Galois theory I

Recall: $\begin{array}{ccc} K & \dashrightarrow & L \\ | & \nearrow & \\ F & & \end{array}$ Given K/F finite extension, and L a normal extension of F containing K.
then $\mathrm{Hom}_F(K,L) \leq [K:F]$ and equality holds if K/F is separable.

Definition. We say that an algebraic extension K/F is **Galois** if it is separable and normal.

Define $\mathrm{Gal}(K/F) := \mathrm{Aut}_F(K) = \{\phi : K \to K \text{ isom s.t. } \phi|_F = id\}$, called the **Galois group** of K over F (K在F上的伽罗华群)

* Consider the above situation with $K=L$ finite Galois over F

then each $\phi \in \mathrm{Hom}_F(K,K)$ is an automorphism of K fixing F (b/c ϕ is injective & K/F fin dim'l $\Rightarrow \phi$ bij.)

and $\#\mathrm{Hom}_F(K,K) = [K:F] \Rightarrow \#\mathrm{Gal}(K/F) = [K:F]$

Example: $K = \mathbb{Q}(\sqrt{2},\sqrt{3})$ $\quad \mathrm{Gal}(K/F) = \{1, \sigma, \tau, \sigma\tau\}$

$F = \mathbb{Q}$ where 1 is the identity map

$$\sigma(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) = a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6}$$

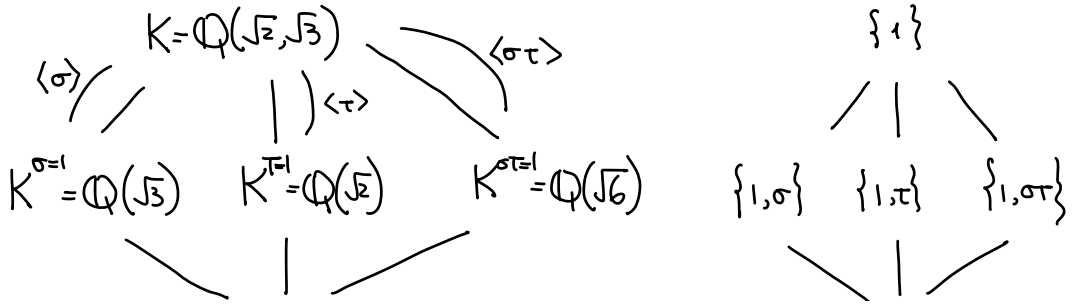
$$\tau(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) = a+b\sqrt{2}-c\sqrt{3}-d\sqrt{6}$$

$$\sigma\tau(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) = a-b\sqrt{2}-c\sqrt{3}+d\sqrt{6}.$$

$$K^{\sigma=1} = \{x \in K ; \sigma(x)=x\} = \{a+c\sqrt{3} ; a,c \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{3})$$

$$K^{\tau=1} = \{x \in K, \tau(x)=x\} = \{a+b\sqrt{2} ; a,b \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{2})$$

$$K^{\sigma\tau=1} = \{x \in K, \sigma\tau(x)=x\} = \{a+d\sqrt{6} ; a,d \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{6})$$



Q $\{1, \tau, \sigma, \sigma\tau\}$

Remark: If a group H acts on a field K by automorphisms, then
$K^H = \{k \in K ; \sigma(k) = k \ \forall \sigma \in H\}$ is a subfield.

Theorem (Galois theory)

Let K/F be a finite Galois extension with $G := Gal(K/F)$

(1) There's a one-to-one correspondence between

$$\{\text{subgroups } H \leq G\} \longleftrightarrow \{\text{Intermediate field extensions}\}$$

$$H \longmapsto K^H = \{x \in K \mid h(x) = x, \forall h \in H\}$$

$$Gal(K/E) = \{g \in G ; g|_E = id\} \longleftarrow E$$

(to be proved next time.)

(2) The correspondence is inclusion-reversive:

$$H_1 \subseteq H_2 \iff K^{H_1} \supseteq K^{H_2}$$

Proof: $H_1 \subseteq H_2 \Rightarrow K^{H_1} \supseteq K^{H_2}$ obvious (b/c $\forall x, H_2 x = x \Rightarrow H_1 x = x$.)

$E_1 \subseteq E_2 \Rightarrow Gal(K/E_2) \subseteq Gal(K/E_1)$ (b/c $\forall h \in Gal(K/F), h|_{E_2} = id \Rightarrow h|_{E_1} = id$.)

(3) $\#H = [K : K^H]$, $[G : H] = [K^H : F]$

Proof: K separable + normal $\Rightarrow [K : K^H] = \#Gal(K/K^H) = \#H$

From this, $\#H \cdot [G : H] = \#G = [K : F] = [K : K^H] \cdot [K^H : F]$

(K/F Galois)

So $[G : H] = [K^H : F]$.

(4) If $H \longleftrightarrow E$, then

$$gHg^{-1} \longleftrightarrow g(E)$$

Proof: NTS $E = K^H \overset{?}{\Rightarrow} g(E) = K^{gHg^{-1}}$

But $x \in K^{gHg^{-1}} \Leftrightarrow gHg^{-1}x = x \Leftrightarrow Hg^{-1}x = g^{-1}x \Leftrightarrow g^{-1}x \in K^H = E \Leftrightarrow x \in g(E)$.

(5) $H \leq G$ is a normal subgroup $\Leftrightarrow$ K^H is a normal extension of F.

In this case, $\mathrm{Gal}(K^H/F) \simeq G/H$.

"$\Leftarrow$" if K / K^H / F — K^H/F is a normal extension,

then any automorphism $\sigma : K \to K$ that fixes F must stabilize K^H

$\Rightarrow \sigma(K^H) = K^H \ \forall \sigma \in \mathrm{Gal}(K/F)$ $\Rightarrow \sigma H \sigma^{-1} = H$. $\Rightarrow H$ normal.

($K^H = K^{\sigma H \sigma^{-1}}$)

"$\Rightarrow$" If $H \trianglelefteq G$ is normal, WTS, K^H is a normal extension of F.

* If $f(x)$ is an irreducible polynomial in $F[x]$ that has a zero α in K^H

WTS: $f(x)$ splits completely in K^H.

(know: $f(x)$ splits completely in K.)

Useful Lemma If K/F is Galois and $f(x)$ is an irreducible polynomial that splits in K,

assume that α is a root of $f(x)$, then other zeros are exactly $\{\sigma(\alpha) ; \sigma \in \mathrm{Gal}(K/F)\}$

Proof: Let $g(x) := \prod_{\sigma \in \mathrm{Gal}(K/F)} (x - \sigma(\alpha)) \in F[x]$

↑ b/c all coeffs are invariant under $\mathrm{Gal}(K/F)$.

In $K[x]$, $(f(x), g(x)) \neq (1) \Rightarrow$ In $F[x]$, $(f(x), g(x)) \neq (1)$

But $f(x)$ irreducible in $F[x] \Rightarrow f(x) \mid g(x) \Rightarrow$ all zeros are $\sigma(\alpha)$'s. $\square$

By Lemma, all zeros of $f(x)$ are $\sigma(\alpha)$'s for some $\sigma \in \mathrm{Gal}(K/F)$

$\alpha \in K^H \Rightarrow \sigma(\alpha) \in K^{\sigma H \sigma^{-1}} = K^H \ \forall \sigma \Rightarrow f(x)$ splits in K^H.

Proof of $H \trianglelefteq G$, K^H/F normal $\Rightarrow \mathrm{Gal}(K^H/F) \simeq G/H$

Consider the following homomorphism $\eta : \mathrm{Gal}(K/F) \longrightarrow \mathrm{Gal}(K^H/F)$

$\sigma \longmapsto \sigma|_{K^H}$

This makes sense because K^H is normal $/F \Rightarrow \sigma$ stabilizes K^H

$$\ker \eta = \{ \sigma : K \xrightarrow{\sim} K \mid \sigma|_{K^H} = id \} = Gal(K/K^H) = H$$

By 1st Isom Thm, $\rightsquigarrow \bar{\eta} : G/H \hookrightarrow Gal(K^H/F)$

Two proofs of $\bar{\eta}$ being surjective & hence an isomorphism

(i) By counting, $\#(G/H) \overset{(3)}{=} [K^H : F] = \#Gal(K^H/F)$, so surjective.

(ii) Given $\sigma \in Gal(K^H/F)$,

$$\begin{array}{ccc} K & \dashrightarrow & K \\ | & & | \\ K^H & \xrightarrow{\sigma} & K^H \\ & \diagdown \quad \diagup & \\ & F & \end{array}$$

As K/K^H is normal, $\exists$ isom. $\tilde{\sigma} : K \to K$ s.t. $\tilde{\sigma}|_{K^H} = \sigma$

So $\bar{\eta}$ is surjective.

- So we have $Gal(K^H/F) \simeq G/H$.

(6) If $H_1, H_2 \longleftrightarrow E_1, E_2$

then $H_1 \cap H_2 \longleftrightarrow E_1 E_2$ and $\langle H_1, H_2 \rangle \longleftrightarrow E_1 \cap E_2$

Proof: $Gal(K/E_1E_2) = \{ h \in Gal(K/F) \text{ s.t. } h|_{E_1E_2} = id \}$

$= \{ h \in Gal(K/F) \text{ s.t. } h|_{E_1} = id, h|_{E_2} = id \} = H_1 \cap H_2.$

$K^{\langle H_1 \cap H_2 \rangle} = K^{H_1} \cap K^{H_2} = E_1 \cap E_2.$ □

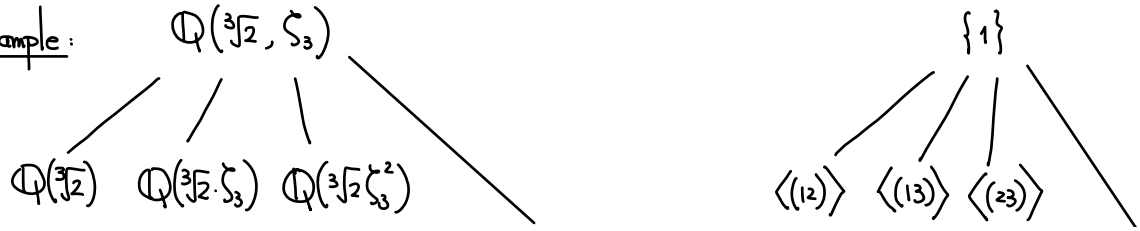
Slogan: To understand a finite (separable) extension K/F,

we consider its Galois (normal) closure L

$$\begin{array}{ccc} H & & L \\ & K & \\ & | & \\ & F & \end{array} \qquad G$$

properties of $K/F \longleftrightarrow$ properties of the coset G/H

Example:

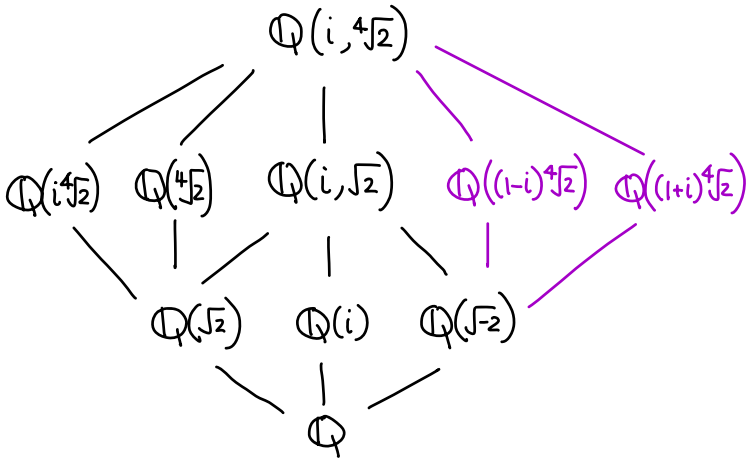


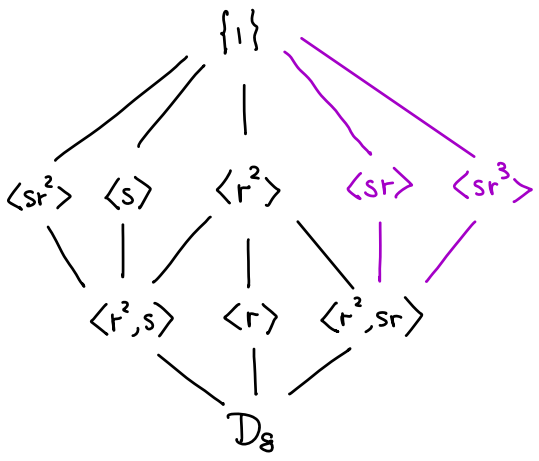
Example: A case of D_8 : $\theta = \sqrt[4]{2}$

The normal closure of $\mathbb{Q}(\sqrt[4]{2})$ is $\mathbb{Q}(i, \sqrt[4]{2})$

$s : i \mapsto -i \,,\ \sqrt[4]{2} \mapsto \sqrt[4]{2}$ $\qquad$ $rsrs : \sqrt[4]{2} \xmapsto{s} \sqrt[4]{2} \xmapsto{r} i\sqrt[4]{2} \xmapsto{s} -i\sqrt[4]{2} \xmapsto{r} \sqrt[4]{2}$

$r : \sqrt[4]{2} \mapsto i\sqrt[4]{2} \,,\ i \mapsto i$ $\qquad$ $i \mapsto i$ $\Rightarrow srs = r^{-1}$





Here $sr^2 : i \mapsto -i$ $\Rightarrow \mathbb{Q}(i, \sqrt[4]{2})^{sr^2=1} = \mathbb{Q}(i\sqrt[4]{2})$.

$\sqrt[4]{2} \mapsto -\sqrt[4]{2}$

$sr : i \mapsto -i \,,\ \sqrt[4]{2} \xmapsto{r} i\sqrt[4]{2} \xmapsto{s} -i\sqrt[4]{2}$

So $\underbrace{\sqrt[4]{2} - i\sqrt[4]{2}}_{\text{square} = -2i\sqrt{2} = -2\sqrt{-2}.} \in \mathbb{Q}(i, \sqrt[4]{2})^{sr=1}$

Finite fields.

q = a power of $p = p^r$

$\rightsquigarrow$ a unique finite field of q elements : $\mathbb{F}_q$ (perfect field)

Have shown: $\mathbb{F}_{q^n}$ = finite field of q^n elements; it is a normal (separable) extension of $\mathbb{F}_q$

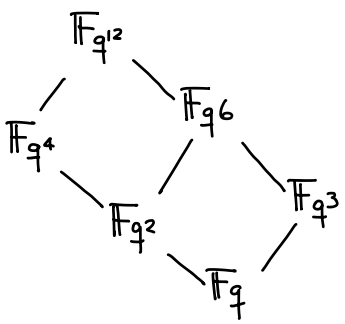
$\mathbb{F}_{q^n}$ $\qquad$ $\phi_q : \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_{q^n}$ called the q-Frobenius (same as composing ϕ_p r times)

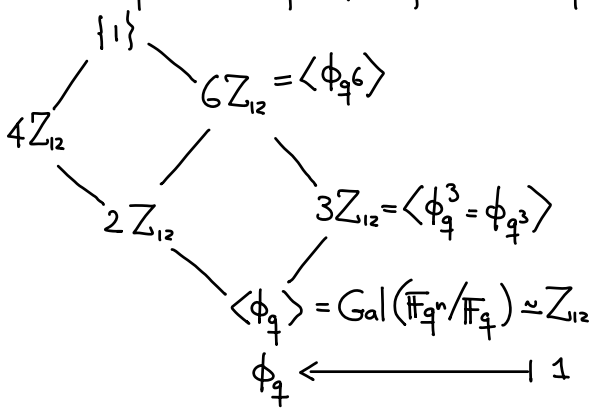
| $\qquad$ $a \mapsto a^q$

$\mathbb{F}_q$ $\qquad$ $\phi_q(a) = a \iff a^q = a \iff a \in \mathbb{F}_q$.

Similarly, $\phi_q^n(b) = b$, $\forall b \in \mathbb{F}_{q^n}$, so $\phi_q^n = id$ on $\mathbb{F}_{q^n}$ (not for smaller exponents.)

Example:





Definition. We say an extension K/F is abelian (阿贝尔扩张) if K/F is Galois and $Gal(K/F)$ is an abelian group.

Cyclotomic fields.

Let $\mu_n := \{n^{th} \text{ roots of unity in } \mathbb{C}\} = \langle \zeta_n \rangle \simeq \mathbb{Z}/n\mathbb{Z}$, where $\zeta_n = e^{2\pi i/n}$

Define $\mathbb{Q}(\mu_n) = \mathbb{Q}(\zeta_n) \subseteq \mathbb{C}$, a finite extension of $\mathbb{Q}$

A primitive n^{th} root of unity (本原 n 次单位根) is a generator of μ_n

$= \zeta_n^a$ for some $a \in (\mathbb{Z}/n\mathbb{Z})^\times$

Define $\Phi_n(x) = \prod_{a \in (\mathbb{Z}/n\mathbb{Z})^\times} (x - \zeta_n^a)$

Then $x^n - 1 = \prod_{b \in \mathbb{Z}/n\mathbb{Z}} (x - \zeta_n^b) = \prod_{d|n} \prod_{i \in (\mathbb{Z}/\frac{n}{d}\mathbb{Z})^\times} (x - \zeta_n^{di}) = \prod_{d|n} \Phi_{\frac{n}{d}}(x) = \prod_{d|n} \Phi_d(x)$

($\zeta_n^{di} = \zeta_{n/d}^i$; write $b = d \cdot i$ for $d = \gcd(b, n)$)

$\Rightarrow$ Inductively, $\Phi_n(x) = \dfrac{x^n - 1}{\prod_{d|n} \Phi_d(x)}$ (This makes sense in $\mathbb{Q}[x]$ $\xRightarrow{\text{Gauss Lemma}}$ This makes sense in $\mathbb{Z}[x]$)

is a monic polynomial in $\mathbb{Z}[x]$ of degree $\varphi(n)$

Theorem $\Phi_n(x)$ is an irreducible polynomial in $\mathbb{Q}[x]$. So $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$

- The Galois group of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is $(\mathbb{Z}/n\mathbb{Z})^\times$

$\forall a \in (\mathbb{Z}/n\mathbb{Z})^\times$, $\mathbb{Q}(\zeta_n) \xrightarrow{\sim} \dfrac{\mathbb{Q}[x]}{(\Phi_n(x))} \xrightarrow{\sim} \mathbb{Q}(\zeta_n)$

$\zeta_n \longleftarrow x + \Phi_n(x) \longmapsto \zeta_n^a$

i.e., $\sigma_a : \mathbb{Q}(\zeta_n) \longrightarrow \mathbb{Q}(\zeta_n)$

$\zeta_n \longmapsto \zeta_n^a$