

Chapter I

Galois Theory

I.1. Motivation

Given a polynomial

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0 \\ \in \mathbb{Q}[X],$$

can we express the roots of f in terms of radical expressions in $\mathbb{Q}$ and the coefficients $a_n, \dots, a_0$ of f ?

Example 1: a) $f(X) = X^7 - 3$
 roots: $\sqrt[7]{3} \zeta^k, \zeta := e^{2\pi i / 7}$

b) $f(X) = X^2 + pX + q$
 roots: $x_{1,2} = -\frac{p}{2} \pm \sqrt{\left(\frac{p}{2}\right)^2 - q}$

2 [Cardano - Tartaglia]

a) (Cardano's formula)

$$q(x) = x^3 + px + q$$

with

$$\frac{q^2}{4} + \frac{p^3}{27} > 0$$

resp: (put $\sqrt[3]{\cdot} = e^{2\pi i \frac{k}{3}}$)

$$= \frac{-1 + \sqrt{13}}{2}$$

$$\sqrt[3]{\frac{q^2}{4}} u_1 + \sqrt[3]{\frac{p^3}{27}} u_2, \quad i=0,1,2$$

with $u_{1,2} = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$

Question 2: What happens when

$$\frac{q^2}{4} + \frac{p^3}{27} \leq 0?$$

d) For a quadratic, see Ferrari's method.

What about quintics?

3

I.2. Algebraic field extensions (Reserp)

Def 3: Let $L|F$ be a field extension, i.e. $(L, +, \cdot)$ is a field and F is a subfield.

a) An elt $x \in L$ is algebraic over F if $\exists f(x) \in F[x] \setminus \{0\}$ s.t. $f(x) = 0$

b) $L|F$ is called algebraic if all elts of L are algebraic over F .

Example 4: $\mathbb{Q}[i] = \{a + ib \mid a, b \in \mathbb{Q}\}$
and $\mathbb{Q}(x) = \left\{ \frac{p(x)}{q(x)} \mid p, q \in \mathbb{Q}[x], q \neq 0 \right\}$

are field extensions of $\mathbb{Q}$.

$\mathbb{Q}[x]|\mathbb{Q}$ is algebraic as

atib is a root of

$$(X-a)^2 + b^2 = X^2 - 2aX + a^2 + b^2$$

$\mathbb{Q}(X) | \mathbb{Q}$ is not algebraic, as

X is not algebraic over $\mathbb{Q}$
(Prove this!)

Prop 5: (Nover low) Given a
tower of field ext. $L | E | F$,
then are equivalent:

- 1° $L | E$ and $E | F$ are alg.
- 2° $L | F$ is algebraic

Proof: $2^\circ \Rightarrow 1^\circ$ obvious

$1^\circ \Rightarrow 2^\circ$ Take $x \in L$. Then
 x is alg. over E .

Then $\exists f(X) = X^m + a_{m-1}X^{m-1} + \dots + a_1X + a_0 \in E[X]$
such that $f(x) = 0$.

$\Rightarrow x$ is algebraic over

$$E' := F[a_{m-1}, a_{m-2}, \dots, a_0]$$

(E' is a field (Prove this!))

as $a_{m-1}, \dots, a_0$ are alg.
over F)

See $E'[X]$ as an E' vector space
and an F - " -

$$x \text{ alg over } E' \Rightarrow \dim_{E'} E'[X] < \infty$$

$$a_0, \dots, a_{m-1} \text{ alg over } F \Rightarrow \dim_F E' < \infty$$

$$\text{Thus } \dim_F E'[X] < \infty$$

and x is algebraic over F $\square$

1.3 Separable field extensions

Def 6: Let L/F be algebraic.

a) $x \in L$ is called separable, if its minimal polynomial has $\deg(f)$ pairwise different roots in L (an algebraic closure of L)

a) L/F is called separable if all $\alpha \in L$ are $\frac{n-1}{F}$.

Platz: There is also a notion of separable extension for the non-algebraic case. (Not used in this course)

Lemma 8: Let f be the minimal $\text{sp}^f x$ over F . T.a.e.

1^0 x separable over F

2^0 $\text{gcd}(f, f') = 1$.

3^0 $\exists h, g \in F[x]: hf + g f' = 1$ (Bézout)

(Recap $\text{gcd}(g, h)$ (with $g \neq 0$) is the monic polynomial of largest degree which divides g and h .)

Proof: $\exists m \in \mathbb{F}: f(x) = (x - \alpha_1) \cdots (x - \alpha_m)$

$$f'(x) = \sum_{i=1}^m (x - \alpha_1) \cdots (\widehat{x - \alpha_i}) \cdots (x - \alpha_m)$$

$1^0 \Rightarrow 2^0$ If x is separable over F , then $\alpha_1, \dots, \alpha_m$ are pairwise different

$\Rightarrow f$ and f' have no common root.

$\Rightarrow \text{gcd}(f, f') = 1$.

$2^0 \Rightarrow 3^0$ Bézout

$3^0 \Rightarrow 1^0$ Take $h = g \cdot 0$. $hf + g f' = 1$.

Assume X is not separable. $\mathbb{F}$

$$\Rightarrow \exists i, j: x_i = x_j$$

$$\Rightarrow x_i \text{ is a root of } f \text{ and } f'$$

$$\Rightarrow x_i \text{ is a root of } 1$$

$$1 + 0 \cdot x^0 = 1$$

□

Example 9: a) $\mathbb{F}_p(X^{1/p}) | \mathbb{F}_p(X)$

is not separable, as

$$f(T) := T^p - X$$

is the minimal polynomial of $X^{1/p}$ and $f'(T) = pT = 0$

$$\gcd(f, f') = \gcd(T, 0) = f \neq 1.$$

e) $\bar{\mathbb{Q}} | \mathbb{Q}$ is separable

as for each irreducible polynomial f (in particular $\deg(f) \geq 1$)

$$\text{we have } \deg(f') = \deg(f) - 1$$

$$\text{and thus } \gcd(f, f') = 1.$$

Def 10: A field F is called perfect if $F|F$ is separable.

Example 11:

a) $\mathbb{F}_q$ is perfect ($q = p^e$, p prime, $e \in \mathbb{N}$)

b) $\text{char}(F) = 0 \Rightarrow F$ is perfect.

We characterize separability with extensions of field embeddings

Def 12: Let E, F be two fields

A ring homomorphism

$$\varphi: F \rightarrow E \text{ with } \varphi(1) = 1$$

is called a field embedding

Given $F_1 | F$, $E_1 | E$

and $\varphi_1: F_1 \rightarrow E_1$ a field emb.

φ_1 is called an extension of φ

$$\text{if } \varphi_1|_F = \varphi.$$

10

alg

Prop 13: Let $L/E/F$ be field extension and L/E finite, i.e. $[L:E] = \dim_E(L) < \infty$.

Then are equivalent

1° L/E separable

2° $\exists [L:E]$ many extensions of id_E into $\bar{E}$ on L

3° $\forall$ field embedding $\varphi: E \hookrightarrow \bar{F}$ $\exists [L:E]$ many extensions of φ into $\bar{F}$ on L .

Lemma 14: Let α be alg. over E and E/F alg. and $\varphi: E \hookrightarrow \bar{F}$ be an embedding.

Then $\exists$ at most $[E:F]$ extensions of φ on $E[\alpha]$ into $\bar{F}$.

Proof: Let f be the minimal of α/E .
 $f(X) = X^m + a_{m-1}X^{m-1} + \dots + a_0 \in E[X]$

$$\text{Then } f^{(q)}(X) := X^m + \varphi(a_{m-1})X^{m-1} + \dots + \varphi(a_0)X + \varphi(a_0)$$

is the minimal of α roots over $\varphi(E)$.

$\Rightarrow$ # extensions of φ

$$= \# \text{ roots of } f^{(q)} \text{ in } \bar{F} \leq m = [E[X]:E]$$

□

Proof of Prop 13: 2° $\Rightarrow$ 2° ✓
 using that $E \subseteq \bar{F}$.

$$1^\circ \Rightarrow 3^\circ \quad L = E[\beta_1, \beta_2, \dots, \beta_r]$$

$$\text{Put } E_i := E[\beta_1, \dots, \beta_i]$$

By the argument of Lemma 14 we have

$$[E_i:E] \text{ ext of } \varphi \text{ for } E_i$$

$$[E_i:E_i] \text{ ext of each ext of } \varphi$$

$$\text{for } E_i.$$

Thus we have

$$[E_1:E] \dots [E_r:E] \text{ ext of } \varphi$$

$$\text{for } L$$

$$2^\circ \Rightarrow 1^\circ \text{ extension}$$

□

Prop 15: (tower law)

Let $L|E|F$ be alg.

Then are equivalent

1° $L|E$ and $E|F$ are separable

2° $L|F$ is separable.

Proof: $2^\circ \Rightarrow 1^\circ$ obvious

$1^\circ \Rightarrow 2^\circ$: Similar to the proof of the tower law in prop 5, but using extension of emb. i.e. Prop 13. $\square$

Prop 16: let $\alpha, \beta \in F$ o.h. α is separable/ F .

Then $\exists \gamma \in F: F[\alpha, \beta] = F[\gamma]$.

Proof: look up "Primitive element theorem" $\square$

Example 17: $L = \mathbb{Q}[\sqrt{2}, \sqrt{3}] / \mathbb{Q}$ is separable
 ∞ char($\mathbb{Q}$) = 0
 Further $L = \mathbb{Q}[\sqrt{2} + \sqrt{3}]$, as

$$\sqrt{6} \in \mathbb{Q}[\sqrt{2} + \sqrt{3}]$$

$$(\sqrt{6})^2 = \frac{(\sqrt{2} + \sqrt{3})^2 - 5}{2}$$

and therefore $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$ because

$$\sqrt{6}(\sqrt{2} + \sqrt{3}) = 2\sqrt{3} + 3\sqrt{2}$$

is an elt. of $\mathbb{Q}(\sqrt{2} + \sqrt{3})$

I.3. Galois extensions

15

Def 18: An algebraic field extension L/F is called normal if every embedding $\varphi: L \hookrightarrow \bar{L}$, $\varphi|_F = \text{id}_F$, satisfies $\varphi(L) = L$.

Example 19:

a) $E := \mathbb{Q}(\sqrt[3]{2}) | \mathbb{Q}$ is not normal,
as $\varphi: \mathbb{Q}(\sqrt[3]{2}) \rightarrow \mathbb{C} \subseteq \mathbb{C}$
with
 $\varphi(\sqrt[3]{2}) := e^{2\pi i \frac{1}{3}} \sqrt[3]{2}$

satisfies $\text{im}(\varphi) \not\subseteq \mathbb{R}$, so
 $\text{im}(\varphi) \neq \mathbb{Q}(\sqrt[3]{2})$

b) $L = \mathbb{Q}(\sqrt[3]{2}, \frac{-1+i\sqrt{3}}{2}) | \mathbb{Q}$ is
normal, because any
field embedding
 $\varphi: L \rightarrow \mathbb{C}$

Definition

$$Q(\sqrt[n]{2}) = e^{2\pi i \frac{k}{n} \sqrt[n]{2}} \in L$$

$$r, l \in \mathbb{N}$$

Remark 20: In Def. 18 it is enough
no check $Q(L) \subseteq L$.

Proof: Suppose $\forall Q: L/F \rightarrow L/F$ (*)
natively $Q(L) \subseteq L$

Take Q . Extend Q to $\bar{L}$ (possible as $\bar{L}/L$ is algebraic)

$$\begin{array}{ccc} \bar{Q}: \bar{L} & \xrightarrow{\quad} & \bar{L} \\ \cup & \cup & \cup \\ L & \xrightarrow{\quad Q \quad} & L \\ \cup & \cup & \cup \\ F & \xrightarrow{\text{id}} & F \end{array}$$

Observe:

$\bar{Q}$ is surjective, because $\bar{Q}(\bar{L})$ is algebraically closed and $\bar{L}/\bar{Q}(\bar{L})$ is algebraic.

$\bar{Q}$ is also injective, so bijective.

$$\begin{aligned} \text{Now } (Q^{-1})(L) &\subseteq L, \text{ as } Q^{-1} \text{ is bijective.} \\ \Rightarrow Q(L) &\supseteq Q(Q^{-1}(L)) \supseteq L \\ \text{So } Q(L) &= L. \quad \square \end{aligned}$$

Notation 21: Let L/F be a field extension.

$$\text{Aut}(L/F) := \{Q: L \rightarrow L \mid Q \text{ is a field automorphism with } Q|_F = \text{id}_F\}$$

set of automorphisms of L/F

Exercise 22: (self-study)

$$\begin{aligned} L &= \bar{F}_p. \text{ Then } \forall n \in \mathbb{N} \\ \exists! E \subseteq L &\text{ such that } [E: F_p] = n. \end{aligned}$$

In particular each such E is normal over F_p .

$$\text{(We denote } E = (F_p^n))$$

Def 23: $L|F$ is called Galois, if it is separable and normal.

We write $G(L|F)$ for $\text{Aut}(L|F)$ the Galois group of $L|F$.

Example 24:

a) $\text{Aut}(\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}) = \{ \text{id}, \sigma(\sqrt[3]{2}) \}$

e) $L = \mathbb{Q}(\sqrt[3]{2}, \omega) \quad \omega = e^{2\pi i/3}$

Then $L|\mathbb{Q}$ is alg., sep. and normal, i.e. Galois.

$|G(L|\mathbb{Q})| = [L:\mathbb{Q}]$ by sep. and normality.

Claim: $[L:\mathbb{Q}] = 6$

Proof: $E = \mathbb{Q}(\sqrt[3]{2})$

$[E:\mathbb{Q}] = 3$, as $X^3 - 2$ is irred. (It cannot factorise / 0 as deg = 3 and it has no rational root)

$[L:E] = 2$, as $L = E[\omega]$
 $\omega \notin E$ and $\omega^2 + \omega + 1 = 0$.

Thus $[L:\mathbb{Q}] = [L:E][E:\mathbb{Q}] = 6$. $\square$

Claim: $G(L|\mathbb{Q}) \simeq S_6 = \text{Sym}(1, 2, 3)$

Proof: $G(L|\mathbb{Q})$ is not abelian:

$\sigma: E \rightarrow L \quad \sigma(\sqrt[3]{2}) = \omega\sqrt[3]{2}$
 has base extension to L , by separability of $L|E$.

$\sigma_{112}(\omega) = \omega^2$

$\sigma_1(\sigma_2(\sqrt[3]{2})) = \sigma_1(\omega\sqrt[3]{2}) = \omega^2\sqrt[3]{2}$

$\sigma_2(\sigma_1(\sqrt[3]{2})) = \sigma_2(\omega\sqrt[3]{2}) = \omega\sqrt[3]{2}$ $\square$

Further observation:

a1) We can spot the following intermediate fields I :

$$(L|I|D)$$

$$D, L, E, D(\omega^{\frac{3}{2}}\sqrt[3]{2}), D(\omega^{\frac{3}{2}}\sqrt[3]{2}),$$

$D(\omega)$. Are there more?

a2) S_3 has the following subgroups

$$S_3, \{1\}, \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \text{id} \right\}, \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \text{id} \right\},$$

$$\left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \text{id} \right\}, \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \text{id} \right\},$$

$$\left\{ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\}$$

They are all as a subgroup H of S_3 with $H \cong S_3$ has order ≤ 3 , or must be cyclic.

There are exactly 3 normal subgroups: S_3 , $\{1\}$, $\langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \rangle$

and we have exactly three normal extensions $L|D$.

$$D|D; L|D; D(\omega)|D.$$

Notation 25: Let G be a group.

$$\text{gp} \leq (G) := \{H \mid H \text{ subgroup of } G\}$$

$$\text{gp} \trianglelefteq (G) := \{H \in \text{gp}(G) \mid H \trianglelefteq G\}$$

order normal subgroups of G .

Let $L|F$ be a field extension.

$$\text{int}(L|F) := \{I \subseteq L \mid I \text{ intermediate field in } L|F\}$$

If $L|F$ is Galois, we write

$$\text{int}_{\text{Gal}}(L|F) := \{I \in \text{int}(L|F) \mid I|F \text{ Galois}\}$$

Theorem 26 Main Theorem of Galois Theory

Let L/F be a finite Galois extension. (a) Then the map

$$\Phi: \text{int}(L/F) \longrightarrow \text{gr}_\Phi(G(L/F))$$

$$\Phi(I) := G(L/I)$$

is bijective and the inverse satisfies

$$\Phi^{-1}(H) = L^H := \{x \in L \mid h(x) = x \quad \forall h \in H\}$$

(set of H -fixed points in L)

(c) We have the following commutative diagram with bijective rows.

$$\begin{array}{ccc} \text{int}(L/F) & \xrightarrow{\Phi} & \text{gr}_\Phi(G(L/F)) \\ \downarrow U & \searrow G & \downarrow U \\ \text{int}_{\text{gal}}(L/F) & \xrightarrow{\sim} & \text{gr}_\Phi(G(L/F)) \end{array}$$

(c) For $I \in \text{int}_{\text{gal}}(L/F)$ we have

$$\frac{G(L/F)}{G(L/I)} \xrightarrow{\sim} G(I/F).$$

via restriction.

Lemma 27: Let L/F be finite Galois

Then $L_{G(L/F)} = F$

Proof: Take $x \in L_{G(L/F)}$. Assume $x \neq F$.

Put $E := F[x]$. E/F separable and $E \neq F$.

$\Rightarrow \exists \varphi: E \hookrightarrow \bar{F}: \varphi \neq \text{id}_E$ and $\varphi|_F = \text{id}_F$.
field emb.

Extend φ further to L , still call it φ , i.e. $\varphi \in G(L/F)$ and $\varphi(x) \neq x$.
 $\square$

24

Lemma 28: Let $L|F$ be a finite field extension and $H \leq \text{Aut}(L|F)$.

Then

$$L|L^H \text{ is Galois with } \mathcal{G}(L|L^H) = H.$$

Proof: 1st: $L|L^H$ is separable:

$$x \in L. \text{ But } f(x) := \prod_{\sigma \in H} (\sigma(x) - \sigma(x))$$

f has coefficients in L^H , as x is separable over L^H .

2nd: $L|L^H$ is normal:

$$\varphi: L|L^H \hookrightarrow L|L^H$$

By Prop 16. $\exists x \in L: L = L^H[x]$, as $L|L^H$ is finite and separable.

Consider above polynomial f .

$$f(x) = \prod_{\sigma \in H} (\sigma(x) - \sigma(x))$$

$$\varphi|_{L^H} = \text{id}_{L^H}$$

25

Compare with $\Rightarrow \mathcal{G}(x) = \mathcal{G}(x)$ for some $\sigma \in H$.

$$\Rightarrow \mathcal{G} = \mathcal{G}, \text{ in particular } \mathcal{G}(L) = L.$$

3rd: $\mathcal{G}(L|L^H) = H$. See the 2nd part.

□

Lemma 29: Let $L|F$ be finite and normal and $H \trianglelefteq \text{Aut}(L|F)$. Then $L^H|F$ is normal and

$$\text{Aut}(L|F) / H \cong \text{Aut}(L^H|F)$$

via restriction.

Proof: exercise □

26

Proof of Theorem 26:

- (a) follows from Lem 27 and 28.
 (b) follows from (a) and Lem 29.
 (c) follows from Lem 29. $\square$

Exercise 30: (self-study)

What happens in the case of infinite Galois extensions?

We have a modification of Lem 27/28.

Lem (27/28)': Let L/F be Galois and $E \in \text{int}(L/F)$ or $L(E|E) \trianglelefteq G(L|F)$.

Then: $(L^E)' \subseteq G(L|F) = F$

(2.9') $E|F$ is Galois and

$$G(L|F)/G(L|E) \xrightarrow{\sim} G(E|F)$$

via restriction.

Proof: Lem 27 doesn't need $[L:F] < \infty$ and $\text{Gal}(L^E|F) \subseteq G(L|F) = E$ so now that $E|F$ is normal. $\square$

27

I 4. Abelian extensions.

Def 31: A field extension $K|F$ is called abelian if it is Galois and $G(K|F)$ is abelian.

We recall a notation.

Notation 32: Let K and E be two subfields of L .

We denote by KE the smallest subfield of L which contains $K \cup E$. Composition of K and E .

(a) When each element of K is algebraic over E then

$$KE = \left\{ \sum_{i=1}^n k_i e_i \mid e_i \in E, k_i \in K, e_i \in E \right\}$$

(set of sums of products)

(b) In general KE is the quotient field of the RHS in (a).

Our main goal is the following theorem.

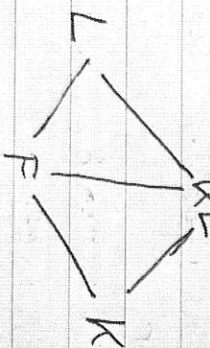
Theorem 33: a) let $L|F$ be abelian and $E \in \text{int}(L|F)$

Then $L|E$ and $E|F$ are abelian

b) let $L|F$ and $K|F$ be abelian and contained in a bigger field. Then $LK|F$ is abelian.

c) let $L|F$ and $E|F$ be contained in a bigger field and suppose $L|F$ is abelian. Then $LE|E$ is abelian.

Remark 34: Diagram



as says: $L|F$ ab. $\Rightarrow K|L|K$ ab.

a) and b) say: $L|F$ and $K|F$ ab.

$\Rightarrow$ Every ext. in the diag. is abelian.

Inlude: Algebraic closure and separable closure.

Prop 35: let $L|F$ be a field ext.

a) let $\alpha, \beta \in L$, $\beta \neq 0$, be alg. over F . Then $\alpha \pm \beta$

and $\alpha\beta$ are algebraic over F .

b) $F^{\text{alg}} = \{ \alpha \in L \mid \alpha \text{ alg over } F \}$

is an intermediate field of $L|F$, called algebraic closure of F in L .

Proof:

a) α alg. $/F$ and β alg. $/F(\alpha)$

Thus $F(\alpha, \beta)$ has finite de-

gree $/F$.

$\Rightarrow \forall x \in F(\alpha, \beta): [F(x):F] < \infty$

$\Rightarrow \forall x \in F(\alpha, \beta)$

$x \in F(\alpha, \beta)$

So $\alpha \pm \beta$, $\alpha\beta$, $\alpha\beta^{-1}$ are alg. $/F$.

b) follows from a) $\square$

We have a similar proposition for separability.

Prop 36: Let $L|F$ be an alg. field extension.

a) Suppose $\alpha, \beta \in L, \beta \neq 0$, and α, β are separable over F .

Then $\alpha \pm \beta, \alpha\beta, \alpha\beta^{-1}$ are sep. over F .

$\overline{L}_{\text{sep}} := \{\alpha \in L \mid \alpha \text{ sep. over } F\}$
is a field, called the separable closure of F in L .

Proof: a) follows from a)

To prove a) we need to show that $F[\alpha]|F$ and $F[\alpha, \beta]|F[\alpha]$ are separable and use the tower lemma (Prop. 15).

$\text{minpol}_{\alpha, F}$ and $\text{minpol}_{\beta, F[\alpha]}$ in L

have no multiple roots as α, β are separable over F .

Thus the number of extensions of id_F to $F[\alpha]$ into $\bar{L}$ is $[F[\alpha]:F]$ and of $\text{id}_{F[\alpha]}$ to $F[\alpha, \beta]$ into $\bar{L}$ is $[F[\alpha, \beta]:F[\alpha]]$. Thus both field ext. are separable. $\square$

Remark 37: There is no logic circle here. The construction of the algebraic closure of L does not need the concept of separability. (See homework for Week 2)

Example 38:

a) $\mathbb{Q}(\sqrt{2}) : \overline{\mathbb{Q}}^{\sqrt{2}} = \{x \in \overline{\mathbb{Q}} \mid x \text{ alg. over } \mathbb{Q}\}$ is countable.

Thus $\overline{\mathbb{Q}}^{\sqrt{2}} \subsetneq \overline{\mathbb{Q}}$.

Further $\overline{\mathbb{Q}}^{\sqrt{2}}$ is alg. closed.

Proof: But $\mathbb{E} := \overline{\mathbb{Q}}^{\sqrt{2}}$.

Take $f(x) \in \mathbb{E}[x], \deg(f) \geq 1$

32

F is alg. closed $\Rightarrow \exists \lambda \in \mathbb{C} : f(\lambda) = 0$
 $E[\lambda]/E \mid \mathbb{Q}$ tower of alg. extension
 $\Rightarrow E[\lambda]/\mathbb{Q}$ alg. $\Rightarrow \lambda \in \overline{\mathbb{Q}}^{\text{alg}} = E$
 Prop 5 $\square$

8) Find an alg. extension L/F
 such that $F^{L, \text{inv}} \neq L$.
 (hint: F should not be perfect.)

33

Proof of Theorem 33:

a) $G(L|F)$ is abelian and $G(L|E) \trianglelefteq G(L|F)$
 So $L|E$ and $E|F$ are abelian
 by Lem (29).

a) $L|F$ is alg.
 So $KL = E \sum_{i=1}^t k_i e_i \mid \lambda e \mid \mu, k_i \in K$
 $k_i \in L$?

Prop 35/36 $\Rightarrow KL|F$ is alg. + dep.

Normal? Take $\overline{F}$ a.l. $KL \subseteq \overline{F}$.
 and $\varphi \in \text{Aut}(\overline{F}|F)$.

$KL|F$ normal $\Rightarrow \varphi(K) = K, \varphi(L) = L$
 $\Rightarrow \varphi(KL) \subseteq KL$.

Abelian? $\varphi, \psi \in G(KL|F)$.

$$\begin{aligned} \varphi(\psi(\sum k_i e_i)) &= \sum \varphi(\psi(k_i)) \varphi(\psi(e_i)) \\ &= \sum \psi(\varphi(k_i)) \psi(\varphi(e_i)) \\ &\text{as } KL|F, L|F \text{ are ab.} \\ &= \psi(\varphi(\sum k_i e_i)). \quad \square \end{aligned}$$

c) Similar to b)

 $\square$

34

Example 39: (n th cyclotomic field extension)

ζ primitive n th root of unity
 $\mathbb{Q}(\zeta) / \mathbb{Q}$ is abelian

- Galois, because $\text{char}(\mathbb{Q}) = 0$
 and all conjugates of ζ
 are in $\mathbb{Q}(\zeta)$.

(the conjugates of ζ are ζ^a ,
 $a \in (\mathbb{Z}/n\mathbb{Z})^\times$) exercise

- abelian: $\varphi, \psi \in \mathcal{G}(\mathbb{Q}(\zeta) / \mathbb{Q})$.

$$\text{say } \varphi(\zeta) = \zeta^a, \psi(\zeta) = \zeta^b$$

$$\Rightarrow \varphi(\psi(\zeta)) = \varphi(\zeta^b) = (\varphi(\zeta))^b = \zeta^{ab}$$

$$\psi(\varphi(\zeta)) = \psi(\zeta^a) = \zeta^{ba}$$

$$\Rightarrow \varphi \circ \psi = \psi \circ \varphi$$

Def 40: L/F abelian

$$\overline{F}^{L, ab} := \{ \alpha \in L \mid F(\alpha) \mid F \text{ is abelian} \}$$

maximal abelian subextension of L/F

Prop 41: Let L/F be finite Galois.

Put $E := \overline{F}^{L, ab}$.

Then

$$G(L/E) = [G, G]$$

(commutator

subgroup of G)

$$\text{and } G(E/F) = G^{ab} := G / [G, G].$$

(Here $G := G(L/F)$)

Proof: E/F is normal and sep.,
so Galois.

$G(E|F) = \frac{G}{G(L|E)}$ is abelian.

Thus $[G, G] \leq G(L|E)$.
 $26 \Rightarrow \exists E'|E: G(L|E') = [G, G]$.

$$[G, G] \trianglelefteq G \Rightarrow G(E'|F) \trianglelefteq \frac{G}{[G, G]}.$$

in particular abelian.

$$\Rightarrow E' \subseteq E. \text{ Thus } E = E'.$$

□

Example 42: $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$

$$G(L|\mathbb{Q}) \trianglelefteq S_3. \text{ But } K = \mathbb{Q}(\omega) \text{ is abelian.}$$

$$\Rightarrow G(L|K) \trianglelefteq [S_3, S_3] = A_3$$

$$= \langle (123), (132) \rangle$$

$$\text{Thus } K = \mathbb{Q}(\omega).$$

$$G(\mathbb{Q}(\omega)|\mathbb{Q}) \trianglelefteq C_2.$$

15. Composition with Galois extension

We have a generalization of Thm 33 for Galois extensions.

Thm 43: a) Let $L|F$ be Galois and $E \subseteq \text{mid}(L|F)$. Then $L|E$ Galois.
 • If $G(L|E) \trianglelefteq G(L|F)$, then $E|F$ Galois.

b) Let $L|F$ and $K|F$ be Galois and contained in a common field. Then $LK|F$ Galois.

c) Let $K|F$ be Galois and $L|F$ be a field extension of K . Then $L|K$ is Galois in a field.

Then $LK|L$ is Galois and $G(LK|L) \subseteq G(K|K) = 1$.
 $g \mapsto g|_K$.

Proof: a) $L|E$ is Galois, because $L|E$ is Galois.

$E|F$ is Galois, by 27, it $g(L|E) \triangleq g(L|F)$.

c) Same argument as in the proof of 33b).

c) $K|L$ is alg and sep. by Prop. 35/36.

Take $\bar{L}$ st $K \subseteq \bar{L}$ and

$$Q: K|L \longrightarrow \bar{L}|L.$$

Then for $\sum_{i=1}^t k_i l_i \in K|L$

we have

$$Q\left(\sum_{i=1}^t k_i l_i\right) = \sum_{i=1}^t Q(k_i) l_i \in K|L$$

$Q|_L = \text{id}$ $Q(x) = x$

So $K|L$ is normal.

alg, sep, normal $\Rightarrow K|L$ Galois.

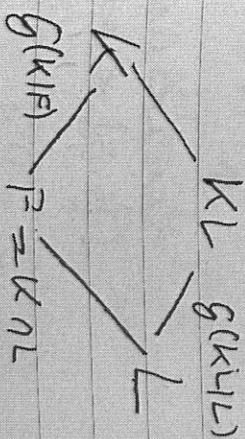
Probas: $g(K|L) \xrightarrow{\text{res}} g(K|L \cap K)$.

Pl: injective: $Q \in g(K|L)$, st

$$Q|_K = \text{id}_K \quad \text{Then } Q|_{K \cap L} = \text{id}.$$

• surjective: (This argument is longer, as we include the case where $K|L \cap K$ is infinite)

Without loss of generality $F = K \cap L$.



Step 1: Case $[K:F] < \infty$.

$$H := \{g \in G(K|F) \mid$$

$$\exists g \in G(K|F) : g = \varphi|_K\}$$

$$\leq G(K|F).$$

$$K^H = \{x \in K \mid \forall g \in H : g(x) = x\}$$

$$= K \cap (K^L)^{G(K|L)}$$

$$= K \cap L = F.$$

$$\uparrow$$

$$26a) \text{ on } K|L \quad ([K:L] < \infty)$$

$$26a) \text{ again } \Rightarrow G(K|F) = H.$$

$$\text{on } K|F$$

$$\uparrow$$

then we used
 $[K:F] < \infty$.

Step 2: $\forall K'|F$ finite subextension of $K|F$ we have

$$(K'|L) \cap K = K'$$

Pf: $K' = F[x]$ (primitive ele. thm.)

Take the normal hull $K''|F$ of $K'|F$ in K .

$$\text{Step 1} \Rightarrow G(K''|L) \cong G(K''|F).$$

$$\Rightarrow \# \text{ conjugates of } x|L = \# \text{ conjugates of } x|F.$$

$$\Rightarrow [L[x]:L] = [F[x]:F]$$

$$\uparrow$$

$$\text{separability} \quad [K'|L:L] \stackrel{||}{=} [K':F]. \quad \square$$

$$\text{Step 3: } K|K'|F \Rightarrow (K'|L) \cap K = K'$$

$$\text{Pf: } K' = \bigcup E$$

$$E|F \subseteq K'|F$$

finite

$$\Rightarrow K'|L = \bigcup EL$$

$$\uparrow$$

$$E|F \subseteq K'|F$$

why?

$$\leq \infty$$

42

$$\Rightarrow (K' \cap K)$$

||

$$\bigcup_{E \subseteq K \mid F} (E \cap L) \cap K$$

||

$$\bigcup (E \cap L) \cap K = \bigcup E = K'$$

$$\stackrel{E}{\uparrow} E = K'$$

Step 2

□

Step 4: We finish the proof of the conjecture.

$$\underline{Q_4}: H' = \text{res}(G(K \cap L))$$

Take $Q \in G(K \cap F)$. But

$$M := \bigcup (K' \cap F, \varphi': K' \cap L \hookrightarrow K \cap L)$$

$$\varphi|_{K'} = \varphi' \Rightarrow (\pi \upharpoonright F, \text{id})$$

43

ordering: $(K_1, \varphi_1) \leq (K_2, \varphi_2)$

$$\Leftrightarrow \text{or } K_1 \subseteq K_2 \text{ and } \varphi_2|_{K_1} = \varphi_1$$

Then $(M, \leq)$ is inductively ordered.

Zorn's Lemma $\Rightarrow \exists (K, \varphi) \in M$ which is $\leq$ maximal.

Assume that $K' \not\subseteq K$.

and take $B \in K \setminus K'$.

$$\text{Step 3} \Rightarrow (K \cap L) \cap K = K'$$

$$\text{Step 2} \Rightarrow [K' \cap B : K'] = [K' \cap B : K' \cap L]$$

$$\Rightarrow \exists [K' \cap B : K'] \text{ many}$$

Prop 13

$$\downarrow \text{extension of } \varphi: K' \cap L \hookrightarrow K \cap L$$

$$\text{to } K' \cap B \hookrightarrow K \cap L$$

$$\Rightarrow$$

$\varphi|_{K' \cap B}$ can be extended to

$$K' \cap B \cap L. \quad \square$$

Corollary 44: Suppose

$K|F, L|F$ are Galois extensions
 $K \cap L = F$ and $K \cup L$ lies in
 a field

Then

$$R: G(K|F) \xrightarrow{\sim} G(K|F) \times G(L|F)$$

$$\text{via } R(\psi) := (\psi|_K, \psi|_L).$$

Proof: injective $\checkmark$

surjective: Take $(\varphi_1, \varphi_2) \in G(K|F) \times G(L|F)$

$$\text{Thm 43} \Rightarrow \exists \psi \in G(K|L),$$

$$\psi|_L \in G(K \cap L|L):$$

$$R(\psi_1) = (\varphi_1, \text{id}_L)$$

$$\wedge R(\psi_2) = (\text{id}_K, \varphi_2)$$

$$\Rightarrow R(\psi_1 \circ \psi_2) = R(\psi_1) \cdot R(\psi_2)$$

$$= (\varphi_1, \text{id}_L) (\text{id}_K, \varphi_2) = (\varphi_1, \varphi_2) \quad \square$$

Example 45:

$$\begin{aligned} & G(\mathbb{Q}(\sqrt{2} + \sqrt{3})|\mathbb{Q}) \\ &= G(\mathbb{Q}(\sqrt{2}, \sqrt{3})|\mathbb{Q}) \\ &\cong G(\mathbb{Q}(\sqrt{2})|\mathbb{Q}) \times G(\mathbb{Q}(\sqrt{3})|\mathbb{Q}) \\ &\cong C_2 \times C_2. \end{aligned}$$