Math-123: The fundamental theorem of Galois theory

Sebastien Vasey

Harvard University

April 3, 2020

Reminders

Let K/F be a field extension.

- The group of automorphisms of K fixing F is written $\mathrm{Aut}(K/F)$.

Reminders

Let K/F be a field extension.

- The group of automorphisms of K fixing F is written $\mathrm{Aut}(K/F)$.
- K/F is *Galois* if $|\mathrm{Aut}(K/F)| = [K : F]$. In this case, we call $\mathrm{Aut}(K/F)$ the *Galois group* of K over F.

Reminders

Let K/F be a field extension.

- The group of automorphisms of K fixing F is written $\mathrm{Aut}(K/F)$.
- K/F is *Galois* if $|\mathrm{Aut}(K/F)| = [K : F]$. In this case, we call $\mathrm{Aut}(K/F)$ the *Galois group* of K over F.
- Splitting fields of separable polynomials are Galois.

Reminders

Let K/F be a field extension.

- The group of automorphisms of K fixing F is written $\text{Aut}(K/F)$.
- K/F is *Galois* if $|\text{Aut}(K/F)| = [K : F]$. In this case, we call $\text{Aut}(K/F)$ the *Galois group* of K over F.
- Splitting fields of separable polynomials are Galois.
- Each subgroup H of $\text{Aut}(K/F)$ has a *fixed field*: the set of all elements of K fixed by H.

Example

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

Example

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

$\mathrm{Aut}(K/F) = \{1, \sigma, \tau, \sigma\tau\}$, where σ sends $\sqrt{2}$ to $-\sqrt{2}$ and fixes $\sqrt{3}$, τ sends $\sqrt{3}$ to $-\sqrt{3}$ and fixes $\sqrt{2}$. $\mathrm{Aut}(K/F) \cong Z_2 \times Z_2$

Example

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

$\text{Aut}(K/F) = \{1, \sigma, \tau, \sigma\tau\}$, where σ sends $\sqrt{2}$ to $-\sqrt{2}$ and fixes $\sqrt{3}$, τ sends $\sqrt{3}$ to $-\sqrt{3}$ and fixes $\sqrt{2}$. $\text{Aut}(K/F) \cong Z_2 \times Z_2$

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

Example

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

$\text{Aut}(K/F) = \{1, \sigma, \tau, \sigma\tau\}$, where σ sends $\sqrt{2}$ to $-\sqrt{2}$ and fixes $\sqrt{3}$, τ sends $\sqrt{3}$ to $-\sqrt{3}$ and fixes $\sqrt{2}$. $\text{Aut}(K/F) \cong Z_2 \times Z_2$

For each *subgroup* of $\text{Aut}(K/F)$, 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

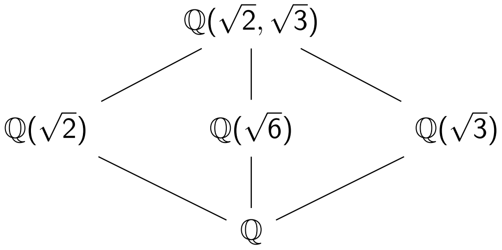
$F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

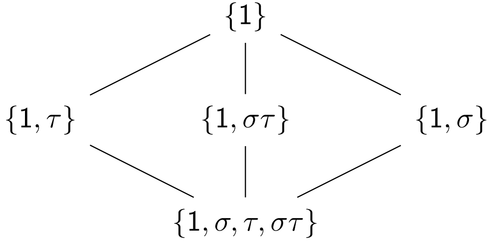
$\text{Aut}(K/F) = \{1, \sigma, \tau, \sigma\tau\}$, where σ sends $\sqrt{2}$ to $-\sqrt{2}$ and fixes $\sqrt{3}$, τ sends $\sqrt{3}$ to $-\sqrt{3}$ and fixes $\sqrt{2}$. $\text{Aut}(K/F) \cong Z_2 \times Z_2$

For each *subgroup* of $\text{Aut}(K/F)$, 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 computed earlier that $K = \mathbb{Q}(\sqrt[3]{2}, \rho)$, where $\rho = e^{2\pi i/3}$, and $K/\mathbb{Q}$ has degree 6.

Another example

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

We computed earlier that $K = \mathbb{Q}(\sqrt[3]{2}, \rho)$, where $\rho = e^{2\pi i/3}$, and $K/\mathbb{Q}$ has degree 6.

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

Another example

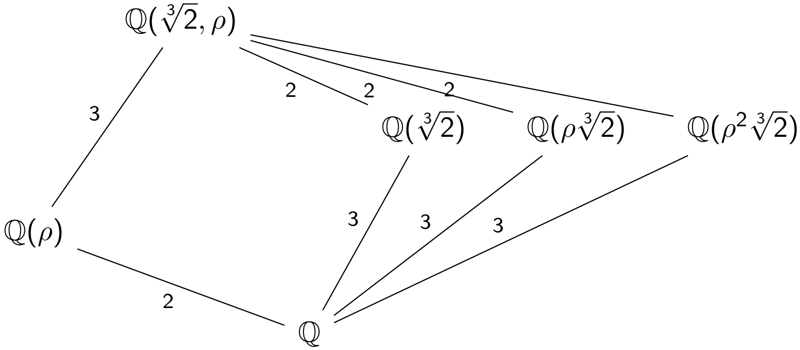
$F = \mathbb{Q}$, K is the splitting field of $x^3 - 2$.

We computed earlier that $K = \mathbb{Q}(\sqrt[3]{2}, \rho)$, where $\rho = e^{2\pi i/3}$, and $K/\mathbb{Q}$ has degree 6.

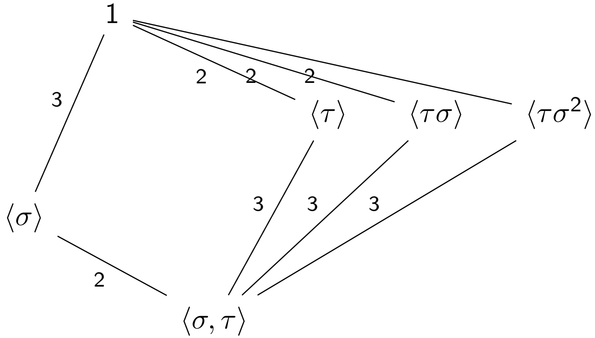
Let $\sigma : \sqrt[3]{2} \mapsto \rho\sqrt[3]{2}$, $\rho \mapsto \rho$, and $\tau : \sqrt[3]{2} \mapsto \sqrt[3]{2}$, $\rho \mapsto \rho^2$.

Then $\mathrm{Aut}(K/F)$ is generated by σ and τ, and we can show $\mathrm{Aut}(K/F) \cong S_3$.

Known subfields:



Subgroups of the Galois group:



Theorem (Fundamental theorem of Galois theory)

If K/F is a Galois extension, there is a bijective correspondence between subgroups of $\mathrm{Aut}(K/F)$ and intermediate fields L with $F \subseteq L \subseteq K$. The correspondence is given by taking fixed fields.

Theorem (Fundamental theorem of Galois theory)

If K/F is a Galois extension, there is a bijective correspondence between subgroups of $\mathrm{Aut}(K/F)$ and intermediate fields L with $F \subseteq L \subseteq K$. The correspondence is given by taking fixed fields.

The fundamental theorem actually gives a lot more information. Today's goal is to prove it.

Theorem (Fundamental theorem of Galois theory)

If K/F is a Galois extension, there is a bijective correspondence between subgroups of $\mathrm{Aut}(K/F)$ and intermediate fields L with $F \subseteq L \subseteq K$. The correspondence is given by taking fixed fields.

The fundamental theorem actually gives a lot more information. Today's goal is to prove it.

The proof will use linear algebra!

Characters

Definition

A *character* of a group G with values in a field L is a homomorphism $\chi : G \to L^\times$.

Characters

Definition

A *character* of a group G with values in a field L is a homomorphism $\chi : G \to L^\times$.

Note: any automorphism of a field K yields a character of $K^\times$ with values in K.

Characters

Definition

A *character* of a group G with values in a field L is a homomorphism $\chi : G \to L^\times$.

Note: any automorphism of a field K yields a character of $K^\times$ with values in K.

Theorem (Linear independence of characters)

If $\chi_1, \chi_2, \ldots, \chi_n$ are distinct character of G with values in L, then they are L-linearly independent: $a_1\chi_1 + \ldots + a_n\chi_n = 0$ implies $a_1 = a_2 = \ldots = a_n = 0$.

Theorem (Linear independence of characters)

If $\chi_1, \chi_2, \ldots, \chi_n$ are distinct character of G with values in L, then they are linearly independent: $a_1\chi_1 + \ldots + a_n\chi_n = 0$ implies $a_1 = a_2 = \ldots = a_n = 0$.

Proof: Suppose for a contradiction $\chi_1, \ldots, \chi_n$ are linearly dependent. Choose n least where this happens. Pick $a_1, a_2, \ldots, a_n$ not all zero such that:

$$a_1\chi_1 + \ldots + a_n\chi_n = 0$$

Theorem (Linear independence of characters)

If $\chi_1, \chi_2, \ldots, \chi_n$ are distinct character of G with values in L, then they are linearly independent: $a_1\chi_1 + \ldots + a_n\chi_n = 0$ implies $a_1 = a_2 = \ldots = a_n = 0$.

Proof: Suppose for a contradiction $\chi_1, \ldots, \chi_n$ are linearly dependent. Choose n least where this happens. Pick $a_1, a_2, \ldots, a_n$ not all zero such that:

$$a_1\chi_1 + \ldots + a_n\chi_n = 0$$

Pick $g_0 \in G$ such that $\chi_1(g_0) \neq \chi_n(g_0)$. For any $g \in G$:

Theorem (Linear independence of characters)

If $\chi_1, \chi_2, \ldots, \chi_n$ are distinct character of G with values in L, then they are linearly independent: $a_1\chi_1 + \ldots + a_n\chi_n = 0$ implies $a_1 = a_2 = \ldots = a_n = 0$.

Proof: Suppose for a contradiction $\chi_1, \ldots, \chi_n$ are linearly dependent. Choose n least where this happens. Pick $a_1, a_2, \ldots, a_n$ not all zero such that:

$$a_1\chi_1 + \ldots + a_n\chi_n = 0$$

Pick $g_0 \in G$ such that $\chi_1(g_0) \neq \chi_n(g_0)$. For any $g \in G$:

$$a_1\chi_1(g_0g) + a_2\chi_2(g_0g) + \ldots + a_n\chi_n(g_0g) = 0$$

For any $g \in G$,

$$a_1\chi_1(g_0)\chi_1(g) + a_2\chi_2(g_0)\chi_2(g) + \ldots + a_n\chi_n(g_0)\chi_n(g) = 0$$

For any $g \in G$,

$$a_1\chi_1(g_0)\chi_1(g) + a_2\chi_2(g_0)\chi_2(g) + \ldots + a_n\chi_n(g_0)\chi_n(g) = 0$$

Also (multiplying $a_1\chi_1 + a_2\chi_2 + \ldots + a_n\chi_n = 0$ by $\chi_n(g_0)$ and plugging in g):

$$a_1\chi_n(g_0)\chi_1(g) + a_2\chi_n(g_0)\chi_2(g) + \ldots + a_n\chi_n(g_0)\chi_n(g) = 0$$

For any $g \in G$,

$$a_1\chi_1(g_0)\chi_1(g) + a_2\chi_2(g_0)\chi_2(g) + \ldots + a_n\chi_n(g_0)\chi_n(g) = 0$$

Also (multiplying $a_1\chi_1 + a_2\chi_2 + \ldots + a_n\chi_n = 0$ by $\chi_n(g_0)$ and plugging in g):

$$a_1\chi_n(g_0)\chi_1(g) + a_2\chi_n(g_0)\chi_2(g) + \ldots + a_n\chi_n(g_0)\chi_n(g) = 0$$

Subtracting the two, we get:

$$a_1(\chi_1(g_0)-\chi_n(g_0))\chi_1(g)+\ldots+a_{n-1}(\chi_{n-1}(g_0)-\chi_n(g_0))\chi_{n-1}(g) = 0$$

For any $g \in G$,

$$a_1\chi_1(g_0)\chi_1(g) + a_2\chi_2(g_0)\chi_2(g) + \ldots + a_n\chi_n(g_0)\chi_n(g) = 0$$

Also (multiplying $a_1\chi_1 + a_2\chi_2 + \ldots + a_n\chi_n = 0$ by $\chi_n(g_0)$ and plugging in g):

$$a_1\chi_n(g_0)\chi_1(g) + a_2\chi_n(g_0)\chi_2(g) + \ldots + a_n\chi_n(g_0)\chi_n(g) = 0$$

Subtracting the two, we get:

$$a_1(\chi_1(g_0)-\chi_n(g_0))\chi_1(g)+\ldots+a_{n-1}(\chi_{n-1}(g_0)-\chi_n(g_0))\chi_{n-1}(g) = 0$$

Since $\chi_1(g_0) \neq \chi_n(g_0)$, this gives a nontrivial relation between $\chi_1, \ldots, \chi_{n-1}$, contradicting minimality of n.

We will use linear independence of distinct characters to prove:

Theorem (Key theorem)

If K is a field and G is a finite subgroup of $\mathrm{Aut}(K)$ with fixed field F, then $|G| = [K : F]$.

We will use linear independence of distinct characters to prove:

Theorem (Key theorem)

If K is a field and G is a finite subgroup of $\mathrm{Aut}(K)$ with fixed field F, then $|G| = [K : F]$.

Note: before, we started with a certain kind of field F and saw that $|\mathrm{Aut}(K/F)| = [K : F]$. Here, we start with the group, and deduce the same equation for its fixed field F.

Lemma

Let G be a finite subgroup of $\mathrm{Aut}(K)$. Let F be the fixed field. Then $|G| \leq [K : F]$.

Lemma

Let G be a finite subgroup of $\text{Aut}(K)$. Let F be the fixed field. Then $|G| \leq [K : F]$.

Proof: Suppose for a contradiction that $n = |G| > [K : F] = m$. Write $G = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$. Let $\omega_1, \omega_2, \ldots, \omega_m$ be a basis for K over F. Let's study how G acts on the basis.

Lemma

Let G be a finite subgroup of $\mathrm{Aut}(K)$. Let F be the fixed field. Then $|G| \leq [K : F]$.

Proof: Suppose for a contradiction that $n = |G| > [K : F] = m$. Write $G = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$. Let $\omega_1, \omega_2, \ldots, \omega_m$ be a basis for K over F. Let's study how G acts on the basis. Consider the system of equation:

$$\begin{aligned} \sigma_1(\omega_1)x_1 + \sigma_2(\omega_1)x_2 + \ldots + \sigma_n(\omega_1)x_n &= 0 \\ \ldots \\ \sigma_1(\omega_m)x_1 + \sigma_2(\omega_m)x_2 + \ldots + \sigma_n(\omega_m)x_n &= 0 \end{aligned}$$

Since $n > m$, there is a nonzero solution, $\beta_1, \ldots, \beta_n \in K$.

Lemma

Let G be a finite subgroup of $\text{Aut}(K)$. Let F be the fixed field. Then $|G| \leq [K : F]$.

Proof: Suppose for a contradiction that $n = |G| > [K : F] = m$. Write $G = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$. Let $\omega_1, \omega_2, \ldots, \omega_m$ be a basis for K over F. Let's study how G acts on the basis. Consider the system of equation:

$$\begin{aligned} \sigma_1(\omega_1)x_1 + \sigma_2(\omega_1)x_2 + \ldots + \sigma_n(\omega_1)x_n &= 0 \\ \ldots \\ \sigma_1(\omega_m)x_1 + \sigma_2(\omega_m)x_2 + \ldots + \sigma_n(\omega_m)x_n &= 0 \end{aligned}$$

Since $n > m$, there is a nonzero solution, $\beta_1, \ldots, \beta_n \in K$.

Consider any $\alpha \in K$. Write $\alpha = a_1\omega_1 + \ldots + a_m\omega_m$, $a_i \in F$. Note $\sigma_i(a_k\omega_j) = a_k\sigma_i(\omega_j)$ (F is the fixed field).

$\alpha = a_1\omega_1 + \ldots + a_m\omega_m$

$$\begin{aligned}
\sigma_1(\omega_1)\beta_1 + \sigma_2(\omega_1)\beta_2 + \ldots + \sigma_n(\omega_1)\beta_n &= 0 \\
&\cdots \\
\sigma_1(\omega_m)\beta_1 + \sigma_2(\omega_m)\beta_2 + \ldots + \sigma_n(\omega_m)\beta_n &= 0
\end{aligned}$$

$\alpha = a_1\omega_1 + \ldots + a_m\omega_m$

$$\begin{aligned}\sigma_1(\omega_1)\beta_1 + \sigma_2(\omega_1)\beta_2 + \ldots + \sigma_n(\omega_1)\beta_n &= 0\\ &\cdots\\ \sigma_1(\omega_m)\beta_1 + \sigma_2(\omega_m)\beta_2 + \ldots + \sigma_n(\omega_m)\beta_n &= 0\end{aligned}$$

Multiply the ith equation by a_i, and sum them up:

$$\sigma_1(a_1\omega_1 + a_2\omega_2 + \ldots + a_m\omega_m)\beta_1 + \sigma_2(\ldots)\beta_2 + \ldots + \sigma_n(\ldots)\beta_n = 0$$

$\alpha = a_1\omega_1 + \ldots + a_m\omega_m$

$$\begin{aligned} \sigma_1(\omega_1)\beta_1 + \sigma_2(\omega_1)\beta_2 + \ldots + \sigma_n(\omega_1)\beta_n &= 0 \\ &\ldots \\ \sigma_1(\omega_m)\beta_1 + \sigma_2(\omega_m)\beta_2 + \ldots + \sigma_n(\omega_m)\beta_n &= 0 \end{aligned}$$

Multiply the ith equation by a_i, and sum them up:

$$\sigma_1(a_1\omega_1 + a_2\omega_2 + \ldots + a_m\omega_m)\beta_1 + \sigma_2(\ldots)\beta_2 + \ldots + \sigma_n(\ldots)\beta_n = 0$$

We get that $\sigma_1(\alpha)\beta_1 + \ldots + \sigma_n(\alpha)\beta_n = 0$.

$\alpha = a_1\omega_1 + \ldots + a_m\omega_m$

$$\sigma_1(\omega_1)\beta_1 + \sigma_2(\omega_1)\beta_2 + \ldots + \sigma_n(\omega_1)\beta_n = 0$$
$$\ldots$$
$$\sigma_1(\omega_m)\beta_1 + \sigma_2(\omega_m)\beta_2 + \ldots + \sigma_n(\omega_m)\beta_n = 0$$

Multiply the ith equation by a_i, and sum them up:

$\sigma_1(a_1\omega_1 + a_2\omega_2 + \ldots + a_m\omega_m)\beta_1 + \sigma_2(\ldots)\beta_2 + \ldots + \sigma_n(\ldots)\beta_n = 0$

We get that $\sigma_1(\alpha)\beta_1 + \ldots + \sigma_n(\alpha)\beta_n = 0$.

α was an arbitrary element of K, so $\sigma_1\beta_1 + \ldots + \sigma_n\beta_n = 0$. This contradicts linear independence of characters.

Lemma

Let $G = \{\sigma_1 = 1, \sigma_2, \ldots, \sigma_n\}$ be a subgroup of $\mathrm{Aut}(K)$ with fixed field F. Then $|G| \geq [K : F]$.

Lemma

Let $G = \{\sigma_1 = 1, \sigma_2, \ldots, \sigma_n\}$ be a subgroup of $\mathrm{Aut}(K)$ with fixed field F. Then $|G| \geq [K : F]$.

Proof: Suppose for a contradiction $n = |G| < [K : F]$. Let $\alpha_1, \ldots, \alpha_{n+1}$ be F-linearly independent in K. Look at the system:

Lemma

Let $G = \{\sigma_1 = 1, \sigma_2, \ldots, \sigma_n\}$ be a subgroup of $\mathrm{Aut}(K)$ with fixed field F. Then $|G| \geq [K : F]$.

Proof: Suppose for a contradiction $n = |G| < [K : F]$. Let $\alpha_1, \ldots, \alpha_{n+1}$ be F-linearly independent in K. Look at the system:

$$\begin{aligned} \sigma_1(\alpha_1)x_1 + \sigma_1(\alpha_2)x_2 + \ldots + \sigma_1(\alpha_{n+1})x_{n+1} &= 0 \\ \ldots \\ \sigma_n(\alpha_1)x_1 + \sigma_n(\alpha_2)x_2 + \ldots + \sigma_n(\alpha_{n+1})x_{n+1} &= 0 \end{aligned}$$

Lemma

Let $G = \{\sigma_1 = 1, \sigma_2, \ldots, \sigma_n\}$ be a subgroup of $\mathrm{Aut}(K)$ with fixed field F. Then $|G| \geq [K : F]$.

Proof: Suppose for a contradiction $n = |G| < [K : F]$. Let $\alpha_1, \ldots, \alpha_{n+1}$ be F-linearly independent in K. Look at the system:

$$\begin{aligned} \sigma_1(\alpha_1)x_1 + \sigma_1(\alpha_2)x_2 + \ldots + \sigma_1(\alpha_{n+1})x_{n+1} &= 0 \\ \ldots \\ \sigma_n(\alpha_1)x_1 + \sigma_n(\alpha_2)x_2 + \ldots + \sigma_n(\alpha_{n+1})x_{n+1} &= 0 \end{aligned}$$

This has a solution $\beta_1, \ldots, \beta_{n+1} \in K$ with not all β_i's zero. Choose the one with the minimal number of nonzeroes.

Lemma

Let $G = \{\sigma_1 = 1, \sigma_2, \ldots, \sigma_n\}$ be a subgroup of $\mathrm{Aut}(K)$ with fixed field F. Then $|G| \geq [K : F]$.

Proof: Suppose for a contradiction $n = |G| < [K : F]$. Let $\alpha_1, \ldots, \alpha_{n+1}$ be F-linearly independent in K. Look at the system:

$$\begin{aligned} \sigma_1(\alpha_1)x_1 + \sigma_1(\alpha_2)x_2 + \ldots + \sigma_1(\alpha_{n+1})x_{n+1} &= 0 \\ \ldots \\ \sigma_n(\alpha_1)x_1 + \sigma_n(\alpha_2)x_2 + \ldots + \sigma_n(\alpha_{n+1})x_{n+1} &= 0 \end{aligned}$$

This has a solution $\beta_1, \ldots, \beta_{n+1} \in K$ with not all β_i's zero. Choose the one with the minimal number of nonzeroes. Renumbering, without loss of generality $\beta_{n+1} \neq 0$. Dividing everything by β_{n+1}, without loss of generality $1 = \beta_{n+1} \in F$. We will show that all the β_i's are in F. This is a contradiction: σ_1 is the identity and $\alpha_1, \ldots, \alpha_{n+1}$ are supposed to be F-linearly independent.

We have the equations $\sigma_i(\alpha_1)\beta_1 + \ldots + \sigma_i(\alpha_{n+1})\beta_{n+1} = 0$ for each i, and we know $0 \neq \beta_{n+1} \in F$.

We have the equations $\sigma_i(\alpha_1)\beta_1 + \ldots + \sigma_i(\alpha_{n+1})\beta_{n+1} = 0$ for each i, and we know $0 \neq \beta_{n+1} \in F$.

If $\beta_j \notin F$ for some j, then assume for simplicity $j = 1$ and by definition of the fixed field there is an automorphism $\sigma_{k_0} \in G$ such that $\sigma_{k_0}(\beta_1) \neq \beta_1$.

We have the equations $\sigma_i(\alpha_1)\beta_1 + \ldots + \sigma_i(\alpha_{n+1})\beta_{n+1} = 0$ for each i, and we know $0 \neq \beta_{n+1} \in F$.

If $\beta_j \notin F$ for some j, then assume for simplicity $j = 1$ and by definition of the fixed field there is an automorphism $\sigma_{k_0} \in G$ such that $\sigma_{k_0}(\beta_1) \neq \beta_1$.

Applying σ_{k_0} to the above, we get that $\sigma_{k_0}\sigma_i(\alpha_1)\sigma_{k_0}(\beta_1) + \ldots + \sigma_{k_0}\sigma_i(\alpha_{n+1})\sigma_{k_0}(\beta_{n+1}) = 0$.

We have the equations $\sigma_i(\alpha_1)\beta_1 + \ldots + \sigma_i(\alpha_{n+1})\beta_{n+1} = 0$ for each i, and we know $0 \neq \beta_{n+1} \in F$.

If $\beta_j \notin F$ for some j, then assume for simplicity $j = 1$ and by definition of the fixed field there is an automorphism $\sigma_{k_0} \in G$ such that $\sigma_{k_0}(\beta_1) \neq \beta_1$.

Applying σ_{k_0} to the above, we get that
$\sigma_{k_0}\sigma_i(\alpha_1)\sigma_{k_0}(\beta_1) + \ldots + \sigma_{k_0}\sigma_i(\alpha_{n+1})\sigma_{k_0}(\beta_{n+1}) = 0$.

Note that $\sigma_{k_0}(\beta_{n+1}) = \beta_{n+1}$.

We have the equations $\sigma_i(\alpha_1)\beta_1 + \ldots + \sigma_i(\alpha_{n+1})\beta_{n+1} = 0$ for each i, and we know $0 \neq \beta_{n+1} \in F$.

If $\beta_j \notin F$ for some j, then assume for simplicity $j = 1$ and by definition of the fixed field there is an automorphism $\sigma_{k_0} \in G$ such that $\sigma_{k_0}(\beta_1) \neq \beta_1$.

Applying σ_{k_0} to the above, we get that $\sigma_{k_0}\sigma_i(\alpha_1)\sigma_{k_0}(\beta_1) + \ldots + \sigma_{k_0}\sigma_i(\alpha_{n+1})\sigma_{k_0}(\beta_{n+1}) = 0$.

Note that $\sigma_{k_0}(\beta_{n+1}) = \beta_{n+1}$.

Also note $\sigma_{k_0}\sigma_1, \sigma_{k_0}\sigma_2, \ldots, \sigma_{k_0}\sigma_n$ is just a permutation of $\sigma_1, \ldots, \sigma_n$. So rearranging the equations, we can assume without loss that $\sigma_i(\alpha_1)\sigma_{k_0}(\beta_1) + \ldots + \sigma_i(\alpha_{n+1})\beta_{n+1} = 0$.

We have the equations $\sigma_i(\alpha_1)\beta_1 + \ldots + \sigma_i(\alpha_{n+1})\beta_{n+1} = 0$ for each i, and we know $0 \neq \beta_{n+1} \in F$.

If $\beta_j \notin F$ for some j, then assume for simplicity $j = 1$ and by definition of the fixed field there is an automorphism $\sigma_{k_0} \in G$ such that $\sigma_{k_0}(\beta_1) \neq \beta_1$.

Applying σ_{k_0} to the above, we get that $\sigma_{k_0}\sigma_i(\alpha_1)\sigma_{k_0}(\beta_1) + \ldots + \sigma_{k_0}\sigma_i(\alpha_{n+1})\sigma_{k_0}(\beta_{n+1}) = 0$.

Note that $\sigma_{k_0}(\beta_{n+1}) = \beta_{n+1}$.

Also note $\sigma_{k_0}\sigma_1, \sigma_{k_0}\sigma_2, \ldots, \sigma_{k_0}\sigma_n$ is just a permutation of $\sigma_1, \ldots, \sigma_n$. So rearranging the equations, we can assume without loss that $\sigma_i(\alpha_1)\sigma_{k_0}(\beta_1) + \ldots + \sigma_i(\alpha_{n+1})\beta_{n+1} = 0$.

Subtract this from the equation in the first paragraph: $(\beta_1 - \sigma_{k_0}(\beta_1))\sigma_i(\alpha_1) + \ldots + (\beta_n - \sigma_{k_0}(\beta_n))\sigma_i(\alpha_n) = 0$.

We have the equations $\sigma_i(\alpha_1)\beta_1 + \ldots + \sigma_i(\alpha_{n+1})\beta_{n+1} = 0$ for each i, and we know $0 \neq \beta_{n+1} \in F$.

If $\beta_j \notin F$ for some j, then assume for simplicity $j = 1$ and by definition of the fixed field there is an automorphism $\sigma_{k_0} \in G$ such that $\sigma_{k_0}(\beta_1) \neq \beta_1$.

Applying σ_{k_0} to the above, we get that $\sigma_{k_0}\sigma_i(\alpha_1)\sigma_{k_0}(\beta_1) + \ldots + \sigma_{k_0}\sigma_i(\alpha_{n+1})\sigma_{k_0}(\beta_{n+1}) = 0$.

Note that $\sigma_{k_0}(\beta_{n+1}) = \beta_{n+1}$.

Also note $\sigma_{k_0}\sigma_1, \sigma_{k_0}\sigma_2, \ldots, \sigma_{k_0}\sigma_n$ is just a permutation of $\sigma_1, \ldots, \sigma_n$. So rearranging the equations, we can assume without loss that $\sigma_i(\alpha_1)\sigma_{k_0}(\beta_1) + \ldots + \sigma_i(\alpha_{n+1})\beta_{n+1} = 0$.

Subtract this from the equation in the first paragraph: $(\beta_1 - \sigma_{k_0}(\beta_1))\sigma_i(\alpha_1) + \ldots + (\beta_n - \sigma_{k_0}(\beta_n))\sigma_i(\alpha_n) = 0$.

Thus $\beta_1 - \sigma_{k_0}(\beta_1), \ldots, \beta_n - \sigma_{k_0}(\beta_n), 0$ is a solution with fewer zeroes than before, contradiction.

Theorem (Key theorem)

If G is a finite subgroup of $\mathrm{Aut}(K)$ with fixed field F, then $|G| = [F : K]$.

Theorem (Key theorem)

If G is a finite subgroup of $\mathrm{Aut}(K)$ with fixed field F, then $|G| = [F : K]$.

Corollary

If K/F is any finite extension, then $|\mathrm{Aut}(K/F)| \leq [K : F]$ with equality if and only if F is the fixed field of $\mathrm{Aut}(K/F)$. Thus K/F is Galois if and only if F is the fixed field of $\mathrm{Aut}(K/F)$.

Theorem (Key theorem)

If G is a finite subgroup of $\mathrm{Aut}(K)$ with fixed field F, then $|G| = [F : K]$.

Corollary

If K/F is any finite extension, then $|\mathrm{Aut}(K/F)| \leq [K : F]$ with equality if and only if F is the fixed field of $\mathrm{Aut}(K/F)$. Thus K/F is Galois if and only if F is the fixed field of $\mathrm{Aut}(K/F)$.

Proof.

Let F_1 be the fixed field of $G = \mathrm{Aut}(K/F)$. Of course, $F \subseteq F_1 \subseteq K$.

Theorem (Key theorem)

If G is a finite subgroup of $\text{Aut}(K)$ with fixed field F, then $|G| = [F : K]$.

Corollary

If K/F is any finite extension, then $|\text{Aut}(K/F)| \leq [K : F]$ with equality if and only if F is the fixed field of $\text{Aut}(K/F)$. Thus K/F is Galois if and only if F is the fixed field of $\text{Aut}(K/F)$.

Proof.

Let F_1 be the fixed field of $G = \text{Aut}(K/F)$. Of course, $F \subseteq F_1 \subseteq K$.

By the key theorem, $[K : F_1] = |\text{Aut}(K/F)|$. Thus $[K : F] = [K : F_1][F_1 : F] = |\text{Aut}(K/F)|[F_1 : F]$.

Theorem (Key theorem)

If G is a finite subgroup of $\mathrm{Aut}(K)$ with fixed field F, then $|G| = [F : K]$.

Corollary

If K/F is any finite extension, then $|\mathrm{Aut}(K/F)| \leq [K : F]$ with equality if and only if F is the fixed field of $\mathrm{Aut}(K/F)$. Thus K/F is Galois if and only if F is the fixed field of $\mathrm{Aut}(K/F)$.

Proof.

Let F_1 be the fixed field of $G = \mathrm{Aut}(K/F)$. Of course, $F \subseteq F_1 \subseteq K$.

By the key theorem, $[K : F_1] = |\mathrm{Aut}(K/F)|$. Thus $[K : F] = [K : F_1][F_1 : F] = |\mathrm{Aut}(K/F)|[F_1 : F]$.

Thus $[K : F] \geq |\mathrm{Aut}(K/F)|$ with equality if and only if $F_1 = F$. □

Lemma

If K/F is a Galois extension, then every irreducible $p(x) \in F[x]$ which has a root in K is separable and splits completely in K.

Lemma

If K/F is a Galois extension, then every irreducible $p(x) \in F[x]$ which has a root in K is separable and splits completely in K.

Proof.

Let $G = \text{Aut}(K/F) = \{\sigma_1 = 1, \sigma_2, \ldots, \sigma_n\}$. Let $\alpha \in K$ be a root of $p(x)$. Consider $\alpha, \sigma_2(\alpha), \sigma_3(\alpha), \ldots, \sigma_n(\alpha)$.

Lemma

If K/F is a Galois extension, then every irreducible $p(x) \in F[x]$ which has a root in K is separable and splits completely in K.

Proof.

Let $G = \text{Aut}(K/F) = \{\sigma_1 = 1, \sigma_2, \ldots, \sigma_n\}$. Let $\alpha \in K$ be a root of $p(x)$. Consider $\alpha, \sigma_2(\alpha), \sigma_3(\alpha), \ldots, \sigma_n(\alpha)$.

Say r of them are distinct, $\alpha = \alpha_1, \ldots, \alpha_r$. Any member of G permutes the α_i's.

Lemma

If K/F is a Galois extension, then every irreducible $p(x) \in F[x]$ which has a root in K is separable and splits completely in K.

Proof.

Let $G = \mathrm{Aut}(K/F) = \{\sigma_1 = 1, \sigma_2, \ldots, \sigma_n\}$. Let $\alpha \in K$ be a root of $p(x)$. Consider $\alpha, \sigma_2(\alpha), \sigma_3(\alpha), \ldots, \sigma_n(\alpha)$.

Say r of them are distinct, $\alpha = \alpha_1, \ldots, \alpha_r$. Any member of G permutes the α_i's.

Consider $f(x) = (x - \alpha)(x - \alpha_2)\ldots(x - \alpha_r)$. Where are its coefficients?

Lemma

If K/F is a Galois extension, then every irreducible $p(x) \in F[x]$ which has a root in K is separable and splits completely in K.

Proof.

Let $G = \mathrm{Aut}(K/F) = \{\sigma_1 = 1, \sigma_2, \ldots, \sigma_n\}$. Let $\alpha \in K$ be a root of $p(x)$. Consider $\alpha, \sigma_2(\alpha), \sigma_3(\alpha), \ldots, \sigma_n(\alpha)$.

Say r of them are distinct, $\alpha = \alpha_1, \ldots, \alpha_r$. Any member of G permutes the α_i's.

Consider $f(x) = (x - \alpha)(x - \alpha_2) \ldots (x - \alpha_r)$. Where are its coefficients?

They are fixed by the members of G, so lie in the fixed field of G, which is F because K/F is Galois. Thus $f(x) \in F[x]$.

Lemma

If K/F is a Galois extension, then every irreducible $p(x) \in F[x]$ which has a root in K is separable and splits completely in K.

Proof.

Let $G = \mathrm{Aut}(K/F) = \{\sigma_1 = 1, \sigma_2, \ldots, \sigma_n\}$. Let $\alpha \in K$ be a root of $p(x)$. Consider $\alpha, \sigma_2(\alpha), \sigma_3(\alpha), \ldots, \sigma_n(\alpha)$.

Say r of them are distinct, $\alpha = \alpha_1, \ldots, \alpha_r$. Any member of G permutes the α_i's.

Consider $f(x) = (x - \alpha)(x - \alpha_2) \ldots (x - \alpha_r)$. Where are its coefficients?

They are fixed by the members of G, so lie in the fixed field of G, which is F because K/F is Galois. Thus $f(x) \in F[x]$.

Moreover, $p(x)$ divides $f(x)$ (it is the minimal polynomial), and $f(x)$ divides $p(x)$ because it has fewer roots. Thus $f(x)$ and $p(x)$ are the same up to a unit, and the result follows. □

Lemma

If K/F is a Galois extension, then every irreducible $p(x) \in F[x]$ which has a root in K is separable and splits completely in K.

Corollary

An extension K/F is Galois if and only if it is the splitting field of a separable polynomial over F.

Lemma

If K/F is a Galois extension, then every irreducible $p(x) \in F[x]$ which has a root in K is separable and splits completely in K.

Corollary

An extension K/F is Galois if and only if it is the splitting field of a separable polynomial over F.

Proof.

We saw the right to left direction already. For the converse, let $\omega_1, \ldots, \omega_n$ be a basis for K/F, with minimal polynomials $p_1, p_2, \ldots, p_n$.

Lemma

If K/F is a Galois extension, then every irreducible $p(x) \in F[x]$ which has a root in K is separable and splits completely in K.

Corollary

An extension K/F is Galois if and only if it is the splitting field of a separable polynomial over F.

Proof.

We saw the right to left direction already. For the converse, let $\omega_1, \ldots, \omega_n$ be a basis for K/F, with minimal polynomials $p_1, p_2, \ldots, p_n$.

Each p_i is separable and splits completely in K by the lemma.

Lemma

If K/F is a Galois extension, then every irreducible $p(x) \in F[x]$ which has a root in K is separable and splits completely in K.

Corollary

An extension K/F is Galois if and only if it is the splitting field of a separable polynomial over F.

Proof.

We saw the right to left direction already. For the converse, let $\omega_1, \ldots, \omega_n$ be a basis for K/F, with minimal polynomials $p_1, p_2, \ldots, p_n$.

Each p_i is separable and splits completely in K by the lemma. Let $q_1(x), \ldots, q_r(x)$ be a listing of the distinct p_i's. Let $g(x) = q_1(x)q_2(x) \ldots q_r(x)$. Then K is the splitting field of $g(x)$.

□

Corollary

An extension K/F is Galois if and only if it is the splitting field of a separable polynomial over F.

Corollary

If K/F is Galois and $F \subseteq E \subseteq K$, then K/E is Galois.

Corollary

An extension K/F is Galois if and only if it is the splitting field of a separable polynomial over F.

Corollary

If K/F is Galois and $F \subseteq E \subseteq K$, then K/E is Galois.

Proof.

K/F is the splitting field of some $f(x) \in F[x]$, so is also the splitting field of $f(x)$ considered as a polynomial in $E[x]$. $\square$

Theorem (Key theorem)

If G is a finite subgroup of $\mathrm{Aut}(K)$ with fixed field F, then $|G| = [F : K]$.

Corollary

If G is a finite subgroup of $\mathrm{Aut}(K)$ with fixed field F, then $G = \mathrm{Aut}(K/F)$.

Theorem (Key theorem)

If G is a finite subgroup of $\mathrm{Aut}(K)$ with fixed field F, then $|G| = [F : K]$.

Corollary

If G is a finite subgroup of $\mathrm{Aut}(K)$ with fixed field F, then $G = \mathrm{Aut}(K/F)$.

Proof.

Clearly, any element of G is in $\mathrm{Aut}(K/F)$. Thus $|G| \leq |\mathrm{Aut}(K/F)|$.

Theorem (Key theorem)

If G is a finite subgroup of $\text{Aut}(K)$ with fixed field F, then $|G| = [F : K]$.

Corollary

If G is a finite subgroup of $\text{Aut}(K)$ with fixed field F, then $G = \text{Aut}(K/F)$.

Proof.

Clearly, any element of G is in $\text{Aut}(K/F)$. Thus $|G| \leq |\text{Aut}(K/F)|$.

By key theorem, $|G| = [K : F]$, so K/F is finite.

Theorem (Key theorem)

If G is a finite subgroup of $\mathrm{Aut}(K)$ with fixed field F, then $|G| = [F : K]$.

Corollary

If G is a finite subgroup of $\mathrm{Aut}(K)$ with fixed field F, then $G = \mathrm{Aut}(K/F)$.

Proof.

Clearly, any element of G is in $\mathrm{Aut}(K/F)$. Thus $|G| \leq |\mathrm{Aut}(K/F)|$.

By key theorem, $|G| = [K : F]$, so K/F is finite.

By earlier corollary, $|\mathrm{Aut}(K/F)| \leq [K : F]$.

Theorem (Key theorem)

If G is a finite subgroup of $\mathrm{Aut}(K)$ with fixed field F, then $|G| = [F : K]$.

Corollary

If G is a finite subgroup of $\mathrm{Aut}(K)$ with fixed field F, then $G = \mathrm{Aut}(K/F)$.

Proof.

Clearly, any element of G is in $\mathrm{Aut}(K/F)$. Thus $|G| \leq |\mathrm{Aut}(K/F)|$.

By key theorem, $|G| = [K : F]$, so K/F is finite.

By earlier corollary, $|\mathrm{Aut}(K/F)| \leq [K : F]$.

So we have $[K : F] = |G| \leq |\mathrm{Aut}(K/F)| \leq [K : F]$, so equality holds. □

Corollary

If G is a finite subgroup of $\text{Aut}(K)$ with fixed field F, then $G = \text{Aut}(K/F)$.

Corollary

If G is a finite subgroup of $\mathrm{Aut}(K)$ with fixed field F, then $G = \mathrm{Aut}(K/F)$.

Corollary

If $G_1 \neq G_2$ are distinct finite subgroups of $\mathrm{Aut}(K)$, then their fixed fields are distinct.

Corollary

If G is a finite subgroup of $\mathrm{Aut}(K)$ with fixed field F, then $G = \mathrm{Aut}(K/F)$.

Corollary

If $G_1 \neq G_2$ are distinct finite subgroups of $\mathrm{Aut}(K)$, then their fixed fields are distinct.

Proof.

Let F_1, F_2 be the fixed fields of G_1, G_2. By previous corollary, $G_1 = \mathrm{Aut}(K/F_1)$, $G_2 = \mathrm{Aut}(K/F_2)$. Thus if $F_1 = F_2$, then $G_1 = G_2$. □

The fundamental theorem, part I

Theorem

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

The fundamental theorem, part I

Theorem

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

There is a bijection between the subfields E of K containing F, and the subgroups H of G.

The fundamental theorem, part I

Theorem

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

There is a bijection between the subfields E of K containing F, and the subgroups H of G.

This bijection is given by sending E to the elements of G fixing E, and the inverse sends H to the fixed field of H. Moreover:

The fundamental theorem, part I

Theorem

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

There is a bijection between the subfields E of K containing F, and the subgroups H of G.

This bijection is given by sending E to the elements of G fixing E, and the inverse sends H to the fixed field of H. Moreover:

1. (Inclusion-reversing correspondence) If E_1, E_2 correspond to H_1, H_2, then E_1 is a subfield of E_2 if and only if H_2 is a subgroup of H_1.

The fundamental theorem, part I

Theorem

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

There is a bijection between the subfields E of K containing F, and the subgroups H of G.

This bijection is given by sending E to the elements of G fixing E, and the inverse sends H to the fixed field of H. Moreover:

1. (Inclusion-reversing correspondence) If E_1, E_2 correspond to H_1, H_2, then E_1 is a subfield of E_2 if and only if H_2 is a subgroup of H_1.
2. $[K : E] = |H|$ and $[E : F] = |G : H|$.

The fundamental theorem, part I

Theorem

Let K/F be a Galois extension and let $G = \text{Aut}(K/F)$ be the Galois group.

There is a bijection between the subfields E of K containing F, and the subgroups H of G.

This bijection is given by sending E to the elements of G fixing E, and the inverse sends H to the fixed field of H. Moreover:

1. (Inclusion-reversing correspondence) If E_1, E_2 correspond to H_1, H_2, then E_1 is a subfield of E_2 if and only if H_2 is a subgroup of H_1.
2. $[K : E] = |H|$ and $[E : F] = |G : H|$.
3. K/E is always Galois, with Galois group $\text{Aut}(K/E) = H$.

The fundamental theorem: picture

$$
\begin{array}{c}
K = \text{ fixed field of } 1 \\
{\scriptstyle |H|}\Big| \\
E = \text{ fixed field of } H \\
{\scriptstyle |G:H|}\Big| \\
F = \text{ fixed field of } G
\end{array}
$$

$$
\begin{array}{c}
1 = \text{ automorphisms fixing } K \\
{\scriptstyle [K:E]}\Big| \\
H = \text{ automorphisms fixing } E \\
{\scriptstyle [E:F]}\Big| \\
G = \mathrm{Aut}(K/F) = \text{ automorphisms fixing F}
\end{array}
$$

Proof of fundamental theorem, part I

We have already proven that the map sending a group to its fixed field is injective.

Proof of fundamental theorem, part I

We have already proven that the map sending a group to its fixed field is injective.

We have also seen that K/E is Galois for any intermediate field E, so E is the fixed field of $\text{Aut}(K/E)$. This shows the correspondence is surjective.

Proof of fundamental theorem, part I

We have already proven that the map sending a group to its fixed field is injective.

We have also seen that K/E is Galois for any intermediate field E, so E is the fixed field of $\mathrm{Aut}(K/E)$. This shows the correspondence is surjective.

Also, if E is the fixed field of H then $\mathrm{Aut}(K/E) = H$ so $|H| = \mathrm{Aut}(K/E) = [K : E]$, and we also know $[K : F] = |G|$, so taking quotients and using multiplicativity of degrees, $|G/H| = |G|/|H| = [E : F]$.

Summary

If K/F is a Galois extension (equivalently, the splitting field of a separable polynomial), then there is a perfect correspondence between subgroups of $\mathrm{Aut}(K/F)$ and intermediate fields, given by taking fixed fields.