Math-123: The fundamental theorem of Galois theory, part II

Sebastien Vasey

Harvard University

April 8, 2020

Recall...

Let K/F be a field extension. Galois theory studies the group $\mathrm{Aut}(K/F)$ of automorphisms of K fixing F.

Recall...

Let K/F be a field extension. Galois theory studies the group $\mathrm{Aut}(K/F)$ of automorphisms of K fixing F.

If K/F is finite, then $|\mathrm{Aut}(K/F)| \leq [K : F]$. If equality holds, we call K/F a *Galois extension*.

Recall...

Let K/F be a field extension. Galois theory studies the group $\mathrm{Aut}(K/F)$ of automorphisms of K fixing F.

If K/F is finite, then $|\mathrm{Aut}(K/F)| \leq [K : F]$. If equality holds, we call K/F a *Galois extension*.

Subgroups of $\mathrm{Aut}(K/F)$ have a corresponding *fixed field*.

The fundamental theorem, part I (last time)

Theorem

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

The fundamental theorem, part I (last time)

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 (last time)

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:

The fundamental theorem, part I (last time)

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 (last time)

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 (last time)

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

$$K = \text{ fixed field of } 1$$

$$\Big|\, |H| = |H{:}1|$$

$$E = \text{ fixed field of } H$$

$$\Big|\, |G{:}H|$$

$$F = \text{ fixed field of } G$$

$$1 = \text{ automorphisms fixing } K$$

$$\Big|\, [K{:}E]$$

$$H = \text{ automorphisms fixing } E$$

$$\Big|\, [E{:}F]$$

$$G = \mathrm{Aut}(K/F) = \text{ automorphisms fixing F}$$

The fundamental theorem, part II

Theorem

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

The fundamental theorem, part II

Theorem

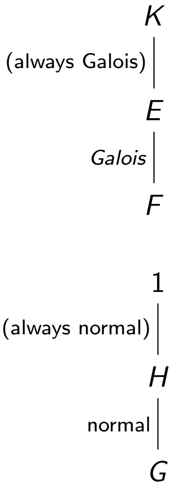
Let K/F be a Galois extension with Galois group $G = \text{Aut}(K/F)$. Let E be an intermediate field ($F \subseteq E \subseteq K$), with corresponding group $H = \text{Aut}(K/E)$.

The fundamental theorem, part II

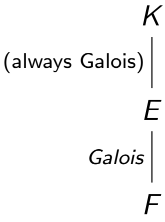
Theorem

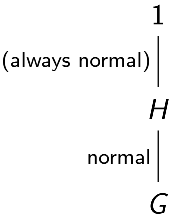
Let K/F be a Galois extension with Galois group $G = \mathrm{Aut}(K/F)$.
Let E be an intermediate field ($F \subseteq E \subseteq K$), with corresponding group $H = \mathrm{Aut}(K/E)$.
Then E is Galois over F if and only if H is a normal subgroup of G. In this case, $\mathrm{Aut}(E/F) \cong G/H$.

The fundamental theorem, part II: picture



The fundamental theorem, part II: picture

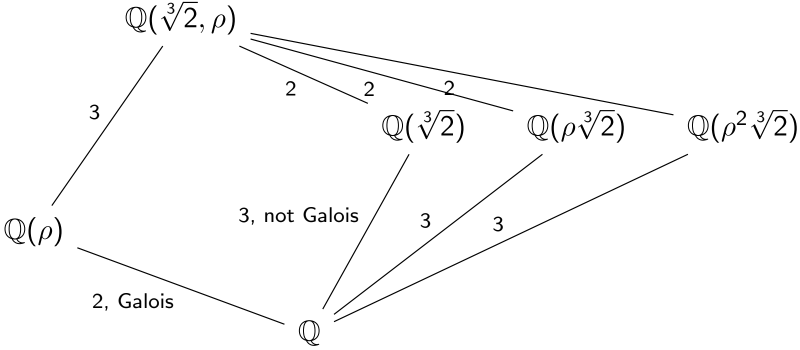




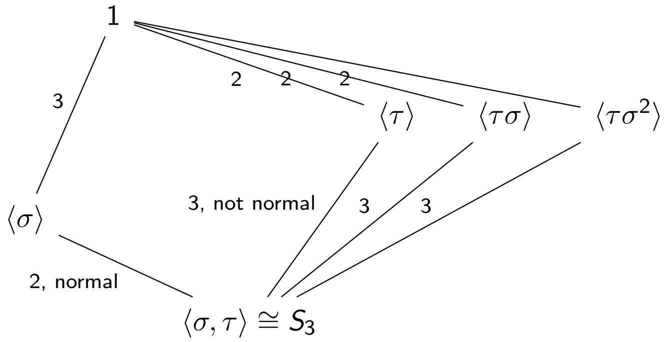
If H is normal in G, then
$G/H = \mathrm{Aut}(K/F)/\mathrm{Aut}(K/E) \cong \mathrm{Aut}(E/F)$.

Part II in action, splitting fields of $x^3 - 2$

$(\rho = e^{2\pi i/3})$



Part II in action, splitting field of $x^3 - 2$: group side



Proof of part II: Fix a subgroup H of G, let E be its fixed field. How do the members of $\mathrm{Aut}(E/F)$ relate to members of $\mathrm{Aut}(K/F)$?

Given $\sigma \in \mathrm{Aut}(K/F)$, $\sigma \restriction E$ may not be in $\mathrm{Aut}(E/F)$ (maybe $\sigma[E] \neq E$). What is true is that $\sigma \restriction E$ is an embedding ($=$ injective homomorphism) of E into K, fixing F

Proof of part II: Fix a subgroup H of G, let E be its fixed field. How do the members of $\mathrm{Aut}(E/F)$ relate to members of $\mathrm{Aut}(K/F)$?

Given $\sigma \in \mathrm{Aut}(K/F)$, $\sigma \upharpoonright E$ may not be in $\mathrm{Aut}(E/F)$ (maybe $\sigma[E] \neq E$). What is true is that $\sigma \upharpoonright E$ is an embedding ($=$ injective homomorphism) of E into K, fixing F

Conversely, if $\tau : E \to K$ is an embedding fixing F, then it is an isomorphism of E onto $\tau[E]$.

Proof of part II: Fix a subgroup H of G, let E be its fixed field. How do the members of $\mathrm{Aut}(E/F)$ relate to members of $\mathrm{Aut}(K/F)$?

Given $\sigma \in \mathrm{Aut}(K/F)$, $\sigma \upharpoonright E$ may not be in $\mathrm{Aut}(E/F)$ (maybe $\sigma[E] \neq E$). What is true is that $\sigma \upharpoonright E$ is an embedding ($=$ injective homomorphism) of E into K, fixing F

Conversely, if $\tau : E \to K$ is an embedding fixing F, then it is an isomorphism of E onto $\tau[E]$.

As K/F is Galois, K is the splitting field of a separable polynomial $f(x) \in F[x]$. K is the splitting field of $f(x) \in E[x]$ and the splitting field of $\tau(f(x)) = f(x) \in \tau[E][x]$. By results about splitting fields, τ extends to $\sigma \in \mathrm{Aut}(K/F)$.

$$\begin{array}{ccc} K & \xrightarrow[\sigma]{\cong} & K \\ \Big| & & \Big| \\ E & \xrightarrow[\tau]{\cong} & \tau[E] \end{array}$$

So let $\mathrm{Emb}(E/F)$ denote the set of embeddings of E into K fixing F. We showed $\sigma \mapsto \sigma \restriction E$ gives a surjection from $G = \mathrm{Aut}(K/F)$ onto $\mathrm{Emb}(E/F)$.

So let $\mathrm{Emb}(E/F)$ denote the set of embeddings of E into K fixing F. We showed $\sigma \mapsto \sigma \restriction E$ gives a surjection from $G = \mathrm{Aut}(K/F)$ onto $\mathrm{Emb}(E/F)$.

$\sigma \restriction E = \sigma' \restriction E$ if and only if $(\sigma^{-1}\sigma') \restriction E$ is the identity.

So let $\mathrm{Emb}(E/F)$ denote the set of embeddings of E into K fixing F. We showed $\sigma \mapsto \sigma \upharpoonright E$ gives a surjection from $G = \mathrm{Aut}(K/F)$ onto $\mathrm{Emb}(E/F)$.

$\sigma \upharpoonright E = \sigma' \upharpoonright E$ if and only if $(\sigma^{-1}\sigma') \upharpoonright E$ is the identity.

That is, $\sigma^{-1}\sigma'$ must fix E: it must be in $\mathrm{Aut}(K/E) = H$.

So let $\mathrm{Emb}(E/F)$ denote the set of embeddings of E into K fixing F. We showed $\sigma \mapsto \sigma \restriction E$ gives a surjection from $G = \mathrm{Aut}(K/F)$ onto $\mathrm{Emb}(E/F)$.

$\sigma \restriction E = \sigma' \restriction E$ if and only if $(\sigma^{-1}\sigma') \restriction E$ is the identity.

That is, $\sigma^{-1}\sigma'$ must fix E: it must be in $\mathrm{Aut}(K/E) = H$.

Thus $\sigma \restriction E = \sigma' \restriction E$ if and only if $\sigma' \in \sigma H$ (if and only if $\sigma' H = \sigma H$). So the distinct $\sigma \restriction E$'s are in bijection with the cosets of H in G: $|\mathrm{Emb}(E/F)| = [G : H] = [E : F]$.

So let $\mathrm{Emb}(E/F)$ denote the set of embeddings of E into K fixing F. We showed $\sigma \mapsto \sigma \restriction E$ gives a surjection from $G = \mathrm{Aut}(K/F)$ onto $\mathrm{Emb}(E/F)$.

$\sigma \restriction E = \sigma' \restriction E$ if and only if $(\sigma^{-1}\sigma') \restriction E$ is the identity.

That is, $\sigma^{-1}\sigma'$ must fix E: it must be in $\mathrm{Aut}(K/E) = H$.

Thus $\sigma \restriction E = \sigma' \restriction E$ if and only if $\sigma' \in \sigma H$ (if and only if $\sigma' H = \sigma H$). So the distinct $\sigma \restriction E$'s are in bijection with the cosets of H in G: $|\mathrm{Emb}(E/F)| = [G : H] = [E : F]$.

So E/F is Galois if and only if $|\mathrm{Emb}(E/F)| = |\mathrm{Aut}(E/F)|$. In other words, E/F is Galois if and only if $\sigma[E] = E$ for all $\sigma \in G$.

So let $\mathrm{Emb}(E/F)$ denote the set of embeddings of E into K fixing F. We showed $\sigma \mapsto \sigma \restriction E$ gives a surjection from $G = \mathrm{Aut}(K/F)$ onto $\mathrm{Emb}(E/F)$.

$\sigma \restriction E = \sigma' \restriction E$ if and only if $(\sigma^{-1}\sigma') \restriction E$ is the identity.

That is, $\sigma^{-1}\sigma'$ must fix E: it must be in $\mathrm{Aut}(K/E) = H$.

Thus $\sigma \restriction E = \sigma' \restriction E$ if and only if $\sigma' \in \sigma H$ (if and only if $\sigma' H = \sigma H$). So the distinct $\sigma \restriction E$'s are in bijection with the cosets of H in G: $|\mathrm{Emb}(E/F)| = [G : H] = [E : F]$.

So E/F is Galois if and only if $|\mathrm{Emb}(E/F)| = |\mathrm{Aut}(E/F)|$. In other words, E/F is Galois if and only if $\sigma[E] = E$ for all $\sigma \in G$.

Fix $\sigma \in G$. When is $\sigma[E] = E$? By the Galois correspondence, precisely when their fixing subgroups are equal:
$\mathrm{Aut}(K/E) = \mathrm{Aut}(K/\sigma[E])$

So let $\mathrm{Emb}(E/F)$ denote the set of embeddings of E into K fixing F. We showed $\sigma \mapsto \sigma \restriction E$ gives a surjection from $G = \mathrm{Aut}(K/F)$ onto $\mathrm{Emb}(E/F)$.

$\sigma \restriction E = \sigma' \restriction E$ if and only if $(\sigma^{-1}\sigma') \restriction E$ is the identity.

That is, $\sigma^{-1}\sigma'$ must fix E: it must be in $\mathrm{Aut}(K/E) = H$.

Thus $\sigma \restriction E = \sigma' \restriction E$ if and only if $\sigma' \in \sigma H$ (if and only if $\sigma' H = \sigma H$). So the distinct $\sigma \restriction E$'s are in bijection with the cosets of H in G: $|\mathrm{Emb}(E/F)| = [G : H] = [E : F]$.

So E/F is Galois if and only if $|\mathrm{Emb}(E/F)| = |\mathrm{Aut}(E/F)|$. In other words, E/F is Galois if and only if $\sigma[E] = E$ for all $\sigma \in G$.

Fix $\sigma \in G$. When is $\sigma[E] = E$? By the Galois correspondence, precisely when their fixing subgroups are equal:
$\mathrm{Aut}(K/E) = \mathrm{Aut}(K/\sigma[E])$

Claim: $\mathrm{Aut}(K/\sigma[E]) = \sigma H \sigma^{-1}$ $(= \sigma \mathrm{Aut}(K/E)\sigma^{-1})$.

Claim: $\mathrm{Aut}(K/\sigma[E]) = \sigma H \sigma^{-1}$ $(= \sigma\mathrm{Aut}(K/E)\sigma^{-1})$.

Claim: $\text{Aut}(K/\sigma[E]) = \sigma H \sigma^{-1}$ $(= \sigma\text{Aut}(K/E)\sigma^{-1})$.

Proof of Claim: Suppose $\tau \in \text{Aut}(K/\sigma[E])$. Let $\tau' := \sigma^{-1}\tau\sigma$. Then $\tau = \sigma\tau'\sigma^{-1}$ and for all $a \in E$,
$\tau'(a) = \sigma^{-1}\tau\sigma(a) = \sigma^{-1}\sigma(a) = a$. Thus $\tau' \in H$.

Claim: $\mathrm{Aut}(K/\sigma[E]) = \sigma H \sigma^{-1}$ $(= \sigma \mathrm{Aut}(K/E)\sigma^{-1})$.

Proof of Claim: Suppose $\tau \in \mathrm{Aut}(K/\sigma[E])$. Let $\tau' := \sigma^{-1}\tau\sigma$. Then $\tau = \sigma\tau'\sigma^{-1}$ and for all $a \in E$,
$\tau'(a) = \sigma^{-1}\tau\sigma(a) = \sigma^{-1}\sigma(a) = a$. Thus $\tau' \in H$.

This shows $\mathrm{Aut}(K/\sigma[E]) \subseteq \sigma H \sigma^{-1}$. For the converse, observe $|\mathrm{Aut}(K/\sigma[E])| = |\mathrm{Aut}(K/E)| = [K : E] = |H| = |\sigma H \sigma^{-1}|$. $\dagger_{\text{Claim}}$

Thus E/F is Galois if and only if $\sigma[E] = E$ for all $\sigma \in G$ if and only if $H = \sigma H \sigma^{-1}$ for all $\sigma \in G$, which means precisely that H is normal in G.

Claim: $\mathrm{Aut}(K/\sigma[E]) = \sigma H \sigma^{-1}$ $(= \sigma \mathrm{Aut}(K/E)\sigma^{-1})$.

Proof of Claim: Suppose $\tau \in \mathrm{Aut}(K/\sigma[E])$. Let $\tau' := \sigma^{-1}\tau\sigma$. Then $\tau = \sigma\tau'\sigma^{-1}$ and for all $a \in E$,
$\tau'(a) = \sigma^{-1}\tau\sigma(a) = \sigma^{-1}\sigma(a) = a$. Thus $\tau' \in H$.

This shows $\mathrm{Aut}(K/\sigma[E]) \subseteq \sigma H \sigma^{-1}$. For the converse, observe $|\mathrm{Aut}(K/\sigma[E])| = |\mathrm{Aut}(K/E)| = [K : E] = |H| = |\sigma H \sigma^{-1}|$. $\dagger_{\mathrm{Claim}}$

Thus E/F is Galois if and only if $\sigma[E] = E$ for all $\sigma \in G$ if and only if $H = \sigma H \sigma^{-1}$ for all $\sigma \in G$, which means precisely that H is normal in G.

We saw the members of $\mathrm{Aut}(E/F)$ are in bijections with cosets of H in G and this bijection respects composition, so gives an isomorphism of $\mathrm{Aut}(E/F)$ with G/H. This concludes the proof of part II!

Fundamental theorem, part III

Theorem

If E_1, E_2 correspond to H_1, H_2, then $E_1 \cap E_2$ corresponds to $\langle H_1, H_2 \rangle$, and $E_1 E_2$ corresponds to $H_1 \cap H_2$.

Fundamental theorem, part III

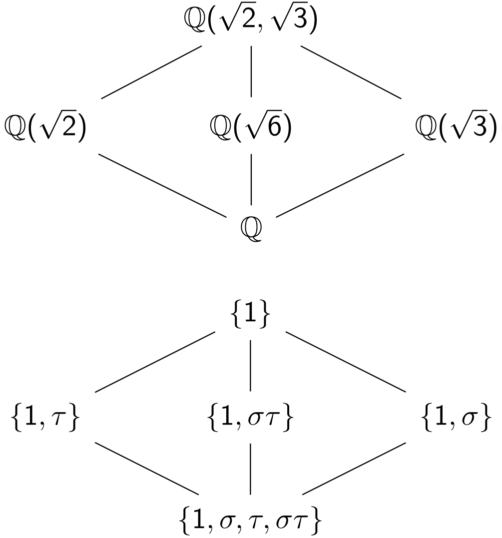
Theorem

If E_1, E_2 correspond to H_1, H_2, then $E_1 \cap E_2$ corresponds to $\langle H_1, H_2 \rangle$, and $E_1 E_2$ corresponds to $H_1 \cap H_2$.

Proof.

Exercise! Use the definition of the fixed field. $\square$

Part III in action: $\mathbb{Q}(\sqrt{2}, \sqrt{3})$



Example: $\mathbb{Q}(\sqrt{2}+\sqrt{3})$

Let's compute the minimal polynomial of $\sqrt{2}+\sqrt{3}$ using Galois theory.

Example: $\mathbb{Q}(\sqrt{2}+\sqrt{3})$

Let's compute the minimal polynomial of $\sqrt{2}+\sqrt{3}$ using Galois theory.

Recall $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ is a Galois extension of degree 4 (It is the splitting field of $(x^2-2)(x^2-3)$).

Example: $\mathbb{Q}(\sqrt{2}+\sqrt{3})$

Let's compute the minimal polynomial of $\sqrt{2}+\sqrt{3}$ using Galois theory.

Recall $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ is a Galois extension of degree 4 (It is the splitting field of $(x^2-2)(x^2-3)$).

Clearly, $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3}) = K$. The roots of the minimal polynomial $f(x)$ of $\sqrt{2}+\sqrt{3}$ are the images of $\sqrt{2}+\sqrt{3}$ under the members of $\mathrm{Aut}(K/\mathbb{Q})$ (called the *conjugates under* $Aut(K/\mathbb{Q})$).

Example: $\mathbb{Q}(\sqrt{2}+\sqrt{3})$

Let's compute the minimal polynomial of $\sqrt{2}+\sqrt{3}$ using Galois theory.

Recall $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ is a Galois extension of degree 4 (It is the splitting field of $(x^2-2)(x^2-3)$).

Clearly, $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3}) = K$. The roots of the minimal polynomial $f(x)$ of $\sqrt{2}+\sqrt{3}$ are the images of $\sqrt{2}+\sqrt{3}$ under the members of $\text{Aut}(K/\mathbb{Q})$ (called the *conjugates under Aut*$(K/\mathbb{Q})$).

Therefore $f(x)$ has $\pm\sqrt{2}\pm\sqrt{3}$ as roots. They are all distinct.

Example: $\mathbb{Q}(\sqrt{2}+\sqrt{3})$

Let's compute the minimal polynomial of $\sqrt{2}+\sqrt{3}$ using Galois theory.

Recall $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ is a Galois extension of degree 4 (It is the splitting field of $(x^2-2)(x^2-3)$).

Clearly, $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3}) = K$. The roots of the minimal polynomial $f(x)$ of $\sqrt{2}+\sqrt{3}$ are the images of $\sqrt{2}+\sqrt{3}$ under the members of $\mathrm{Aut}(K/\mathbb{Q})$ (called the *conjugates under Aut*$(K/\mathbb{Q})$).

Therefore $f(x)$ has $\pm\sqrt{2}\pm\sqrt{3}$ as roots. They are all distinct.

$$f(x) = (x-(\sqrt{2}+\sqrt{3}))(x-(\sqrt{2}-\sqrt{3}))(x-(-\sqrt{2}+\sqrt{3}))(x-(-\sqrt{2}-\sqrt{3}))$$

Example: $\mathbb{Q}(\sqrt{2}+\sqrt{3})$

Let's compute the minimal polynomial of $\sqrt{2}+\sqrt{3}$ using Galois theory.

Recall $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ is a Galois extension of degree 4 (It is the splitting field of $(x^2-2)(x^2-3)$).

Clearly, $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3}) = K$. The roots of the minimal polynomial $f(x)$ of $\sqrt{2}+\sqrt{3}$ are the images of $\sqrt{2}+\sqrt{3}$ under the members of $\mathrm{Aut}(K/\mathbb{Q})$ (called the *conjugates under Aut*$(K/\mathbb{Q})$).

Therefore $f(x)$ has $\pm\sqrt{2}\pm\sqrt{3}$ as roots. They are all distinct.

$$f(x) = (x-(\sqrt{2}+\sqrt{3}))(x-(\sqrt{2}-\sqrt{3}))(x-(-\sqrt{2}+\sqrt{3}))(x-(-\sqrt{2}-\sqrt{3}))$$

By direct computation, $f(x) = x^4 - 10x^2 + 1$.

Example: $\mathbb{Q}(\sqrt{2}+\sqrt{3})$

Let's compute the minimal polynomial of $\sqrt{2}+\sqrt{3}$ using Galois theory.

Recall $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ is a Galois extension of degree 4 (It is the splitting field of $(x^2-2)(x^2-3)$).

Clearly, $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3}) = K$. The roots of the minimal polynomial $f(x)$ of $\sqrt{2}+\sqrt{3}$ are the images of $\sqrt{2}+\sqrt{3}$ under the members of $\mathrm{Aut}(K/\mathbb{Q})$ (called the *conjugates under Aut*$(K/\mathbb{Q})$).

Therefore $f(x)$ has $\pm\sqrt{2}\pm\sqrt{3}$ as roots. They are all distinct.

$$f(x) = (x-(\sqrt{2}+\sqrt{3}))(x-(\sqrt{2}-\sqrt{3}))(x-(-\sqrt{2}+\sqrt{3}))(x-(-\sqrt{2}-\sqrt{3}))$$

By direct computation, $f(x) = x^4 - 10x^2 + 1$.

In particular, this polynomial is irreducible, and $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ has degree 4, so is equal to $\mathbb{Q}(\sqrt{2},\sqrt{3})$.

Example: splitting field K of $x^8 - 2$

K is generated by $\theta = \sqrt[8]{2}$ and $\zeta = e^{2\pi i/8}$, a primitive 8th root of unity, so $K = \mathbb{Q}(\sqrt[8]{2}, \zeta)$.

Example: splitting field K of $x^8 - 2$

K is generated by $\theta = \sqrt[8]{2}$ and $\zeta = e^{2\pi i/8}$, a primitive 8th root of unity, so $K = \mathbb{Q}(\sqrt[8]{2}, \zeta)$.

Any automorphism of K is determined by what it does to $\sqrt[8]{2}$ and to ζ. It can take $\sqrt[8]{2}$ to 8 different possibilities, and ζ to $\phi(8)$ ($=$ the number of primitive 8th root of unity) different possibilities. Observe $\phi(8) = 2^3 - 2^2 = 4$.

Example: splitting field K of $x^8 - 2$

K is generated by $\theta = \sqrt[8]{2}$ and $\zeta = e^{2\pi i/8}$, a primitive 8th root of unity, so $K = \mathbb{Q}(\sqrt[8]{2}, \zeta)$.

Any automorphism of K is determined by what it does to $\sqrt[8]{2}$ and to ζ. It can take $\sqrt[8]{2}$ to 8 different possibilities, and ζ to $\phi(8)$ (= the number of primitive 8th root of unity) different possibilities. Observe $\phi(8) = 2^3 - 2^2 = 4$.

WARNING: Does it mean there are $8 \cdot 4 = 32$ automorphisms?

Example: splitting field K of $x^8 - 2$

K is generated by $\theta = \sqrt[8]{2}$ and $\zeta = e^{2\pi i/8}$, a primitive 8th root of unity, so $K = \mathbb{Q}(\sqrt[8]{2}, \zeta)$.

Any automorphism of K is determined by what it does to $\sqrt[8]{2}$ and to ζ. It can take $\sqrt[8]{2}$ to 8 different possibilities, and ζ to $\phi(8)$ (= the number of primitive 8th root of unity) different possibilities. Observe $\phi(8) = 2^3 - 2^2 = 4$.

WARNING: Does it mean there are $8 \cdot 4 = 32$ automorphisms? No! For example $\theta^4 = \sqrt{2} = \zeta + \zeta^7$, so we cannot send θ to θ and ζ to ζ^3 for example.

Example: splitting field K of $x^8 - 2$

K is generated by $\theta = \sqrt[8]{2}$ and $\zeta = e^{2\pi i/8}$, a primitive 8th root of unity, so $K = \mathbb{Q}(\sqrt[8]{2}, \zeta)$.

Any automorphism of K is determined by what it does to $\sqrt[8]{2}$ and to ζ. It can take $\sqrt[8]{2}$ to 8 different possibilities, and ζ to $\phi(8)$ (= the number of primitive 8th root of unity) different possibilities. Observe $\phi(8) = 2^3 - 2^2 = 4$.

WARNING: Does it mean there are $8 \cdot 4 = 32$ automorphisms? No! For example $\theta^4 = \sqrt{2} = \zeta + \zeta^7$, so we cannot send θ to θ and ζ to ζ^3 for example.

There may be more relations: checking directly that a certain mapping gives an automorphism is annoying. It is better to compute the degree of the extension first.

Example: splitting field K of $x^8 - 2$

K is generated by $\theta = \sqrt[8]{2}$ and $\zeta = e^{2\pi i/8}$, a primitive 8th root of unity, so $K = \mathbb{Q}(\sqrt[8]{2}, \zeta)$.

Any automorphism of K is determined by what it does to $\sqrt[8]{2}$ and to ζ. It can take $\sqrt[8]{2}$ to 8 different possibilities, and ζ to $\phi(8)$ (= the number of primitive 8th root of unity) different possibilities. Observe $\phi(8) = 2^3 - 2^2 = 4$.

WARNING: Does it mean there are $8 \cdot 4 = 32$ automorphisms? No! For example $\theta^4 = \sqrt{2} = \zeta + \zeta^7$, so we cannot send θ to θ and ζ to ζ^3 for example.

There may be more relations: checking directly that a certain mapping gives an automorphism is annoying. It is better to compute the degree of the extension first.

We have that $\zeta = \frac{\sqrt{2}}{2}(1 + i)$, so in fact we can show that $K = \mathbb{Q}(\sqrt[8]{2}, i)$.

Example: splitting field K of $x^8 - 2$

K is generated by $\theta = \sqrt[8]{2}$ and $\zeta = e^{2\pi i/8}$, a primitive 8th root of unity, so $K = \mathbb{Q}(\sqrt[8]{2}, \zeta)$.

Any automorphism of K is determined by what it does to $\sqrt[8]{2}$ and to ζ. It can take $\sqrt[8]{2}$ to 8 different possibilities, and ζ to $\phi(8)$ (= the number of primitive 8th root of unity) different possibilities. Observe $\phi(8) = 2^3 - 2^2 = 4$.

WARNING: Does it mean there are $8 \cdot 4 = 32$ automorphisms? No! For example $\theta^4 = \sqrt{2} = \zeta + \zeta^7$, so we cannot send θ to θ and ζ to ζ^3 for example.

There may be more relations: checking directly that a certain mapping gives an automorphism is annoying. It is better to compute the degree of the extension first.

We have that $\zeta = \frac{\sqrt{2}}{2}(1 + i)$, so in fact we can show that $K = \mathbb{Q}(\sqrt[8]{2}, i)$.

This has degree at most $2 \cdot 8 = 16$, but strictly more than 8 (i is not real), so must have degree 16.

Splitting field of $x^8 - 2$, continued

So $K = \mathbb{Q}(\sqrt[8]{2}, i)$ is the splitting field of $x^8 - 2$ and has degree 16.

Splitting field of $x^8 - 2$, continued

So $K = \mathbb{Q}(\sqrt[8]{2}, i)$ is the splitting field of $x^8 - 2$ and has degree 16.

It is a Galois extension, so $G = \mathrm{Aut}(K/\mathbb{Q})$ has 16 elements. They are determined by what they do to $\theta = \sqrt[8]{2}$ and i.

Splitting field of $x^8 - 2$, continued

So $K = \mathbb{Q}(\sqrt[8]{2}, i)$ is the splitting field of $x^8 - 2$ and has degree 16.

It is a Galois extension, so $G = \mathrm{Aut}(K/\mathbb{Q})$ has 16 elements. They are determined by what they do to $\theta = \sqrt[8]{2}$ and i.

i is a root of $x^2 + 1$, so automorphisms send it to $\pm i$.

Splitting field of $x^8 - 2$, continued

So $K = \mathbb{Q}(\sqrt[8]{2}, i)$ is the splitting field of $x^8 - 2$ and has degree 16.

It is a Galois extension, so $G = \mathrm{Aut}(K/\mathbb{Q})$ has 16 elements. They are determined by what they do to $\theta = \sqrt[8]{2}$ and i.

i is a root of $x^2 + 1$, so automorphisms send it to $\pm i$.

$\sqrt[8]{2}$ is a root of $x^8 - 2$, so automorphisms send it to $\zeta^a \sqrt[8]{2}$, for $a = 0, 1, 2, \ldots, 7$.

Splitting field of $x^8 - 2$, continued

So $K = \mathbb{Q}(\sqrt[8]{2}, i)$ is the splitting field of $x^8 - 2$ and has degree 16.

It is a Galois extension, so $G = \mathrm{Aut}(K/\mathbb{Q})$ has 16 elements. They are determined by what they do to $\theta = \sqrt[8]{2}$ and i.

i is a root of $x^2 + 1$, so automorphisms send it to $\pm i$.

$\sqrt[8]{2}$ is a root of $x^8 - 2$, so automorphisms send it to $\zeta^a \sqrt[8]{2}$, for $a = 0, 1, 2, \ldots, 7$.

This gives 16 possibilities, so all of these choices are indeed automorphisms. Let σ send θ to $\zeta\theta$, and fix i. Let τ send θ to θ and i to $-i$.

Splitting field of $x^8 - 2$, continued

So $K = \mathbb{Q}(\sqrt[8]{2}, i)$ is the splitting field of $x^8 - 2$ and has degree 16.

It is a Galois extension, so $G = \mathrm{Aut}(K/\mathbb{Q})$ has 16 elements. They are determined by what they do to $\theta = \sqrt[8]{2}$ and i.

i is a root of $x^2 + 1$, so automorphisms send it to $\pm i$.

$\sqrt[8]{2}$ is a root of $x^8 - 2$, so automorphisms send it to $\zeta^a \sqrt[8]{2}$, for $a = 0, 1, 2, \ldots, 7$.

This gives 16 possibilities, so all of these choices are indeed automorphisms. Let σ send θ to $\zeta\theta$, and fix i. Let τ send θ to θ and i to $-i$.

$G = \langle \sigma, \theta \rangle$, σ has order 2, θ has order 8. We can also compute that $\sigma\tau = \tau\sigma^3$ (details in the book).

Splitting field of $x^8 - 2$, continued

So $K = \mathbb{Q}(\sqrt[8]{2}, i)$ is the splitting field of $x^8 - 2$ and has degree 16.

It is a Galois extension, so $G = \text{Aut}(K/\mathbb{Q})$ has 16 elements. They are determined by what they do to $\theta = \sqrt[8]{2}$ and i.

i is a root of $x^2 + 1$, so automorphisms send it to $\pm i$.

$\sqrt[8]{2}$ is a root of $x^8 - 2$, so automorphisms send it to $\zeta^a \sqrt[8]{2}$, for $a = 0, 1, 2, \ldots, 7$.

This gives 16 possibilities, so all of these choices are indeed automorphisms. Let σ send θ to $\zeta\theta$, and fix i. Let τ send θ to θ and i to $-i$.

$G = \langle \sigma, \theta \rangle$, σ has order 2, θ has order 8. We can also compute that $\sigma\tau = \tau\sigma^3$ (details in the book).

This determines the group completely: it is a "quasidihedral group" of order 16. See the book for the computation of the subgroups and subfields.

Galois groups of finite fields

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

Galois groups of finite fields

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

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

Galois groups of finite fields

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

We showed earlier 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 $a \in F$.

Galois groups of finite fields

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

We showed earlier 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.

Galois groups of finite fields

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

We showed earlier 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 $a \in F$.

Galois groups of finite fields

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

We showed earlier 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.

Galois groups of finite fields

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

We showed earlier 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 K/F is cyclic of order n, generated by the Frobenius map: $\mathrm{Aut}(K/F) \cong \mathbb{Z}/n\mathbb{Z}$.

σ has order n, so the Galois group of K/F is cyclic of order n, generated by the Frobenius map: $\mathrm{Aut}(K/F) \cong \mathbb{Z}/n\mathbb{Z}$.

σ has order n, so the Galois group of K/F is cyclic of order n, generated by the Frobenius map: $\mathrm{Aut}(K/F) \cong \mathbb{Z}/n\mathbb{Z}$.

By the fundamental theorem, subfields of $\mathbb{F}_{p^n}$ and subgroups of $\mathbb{Z}/n\mathbb{Z}$ are in one to one correspondence.

σ has order n, so the Galois group of K/F is cyclic of order n, generated by the Frobenius map: $\text{Aut}(K/F) \cong \mathbb{Z}/n\mathbb{Z}$.

By the fundamental theorem, subfields of $\mathbb{F}_{p^n}$ and subgroups of $\mathbb{Z}/n\mathbb{Z}$ are in one to one correspondence.

Subgroups of $\mathbb{Z}/n\mathbb{Z}$ are those generated by d, d a divisor of n.

σ has order n, so the Galois group of K/F is cyclic of order n, generated by the Frobenius map: $\text{Aut}(K/F) \cong \mathbb{Z}/n\mathbb{Z}$.

By the fundamental theorem, subfields of $\mathbb{F}_{p^n}$ and subgroups of $\mathbb{Z}/n\mathbb{Z}$ are in one to one correspondence.

Subgroups of $\mathbb{Z}/n\mathbb{Z}$ are those generated by d, d a divisor of n.

So for every divisor d of n, there is a unique subfield E of $\mathbb{F}_{p^n}$, and there are no other subfields.

σ has order n, so the Galois group of K/F is cyclic of order n, generated by the Frobenius map: $\text{Aut}(K/F) \cong \mathbb{Z}/n\mathbb{Z}$.

By the fundamental theorem, subfields of $\mathbb{F}_{p^n}$ and subgroups of $\mathbb{Z}/n\mathbb{Z}$ are in one to one correspondence.

Subgroups of $\mathbb{Z}/n\mathbb{Z}$ are those generated by d, d a divisor of n.

So for every divisor d of n, there is a unique subfield E of $\mathbb{F}_{p^n}$, and there are no other subfields.

More precisely: if σ is the Frobenius map, d a divisor of n, H the subgroup generated by σ^d, then $|H| = \frac{n}{d}$, so if E is the fixed field, $[K : E] = \frac{n}{d}$ and $[E : F] = d$.

σ has order n, so the Galois group of K/F is cyclic of order n, generated by the Frobenius map: $\mathrm{Aut}(K/F) \cong \mathbb{Z}/n\mathbb{Z}$.

By the fundamental theorem, subfields of $\mathbb{F}_{p^n}$ and subgroups of $\mathbb{Z}/n\mathbb{Z}$ are in one to one correspondence.

Subgroups of $\mathbb{Z}/n\mathbb{Z}$ are those generated by d, d a divisor of n.

So for every divisor d of n, there is a unique subfield E of $\mathbb{F}_{p^n}$, and there are no other subfields.

More precisely: if σ is the Frobenius map, d a divisor of n, H the subgroup generated by σ^d, then $|H| = \frac{n}{d}$, so if E is the fixed field, $[K : E] = \frac{n}{d}$ and $[E : F] = d$.

By uniqueness of finite fields, $E = \mathbb{F}_{p^d}$.

σ has order n, so the Galois group of K/F is cyclic of order n, generated by the Frobenius map: $\text{Aut}(K/F) \cong \mathbb{Z}/n\mathbb{Z}$.

By the fundamental theorem, subfields of $\mathbb{F}_{p^n}$ and subgroups of $\mathbb{Z}/n\mathbb{Z}$ are in one to one correspondence.

Subgroups of $\mathbb{Z}/n\mathbb{Z}$ are those generated by d, d a divisor of n.

So for every divisor d of n, there is a unique subfield E of $\mathbb{F}_{p^n}$, and there are no other subfields.

More precisely: if σ is the Frobenius map, d a divisor of n, H the subgroup generated by σ^d, then $|H| = \frac{n}{d}$, so if E is the fixed field, $[K : E] = \frac{n}{d}$ and $[E : F] = d$.

By uniqueness of finite fields, $E = \mathbb{F}_{p^d}$.

Since cyclic groups are abelian, all the subgroups are normal, so E/F is Galois (which we knew already).

Irreducible polynomials over $\mathbb{F}_p$

Remember that in the assignments you built some finite fields by hand by exhibiting irreducible elements in $\mathbb{F}_p[x]$ of certain degrees.

Irreducible polynomials over $\mathbb{F}_p$

Remember that in the assignments you built some finite fields by hand by exhibiting irreducible elements in $\mathbb{F}_p[x]$ of certain degrees.

In general they are not so easy to find: given n and p, is there even an irreducible polynomial of degree n in $\mathbb{F}_p[x]$?

Irreducible polynomials over $\mathbb{F}_p$

Remember that in the assignments you built some finite fields by hand by exhibiting irreducible elements in $\mathbb{F}_p[x]$ of certain degrees.

In general they are not so easy to find: given n and p, is there even an irreducible polynomial of degree n in $\mathbb{F}_p[x]$? The answer is yes:

Theorem

The extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ is simple: $\mathbb{F}_{p^n} = \mathbb{F}_p(\theta)$ for some θ. In particular, the minimal polynomial of θ is irreducible in $\mathbb{F}_p[x]$ of degree n.

Irreducible polynomials over $\mathbb{F}_p$

Remember that in the assignments you built some finite fields by hand by exhibiting irreducible elements in $\mathbb{F}_p[x]$ of certain degrees.

In general they are not so easy to find: given n and p, is there even an irreducible polynomial of degree n in $\mathbb{F}_p[x]$? The answer is yes:

Theorem

The extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ is simple: $\mathbb{F}_{p^n} = \mathbb{F}_p(\theta)$ for some θ. In particular, the minimal polynomial of θ is irreducible in $\mathbb{F}_p[x]$ of degree n.

Proof.

We say any finite subgroup of the group of units of a field is cyclic, so $\mathbb{F}_{p^n}^{\times}$ is cyclic: take θ to be a generator. □

Theorem

For each prime p and each n, there are irreducible polynomials in $\mathbb{F}_p[x]$ of degree n.

Okay, but what are these irreducible polynomials?

Theorem

For each prime p and each n, there are irreducible polynomials in $\mathbb{F}_p[x]$ of degree n.

Okay, but what are these irreducible polynomials?

Say $\mathbb{F}_{p^n} = \mathbb{F}_p(\theta)$. Since $\mathbb{F}_{p^n}$ is just the set of all rots of the polynomial $x^{p^n} - x$, this means θ is a root, so its minimal polynomial divides $x^{p^n} - x$.

Theorem

For each prime p and each n, there are irreducible polynomials in $\mathbb{F}_p[x]$ of degree n.

Okay, but what are these irreducible polynomials?

Say $\mathbb{F}_{p^n} = \mathbb{F}_p(\theta)$. Since $\mathbb{F}_{p^n}$ is just the set of all rots of the polynomial $x^{p^n} - x$, this means θ is a root, so its minimal polynomial divides $x^{p^n} - x$.

Conversely, if $p(x) \in \mathbb{F}_p[x]$ is any irreducible polynomial of degree d which divides $x^{p^n} - x$, and $p(\alpha) = 0$, then $\mathbb{F}_p(\alpha)$ is a subfield of $\mathbb{F}_{p^n}$ of degree d.

Theorem

For each prime p and each n, there are irreducible polynomials in $\mathbb{F}_p[x]$ of degree n.

Okay, but what are these irreducible polynomials?

Say $\mathbb{F}_{p^n} = \mathbb{F}_p(\theta)$. Since $\mathbb{F}_{p^n}$ is just the set of all rots of the polynomial $x^{p^n} - x$, this means θ is a root, so its minimal polynomial divides $x^{p^n} - x$.

Conversely, if $p(x) \in \mathbb{F}_p[x]$ is any irreducible polynomial of degree d which divides $x^{p^n} - x$, and $p(\alpha) = 0$, then $\mathbb{F}_p(\alpha)$ is a subfield of $\mathbb{F}_{p^n}$ of degree d.

We have just seen that $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^d}$. In particular, d divides n. Since $\mathbb{F}_p(\alpha)$ is Galois, it contains *all* the roots of $p(x)$.

Theorem

For each prime p and each n, there are irreducible polynomials in $\mathbb{F}_p[x]$ of degree n.

Okay, but what are these irreducible polynomials?

Say $\mathbb{F}_{p^n} = \mathbb{F}_p(\theta)$. Since $\mathbb{F}_{p^n}$ is just the set of all rots of the polynomial $x^{p^n} - x$, this means θ is a root, so its minimal polynomial divides $x^{p^n} - x$.

Conversely, if $p(x) \in \mathbb{F}_p[x]$ is any irreducible polynomial of degree d which divides $x^{p^n} - x$, and $p(\alpha) = 0$, then $\mathbb{F}_p(\alpha)$ is a subfield of $\mathbb{F}_{p^n}$ of degree d.

We have just seen that $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^d}$. In particular, d divides n. Since $\mathbb{F}_p(\alpha)$ is Galois, it contains *all* the roots of $p(x)$.

Putting all of this together: $x^{p^n} - x$ is the product of $(x - \beta)$, for β a root. β has a certain minimal polynomial of degree d. That degree must divide n. Conversely, any irreducible poly with degree d dividing n must generate $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$, so divides $x^{p^n} - x$.

Theorem

$x^{p^n} - x$ is the product of all the distinct irreducible polynomials in $\mathbb{F}_p[x]$ of degree d, where d runs through all the divisors of n.

This can be used to produce irreducible polynomials recursively, count how many there are, etc. (see DF)

A fun result

Theorem

The irreducible $x^4 + 1 \in \mathbb{Z}[x]$ is reducible modulo every prime.

Proof: If $p = 2$, $x^4 + 1 = (x + 1)^4$. Assume now p is odd.

A fun result

Theorem

The irreducible $x^4 + 1 \in \mathbb{Z}[x]$ is reducible modulo every prime.

Proof: If $p = 2$, $x^4 + 1 = (x + 1)^4$. Assume now p is odd.

Modulo 8, p is either 1, 3, 5, 7, so 8 divides $p^2 - 1$.

A fun result

Theorem

The irreducible $x^4 + 1 \in \mathbb{Z}[x]$ is reducible modulo every prime.

Proof: If $p = 2$, $x^4 + 1 = (x + 1)^4$. Assume now p is odd.

Modulo 8, p is either 1, 3, 5, 7, so 8 divides $p^2 - 1$.

Thus $x^8 - 1$ divides $x^{p^2-1} - 1$.

A fun result

Theorem

The irreducible $x^4 + 1 \in \mathbb{Z}[x]$ is reducible modulo every prime.

Proof: If $p = 2$, $x^4 + 1 = (x + 1)^4$. Assume now p is odd.

Modulo 8, p is either 1, 3, 5, 7, so 8 divides $p^2 - 1$.

Thus $x^8 - 1$ divides $x^{p^2-1} - 1$. *[Why? Think about properties of groups of roots of unity!]*

A fun result

Theorem

The irreducible $x^4 + 1 \in \mathbb{Z}[x]$ is reducible modulo every prime.

Proof: If $p = 2$, $x^4 + 1 = (x + 1)^4$. Assume now p is odd.

Modulo 8, p is either 1, 3, 5, 7, so 8 divides $p^2 - 1$.

Thus $x^8 - 1$ divides $x^{p^2-1} - 1$. *[Why? Think about properties of groups of roots of unity!]*

We have: $x^4 + 1 | x^8 - 1 | x^{p^2-1} - 1 | x^{p^2} - x$. Thus all roots of $x^4 + 1$ are roots of $x^{p^2} - x$, so are in $\mathbb{F}_{p^2}$.

A fun result

Theorem

The irreducible $x^4 + 1 \in \mathbb{Z}[x]$ is reducible modulo every prime.

Proof: If $p = 2$, $x^4 + 1 = (x+1)^4$. Assume now p is odd.

Modulo 8, p is either 1, 3, 5, 7, so 8 divides $p^2 - 1$.

Thus $x^8 - 1$ divides $x^{p^2-1} - 1$. *[Why? Think about properties of groups of roots of unity!]*

We have: $x^4 + 1 | x^8 - 1 | x^{p^2-1} - 1 | x^{p^2} - x$. Thus all roots of $x^4 + 1$ are roots of $x^{p^2} - x$, so are in $\mathbb{F}_{p^2}$.

If $x^4 + 1$ is irreducible over $\mathbb{F}_p[x]$, that would mean it generates an extension K of degree 4, with $\mathbb{F}_p \subseteq K \subseteq \mathbb{F}_{p^2}$. However $\mathbb{F}_{p^2}/\mathbb{F}_p$ has degree 2, contradiction.

Summary

- Fundamental theorem, part II: If K/F is Galois and E is an intermediate field, E/F is Galois if and only if $\mathrm{Aut}(K/E)$ is normal in $\mathrm{Aut}(K/F)$. In this case, $\mathrm{Aut}(E/F) \cong \mathrm{Aut}(K/F)/\mathrm{Aut}(K/E)$.

Summary

- Fundamental theorem, part II: If K/F is Galois and E is an intermediate field, E/F is Galois if and only if $\mathrm{Aut}(K/E)$ is normal in $\mathrm{Aut}(K/F)$. In this case, $\mathrm{Aut}(E/F) \cong \mathrm{Aut}(K/F)/\mathrm{Aut}(K/E)$.
- The Galois group of $\mathbb{F}_{p^n}/\mathbb{F}_p$ is cyclic of order n, generated by the Frobenius map. Thus $\mathbb{F}_{p^d}$ is the only subfield of $\mathbb{F}_{p^n}$, for d a divisor of n.