\psi(a + b2^{1/3} + c4^{1/3} + d\zeta_3 + e2^{1/3}\zeta_3 + f4^{1/3}\zeta_3) = a + b2^{1/3} + c4^{1/3} + d\zeta_3^2 + e2^{1/3}\zeta_3^2 + f4^{1/3}\zeta_3^2$ 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 $\varphi(a + b2^{1/3} + c4^{1/3} + d\zeta_3 + e2^{1/3}\zeta_3 + f4^{1/3}\zeta_3) = (a + d) + (b + e)2^{1/3} + (c + f)4^{1/3} - d\zeta_3 - e2^{1/3}\zeta_3 - f4^{1/3}\zeta_3$.
- Hence the elements of E have $a + d = a$, $b + e = b$, $c + f = c$, $-d = d$, $-e = e$, $-f = f$.
- These reduce to $d = e = f = 0$, so E's elements are $a + b2^{1/3} + c4^{1/3}$. This means $E = \mathbb{Q}(2^{1/3})$.

Fixed Fields, XII

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.

- In the language of group actions, this is the stabilizer of E under the group action of $\mathrm{Aut}(K/F)$ on subsets of K.
- In the language of automorphisms of extensions, this "fixing subgroup" is the group $\mathrm{Aut}(K/E)$, which is naturally a subgroup of $\mathrm{Aut}(K/F)$, since any automorphism of K fixing E automatically also fixes the subfield F of E.

Fixed Fields, XIII

Examples:

1. Suppose $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$.
   - Take σ, τ as before with $\sigma(\sqrt{2}, \sqrt{3}) = (-\sqrt{2}, \sqrt{3})$ and $\tau(\sqrt{2}, \sqrt{3}) = (\sqrt{2}, -\sqrt{3})$.
   - For the subfield $\mathbb{Q}(\sqrt{3})$, the automorphisms fixing it are the identity and τ.
   - For the subfield $\mathbb{Q}(\sqrt{2})$, the automorphisms fixing it are the identity and σ.
   - For the subfield $\mathbb{Q}(\sqrt{6})$, the automorphisms fixing it are the identity and $\sigma\tau$.
   - For the subfield $\mathbb{Q}$, all four automorphisms fix this subfield.
   - For the subfield $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, the only automorphism fixing it is the identity.

Fixed Fields, XIV

Examples:

2. Suppose $K = \mathbb{Q}(2^{1/3}, \zeta_3)/\mathbb{Q}$.
   - 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, note σ fixes E, hence so does $\langle\sigma\rangle$, but the other automorphisms of K map ζ_3 to ζ_3^2 and thus they do not fix E.
   - If E is the subfield $\mathbb{Q}(\sqrt[3]{2})$, then the subgroup of $\mathrm{Aut}(K/\mathbb{Q})$ fixing E is $\langle\tau\rangle$, where $\tau(2^{1/3}, \zeta_3) = (2^{1/3}, \zeta_3^2)$. To see this observe that $\langle\tau\rangle$ does fix E, but none of the other automorphisms of K fix $\sqrt[3]{2}$.
   - In a similar way, the fixing subgroup of $\mathbb{Q}(\sqrt[3]{2}\zeta_3)$ is $\langle\tau\sigma\rangle$, since $\tau\sigma(\sqrt[3]{2}\zeta_3) = \tau(\sqrt[3]{2}\zeta_3^2) = \sqrt[3]{2}\zeta_3$, while the fixing subgroup of $\mathbb{Q}(\sqrt[3]{2}\zeta_3^2)$ is $\langle\tau\sigma^2\rangle$.

Fixed Fields, XIV

Examples:

3. Suppose $K = \mathbb{Q}(2^{1/4})/\mathbb{Q}$.
   - If $E = \mathbb{Q}(\sqrt{2})$, 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 $\mathrm{Aut}(K/\mathbb{Q})$.
   - If $E = \mathbb{Q}(2^{1/4})$ then only the identity fixes E.

Fixed Fields, XV

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.

Fixed Fields, XVI

Examples:

1. Consider $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
   - 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).

Fixed Fields, XVII

Examples:

2. Consider $K = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$.
   - The fixed fields of the possible subgroups $\{e\}$, $\langle\sigma\rangle$, $\langle\tau\rangle$, $\langle\tau\sigma\rangle$, $\langle\tau\sigma^2\rangle$, and $\langle\sigma,\tau\rangle$ of $\mathrm{Aut}(K/\mathbb{Q})$ are $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$, $\mathbb{Q}(\zeta_3)$, $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt[3]{2}\zeta_3)$, and $\mathbb{Q}(\sqrt[3]{2}\zeta_3^2)$ and $\mathbb{Q}$ respectively.
   - Inversely, the automorphism groups $\mathrm{Aut}(K/E)$ for each of the subfields $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$, $\mathbb{Q}(\zeta_3)$, $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt[3]{2}\zeta_3)$, and $\mathbb{Q}(\sqrt[3]{2}\zeta_3^2)$ and $\mathbb{Q}$ are $\{e\}$, $\langle\sigma\rangle$, $\langle\tau\rangle$, $\langle\tau\sigma\rangle$, $\langle\tau\sigma^2\rangle$, and $\langle\sigma,\tau\rangle$ respectively.
   - Thus, the two maps are inverses for $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$, 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).

Fixed Fields, XVIII

Examples:

3. Consider $K = \mathbb{Q}(2^{1/4})/\mathbb{Q}$.
   - 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 $\langle\sigma\rangle$.
4. Consider $K = \mathbb{Q}(2^{1/3})/\mathbb{Q}$.
   - 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.

Fixed Fields, XX

In two of the examples, our maps were inverses, while in the other two, they were not.

- Note that the fields in the first two examples were Galois extension (i.e., a splitting field of a separable polynomial), while the fields in the second and third examples were not.
- In examples 3 and 4, $\mathrm{Aut}(K/\mathbb{Q})$ 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 is now 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.

The Fundamental Theorem of Galois Theory, I

As we have seen via a few examples, when K/F is a Galois extension there appears to be a natural inclusion-reversing correspondence between subgroups of the automorphism group $G = \mathrm{Gal}(K/F)$ and intermediate fields E of K/F:

$$\left\{\begin{array}{c}\text{Subfields } E \text{ of } K \\ \text{Containing } F\end{array}\right\} \begin{array}{c}\xrightarrow{\text{Elements of } G \text{ Fixing } E} \\ \xleftarrow{\text{Elements of } K \text{ Fixed By } H}\end{array} \left\{\begin{array}{c}\text{Subgroups} \\ H \text{ of } G\end{array}\right\}$$

Our goal next time will be to prove that this "Galois correspondence" does indeed give an inclusion-reversing bijection between the intermediate fields E of K/F and the subgroups H of $G = \mathrm{Gal}(K/F)$.

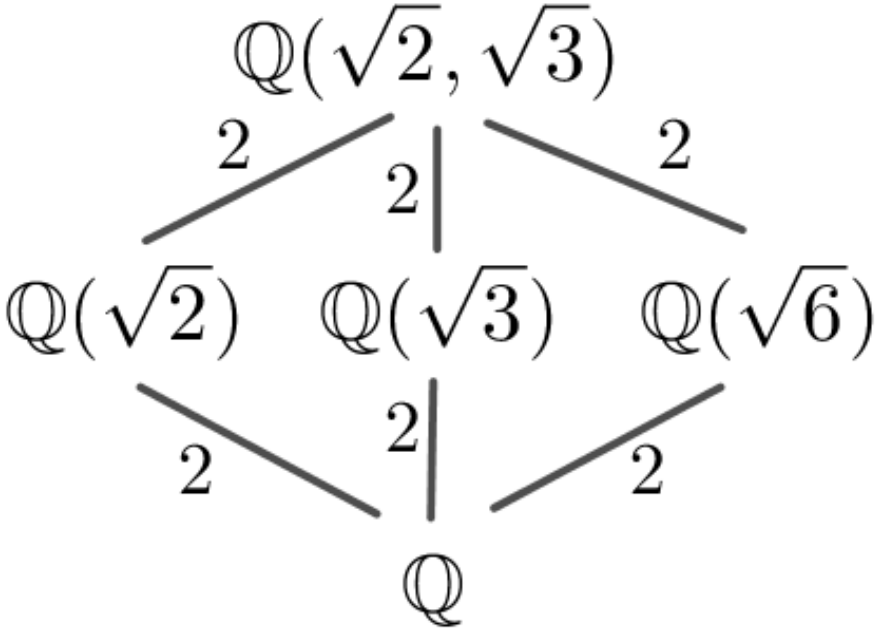
The Fundamental Theorem of Galois Theory, II

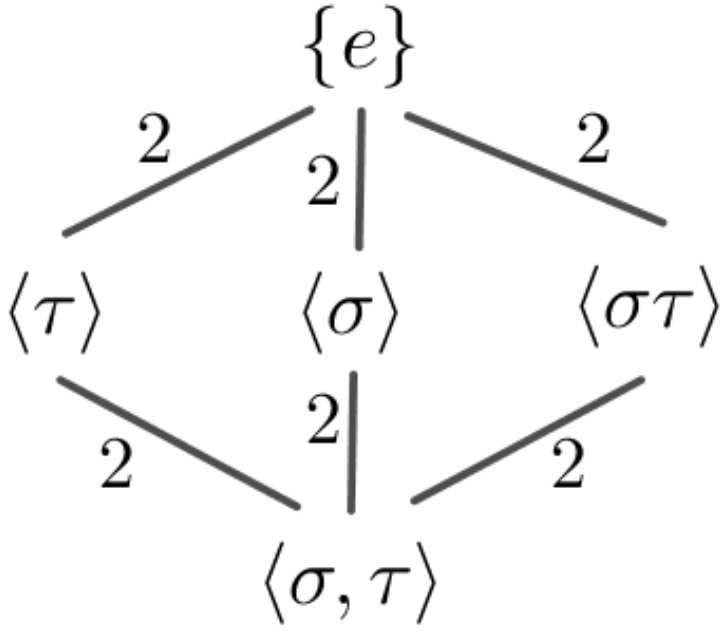
For now, we can give a few illustrations of the Galois correspondence:

- Consider $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ 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 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.

The Fundamental Theorem of Galois Theory, III

Here are the corresponding subgroup and subfield diagrams for $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ (where we have also labeled the diagrams with the relative extension degrees and subgroup indices and drawn the subgroup diagram upside-down):





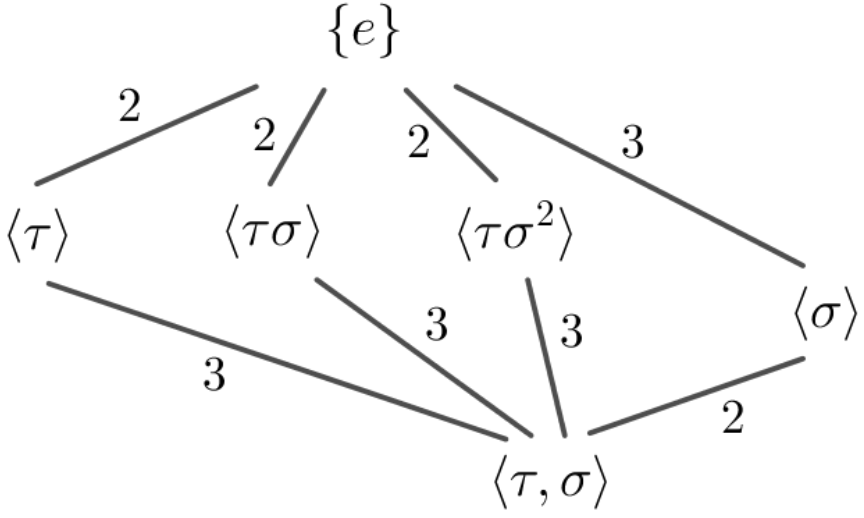
The Fundamental Theorem of Galois Theory, IV

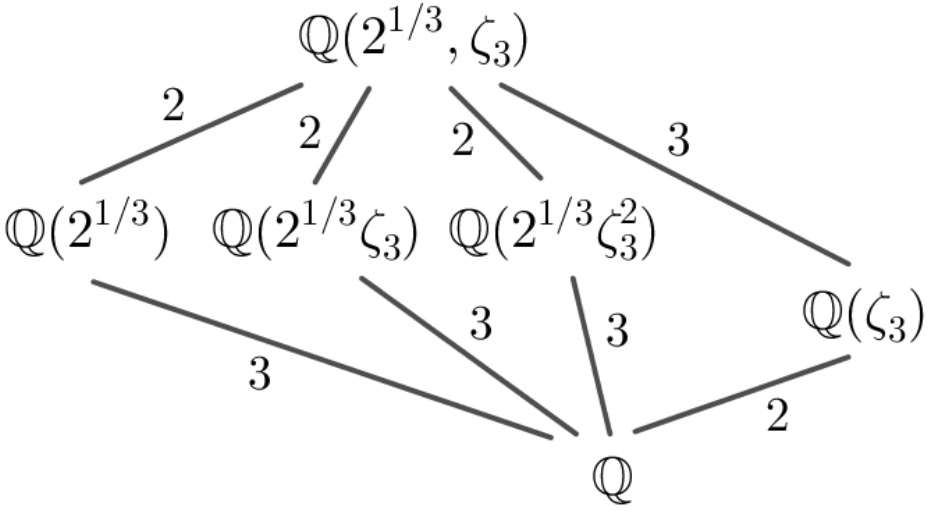
For another example, consider $K = \mathbb{Q}(2^{1/3}, \zeta_3)/\mathbb{Q}$.

- We have previously described the automorphisms $\sigma(2^{1/3}, \zeta_3) = (2^{1/3}\zeta_3, \zeta_3)$ and $\tau(2^{1/3}, \zeta_3) = (2^{1/3}, \zeta_3^2)$.
- As we have noted, 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.

The Fundamental Theorem of Galois Theory, V

Here are the corresponding subgroup and subfield diagrams for $\mathbb{Q}(2^{1/3}, \zeta_3)/\mathbb{Q}$:





Notice here there are also correspondences between the subfield degrees and the indexes of subgroups. We will establish these properties, and several others, next time.

Summary

We discussed automorphisms of splitting fields and introduced the notion of a Galois group.

We discussed fixed fields of automorphisms.

We introduced the fundamental theorem of Galois theory.

Next lecture: Characterizing Galois extensions, the proof and examples of the fundamental theorem of Galois theory.