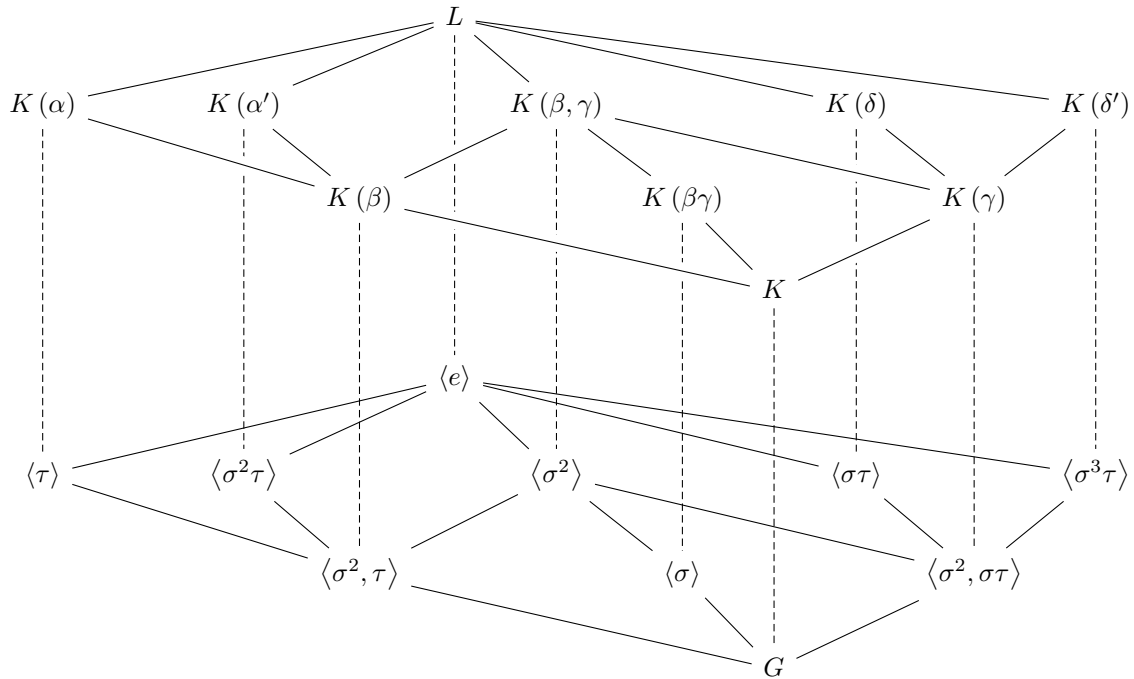# M3P11 Galois Theory

Lectured by Prof Alessio Corti
Typed by David Kurniadi Angdinata

Spring 2019

$$G = \mathrm{Gal}\,(L/K) \cong \mathcal{D}_8$$

Syllabus

Field extensions. Irreducible polynomials. Normal extensions. Separable extensions. Fundamental theorem of Galois theory. Galois theory of quadratic polynomials. Galois theory of biquadratic polynomials. Galois theory of finite fields. Galois theory of cubic polynomials. Reduction modulo prime.

Contents

0 Introduction

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

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.

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields.

- **Quadratic fields**
$$\mathbb{Q}\left(\sqrt{2}\right) = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\} = \mathbb{Q}[X] / \left\langle X^2 - 2 \right\rangle.$$
  are also fields, since
$$\frac{1}{\left(a + b\sqrt{2}\right)} = \frac{a - b\sqrt{2}}{a^2 - 2b^2}.$$

- 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 $p \nmid a$. 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 $\operatorname{ch} K = 0$, or there exists p prime such that $m = 0$ if and only if $p \mid m$, so K has characteristic $\operatorname{ch} K = p$.

- For K a field,
$$K(X) = \operatorname{Frac} K[X] = \left\{\phi(X) = \frac{f(X)}{g(X)} \mid f, g \in K[X],\ g \neq 0\right\}.$$
  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.

1 What is Galois theory?

1.1 Field extensions

Definition 1.1. A **field homomorphism** is a function $\phi : K_1 \to K_2$ that preserves the field operations, for all $a, b \in K_1$,

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

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 and α. This is not to be confused with $k(X)$.

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

- $\alpha = \sqrt{2}$, so $\mathbb{Q}\left(\sqrt{2}\right)$.

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

Definition 1.2. 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 1.3. Consider a field k and $f \in k[X]$. We say that $k \subset K$ is a **splitting field** for f if

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

Example.

- If $f(X) = X^2 - 2 \in \mathbb{Q}[X]$, then $K = \mathbb{Q}\left(\sqrt{2}\right)$ 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 $K = \mathbb{Q}\left(\sqrt{-2}\right)$.

- 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, but $K = \mathbb{Q}\left(\sqrt[3]{2}, \omega\right)$, where $\omega = \frac{-1+\sqrt{-3}}{2}$, is a splitting field. Then

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

1.2 Galois correspondence

Theorem 1.4 (Fundamental theorem of Galois theory, Galois correspondence). *Assume characteristic zero. Let $k \subset K$ be the splitting field of $f(X) \in k[X]$. Let*

$$G = \left\{\sigma : K \to K \mid \sigma \text{ field automorphism}, \ \sigma|_k = \mathrm{id}_k\right\}.$$

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

$$
\begin{array}{rcl}
\{k \subset K_1 \subset K \mid K_1 \text{ subfield}\} & \longleftrightarrow & \{H \leq G \mid H \text{ subgroup}\} \\
K_1 & \longmapsto & \{\sigma \in G \mid \forall \lambda \in K_1, \ \sigma(\lambda) = \lambda\} \\
\{\lambda \in K \mid \forall \sigma \in H, \ \sigma(\lambda) = \lambda\} & \longleftarrow & H \leq G
\end{array}.
$$

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.

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 $G = \{\mathrm{id}\}$. 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 $L = K\left(\sqrt{\Delta}\right) = \left\{a + b\sqrt{\Delta} \;\middle|\; a, b \in K\right\}$. Then $K \subset L$ and $G = \{\sigma : L \to L \mid \sigma|_K = \mathrm{id}_K\} = \mathcal{C}_2$ is generated by $\sigma : a + b\sqrt{\Delta} \mapsto a - b\sqrt{\Delta}$. The following is further specialisation.

- Let $K = \mathbb{R}$ and $\Delta = -1$. Then $L = \mathbb{C} = \left\{a + b\sqrt{-1} \mid a, b \in \mathbb{R}\right\}$, and $G = \mathcal{C}_2$ is generated by complex conjugation $\sigma : a + b\sqrt{-1} \mapsto a - b\sqrt{-1}$.

- Let $K = \mathbb{Q}$ and $\Delta = 2$. Then $L = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\}$, and $G = \mathcal{C}_2$ is generated by $\sigma : a + b\sqrt{2} \mapsto a - b\sqrt{2}$.

The fundamental theorem implies there does not exist $K \subsetneq K_1 \subsetneq K\left(\sqrt{\Delta}\right) = L$. Consider $x \in L \setminus K$, so $x = a + b\sqrt{\Delta}$, and $b \neq 0$, and then $\sqrt{\Delta} = (x - a)/b$, so $K(x) = L$.

1.3   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

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

Remark. For any splitting field of f, there is always a natural inclusion group homomorphism $\rho : G \hookrightarrow S(\lambda_1, \ldots, \lambda_n)$, where $S(\lambda_1, \ldots, \lambda_n)$ is the group of permutations of the roots of $f = X^n + a_1 X^{n-1} + \cdots + a_n$.

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

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

- ρ is injective, since if for all i, $\sigma(\lambda_i) = \lambda_i$, then $\sigma = \mathrm{id}$ on $K(\lambda_1, \ldots, \lambda_n) = L$.

Definition 1.5. $K \subset L$ is **finite** if L is a finite-dimensional K-vector space. The **degree** of L over K is

$$[L : K] = \dim_K L.$$

Theorem 1.6 (Tower law). *Let $K \subset L \subset F$. Then*

$$[F : K] = [F : L][L : K].$$

Proof. Suppose $y_1, \ldots, y_m$ is a basis of F as a vector space over L. Suppose $x_1, \ldots, x_n$ 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

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

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

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

  Plugging 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

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

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

$$\square$$

5

Theorem 1.7. *Suppose $f(X) \in K[X]$ is irreducible such that $f(\lambda) = 0$, then $[K(\lambda) : K] = \deg f$.*
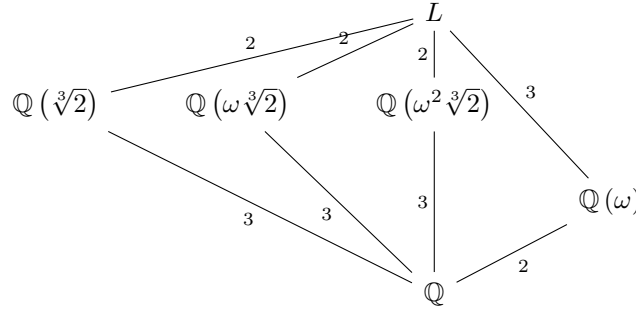
If $K = \mathbb{Q}\left(\sqrt[3]{2}\right)$, then $[K : \mathbb{Q}] = 3$. Let $L = \mathbb{Q}\left(\sqrt[3]{2}, \omega\right) = \mathbb{Q}\left(\sqrt[3]{2}\right)\left(\sqrt{-3}\right)$ be the splitting field of $X^3 - 2$ over $\mathbb{Q}$. What is $\left[L : \mathbb{Q}\left(\sqrt[3]{2}\right)\right]$? 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,

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

Then $X^2 + 3$ is irreducible over $\mathbb{Q}\left(\sqrt[3]{2}\right)$, so by Theorem 1.7 $\left[L : \mathbb{Q}\left(\sqrt[3]{2}\right)\right] = 2$ and $[L : \mathbb{Q}] = 6$. Otherwise $X^2 + 3$ is not irreducible, so $\mathbb{Q}\left(\sqrt[3]{2}\right) = L$ and $[L : \mathbb{Q}] = 3$, a contradiction. Similarly, [1]

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

The lattice of subfields is

Claim that there are no other fields. Suppose $\mathbb{Q} \subsetneq K \subsetneq L$ is such a field. By the tower law $[K : \mathbb{Q}] = 2, 3$. Suppose $[K : \mathbb{Q}] = 2$. Then
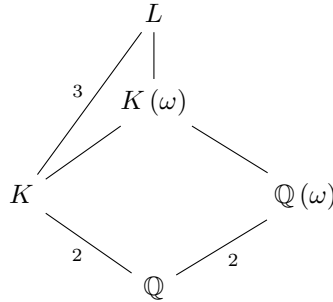
Then $\omega \in K$, that is $\mathbb{Q}(\omega) \subset K$, so by the tower law $\mathbb{Q}(\omega) = K$. Otherwise $\omega \notin K$, so $[K(\omega) : K] = 2$, so $[K(\omega) : \mathbb{Q}] = 4$ contradicts the tower law for $\mathbb{Q} \subset K(\omega) \subset L$. Suppose $[K : \mathbb{Q}] = 3$. Then
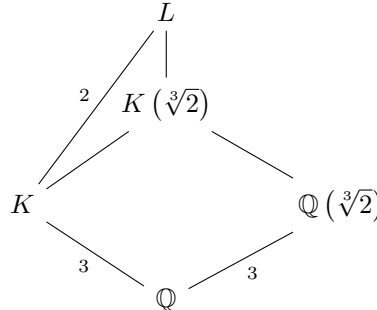
Claim that $X^3 - 2 \in K[X]$ splits. Suppose that it were irreducible, then $\left[K\left(\sqrt[3]{2}\right) : K\right] = 3$, which contradicts the tower law for $K \subset K\left(\sqrt[3]{2}\right) \subset L$. So it has a root in K. Either $\sqrt[3]{2} \in K$, $\omega\sqrt[3]{2} \in K$, or $\omega^2\sqrt[3]{2} \in K$. Thus $\mathbb{Q}\left(\sqrt[3]{2}\right) = K$, $\mathbb{Q}\left(\omega\sqrt[3]{2}\right) = K$, or $\mathbb{Q}\left(\omega^2\sqrt[3]{2}\right) = K$.

---

[1]Exercise

I want to prove that

$$G = \mathrm{Aut}_{\mathbb{Q}} L = \left\{ \sigma : L \to L \ \middle| \ \sigma|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}} \right\} = \mathcal{S}_3.$$

Let $\sigma = (12)$. 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 $\rho(\sigma) = (12)$ 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, so

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

contain an element of order two, and

$$\rho \ : \quad \begin{array}{rcl} \mathrm{Gal}\left(L/\mathbb{Q}\left(\sqrt[3]{2}\right)\right) & \longmapsto & (23) \\ \mathrm{Gal}\left(L/\mathbb{Q}\left(\omega^2\sqrt[3]{2}\right)\right) & \longmapsto & (12) \\ \mathrm{Gal}\left(L/\mathbb{Q}\left(\omega\sqrt[3]{2}\right)\right) & \longmapsto & (13). \end{array}$$

The lattice of subgroups is
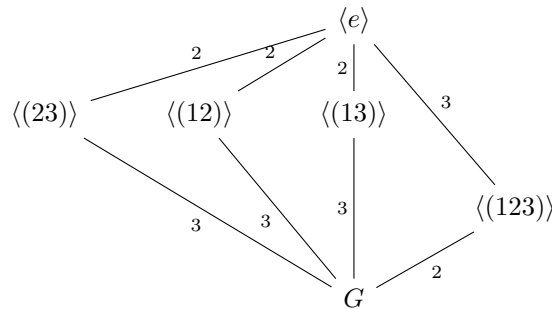
Thus $\mathbb{Q}(\omega)/\mathbb{Q}$ is the splitting field of $X^2 + X + 1$ and of $X^2 + 3$. We can learn the following. Let $k \subset L$ be a splitting field. Consider $k \subset K \subset L$. Then $K \subset L$ is also a splitting field. The corresponding $H \leq G$ is the Galois group $\mathrm{Gal}(L/K)$. 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 $\mathrm{Gal}(K/k) = G/H$.

2 Fundamental theorem of Galois theory

2.1 Elementary facts

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

$$
\begin{array}{rclcl}
e_a & : & K[X] & \longrightarrow & K[a] \subset L \\
    &   & f(X) & \longmapsto & f(a)
\end{array}
$$

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

Definition 2.1. $f(X) = a_0 X^n + \cdots + a_n \in K[X]$ 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

$$
\begin{array}{c}
K(X) \\
\cup \qquad \searrow^{\widetilde{e_a}} \\
 \quad {\scriptstyle \sim} \\
K[X] \xrightarrow[\ e_a\ ]{} K(a) \subset L
\end{array}
\qquad .
$$

- 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

$$
\begin{array}{c}
K[X] \xrightarrow{\ e_a\ } K[a] \cong K(a) \subset L \\
\cup \qquad {\scriptstyle \sim} \nearrow_{[e_a]} \\
K[X]/\langle f_a \rangle
\end{array}
\qquad .
$$

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

Remark. Let $g(X) \in K[X]$ and $g(a) \neq 0$. Claim that $1/g(a) \in K[a]$. Indeed $\gcd(f_a, g) = 1$ in $K[X]$ and $f_a \nmid g$. There exists $\phi, \psi \in K[X]$ such that $f_a \phi + g \psi = 1$ 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

$$
\mathrm{Em}_K(K(a), F) = \{\sigma : K(a) \to F \mid \sigma \text{ field homomorphism}, \ \ \sigma|_K = \mathrm{id}_K \},
$$

where

$$
\begin{array}{c}
K(a) \\
\lhook\joinrel\relbar \qquad \vdots \\
K \qquad\qquad \vdots\, \sigma \quad . \\
\lhook\joinrel\relbar \qquad \downarrow \\
F
\end{array}
$$

Corollary 2.3. *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,
$$
\mathrm{Em}_K(K(a), F) = \{b \in F \mid f_a(b) = 0\}.
$$

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

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

is the minimal polynomial of a over K. Claim that $1, \ldots, a^{n-1}$ 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 implies that
  $$g(X) = f(X) q(X) + r(X), \qquad m = \deg r(X) < n.$$
  Then $r(X) = \lambda_0 + \cdots + \lambda_m X^m$ and $g(a) = r(a) = \lambda_0 + \cdots + \lambda_m a^m$.

- The set is linearly independent, otherwise there exists
  $$g(X) = \lambda_0 + \cdots + \lambda_{n-1} X^{n-1} \in K[X], \qquad g(a) = 0,$$
  and f was not the minimal polynomial.

Then $\sigma(a)$ 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,

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

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

$$\begin{array}{ccc}
\mathrm{Em}_K(K(a), F) & \longleftrightarrow & \{b \in F \mid f(b) = 0\} \\
\sigma & \longmapsto & \sigma(a) \\
[e_b][e_a]^{-1} & \longleftarrow\!\shortmid & b
\end{array}.$$

$\square$

Corollary 2.4. *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. $\square$

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 $a_1, \ldots, a_m \in L$ such that $L = K(a_1, \ldots, a_m)$.

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

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

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

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

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

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

Remark. Suppose $k \subset K$. Then $\mathrm{Em}_k(K, K) = G = \mathrm{Gal}(K/k)$. Indeed every k-homomorphism $\sigma : K \to K$ is automatically invertible. We know σ is injective, so σ is also surjective because σ is a k-linear endomorphism of a finite-dimensional k-vector space.

2.2   Axiomatics

Proposition 2.5. *Fix* $k \subset K$ *and* $k \subset L$. *Then*

$$\# \operatorname{Em}_k (K, L) \leq [K : k].$$

Proof.

- Special case. If $K = k(a)$, let $f(X) \in k[X]$ be the minimal polynomial of a. Then $\operatorname{Em}_k (k(a), L)$ is the roots of $f(X)$ in L, so as proved last time,

$$\# \operatorname{Em}_k (K, L) = \# \{\text{roots}\} \leq \deg f = [k(a) : k].$$

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

  Consider the restriction map

$$\rho : \operatorname{Em}_k (K, L) \to \operatorname{Em}_k (k(a), L).$$

  Fix $y \in \operatorname{Em}_k (k(a), L)$. Then

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

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

$$\# \operatorname{Em}_k (K, L) \leq \sum_{y \in \operatorname{Em}_k (k(a), L)} \# \rho^{-1}(y) \leq [k(a) : k][K : k(a)] = [K : k],$$

  by the tower law.

$\square$

Proposition 2.6. *Suppose given two field extensions* $k \subset K$ *and* $k \subset L$. *Then there is a non-unique bigger common field*

that contains both.

More formally, suppose given $\sigma_1 \in \operatorname{Em}(k, K)$ and $\sigma_2 \in \operatorname{Em}(k, L)$, then there exist Ω, $\phi_1 \in \operatorname{Em}(K, \Omega)$, and $\phi_2 \in \operatorname{Em}(L, \Omega)$ such that $\phi_1 \circ \sigma_1 = \phi_2 \circ \sigma_2$. Another more precise way to state this is there exists $k \subset \Omega$ such that $\operatorname{Em}_k (K, \Omega)$ and $\operatorname{Em}_k (L, \Omega)$ are both non-empty.

Remark. 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

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 $\sigma \in \mathrm{Em}_k(k(a), E)$ such that $\sigma(a) = \alpha$, so

$$
\begin{array}{ccc}
 & k(a) & \\
\subset & & \raisebox{0.5em}{$\xdashrightarrow{\ \sigma\ }$} \\
k & & E \quad . \\
 & \subset \qquad \subset & \\
 & L &
\end{array}
$$
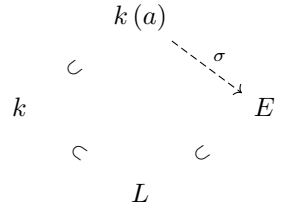
- General case. By induction on $[K : k]$. If $[K : k] = 1$, take $\Omega = L$. If $[K : k] > 1$, take $a \in K \setminus k$, so

$$
\begin{array}{ccccc}
 & & K & & \\
 & \subset & & \subset & \\
 & k(a) & & \Omega & \\
 \subset & & \subset & & \subset \quad . \\
 k & & & E & \\
 & \subset & & \subset & \\
 & & L & &
\end{array}
$$

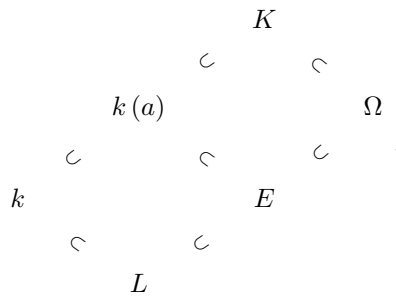By special case there exists E as in the diagram. By tower law $[K : k(a)] < [K : k]$ hence by induction find Ω as in the diagram. Then Ω solves the original problem.

$\square$

Proposition 2.7. *Let L be any field and G be a finite group acting on L as automorphisms. Let*

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

Consider $\mathrm{Aut}_K L = K^\dagger$. 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

$$
\begin{array}{ccl}
\{F \mid k \subset F \subset \Omega\} & \longleftrightarrow & \{G \mid G \leq \mathrm{Aut}_k \Omega\} \\
F & \longmapsto & \mathrm{Aut}_F \Omega = F^\dagger \\
\mathrm{Fix}\, G = G^* & \longleftarrow & G
\end{array} \quad .
$$

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

Proposition 2.7 follows from the following lemma.

Lemma 2.8. *$K \subset L$ is a finite extension of degree $[L : K] \leq \#G$.*

Proof of Proposition 2.7. $\mathrm{Aut}_K L = \mathrm{Em}_K(L, L)$ because $K \subset L$ is finite. From Proposition 2.5, $\#\mathrm{Aut}_K L \leq [L : K]$. By Lemma 2.8,

$$
[L : K] \leq \#\mathrm{Em}_K(L, L) \leq [L : K],
$$

so $\#G = \#\mathrm{Em}_K(L, L)$. By what we said, $G \subset \mathrm{Em}_K(L, L)$, so $G = \mathrm{Em}_K(L, L)$. $\square$

Lecture 9 is a problems class.

Proof of Lemma 2.8. Write $G = \{\sigma_1, \ldots, \sigma_n\}$ for $n = \#G$. Want that all $(n+1)$-tuples $a_1, \ldots, a_{n+1} \in L$ are linearly dependent over K. Let $a_1, \ldots, a_{n+1} \in L$. Consider the $n+1$ vectors in L^n. Let

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

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

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

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

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

for some $1 \leq k \leq n+1$ with for all $i \in \{1, \ldots, k\}$, $x_i \neq 0$, such k is the smallest, and $x_1 = 1$. Claim that all these $x_i \in K = L^G$. This does it, by reading j-th row where $\sigma_j = \mathrm{id}_G$. Take $\sigma \in G$. Then

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

Note that

$$\begin{array}{ccc} G & \longrightarrow & G \\ \tau & \longmapsto & \sigma \circ \tau \end{array}$$

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

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

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

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

contradicting k minimal. $\qquad\square$

2.3   Galois correspondence

Definition 2.9. $k \subset K$ is **normal** if

$$\forall k \subset \Omega, \ \forall \sigma_1, \sigma_2 \in \mathrm{Em}_k(K, \Omega), \ \exists \sigma \in \mathrm{Em}_k(K, K), \ \sigma_2 = \sigma_1 \circ \sigma. \tag{5}$$

$$\Omega$$

$$\sigma_1(K) \xleftarrow[\sigma_1]{\quad} K \xrightarrow[\sigma_2]{\quad} \sigma_2(K) \ \cdot$$

$$k$$

Equivalently, $k \subset K$ is normal if

$$\forall k \subset \Omega, \ \forall \sigma_1, \sigma_2 \in \mathrm{Em}_k(K, \Omega), \ \sigma_2(K) \subset \sigma_1(K). \tag{6}$$

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 $\lambda \in K$, $\sigma_2(\lambda) = \sigma_1(\sigma(\lambda)) \in \sigma_1(K)$, so $\sigma_2(K) \subset \sigma_1(K)$.

$(6) \implies (5)$. Work inside Ω, so $k \subset \sigma_2(K) \subset \sigma_1(K) \subset \Omega$. Tower law implies that

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

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

Equivalently, $k \subset K$ is normal if for all $K \subset \Omega$, for all $\sigma \in \mathrm{Em}_k(K, \Omega)$, $\sigma(K) \subset K$.

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

Lemma 2.10. *Suppose $k \subset K$ is normal. Consider $k \subset L \subset K$. Then also $L \subset K$ is normal.*

Proof. If $\sigma \in \mathrm{Em}_L(K, \Omega)$, then $\sigma \in \mathrm{Em}_k(K, \Omega)$. $\qquad\qquad\square$

The following is a warning.

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

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

  Then $k \subset K$ 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 2.11. $k \subset K$ 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 $x \in \mathrm{Em}_k(K_1, \Omega)$ and $y_1, y_2 \in \mathrm{Em}_k(K_2, \Omega)$ such that

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

The 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 2.12. *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.

$\implies$ Obvious, since $K \subset K_1 \subset K_2 \subset L$ leads to $k \subset K_1 \subset K_2 \subset L$.

$\impliedby$ I will do later.

$\qquad\qquad\square$

Theorem 2.13 (Fundamental theorem of Galois theory, Galois correspondence)**.** *Let $k \subset K$ be normal and separable. Let $G = \mathrm{Em}_k(K, K)$. Then there is a one-to-one correspondence*

$$
\begin{aligned}
\{k \subset L \subset K\} &\longleftrightarrow \{H \leq G\} \\
L &\longmapsto L^\dagger = \{\sigma \in G \mid \forall \lambda \in L,\ \sigma(\lambda) = \lambda\} \ . \\
H^* = \{\lambda \in K \mid \forall \sigma \in H,\ \sigma(\lambda) = \lambda\} &\longleftarrow H
\end{aligned}
$$

Proof. We show that for all $H \leq G$, $(H^*)^\dagger = H$ and for all $k \subset L \subset K$, $(L^\dagger)^* = L$. 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 $(k^\dagger)^* = k$, 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 exist Ω and $x_1 \neq x_2 \in \mathrm{Em}_k(k(\lambda), \Omega)$ such that

$$
\begin{array}{c}
K \\
| \quad \diagup \; \widetilde{x_1}, \widetilde{x_2} \\
k(\lambda) \xrightarrow{x_1, x_2} \Omega \quad , \\
| \quad \diagup \\
k
\end{array}
$$

so $x_1(\lambda) \neq x_2(\lambda)$. 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 $\sigma \in \mathrm{Em}_k(K, K)$ such that $\widetilde{x_2} = \widetilde{x_1} \circ \sigma$ then clearly $\sigma(\lambda) \neq \lambda$.   □

Lemma 2.14. *Suppose $k \subset K$ is normal. Then for all towers $k \subset F \subset K \subset \Omega$, the natural restriction*

$$
\rho : \mathrm{Em}_k(K, \Omega) \to \mathrm{Em}_k(F, \Omega)
$$

is surjective.

Lemma 2.14 says for all $\sigma \in \mathrm{Em}_k(F, \Omega)$, there exists $\widetilde{\sigma} \in \mathrm{Em}_k(K, \Omega)$ such that $\widetilde{\sigma}|_F = \sigma$, so

$$
\begin{array}{c}
K \\
| \quad \diagup \; \widetilde{\sigma} \\
F \xrightarrow{\sigma} \Omega \quad \cdot \\
| \quad \diagup \\
k
\end{array}
$$

Proof. We know that there exists $K \subset \widetilde{\Omega}$ such that $\psi : \Omega \hookrightarrow \widetilde{\Omega}$. There are two embeddings $\phi_1 : K \subset \Omega \xrightarrow{\psi} \widetilde{\Omega}$ and $\phi_2 : K \hookrightarrow \widetilde{\Omega}$. Because $k \subset K$ is normal $\phi_2(K) \subset \phi_1(K) \subset \psi(\Omega)$. That proves that $\widetilde{\sigma}$ exists.   □

Corollary 2.15. *Suppose $k \subset K$ is normal. Then for all towers $k \subset F \subset K \subset \Omega$,*

$$
\mathrm{Em}_k(F, K) \to \mathrm{Em}_k(F, \Omega)
$$

is also surjective.

Corollary 2.15 states that for all $\sigma \in \mathrm{Em}_k(F, \Omega)$, $\sigma(F) \subset K$, so

$$
\begin{array}{c}
\Omega \\
| \quad \diagdown \\
K \xdashrightarrow{\widetilde{\sigma}} \widetilde{\sigma}(K) \\
| \quad \diagdown \quad | \quad \cdot \\
F \xrightarrow{\sigma} \sigma(F) \\
| \quad \diagup \\
k
\end{array}
$$

Proof. This clearly follows from Lemma 2.14, since $\sigma(F) \subset \widetilde{\sigma}(K) \subset K$ by definition of normal.   □

3   Normal and separable extensions

3.1   Normal extensions

Theorem 3.1. *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, so f_i is irreducible and by 1 it splits completely. Then 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 $\sigma \in \mathrm{Em}_k(k(\lambda), \Omega)$ such that $\sigma(\lambda) = \mu$, so

$$
\begin{array}{c}
K \\
| \\
F = k(\lambda) \xrightarrow{\ \sigma\ } \sigma(F) \subset \Omega \ni \mu \ \cdot \\
| \qquad\qquad\nearrow \\
k
\end{array}
$$

By Corollary 2.15, $\sigma(F) \subset K$, so $\mu \in K$.

$\square$

Exercise. Prove that any two splitting fields of $f \in k[X]$ are k-isomorphic, not necessarily in a unique way.

Proposition 3.2. *Let $k \subset L$ be a field extension. Then there exists a tower $k \subset L \subset K$ such that $k \subset K$ is normal.*

Proof. We use normal if and only if splitting field. Pick $\lambda_1, \ldots, \lambda_n \in L$ such that $L = k(\lambda_1, \ldots, \lambda_n)$. Let $f_i \in k[X]$ be the minimal polynomial of λ_i over k. Let K be the splitting field of $f = \prod_{i=1}^{n} f_i \in L[X]$. Claim that K is the splitting field of f over k. The key point is to argue that K is generated by the roots of f over k. $\square$

3.2   Separable polynomials

Definition 3.3. A polynomial $f \in k[X]$ is **separable** if it has $n = \deg f$ distinct roots in any field $k \subset K$ such that $f \in K[X]$ splits completely.

Remark. It is not completely obvious that this definition is independent of K. To see this, use the fact that any two splitting fields are isomorphic.

Example.

- Let $k = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Then $X^p - a^p = (X - a)^p$ is not separable, since in characteristic p, $(a + b)^p = a^p + b^p$.

- Let $k = \mathbb{F}_p(t)$. Then $X^p - t$ is an irreducible polynomial. Why? Let $K = \mathbb{F}_p(t)[u] / \langle u^p - t \rangle = \mathbb{F}_p(u)$. In $K[X]$, $X^p - t = (X - u)^p$.

For all k, define the **derivation** as

$$\begin{array}{rcl} \mathrm{D} & : & k\left[X\right] \longrightarrow k\left[X\right] \\ & & X^n \longmapsto nX^{n-1} \end{array},$$

and extend linearly to all of $k\left[X\right]$. The following are some properties.

- D is k-linear, that is for all $\lambda, \mu \in k$, for all $f, g \in k\left[X\right]$,

$$\mathrm{D}\left(\lambda f + \mu g\right) = \lambda \mathrm{D}f + \mu \mathrm{D}g.$$

- Leibnitz rule, that is for all $f, g \in k\left[X\right]$,

$$\mathrm{D}fg = f\mathrm{D}g + g\mathrm{D}f.$$

Most important thing to know in characteristic p, if $p \mid n$ then $\mathrm{D}X^n = nX^{n-1} = 0$. If $\mathrm{D}f = 0$ that does not mean f is constant. This just means that there exists $h \in k\left[X\right]$ such that $f\left(X\right) = h\left(X^p\right)$.

Proposition 3.4. $f\left(X\right) \in k\left[X\right]$ *is separable if and only if* $\gcd\left(f, \mathrm{D}f\right) = 1$.

In $\mathbb{R}\left[x\right]$, f is inseparable if and only if there exists a multiple root, a critical point, which is a root of $\mathrm{D}f$.

Lemma 3.5. *Let* $f, g \in k\left[X\right]$ *and* $c = \gcd\left(f, g\right)$ *in* $k\left[X\right]$. *Let* $k \subset L$ *be an extension. Then* $c = \gcd\left(f, g\right)$ *in* $L\left[X\right]$.

Proof. Indeed, if $c \mid f$ and $c \mid g$ in $k\left[X\right]$ then also in $L\left[X\right]$. We also know that there exists $\phi, \psi \in k\left[X\right]$ such that

$$f\phi + g\psi = c \tag{7}$$

in $k\left[X\right]$, and hence also in $L\left[X\right]$. Suppose that $u \mid f$ and $u \mid g$ in $L\left[X\right]$, so $u \mid c$ in $L\left[X\right]$ by (7). $\square$

Proof of Proposition 3.4. Let $k \subset L$ be any field where f splits completely. We can do the proof in $L\left[X\right]$. That is, we may assume that f splits completely, so

$$f\left(X\right) = \prod_i \left(X - \lambda_i\right).$$

$\Longleftarrow$ Assume for a contradiction that f is not separable then $f\left(X\right) = \left(X - \lambda\right)^2 g\left(X\right)$. Then

$$\mathrm{D}f\left(X\right) = 2\left(X - \lambda\right)g\left(X\right) + \left(X - \lambda\right)^2 \mathrm{D}g\left(X\right) = \left(X - \lambda\right)\left(2g\left(X\right) + \left(X - \lambda\right)\mathrm{D}g\left(X\right)\right).$$

That is, $\left(X - \lambda\right) \mid f$ and $\left(X - \lambda\right) \mid \mathrm{D}f$, so $\gcd\left(f, \mathrm{D}f\right) \neq 1$.

$\Longrightarrow$ For all $i \neq j$, $\lambda_i \neq \lambda_j$, so

$$\mathrm{D}f = \sum_i \left(\prod_{j \neq i}\left(X - \lambda_j\right)\right).$$

Claim that for all i, $\left(X - \lambda_i\right) \nmid \mathrm{D}f$. I hope you see this. This shows $\gcd\left(f, \mathrm{D}f\right) = 1$.

$\square$

Theorem 3.6. $f \in k\left[X\right]$ *irreducible is inseparable if and only if*

- ch $k = p > 0$, *and*

- *there exists* $h \in k\left[X\right]$ *such that* $f\left(X\right) = h\left(X^p\right)$.

Proof. Indeed f is inseparable if and only if $\gcd\left(f, \mathrm{D}f\right) \neq 1$, if and only if $\mathrm{D}f = 0$, since f is irreducible so $\gcd\left(f, \mathrm{D}f\right) \neq 1$ if and only if $f \mid \mathrm{D}f$, and $\deg \mathrm{D}f < \deg f$. $\square$

Definition 3.7. A field k in $\operatorname{ch} k = p > 0$ is **perfect** if for all $a \in k$ there exists $b \in k$ such that $b^p = a$.

Proposition 3.8. *If k is perfect then $f \in k[X]$ is irreducible implies that $f(X)$ is separable.*

Proof. If f were inseparable then $f(X) = h(X^p)$. For all i, finding $b_i^p = a_i$,

$$h(X) = X^n + a_1 X^{n-1} + \cdots + a_n = X^n + b_1^p X^{n-1} + \cdots + b_n^p.$$

Thus $f(X) = h(X^p) = \left(X^n + b_1 X^{n-1} + \cdots + b_n\right)^p$, so f is not irreducible. $\square$

Example. All finite fields are perfect. Suppose F is a finite field. Then $\operatorname{ch} F = p > 0$ so $\mathbb{F}_p \subset F$ therefore $[\mathbb{F} : \mathbb{F}_p] = n < 0$, and $\dim_{\mathbb{F}_p} F = n < \infty$, so $F \cong (\mathbb{F}_p)^n$ as a vector space over $\mathbb{F}_p$, so F has p^n elements. The group $F^\times = F \setminus \{0\}$ has $p^n - 1$ elements. So for all $a \in F^\times$, $a^{p^n - 1} = 1$. For all $a \in F$, $a^{p^n} = a$, so $\left(a^{p^{n-1}}\right)^p = a$, and this shows F is perfect.

Definition 3.9. Consider $k \subset L$. An element $a \in L$ is **separable** over k if the minimal polynomial $f(X) \in k[X]$ of a is a separable polynomial.

Lecture 15 is a problems class.
Lecture 16 is a problems class.
Lecture 17 is a class test.

3.3 Separable degree

Definition 3.10. Let $k \subset K$. Choose $K \subset \Omega$ such that $k \subset \Omega$ is normal. Define the **separable degree** as

$$[K : k]_s = \# \operatorname{Em}_k(K, \Omega).$$

Remark. $[K : k]_s$ does not depend on $K \subset \Omega$. Suppose $k \subset \Omega_1$ and $k \subset \Omega_2$ are normal. Then there exists a bigger field $\widetilde{\Omega}$ such that $\Omega_1 \subset \widetilde{\Omega}$ and $\Omega_2 \subset \widetilde{\Omega}$. Then

$$\operatorname{Em}_k(K, \Omega_1) = \operatorname{Em}_k\left(K, \widetilde{\Omega}\right) = \operatorname{Em}_k(K, \Omega_2),$$

by Corollary 2.15 a while ago.

Remark. We can restate the definition of a separable extension. Recall that $k \subset K$ is separable if for all towers $k \subset K_1 \subset K_2 \subset K$, there exist $\Omega, y : K_1 \to \Omega, x_1, x_2 : K_2 \to \Omega$ such that $x_1 \neq x_2$ and $x_1|_{K_1} = x_2|_{K_2} = y$, so $[K_2 : K_1]_s \neq 1$. Thus $k \subset K$ is separable if for all towers $k \subset K_1 \subset K_2 \subset K$, $[K_2 : K_1]_s = 1$ implies that $K_1 = K_2$.

Theorem 3.11 (Tower law). *For all $k \subset K \subset L$,*

$$[L : k]_s = [L : K]_s [K : k]_s.$$

Proof. Choose $L \subset \Omega$ such that $k \subset \Omega$ is normal, so

$$
\begin{array}{c}
L \\
\cup \quad \searrow^{y} \\
K \xrightarrow[x = y|_K]{} \Omega \\
\cup \quad \curvearrowleft \\
k
\end{array}
$$

Then

$$\rho : \operatorname{Em}_k(L, \Omega) \to \operatorname{Em}_k(K, \Omega).$$

is surjective, so for all $x \in \operatorname{Em}_k(K, \Omega)$, there exists $y \in \operatorname{Em}_k(L, \Omega)$ such that $y|_K = x$, so $\rho^{-1}(x) = \operatorname{Em}_K(L, \Omega)$. Then

$$[L : k]_s = \# \operatorname{Em}_k(L, \Omega) = \sum_{x \in \operatorname{Em}_k(K, \Omega)} \# \rho^{-1}(x) = \sum_{x \in \operatorname{Em}_k(K, \Omega)} [L : K]_s = [L : K]_s [K : k]_s.$$

$\square$

3.4   Separable extensions

Recall that for $k \subset K$, we said $a \in K$ is separable over k if the minimal polynomial $f(X) \in k[X]$ of a is a separable polynomial.

Theorem 3.12. $k \subset K$ *is separable if and only if* $[K : k]_s = [K : k]$.

Proof.

Step 1. $[K : k]_s = [K : k]$ implies that $k \subset K$ is separable. Recall $[K : k]_s \leq [K : k]$. Statement follows from two tower laws for $k \subset K_1 \subset K_2 \subset K$, so $[K_2 : K_1]_s = [K_2 : K_1]$. So if $[K_2 : K_1]_s = 1$ then $[K_2 : K_1] = 1$ then $K_1 = K_2$.

Step 2. Suppose that $k \subset k(a)$ is separable then a is separable. Let $f(X) \in k[X]$ be the minimal polynomial. Suppose for a contradiction that it is not a separable polynomial. Then f is irreducible and $f \mid \mathrm{D}f$, so $\mathrm{D}f \equiv 0$, so $\mathrm{ch}\, k = p$ and there exists $h(X) \in k[X]$ irreducible such that $f = h(X^p)$. Let $b = a^p$ and consider $k \subset k(b) \subset k(a)$, so a is a root of $X^p - b \in k(b)[X]$. Then

$$p \deg h = [k(a) : k] = [k(a) : k(b)][k(b) : k] = [k(a) : k(b)] \deg h,$$

so $[k(a) : k(b)] = p$. Thus $X^p - b = (X - a)^p$ is the minimal polynomial of a over $k(b)$, so $[k(a) : k(b)]_s = 1$ contradicts step 1 and two tower laws.

Step 3. For $k \subset k(a)$, $k \subset k(a)$ is separable, so $[k(a) : k]_s = [k(a) : k]$. This is obvious from step 2. Then $[k(a) : k]$ is the degree of the minimal polynomial and $[k(a) : k]_s$ is the number of roots of minimal polynomial.

Step 4. End of proof, by a familiar method. Let us do the general case by induction on $[K : k]$. If $k = K$ then there is nothing to prove. Otherwise pick $a \in K \setminus k$. We know that both $k \subset k(a)$ and $k(a) \subset K$ are separable. Then $[K : k(a)] < [K : k]$ by tower law, hence by induction $[K : k(a)]_s = [K : k(a)]$. We also know $[k(a) : k]_s = [k(a) : k]$. Two tower laws imply that $[K : k]_s = [K : k]$.

$\square$

Corollary 3.13. *For all towers* $k \subset K \subset L$, *if* $k \subset K$ *and* $K \subset L$ *are separable then* $k \subset L$ *is separable.*

Corollary 3.14. $k \subset K$ *is separable if and only if for all* $a \in K$, a *is separable over* k.

Proof. Suppose $k \subset K$ is separable. Pick $a \in K$ then $k \subset k(a)$ is also separable. By step 2 last time, a is separable. Conversely, suppose for all $a \in K$, a is separable over k. Pick $a \in K \setminus k$. I claim $k \subset k(a)$ is separable. Then

$$[k(a) : k]_s = \#\{\text{roots of minimal polynomial } f\} = \deg f = [k(a) : k],$$

so $k \subset k(a)$ is separable. We want to show that $k(a) \subset K$ is separable, by the following lemma. $\square$

Lemma 3.15. *Let* $k \subset L \subset K$. *For* $\lambda \in K$, λ *is separable over* k *implies that* λ *is separable over* L.

Proof. The minimal polynomial over L divides the minimal polynomial over k. $\square$

4   Examples

4.1   Biquadratic extensions

Let

$$K \subset K \left(\sqrt{a \pm \sqrt{b}} \right) = L, \qquad c = a^2 - b, \qquad \beta = \sqrt{b} \notin K, \qquad \alpha = \sqrt{a + \beta} \in L, \qquad \alpha' = \sqrt{a - \beta} \in L.$$

We know that $\pm \alpha$ and $\pm \alpha'$ are the roots of

$$f(X) = X^4 - 2aX^2 + c. \tag{8}$$

This time we are not assuming (8) is irreducible. Let

$$\delta = \alpha + \alpha', \qquad \delta' = \alpha - \alpha', \qquad \gamma = \alpha \alpha' = \sqrt{c}.$$

Then

$$\gamma^2 = c, \qquad \delta^2 = 2(a + \gamma), \qquad \delta'^2 = 2(a - \gamma), \qquad \delta \delta' = 2\beta, \qquad \alpha = \frac{\delta + \delta'}{2}, \qquad \alpha' = \frac{\delta - \delta'}{2},$$

and $\pm \delta$ and $\pm \delta'$ are the roots of

$$g(Y) = Y^4 - 4aY^2 + 4b.$$

Then L is the splitting field of g. Assume

1. $\operatorname{ch} K \neq 2$, and

2. b is not a square in K, that is $[K(\beta) : K] = 2$.

Claim that the extension $K \subset L$ is separable. It is the splitting field of $f(X)$. I need to check $\gcd(f, \mathrm{D}f) = 1$, where

$$\mathrm{D}f = 4X^3 - 4aX = 4X\left(X^2 - a\right).$$

f and $\mathrm{D}f$ have no common roots, since $X = 0$ is not a root of f and $X = \pm\sqrt{a}$ is not a root of f, since $b \neq 0$.

Theorem 4.1. *Assume 1 and 2.*

1. *Suppose bc and c are not squares. Then*

$$[L : K] = 8, \qquad G = \mathcal{D}_8,$$

and $f(X)$ is irreducible.

2. *Suppose bc is a square, so c is not a square. Then*

$$[L : K] = 4, \qquad G = \mathcal{C}_4,$$

and $f(X)$ is irreducible.

3. *Suppose c is a square, so bc is not a square. Then*

   - *either $2(a + \gamma)$ and $2(a - \gamma)$ are both not squares in K, then*

$$[L : K] = 4, \qquad G = \mathcal{C}_2 \times \mathcal{C}_2,$$

   and $f(X)$ is irreducible.
   - *or one of $2(a + \gamma)$ or $2(a - \gamma)$ is a square in K, but not the other, then*

$$[L : K] = [K(\beta) : K] = 2, \qquad G = \mathcal{C}_2,$$

   and $f(X)$ is reducible.

Lemma 4.2. *Let $B \in F$ and $A \in F$ be not square in F. If B is square in $F\left(\sqrt{A}\right)$ then either B is square in F or AB is square in F.*
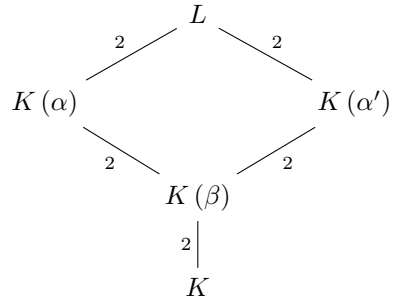
Proof. Let $B = \left(x + y\sqrt{A}\right)^2 = \left(x^2 + Ay^2\right) + 2xy\sqrt{A}$. Then

- either $x = 0$, so $B = Ay^2$, so $AB = (Ay)^2$ is square in F,

- or $y = 0$, so $B = x^2$, so $B = x^2$ is square in F.

$\square$

Proof of Theorem 4.1.

1. The strategy is $[K(\alpha) : K(\beta)] = [K(\alpha') : K(\beta)] = 2$ and $K(\alpha) \neq K(\alpha')$, so

$$
\begin{array}{ccc}
 & L & \\
{\scriptstyle 2}\nearrow & & \nwarrow{\scriptstyle 2} \\
K(\alpha) & & K(\alpha') \\
{\scriptstyle 2}\searrow & & \swarrow{\scriptstyle 2} \\
 & K(\beta) & \\
 & {\scriptstyle 2}\mid & \\
 & K &
\end{array}
\quad .
$$

- The key idea is that suppose $\alpha \in K(\beta) = \{x + y\beta \mid x, y \in K\}$. There exist $x, y \in K$ such that $\alpha = x + y\beta$. Then $(x + y\beta)^2 = a + \beta$ and $(x - y\beta)^2 = a - \beta$, so

$$K \ni \left(x^2 - y^2 b\right)^2 = \left(\left(x + y\beta\right)\left(x - y\beta\right)\right)^2 = \left(a + \beta\right)\left(a - \beta\right) = a^2 - b = c,$$

so c is a square in K. Similarly, $\alpha' \in K(\beta)$, so $\alpha \in K(\beta)$, so c is a square in K, and c is not a square therefore $\alpha \notin K(\beta)$ and $\alpha' \notin K(\beta)$, that is $[K(\alpha) : K(\beta)] = [K(\alpha') : K(\beta)] = 2$.

- Suppose for a contradiction $\alpha' \in K(\alpha)$, that is $a - \beta$ is square in $K(\alpha) = K(\beta)\left(\sqrt{a + \beta}\right)$. Apply Lemma 4.2 with

$$F = K(\beta), \qquad A = a + \beta, \qquad B = a - \beta.$$

Then either B is square in F, a contradiction, or AB is square in F, that is $(a + \beta)(a - \beta) = a^2 - b = c$ is a square in $K(\beta)$. Apply Lemma 4.2 again with

$$F = K, \qquad A = b, \qquad B = c.$$

Then either c is square in K or bc is square in K, which are contradictions. Thus $K(\alpha) \neq K(\alpha')$.

Then $\#G = 8$. Let $\sigma \in G$. Then

- either $\sigma(\beta) = \beta$, so there are four possibilities $\sigma(\alpha) = \pm\alpha$ and $\sigma(\alpha') = \pm\alpha'$,

- or $\sigma(\beta) = -\beta$, so there are four possibilities $\sigma(\alpha) = \pm\alpha'$ and $\sigma(\alpha') = \pm\alpha$, since $\sigma\left(y^2 - a - \beta\right) = y^2 - a + \beta$.

Because $\#G = 8$ all these permutations are elements of G. Thus $G = \mathcal{D}_8$ is the group of symmetries of the square

$$
\begin{array}{ccccc}
 & & \alpha' & & \\
 & \nearrow & & \searrow & \\
-\alpha & & \curvearrowleft \sigma & & \alpha \qquad \updownarrow \tau \quad . \\
 & \searrow & & \nearrow & \\
 & & -\alpha' & &
\end{array}
$$

The lattice of subgroups is

$$
\begin{array}{c}
\langle e\rangle \\
\langle\tau\rangle \quad \langle\sigma^2\tau\rangle \quad \langle\sigma^2\rangle \quad \langle\sigma\tau\rangle \quad \langle\sigma^3\tau\rangle \\
\langle\sigma^2,\tau\rangle \quad \langle\sigma\rangle \quad \langle\sigma^2,\sigma\tau\rangle \\
G
\end{array}
$$

The lattice of subfields is

$$
\begin{array}{c}
L \\
K(\alpha) \quad K(\alpha') \quad K(\beta,\gamma) \quad K(\delta) \quad K(\delta') \\
K(\beta) \quad K(\beta\gamma) \quad K(\gamma) \\
K
\end{array}
$$
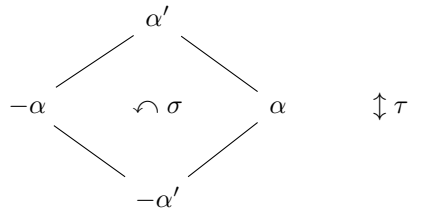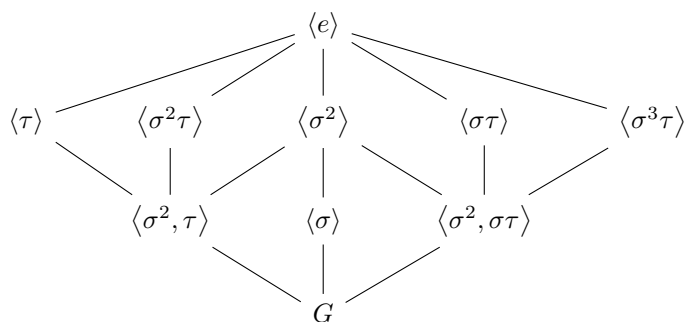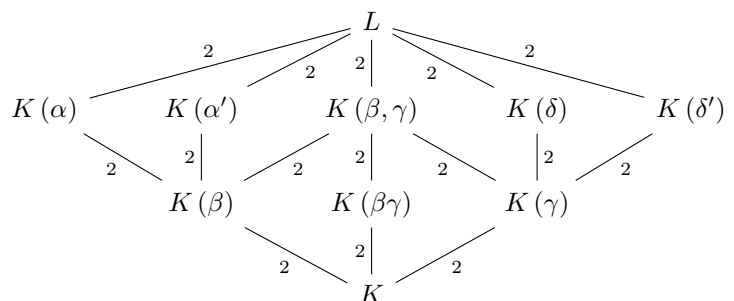
2. $K(\beta\gamma) = K$, so $K(\beta) = K(\gamma)$, where $\beta \notin K$. Suppose $a + \beta$ is square in $K(\beta)$. There exist $x, y \in K$ such that $a + \beta = (x + y\beta)^2 = x^2 + y^2 b + 2xy\beta$, so $(x - y\beta)^2 = a - \beta$, then

$$
K \ni \left(x^2 - by^2\right)^2 = \left((x + y\beta)(x - y\beta)\right)^2 = (a + \beta)(a - \beta) = a^2 - b = c,
$$

so c is square in K, a contradiction. Then

$$
L = K(\alpha) = K(\alpha') = K(\delta) = K(\delta')
$$
$$
2\,\Big|
$$
$$
K(\beta) = K(\gamma) = K(\beta,\gamma) \qquad .
$$
$$
2\,\Big|
$$
$$
K = K(\beta\gamma)
$$

Claim that $G = \mathcal{C}_4$. What's different? $\alpha\alpha' = \gamma$ and $\beta\gamma \in K$. Let $\sigma \in G$. If $\sigma(\beta) = \beta$ then $\sigma(\alpha) = \pm\alpha$.

- $\sigma(\alpha) = \alpha$ gives $\sigma(\alpha') = \alpha'$, and
- $\sigma(\alpha) = -\alpha$ gives $\sigma(\alpha') = -\alpha'$.

If $\sigma(\beta) = -\beta$ then $\sigma(\alpha) = \pm\alpha'$.

- $\sigma(\alpha) = \alpha'$ gives $\sigma(\alpha') = -\alpha$, and
- $\sigma(\alpha) = -\alpha'$ gives $\sigma(\alpha') = \alpha$.

$$
\begin{array}{c}
\alpha' \\
-\alpha \qquad \circlearrowleft \sigma \qquad \alpha \;\cdot \\
-\alpha'
\end{array}
$$

Thus $G = \mathcal{C}_4$.

3. $L = K\left(\sqrt{2\left(a \pm \gamma\right)}\right)$ is the splitting field of $g\left(Y\right) = \left(Y^2 - 2a - 2\gamma\right)\left(Y^2 - 2a + 2\gamma\right)$. Then

$$L = K\left(\delta, \delta'\right)$$

$$K\left(\beta\right) \qquad K\left(\delta\right) \qquad K\left(\delta'\right) \cdot$$

$$2 \qquad \overset{\leq 2}{\big|} \qquad \leq 2$$

$$K$$

If $[L : K] = 4$ then $G = \mathcal{C}_2 \times \mathcal{C}_2$. Note that $[L : K]$ cannot be 1. Can it be $[L : K] = 2$? At least one of $2\left(a + \gamma\right)$ and $2\left(a - \gamma\right)$ is not square in K. Suppose $2\left(a - \gamma\right)$ is not square in K. Can it be that $2\left(a + \gamma\right)$ is square in $K\left(\sqrt{2\left(a - \gamma\right)}\right) = K\left(\delta'\right)$? By Lemma 4.2

- either $2\left(a + \gamma\right)$ is square in K, which is possible,

- or $2\left(a + \gamma\right)2\left(a - \gamma\right) = 4\left(a^2 - c\right) = 4b$ is square in K, which is impossible.

The conclusion is

- either $[L : K] = 4$, $f\left(X\right)$ is irreducible, and $G = \mathcal{C}_2 \times \mathcal{C}_2$,

- or one of $2\left(a + \gamma\right)$ or $2\left(a - \gamma\right)$ is square in K but not the other, $[L : K] = 2$, $f\left(X\right)$ is not irreducible, and $G = \mathcal{C}_2$.

$\square$

Example. All over $\mathbb{Q}$.

- Let

$$f\left(X\right) = X^4 - 2, \qquad L = \mathbb{Q}\left(\sqrt{\pm\sqrt{2}}\right).$$

Then $[L : \mathbb{Q}] = 8$ and $G = \mathcal{D}_8$.

- Let

$$f\left(X\right) = X^4 - 4X^2 + 2, \qquad L = \mathbb{Q}\left(\sqrt{2 + \sqrt{2}}\right).$$

Then $[L : \mathbb{Q}] = 4$ and $G = \mathcal{C}_4$.

- Let

$$f\left(X\right) = X^4 - X^2 + 1, \qquad L = \mathbb{Q}\left(e^{\frac{2\pi i}{12}}\right) = \mathbb{Q}\left(i, \sqrt{3}\right).$$

Then $[L : \mathbb{Q}] = 4$ and $G = \mathcal{C}_2 \times \mathcal{C}_2$.

- Let

$$f\left(X\right) = X^4 - 10X^2 + 1, \qquad L = \mathbb{Q}\left(\sqrt{5 + 2\sqrt{6}}\right) = \mathbb{Q}\left(\sqrt{2} + \sqrt{3}\right) = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right).$$

Then $[L : \mathbb{Q}] = 4$ and $G = \mathcal{C}_2 \times \mathcal{C}_2$.

- Let

$$f\left(X\right) = X^4 - 6X^2 + 1 = \left(X^2 - 2X - 1\right)\left(X^2 + 2X - 1\right), \qquad L = \mathbb{Q}\left(\sqrt{3 + 2\sqrt{2}}\right) = \mathbb{Q}\left(\sqrt{2}\right).$$

Then $[L : \mathbb{Q}] = 2$ and $G = \mathcal{C}_2$.

22

4.2   Finite fields

If F is finite, then it has $\operatorname{ch} F = p$ for some prime p. Then $F_p \subset F$. Because F is finite, it is a finite-dimensional vector space over $\mathbb{F}_p$. As a vector space $F \cong (\mathbb{F}_p)^m$ where $m = \dim_{\mathbb{F}_p} F = [F : \mathbb{F}_p]$, so $\#F$ is a power of p.

Theorem 4.3. *Fix a prime $p > 0$. Then for all $m \in \mathbb{Z}_{\geq 1}$, there exists a unique, up to non-unique isomorphism, finite field with $q = p^m$ elements. The notation is $\mathbb{F}_q$. Moreover,*

$$G = \operatorname{Gal}(\mathbb{F}_q / \mathbb{F}_p) = \mathbb{Z}/m\mathbb{Z}.$$

Proof. Suppose $\#F = q$. Then $F^\times = F \setminus \{0\}$ is a group with $q - 1$ elements. That is, if $\lambda \in F \setminus \{0\}$ then $\lambda^{q-1} = 1$, and

$$\mathbb{F}_p[X] \ni X^{q-1} - 1 = \prod_{\lambda \in F \setminus \{0\}} (X - \lambda) \in \mathbb{F}_q[X].$$

Every such field is a splitting field of $X^{q-1} - 1$. Any two splitting fields are isomorphic. This does the uniqueness part. As for the existence part, let F be a splitting field over $\mathbb{F}_p$ of $f(X) = X^{q-1} - 1 \in \mathbb{F}_p[X]$. Let us prove that F has q elements. Since $\mathbb{F}_p$ is a perfect field, for all $\lambda \in \mathbb{F}_p$ there exists $\mu \in \mathbb{F}_p$ such that $\mu^p = \lambda$. In particular $f(X)$ has $q - 1$ distinct roots in F. Let us call them $\lambda_1, \dots, \lambda_{q-1}$. Claim that

$$F' = \{0, \lambda_1, \dots, \lambda_{q-1}\}$$

is a field, then clearly $F' = F$. We need to show that

- F is closed under addition,

- F is closed under multiplication, and

- things in $F \setminus \{0\}$ have inverses.

F is closed under multiplication and inverses since for all n, $\{\lambda \mid \lambda^n = 1\}$ is a group, and F is closed under addition since for all $a, b \in F$, $(a + b)^q = a^q + b^q$, for example

$$(a + b)^p = a^p + \binom{p}{1} a^{p-1} b + \dots + \binom{p}{p-1} ab^{p-1} + b^p, \qquad \forall 1 \leq k \leq p - 1, \ p \,\Big|\, \binom{p}{k}.$$

Claim that the function

$$\begin{array}{rccc} F & : & \mathbb{F}_q & \longrightarrow & \mathbb{F}_q \\ & & a & \longmapsto & a^p \end{array}$$

is a field automorphism, that is $F \in G$, of order exactly m. It is a field automorphism, since

$$F(ab) = (ab)^p = a^p b^p = F(a) F(b), \qquad F\left(\frac{a}{b}\right) = \left(\frac{a}{b}\right)^p = \frac{a^p}{b^p} = \frac{F(a)}{F(b)},$$

$$F(a + b) = (a + b)^p = a^p + b^p = F(a) + F(b), \qquad F(1) = 1, \qquad F(0) = 0.$$

Certainly $F^m = F \circ \dots \circ F = \operatorname{id}$, since for all $\lambda \in \mathbb{F}_q$, $\lambda^q = \lambda$. Otherwise if the order is $k < m$ then for all $\lambda \in \mathbb{F}_q$, $\lambda^{p^k} = \lambda$, so $X^{p^k} - X$ has $q > p^k$ roots, a contradiction. $\qquad \square$

4.3   Symmetric polynomials

Consider

$$f(X) = (X - x_1) \dots (X - x_n) = X^n - \sigma_1 X^{n-1} + \dots \pm \sigma_n \in K(x_1, \dots, x_n)[X],$$

where

$$\sigma_1 = \sigma_1(x_1, \dots, x_n) = \sum_{i \leq i \leq n} x_i, \qquad \sigma_2 = \sigma_2(x_1, \dots, x_n) = \sum_{i \leq i \leq j \leq n} x_i x_j, \qquad \dots.$$

Here $\sigma_1 \in K[x_1, \dots, x_n]$ are the **elementary symmetric polynomials**. Let

$$\delta = \prod_{\text{roots of } f} (x_i - x_j), \qquad \Delta = \delta^2 = \prod_{\text{roots of } f} (x_i - x_j)^2.$$

Definition 4.4. $\sigma \in K[x_1, \ldots, x_n]$ is **symmetric** if and only if for all $g \in \mathcal{S}_n$

$$\sigma\left(x_{g(1)}, \ldots, x_{g(n)}\right) = \sigma\left(x_1, \ldots, x_n\right).$$

Example. Consider a degree two polynomial $(X - x_1)(X - x_2) = X^2 - \sigma_1 X + \sigma_2$.

- Then $\delta = x_1 - x_2$ is not symmetric, since for $g = (12)$,

$$\delta\left(x_{g(1)}, x_{g(2)}\right) = \delta\left(x_2, x_1\right) = x_2 - x_1 = -\delta\left(x_1, x_2\right).$$

- But

$$\Delta = \delta^2 = (x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1 x_2 = \sigma_1^2 - 4\sigma_2$$

   is symmetric.

Example. Let $f(X) = X^3 - \sigma_1 X^2 + \sigma_2 X - \sigma_3$. The plan is to write an invariant telling us when a cubic has repeated roots. Then $\delta = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$ is not symmetric under $\mathcal{S}_3$, but it is invariant under $\mathcal{A}_3 = \langle (123) \rangle \cong \mathcal{C}_2$. Can I write $\delta^2 = \Delta$ as a polynomial in

$$\sigma_1 = x_1 + x_2 + x_3, \qquad \sigma_2 = x_1 x_2 + x_1 x_3 + x_2 x_3, \qquad \sigma_3 = x_1 x_2 x_3?$$

Yes,

$$\Delta = \sigma_1^2 \sigma_2^2 - 4\sigma_1^3 \sigma_3 - 4\sigma_2^3 + 18\sigma_1 \sigma_2 \sigma_3 - 27\sigma_3^2.$$

For $X^3 + 3pX + 2q$,

$$\Delta = -2^2 3^3 \left(p^3 + q^2\right).$$

The exact expression is totally relevant.

Can we find a formula for discriminant of a degree n polynomial? It is a general fact that all symmetric polynomials are polynomials in the elementary symmetric polynomials, so

$$K[x_1, \ldots, x_n]^{\mathcal{S}_n} = K[\sigma_1, \ldots, \sigma_n] \subset K(\sigma_1, \ldots, \sigma_n).$$

Theorem 4.5. *Consider a degree n separable polynomial $f(X) = X^n + a_1 X^{n-1} + \cdots + a_n \in k[X]$. Let $k \subset L$ be the splitting field of f. Then $G \subset \mathcal{A}_n$ if and only if Δ is a square in k.*

By Galois theory $\Delta \in k$, because Δ is symmetric, that is $\mathcal{S}_n$-invariant, and hence G-invariant.

Proof. $G \subset \mathcal{A}_n$ if and only if δ is G-invariant, if and only if $\delta \in k$. $\qquad\qquad\square$

Remark.

- We know $K \subset L$ is a normal and separable splitting field of $f \in K[X]$ implies that $G \subset \mathcal{S}_n$.

- If in addition $f \in k[X]$ is irreducible then G is transitive, that is for all λ and μ roots of f there exists $\sigma \in G$ such that $\sigma(\lambda) = \mu$.

Theorem 4.6. *Consider an irreducible cubic polynomial $X^3 - \sigma_1 X^2 + \sigma_2 X - \sigma_3$, and $k \subset L$ be the splitting field then $G = \mathcal{S}_3$ iff Δ is not square in k, and $G = \mathcal{A}_3 = \mathcal{C}_3$ iff Δ is square in k.*

Example. For $K = \mathbb{Q}$,

$f(X)$	Δ	G
$X^3 - X - 1$	-23	$\mathcal{S}_3$
$X^3 - 3X - 1$	81	$\mathcal{A}_3$
$X^3 - 4X - 1$	229	$\mathcal{S}_3$
$X^3 - 5X - 1$	473	$\mathcal{S}_3$
$X^3 - 6X - 1$	837	$\mathcal{S}_3$

5   Irreducible polynomials

Proposition 5.1. *Suppose* $f(X) = a_0 + \cdots + a_d X^d \in \mathbb{Z}[X]$ *has a root* $p/q \in \mathbb{Q}$ *with* $\gcd(p, q) = 1$, *then* $p \mid a_0$ *and* $q \mid a_d$.

Example.

- $X^5 - 5$ has no rational roots. Note that this does not show $X^5 - 5$ is irreducible over $\mathbb{Q}$.

- $X^3 - 2$ is irreducible over $\mathbb{Q}$.

Proof. Let $f(p/q) = a_0 + \cdots + a_d (p/q)^d = 0$. Multiplying by q^d, $a_0 q^d + \cdots + a_d p^d = 0$. Then $q \mid a_0 q^d + \cdots + a_{d-1} q p^{d-1}$, so $q \mid a_d p^d$. Note that if $c \mid ab$ and $\gcd(c, a) = 1$ then $c \mid b$. Then $\gcd(q, p^d) = 1$, so $q \mid a_d$. Similarly $p \mid a_0$. $\qquad\square$

Remark. If K is a field then $K[X]$ is a Euclidean domain, in particular unique factorisation holds, in particular $K[X]$ is an integral domain, that is for all $a, b \in K[X]$ if $ab = 0$, then either $a = 0$ or $b = 0$.

Suppose that you want to show $n \in \mathbb{Z}$ is prime. Try to factor by all primes $p < \sqrt{n}$.

Example. 97 is prime because $2 \nmid 97, 3 \nmid 97, 5 \nmid 97, 7 \nmid 97$.

A question is can such a method work with polynomials $f(X) \in \mathbb{Q}[X]$? Yes but we will not go there because it is not very practical. This method is ok in $\mathbb{F}_p[X]$, where p is prime, and this leads to a useful strategy.

Example. Is $X^5 - 5 \in \mathbb{Q}[X]$ irreducible?

- It is not irreducible in $\mathbb{F}_2[X]$ since $X^5 - 5 \equiv X^5 + 1 \mod 2$ and $X = 1$ is a root.

- It is not irreducible in $\mathbb{F}_3[X]$ since $X^5 - 5 \equiv X^5 + 1 \mod 3$ and $X = -1$ is a root.

- It is not irreducible in $\mathbb{F}_5[X]$ since $X^5 - 5 \equiv X^5 \mod 5$ and $X = 0$ is a root.

- Is it irreducible in $\mathbb{F}_7[X]$? [2]

Lemma 5.2 (Gauss' lemma). *Suppose* $f(X) = a_0 + \cdots + a_d X^d \in \mathbb{Z}[X]$ *for* $\gcd(a_0, \ldots, a_d) = 1$ *factorises non-trivially in* $\mathbb{Q}[X]$. *Then it factors non-trivially in* $\mathbb{Z}[X]$.

Corollary 5.3. *If* $f(X)$ *is prime in* $\mathbb{F}_p[X]$, *for some* p, *then it is prime in* $\mathbb{Q}[X]$.

Proof. Otherwise $f(X)$ factors in $\mathbb{F}_p[X]$. $\qquad\square$

Proof of Lemma 5.2. Suppose $f(X) = g(X) h(X)$ in $\mathbb{Q}[X]$ for $g(X), h(X) \in \mathbb{Q}[X]$. There is a $c \in \mathbb{Z}$ such that

$$cf(X) = g'(X) h'(X), \qquad g'(X), h'(X) \in \mathbb{Z}[X], \qquad g' = \lambda g, \qquad h' = \mu h, \qquad \lambda, \mu \in \mathbb{Q}. \qquad (9)$$

There is a smallest such c. I claim $c = 1$. Otherwise there exists p prime such that $p \mid c$, so (9) is

$$0 = \overline{g'}(X) \overline{h'}(X) \in \mathbb{F}_p[X].$$

Either $p \mid g'(X)$, that is p divides all coefficients of g', or $p \mid h'(X)$, a contradiction. $\qquad\square$

Corollary 5.4 (Eisenstein). $f(X) = a_0 + \cdots + a_d X^d \in \mathbb{Z}[X]$ *is irreducible in* $\mathbb{Q}[X]$ *if there exists* p *prime such that* $p \nmid a_d$ *but* $p \mid a_i$ *for* $i < d$ *and* $p^2 \nmid a_0$.

Proof. Work in $\mathbb{F}_p[X]$. Then $f(X) \equiv a_d X^d \mod p$. If $f(X) = h(X) g(X)$ in $\mathbb{Z}[X]$, then

$$h(X) \equiv b_k X^k \mod p, \qquad g(X) \equiv c_{d-k} X^{d-k} \mod p,$$

and that means that $h(X) = b_0 + \cdots + b_k X^k$ and $p \mid b_i$ for $i < k$, and $g(X) = c_0 + \cdots + c_{d-k} X^{d-k}$ and $p \mid c_i$ for $i < d - k$. Thus $p^2 \mid a_0 = b_0 c_0$, a contradiction. $\qquad\square$

Example. $X^5 - 5$ is irreducible by Eisenstein and $p = 5$.

Lecture 25 is a problems class.
Lecture 26 is a problems class.

---

[2]Exercise

6   Reduction modulo prime

Theorem 6.1. *Let $f(X) \in \mathbb{Z}[X]$ be monic of degree n, $\mathbb{Q} \subset K$ be the splitting field of f, and $G = \mathrm{Gal}(K/\mathbb{Q}) \subset \mathcal{S}_n$. For p prime, denote by $\overline{f}$ as f viewed in $\mathbb{F}_p[X]$. If there exists p such that $\overline{f} \in \mathbb{F}_p[X]$ has n distinct roots in a splitting field and $\overline{f} = \prod_{i=1}^{k} \overline{f_i}(X) \in \mathbb{F}_p[X]$, with $\overline{f_i} \in \mathbb{F}_p[X]$ irreducible of degree n_i, then there exists $\sigma \in G \subset \mathcal{S}_n$ of cycle decomposition type*

$$(n_1)\ldots(n_k).$$

The plan is to understand the statement and prove it, following Jacobson's basic algebra I page 301. I want to use Theorem 6.1 to write down an explicit degree five polynomial $f \in \mathbb{Z}[X]$ such that $G = \mathcal{S}_5$.

Proposition 6.2. *Suppose that r is prime and let $G \subset \mathcal{S}_r$ be a subgroup. If G contains an r-cycle and one transposition, then $G = \mathcal{S}_r$.*

Proof. Say $\sigma = (12345) \in G$ and $(12) \in G$, by relabelling. Then $\sigma^{-i}(12)\sigma^i = ((1-i)(2-i))$ implies that $(12),(23),(34),(45) \in G$. A general fact is that for all n, $(12),\ldots,((n-1)n)$ generate $\mathcal{S}_n$, since $a < b$ implies that $(ab) = (a(a+1))((a+1)b)(a(a+1))$. $\qquad\square$

The following is the plan.

- Find an irreducible monic degree five $\phi(X) \in \mathbb{F}_2[X]$.

- Find an irreducible monic degree two $\psi(X) \in \mathbb{F}_3[X]$.

- Find $f \in \mathbb{Z}[X]$ such that $f \equiv \phi$ in $\mathbb{F}_2[X]$ and $f \equiv X(X-1)(X+1)\psi$ in $\mathbb{F}_3[X]$.

Theorem 6.1 implies that $G = \mathcal{S}_5$.

- The irreducible degree two polynomial in $\mathbb{F}_2[X]$ is $X^2 + X + 1$.

- The irreducible degree two polynomials in $\mathbb{F}_3[X]$ are $X^2 + 1$, and two more.

Claim that

$$f \equiv \phi(X) = X^5 + X^3 + 1 \in \mathbb{F}_2[X]$$

is irreducible. Need to check that ϕ has no root in $\mathbb{F}_2$ and ϕ is not divisible by $X^2 + X + 1$. Then

$$f \equiv X(X-1)(X+1)(X^2+1) = X^5 - X \in \mathbb{F}_3[X].$$

Thus

$$f(X) = X^5 + 3X^3 + 2X + 3.$$

Definition 6.3. The **character** of a monoid P to K is $\chi : P \to K$ such that

- $\chi(0) = 1$, and

- for all $p_1, p_2 \in P$, $\chi(p_1 + p_2) = \chi(p_1)\chi(p_2)$.

Remark. If K is a field and A is a set then $\{f : A \to K\}$ is a K-vector space.

Theorem 6.4 (Linear independence of characters, Dedekind independence theorem)**.** *Let K be a field and P be a monoid, such as $P = \mathbb{N}$. Any set of distinct non-zero characters*

$$\chi_1 : P \to K, \qquad \ldots, \qquad \chi_n : P \to K, \qquad \ldots$$

is linearly independent in the vector space $\{f : P \to K\}$.

Proof. Assume for a contradiction that

$$\lambda_1\chi_1 + \cdots + \lambda_n\chi_n = 0. \tag{10}$$

We may assume (10) to be the shortest. We may assume for all i, $\lambda_i \neq 0$, and $n \geq 2$, since all are not zero. There exists p such that $\chi_1(p) \neq \chi_2(p)$, so

$$\lambda_1\chi_1(p)\chi_1 + \cdots + \lambda_n\chi_n(p)\chi_n = 0. \tag{11}$$

Because (10) is the shortest then (10) and (11) are multiples of each other, so $\chi_1(p) = \chi_2(p)$, a contradiction. $\qquad\square$

Theorem 6.5. *Let $f(X) \in \mathbb{Z}[X]$ be degree n monic, $\mathbb{Q} \subset K$ be the splitting field of f, $G = \mathrm{Gal}(K/\mathbb{Q}) \subset \mathcal{S}_n$, and $\lambda_1, \ldots, \lambda_n \in K$ be the roots of $f(X)$. Let p be a prime. Denote by $\overline{f}$ the image of f modulo p. Assume $\overline{f}$ is separable. Let $\mathbb{F}_p \subset F$ be a splitting field for $\overline{f}$, so $\overline{f}$ has n distinct roots in F. Let $R \subset K$ be the subring generated by the roots of f, so $R = \mathbb{Z}[\lambda_1, \ldots, \lambda_n]$. Then*

    1. there exists a ring homomorphism $\psi : R \to F$,

    2. if $\psi' : R \to F$ is a ring homomorphism then ψ' induces a bijection

$$\phi' : \{\text{roots of } f(X) \ \text{in } R\} \to \{\text{roots of } \overline{f}(X) \ \text{in } F\},$$

    3. $\psi' : R \to F$ is a ring homomorphism if and only if there exists $\sigma \in G$ such that $\psi' = \psi \circ \sigma$.

Lecture 29 is a class test.

Proof.

Step 1. R is a finitely generated free $\mathbb{Z}$-module, since R is generated as a $\mathbb{Z}$-module by $\lambda_1^{e_1}, \ldots, \lambda_n^{e_n}$ where $0 \le e_i < n$.

Step 2. Let $u_1, \ldots, u_d$ be a basis of R as $\mathbb{Z}$-module. This is a basis of K as a $\mathbb{Q}$-vector space, so $d = [K : \mathbb{Q}]$. Then $u_1, \ldots, u_d$ are clearly linearly dependent over $\mathbb{Q}$. Next let $\mathbb{Q} \subset \mathbb{Q}R \subset K$. Then $\mathbb{Q}R$ is a subring containing $\mathbb{Q}$, so $\mathbb{Q}R$ is a field. If $K \subset L$ is finite and $K \subset R \subset L$ then R is a ring implies that R is a field. [3] Then $\mathbb{Q}R$ contains all roots of f, so $\mathbb{Q}R = K$, that is $u_1, \ldots, u_d$ generate K over $\mathbb{Q}$.

Step 3. Proof of 1. Let $\mathfrak{m} \supset \langle p \rangle$ be a maximal ideal in R then $\mathbb{F}_p \subset R/\mathfrak{m}$ is a finite field. Then $\pi : R \to R/\mathfrak{m}$ gives

$$f(X) = \prod_{i=1}^{n} (X - \lambda_i) \mapsto \overline{f}(X) = \prod_{i=1}^{n} (X - \pi(\lambda_i)),$$

that is $\overline{f}(X)$ splits in $R/\mathfrak{m}[X]$. Then R is generated by λ_i implies that $R/\mathfrak{m}$ is generated by $\pi(\lambda_i)$, so $R/\mathfrak{m}$ is a splitting field for $\overline{f} \in \mathbb{F}_p[X]$. Thus $R/\mathfrak{m} \cong F$.

Step 4. Proof of 2. Easy. $\psi' : R \to F$ gives

$$f(X) = \prod_{i=1}^{n} (X - \lambda_i) \mapsto \overline{f}(X) = \prod_{i=1}^{n} (X - \pi(\lambda_i)),$$

so $\{\lambda_i\} \mapsto \{\pi(\lambda_i)\}$.

Step 5. Proof of 3. The converse is obvious. Let $\sigma \in G$ and $G = \{\sigma_1, \ldots, \sigma_N\}$ for $\mathrm{rk}_{\mathbb{Z}} R = N = [K : \mathbb{Q}]$. Consider $\psi_i = \psi \circ \sigma_i : P \to F$ where $P = (R \setminus \{0\}, \times)$ is a semigroup. Suppose $\psi_{N+1} : P \to F$ is another character. If for all i, $\psi_{N+1} \ne \psi_i$, we will derive a contradiction. Let $r_1, \ldots, r_N$ be a basis of R as a $\mathbb{Z}$-module. Solve for $x_i \in F$ for $i = 1, \ldots, N$ in

$$\left\{ \sum_{i=1}^{N+1} x_i \psi_i(r_j) = 0 \ \middle| \ 1 \le j \le N \right\},$$

which has N equations in $(N+1)$ variables in F. Since r_j is a $\mathbb{Z}$-basis this implies $\sum_{i=1}^{N+1} x_i \psi_j = 0$, and this contradicts Dedekind.

$\square$

Proof of Theorem 6.1. Let R and $\psi : R \to F$ be as above. Consider $Fr \in \mathrm{Gal}(F/\mathbb{F}_p)$ then $\psi' = Fr \circ \psi : R \to F$ is a ring homomorphism. By Theorem 6.5.3 there exists $\sigma \in G$ such that $Fr \circ \psi = \psi \circ \sigma$. $\square$

---

[3]Exercise