Math-123: Finite fields, Composite extensions

Sebastien Vasey

Harvard University

April 10, 2020

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 $|\text{Aut}(K/F)| = [K : F] = n$.

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 $a \in F$.

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: $\text{Aut}(K/F) \cong \mathbb{Z}/n\mathbb{Z}$.

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: $\mathrm{Aut}(K/F) \cong \mathbb{Z}/n\mathbb{Z}$.

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.

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.

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 roots 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 roots 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 roots 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 roots 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 $x^4 + 1$ were irreducible over $\mathbb{F}_p[x]$, then it would generate 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.

Composite extensions

Theorem

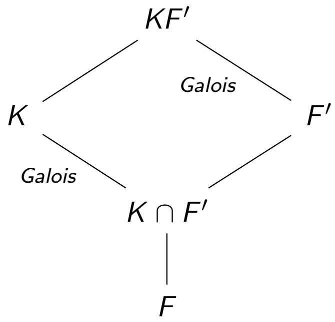
Suppose K/F is a Galois extension and F'/F is any extension. Then KF'/F' is a Galois extension.

Composite extensions

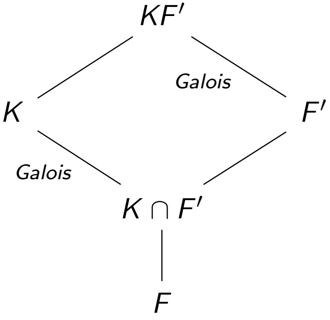
Theorem

Suppose K/F is a Galois extension and F'/F is any extension.
Then KF'/F' is a Galois extension.
The Galois group is $\mathrm{Aut}(KF'/F') \cong \mathrm{Aut}(K/K \cap F')$.

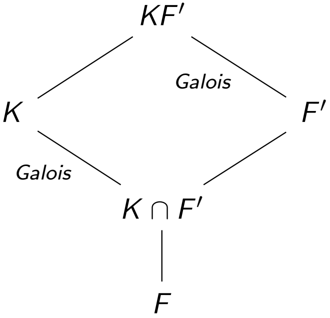
Galois group of composite extensions: picture



$\mathrm{Aut}(K/(K \cap F')) \cong \mathrm{Aut}(KF'/F')$

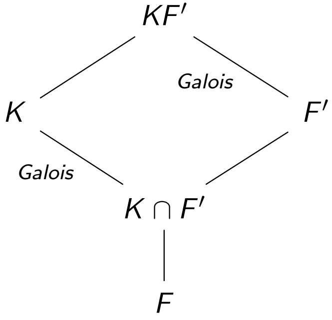


Proof of Theorem: K/F is the splitting field of a separable $f(x) \in F[x]$. Thus KF'/F' is the splitting field of $f(x)$, seen as a poly in $F'[x]$. Thus KF'/F' is Galois.



Proof of Theorem: K/F is the splitting field of a separable $f(x) \in F[x]$. Thus KF'/F' is the splitting field of $f(x)$, seen as a poly in $F'[x]$. Thus KF'/F' is Galois.

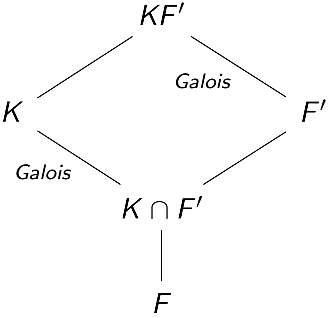
Define a map $\phi : \text{Aut}(KF'/F') \to \text{Aut}(K/F)$ by $\phi(\sigma) = \sigma \restriction K$.



Proof of Theorem: K/F is the splitting field of a separable $f(x) \in F[x]$. Thus KF'/F' is the splitting field of $f(x)$, seen as a poly in $F'[x]$. Thus KF'/F' is Galois.

Define a map $\phi : \mathrm{Aut}(KF'/F') \to \mathrm{Aut}(K/F)$ by $\phi(\sigma) = \sigma \restriction K$.

Since K/F is a Galois extension, it is a well-defined map (seen last time).

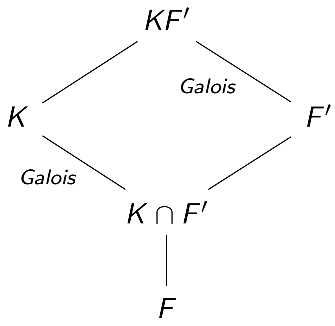


Proof of Theorem: K/F is the splitting field of a separable $f(x) \in F[x]$. Thus KF'/F' is the splitting field of $f(x)$, seen as a poly in $F'[x]$. Thus KF'/F' is Galois.

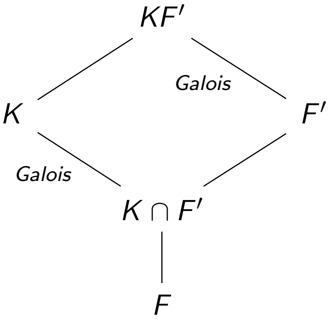
Define a map $\phi : \mathrm{Aut}(KF'/F') \to \mathrm{Aut}(K/F)$ by $\phi(\sigma) = \sigma \restriction K$.

Since K/F is a Galois extension, it is a well-defined map (seen last time).

The elements of the kernel fix both K and F', hence fix KF'. Thus the kernel is trivial: ϕ is injective.

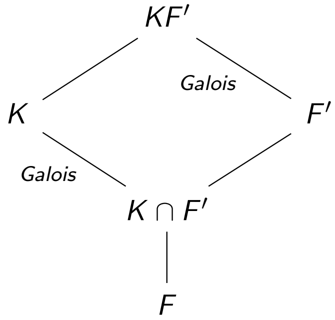


$\phi : \mathrm{Aut}(KF'/F') \to \mathrm{Aut}(K/F)$, $\phi(\sigma) = \sigma \restriction K$ is injective.



$\phi : \text{Aut}(KF'/F') \to \text{Aut}(K/F)$, $\phi(\sigma) = \sigma \restriction K$ is injective.

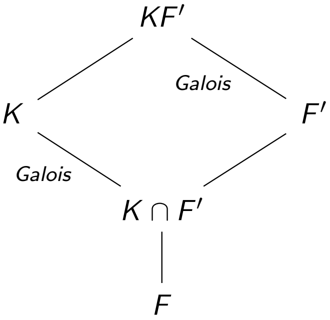
Let H be the image of ϕ. Let K_H be the fixed field of H (in K/F). Every element of H fixes F', so $F' \cap K \subseteq K_H$.



$\phi : \text{Aut}(KF'/F') \to \text{Aut}(K/F)$, $\phi(\sigma) = \sigma \restriction K$ is injective.

Let H be the image of ϕ. Let K_H be the fixed field of H (in K/F). Every element of H fixes F', so $F' \cap K \subseteq K_H$.

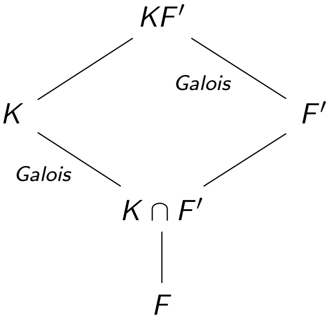
$K_H F'$ is fixed by $\text{Aut}(KF'/F')$:



$\phi : \mathrm{Aut}(KF'/F') \to \mathrm{Aut}(K/F)$, $\phi(\sigma) = \sigma \restriction K$ is injective.

Let H be the image of ϕ. Let K_H be the fixed field of H (in K/F). Every element of H fixes F', so $F' \cap K \subseteq K_H$.

$K_H F'$ is fixed by $\mathrm{Aut}(KF'/F')$: if $\sigma \in \mathrm{Aut}(KF'/F')$, then σ fixes F', and $\sigma \restriction K$ is in the image of ϕ, so fixes K_H.

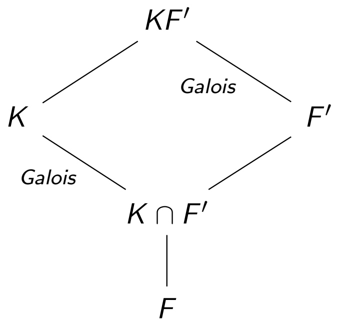


$\phi : \mathrm{Aut}(KF'/F') \to \mathrm{Aut}(K/F)$, $\phi(\sigma) = \sigma \restriction K$ is injective.

Let H be the image of ϕ. Let K_H be the fixed field of H (in K/F). Every element of H fixes F', so $F' \cap K \subseteq K_H$.

$K_H F'$ is fixed by $\mathrm{Aut}(KF'/F')$: if $\sigma \in \mathrm{Aut}(KF'/F')$, then σ fixes F', and $\sigma \restriction K$ is in the image of ϕ, so fixes K_H.

So we have $K_H \subseteq F'$, so $K_H = K \cap F'$.



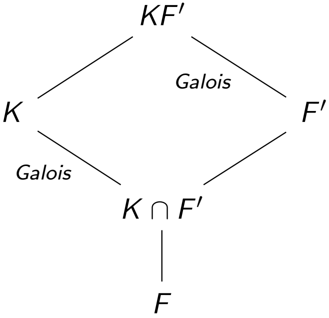
$\phi : \mathrm{Aut}(KF'/F') \to \mathrm{Aut}(K/F)$, $\phi(\sigma) = \sigma \restriction K$ is injective.

Let H be the image of ϕ. Let K_H be the fixed field of H (in K/F). Every element of H fixes F', so $F' \cap K \subseteq K_H$.

$K_H F'$ is fixed by $\mathrm{Aut}(KF'/F')$: if $\sigma \in \mathrm{Aut}(KF'/F')$, then σ fixes F', and $\sigma \restriction K$ is in the image of ϕ, so fixes K_H.

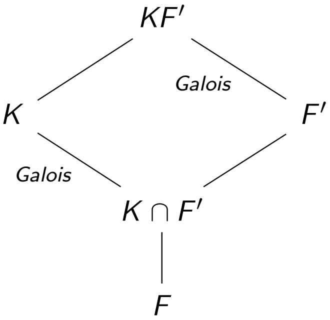
So we have $K_H \subseteq F'$, so $K_H = K \cap F'$.

Thus $H = \mathrm{Aut}(K/K \cap F')$, and we are done (first iso theorem).



Corollary

$$[KF' : F] = \frac{[K : F][F' : F]}{[K \cap F' : F]}$$



Corollary

$$[KF' : F] = \frac{[K : F][F' : F]}{[K \cap F' : F]}$$

Proof.

$[KF' : F] = [KF' : F'][F' : F] = [K : K \cap F'][F' : F]$. □

Corollary

Let K_1/F, K_2/F be Galois extensions. Then:

Corollary

Let K_1/F, K_2/F be Galois extensions. Then:

1. $(K_1 \cap K_2)/F$ is Galois.

Corollary

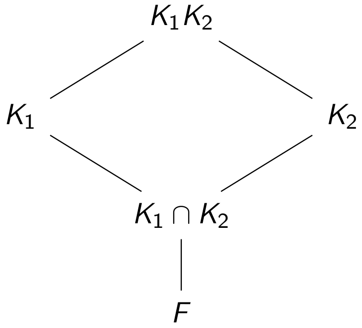
Let K_1/F, K_2/F be Galois extensions. Then:

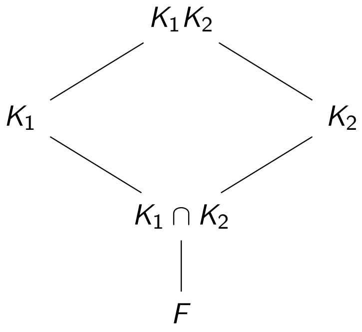
1. $(K_1 \cap K_2)/F$ is Galois.
2. K_1K_2/F is Galois, with Galois group isomorphic to the subgroup of $\mathrm{Aut}(K_1/F) \times \mathrm{Aut}(K_2/F)$ consisting of pairs (σ_1, σ_2) agreeing on $K_1 \cap K_2$.

Corollary

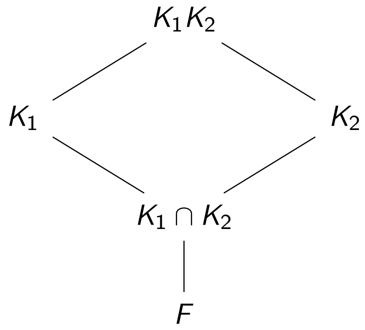
Let K_1/F, K_2/F be Galois extensions. Then:

1. $(K_1 \cap K_2)/F$ is Galois.
2. K_1K_2/F is Galois, with Galois group isomorphic to the subgroup of $\mathrm{Aut}(K_1/F) \times \mathrm{Aut}(K_2/F)$ consisting of pairs (σ_1, σ_2) agreeing on $K_1 \cap K_2$.



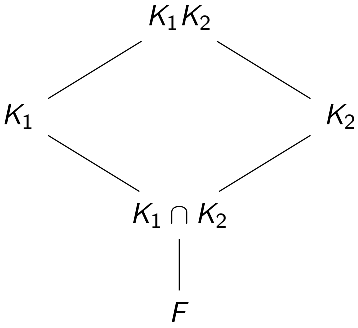


Proof that $(K_1 \cap K_2)/F$ **is Galois**: Let $p(x) \in F[x]$ be irreducible with a root α in $K_1 \cap K_2$.

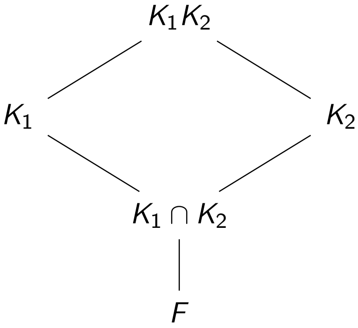


Proof that $(K_1 \cap K_2)/F$ is Galois: Let $p(x) \in F[x]$ be irreducible with a root α in $K_1 \cap K_2$.

All the roots of $p(x)$ lie in K_1 *and* in K_2 (characterization of Galois extensions). Thus all the roots of $p(x)$ lie in $K_1 \cap K_2$. Thus $K_1 \cap K_2/F$ is Galois.

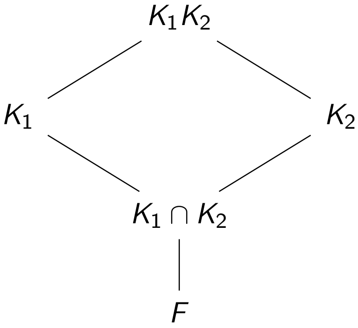


Proof that $(K_1K_2)/F$ **is Galois**: Say K_1/F is the splitting field of a separable $f_1(x)$, K_2/F is the splitting field of a separable $f_2(x)$.

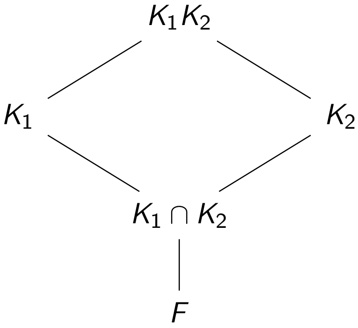


Proof that $(K_1K_2)/F$ is Galois: Say K_1/F is the splitting field of a separable $f_1(x)$, K_2/F is the splitting field of a separable $f_2(x)$.

Then K_1K_2 is the splitting field of $f_1(x)f_2(x)$. Removing repeated irreducible factors, we get that K_1K_2 is the splitting field of a separable polynomial.

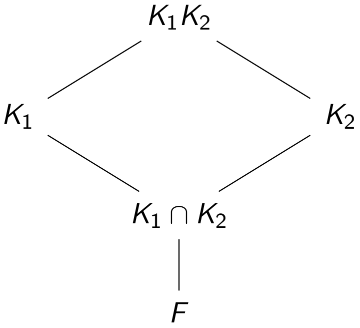


Description of the Galois group of K_1K_2/F: Consider $\phi : \mathrm{Aut}(K_1K_2/F) \to \mathrm{Aut}(K_1/F) \times \mathrm{Aut}(K_2/F)$ given by $\phi(\sigma) = (\sigma \restriction K_1, \sigma \restriction K_2)$.



Description of the Galois group of K_1K_2/F: Consider $\phi : \mathrm{Aut}(K_1K_2/F) \to \mathrm{Aut}(K_1/F) \times \mathrm{Aut}(K_2/F)$ given by $\phi(\sigma) = (\sigma \restriction K_1, \sigma \restriction K_2)$.

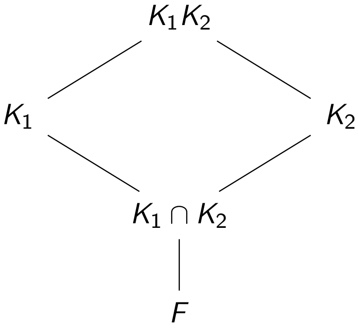
The kernel is trivial, so ϕ is injective.



Description of the Galois group of K_1K_2/F: Consider $\phi : \mathrm{Aut}(K_1K_2/F) \to \mathrm{Aut}(K_1/F) \times \mathrm{Aut}(K_2/F)$ given by $\phi(\sigma) = (\sigma \upharpoonright K_1, \sigma \upharpoonright K_2)$.

The kernel is trivial, so ϕ is injective.

Let H be the subgroup of $\mathrm{Aut}(K_1/F) \times \mathrm{Aut}(K_2/F)$ of all (σ_1, σ_2) that agree on $K_1 \cap K_2$. The image of ϕ is contained in H.

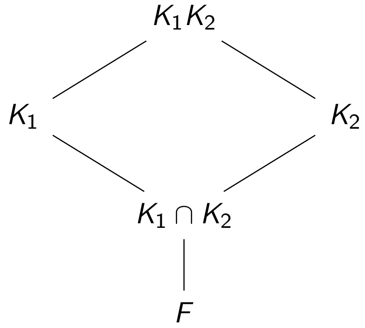


Description of the Galois group of K_1K_2/F: Consider $\phi : \mathrm{Aut}(K_1K_2/F) \to \mathrm{Aut}(K_1/F) \times \mathrm{Aut}(K_2/F)$ given by $\phi(\sigma) = (\sigma \restriction K_1, \sigma \restriction K_2)$.

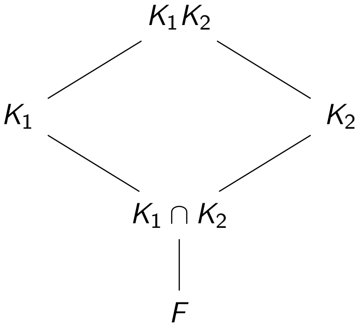
The kernel is trivial, so ϕ is injective.

Let H be the subgroup of $\mathrm{Aut}(K_1/F) \times \mathrm{Aut}(K_2/F)$ of all (σ_1, σ_2) that agree on $K_1 \cap K_2$. The image of ϕ is contained in H.

We will show that $|H| = |\mathrm{Aut}(K_1K_2/F)|$, so the image has to be all of H.

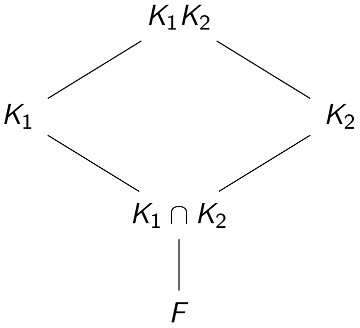


H is the subgroup of $\mathrm{Aut}(K_1/F) \times \mathrm{Aut}(K_2/F)$ of all (σ_1, σ_2) that agree on $K_1 \cap K_2$.



H is the subgroup of $\mathrm{Aut}(K_1/F) \times \mathrm{Aut}(K_2/F)$ of all (σ_1, σ_2) that agree on $K_1 \cap K_2$.

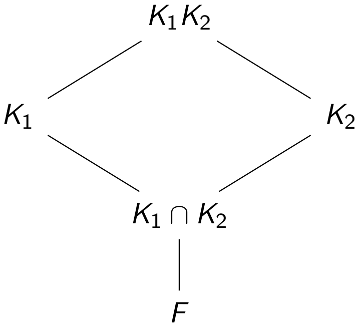
If $\sigma_1 \in \mathrm{Aut}(K_1/F)$, how many $\sigma_2 \in \mathrm{Aut}(K_2/F)$ are there so that $(\sigma_1, \sigma_2) \in H$?



H is the subgroup of $\mathrm{Aut}(K_1/F) \times \mathrm{Aut}(K_2/F)$ of all (σ_1, σ_2) that agree on $K_1 \cap K_2$.

If $\sigma_1 \in \mathrm{Aut}(K_1/F)$, how many $\sigma_2 \in \mathrm{Aut}(K_2/F)$ are there so that $(\sigma_1, \sigma_2) \in H$?

Exactly $|\mathrm{Aut}(K_2/K_1 \cap K_2)|$ (exercise).

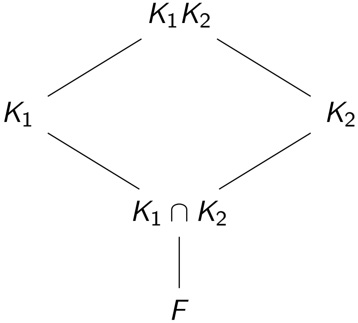


H is the subgroup of $\mathrm{Aut}(K_1/F) \times \mathrm{Aut}(K_2/F)$ of all (σ_1, σ_2) that agree on $K_1 \cap K_2$.

If $\sigma_1 \in \mathrm{Aut}(K_1/F)$, how many $\sigma_2 \in \mathrm{Aut}(K_2/F)$ are there so that $(\sigma_1, \sigma_2) \in H$?

Exactly $|\mathrm{Aut}(K_2/K_1 \cap K_2)|$ (exercise).

$|H| = |\mathrm{Aut}(K_1/F)||\mathrm{Aut}(K_2/K_1 \cap K_2)| = |\mathrm{Aut}(K_1/F)|\frac{|\mathrm{Aut}(K_2/F)|}{|\mathrm{Aut}(K_1 \cap K_2/F)|}$.



H is the subgroup of $\mathrm{Aut}(K_1/F) \times \mathrm{Aut}(K_2/F)$ of all (σ_1, σ_2) that agree on $K_1 \cap K_2$.

If $\sigma_1 \in \mathrm{Aut}(K_1/F)$, how many $\sigma_2 \in \mathrm{Aut}(K_2/F)$ are there so that $(\sigma_1, \sigma_2) \in H$?

Exactly $|\mathrm{Aut}(K_2/K_1 \cap K_2)|$ (exercise).

$|H| = |\mathrm{Aut}(K_1/F)||\mathrm{Aut}(K_2/K_1 \cap K_2)| = |\mathrm{Aut}(K_1/F)|\frac{|\mathrm{Aut}(K_2/F)|}{|\mathrm{Aut}(K_1 \cap K_2/F)|}$.

Using the previous corollary, $|H| = [K_1K_2 : F]$, as desired.

Corollary

Let K_1/F, K_2/F be Galois extensions. If $K_1 \cap K_2 = F$, then $\mathrm{Aut}(K_1 K_2/F) \cong \mathrm{Aut}(K_1/F) \times \mathrm{Aut}(K_2/F)$.

Corollary

Let K_1/F, K_2/F be Galois extensions. If $K_1 \cap K_2 = F$, then $\mathrm{Aut}(K_1K_2/F) \cong \mathrm{Aut}(K_1/F) \times \mathrm{Aut}(K_2/F)$.

For example: take $F = \mathbb{Q}$, $K_1 = \mathbb{Q}(\sqrt{2})$,$K_2 = \mathbb{Q}(\sqrt{3})$.

Corollary

Let K_1/F, K_2/F be Galois extensions. If $K_1 \cap K_2 = F$, then $\mathrm{Aut}(K_1K_2/F) \cong \mathrm{Aut}(K_1/F) \times \mathrm{Aut}(K_2/F)$.

For example: take $F = \mathbb{Q}$, $K_1 = \mathbb{Q}(\sqrt{2})$,$K_2 = \mathbb{Q}(\sqrt{3})$.

Each extension is Galois, with Galois group Z_2 $(= \mathbb{Z}/2\mathbb{Z})$.

Corollary

Let K_1/F, K_2/F be Galois extensions. If $K_1 \cap K_2 = F$, then $\mathrm{Aut}(K_1K_2/F) \cong \mathrm{Aut}(K_1/F) \times \mathrm{Aut}(K_2/F)$.

For example: take $F = \mathbb{Q}$, $K_1 = \mathbb{Q}(\sqrt{2})$,$K_2 = \mathbb{Q}(\sqrt{3})$.

Each extension is Galois, with Galois group Z_2 $(= \mathbb{Z}/2\mathbb{Z})$.

We know $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, so $K_1 \neq K_2$.

Corollary

Let K_1/F, K_2/F be Galois extensions. If $K_1 \cap K_2 = F$, then $\text{Aut}(K_1K_2/F) \cong \text{Aut}(K_1/F) \times \text{Aut}(K_2/F)$.

For example: take $F = \mathbb{Q}$, $K_1 = \mathbb{Q}(\sqrt{2})$,$K_2 = \mathbb{Q}(\sqrt{3})$.

Each extension is Galois, with Galois group Z_2 ($= \mathbb{Z}/2\mathbb{Z}$).

We know $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, so $K_1 \neq K_2$.

Thus $F \subseteq K_1 \cap K_2 \subsetneq K_1$. By the Galois correspondence (or just looking at degrees), $F = K_1 \cap K_2$.

Corollary

Let K_1/F, K_2/F be Galois extensions. If $K_1 \cap K_2 = F$, then $\mathrm{Aut}(K_1K_2/F) \cong \mathrm{Aut}(K_1/F) \times \mathrm{Aut}(K_2/F)$.

For example: take $F = \mathbb{Q}$, $K_1 = \mathbb{Q}(\sqrt{2})$,$K_2 = \mathbb{Q}(\sqrt{3})$.

Each extension is Galois, with Galois group Z_2 $(= \mathbb{Z}/2\mathbb{Z})$.

We know $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, so $K_1 \neq K_2$.

Thus $F \subseteq K_1 \cap K_2 \subsetneq K_1$. By the Galois correspondence (or just looking at degrees), $F = K_1 \cap K_2$.

So $\mathrm{Aut}(K_1K_2/F) = \mathrm{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) \cong Z_2 \times Z_2$.

Separable extensions

Definition

An extension E/F is *separable* if every element in E is the root of a separable polynomial in $F[x]$.

Separable extensions

Definition

An extension E/F is *separable* if every element in E is the root of a separable polynomial in $F[x]$.

Note: if F has characteristic zero (or more generally is perfect), then any irreducible polynomial is separable.

Separable extensions

Definition

An extension E/F is *separable* if every element in E is the root of a separable polynomial in $F[x]$.

Note: if F has characteristic zero (or more generally is perfect), then any irreducible polynomial is separable.

Thus *any algebraic extension of a perfect field is separable.*

Corollary

If E/F is any finite separable extension, then E is contained in an extension K which is Galois over F, and is minimal (no proper subfield of K containing E is Galois over F).

Corollary

If E/F is any finite separable extension, then E is contained in an extension K which is Galois over F, and is minimal (no proper subfield of K containing E is Galois over F).

Proof.

Let $f_1(x), f_2(x), \ldots, f_n(x)$ be the minimal polynomials for a basis of E/F (they are separable).

Corollary

If E/F is any finite separable extension, then E is contained in an extension K which is Galois over F, and is minimal (no proper subfield of K containing E is Galois over F).

Proof.

Let $f_1(x), f_2(x), \ldots, f_n(x)$ be the minimal polynomials for a basis of E/F (they are separable).
Let K_1/F, K_2/F, ..., K_n/F be the splitting fields. They are Galois extensions.

Corollary

If E/F is any finite separable extension, then E is contained in an extension K which is Galois over F, and is minimal (no proper subfield of K containing E is Galois over F).

Proof.

Let $f_1(x), f_2(x), \ldots, f_n(x)$ be the minimal polynomials for a basis of E/F (they are separable).
Let K_1/F, K_2/F, ..., K_n/F be the splitting fields. They are Galois extensions.
So $K_1 K_2 \ldots K_n/F$ is a Galois extension containing E.

Corollary

If E/F is any finite separable extension, then E is contained in an extension K which is Galois over F, and is minimal (no proper subfield of K containing E is Galois over F).

Proof.

Let $f_1(x), f_2(x), \ldots, f_n(x)$ be the minimal polynomials for a basis of E/F (they are separable).
Let K_1/F, K_2/F, ..., K_n/F be the splitting fields. They are Galois extensions.
So $K_1K_2\ldots K_n/F$ is a Galois extension containing E.
It has only finitely-many subfields, since the Galois group is finite.

Corollary

If E/F is any finite separable extension, then E is contained in an extension K which is Galois over F, and is minimal (no proper subfield of K containing E is Galois over F).

Proof.

Let $f_1(x), f_2(x), \ldots, f_n(x)$ be the minimal polynomials for a basis of E/F (they are separable).
Let K_1/F, K_2/F, ..., K_n/F be the splitting fields. They are Galois extensions.
So $K_1 K_2 \ldots K_n/F$ is a Galois extension containing E.
It has only finitely-many subfields, since the Galois group is finite.
Take the intersection K of all the subfields containing E that are Galois over F.

Corollary

If E/F is any finite separable extension, then E is contained in an extension K which is Galois over F, and is minimal (no proper subfield of K containing E is Galois over F).

Proof.

Let $f_1(x), f_2(x), \ldots, f_n(x)$ be the minimal polynomials for a basis of E/F (they are separable).
Let K_1/F, K_2/F, ..., K_n/F be the splitting fields. They are Galois extensions.
So $K_1K_2\ldots K_n/F$ is a Galois extension containing E.
It has only finitely-many subfields, since the Galois group is finite.
Take the intersection K of all the subfields containing E that are Galois over F. □

The Galois extension K is called the *Galois closure of E over F*.

Summary

- 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.

Summary

- 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.
- If K_1/F, K_2/F are Galois, then $K_1 \cap K_2/F$ and K_1K_2/F are Galois. If $K_1 \cap K_2 = F$, then the Galois group of K_1K_2/F is the product of the Galois groups of K_1/F and K_2/F.

Summary

- 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.
- If K_1/F, K_2/F are Galois, then $K_1 \cap K_2/F$ and K_1K_2/F are Galois. If $K_1 \cap K_2 = F$, then the Galois group of K_1K_2/F is the product of the Galois groups of K_1/F and K_2/F.
- If E/F is any finite separable extension, then there is a minimal extension K/E which is Galois over F, called the *Galois closure* of E over F.