Math-123: Basic definitions of Galois theory

Sebastien Vasey

Harvard University

April 1, 2020

Announcement

It was decided last week that every class at Harvard this semester will be evaluated Sat/Unsat ("SEM/UEM").

Announcement

It was decided last week that every class at Harvard this semester will be evaluated Sat/Unsat ("SEM/UEM").

I updated the syllabus to describe how I will determine your grade.

Announcement

It was decided last week that every class at Harvard this semester will be evaluated Sat/Unsat ("SEM/UEM").

I updated the syllabus to describe how I will determine your grade.

If your class score is at least 70%, you get SEM.

Announcement

It was decided last week that every class at Harvard this semester will be evaluated Sat/Unsat ("SEM/UEM").

I updated the syllabus to describe how I will determine your grade.

If your class score is at least 70%, you get SEM.

If you are below 70%, you may or may not get SEM depending on class performance, participation, special circumstances, etc.

Finishing the proof from last time

Recall $\zeta_n := e^{2\pi i/n}$.

Finishing the proof from last time

Recall $\zeta_n := e^{2\pi i/n}$.

Definition

The *nth cyclotomic polynomial,* $\Phi_n(x)$ is the polynomial whose roots are the *primitive* nth roots of unity:

$$\Phi_n(x) := \prod_{1 \le k \le n, (k,n)=1} (x - \zeta_n^k)$$

Finishing the proof from last time

Recall $\zeta_n := e^{2\pi i/n}$.

Definition

The *nth cyclotomic polynomial,* $\Phi_n(x)$ is the polynomial whose roots are the *primitive* nth roots of unity:

$$\Phi_n(x) := \prod_{1 \leq k \leq n, (k,n)=1} (x - \zeta_n^k)$$

We proved that $\Phi_n(x)$ is a monic polynomial of degree $\phi(n)$, with integer coefficients.

Lemma

If $g(x) \in \mathbb{F}_p[x]$, then $g(x^p) = (g(x))^p$.

Lemma

If $g(x) \in \mathbb{F}_p[x]$, then $g(x^p) = (g(x))^p$.

Proof.

Say $g(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$. By properties of the Frobenius map, $g(x)^p = a_n^p x^{pn} + a_{n-1}^p x^{p(n-1)} + \ldots + a_0^p$.

Lemma

If $g(x) \in \mathbb{F}_p[x]$, then $g(x^p) = (g(x))^p$.

Proof.

Say $g(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$. By properties of the Frobenius map, $g(x)^p = a_n^p x^{pn} + a_{n-1}^p x^{p(n-1)} + \ldots + a_0^p$.

Now use that $a^p = a$ for every $a \in \mathbb{F}_p$ (Lagrange's theorem applied to the group of units $\mathbb{F}_p^\times$ – also called Fermat's little theorem).

Lemma

If $g(x) \in \mathbb{F}_p[x]$, then $g(x^p) = (g(x))^p$.

Proof.

Say $g(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$. By properties of the Frobenius map, $g(x)^p = a_n^p x^{pn} + a_{n-1}^p x^{p(n-1)} + \ldots + a_0^p$.

Now use that $a^p = a$ for every $a \in \mathbb{F}_p$ (Lagrange's theorem applied to the group of units $\mathbb{F}_p^\times$ – also called Fermat's little theorem).

Get $g(x)^p = a_n x^{pn} + a_{n-1} x^{p(n-1)} + \ldots + a_0 = g(x^p)$. $\square$

Theorem

$\Phi_n(x)$ is irreducible in $\mathbb{Z}[x]$. Thus the degree of $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$ is $\phi(n)$.

Theorem

$\Phi_n(x)$ is irreducible in $\mathbb{Z}[x]$. Thus the degree of $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$ is $\phi(n)$.

Proof: Write $\Phi_n(x) = f(x)g(x)$, for f, g monic in $\mathbb{Z}[x]$, f irreducible with some primitive root of unity ζ as a root.

Theorem

$\Phi_n(x)$ is irreducible in $\mathbb{Z}[x]$. Thus the degree of $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$ is $\phi(n)$.

Proof: Write $\Phi_n(x) = f(x)g(x)$, for f, g monic in $\mathbb{Z}[x]$, f irreducible with some primitive root of unity ζ as a root.

Let p be a prime not dividing n. Then ζ^p is a primitive root of unity. Either $f(\zeta^p) = 0$ or $g(\zeta^p) = 0$.

Theorem

$\Phi_n(x)$ is irreducible in $\mathbb{Z}[x]$. Thus the degree of $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$ is $\phi(n)$.

Proof: Write $\Phi_n(x) = f(x)g(x)$, for f, g monic in $\mathbb{Z}[x]$, f irreducible with some primitive root of unity ζ as a root.

Let p be a prime not dividing n. Then ζ^p is a primitive root of unity. Either $f(\zeta^p) = 0$ or $g(\zeta^p) = 0$.

If $g(\zeta^p) = 0$, then ζ is a root of $g(x^p)$, so since $f(x)$ is the minimal polynomial of ζ, $f(x)$ divides $g(x^p)$ in $\mathbb{Z}[x]$:

Theorem

$\Phi_n(x)$ is irreducible in $\mathbb{Z}[x]$. Thus the degree of $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$ is $\phi(n)$.

Proof: Write $\Phi_n(x) = f(x)g(x)$, for f, g monic in $\mathbb{Z}[x]$, f irreducible with some primitive root of unity ζ as a root.

Let p be a prime not dividing n. Then ζ^p is a primitive root of unity. Either $f(\zeta^p) = 0$ or $g(\zeta^p) = 0$.

If $g(\zeta^p) = 0$, then ζ is a root of $g(x^p)$, so since $f(x)$ is the minimal polynomial of ζ, $f(x)$ divides $g(x^p)$ in $\mathbb{Z}[x]$:

$$g(x^p) = f(x)h(x)$$

Theorem

$\Phi_n(x)$ is irreducible in $\mathbb{Z}[x]$. Thus the degree of $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$ is $\phi(n)$.

Proof: Write $\Phi_n(x) = f(x)g(x)$, for f, g monic in $\mathbb{Z}[x]$, f irreducible with some primitive root of unity ζ as a root.

Let p be a prime not dividing n. Then ζ^p is a primitive root of unity. Either $f(\zeta^p) = 0$ or $g(\zeta^p) = 0$.

If $g(\zeta^p) = 0$, then ζ is a root of $g(x^p)$, so since $f(x)$ is the minimal polynomial of ζ, $f(x)$ divides $g(x^p)$ in $\mathbb{Z}[x]$:

$$g(x^p) = f(x)h(x)$$

Reducing modulo p, we get $\bar{g}(x^p) = (\bar{g}(x))^p = \bar{f}(x)\bar{g}(x)$.

Theorem

$\Phi_n(x)$ is irreducible in $\mathbb{Z}[x]$. Thus the degree of $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$ is $\phi(n)$.

Proof: Write $\Phi_n(x) = f(x)g(x)$, for f, g monic in $\mathbb{Z}[x]$, f irreducible with some primitive root of unity ζ as a root.

Let p be a prime not dividing n. Then ζ^p is a primitive root of unity. Either $f(\zeta^p) = 0$ or $g(\zeta^p) = 0$.

If $g(\zeta^p) = 0$, then ζ is a root of $g(x^p)$, so since $f(x)$ is the minimal polynomial of ζ, $f(x)$ divides $g(x^p)$ in $\mathbb{Z}[x]$:

$$g(x^p) = f(x)h(x)$$

Reducing modulo p, we get $\bar{g}(x^p) = (\bar{g}(x))^p = \bar{f}(x)\bar{g}(x)$.

So $\bar{f}$ and $\bar{g}$ have an irreducible factor in common in $\mathbb{F}_p[x]$!

Proof of irreducibility of Φ_n, continued

We know also $\bar{f}\bar{g} = \overline{\Phi_n}(x)$. Since $\bar{f}$ and $\bar{g}$ have a factor in common, $\overline{\Phi_n}(x)$ has a multiple root in $\mathbb{F}_p[x]$.

Proof of irreducibility of Φ_n, continued

We know also $\bar{f}\bar{g} = \overline{\Phi_n}(x)$. Since $\bar{f}$ and $\bar{g}$ have a factor in common, $\overline{\Phi_n}(x)$ has a multiple root in $\mathbb{F}_p[x]$.

Thus $x^n - 1$ also has a multiple root in $\mathbb{F}_p[x]$. We saw before that if p does not divide n, $x^n - 1$ is separable, contradiction.

Proof of irreducibility of Φ_n, continued

We know also $\bar{f}\bar{g} = \overline{\Phi_n}(x)$. Since $\bar{f}$ and $\bar{g}$ have a factor in common, $\overline{\Phi_n}(x)$ has a multiple root in $\mathbb{F}_p[x]$.

Thus $x^n - 1$ also has a multiple root in $\mathbb{F}_p[x]$. We saw before that if p does not divide n, $x^n - 1$ is separable, contradiction.

We had that $\Phi_n(x) = f(x)g(x)$, f irreducible, and we took ζ a root of f. We showed $g(\zeta^p) \neq 0$ for any prime p not dividing n.

Proof of irreducibility of Φ_n, continued

We know also $\bar{f}\bar{g} = \overline{\Phi_n}(x)$. Since $\bar{f}$ and $\bar{g}$ have a factor in common, $\overline{\Phi_n}(x)$ has a multiple root in $\mathbb{F}_p[x]$.

Thus $x^n - 1$ also has a multiple root in $\mathbb{F}_p[x]$. We saw before that if p does not divide n, $x^n - 1$ is separable, contradiction.

We had that $\Phi_n(x) = f(x)g(x)$, f irreducible, and we took ζ a root of f. We showed $g(\zeta^p) \neq 0$ for any prime p not dividing n.

Thus $f(\rho^p) = 0$ for *any* root ρ of f and *any* prime p not dividing n.

Proof of irreducibility of Φ_n, continued

We know also $\bar{f}\bar{g} = \overline{\Phi_n}(x)$. Since $\bar{f}$ and $\bar{g}$ have a factor in common, $\overline{\Phi_n}(x)$ has a multiple root in $\mathbb{F}_p[x]$.

Thus $x^n - 1$ also has a multiple root in $\mathbb{F}_p[x]$. We saw before that if p does not divide n, $x^n - 1$ is separable, contradiction.

We had that $\Phi_n(x) = f(x)g(x)$, f irreducible, and we took ζ a root of f. We showed $g(\zeta^p) \neq 0$ for any prime p not dividing n.

Thus $f(\rho^p) = 0$ for *any* root ρ of f and *any* prime p not dividing n.

If ζ is a root of f, any other primitive root of unity is of the form ζ^k, k coprime to n. Thus $k = p_1 p_2 \ldots p_m$, with the p_i's primes not dividing n.

Proof of irreducibility of Φ_n, continued

We know also $\bar{f}\bar{g} = \overline{\Phi_n}(x)$. Since $\bar{f}$ and $\bar{g}$ have a factor in common, $\overline{\Phi_n}(x)$ has a multiple root in $\mathbb{F}_p[x]$.

Thus $x^n - 1$ also has a multiple root in $\mathbb{F}_p[x]$. We saw before that if p does not divide n, $x^n - 1$ is separable, contradiction.

We had that $\Phi_n(x) = f(x)g(x)$, f irreducible, and we took ζ a root of f. We showed $g(\zeta^p) \neq 0$ for any prime p not dividing n.

Thus $f(\rho^p) = 0$ for *any* root ρ of f and *any* prime p not dividing n.

If ζ is a root of f, any other primitive root of unity is of the form ζ^k, k coprime to n. Thus $k = p_1 p_2 \ldots p_m$, with the p_i's primes not dividing n.

We showed $f(\zeta^{p_1}) = 0$. Thus applying the previous observation to $\rho = \zeta^{p_1}$ and $p = p_2$, $f(\zeta^{p_1 p_2}) = 0$.

Proof of irreducibility of Φ_n, continued

We know also $\bar{f}\bar{g} = \overline{\Phi_n}(x)$. Since $\bar{f}$ and $\bar{g}$ have a factor in common, $\overline{\Phi_n}(x)$ has a multiple root in $\mathbb{F}_p[x]$.

Thus $x^n - 1$ also has a multiple root in $\mathbb{F}_p[x]$. We saw before that if p does not divide n, $x^n - 1$ is separable, contradiction.

We had that $\Phi_n(x) = f(x)g(x)$, f irreducible, and we took ζ a root of f. We showed $g(\zeta^p) \neq 0$ for any prime p not dividing n.

Thus $f(\rho^p) = 0$ for *any* root ρ of f and *any* prime p not dividing n.

If ζ is a root of f, any other primitive root of unity is of the form ζ^k, k coprime to n. Thus $k = p_1 p_2 \ldots p_m$, with the p_i's primes not dividing n.

We showed $f(\zeta^{p_1}) = 0$. Thus applying the previous observation to $\rho = \zeta^{p_1}$ and $p = p_2$, $f(\zeta^{p_1 p_2}) = 0$.

Continuing in this way, we get that $f(\zeta^{p_1 p_2 \cdots p_m}) = 0$. Thus f has *all* primitive roots of unity as roots, so $f = \Phi_n$, as desired.

Galois theory

The idea: study automorphisms of fields, and how they permute roots of polynomials.

Galois theory

The idea: study automorphisms of fields, and how they permute roots of polynomials.

Definition

- An isomorphism σ of a field K to itself is called an *automorphism* of K.

Galois theory

The idea: study automorphisms of fields, and how they permute roots of polynomials.

Definition

- An isomorphism σ of a field K to itself is called an *automorphism* of K.
- We write $\mathrm{Aut}(K)$ for the set of all automorphisms of K.

Galois theory

The idea: study automorphisms of fields, and how they permute roots of polynomials.

Definition

- An isomorphism σ of a field K to itself is called an *automorphism* of K.
- We write $\mathrm{Aut}(K)$ for the set of all automorphisms of K.
- An automorphism σ of K *fixes* an element a if $\sigma(a) = a$. We say σ *fixes* a set A if $\sigma(a) = a$ for all $a \in A$.

Galois theory

The idea: study automorphisms of fields, and how they permute roots of polynomials.

Definition

- An isomorphism σ of a field K to itself is called an *automorphism* of K.
- We write $\mathrm{Aut}(K)$ for the set of all automorphisms of K.
- An automorphism σ of K *fixes* an element a if $\sigma(a) = a$. We say σ *fixes* a set A if $\sigma(a) = a$ for all $a \in A$.
- If K is an extension of F, we write $\mathrm{Aut}(K/F)$ for the set of all automorphisms of K which fix F.

Two key observations

1. $\text{Aut}(K)$ is a group under composition, and $\text{Aut}(K/F)$ is a subgroup.

Two key observations

1. $\mathrm{Aut}(K)$ is a group under composition, and $\mathrm{Aut}(K/F)$ is a subgroup.
2. If K/F is an extension, $f(x) \in F[x]$, $\alpha \in K$ is a root of f, then for any $\sigma \in \mathrm{Aut}(K/F)$, $\sigma(\alpha)$ is also a root of f.

Two key observations

1. $\text{Aut}(K)$ is a group under composition, and $\text{Aut}(K/F)$ is a subgroup.
2. If K/F is an extension, $f(x) \in F[x]$, $\alpha \in K$ is a root of f, then for any $\sigma \in \text{Aut}(K/F)$, $\sigma(\alpha)$ is also a root of f.

The second observation says that automorphisms *permute* the roots of a polynomial. Abstractly: the group $\text{Aut}(K/F)$ *acts* on these roots.

Examples

- $\mathrm{Aut}(\mathbb{Q}) = \{\mathrm{id}\}$, since any automorphism must fix 1 and preserve sums and quotients. We write 1 instead of id, so $\mathrm{Aut}(\mathbb{Q}) = \{1\}$.

Examples

- $\mathrm{Aut}(\mathbb{Q}) = \{\mathrm{id}\}$, since any automorphism must fix 1 and preserve sums and quotients. We write 1 instead of id, so $\mathrm{Aut}(\mathbb{Q}) = \{1\}$.
- Similarly, $\mathrm{Aut}(\mathbb{F}_p) = \{1\}$. In general, any automorphism fixes the prime field.

Examples

- $\mathrm{Aut}(\mathbb{Q}) = \{\mathrm{id}\}$, since any automorphism must fix 1 and preserve sums and quotients. We write 1 instead of id, so $\mathrm{Aut}(\mathbb{Q}) = \{1\}$.
- Similarly, $\mathrm{Aut}(\mathbb{F}_p) = \{1\}$. In general, any automorphism fixes the prime field.
- Let $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt{2})$. Note $\mathrm{Aut}(K) = \mathrm{Aut}(K/F)$. Let $\sigma \in \mathrm{Aut}(K)$.

Examples

- $\mathrm{Aut}(\mathbb{Q}) = \{\mathrm{id}\}$, since any automorphism must fix 1 and preserve sums and quotients. We write 1 instead of id, so $\mathrm{Aut}(\mathbb{Q}) = \{1\}$.
- Similarly, $\mathrm{Aut}(\mathbb{F}_p) = \{1\}$. In general, any automorphism fixes the prime field.
- Let $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt{2})$. Note $\mathrm{Aut}(K) = \mathrm{Aut}(K/F)$. Let $\sigma \in \mathrm{Aut}(K)$.
  - $\sqrt{2}$ is a root of $x^2 - 2$, so $\tau(\sqrt{2})$ is a root of $x^2 - 2$. Thus $\tau(\sqrt{2}) = \pm\sqrt{2}$.

Examples

- $\mathrm{Aut}(\mathbb{Q}) = \{\mathrm{id}\}$, since any automorphism must fix 1 and preserve sums and quotients. We write 1 instead of id, so $\mathrm{Aut}(\mathbb{Q}) = \{1\}$.
- Similarly, $\mathrm{Aut}(\mathbb{F}_p) = \{1\}$. In general, any automorphism fixes the prime field.
- Let $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt{2})$. Note $\mathrm{Aut}(K) = \mathrm{Aut}(K/F)$. Let $\sigma \in \mathrm{Aut}(K)$.
  - $\sqrt{2}$ is a root of $x^2 - 2$, so $\tau(\sqrt{2})$ is a root of $x^2 - 2$. Thus $\tau(\sqrt{2}) = \pm\sqrt{2}$.
  - Any element of K is of the form $\alpha = a + b\sqrt{2}$, $a, b \in \mathbb{Q}$, so $\tau(\alpha) = a + b\tau(\sqrt{2})$, so τ is determined by its value on $\sqrt{2}$.

Examples

- $\mathrm{Aut}(\mathbb{Q}) = \{\mathrm{id}\}$, since any automorphism must fix 1 and preserve sums and quotients. We write 1 instead of id, so $\mathrm{Aut}(\mathbb{Q}) = \{1\}$.
- Similarly, $\mathrm{Aut}(\mathbb{F}_p) = \{1\}$. In general, any automorphism fixes the prime field.
- Let $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt{2})$. Note $\mathrm{Aut}(K) = \mathrm{Aut}(K/F)$. Let $\sigma \in \mathrm{Aut}(K)$.
  - $\sqrt{2}$ is a root of $x^2 - 2$, so $\tau(\sqrt{2})$ is a root of $x^2 - 2$. Thus $\tau(\sqrt{2}) = \pm\sqrt{2}$.
  - Any element of K is of the form $\alpha = a + b\sqrt{2}$, $a, b \in \mathbb{Q}$, so $\tau(\alpha) = a + b\tau(\sqrt{2})$, so τ is determined by its value on $\sqrt{2}$.
  - If $\tau(\sqrt{2}) = \sqrt{2}$, τ is the identity. On the other hand $\tau(\sqrt{2}) = -\sqrt{2}$ is an automorphism (can check directly, or use uniqueness of simple extensions).

Examples

- $\mathrm{Aut}(\mathbb{Q}) = \{\mathrm{id}\}$, since any automorphism must fix 1 and preserve sums and quotients. We write 1 instead of id, so $\mathrm{Aut}(\mathbb{Q}) = \{1\}$.
- Similarly, $\mathrm{Aut}(\mathbb{F}_p) = \{1\}$. In general, any automorphism fixes the prime field.
- Let $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt{2})$. Note $\mathrm{Aut}(K) = \mathrm{Aut}(K/F)$. Let $\sigma \in \mathrm{Aut}(K)$.
  - $\sqrt{2}$ is a root of $x^2 - 2$, so $\tau(\sqrt{2})$ is a root of $x^2 - 2$. Thus $\tau(\sqrt{2}) = \pm\sqrt{2}$.
  - Any element of K is of the form $\alpha = a + b\sqrt{2}$, $a, b \in \mathbb{Q}$, so $\tau(\alpha) = a + b\tau(\sqrt{2})$, so τ is determined by its value on $\sqrt{2}$.
  - If $\tau(\sqrt{2}) = \sqrt{2}$, τ is the identity. On the other hand $\tau(\sqrt{2}) = -\sqrt{2}$ is an automorphism (can check directly, or use uniqueness of simple extensions).
  - Thus $\mathrm{Aut}(K/F) = \{1, \sigma\}$, where σ sends $\sqrt{2}$ to $-\sqrt{2}$. It is the cyclic group of order 2.

One more example

Let $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[3]{2})$.

One more example

Let $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[3]{2})$.

As before, any automorphism is determined by what it does to $\sqrt[3]{2}$.

One more example

Let $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[3]{2})$.

As before, any automorphism is determined by what it does to $\sqrt[3]{2}$.

If $\tau \in \mathrm{Aut}(K/F)$, $\tau(\sqrt[3]{2})$ must be a root of $x^3 - 2$. However the other roots of $x^3 - 2$ are not real numbers, so are not in K. Thus $\tau(\sqrt[3]{2}) = \sqrt[3]{2}$.

One more example

Let $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[3]{2})$.

As before, any automorphism is determined by what it does to $\sqrt[3]{2}$.

If $\tau \in \mathrm{Aut}(K/F)$, $\tau(\sqrt[3]{2})$ must be a root of $x^3 - 2$. However the other roots of $x^3 - 2$ are not real numbers, so are not in K. Thus $\tau(\sqrt[3]{2}) = \sqrt[3]{2}$.

This shows that $\mathrm{Aut}(K/F) = \{1\}$, the trivial group.

From field to group and back

Fix a field K.

Given a subfield F, we get a group $\mathrm{Aut}(K/F)$.

From field to group and back

Fix a field K.

Given a subfield F, we get a group $\mathrm{Aut}(K/F)$.

Going back, if we fix a subgroup H of $\mathrm{Aut}(K)$, we can get a subfield:

From field to group and back

Fix a field K.

Given a subfield F, we get a group $\mathrm{Aut}(K/F)$.

Going back, if we fix a subgroup H of $\mathrm{Aut}(K)$, we can get a subfield:

Definition

The *fixed field of* H is the subfield of K of all elements fixed by every automorphism in H.

From field to group and back

Fix a field K.

Given a subfield F, we get a group $\mathrm{Aut}(K/F)$.

Going back, if we fix a subgroup H of $\mathrm{Aut}(K)$, we can get a subfield:

Definition

The *fixed field of* H is the subfield of K of all elements fixed by every automorphism in H.

(one can check it is indeed a subfield: if a and b are fixed, ab, $a+b$, a/b are fixed too!).

Going from subfield to groups, and back, give *inclusion-reversing operations*:

Going from subfield to groups, and back, give *inclusion-reversing operations*:

1. If $F_1 \subseteq F_2 \subseteq K$, then $\mathrm{Aut}(K/F_2) \subseteq \mathrm{Aut}(K/F_1)$. [The fewer things to fix, the more automorphisms].

Going from subfield to groups, and back, give *inclusion-reversing operations*:

1. If $F_1 \subseteq F_2 \subseteq K$, then $\text{Aut}(K/F_2) \subseteq \text{Aut}(K/F_1)$. [The fewer things to fix, the more automorphisms].
2. If $H_1 \subseteq H_2 \subseteq \text{Aut}(K)$, with fixed fields F_1, F_2, then $F_2 \subseteq F_1$ [Fewer automorphisms fix more things].

Back to the examples

$K = \mathbb{Q}(\sqrt{2})$, $F = \mathbb{Q}$.

Back to the examples

$K = \mathbb{Q}(\sqrt{2})$, $F = \mathbb{Q}$. The fixed field of $\mathrm{Aut}(K/F)$ is the set of elements of $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ fixed by *all* automorphisms.

Back to the examples

$K = \mathbb{Q}(\sqrt{2})$, $F = \mathbb{Q}$. The fixed field of $\mathrm{Aut}(K/F)$ is the set of elements of $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ fixed by *all* automorphisms.

In particular we need $a + b\sqrt{2} = a - b\sqrt{2}$, so $b = 0$. Any automorphism fixes the rationals, so the fixed field of $\mathrm{Aut}(K/F)$ is $\mathbb{Q}$.

Back to the examples

$K = \mathbb{Q}(\sqrt{2})$, $F = \mathbb{Q}$. The fixed field of $\mathrm{Aut}(K/F)$ is the set of elements of $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ fixed by *all* automorphisms.

In particular we need $a + b\sqrt{2} = a - b\sqrt{2}$, so $b = 0$. Any automorphism fixes the rationals, so the fixed field of $\mathrm{Aut}(K/F)$ is $\mathbb{Q}$.

The fixed field of $\{1\}$ is $\mathbb{Q}(\sqrt{2})$.

Back to the examples

$K = \mathbb{Q}(\sqrt{2})$, $F = \mathbb{Q}$. The fixed field of $\mathrm{Aut}(K/F)$ is the set of elements of $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ fixed by *all* automorphisms.

In particular we need $a + b\sqrt{2} = a - b\sqrt{2}$, so $b = 0$. Any automorphism fixes the rationals, so the fixed field of $\mathrm{Aut}(K/F)$ is $\mathbb{Q}$.

The fixed field of $\{1\}$ is $\mathbb{Q}(\sqrt{2})$.

Suppose now $K = \mathbb{Q}(\sqrt[3]{2})$, $F = \mathbb{Q}$. The fixed field of $\mathrm{Aut}(K/F) = \{1\}$ is just $\mathbb{Q}(\sqrt[3]{2})$: there is only one automorphism, the identity, which fixes everything.

Back to the examples

$K = \mathbb{Q}(\sqrt{2})$, $F = \mathbb{Q}$. The fixed field of $\mathrm{Aut}(K/F)$ is the set of elements of $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ fixed by *all* automorphisms.

In particular we need $a + b\sqrt{2} = a - b\sqrt{2}$, so $b = 0$. Any automorphism fixes the rationals, so the fixed field of $\mathrm{Aut}(K/F)$ is $\mathbb{Q}$.

The fixed field of $\{1\}$ is $\mathbb{Q}(\sqrt{2})$.

Suppose now $K = \mathbb{Q}(\sqrt[3]{2})$, $F = \mathbb{Q}$. The fixed field of $\mathrm{Aut}(K/F) = \{1\}$ is just $\mathbb{Q}(\sqrt[3]{2})$: there is only one automorphism, the identity, which fixes everything.

So in this case, $\mathbb{Q}$ is not the fixed field of any subgroup. Intuitively, we are "missing roots" for $x^3 - 2$.

Automorphisms of the splitting field

Theorem

Let K be the splitting field of a polynomial $f(x) \in F[x]$. Then $\mathrm{Aut}(K/F)$ has at most $[K : F]$ elements, with equality if f is separable.

Automorphisms of the splitting field

Theorem

Let K be the splitting field of a polynomial $f(x) \in F[x]$. Then $\mathrm{Aut}(K/F)$ has at most $[K : F]$ elements, with equality if f is separable.

Proof: We more generally ask: given an isomorphism $\phi : F \cong F'$, K a splitting field of $f(x)$, K' a splitting field of the corresponding polynomial $f' = \phi(f)$, how many isomorphisms $\sigma : K \cong K'$ does ϕ extend to?

$$\begin{array}{ccc} K & \xrightarrow[\sigma]{\cong} & K' \\ | & & | \\ F & \xrightarrow[\phi]{\cong} & F' \end{array}$$

Automorphisms of the splitting field

Theorem

Let K be the splitting field of a polynomial $f(x) \in F[x]$. Then $\mathrm{Aut}(K/F)$ has at most $[K : F]$ elements, with equality if f is separable.

Proof: We more generally ask: given an isomorphism $\phi : F \cong F'$, K a splitting field of $f(x)$, K' a splitting field of the corresponding polynomial $f' = \phi(f)$, how many isomorphisms $\sigma : K \cong K'$ does ϕ extend to?

$$\begin{array}{ccc} K & \xrightarrow[\sigma]{\cong} & K' \\ | & & | \\ F & \xrightarrow[\phi]{\cong} & F' \end{array}$$

The special case we care about is when $F = F'$, ϕ is the identity, $K = K'$.

$$
\begin{array}{ccc}
K & \xrightarrow[\sigma]{\cong} & K' \\
\Big| & & \Big| \\
F & \xrightarrow[\phi]{\cong} & F'
\end{array}
$$

$$\begin{array}{ccc} K & \xrightarrow[\sigma]{\cong} & K' \\ | & & | \\ F & \xrightarrow[\phi]{\cong} & F' \end{array}$$

We proceed by induction on $n := [K : F]$. If $n = 1$, $\sigma = \phi$ is the only extension. Assume now $n \geq 2$.

$$
\begin{array}{ccc}
K & \xrightarrow[\sigma]{\cong} & K' \\
\Big| & & \Big| \\
F & \xrightarrow[\phi]{\cong} & F'
\end{array}
$$

We proceed by induction on $n := [K : F]$. If $n = 1$, $\sigma = \phi$ is the only extension. Assume now $n \geq 2$.

Let $p(x)$ be an irreducible factor of $f(x)$, $p'(x)$ the corresponding irreducible factor of $f'(x)$. Fix a root α of $p(x)$. For any root α' of $p'(x)$, we get a picture like below with $\phi'(\alpha) = \alpha'$.

$$\begin{array}{ccc} K & \xrightarrow[\sigma]{\cong} & K' \\ \Big| & & \Big| \\ F & \xrightarrow[\phi]{\cong} & F' \end{array}$$

We proceed by induction on $n := [K : F]$. If $n = 1$, $\sigma = \phi$ is the only extension. Assume now $n \geq 2$.

Let $p(x)$ be an irreducible factor of $f(x)$, $p'(x)$ the corresponding irreducible factor of $f'(x)$. Fix a root α of $p(x)$. For any root α' of $p'(x)$, we get a picture like below with $\phi'(\alpha) = \alpha'$.

$$\begin{array}{ccc} K & \xrightarrow[\sigma]{\cong} & K' \\ \Big| & & \Big| \\ F(\alpha) & \xrightarrow[\phi']{\cong} & F'(\alpha') \\ \Big| & & \Big| \\ F & \xrightarrow[\phi]{\cong} & F' \end{array}$$

$$
\begin{array}{ccc}
K & \xrightarrow[\sigma]{\cong} & K' \\
\Big| & & \Big| \\
F(\alpha) & \xrightarrow[\phi']{\cong} & F'(\alpha') \\
\Big| & & \Big| \\
F & \xrightarrow[\phi]{\cong} & F'
\end{array}
$$

$$
\begin{array}{ccc}
K & \xrightarrow[\sigma]{\cong} & K' \\
\Big| & & \Big| \\
F(\alpha) & \xrightarrow[\phi']{\cong} & F'(\alpha') \\
\Big| & & \Big| \\
F & \xrightarrow[\phi]{\cong} & F'
\end{array}
$$

By the induction hypothesis, there are (at most) $[K : F(\alpha)]$-many ways to extend each ϕ' to a σ, with equality if $\frac{f(x)}{x-\alpha}$ is separable.

$$
\begin{array}{ccc}
K & \xrightarrow[\sigma]{\cong} & K' \\
\Big| & & \Big| \\
F(\alpha) & \xrightarrow[\phi']{\cong} & F'(\alpha') \\
\Big| & & \Big| \\
F & \xrightarrow[\phi]{\cong} & F'
\end{array}
$$

By the induction hypothesis, there are (at most) $[K : F(\alpha)]$-many ways to extend each ϕ' to a σ, with equality if $\frac{f(x)}{x-\alpha}$ is separable.

There are as many ways to extend ϕ to ϕ' as there are roots for $p(x)$. This number of roots is at most the degree of $p(x)$, with equality if $p(x)$ is separable.

$$
\begin{array}{ccc}
K & \xrightarrow[\sigma]{\cong} & K' \\
| & & | \\
F(\alpha) & \xrightarrow[\phi']{\cong} & F'(\alpha') \\
| & & | \\
F & \xrightarrow[\phi]{\cong} & F'
\end{array}
$$

By the induction hypothesis, there are (at most) $[K : F(\alpha)]$-many ways to extend each ϕ' to a σ, with equality if $\frac{f(x)}{x-\alpha}$ is separable.

There are as many ways to extend ϕ to ϕ' as there are roots for $p(x)$. This number of roots is at most the degree of $p(x)$, with equality if $p(x)$ is separable.

In total, there are at most $[F(\alpha) : F] \cdot [K : F(\alpha)] = [K : F]$ extensions, with equality if $f(x)$ is separable.

Exercise: prove more generally that if K/F is a finite extension, then $|\mathrm{Aut}(K/F)| \leq [K : F]$.

Exercise: prove more generally that if K/F is a finite extension, then $|\mathrm{Aut}(K/F)| \leq [K : F]$.

Definition

A finite extension K/F is *Galois* if $|\mathrm{Aut}(K/F)| = [K : F]$. If K/F is Galois, we call $\mathrm{Aut}(K/F)$ the *Galois group* of K/F.

Exercise: prove more generally that if K/F is a finite extension, then $|\mathrm{Aut}(K/F)| \leq [K : F]$.

Definition

A finite extension K/F is *Galois* if $|\mathrm{Aut}(K/F)| = [K : F]$. If K/F is Galois, we call $\mathrm{Aut}(K/F)$ the *Galois group* of K/F.

We have just shown:

Theorem

If K is the splitting field of a separable polynomial in $F[x]$, then K/F is Galois.

Exercise: prove more generally that if K/F is a finite extension, then $|\mathrm{Aut}(K/F)| \leq [K : F]$.

Definition

A finite extension K/F is *Galois* if $|\mathrm{Aut}(K/F)| = [K : F]$. If K/F is Galois, we call $\mathrm{Aut}(K/F)$ the *Galois group* of K/F.

We have just shown:

Theorem

If K is the splitting field of a separable polynomial in $F[x]$, then K/F is Galois.

The converse is also true (to be proven later).

Exercise: prove more generally that if K/F is a finite extension, then $|\mathrm{Aut}(K/F)| \leq [K : F]$.

Definition

A finite extension K/F is *Galois* if $|\mathrm{Aut}(K/F)| = [K : F]$. If K/F is Galois, we call $\mathrm{Aut}(K/F)$ the *Galois group* of K/F.

We have just shown:

Theorem

If K is the splitting field of a separable polynomial in $F[x]$, then K/F is Galois.

The converse is also true (to be proven later).

Example: $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is Galois, but $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not Galois.

Exercise: prove more generally that if K/F is a finite extension, then $|\text{Aut}(K/F)| \leq [K : F]$.

Definition

A finite extension K/F is *Galois* if $|\text{Aut}(K/F)| = [K : F]$. If K/F is Galois, we call $\text{Aut}(K/F)$ the *Galois group* of K/F.

We have just shown:

Theorem

If K is the splitting field of a separable polynomial in $F[x]$, then K/F is Galois.

The converse is also true (to be proven later).

Example: $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is Galois, but $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not Galois.

In general, the splitting field of *any* polynomial in $\mathbb{Q}[x]$ is Galois over $\mathbb{Q}$: consider the product of its distinct irreducible factors.

Slogan: to do Galois theory, we need to have “enough roots”, so work over splitting fields!

Slogan: to do Galois theory, we need to have "enough roots", so work over splitting fields!

Definition

The *Galois group* of a polynomial $f(x) \in F[x]$ is the Galois group of a splitting field for $f(x)$ over F.

Example

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

Example

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

K is the splitting field of $(x^2 - 2)(x^2 - 3)$, so is Galois.

Example

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

K is the splitting field of $(x^2 - 2)(x^2 - 3)$, so is Galois.

What is its Galois group?

Example

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

K is the splitting field of $(x^2 - 2)(x^2 - 3)$, so is Galois.

What is its Galois group? Proceed in several steps:

1. Any automorphism is determined by what it does to $\sqrt{2}$ and $\sqrt{3}$.

Example

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

K is the splitting field of $(x^2 - 2)(x^2 - 3)$, so is Galois.

What is its Galois group? Proceed in several steps:

1. Any automorphism is determined by what it does to $\sqrt{2}$ and $\sqrt{3}$.
2. Any automorphism sends $\sqrt{2}$ to $\pm\sqrt{2}$, and $\sqrt{3}$ to $\pm\sqrt{3}$.

Example

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

K is the splitting field of $(x^2 - 2)(x^2 - 3)$, so is Galois.

What is its Galois group? Proceed in several steps:

1. Any automorphism is determined by what it does to $\sqrt{2}$ and $\sqrt{3}$.
2. Any automorphism sends $\sqrt{2}$ to $\pm\sqrt{2}$, and $\sqrt{3}$ to $\pm\sqrt{3}$.
3. Thus there are four candidates for automorphisms: the identity, the map σ sending $\sqrt{2}$ to $-\sqrt{2}$ and keeping $\sqrt{3}$ constant, the map τ sending $\sqrt{3}$ to $-\sqrt{3}$ and keeping $\sqrt{2}$ constant, and $\sigma\tau$ ($\sqrt{2} \mapsto -\sqrt{2}$; $\sqrt{3} \mapsto -\sqrt{3}$).

Example

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

K is the splitting field of $(x^2 - 2)(x^2 - 3)$, so is Galois.

What is its Galois group? Proceed in several steps:

1. Any automorphism is determined by what it does to $\sqrt{2}$ and $\sqrt{3}$.
2. Any automorphism sends $\sqrt{2}$ to $\pm\sqrt{2}$, and $\sqrt{3}$ to $\pm\sqrt{3}$.
3. Thus there are four candidates for automorphisms: the identity, the map σ sending $\sqrt{2}$ to $-\sqrt{2}$ and keeping $\sqrt{3}$ constant, the map τ sending $\sqrt{3}$ to $-\sqrt{3}$ and keeping $\sqrt{2}$ constant, and $\sigma\tau$ ($\sqrt{2} \mapsto -\sqrt{2}$; $\sqrt{3} \mapsto -\sqrt{3}$).
4. We have to see which of these possibilities really gives an automorphism. Here it is easy: $|\mathrm{Aut}(K/F)| = [K : F] = 4$, so there are four automorphisms, so all of them give automorphisms.

Example

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

K is the splitting field of $(x^2 - 2)(x^2 - 3)$, so is Galois.

What is its Galois group? Proceed in several steps:

1. Any automorphism is determined by what it does to $\sqrt{2}$ and $\sqrt{3}$.
2. Any automorphism sends $\sqrt{2}$ to $\pm\sqrt{2}$, and $\sqrt{3}$ to $\pm\sqrt{3}$.
3. Thus there are four candidates for automorphisms: the identity, the map σ sending $\sqrt{2}$ to $-\sqrt{2}$ and keeping $\sqrt{3}$ constant, the map τ sending $\sqrt{3}$ to $-\sqrt{3}$ and keeping $\sqrt{2}$ constant, and $\sigma\tau$ ($\sqrt{2} \mapsto -\sqrt{2}$; $\sqrt{3} \mapsto -\sqrt{3}$).
4. We have to see which of these possibilities really gives an automorphism. Here it is easy: $|\mathrm{Aut}(K/F)| = [K : F] = 4$, so there are four automorphisms, so all of them give automorphisms.
5. The Galois group is $\{1, \sigma, \tau, \sigma\tau\}$. All elements have order 2, so it is isomorphic to $Z_2 \times Z_2$ (the Klein 4-group).

Example continued

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

Example continued

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

For each *subgroup* of $\mathrm{Aut}(K/F)$, there corresponds a fixed field.

Example continued

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

For each *subgroup* of $\mathrm{Aut}(K/F)$, there corresponds a fixed field.

To compute it, use that $1, \sqrt{2}$, $\sqrt{3}$, $\sqrt{6} = \sqrt{2}\sqrt{3}$ is a basis for the extension.

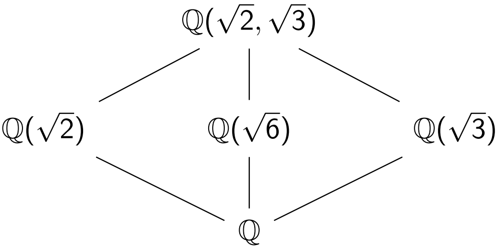
Example continued

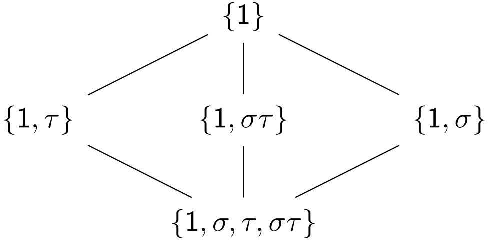
$F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

For each *subgroup* of $\mathrm{Aut}(K/F)$, there corresponds a fixed field.

To compute it, use that $1, \sqrt{2}$, $\sqrt{3}$, $\sqrt{6} = \sqrt{2}\sqrt{3}$ is a basis for the extension.

Subgroup	Fixed field
$\{1\}$	$\mathbb{Q}(\sqrt{2}, \sqrt{3})$
$\{1, \sigma\}$	$\mathbb{Q}(\sqrt{3})$
$\{1, \sigma\tau\}$	$\mathbb{Q}(\sqrt{6})$
$\{1, \tau\}$	$\mathbb{Q}(\sqrt{2})$
$\{1, \sigma, \tau, \sigma\tau\}$	$\mathbb{Q}$


$\mathbb{Q}(\sqrt{2}, \sqrt{3})$
$\mathbb{Q}(\sqrt{2})$
$\mathbb{Q}(\sqrt{6})$
$\mathbb{Q}(\sqrt{3})$
$\mathbb{Q}$


$\{1\}$
$\{1, \tau\}$
$\{1, \sigma\tau\}$
$\{1, \sigma\}$
$\{1, \sigma, \tau, \sigma\tau\}$

Another example

$F = \mathbb{Q}$, K is the splitting field of $x^3 - 2$.

Another example

$F = \mathbb{Q}$, K is the splitting field of $x^3 - 2$.

We saw the roots of $x^3 - 2$ are of the form $\sqrt[3]{2}$, $\rho\sqrt[3]{2}$, $\rho^2\sqrt[3]{2}$, where $\rho = \zeta_3 = e^{2\pi i/3}$.

Another example

$F = \mathbb{Q}$, K is the splitting field of $x^3 - 2$.

We saw the roots of $x^3 - 2$ are of the form $\sqrt[3]{2}$, $\rho\sqrt[3]{2}$, $\rho^2\sqrt[3]{2}$, where $\rho = \zeta_3 = e^{2\pi i/3}$.

The splitting field is $\mathbb{Q}(\sqrt[3]{2}, \rho)$, and has degree 6 (computed earlier).

Another example

$F = \mathbb{Q}$, K is the splitting field of $x^3 - 2$.

We saw the roots of $x^3 - 2$ are of the form $\sqrt[3]{2}$, $\rho\sqrt[3]{2}$, $\rho^2\sqrt[3]{2}$, where $\rho = \zeta_3 = e^{2\pi i/3}$.

The splitting field is $\mathbb{Q}(\sqrt[3]{2}, \rho)$, and has degree 6 (computed earlier).

Any automorphism of K/F must permute the roots of $x^3 - 2$. There are $3! = 6$ such permutations and we know $|\mathrm{Aut}(K/F)| = [K : F] = 6$. Thus any permutation of the roots induces an automorphism, and $\mathrm{Aut}(K/F) \cong S_3$.

Another example

$F = \mathbb{Q}$, K is the splitting field of $x^3 - 2$.

We saw the roots of $x^3 - 2$ are of the form $\sqrt[3]{2}$, $\rho\sqrt[3]{2}$, $\rho^2\sqrt[3]{2}$, where $\rho = \zeta_3 = e^{2\pi i/3}$.

The splitting field is $\mathbb{Q}(\sqrt[3]{2}, \rho)$, and has degree 6 (computed earlier).

Any automorphism of K/F must permute the roots of $x^3 - 2$. There are $3! = 6$ such permutations and we know $|\mathrm{Aut}(K/F)| = [K : F] = 6$. Thus any permutation of the roots induces an automorphism, and $\mathrm{Aut}(K/F) \cong S_3$.

Another way to think about it: It suffices to describe the automorphism on the generators $\sqrt[3]{2}$ and ρ.

Another example

$F = \mathbb{Q}$, K is the splitting field of $x^3 - 2$.

We saw the roots of $x^3 - 2$ are of the form $\sqrt[3]{2}$, $\rho\sqrt[3]{2}$, $\rho^2\sqrt[3]{2}$, where $\rho = \zeta_3 = e^{2\pi i/3}$.

The splitting field is $\mathbb{Q}(\sqrt[3]{2}, \rho)$, and has degree 6 (computed earlier).

Any automorphism of K/F must permute the roots of $x^3 - 2$. There are $3! = 6$ such permutations and we know $|\mathrm{Aut}(K/F)| = [K : F] = 6$. Thus any permutation of the roots induces an automorphism, and $\mathrm{Aut}(K/F) \cong S_3$.

Another way to think about it: It suffices to describe the automorphism on the generators $\sqrt[3]{2}$ and ρ.

$\sqrt[3]{2}$ can be sent to a root of $x^3 - 2$, ρ can be sent to ρ or ρ^2. All these possibilities give automorphisms by counting.

Let $\sigma : \sqrt[3]{2} \mapsto \rho\sqrt[3]{2}$, $\rho \mapsto \rho$, and $\tau : \sqrt[3]{2} \mapsto \sqrt[3]{2}$, $\rho \mapsto \rho^2$.

Let $\sigma : \sqrt[3]{2} \mapsto \rho\sqrt[3]{2}$, $\rho \mapsto \rho$, and $\tau : \sqrt[3]{2} \mapsto \sqrt[3]{2}$, $\rho \mapsto \rho^2$.

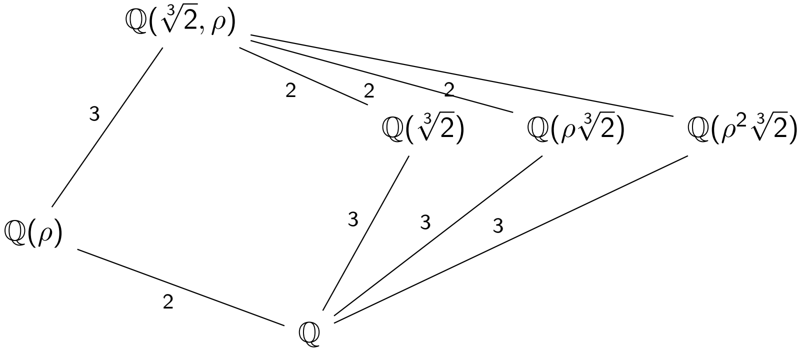
Then $\text{Aut}(K/F)$ is generated by σ and τ, and we can again show $\text{Aut}(K/F) \cong S_3$ (see the book for full computation).

Let $\sigma : \sqrt[3]{2} \mapsto \rho\sqrt[3]{2}$, $\rho \mapsto \rho$, and $\tau : \sqrt[3]{2} \mapsto \sqrt[3]{2}$, $\rho \mapsto \rho^2$.

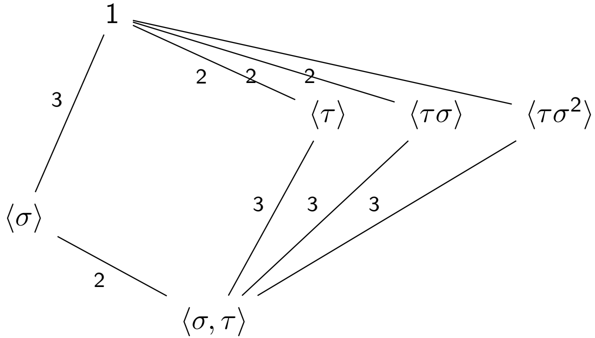
Then $\text{Aut}(K/F)$ is generated by σ and τ, and we can again show $\text{Aut}(K/F) \cong S_3$ (see the book for full computation).

We can also determine the fixed fields...

Fixed fields:



Subgroups of the Galois group:



One more example

$F = \mathbb{F}_p$, $K = \mathbb{F}_{p^n}$.

One more example

$F = \mathbb{F}_p$, $K = \mathbb{F}_{p^n}$.

We showed K was the splitting field of $x^{p^n} - x$, a separable polynomial, so K/F is Galois, and $|\mathrm{Aut}(K/F)| = [K : F] = n$.

One more example

$F = \mathbb{F}_p$, $K = \mathbb{F}_{p^n}$.

We showed K was the splitting field of $x^{p^n} - x$, a separable polynomial, so K/F is Galois, and $|\mathrm{Aut}(K/F)| = [K : F] = n$.

An example of an automorphism: the Frobenius map σ sending $a \mapsto a^p$ for all $a \in F$.

One more example

$F = \mathbb{F}_p$, $K = \mathbb{F}_{p^n}$.

We showed K was the splitting field of $x^{p^n} - x$, a separable polynomial, so K/F is Galois, and $|\mathrm{Aut}(K/F)| = [K : F] = n$.

An example of an automorphism: the Frobenius map σ sending $a \mapsto a^p$ for all $a \in F$.

In fact, for each $k \geq 1$, σ^k, the map sending a to a^{p^k} is also an automorphism.

One more example

$F = \mathbb{F}_p$, $K = \mathbb{F}_{p^n}$.

We showed K was the splitting field of $x^{p^n} - x$, a separable polynomial, so K/F is Galois, and $|\text{Aut}(K/F)| = [K : F] = n$.

An example of an automorphism: the Frobenius map σ sending $a \mapsto a^p$ for all $a \in F$.

In fact, for each $k \geq 1$, σ^k, the map sending a to a^{p^k} is also an automorphism.

What is the order of σ? Note σ^n is the identity: by construction, $a^{p^n} = a$ for all $a \in F$.

One more example

$F = \mathbb{F}_p$, $K = \mathbb{F}_{p^n}$.

We showed K was the splitting field of $x^{p^n} - x$, a separable polynomial, so K/F is Galois, and $|\mathrm{Aut}(K/F)| = [K : F] = n$.

An example of an automorphism: the Frobenius map σ sending $a \mapsto a^p$ for all $a \in F$.

In fact, for each $k \geq 1$, σ^k, the map sending a to a^{p^k} is also an automorphism.

What is the order of σ? Note σ^n is the identity: by construction, $a^{p^n} = a$ for all $a \in F$.

Also, for each $k < n$, the equation $x^{p^k} = x$ has at most p^k solutions, so σ^k is not the identity.

One more example

$F = \mathbb{F}_p$, $K = \mathbb{F}_{p^n}$.

We showed K was the splitting field of $x^{p^n} - x$, a separable polynomial, so K/F is Galois, and $|\mathrm{Aut}(K/F)| = [K : F] = n$.

An example of an automorphism: the Frobenius map σ sending $a \mapsto a^p$ for all $a \in F$.

In fact, for each $k \geq 1$, σ^k, the map sending a to a^{p^k} is also an automorphism.

What is the order of σ? Note σ^n is the identity: by construction, $a^{p^n} = a$ for all $a \in F$.

Also, for each $k < n$, the equation $x^{p^k} = x$ has at most p^k solutions, so σ^k is not the identity.

Thus σ has order n, so the Galois group of F/K is cyclic of order n, generated by the Frobenius map.

Summary

- For finite extensions, we always have that $|\mathrm{Aut}(K/F)| \leq [K : F]$.

Summary

- For finite extensions, we always have that $|\mathrm{Aut}(K/F)| \leq [K : F]$.
- A finite extension K/F is *Galois* if $[K : F] = |\mathrm{Aut}(K/F)|$.

Summary

- For finite extensions, we always have that $|\mathrm{Aut}(K/F)| \leq [K : F]$.
- A finite extension K/F is *Galois* if $[K : F] = |\mathrm{Aut}(K/F)|$.
- The splitting field of a separable polynomial gives a Galois extension.

Summary

- For finite extensions, we always have that $|\text{Aut}(K/F)| \leq [K : F]$.
- A finite extension K/F is *Galois* if $[K : F] = |\text{Aut}(K/F)|$.
- The splitting field of a separable polynomial gives a Galois extension.
- Over $\mathbb{Q}$, the splitting field of any polynomial gives a Galois extension.

Summary

- For finite extensions, we always have that $|\mathrm{Aut}(K/F)| \leq [K : F]$.
- A finite extension K/F is *Galois* if $[K : F] = |\mathrm{Aut}(K/F)|$.
- The splitting field of a separable polynomial gives a Galois extension.
- Over $\mathbb{Q}$, the splitting field of any polynomial gives a Galois extension.
- For each subgroup of the Galois group, there is a corresponding fixed field.

Summary

- For finite extensions, we always have that $|\mathrm{Aut}(K/F)| \leq [K : F]$.
- A finite extension K/F is *Galois* if $[K : F] = |\mathrm{Aut}(K/F)|$.
- The splitting field of a separable polynomial gives a Galois extension.
- Over $\mathbb{Q}$, the splitting field of any polynomial gives a Galois extension.
- For each subgroup of the Galois group, there is a corresponding fixed field.
- From now on, to make our work easier, we will adopt the convention that $(a + b)^n = a^n + b^n$, in any field of any characteristic.

Summary

- For finite extensions, we always have that $|\mathrm{Aut}(K/F)| \leq [K : F]$.
- A finite extension K/F is *Galois* if $[K : F] = |\mathrm{Aut}(K/F)|$.
- The splitting field of a separable polynomial gives a Galois extension.
- Over $\mathbb{Q}$, the splitting field of any polynomial gives a Galois extension.
- For each subgroup of the Galois group, there is a corresponding fixed field.
- From now on, to make our work easier, we will adopt the convention that $(a + b)^n = a^n + b^n$, in any field of any characteristic.
- *[That last one is an April's fool]*.