Math 5111 (Algebra 1)

Lecture #20 of 24 $\sim$ November 19th, 2020

The Fundamental Theorem of Galois Theory

- Characterizations of Galois Extensions
- Proof of the Fundamental Theorem
- Applications of the Fundamental Theorem

This material represents §4.2 from the course notes.

Recall, I

Recall our calculation about automorphisms of splitting fields:

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).

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 $\mathrm{Gal}(K/F)$.

Recall, II

We also defined the fixed field of a subgroup, and its inverse notion, the subgroup of the automorphism group fixing a particular intermediate field:

- If K/F is a field extension and H is a subgroup of $\mathrm{Aut}(K/F)$, then the fixed field of H is the subfield of K fixed by all automorphisms in H.
- If E is an intermediate field of K/F, then the collection of automorphisms in $\mathrm{Aut}(K/F)$ that fix E is a subgroup of $\mathrm{Aut}(K/F)$.
- These two maps are both inclusion-reversing.

Recall, III

As we saw in some examples last time, 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:

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

We now 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 $G = \mathrm{Gal}(K/F)$.

What Are We Doing Today?

Theorem (Fundamental Theorem of Galois Theory)

Let K/F be a Galois extension and let $G = \mathrm{Gal}(K/F)$.

0. *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.*
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. *E/F is Galois if and only if H is a normal subgroup of G, and in that 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.*
6. *The lattice of subgroups of G is the same as the lattice of intermediate fields of K/F turned upside-down.*

Characterizations of Galois Extensions, I

First, we give some characterizations of Galois extensions:

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.)*

But to prove these we first need some *other* results....

Characterizations of Galois Extensions, II

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.

Characterizations of Galois Extensions, III

Proof:

- We induct on n. The base case $n = 1$ is trivial, since any embedding of a field is nonzero (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.

Characterizations of Galois Extensions, IV

Proof (continued):

- So, once we cancel, we obtain the new 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.

Characterizations of Galois Extensions, V

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 $[K : E] = |H|$.

As a warning, this proof is fairly long. There is nothing that is particularly conceptually difficult, it just requires a bunch of tedious calculations.

Characterizations of Galois Extensions, VI

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 $d < h$. By basic linear algebra, the homogeneous system of d equations in h variables over K

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

has a nonzero solution $(x_1, \ldots, x_h) = (c_1, \ldots, c_h)$ for $c_i \in K$.

Characterizations of Galois Extensions, VII

Proof (continued):

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

- We have a solution $(x_1, \ldots, x_h) = (c_1, \ldots, c_h)$. For any $a_1, \ldots, a_d \in F$, adding a_i times the ith equation above gives $[a_1\sigma_1(v_1) + a_2\sigma_1(v_2) + \cdots + a_d\sigma_1(v_d)]c_1 + \cdots + [a_1\sigma_h(v_1) + a_2\sigma_h(v_2) + \cdots + a_d\sigma_h(v_d)]c_h = 0$.
- 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 $\sigma_1(w)c_1 + \sigma_2(w)c_2 + \cdots + \sigma_h(w)c_h = 0$.
- But since the a_i are arbitrary elements of F and the v_i are a basis for K/E, the relation above holds for every $w \in K$, meaning that it is a linear dependence of the σ_j.
- This is impossible by the proposition, so $h \leq d$.

Characterizations of Galois Extensions, VIII

Proof (continued more):

- 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 $\alpha_i \in E$.

Characterizations of Galois Extensions, IX

Proof (continued even more):

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

- 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 $\alpha_{k+1} \notin E$.

Characterizations of Galois Extensions, X

Proof (continued even still more):

- Assume $\alpha_{k+1} \notin E$. Then the system is

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

- 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. Now permute the equations back:

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

Characterizations of Galois Extensions, XI

Proof (continued even yet still more):

- Now subtract those two systems. This yields

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

- Then 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 that has all its entries in E. But this contradicts the assumption that the v_i are linearly independent, which is impossible.
- Thus we must have $d = h$, meaning that $[K : E] = |H|$.

Characterizations of Galois Extensions, XII

Now we can establish the characterizations of Galois extensions:

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.)*

We already showed (2) $\implies$ (1) and that (2) $\implies$ (4).
We now show (4) $\implies$ (2), (1) $\iff$ (3), and (1) $\implies$ (4).

Characterizations of Galois Extensions, XIII

Proof (4) $\implies$ (2):

- We need to show that if K/F is a normal, finite, and separable extension, then K/F is the splitting field of some separable polynomial in $F[x]$.
- 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 $m(x)$.

Characterizations of Galois Extensions, XIV

Proof (1) $\iff$ (3):

- We need to show that F is the fixed field of $\mathrm{Aut}(K/F)$ if and only if $|\mathrm{Aut}(K/F)| = [K : F]$.
- So let E be 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 $\mathrm{Aut}(K/F)$.

Characterizations of Galois Extensions, XIV

Proof (1) $\implies$ (4):

- We must show that if K/F is Galois, then K/F is a normal, finite, and separable extension. Galois extensions are by definition finite and separable, so we need only show normality.
- Suppose that $p(x) \in F[x]$ is irreducible and has a root $\alpha \in K$.
- Let $\mathrm{Gal}(K/F) = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ and consider the values $\sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_n(\alpha)$.
- Reorder these values so that $\sigma_1(\alpha), \ldots, \sigma_k(\alpha)$ are distinct and that the others are duplicates.
- Now consider the polynomial $q(x) = (x - \sigma_1(\alpha))(x - \sigma_2(\alpha)) \cdots (x - \sigma_k(\alpha)) \in K[x]$. Note that q is separable by hypothesis, and α is a root of q.
- We will show in fact that $p(x) = q(x)$, and so since K contains all the roots of q, it contains all the roots of p, so since p was arbitrary, this establishes normality of K/F.

Characterizations of Galois Extensions, XV

Proof (1) $\implies$ (4) (continued):

- We have $q(x) = (x - \sigma_1(\alpha))(x - \sigma_2(\alpha)) \cdots (x - \sigma_k(\alpha))$.
- For each $\tau \in \mathrm{Gal}(K/F)$, notice that τ permutes $\sigma_1(\alpha), \ldots, \sigma_k(\alpha)$. Thus, 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 we showed (1) implies (3), the fact that every coefficient of $q(x)$ is fixed by every element of $\mathrm{Gal}(K/F)$ implies that they are all in F, so $q(x) \in F[x]$.
- 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 $p(x) = q(x)$, as claimed. Thus the roots of $p(x)$ are all in K and K/F is normal.

Characterizations of Galois Extensions, XVI

In the last portion of the proof, the elements $\sigma(\alpha)$ for $\sigma \in \mathrm{Gal}(K/F)$ played a crucial role, and they will show up often:

Definition

If K/F is a Galois extension and $\alpha \in K$, the elements $\sigma(\alpha)$ for $\sigma \in \mathrm{Gal}(K/F)$ 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 $\mathrm{Gal}(K/F)$, 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).

Characterizations of Galois Extensions, XVII

Example: Let $K = \mathbb{Q}(2^{1/3}, \zeta_3)/\mathbb{Q}$.

- As we have shown, the Galois group of K is isomorphic to the dihedral group of order 6.
- Thus, to compute Galois conjugates of any element of this field, we simply apply the 6 field automorphisms to it.
- Inside K, there are three Galois conjugates of $2^{1/3}$: they are $2^{1/3}$, $2^{1/3}\zeta_3$, and $2^{1/3}\zeta_3^2$.
- There are six Galois conjugates of $2^{1/3} + \zeta_3$: they 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 $2^{1/3}\zeta_3^2 + \zeta_3^2$.

Characterizations of Galois Extensions, XVIII

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 mapping one of them to another.
- 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.

Characterizations of Galois Extensions, XIX

Example: Calculate the Galois conjugates of $\sqrt{2}+\sqrt{3}$ over $\mathbb{Q}$, and find its minimal polynomial over $\mathbb{Q}$.

Characterizations of Galois Extensions, XIX

Example: Calculate the Galois conjugates of $\sqrt{2}+\sqrt{3}$ over $\mathbb{Q}$, and find its minimal polynomial over $\mathbb{Q}$.

- We work inside $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, since the element $\sqrt{2}+\sqrt{3}$ lies inside this field.
- We know that the Galois group of K is isomorphic to the Klein 4-group.
- Then the Galois conjugates of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$ are $\sqrt{2}+\sqrt{3}$, $\sqrt{2}-\sqrt{3}$, $-\sqrt{2}+\sqrt{3}$, and $-\sqrt{2}-\sqrt{3}$.
- The minimal polynomial of $\sqrt{2}+\sqrt{3}$ over $\mathbb{Q}$ thus has degree 4, and is given explicitly by $(x-\sqrt{2}-\sqrt{3})(x-\sqrt{2}+\sqrt{3})(x+\sqrt{2}-\sqrt{3})(x+\sqrt{2}+\sqrt{3})$ $= x^4 - 10x^2 + 1$.

Putting The Fun in Fundamental Theorem, I

We have now developed all of the preliminaries, so we now dive into the proof of the fundamental theorem of Galois theory.

- We will establish several of the calculation parts first before showing that correspondence maps are actually inverses of one another.

Putting The Fun in Fundamental Theorem, II

Theorem (Fundamental Theorem of Galois Theory)

Let K/F be a Galois extension and let $G = \mathrm{Gal}(K/F)$.

0. *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.*
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. *E/F is Galois if and only if H is a normal subgroup of G, and in that 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.*
6. *The lattice of subgroups of G is the same as the lattice of intermediate fields of K/F turned upside-down.*

Putting The Fun in Fundamental Theorem, III

2. For any intermediate field E, the extension K/E is always Galois, with Galois group H.

- Proof: Suppose that H is a subgroup of G and let E be the fixed field of H.
- As calculated in (1), 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.

Putting The Fun in Fundamental Theorem, IV

2. Subgroup indices correspond to extension degrees, so that $[K : E] = |H|$ and $[E : F] = |G : H|$.

- Proof: 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 in fact, $|H| = |\mathrm{Aut}(K/E)| = [K : E]$.
- For the other statement we have seen that F is the fixed field of $\mathrm{Gal}(K/F)$, and so $[K : F] = |G|$.
- 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.

Putting The Fun in Fundamental Theorem, V

0. 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.

- Proof: For surjectivity of the fixed field map, suppose E is an intermediate field.
- From (2), 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.

Putting The Fun in Fundamental Theorem, VI

0. 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.

- Proof (continued): 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.

Putting The Fun in Fundamental Theorem, VII

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.

- Proof: Suppose 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.

Putting The Fun in Fundamental Theorem, VIII

4. E/F is Galois if and only if H is a normal subgroup of G, and in that case, $\mathrm{Gal}(E/F)$ is isomorphic to G/H.

- Proof: First, the statement that $\sigma(E) = E$ for all $\sigma \in G$ is equivalent to saying that E is normal.
- This follows because, for any $\alpha \in E$, the Galois conjugates $\sigma(\alpha) \in E$ are the other roots of the minimal polynomial of α: thus 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.
- 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.

Putting The Fun in Fundamental Theorem, IX

4. E/F is Galois if and only if H is a normal subgroup of G, and in that case, $\mathrm{Gal}(E/F)$ is isomorphic to G/H.

- Proof (continued): Now suppose 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.
- Then 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.

Putting The Fun in Fundamental Theorem, X

5. Intersections of subgroups correspond to joins of fields, and joins of subgroups correspond to intersections of fields.

- Proof: 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.

Putting The Fun in Fundamental Theorem, XI

5. Intersections of subgroups correspond to joins of fields, and joins of subgroups correspond to intersections of fields.

- Proof (continued): Similarly, $E_1 \cap E_2$ 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 $E_1 \cap E_2$.
- Then 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 $E_1 \cap E_2$.

Putting The Fun in Fundamental Theorem, XII

6. The lattice of subgroups of G is the same as the lattice of intermediate fields of K/F turned upside-down.

- Proof: This follows immediately from (1), (5), and the fact that the Galois correspondence is inclusion-reversing.

Fundamentally Galois Examples, I

We may use the fundamental theorem of Galois theory to extract quite a lot of new information about field extensions.

- If K/F is Galois, then subgroups of the Galois group correspond to intermediate fields.
- Thus, 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 $\mathrm{Gal}(K/F)$.

Fundamentally Galois Examples, II

We can even use the fundamental theorem to say things about non-Galois extensions.

- 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, just as before, 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.

Fundamentally Galois Examples, III

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 $K = \mathbb{Q}(2^{1/3}, \zeta_3)/\mathbb{Q}$ is Galois since it is the splitting field of $x^3 - 2$ over $\mathbb{Q}$, 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 $K/\mathbb{Q}$.

Fundamentally Galois Examples, IV

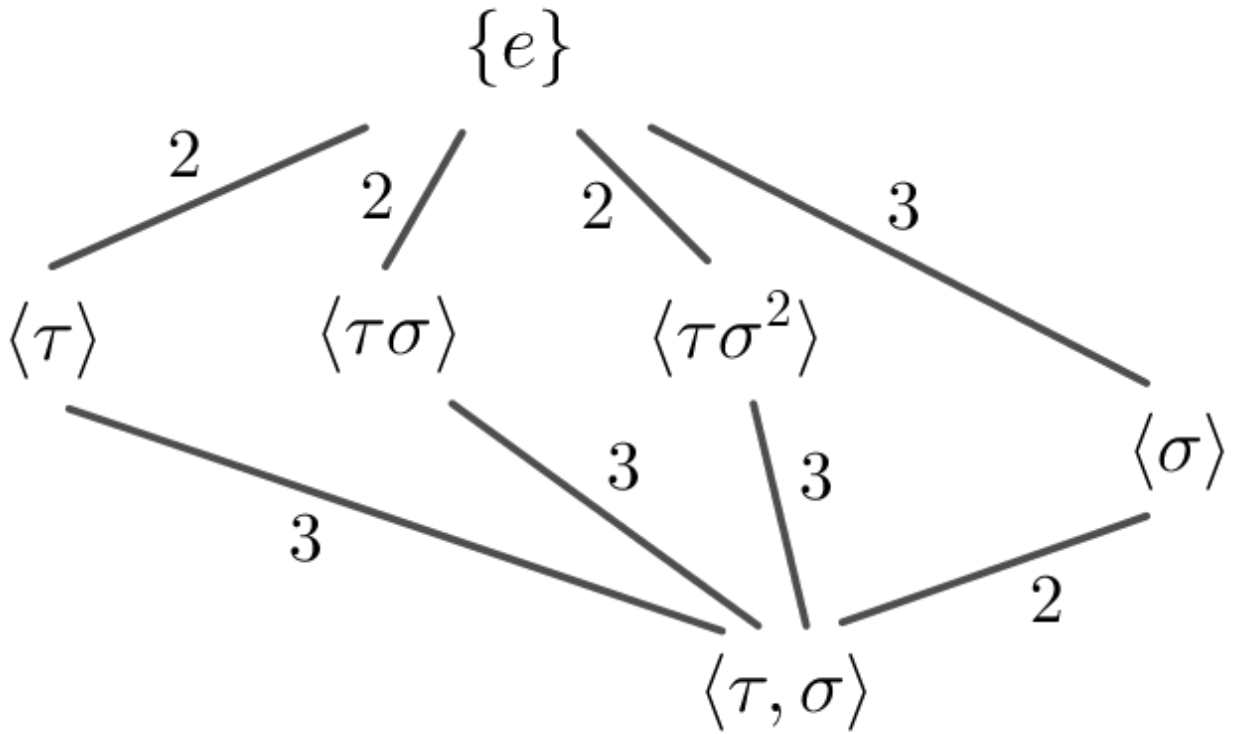
Example: Identify all of the intermediate fields of $\mathbb{Q}(2^{1/3}, \zeta_3)/\mathbb{Q}$ and then draw the subfield lattice.

- 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 $(2\,3)$.

Fundamentally Galois Examples, V

Example: Identify all of the intermediate fields of $\mathbb{Q}(2^{1/3}, \zeta_3)/\mathbb{Q}$ and then draw the subfield lattice.

- 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:



Fundamentally Galois Examples, VI

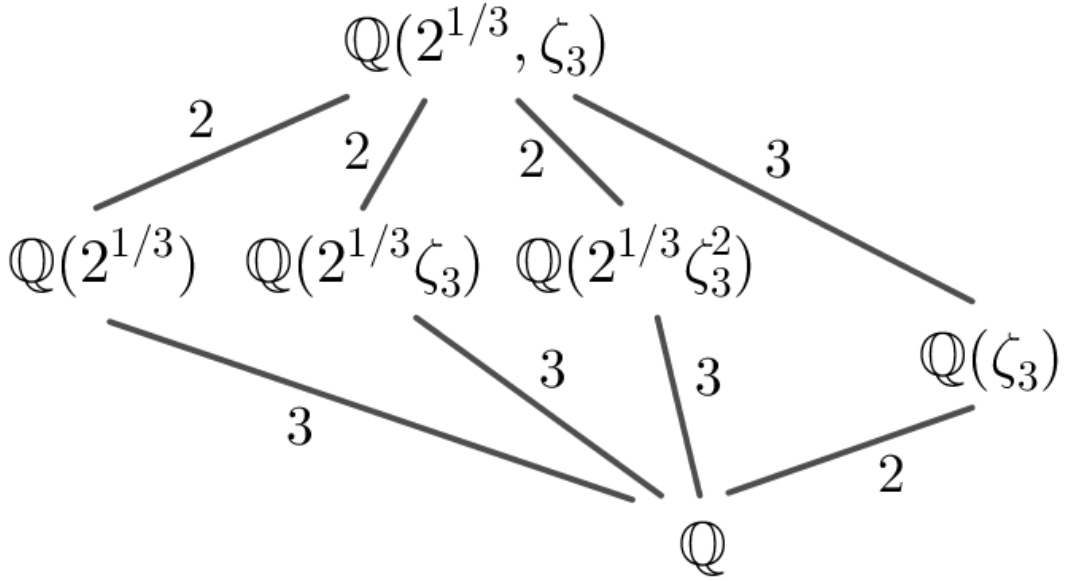
Example: Identify all of the intermediate fields of $\mathbb{Q}(2^{1/3}, \zeta_3)/\mathbb{Q}$ and then draw the subfield lattice.

- 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 $\mathbb{Q}(2^{1/3})$.

Fundamentally Galois Examples, VII

Example: Identify all of the intermediate fields of $\mathbb{Q}(2^{1/3}, \zeta_3)/\mathbb{Q}$ and then draw the subfield lattice.

- Since $\langle \tau \rangle$ 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 assemble this information into the full subfield lattice:



Fundamentally Galois Examples, VIII

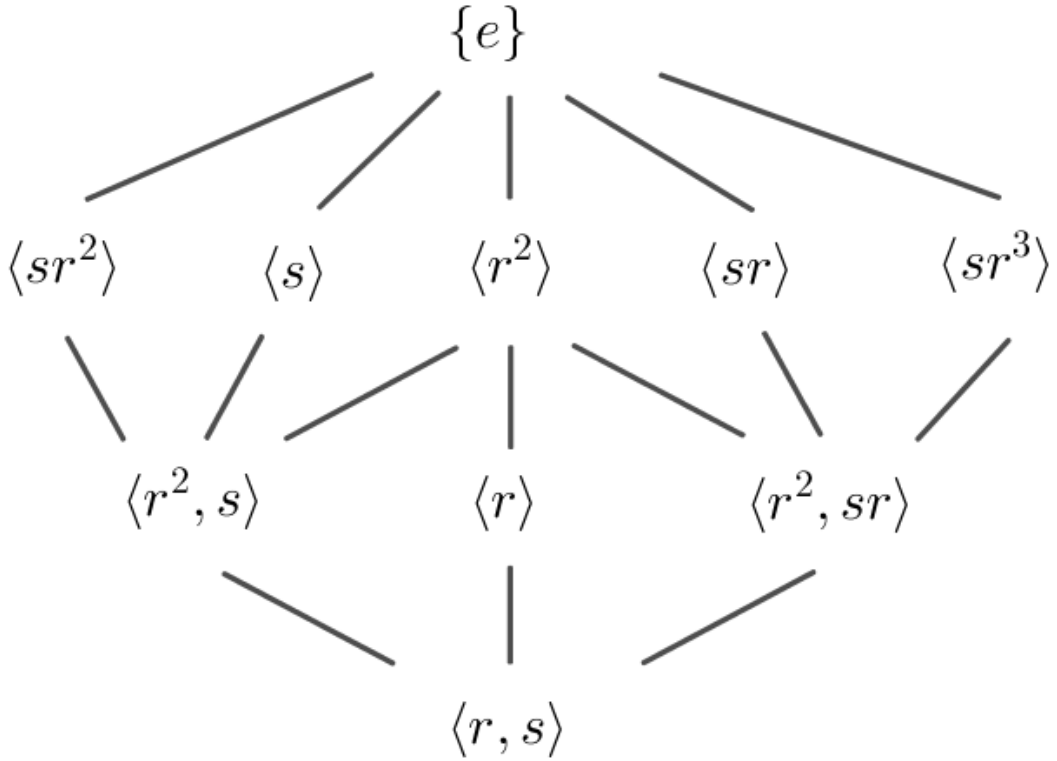
Example: Identify all of the intermediate fields of $\mathbb{Q}(3^{1/4}, i)$ and then draw the subfield lattice.

- 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 $D_{2\cdot 4}$.

Fundamentally Galois Examples, IX

Example: Identify all of the intermediate fields of $\mathbb{Q}(3^{1/4}, i)$ and then draw the subfield lattice.

- 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:



Fundamentally Galois Examples, X

Example: Identify all of the intermediate fields of $\mathbb{Q}(3^{1/4}, i)$ and then draw the subfield 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 $\mathbb{Q}(\sqrt{3})$.

Fundamentally Galois Examples, XI

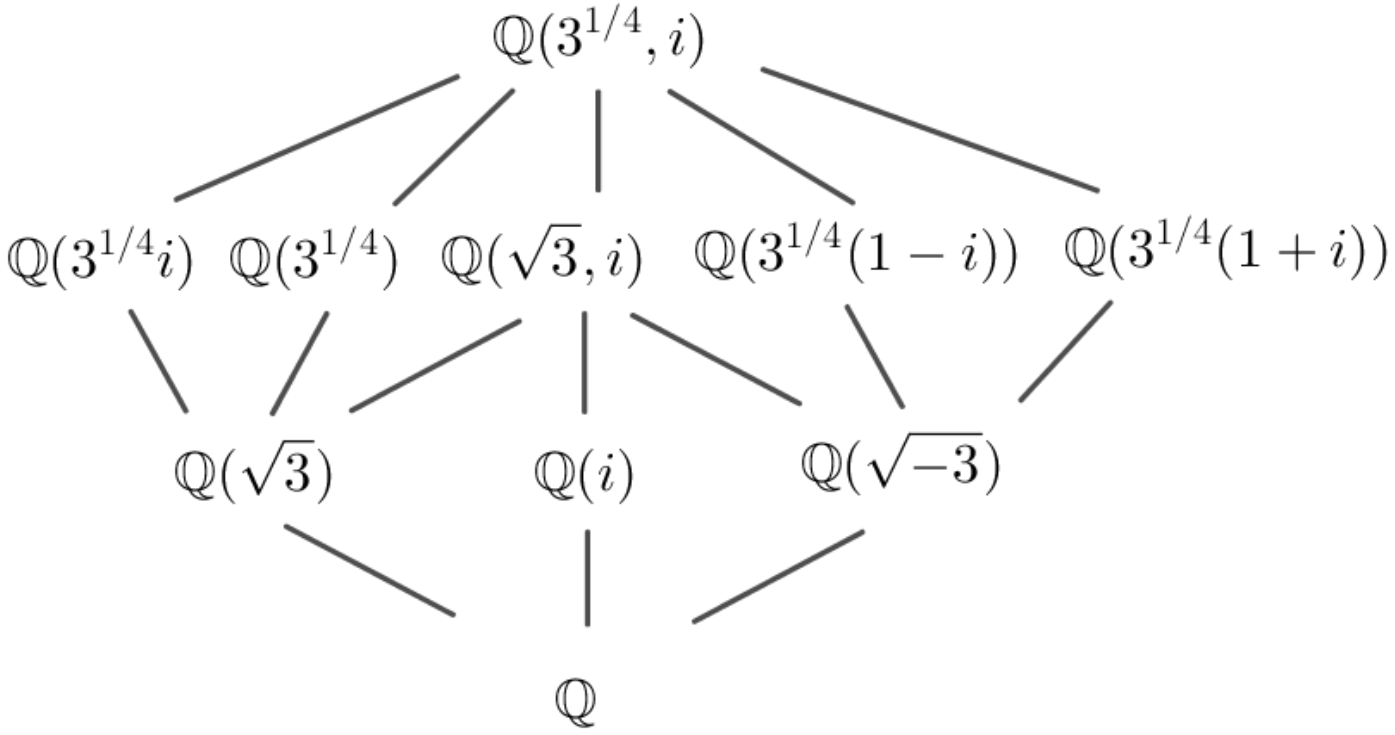
Example: Identify all of the intermediate fields of $\mathbb{Q}(3^{1/4}, i)$ and then draw the subfield lattice.

- 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 fields 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 $r[\mathbb{Q}(3^{1/4}(1-i))] = \mathbb{Q}(3^{1/4}(1+i))$.

Fundamentally Galois Examples, XII

Example: Identify all of the intermediate fields of $\mathbb{Q}(3^{1/4}, i)$ and then draw the subfield lattice.

- So the full subfield lattice is as follows:



Fundamentally Galois Examples, XIII

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 $0 \leq k \leq 5$, 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 $0 \leq k \leq 5$, and must also map ζ_6 to one of its two Galois conjugates over $\mathbb{Q}$, namely ζ_6, $\zeta_6^5 = \overline{\zeta_6}$.

Fundamentally Galois Examples, XIV

Example: Find the splitting field K of $p(x) = x^6 + 3$ over $\mathbb{Q}$ and identify all of its subfields.

- 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 $\zeta_6 \in \mathbb{Q}(\alpha)$, as you showed on Homework 5.
- 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.

Fundamentally Galois Examples, XV

Example: Find the splitting field K of $p(x) = x^6 + 3$ over $\mathbb{Q}$ and identify all of its subfields.

- 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 $\sigma\tau \neq \tau\sigma$.
- 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.

Fundamentally Galois Examples, XVI

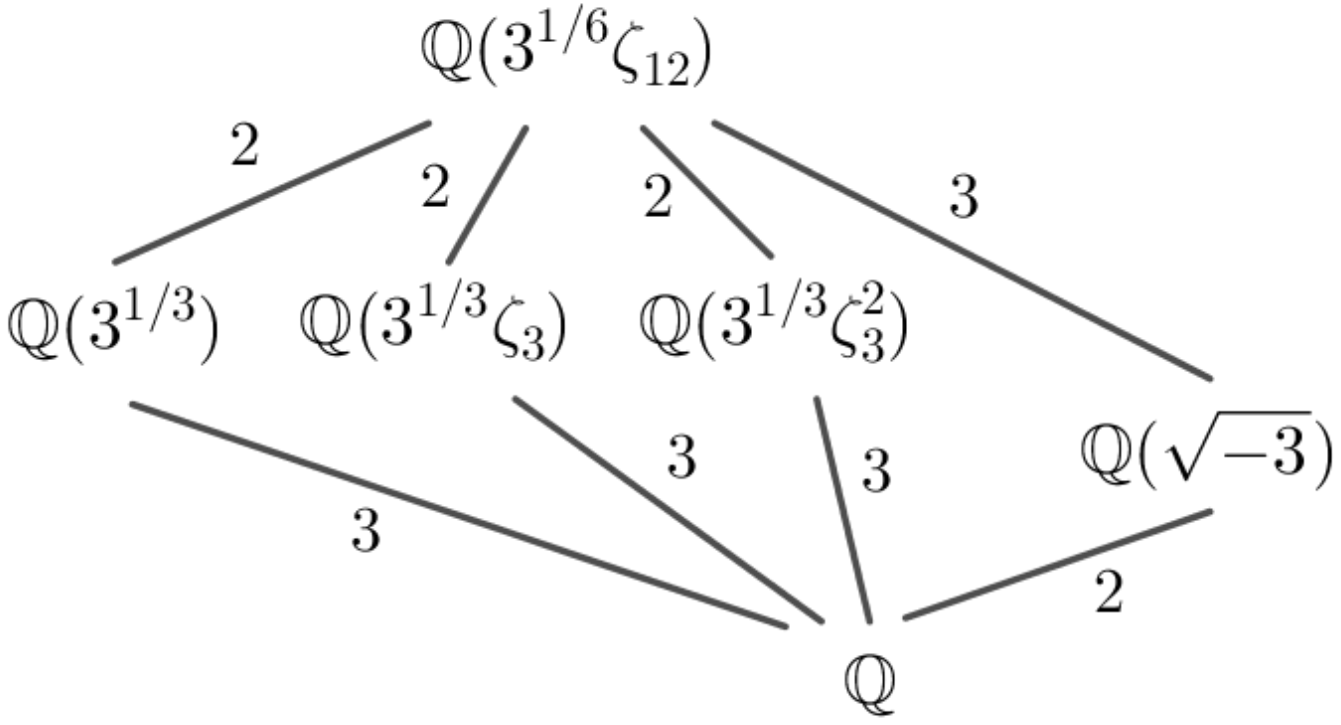
Example: Find the splitting field K of $p(x) = x^6 + 3$ over $\mathbb{Q}$ and identify all of its subfields.

- 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 $\langle\sigma\tau^2\rangle$).

Fundamentally Galois Examples, XVII

Example: Find the splitting field K of $p(x) = x^6 + 3$ over $\mathbb{Q}$ and identify all of its subfields.

- The full subfield diagram is then as follows:



Summary

We established some characterizations of Galois extensions.

We prove the fundamental theorem of Galois theory.

We discussed a number of examples of the Galois correspondence.

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