M3P11 Galois Theory

Lectured by Prof Alessio Corti
Typeset by David Kurniadi Angdinata

Spring 2019

Contents

0 Introduction **3**

1 What is Galois theory? **4**
1.1 Fields 4
1.2 Galois correspondence 5

2 Fields **10**

0 Introduction

Lecture 1
Thursday
10/01/19

The following are 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

1 What is Galois theory?

1.1 Fields

Notation 1.1. 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 1.2.

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.
- 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,
$$\frac{K[x]}{\langle f(x)\rangle}$$
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 1.3. 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 1.4. A **field homomorphism** is a function $\phi : K_1 \to K_2$ that preserves the field operations, for all $a, b \in K_1$,

$$\phi(a + b) = \phi(a) + \phi(b), \qquad \phi(ab) = \phi(a)\phi(b), \qquad \phi(0_{K_1}) = 0_{K_2}, \qquad \phi(1_{K_1}) = 1_{K_2}.$$

Remark 1.5. 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 $\phi(a_1 - a_2) = \phi(a_1) - \phi(a_2) \neq 0$. 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 1.6. 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 1.7.

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

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

Example 1.9.

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

1.2 Galois correspondence

Theorem 1.10 (Fundamental theorem of Galois theory)**.** *Assume characteristic zero. Let $k \subset K$ be the splitting field of $f(x) \in k[x]$. Let*

$$G = \{\textit{field isomorphisms } \sigma : K \to K \mid \sigma \textit{ is a field automorphism of } K \textit{ such that } \sigma|_k = id_k\}.$$

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

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

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 1.11. 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

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

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
$$\sigma : a + b\sqrt{2} \mapsto a - b\sqrt{2}.$$

Theorem 1.10 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 1.12. Let $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ and $L = \mathbb{Q}\left(\sqrt[3]{2}, \omega\right)$, where $\omega = \frac{-1+i\sqrt{3}}{2}$. ω 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 1.13. For any splitting field of f, there is always a natural inclusion group homomorphism

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

the group of permutations of the roots of $f = x^n + a_1 x^{n-1} + \dots + a_n$.

- 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 $K(\lambda_1, \dots, \lambda_n) = L$.

Theorem 1.10 and Remark 1.13 gives $G = \mathfrak{S}_3$.

Lecture 4 Thursday 17/01/19

Definition 1.14. $K \subset L$ 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 1.15 (Tower law)**.** *Let $K \subset L \subset F$. Then $[F : K] = [F : L] [L : K]$.*

Theorem 1.16. *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 1.17.

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

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

Example 1.18. 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

$$\begin{tikzcd}
 & & L \arrow[dll, dash, "2"'] \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "3"] & \\
\mathbb{Q}\left(\sqrt[3]{2}\right) \arrow[drr, dash, "3"'] & \mathbb{Q}\left(\omega^2\sqrt[3]{2}\right) \arrow[dr, dash, "3"] & \mathbb{Q}\left(\omega\sqrt[3]{2}\right) \arrow[d, dash, "3"] & \mathbb{Q}(\omega) \arrow[dl, dash, "2"] \\
 & & \mathbb{Q} &
\end{tikzcd}.$$

(Exercise: $\mathbb{Q}\left(\sqrt[3]{2} + \omega\right) = L$, $\mathbb{Q}\left(\omega^2\sqrt[3]{2}\right) \cap \mathbb{Q}\left(\omega\sqrt[3]{2}\right) = \mathbb{Q}$, and $\mathbb{Q}\left(\sqrt[3]{2}, \omega\sqrt[3]{2}\right) = L$) What is $\left[L : \mathbb{Q}\left(\sqrt[3]{2}\right)\right]$? Note $L = \mathbb{Q}\left(\sqrt[3]{2}\right)\left(\sqrt{-3}\right)$. 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 Theorem 1.15,

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

$2 \mid [L : \mathbb{Q}]$ and $3 \mid [L : \mathbb{Q}]$, so $6 \mid [L : \mathbb{Q}]$. Either $x^2 + 3$ is irreducible over $\mathbb{Q}\left(\sqrt[3]{2}\right)$, so by Theorem 1.16 $\left[L : \mathbb{Q}\left(\sqrt[3]{2}\right)\right] = 2$ 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 Theorem 1.15 $[K : \mathbb{Q}] = 2$ or $[K : \mathbb{Q}] = 3$.

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

$$\begin{tikzcd}
 & L \arrow[d, dash] & \\
 & K(\omega) \arrow[dl, dash] \arrow[dr, dash] & \\
K \arrow[dr, dash, "2"'] & & \mathbb{Q}(\omega) \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

  Either $\omega \in K$, that is $\mathbb{Q}(\omega) \subset K$, so by Theorem 1.15 $\mathbb{Q}(\omega) = K$. 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 $[K : \mathbb{Q}] = 3$.

$$\begin{array}{c} L \\ 2 \\ K(\omega) \\ 3 \\ \mathbb{Q} \end{array}.$$

  Claim that $x^3 - 2 \in K[x]$ splits, so it has a root in K. Either $\sqrt[3]{2} \in K$, $\omega\sqrt[3]{2} \in K$, or $\omega^2\sqrt[3]{2} \in K$.

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 1.15. Suppose $y_1, \ldots, y_m \in F$ is a basis of F as a vector space over L. Suppose $x_1, \ldots, x_n \in L$ 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 $\mu_1, \ldots, \mu_n \in L$ such that

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

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

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

  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, $\lambda_{ij} = 0$.

□

Example 1.19. 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. $Gal_{\mathbb{Q}(\sqrt[3]{2})}(L), Gal_{\mathbb{Q}(\omega^2\sqrt[3]{2})}(L), Gal_{\mathbb{Q}(\omega\sqrt[3]{2})}(L) \subset G$ contain an element of order two, and

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

The lattice of subgroups is

$$\begin{tikzcd}
 & & & \{e\} \arrow[dlll, dash, "2"'] \arrow[dll, dash, "2"] \arrow[dl, dash, "2"] \arrow[ddr, dash, "3"] & \\
\langle (2\ \ 3) \rangle \arrow[ddrrr, dash, "3"'] & \langle (1\ \ 2) \rangle \arrow[ddrr, dash, "3"] & \langle (1\ \ 3) \rangle \arrow[ddr, dash, "3"] & & \\
 & & & & \langle (1\ \ 2\ \ 3) \rangle \arrow[dl, dash, "2"] \\
 & & & G &
\end{tikzcd}.$$

$\mathbb{Q}(\omega)/\mathbb{Q}$ 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 $Gal_k(K) = G/H$.

2 Fields

Lecture 6
Tuesday
22/01/19

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

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

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

Definition 2.1. $f(x) = a_0 x^n + \dots + a_n \in K[x]$ is **monic** if $a_0 = 1$.

Lemma 2.2.

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

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

- *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*

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

Proof. There is nothing to prove. ☐

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 $g(a)\psi(a) = 1$.

Remark 2.3. All of this is saying

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

Let

$$Emb_K(K(a), F) = \{\sigma : K(a) \to F \text{ field homomorphism} \mid \forall \lambda \in K,\ \sigma(\lambda) = \lambda\}.$$

Corollary 2.4. *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,*

$$Emb_K(K(a), F) = \{b \in F \mid f_a(b) = 0\}.$$

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

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

  where $g(a) = 0$, and f was not the minimal polynomial.

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

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

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

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

$\square$

Corollary 2.5. *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. $\square$