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

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

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*

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

*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

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

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 $G = C_2$ 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 $K(x) = L$.

1 Main 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 $f = x^n + a_1 x^{n-1} + \dots + a_n$.

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

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

Lecture 4 Thursday 17/01/19

Definition 1.1. $K \subset L$ is **finite** if L is finite-dimensional as a vector space over K. The **degree** of L over K is

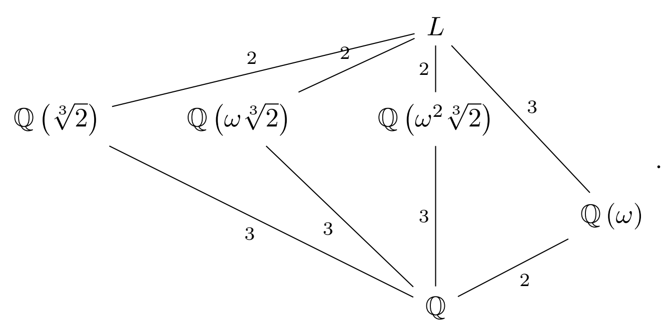
$$[L : K] = \dim_K(L).$$

Theorem 1.2 (Tower law)**.** *Let $K \subset L \subset F$. Then*

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

Theorem 1.3. *Suppose $f(x) \in K[x]$ is irreducible of degree $d = \deg(f)$ and $L = K(\lambda)$ where $f(\lambda) = 0$, then $[K(\lambda) : K] = d$.*

$K = \mathbb{Q}\left(\sqrt[3]{2}\right)$ is a field, and $[K : \mathbb{Q}] = 3$. 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 (Exercise)

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

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,

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

- Either $x^2 + 3$ is irreducible over $\mathbb{Q}\left(\sqrt[3]{2}\right)$, so by Theorem 1.3 $\left[L : \mathbb{Q}\left(\sqrt[3]{2}\right)\right] = 2$ 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 $[K : \mathbb{Q}] = 2$.

$$\begin{tikzcd}[column sep=small]
 & L \arrow[d, no head] \arrow[ddl, no head, "3"'] & \\
 & K(\omega) \arrow[dl, no head] \arrow[dr, no head] & \\
K \arrow[dr, no head, "2"'] & & \mathbb{Q}(\omega) \arrow[dl, no head, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}.$$

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

$$\begin{tikzcd}[column sep=small]
L \arrow[dd, no head, "2"'] \arrow[dr, no head] & \\
 & K\left(\sqrt[3]{2}\right) \arrow[dl, no head] \\
K \arrow[d, no head, "3"'] & \\
\mathbb{Q} &
\end{tikzcd}.$$

  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 1.2. 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, $\lambda_{ij} = 0$.

□

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

$$\begin{tikzcd}
 & & \{e\} \arrow[dll, dash, "2"'] \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "3"] & \\
\left\langle \begin{pmatrix} 2 & 3 \end{pmatrix} \right\rangle & \left\langle \begin{pmatrix} 1 & 2 \end{pmatrix} \right\rangle & \left\langle \begin{pmatrix} 1 & 3 \end{pmatrix} \right\rangle & \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \\
 & & G \arrow[ull, dash, "3"] \arrow[ul, dash, "3"] \arrow[u, dash, "3"] \arrow[ur, dash, "2"'] &
\end{tikzcd}.$$

$\mathbb{Q}(\omega)/\mathbb{Q}$ 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 Elementary facts

Lecture 6 Tuesday 22/01/19

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

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

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

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

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

- *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. ∎

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 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,*

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

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

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

  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

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

$\square$

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. $\square$

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 let

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

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.

3 Axiomatics

Proposition 3.1. *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 $a \in K \setminus k$.

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

Consider the restriction map

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

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

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

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 3.2. *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 3.3. *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 3.3 follows from the following lemma.

Lemma 3.4. *$K \subset L$ is a finite extension of degree $[L : K] \le |G|$.*

Proof of Proposition 3.3. From Proposition 3.1, $Aut_K(L) = Em_K(L, L)$ 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 3.4. 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 $1 \le k \le n+1$ 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 $x_i \in K$. 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 $\sigma \in G$.

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

Note that

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

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 $(3) - (4)$,

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

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

4 Galois correspondence

Definition 4.1. $k \subset K$ is **normal** if

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

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

Equivalently, $k \subset K$ is normal if

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

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 gives

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

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

Lecture 11 Friday 01/02/19

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

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

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

Lemma 4.2. *Suppose $k \subset K$ is normal. Consider $k \subset L \subset K$. Then also $L \subset K$ is normal.*

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

Warning.

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

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

  $k \subset K$ 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 4.3. $k \subset K$ 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

$$\begin{tikzcd}
K & & & \Omega & \\
K_2 \arrow[u, hook] \arrow[r, dotted, "y_1"] \arrow[rrrr, dotted, bend right, "y_2"'] & y_1(K_2) \arrow[urr, hook] & & & y_2(K_2) \arrow[ul, hook'] \\
K_1 \arrow[u, hook] \arrow[rr, "x"] & & x(K_1) \arrow[ul, hook] \arrow[urr, hook'] & & \\
k \arrow[u, hook] & & & &
\end{tikzcd} .$$

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 4.4. *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 4.5 (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

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

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 $\sigma(\lambda) \neq \lambda$.

$\square$

Lecture 12
Tuesday
05/02/19

Lemma 4.6. *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.*

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

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

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

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

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

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

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

Corollary 4.7. *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 $\sigma \in Em_k(F, \Omega)$, $\sigma(F) \subset K$.

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

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

5 Normal extensions

Theorem 5.1. *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 $\lambda_1, \dots, \lambda_m \in K$ such that $K = k(\lambda_1, \dots, \lambda_m)$. 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 $\mu \in K$.

$\square$

(Exercise: prove that any two splitting fields of $f \in k[x]$ are k-isomorphic, not necessarily in a unique way) Lecture 13 Thursday 07/02/19

Proposition 5.2. *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 $\lambda_1, \dots, \lambda_n \in L$ such that $L = k(\lambda_1, \dots, \lambda_n)$. 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. Key point is argue that K is generated by the roots of f over k. $\square$

6 Separable polynomials

Definition 6.1. 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 $x^p - a = (x-a)^p$ 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

$$K = \frac{\mathbb{F}_p(t)[u]}{\langle u^p - t \rangle} = \mathbb{F}_p(u).$$

In $K[x]$, $x^p - t = (x-u)^p$.

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

$$D : \begin{array}{ccc} k[x] & \to & k[x] \\ x^n & \mapsto & nx^{n-1} \end{array},$$

and extend linearly to all of $k[x]$. The following are some properties.

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

$$D(\lambda f + \mu g) = \lambda Df + \mu Dg.$$

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

$$D(fg) = fDg + gDf.$$

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

Proposition 6.2. *$f(x) \in k[x]$ is separable if and only if* $\gcd(f, Df) = 1$.

In $\mathbb{R}[x]$, f is inseparable if and only if there exists a multiple root, a critical point, which is a root of Df. Lecture 14 Friday 08/02/19

Lemma 6.3. *Let $f, g \in k[x]$ and $c = \gcd(f, g)$ in $k[x]$. Let $k \subset L$ be an extension. Then $c = \gcd(f, g)$ in $L[x]$.*

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

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

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

Proof of Proposition 6.2. Let $k \subset L$ be any field where f splits completely. We can do the proof in $L[x]$. That is, we may assume that f splits completely, so

$$f(x) = \prod_i (x - \lambda i).$$

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

$$Df(x) = 2(x-\lambda) g(x) + (x-\lambda)^2 Dg(x) = (x-\lambda)(2y(x) + (x-\lambda) Dg(x)).$$

That is, $(x-\lambda) \mid f$ and $(x-\lambda) \mid Df$, so $\gcd(f, Df) \neq 1$.

$\implies$ For all $i \neq j$, $\lambda_i \neq \lambda_j$.

$$Df = \sum_{i=1}^{j} \left(\prod_{j \neq i} (x - \lambda_j) \right).$$

Claim that for all i, $(x - \lambda_i) \nmid Df$. I hope you see this. This shows $\gcd(f, Df) = 1$.

$\square$

Theorem 6.4. *$f \in k[x]$ irreducible is inseparable if and only if*

- *$ch(k) = p > 0$, and*
- *there exists $h \in k[x]$ such that $f(x) = h(x^p)$.*

Proof. Indeed f is inseparable if and only if $\gcd(f, Df) \neq 1$, if and only if $Df = 0$, since f is irreducible so $\gcd(f, Df) \neq 1$ if and only if $f \mid Df$, and $\deg(Df) < \deg(f)$. $\square$

Definition 6.5. A field k in $ch(k) = p > 0$ is **perfect** if for all $a \in k$ there exists $b \in k$ such that $b^p = a$.

Proposition 6.6. *If k is perfect then $f \in k[x]$ is irreducible gives that $f(x)$ is separable.*

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

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

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 $ch(F) = p > 0$ so $\mathbb{F}_p \subset F$ therefore $[\mathbb{F} : \mathbb{F}_p] = n < 0$. $\dim_{\mathbb{F}_p}(F) = n < \infty$, so $F \cong (\mathbb{F}_p)^n$ as a vector space over $\mathbb{F}_p$ gives that 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 6.7. Consider $k \subset K$. 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 Tuesday 12/02/19

Lecture 15 is a problem class.

Lecture 16 Thursday 14/02/19

Lecture 16 is a problem class.

Lecture 17 Friday 15/02/19

Lecture 17 is a test.

7 Separable degree

Lecture 18
Tuesday
19/02/19

Definition 7.1. Let $k \subset K$. Choose $K \subset \Omega$ such that $k \subset \Omega$ is normal. Define the **separable degree** as

$$[K : k]_s = |Em_k(K, \Omega)|.$$

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

$$Em_k(K, \Omega_1) = Em_k\left(K, \widetilde{\Omega}\right) = Em_k(K, \Omega_2),$$

by one of the corollaries a while ago,

$$\begin{tikzcd} \Omega_1 \arrow[dr, dotted, "\widetilde{\sigma}"] & \\ \cup & \\ K \arrow[r, "\sigma"'] & \widetilde{\Omega} \\ \cup & \\ k & \end{tikzcd}.$$

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

$$\begin{tikzcd} K_2 \arrow[dr, dotted, "x_1, x_2"] & \\ \cup & \\ K_1 \arrow[r, "y"'] & \Omega \\ \cup & \\ k & \end{tikzcd},$$

that is $[K_2 : K_1]_s \neq 1$. Thus $k \subset K$ is separable if for all towers $k \subset K_1 \subset K_2 \subset K$,

$$[K_2 : K_1]_s = 1 \qquad \implies \qquad K_1 = K_2.$$

Theorem 7.2 (Tower law)**.** *For all $k \subset K \subset L$,*

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

Proof. Choose $L \subset \Omega$ and $k \subset \Omega$ normal, so

$$\begin{tikzcd} L \arrow[dr, dotted, "y"] & \\ \cup & \\ K \arrow[r, "x = y|_K"'] & \Omega \\ \cup & \\ k & \end{tikzcd}.$$

Study

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

ρ is surjective. For all $x \in Em_k(K, \Omega)$, there exists $y \in Em_k(L, \Omega)$ such that $y |_K = x$. $\rho^{-1}(x) = Em_K(L, \Omega)$. Then

$$[L : k]_s = |Em_k(L, \Omega)| = \sum_{x \in Em_k(K, \Omega)} \left|\rho^{-1}(x)\right| = \sum_{x \in Em_k(K, \Omega)} [L : K]_s = [L : K]_s [K : k]_s.$$

□

8 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 8.1. *$k \subset K$ is separable if and only if $[K : k]_s = [K : k]$.*

Proof.

Step 1. $[K : k]_s = [K : k]$ gives $k \subset K$ is separable. Recall $[K : k]_s \le [K : k]$. 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. f is irreducible and $f \mid Df$ gives that $Df \equiv 0$ so $ch(k) = p$ and there exists $h(x) \in k[x]$ irreducible such that $f = h(x^p)$. Let $b = a^p$ and consider $k \subset k(b) \subset k(a)$. a is a root of $x^p - b \in k(b)[x]$.

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

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 gives $[k(a) : k]_s = [k(a) : k]$. This is obvious from step 2. $[k(a) : k]$ 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. $[K : k(a)] < [K : k]$ 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 give $[K : k]_s = [K : k]$.

□

Lecture 19 Thursday 21/02/19

Corollary 8.2. *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 8.3. *$k \subset K$ 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. □

Lemma 8.4. *Let $k \subset L \subset K$. For $\lambda \in K$, λ is separable over k gives that λ is separable over L.*

Proof. The minimal polynomial over L divides the minimal polynomial over k. □

9 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 $\pm\alpha, \pm\alpha'$ 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 $\pm\delta, \pm\delta'$ are the roots of

$$g(y) = y^4 - 4ay^2 + 4b.$$

L is the splitting field of g. Assume

1. $ch(K) \neq 2$, 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 $\gcd(f, Df) = 1$.

$$Df = 4x^3 - 4ax = 4x\left(x^2 - a\right).$$

f, Df 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 9.1. *Assume* 1 *and* 2*.*

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

$$[L : K] = 8, \qquad G = D_8,$$

and $f(x)$ is irreducible.

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

$$[L : K] = 4, \qquad G = C_4,$$

and $f(x)$ is irreducible.

3. *Suppose c is a square, so bc is not a square. Then*
   - *either $2(a+\gamma), 2(a-\gamma)$ both not squares in K, then*

   $$[L : K] = 4, \qquad G = C_2 \times C_2,$$

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

   $$[L : K] = [K(\beta) : K] = 2, \qquad G = C_2,$$

   and $f(x)$ is reducible.

Lecture 20
Friday
22/02/19

Lemma 9.2. *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 $B = Ay^2$ gives that $AB = (Ay)^2$ is square in F,
- or $y = 0$, so $B = x^2$ gives that $B = x^2$ is square in F.

□

Proof of Theorem 9.1.

1. Strategy is $[K(\alpha) : K(\beta)] = [K(\alpha') : K(\beta)] = 2$ and $K(\alpha) \neq K(\alpha')$.

$$\begin{tikzcd} & L \arrow[dl, dash, "2"'] \arrow[dr, dash, "2"] & \\ K(\alpha) \arrow[dr, dash, "2"'] & & K(\alpha') \arrow[dl, dash, "2"] \\ & K(\beta) \arrow[d, dash, "2"'] & \\ & K & \end{tikzcd}.$$

- 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 $\alpha = x + y\beta$. $(x + y\beta)^2 = a + \beta$ and $(x - y\beta)^2 = a - \beta$ gives

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

so c is a square in K. Similarly, $\alpha' \in K(\beta)$ gives $\alpha \in K(\beta)$, so c is a square in K. 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 9.2 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 9.2 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 $K(\alpha) \neq K(\alpha')$.

$|G| = 8$. 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 $G = D_8$ is the group of symmetries of the square

$$\begin{tikzcd} & \alpha' \arrow[dl, dash] \arrow[dr, dash] & & \\ -\alpha \arrow[dr, dash] & \curvearrowleft \sigma & \alpha \arrow[dl, dash] & \updownarrow \tau \\ & -\alpha' & & \end{tikzcd}.$$

The lattice of subgroups is

$$
\begin{tikzcd}[column sep=small]
 & & & & \{e\} \arrow[dllll, dash] \arrow[dll, dash] \arrow[d, dash] \arrow[drr, dash] \arrow[drrrr, dash] & & & & \\
\langle \tau \rangle \arrow[drr, dash] & & \langle \sigma^2\tau \rangle \arrow[d, dash] & & \langle \sigma^2 \rangle \arrow[dll, dash] \arrow[d, dash] \arrow[drr, dash] & & \langle \sigma\tau \rangle \arrow[d, dash] & & \langle \sigma^3\tau \rangle \arrow[dll, dash] \\
 & & \langle \sigma^2, \tau \rangle \arrow[drr, dash] & & \langle \sigma \rangle \arrow[d, dash] & & \langle \sigma^2, \sigma\tau \rangle \arrow[dll, dash] & & \\
 & & & & G & & & &
\end{tikzcd}
.
$$

The lattice of subfields is

$$
\begin{tikzcd}[column sep=small]
 & & & & L \arrow[dllll, dash, "2"'] \arrow[dll, dash, "2"] \arrow[d, dash, "2"'] \arrow[drr, dash, "2"'] \arrow[drrrr, dash, "2"] & & & & \\
K(\alpha) \arrow[drr, dash, "2"'] & & K(\alpha') \arrow[d, dash, "2"'] & & K(\beta,\gamma) \arrow[dll, dash, "2"] \arrow[d, dash, "2"'] \arrow[drr, dash, "2"'] & & K(\delta) \arrow[d, dash, "2"] & & K(\delta') \arrow[dll, dash, "2"] \\
 & & K(\beta) \arrow[drr, dash, "2"'] & & K(\beta\gamma) \arrow[d, dash, "2"'] & & K(\gamma) \arrow[dll, dash, "2"] & & \\
 & & & & K & & & &
\end{tikzcd}
.
$$

Lecture 21 Tuesday 26/02/19

2. $K(\beta\gamma) = K$, so $K(\beta) = K(\gamma)$. $\beta \notin K$. 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

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

so c is square in K, a contradiction.

$$
\begin{tikzcd}
L = K(\alpha) = K(\alpha') = K(\delta) = K(\delta') \arrow[d, dash, "2"'] \\
K(\beta) = K(\gamma) = K(\beta, \gamma) \arrow[d, dash, "2"'] \\
K = K(\beta\gamma)
\end{tikzcd}
.
$$

Claim that $G = C_4$. 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 $\sigma(\alpha') = \alpha$.

$$
\begin{tikzcd}
 & \alpha' \arrow[dl, dash] \arrow[dr, dash] & \\
-\alpha \arrow[dr, dash] & \curvearrowleft \sigma & \alpha \arrow[dl, dash] \\
 & -\alpha' &
\end{tikzcd}
.
$$

Thus $G = C_4$.

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

$$\begin{tikzcd}
& L = K(\delta, \delta') \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
K(\beta) \arrow[dr, dash, "2"'] & K(\delta) \arrow[d, dash, "\leq 2"'] & K(\delta') \arrow[dl, dash, "\leq 2"] \\
& K &
\end{tikzcd}.$$

If $[L : K] = 4$ then $G = C_2 \times C_2$. Note that $[L : K]$ cannot be 1. Can it be $[L : K] = 2$? At least one of $2(a + \gamma), 2(a - \gamma)$ is not square in K. Suppose $2(a - \gamma)$ is not square in K. Can it be that $2(a + \gamma)$ is square in $K\left(\sqrt{2(a - \gamma)}\right) = K(\delta')$? By Lemma 9.2

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

Conclusion is

- either $[L : K] = 4$, $f(x)$ is irreducible, and $G = C_2 \times C_2$,
- or one of $2(a + \gamma), 2(a - \gamma)$ is square in K but not the other, $[L : K] = 2$, $f(x)$ is not irreducible, and $G = C_2$.

$\square$

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

- Let
$$f(x) = x^4 - 2, \qquad L = \mathbb{Q}\left(\sqrt{\pm\sqrt{2}}\right).$$
Then $[L : \mathbb{Q}] = 8$ and $G = D_8$.
- Let
$$f(x) = x^4 - 4x^2 + 2, \qquad L = \mathbb{Q}\left(\sqrt{2 + \sqrt{2}}\right).$$
Then $[L : \mathbb{Q}] = 4$ and $G = C_4$.
- Let
$$f(x) = x^4 - x^2 + 1, \qquad L = \mathbb{Q}\left(e^{\frac{2\pi i}{12}}\right) = \mathbb{Q}\left(i, \sqrt{3}\right).$$
Then $[L : \mathbb{Q}] = 4$ and $G = C_2 \times C_2$.
- Let
$$f(x) = x^4 - 10x^2 + 1, \qquad L = \mathbb{Q}\left(\sqrt{5 + 2\sqrt{6}}\right) = \mathbb{Q}\left(\sqrt{2} + \sqrt{3}\right) = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right).$$
Then $[L : \mathbb{Q}] = 4$ and $G = C_2 \times C_2$.
- Let
$$f(x) = x^4 - 6x^2 + 1 = \left(x^2 - 2x - 1\right)\left(x^2 + 2x - 1\right), \qquad L = \mathbb{Q}\left(\sqrt{3 + 2\sqrt{2}}\right) = \mathbb{Q}\left(\sqrt{2}\right).$$
Then $[L : \mathbb{Q}] = 2$ and $G = C_2$.

10 Finite fields

Lecture 22 Thursday 28/02/19

If F is finite, then it has $ch(F) = p$ 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 10.1. *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. Notation is $\mathbb{F}_q$. Moreover, $G = Gal_{\mathbb{F}_p}(\mathbb{F}_q) = \mathbb{Z}/m\mathbb{Z}$.*

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

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

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. $\mathbb{F}_p$ is a perfect field, so 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. F is closed under addition since for all $a, b \in F$, $(a+b)^q = a^q + b^q$, for example

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

Claim that the function

$$\begin{array}{cccc} F : & \mathbb{F}_q & \to & \mathbb{F}_q \\ & a & \mapsto & a^p \end{array}$$

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 $F^m = F \circ \dots \circ F = id$, since for all $\lambda \in \mathbb{F}_q$, $\lambda^q = \lambda$. Otherwise if 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. $\square$