M3P11 Galois Theory

Lectured by Prof Alessio Corti
Typeset by David Kurniadi Angdinata

Spring 2019

Contents

0 What is Galois theory?

Lecture 1 Thursday 10/01/19

References.

- E Artin, Galois theory, 1994
- A Grothendieck and M Raynaud, Revêtements étales et groupe fondamental, 2002
- I N Herstein, Topics in algebra, 1975
- M Reid, Galois theory, 2014

Notation. If K is a field, or a ring, I denote

$$K[x] = \{a_0 + \cdots + a_n x^n \mid a_i \in K\},$$

the ring of polynomials with coefficients in K.

Example.

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.
- Quadratic fields
$$\mathbb{Q}\left(\sqrt{2}\right) = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\} = \frac{\mathbb{Q}[x]}{\langle x^2 - 2\rangle}.$$
It is also a field, since
$$\frac{1}{(a + b\sqrt{2})} = \frac{a - b\sqrt{2}}{a^2 - 2b^2}.$$
- If p is prime, $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ is a finite field. If $f(x) \in K[x]$ is irreducible, $K[x] / \langle f(x)\rangle$ is a field. For example, $x^2 - 2$. Both $\mathbb{Z}$ and $K[x]$ have a division algorithm. For example, let $[a] \in \mathbb{Z}/p\mathbb{Z}$ and $[a] \neq 0$, that is $p \mid a$. Since p is prime, $\gcd(p, a) = 1$, so there exist $x, y \in \mathbb{Z}$ such that $ax + py = 1$. Thus $[a] \cdot [x] = 1$ in $\mathbb{Z}/p\mathbb{Z}$.
- For K a field, either for all $m \in \mathbb{Z}$, $m \neq 0$ in K, so K has characteristic $ch(K) = 0$, or there exists p prime such that $m = 0$ if and only if $p \mid m$, so K has characteristic $ch(K) = p$.
- For K a field,
$$K(x) = Frac(K[x]) = \left\{\phi(x) = \frac{f(x)}{g(x)} \;\middle|\; f, g \in K[x],\ g \neq 0\right\}.$$
is also a field, the field of rational functions with coefficients in K. For example, $\mathbb{F}_p(x, Y) = \mathbb{F}_p(x)(Y)$.

Example. Consider algebraic equations in a field K.

- Let $ax^2 + bx^2 + c = 0$ for $a, b, c \in K$ be a quadratic. There is a formula
$$x = \frac{-b + \sqrt{b^2 - 4ac}}{2a}.$$
- For a cubic $y^3 + 3py + 2q = 0$,
$$y = \sqrt[3]{-q + \sqrt{q^2 + p^3}} + \sqrt[3]{-q - \sqrt{q^2 + p^3}}.$$
- There is a formula for quartic equations.
- It is a theorem that there can be no such formula for equations of degree at least five.

Galois theory deals with these easily.

Lecture 2 Friday 11/01/19

Definition 0.1. A **field homomorphism** is a function $\phi : K_1 \to K_2$ that preserves the field operations, for all $a, b \in K_1$,

$$\phi(a+b) = \phi(a) + \phi(b), \qquad \phi(ab) = \phi(a)\phi(b),$$

and $\phi(0_{K_1}) = 0_{K_2}$ and $\phi(1_{K_1}) = 1_{K_2}$.

Remark. All field homomorphisms are injective. If $a \in K_1 \setminus \{0\}$, then there exists $b \in K_1$ such that $ab = 1$, then $\phi(a)\phi(b) = 1$, so $\phi(a) \neq 0$. This easily implies ϕ is injective. If $a_1 \neq a_2$, then $a_1 - a_n \neq 0$, so $0 \neq \phi(a_1 - a_2) = \phi(a_1) - \phi(a_2)$. Then $\phi(a_1) \neq \phi(a_2)$.

We concern ourselves with field extensions $k \subset K$, and every homomorphism is an extension. Consider a field extension $k \subset K$ and $\alpha \in K$. Then $k(\alpha) \subset K$ denotes the smallest subfield of K that contains k, α. Not to be confused with $k(x)$.

Example. There are two very different cases exemplified in $\mathbb{Q} \subset \mathbb{C}$.

- $\alpha = \sqrt{2}$, $\mathbb{Q}(\sqrt{2})$.
- $\alpha = \pi$, $\mathbb{Q}(\pi)$.

Definition 0.2.

- α is **algebraic** over k if $f(\alpha) = 0$ for some $0 \neq f \in k[x]$. Otherwise we say that α is **transcendental** over k.
- The extension $k \subset K$ is **algebraic** if for all $\alpha \in K$, α is algebraic over k.

Definition 0.3. Consider a field k and $f \in k[x]$. We say that $k \subset K$ is a **splitting field** for f if

- $f(x) = a \prod_{i=1}^{n} (x - \lambda_i) \in K[x]$ for $a \in k \setminus \{0\}$, and
- $K = k(\lambda_1, \dots, \lambda_n)$.

Example.

- If $f(x) = x^2 - 2 \in \mathbb{Q}[x]$, then $K = \mathbb{Q}(\sqrt{2})$ is a splitting field for f. Indeed

$$x^2 - 2 = \left(x + \sqrt{2}\right)\left(x - \sqrt{2}\right) \in \mathbb{Q}\left(\sqrt{2}\right)[x].$$

- If $f(x) = x^2 + 2$, then $K = \mathbb{Q}(\sqrt{-2})$.
- If $f(x) = x^3 - 2$, then

$$\mathbb{Q}\left(\sqrt[3]{2}\right) = \left\{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\right\}$$

is not a splitting field. $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$, where $\omega = \frac{-1+\sqrt{3}}{2}$, is a splitting field.

$$x^3 - 2 = \left(x - \sqrt[3]{2}\right)\left(x - \omega\sqrt[3]{2}\right)\left(x - \omega^2\sqrt[3]{2}\right).$$

Theorem 0.4 (Fundamental theorem of Galois theory)**.** *Assume characteristic zero. Let $k \subset K$ be the splitting field of $f(x) \in k[x]$. Let*

$$G = \{\sigma : K \to K \mid \sigma \text{ field automorphism}, \ \sigma \mid_k = id_k\}.$$

*We call this group the **Galois group**. There is a one-to-one correspondence*

$$\begin{array}{rcl} \{k \subset K_1 \subset K \mid K_1 \text{ subfield}\} & \leftrightarrow & \{H \leq G \mid H \text{ subgroup}\} \\ K_1 & \mapsto & \{\sigma \in G \mid \forall \lambda \in K_1, \ \sigma(\lambda) = \lambda\} \\ \{\lambda \in K \mid \forall \sigma \in H, \ \sigma(\lambda) = \lambda\} & \leftarrow\!\shortmid & H \leq G \end{array}.$$

Why is this cool? Fields are hard, groups are easy. We will see that there is a good formula for the roots of $f(x)$ if and only if G is a soluble group.

Lecture 3 Tuesday 15/01/19

Example. Let $\deg(f) = 2$ and $f(x) = x^2 + 2Ax + B \in K[x]$. If K already contains the roots then $L = K$ and $G = \{id\}$. Suppose K does not contain the roots. We still have quadratic formula

$$\lambda_{1,2} = -A \pm \sqrt{A^2 - B}.$$

If $\Delta = A^2 - B$ then $\sqrt{\Delta}$ does not exist in K. We must have

$$L = K\left(\sqrt{\Delta}\right) = \left\{a + b\sqrt{\Delta} \mid a, b \in K\right\}.$$

Then $K \subset L$ and

$$G = \{\sigma : L \to L \mid \sigma \mid_K = id_K\} = C_2$$

is generated by

$$\sigma : a + b\sqrt{\Delta} \mapsto a - b\sqrt{\Delta}.$$

Further specialisation is the following.

- Let $K = \mathbb{R}$ and $\Delta = -1$. Then
$$L = \mathbb{C} = \left\{a + b\sqrt{-1} \mid a, b \in \mathbb{R}\right\},$$
and $G = C_2$ is generated by
$$\sigma : a + b\sqrt{-1} \mapsto a - b\sqrt{-1},$$
complex conjugation.
- Let $K = \mathbb{Q}$ and $\Delta = 2$. Then
$$L = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\},$$
and $G = C_2$ is generated by
$$\sigma : a + b\sqrt{2} \mapsto a - b\sqrt{2}.$$

The fundamental theorem implies there does not exist

$$K \subsetneq K_1 \subsetneq K\left(\sqrt{\Delta}\right) = L.$$

Is this obvious? Consider $x \in L \setminus K$, so $x = a + b\sqrt{\Delta}$, and $b \neq 0$, and then

$$\sqrt{\Delta} = \frac{x - a}{b},$$

so $K(x) = L$.

Example. Let $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ and $L = \mathbb{Q}\left(\sqrt[3]{2}, \omega\right)$, where $\omega = \frac{-1+i\sqrt{3}}{2}$ is a solution of $x^2 + x + 1 = 0$. Then

$$\mathbb{Q}(\omega) = \mathbb{Q}\left(\sqrt{-3}\right), \qquad \mathbb{Q}\left(\sqrt[3]{2}\right) = \left\{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\right\}.$$

Remark. For any splitting field of f, there is always a natural inclusion group homomorphism

$$\rho : G \hookrightarrow S(\lambda_1, \dots, \lambda_n),$$

where $S(\lambda_1, \dots, \lambda_n)$ is the group of permutations of the roots of $f = x^n + a_1x^{n-1} + \dots + a_n$.

- If $\sigma \in G$, $f(\lambda) = 0$, so $\lambda^n + a_1\lambda^{n-1} + \dots + a_n = 0$.

$$0 = \sigma(0) = \sigma\left(\lambda^n + a_1\lambda^{n-1} + \dots + a_n\right) = \sigma(\lambda)^n + a_1\sigma(\lambda)^{n-1} + \dots + a_n.$$

- ρ is injective. If for all i, $\sigma(\lambda_i) = \lambda_i$, then $\sigma = id$ on $K(\lambda_1, \dots, \lambda_n) = L$.

The fundamental theorem and remark gives $G = \mathfrak{S}_3$.

Lecture 4 Thursday 17/01/19

Definition 0.5. $K \subset L$ is **finite** if L is finite-dimensional as a vector space over K. The **degree** of L over K is $[L : K] = \dim_K(L)$.

Two things about this.

Theorem 0.6 (Tower law)**.** *Let $K \subset L \subset F$. Then $[F : K] = [F : L][L : K]$.*

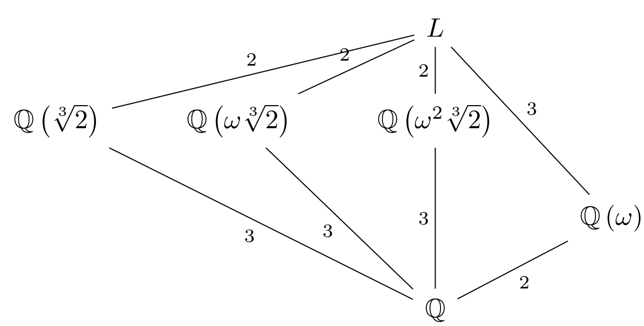
Theorem 0.7. *Suppose $f(x) \in K[x]$ is irreducible of degree $d = \deg(f)$ and $L = K(\lambda)$ where $f(\lambda) = 0$, then $[K(\lambda) : K] = d$.*

Example.

$$K = \mathbb{Q}\left(\sqrt[3]{2}\right) = \left\{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\right\}$$

is a field, and $[K : \mathbb{Q}] = 3$.

Example. Let $L = \mathbb{Q}\left(\sqrt[3]{2}, \omega\right)$ be the splitting field of $x^3 - 2$ over $\mathbb{Q}$. The lattice of subfields is



.

Then

$$\mathbb{Q}\left(\sqrt[3]{2} + \omega\right) = L, \qquad \mathbb{Q}\left(\omega^2\sqrt[3]{2}\right) \cap \mathbb{Q}\left(\omega\sqrt[3]{2}\right) = \mathbb{Q}, \qquad \mathbb{Q}\left(\sqrt[3]{2}, \omega\sqrt[3]{2}\right) = L.$$

(Exercise) What is $\left[L : \mathbb{Q}\left(\sqrt[3]{2}\right)\right]$? Note that $L = \mathbb{Q}\left(\sqrt[3]{2}\right)\left(\sqrt{-3}\right)$. Could $\sqrt{-3} \in \mathbb{Q}\left(\sqrt[3]{2}\right)$? Consider $x^2 + 3 \in \mathbb{Q}\left(\sqrt[3]{2}\right)[x]$. By the tower law,

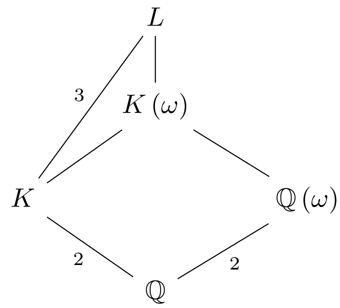
$$\begin{cases} [L : \mathbb{Q}] = [L : \mathbb{Q}(\omega)][\mathbb{Q}(\omega) : \mathbb{Q}] = 2[L : \mathbb{Q}(\omega)] & \implies 2 \mid [L : \mathbb{Q}] \\ [L : \mathbb{Q}] = \left[L : \mathbb{Q}\left(\sqrt[3]{2}\right)\right]\left[\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\right] = 3\left[L : \mathbb{Q}\left(\sqrt[3]{2}\right)\right] & \implies 3 \mid [L : \mathbb{Q}] \end{cases} \implies \quad 6 \mid [L : \mathbb{Q}].$$

- Either $x^2 + 3$ is irreducible over $\mathbb{Q}\left(\sqrt[3]{2}\right)$, so by Theorem 0.7 $\left[L : \mathbb{Q}\left(\sqrt[3]{2}\right)\right] = 2$ and $[L : \mathbb{Q}] = 6$.

- Or $x^2 + 3$ is not irreducible, so $\mathbb{Q}\left(\sqrt[3]{2}\right) = L$ and $[L : \mathbb{Q}] = 3$, a contradiction.

Are there any other fields? Claim that there are no other fields. Suppose $\mathbb{Q} \subsetneq K \subsetneq L$ is such a field. By the tower law $[K : \mathbb{Q}] = 2$ or $[K : \mathbb{Q}] = 3$.

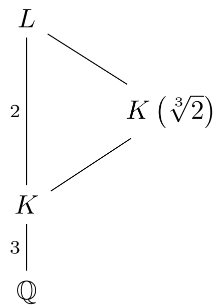
- Suppose $[K : \mathbb{Q}] = 2$.



.

  - Either $\omega \in K$, that is $\mathbb{Q}(\omega) \subset K$, so by the tower law $\mathbb{Q}(\omega) = K$.
  - Or $\omega \notin K$ gives $[K(\omega) : K] = 2$, so $[K(\omega) : \mathbb{Q}] = 4$ contradicts the tower law for $\mathbb{Q} \subset K(\omega) \subset L$.

- Suppose $[K : \mathbb{Q}] = 3$.



.

  Claim that $x^3 - 2 \in K[x]$ splits. Suppose that it were irreducible, then $\left[K\left(\sqrt[3]{2}\right) : K\right] = 3$, which contradicts the tower law for $K \subset K\left(\sqrt[3]{2}\right) \subset L$. So it has a root in K. Either $\sqrt[3]{2} \in K$, $\omega\sqrt[3]{2} \in K$, or $\omega^2\sqrt[3]{2} \in K$. Thus $\mathbb{Q}\left(\sqrt[3]{2}\right) = K$, $\mathbb{Q}\left(\omega\sqrt[3]{2}\right) = K$, or $\mathbb{Q}\left(\omega^2\sqrt[3]{2}\right) = K$.

I want to prove that

$$G = Aut_{\mathbb{Q}}(L) = \{\sigma : L \to L \mid \sigma|_{\mathbb{Q}} = id_{\mathbb{Q}}\} = \mathfrak{S}_3.$$

Lecture 5 Friday 18/01/19

Proof of Theorem 0.6. Suppose $y_1, \dots, y_m \in F$ is a basis of F as a vector space over L. Suppose $x_1, \dots, x_n \in L$ is a basis of L as a vector space over K. Claim that $\{x_i y_j\}$ is a basis of F over K.

- $\{x_i y_j\}$ generates F. Let $z \in F$. There exist $\mu_1, \dots, \mu_n \in L$ such that

  $$z = \mu_1 y_1 + \dots + \mu_n y_n. \tag{1}$$

  $\mu_j \in L$ so for all j there exists $\lambda_{ij} \in K$ such that

  $$\mu_j = x_1\lambda_{1j} + \dots + x_m\lambda_{mj}. \tag{2}$$

  Plug in (2) into (1),

  $$z = \sum_{i,j} \lambda_{ij} x_i y_j.$$

- $\{x_i y_j\}$ are linearly independent over K. Suppose there exists $\lambda_{ij} \in K$ such that

  $$0 = \sum_{i,j} \lambda_{ij} x_i y_j = \sum_j \left(\sum_i \lambda_{ij} x_i\right) y_j,$$

  so for all j, $\sum_i \lambda_{ij} x_i = 0$, so for all j and all i, $\lambda_{ij} = 0$.

$\square$

Example. To show $G = \mathfrak{S}_3$. Let $\sigma = \begin{pmatrix} 1 & 2 \end{pmatrix}$. A basis of $L/\mathbb{Q}$ is

$$1, \sqrt[3]{2}, \sqrt[3]{4}, \omega, \omega\sqrt[3]{2}, \omega\sqrt[3]{4}.$$

- $\sigma(1) = 1$.
- $\sigma\left(\sqrt[3]{2}\right) = \omega\sqrt[3]{2}$.
- $\sigma\left(\omega\sqrt[3]{2}\right) = \sqrt[3]{2}$.
- $\sigma\left(\sqrt[3]{4}\right) = \sigma\left(\sqrt[3]{2}\cdot\sqrt[3]{2}\right) = \omega\sqrt[3]{2}\cdot\omega\sqrt[3]{2} = \omega^2\sqrt[3]{4} = (-\omega-1)\sqrt[3]{4} = -\omega\sqrt[3]{4} - \sqrt[3]{4}$.
- $\sigma(\omega) = \sigma\left(\omega\sqrt[3]{2}/\sqrt[3]{2}\right) = \sigma\left(\omega\sqrt[3]{2}\right)/\sigma\left(\sqrt[3]{2}\right) = \sqrt[3]{2}/\omega\sqrt[3]{2} = 1/\omega = -1-\omega$.
- $\sigma\left(\omega\sqrt[3]{4}\right) = \sigma\left(\omega\sqrt[3]{2}\cdot\sqrt[3]{2}\right) = \sigma\left(\omega\sqrt[3]{2}\right)\cdot\sigma\left(\sqrt[3]{2}\right) = \sqrt[3]{2}\cdot\omega\sqrt[3]{2} = \omega\sqrt[3]{4}$.

Thus

$$\sigma = \begin{pmatrix} 1 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 1 \end{pmatrix}.$$

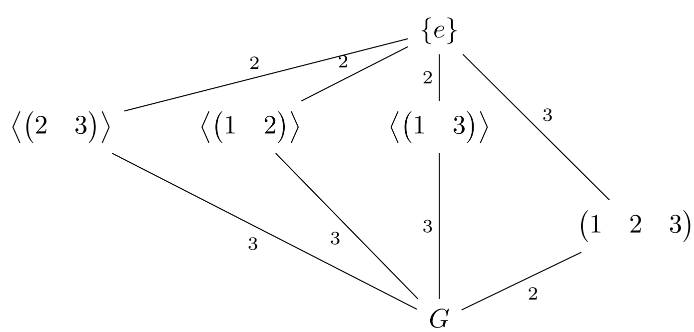
A question is if there were $\sigma \in G$ such that $\rho(\sigma) = \begin{pmatrix} 1 & 2 \end{pmatrix}$ then we have written the matrix of σ as a $\mathbb{Q}$-linear map of L in a basis. But how to check that this $\mathbb{Q}$-linear map is a field homomorphism? We know the Galois correspondence for extensions of degree two.

$$Gal_{\mathbb{Q}\left(\sqrt[3]{2}\right)}(L), Gal_{\mathbb{Q}\left(\omega^2\sqrt[3]{2}\right)}(L), Gal_{\mathbb{Q}\left(\omega\sqrt[3]{2}\right)}(L) \subset G$$

contain an element of order two, and

$$\begin{aligned} \rho : \quad Gal_{\mathbb{Q}\left(\sqrt[3]{2}\right)}(L) &\mapsto \begin{pmatrix} 2 & 3 \end{pmatrix} \\ Gal_{\mathbb{Q}\left(\omega^2\sqrt[3]{2}\right)}(L) &\mapsto \begin{pmatrix} 1 & 2 \end{pmatrix} \\ Gal_{\mathbb{Q}\left(\omega\sqrt[3]{2}\right)}(L) &\mapsto \begin{pmatrix} 1 & 3 \end{pmatrix}. \end{aligned}$$

The lattice of subgroups is



$\mathbb{Q}(\omega)/\mathbb{Q}$ is the splitting field of x^2+x+1 and of x^2+3.

We can learn the following. Let $k \subset L$ be a splitting field. Consider $k \subset K \subset L$. Then $K \subset L$ is also a splitting field. The corresponding $H \leq G$ is the Galois group $Gal_K(L)$. On the other hand $k \subset K$ is not always a splitting field. It is a splitting field if and only if the corresponding $H \leq G$ is a normal subgroup and in that case $Gal_k(K) = G/H$.

1 Elementary facts

Lecture 6 Tuesday 22/01/19

Let $K \subset L$ and $a \in L$. The **evaluation homomorphism**

$$\begin{array}{cccc} e_a : & K[x] & \to & K[a] \subset L \\ & f(x) & \mapsto & f(a) \end{array}$$

is a surjective ring homomorphism, where $K[a]$ is the smallest subring of L containing K and a.

Definition 1.1. $f(x) = a_0 x^n + \dots + a_n \in K[x]$ is **monic** if $a_0 = 1$.

Lemma 1.2.

- *If a is transcendental, e_a is injective and it extends to $\widetilde{e_a} : K(x) \to K(a)$, by*

$$\begin{tikzcd} K(x) \arrow[dr, "\widetilde{e_a}"] & \\ \cup & \\ K[x] \arrow[r, "e_a"'] & L \end{tikzcd} .$$

- *If a is algebraic, then $Ker(e_a) = \langle f_a \rangle$, where $f_a \in K[x]$ is irreducible, or prime, and unique if monic, then called the minimal polynomial of $a \in L/K$. In this case*

$$\begin{tikzcd} K[x] \arrow[r, "e_a"] & K[a] \cong K(a) \subset L \\ \cup & \\ \dfrac{K[x]}{\langle f_a \rangle} \arrow[uur, "\sim", "{[e_a]}"'] & \end{tikzcd} .$$

Proof. There is nothing to prove. $\square$

Remark. Let $g(x) \in K[x]$ and $g(a) \neq 0$. Claim that $1/g(a) \in K[a]$. Indeed $\gcd(f, g) = 1$ in $K[x]$ and $f \nmid g$. There exists $\phi, \psi \in K[x]$ such that $f\phi + g\psi = 1$ and $g(a)\psi(a) = 1$. All of this is saying

- $K[a] \cong K(a)$, and
- $K[x] / \langle f_a \rangle \cong K(a)$.

Let

$$Em_K(K(a), F) = \{\sigma : K(a) \to F \mid \sigma \text{ field homomorphism}, \ \sigma_K = id_K\},$$

where

$$\begin{tikzcd} & K(a) \arrow[dd, dotted, "\sigma"] \\ k \arrow[ur, hook] \arrow[dr, hook] & \\ & F \end{tikzcd} .$$

Corollary 1.3. *For $K \subset L$ and $a \in L$ algebraic over K,*

- $[K(a) : K] = \deg(f_a)$, *and*
- *If $K \subset F$ is an extension,*
$$Em_K(K(a), F) = \{b \in F \mid f_a(b) = 0\}.$$

Proof. Since $K(a) = K[a]$, $[K(a) : K] = \dim_K(K(a)) = \dim_K[K(a)]$. Suppose

$$f(x) = x^n + \mu_1 x^{n-1} + \dots + \mu_n \in K[x]$$

is the minimal polynomial of a over K. Claim that $1, \dots, a^{n-1}$ is a basis of $K[a]$ over K.

- The set generates $K[a]$. Let $c \in K[a]$. There exists $g \in K[x]$ such that $g(a) = c$. Long division gives

  $$g(x) = f(x) q(x) + r(x), \qquad m = \deg(r(x)) < n.$$

  Then $r(x) = \lambda_0 + \dots + \lambda_m x^m$ and $g(a) = r(a) = \lambda_0 + \dots + \lambda_m a^m$.

- The set is linearly independent, otherwise there exists

  $$g(x) = \lambda_0 + \dots + \lambda_{n-1} x^{n-1} \in K[x], g(a) = 0,$$

  and f was not the minimal polynomial.

$\sigma(a)$ is a root of f, since applying σ to $f(a) = 0$ gives

$$0 = \sigma\left(a^n + \mu_1 a^{n-1} + \dots + \mu_n\right) = \sigma(a)^n + \mu_1^{n-1} \sigma(a)^{n-1} + \dots + \mu_n = f(\sigma(a)).$$

Vice versa, if $b \in F$ is a root of f,

$$K(b) \xleftarrow[\sim]{[e_b]} \frac{K[x]}{\langle f \rangle} \xrightarrow[\sim]{[e_a]} K(a),$$

then $\sigma = [e_b][e_a]^{-1}$. Thus there is a one-to-one correspondence

$$\begin{array}{rcl} Em_K(K(a), F) & \leftrightarrow & \{b \in F \mid f(b) = 0\} \\ \sigma & \mapsto & \sigma(a) \\ [e_b][e_a]^{-1} & \leftarrow\!\shortmid & b \end{array}.$$

□

Corollary 1.4. *Let K be a field and $f \in K[x]$. Then there exists $K \subset L$ such that f has a root in L.*

Proof. Take g a prime factor of f. Take $L = K[x] / \langle g \rangle$. In here $a = [x]$ is a root of g hence a root of f. □

Lecture 7 Thursday 24/01/19

From now on in this course, we study field extensions $K \subset L$, always assumed to be finite, so $[L : K] = \dim_K(L) < \infty$.

Remark. $K \subset L$ is finite if and only if

- it is algebraic, that is for all $a \in L$, a is algebraic over K, and
- it is finitely generated, that is there exist $a_1, \dots, a_m \in L$ such that $L = K(a_1, \dots, a_m)$.

An important point of view is that we study all possible field homomorphisms

$$Em(K, L) = \{\sigma : K \to L \mid \sigma \text{ field homomorphism}\}.$$

Often there is a field $k \subset K, L$ in the background which we want to stay fixed, so

$$Em_k(K, L) = \{\sigma : K \to L \mid \sigma \text{ field homomorphism}, \ \sigma|_k = id_k\}.$$

Example. Let $K = \mathbb{Q}\left(\sqrt[3]{2}\right)$. The minimal polynomial of $\sqrt[3]{2}$ is $x^3 - 2$. Let $L = \mathbb{Q}\left(\sqrt[3]{2}, \sqrt{-3}\right)$ be the splitting field of $x^3 - 2$. Then

$$Em_{\mathbb{Q}}(K, L) = Em(K, L) = \left\{\text{roots of } x^3 - 2 \text{ in } L\right\} = \left\{\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\right\}.$$

Remark. Suppose $k \subset K$. $Em_k(K, K) = G = Gal_k(K)$. Indeed every k-homomorphism $\sigma : K \to K$ is automatically invertible. We know σ is injective. σ is also surjective because σ is a k-linear endomorphism of a finite-dimensional k-vector space.

2 Axiomatics

Proposition 2.1. *Fix $k \subset K$ and $k \subset L$. Then $\# Em_k(K, L) \le [K : k]$.*

Proof.

Special case. If $K = k(a)$, let $f(x) \in k[x]$ be the minimal polynomial of a. Then $Em_k(k(a), L)$ is the roots of $f(x)$ in L, so

$$\# Em_k(K, L) = \# \{\text{roots}\} \le \deg(f) = [k(a) : k],$$

as proved last time.

General case. If $k = K$, nothing to do. Otherwise choose $a \in K \setminus k$.

$$\begin{tikzcd} & & L \\ k \arrow[r, phantom, "\subset"] & k(a) \arrow[ur, dotted, "y"] \arrow[r, phantom, "\subset"] & K \arrow[u, dotted] \end{tikzcd}.$$

Consider the restriction map

$$\rho : Em_k(K, L) \to Em_k(k(a), L).$$

Fix $y \in Em_k(k(a), L)$. Then

$$\rho^{-1}(y) = \left\{x : K \to L \mid x|_{k(a)} = id_{k(a)}\right\}.$$

Since $[k(a) : k] > 1$, by the tower law $[K : k(a)] < [K : k]$. By induction we may assume $\#\rho^{-1}(y) \le [K : k(a)]$. So

$$\# Em_k(K, L) \le \sum_{y \in Em_k(k(a), L)} \#\rho^{-1}(y) \le [k(a) : k][K : k(a)] = [K : k],$$

by the tower law.

∎

Proposition 2.2. *Suppose given two field extensions $k \subset K$ and $k \subset L$. Then there is a non-unique bigger common field*

$$\begin{tikzcd} & K \arrow[dr, hook, "\phi_1"] & \\ k \arrow[ur, hook, "\sigma_1"] \arrow[dr, hook, "\sigma_2"'] & & \Omega \\ & L \arrow[ur, hook, "\phi_2"'] & \end{tikzcd}$$

that contains both.

Remark.

- More formally, suppose given $\sigma_1 \in Em(k, K)$ and $\sigma_2 \in Em(k, L)$, then there exists Ω, $\phi_1 \in Em(K, \Omega)$, and $\phi_2 \in Em(L, \Omega)$ such that $\phi_1 \circ \sigma_1 = \phi_2 \circ \sigma_2$.
- I never said that Ω is unique. For example, let $K = \mathbb{Q}\left(\sqrt[3]{2}\right)$ and $L = \mathbb{Q}\left(\sqrt[3]{2}\right)$. One choice is $\Omega = k$. Another choice is $\Omega = \mathbb{Q}\left(\sqrt[3]{2}, \sqrt{-3}\right)$, where

$$\begin{tikzcd} & \mathbb{Q}\left(\sqrt[3]{2}\right) \arrow[dr, hook, "\phi_1 : \sqrt[3]{2} \mapsto \sqrt[3]{2}"] & \\ \mathbb{Q} \arrow[ur, hook, "\sigma"] \arrow[dr, hook, "\sigma"'] & & \mathbb{Q}\left(\sqrt[3]{2}, \sqrt{-3}\right) \\ & \mathbb{Q}\left(\sqrt[3]{2}\right) \arrow[ur, hook, "\phi_2 : \sqrt[3]{2} \mapsto \omega \sqrt[3]{2}"'] & \end{tikzcd}.$$

Another more precise way to state this is there exists $k \subset \Omega$ such that $Em_k(K, \Omega)$ and $Em_k(L, \Omega)$ are both non-empty.

Lecture 8 Friday 25/01/19

Proof.

Special case. If $K = k(a)$, let $f(x) \in k[x]$ be the minimal polynomial of a over k. Let $L \subset E$ be such that $f(x) \in L[x]$ has a root $\alpha \in E$. Then there exists $\sigma \in Em_k(k(a), E)$ such that $\sigma(a) = \alpha$.

$$\begin{tikzcd}
& k(a) \arrow[dr, dotted, "\sigma"] & \\
k \arrow[ur, hook] \arrow[dr, hook] & & E \\
& L \arrow[ur, hook] &
\end{tikzcd}.$$

General case. By induction on $[K : k]$. If $[K : k] = 1$, take $\Omega = L$. If $[K : k] > 1$, take $a \in K \setminus k$.

$$\begin{tikzcd}
& & K \arrow[dr, hook] & \\
& k(a) \arrow[ur, hook] \arrow[dr, hook] & & \Omega \\
k \arrow[ur, hook] \arrow[dr, hook] & & E \arrow[ur, hook] & \\
& L \arrow[ur, hook] & &
\end{tikzcd}.$$

By special case there exists E as in the diagram. By tower law $[K : k(a)] < [K : k]$ hence by induction find Ω as in the diagram. Ω solves the original problem.

$\square$

Proposition 2.3. *Let L be any field and G be a finite group acting on L as automorphisms. Let*

$$K = G^* = Fix(G) = L^G = \{\lambda \in L \mid \forall \sigma \in G,\ \sigma(\lambda) = \lambda\}.$$

Consider $Aut_K(L) = K^\dagger$. Then the obvious inclusion $G \subset K^\dagger = (G^*)^\dagger$ is an equality, so G is all of $K^\dagger$.

Remark. Contextualising, this thing is half of the Galois correspondence.

$$\begin{array}{rcl}
\{F \mid k \subset F \subset \Omega\} & \leftrightarrow & \{G \mid G \le Aut_k(\Omega)\} \\
F & \mapsto & Aut_F(\Omega) = F^\dagger \\
Fix(G) = G^* & \leftarrow\!\shortmid & G
\end{array}.$$

Then to prove the Galois correspondence, we need for all G, $G = (G^*)^\dagger$. We also need for all F, $F = \left(F^\dagger\right)^*$.

Proposition 2.3 follows from the following lemma.

Lemma 2.4. *$K \subset L$ is a finite extension of degree $[L : K] \le |G|$.*

Proof of Proposition 2.3. From Proposition 2.1, $Aut_K(L) = Em_K(L, L)$ because $K \subset L$ is finite, and $\#Em_K(L, L) \le [L : K]$. By the lemma,

$$[L : K] \le \#Em_K(L, L) \le [L : K],$$

so $|G| = \#Em_K(L, L)$. By what we said, $G \subset Em_K(L, L)$, so $G = Em_K(L, L)$. $\square$

Lecture 9 Tuesday 29/01/19

Lecture 9 is a problem class.

Lecture 10 Thursday 31/01/19

Proof of Lemma 2.4. Write $G = \{\sigma_1, \dots, \sigma_n\}$ for $n = |G|$. Want that all $(n+1)$-tuples $a_1, \dots, a_{n+1} \in L$ are linearly dependent over K. Let $a_1, \dots, a_{n+1} \in L$. Consider the $n+1$ vectors in L^n. Let

$$\overline{a_1} = \begin{pmatrix} \sigma_1(a_1) \\ \vdots \\ \sigma_n(a_1) \end{pmatrix}, \ \dots, \ \overline{a_{n+1}} = \begin{pmatrix} \sigma_1(a_{n+1}) \\ \vdots \\ \sigma_n(a_{n+1}) \end{pmatrix} \in L^n.$$

These are linearly dependent over L. There exist $x_1, \dots, x_{n+1} \in L$ not all zero such that

$$x_1 \overline{a_1} + \dots + x_{n+1} \overline{a_{n+1}} = \overline{0}.$$

By reordering the $\overline{a_i}$, may assume

$$x_1 \overline{a_1} + \dots + x_k \overline{a_k} = \overline{0}, \tag{3}$$

for some $1 \le k \le n+1$ with

- for all $i \in \{1, \dots, k\}$, $x_i \ne 0$,
- such k is the smallest, and
- $x_1 = 1$.

Claim that all these $x_i \in K$. This does it, by reading j-th row where $\sigma_j = id_G$. We need to show for all i $x_i \in L^G$. Take $\sigma \in G$.

$$\sigma(x_1) \begin{pmatrix} \sigma(\sigma_1(a_1)) \\ \vdots \\ \sigma(\sigma_n(a_1)) \end{pmatrix} + \dots + \sigma(x_k) \begin{pmatrix} \sigma(\sigma_1(a_k)) \\ \vdots \\ \sigma(\sigma_n(a_k)) \end{pmatrix} = \overline{0} \in L^n.$$

Note that

$$\begin{array}{ccc} G & \to & G \\ \tau & \mapsto & \sigma \circ \tau \end{array}$$

is a bijective function and $\{\sigma \circ \sigma_1, \dots, \sigma \circ \sigma_n\} = G$. Multiplying by σ reshuffles the rows. So in fact,

$$\sigma(x_1) \overline{a_1} + \dots + \sigma(x_k) \overline{a_k} = \overline{0}. \tag{4}$$

Claim that for all i $\sigma(x_i) = x_i$. Otherwise $(3) - (4)$,

$$(x_2 - \sigma(x_2)) \overline{a_2} + \dots + (x_k - \sigma(x_k)) \overline{a_k} = \overline{0}$$

is a shorter solution, contradicting k minimal. $\square$

3 Galois correspondence

Definition 3.1. $k \subset K$ is **normal** if

$$\forall k \subset \Omega,\ \forall \sigma_1, \sigma_2 \in Em_k\left(K, \Omega\right),\ \exists \sigma \in Em_k\left(K, K\right),\ \sigma_2 = \sigma_1 \circ \sigma. \tag{5}$$

$$\begin{tikzcd}
 & \Omega & \\
\sigma_1\left(K\right) \arrow[u, hook] \arrow[rr, bend left, dotted, "\sigma"] & K \arrow[l, "\sigma_1"'] \arrow[r, "\sigma_2"'] & \sigma_2\left(K\right) \arrow[u, hook'] \\
 & k \arrow[ul, hook] \arrow[u, hook] \arrow[ur, hook'] &
\end{tikzcd} .$$

Equivalently, $k \subset K$ is normal if

$$\forall k \subset \Omega,\ \forall \sigma_1, \sigma_2 \in Em_k\left(K, \Omega\right),\ \sigma_2\left(K\right) \subset \sigma_1\left(K\right). \tag{6}$$

Example. $\mathbb{Q} \subset \mathbb{Q}\left(\sqrt[3]{2}\right)$ is not normal. Take $\Omega = \mathbb{Q}\left(\sqrt[3]{2}, \sqrt{-3}\right)$.

(5) $\implies$ (6) Indeed for all $\lambda \in K$, $\sigma_2\left(\lambda\right) = \sigma_1\left(\sigma\left(\lambda\right)\right) \in \sigma_1\left(K\right)$, so $\sigma_2\left(K\right) \subset \sigma_1\left(K\right)$.

(6) $\implies$ (5) Work inside Ω.

$$k \subset \sigma_2\left(K\right) \subset \sigma_1\left(K\right) \subset \Omega.$$

Tower law gives

$$\left[K : k\right] = \left[\sigma_1\left(K\right) : k\right] = \left[\sigma_1\left(K\right) : \sigma_2\left(K\right)\right]\left[\sigma_2\left(K\right) : k\right] = \left[\sigma_1\left(K\right) : \sigma_2\left(K\right)\right]\left[K : k\right].$$

So $\left[\sigma_1\left(K\right) : \sigma_2\left(K\right)\right] = 1$, so $\sigma_1\left(K\right) = \sigma_2\left(K\right)$. Take $\sigma = \sigma_1^{-1} \circ \sigma_2$. σ is clearly bijective and it is more or less obvious that $\sigma \in Em_k\left(K, K\right)$.

Lecture 11
Friday
01/02/19

Equivalently, $k \subset K$ is normal if for all $K \subset \Omega$, for all $\sigma \in Em_k\left(K, \Omega\right)$, $\sigma\left(K\right) \subset K$.

$$\begin{tikzcd}
 & \Omega & \\
K \arrow[ur, hook] \arrow[rr, dotted, "\sigma"] & & \sigma\left(K\right) \arrow[ul, hook'] \\
 & k \arrow[ul, hook] \arrow[ur, hook'] &
\end{tikzcd}$$

Remark. We will see that $k \subset K$ is normal if and only if there exists $f\left(x\right) \in K\left[x\right]$ such that K is a splitting field of f.

Lemma 3.2. *Suppose $k \subset K$ is normal. Consider $k \subset L \subset K$. Then also $L \subset K$ is normal.*

Proof. If $\sigma \in Em_L\left(K, \Omega\right)$, then $\sigma \in Em_k\left(K, \Omega\right)$. $\square$

Warning.

- It is not true in general that $k \subset K$ normal gives $k \subset L$ normal. For example, let

$$k = \mathbb{Q} \subset \mathbb{Q}\left(\sqrt[3]{2}\right) \subset \mathbb{Q}\left(\sqrt[3]{2}, \sqrt{-3}\right) = K.$$

  $k \subset K$ is normal because it is a splitting field but $\mathbb{Q} \subset \mathbb{Q}\left(\sqrt[3]{2}\right)$ is not normal.

- Suppose $k \subset L$ is normal and $L \subset K$ is normal. This does not imply $k \subset K$ is normal. This will be in an example sheet.

Definition 3.3. $k \subset K$ is **separable** if for all $k \subset K_1 \subset K_2 \subset K$, if $K_1 \neq K_2$, there exist $k \subset \Omega$ and embeddings $x \in Em_k(K_1, \Omega)$ and $y_1, y_2 \in Em_k(K_2, \Omega)$ such that

$$\begin{tikzcd}
K & & & \Omega & \\
K_2 \arrow[u, phantom, "\cup"] \arrow[r, dotted, "y_1"] \arrow[rrrr, dotted, bend right, "y_2"'] & y_1(K_2) \arrow[urr, phantom, "\subset"] & & & y_2(K_2) \arrow[ul, phantom, "\supset"] \\
K_1 \arrow[u, phantom, "\cup"] \arrow[rrr, "x"] & & & x(K_1) \arrow[ull, phantom, "\supset"] \arrow[ur, phantom, "\subset"] & \\
k \arrow[u, phantom, "\cup"] \arrow[urrr, phantom, "\subset"] & & & &
\end{tikzcd}.$$

That is, $y_1|_{K_1} = y_2|_{K_1} = x$ but $y_1 \neq y_2$.

Slogan is that embeddings separate fields. We will see that

- in characteristic zero everything is separable, and
- in characteristic p we will have good ways to decide if something is separable.

Lemma 3.4. *Suppose $k \subset K \subset L$. Then $k \subset L$ is separable if and only if $k \subset K$ and $K \subset L$ are separable.*

Proof.

$\Longrightarrow$ Obvious. $K \subset K_1 \subset K_2 \subset L$ leads to $k \subset K_1 \subset K_2 \subset L$.

$\Longleftarrow$ I will do later.

$\square$

Theorem 3.5 (Fundamental theorem of Galois theory)**.** *Let $k \subset K$ be normal and separable. Let $G = Em_k(K, K)$. Then there is a one-to-one correspondence*

$$\begin{array}{rcl} \{k \subset L \subset K\} & \leftrightarrow & \{H \leq G\} \\ L & \mapsto & L^\dagger = \{\sigma \in G \mid \forall \lambda \in L,\ \sigma(\lambda) = \lambda\} \\ H^* = \{\lambda \in K \mid \forall \sigma \in H,\ \sigma(\lambda) = \lambda\} & \leftarrow\!\shortmid & H \end{array}.$$

Proof. We show that for all $H \leq G$, $(H^*)^\dagger = H$ and for all $k \subset L \subset K$, $\left(L^\dagger\right)^* = L$. We already did the former. We just prove the latter now. Note that $L \subset K$ is normal and separable so all I need to show is $\left(k^\dagger\right)^* = k$, that is $k = G^*$ is the fixed field of G. That is, if $\lambda \notin k$, there exists $\sigma : K \to K$ in G such that $\sigma(\lambda) \neq \lambda$. By separability, there exists Ω and $x_1 \neq x_2 \in Em_k(k(\lambda), \Omega)$ such that

$$\begin{tikzcd}
K \arrow[d, dash] \arrow[dr, dotted, "\widetilde{x_1}{,}\widetilde{x_2}"] & \\
k(\lambda) \arrow[r, "x_1{,}x_2"'] \arrow[d, dash] & \Omega \\
k \arrow[ur, dash] &
\end{tikzcd},$$

so $x_1(\lambda) \neq x_2(\lambda)$. Two steps.

- There exist $\widetilde{x_1}, \widetilde{x_2} : K \to \Omega$ extending $x_1, x_2 : k(\lambda) \to \Omega$, by the following lemma.
- Because $k \subset K$ is normal there exists $\sigma \in Em_k(K, K)$ such that $\widetilde{x_2} = \widetilde{x_1} \circ \sigma$ then clearly $\sigma(\lambda) \neq \lambda$.

$\square$

Lemma 3.6. *Suppose $k \subset K$ is normal. Then for all towers $k \subset F \subset K \subset \Omega$, the natural restriction $\rho : Em_k(K, \Omega) \to Em_k(F, \Omega)$ is surjective.*

Lecture 12
Tuesday
05/02/19

The statement says for all $\sigma \in Em_k(F, \Omega)$, there exists $\widetilde{\sigma} \in Em_k(K, \Omega)$ such that $\widetilde{\sigma}\mid_F = \sigma$.

$$\begin{tikzcd}
K \arrow[d, dash] \arrow[dr, dotted, "\widetilde{\sigma}"] & \\
F \arrow[d, dash] \arrow[r, "\sigma"'] & \Omega \\
k \arrow[ur, dash] &
\end{tikzcd}.$$

Proof. We know that there exists $\widetilde{\Omega}$ as follows.

$$\begin{tikzcd}
K \arrow[d, dash] \arrow[r, "\phi_2"] \arrow[dr, dotted, "\widetilde{\sigma}"'] & \widetilde{\Omega} \\
F \arrow[d, dash] \arrow[r, "\sigma"'] & \Omega \arrow[u, "\psi"'] \\
k \arrow[ur, dash] &
\end{tikzcd}.$$

There are two $K \subset \widetilde{\Omega}$,

$$\phi_1 : K \subset \Omega \overset{\psi}{\hookrightarrow} \widetilde{\Omega}, \qquad \phi_2 : K \hookrightarrow \widetilde{\Omega}.$$

Because $k \subset K$ is normal $\phi_2(K) \subset \phi_1(K) \subset \psi(\Omega)$. That proves that $\widetilde{\sigma}$ exists. ☐

Corollary 3.7. *Suppose $k \subset K$ is normal. Then for all towers $k \subset F \subset K \subset \Omega$, $Em_k(F, K) \to Em_k(F, \Omega)$ is also surjective.*

The corollary states that for all $\sigma \in Em_k(F, \Omega)$, $\sigma(F) \subset K$.

$$\begin{tikzcd}
\Omega \arrow[d, dash] \arrow[dr, dash] & \\
K \arrow[d, dash] \arrow[r, dotted, "\widetilde{\sigma}"] \arrow[dr, dash] & \widetilde{\sigma}(K) \arrow[d, dash] \\
F \arrow[d, dash] \arrow[r, "\sigma"'] & \sigma(F) \\
k \arrow[ur, dash] &
\end{tikzcd}.$$

Proof. This clearly follows from the lemma. $\sigma(F) \subset \widetilde{\sigma}(K) \subset K$ by definition of normal. ☐

4 Normal extensions

Theorem 4.1. *For finite $k \subset K$, the following are equivalent.*

1. *For all $f \in k[x]$ irreducible either f has no root in K or f splits completely in K.*
2. *There exists $f \in k[x]$ not necessarily irreducible such that K is a splitting field of f.*
3. *$k \subset K$ is normal.*

Proof.

$1 \implies 2$ There are $\lambda_1, \ldots, \lambda_m \in K$ such that $K = k(\lambda_1, \ldots, \lambda_m)$. For all i let $f_i \in k[x]$ be the minimal polynomial of λ_i. f_i is irreducible and by 1 it splits completely. K is the splitting field of $f(x) = \prod_{i=1}^{m} f_i(x)$.

$2 \implies 3$ Suppose $K \subset \Omega$. Let $\sigma : K \to \Omega$ be another embedding. For all λ_i, $\sigma(\lambda_i)$ is a root of f, so $\sigma(\lambda_i) \subset K$ hence $\sigma(K) \subset K$.

$3 \implies 1$ Let $f(x) \in k[x]$ be irreducible. Suppose there exists $\lambda \in K$ such that $f(\lambda) = 0$. Let Ω be a splitting field of $f(x) \in K[x]$. Let $\mu \in \Omega$ be a root of f. There exists a unique $\sigma \in Em_k(k(\lambda), \Omega)$ such that $\sigma(\lambda) = \mu$.

$$\begin{tikzcd}
K \arrow[d, dash] & \\
F = k(\lambda) \arrow[r, "\sigma"] \arrow[d, dash] & \sigma(F) \subset \Omega \ni \mu \\
k \arrow[ur, dash] &
\end{tikzcd}$$

By corollary, $\sigma(F) \subset K$, so $\mu \in K$.

∎

(Exercise: prove that any two splitting fields of $f \in k[x]$ are k-isomorphic, not necessarily in a unique way)