M3P11 Galois Theory

Lectured by Prof Alessio Corti Typeset by David Kurniadi Angdinata

Spring 2019

M3P11	Galois	Theory

C	_	n	+	_	n	4	_
	n	n	т.	ω	n	Т.	S

0	Introduction	9
1	What is Galois theory?	4

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
- $\bullet\,$ M Reid, Galois theory, 2014

Lecture 1 Thursday 10/01/19

1 What is Galois theory?

Notation 1.1. 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 1.2.

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

$$\mathbb{Q}\left(\sqrt{2}\right) = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\} = \frac{\mathbb{Q}\left[x\right]}{\langle x^2 - 2\rangle}.$$

It is also a field, 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,

$$\frac{K\left[x\right]}{\left\langle f\left(x\right)\right\rangle }$$

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.
- \bullet For K a field,

$$K\left(x\right) = Frac\left(K\left[x\right]\right) = \left\{\phi\left(x\right) = \frac{f\left(x\right)}{g\left(x\right)} \;\middle|\; f, g \in K\left[x\right], \; g \neq 0\right\}.$$

is also a field, the field of rational functions with coefficients in K. For example, $\mathbb{F}_p(x, Y) = \mathbb{F}_p(x)(Y)$.

Example 1.3. Consider algebraic equations in a field K.

• Quadratic $ax^2 + bx^2 + c = 0$ for $a, b, c \in K$. There is a formula

$$x = \frac{-b + \sqrt{b^2 - 4ac}}{2a}.$$

• For 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.

Definition 1.4. A field homomorphism is a function $\phi: K_1 \to K_2$ that preserves the field operations, for all $a, b \in K_1$,

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

Remark 1.5. All field homomorphisms are injective. If $a \in K_1 \setminus \{0\}$, then there exists $b \in K_1$ such that ab = 1, then $\phi(a) \phi(b) = 1$, so $\phi(a) \neq 0$. This easily implies ϕ is injective. If $a_1 \neq a_2$, then $a_1 - a_n \neq 0$, so $\phi(a_1 - a_2) = \phi(a_1) - \phi(a_2) \neq 0$. Then $\phi(a_1) \neq \phi(a_2)$.

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

Example 1.6. There are two very different cases exemplified in $\mathbb{Q} \subset \mathbb{C}$.

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

Definition 1.7.

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

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

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

Example 1.9.

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

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

- 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. $K = \mathbb{Q}\left(\sqrt[3]{2},\omega\right)$, 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 1.10 (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

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

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

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

Lecture 3 Tuesday 15/01/19

Example 1.11. Let $\deg(f) = 2$ and $f(x) = x^2 + 2Ax + B \in K[x]$. If K already contains the roots then L = K and $G = \{id\}$. Suppose K does not contain the roots. We still have quadratic formula

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

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

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

Then $K \subset L$ and

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

is generated by

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

Further specialisation is the following.

• Let $K = \mathbb{R}$ and $\Delta = -1$. Then

$$L = \mathbb{C} = \left\{ a + b\sqrt{-1} \mid a, b \in \mathbb{R} \right\},\,$$

and $G = C_2$ is generated by

$$\sigma: a + b\sqrt{-1} \mapsto a - b\sqrt{-1}$$
,

complex conjugation.

• Let $K = \mathbb{Q}$ and $\Delta = 2$. Then

$$L = \left\{ a + b\sqrt{2} \mid a, b \in \mathbb{Q} \right\},\,$$

and $G = C_2$ is generated by

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

Theorem 1.10 implies there does not exist $K \subsetneq K_1 \subsetneq K\left(\sqrt{\Delta}\right) = L$. Is this obvious? Consider $x \in L \setminus K$, so $x = a + b\sqrt{\Delta}$, and $b \neq 0$, and then

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

so K(x) = L.

Example 1.12. Let $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ and $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$, where $\omega = \frac{-1 + i\sqrt{3}}{2}$. ω is a solution of $x^2 + x + 1 = 0$. Then

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

Remark 1.13. For any splitting field of f, there is always a natural inclusion group homomorphism

$$\rho:G\subset S\left(\lambda_{1},\ldots,\lambda_{n}\right),$$

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

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

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

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

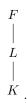
Theorem 1.10 and Remark 1.13 gives $G = \mathfrak{S}_3$.

Definition 1.14. $K \subset L$ is **finite** if L is finite-dimensional as a vector space over K. The **degree** of L over K is $[L:K] = \dim_K(L)$.

Lecture 4 Thursday 17/01/19

Two things about this.

Theorem 1.15 (Tower law). Let



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

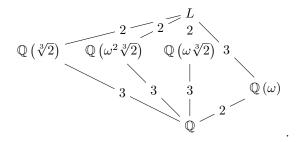
Theorem 1.16. Suppose $f(x) \in K[x]$ is irreducible of degree $d = \deg(f)$ and $L = K(\lambda)$ where $f(\lambda) = 0$, then $[K(\lambda) : K] = d$.

Example 1.17.

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

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

Example 1.18. Let $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$ be the splitting field of $x^3 - 2$ over \mathbb{Q} . The lattice of subfields is

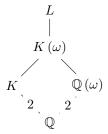


(Exercise: $\mathbb{Q}\left(\sqrt[3]{2} + \omega\right) = L$, $\mathbb{Q}\left(\omega^2\sqrt[3]{2}\right) \cap \mathbb{Q}\left(\omega\sqrt[3]{2}\right) = \mathbb{Q}$, and $\mathbb{Q}\left(\sqrt[3]{2}, \omega\sqrt[3]{2}\right) = L$) What is $[L:\mathbb{Q}\left(\sqrt[3]{2}\right)]$? Note $L = \mathbb{Q}\left(\sqrt[3]{2}\right)\left(\sqrt{-3}\right)$.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

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

 $2 \mid [L:\mathbb{Q}]$ and $3 \mid [L:\mathbb{Q}]$, so $6 \mid [L:\mathbb{Q}]$. Either $x^2 + 3$ is irreducible over $\mathbb{Q}\left(\sqrt[3]{2}\right)$, so by Theorem 1.16 $[L:\mathbb{Q}\left(\sqrt[3]{2}\right)] = 2$ and $[L:\mathbb{Q}] = 6$. Or $x^2 + 3$ is not irreducible, so $\mathbb{Q}\left(\sqrt[3]{2}\right) = L$ and $[L:\mathbb{Q}] = 3$, a contradiction. Are there any other fields? Claim that there are no other fields. Suppose $\mathbb{Q} \subsetneq K \subsetneq L$ is such a field. By Theorem 1.15 $[K:\mathbb{Q}] = 2$ or $[K:\mathbb{Q}] = 3$.

• Suppose $[K:\mathbb{Q}]=2$.



Either $\omega \in K$, that is $\mathbb{Q}(\omega) \subset K$, so by Theorem 1.15 $\mathbb{Q}(\omega) = K$. Or $\omega \notin K$ gives $[K(\omega) : K] = 2$, so $[K(\omega) : \mathbb{Q}] = 4$ contradicts the tower law for $\mathbb{Q} \subset K(\omega) \subset L$.

• Suppose $[K:\mathbb{Q}]=3$.

$$L \\ 2 \\ K(\omega) \\ 3 \\ \mathbb{Q}$$

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

I want to prove that

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

Lecture 5 Friday 18/01/19

Proof of Theorem 1.15. Suppose $y_1, \ldots, y_m \in F$ is a basis of F as a vector space over L. Suppose $x_1, \ldots, x_n \in L$ is a basis of L as a vector space over K. Claim that $\{x_iy_j\}$ is a basis of F over K.

• $\{x_iy_j\}$ generates F. Let $z \in F$. There exist $\mu_1, \ldots, \mu_n \in L$ 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),

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

• $\{x_iy_j\}$ are linearly independent over K. Suppose there exists $\lambda_{ij} \in K$ such that

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

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

Example 1.19. To show $G = \mathfrak{S}_3$. Let $\sigma = \begin{pmatrix} 1 & 2 \end{pmatrix}$. A basis of L/\mathbb{Q} is

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

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

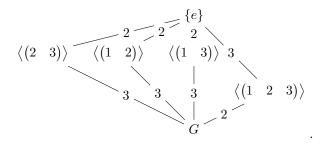
Thus

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

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

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

The lattice of subgroups is



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