Splitting fields recall

(Friedman, Thm 3.5, part I, p. 18).

Thm Let E/F finite extension. TFAE

(1) $\exists f \in F[x]$ s.t. E is a splitting field of f

(2) $\forall$ extension field L/E, if σ is a homomorphism, $\sigma(a)=a$ $\forall a\in F$ ($\sigma|_F = id$), then $\sigma(E)=E$ & σ is an automorphism of E

$$\begin{tikzcd} E \arrow[r, "\sigma"] \arrow[dr, no head] & L \arrow[d, no head] \\ & F \end{tikzcd}$$

(3) $\forall$ irreducible $p\in F[x]$, if p has a root in E then $p(x)$ factors into linear terms in $E[x]$.

$$\begin{tikzcd} L \arrow[d, no head] & L \arrow[d, no head, "\sim \text{ other choice}"] \\ E \arrow[r, "\sigma"] \arrow[dr, no head] & E \arrow[d, no head] \\ & F \end{tikzcd}$$

(2) says that E cannot be moved from its position.

(3) ~~says~~ implies that E is a splitting field for great many polynomials in $F[x]$, that can be built from various elements of E.

(1) $\Rightarrow$ (2) (1) says $E = F(\alpha_1, \ldots, \alpha_n)$ ← roots of f $\quad f = c(x-\alpha_1)\ldots(x-\alpha_n)$ | separable case, add powers in inseparable case

σ takes roots to roots, permutes α_i $\Rightarrow \sigma(F(\alpha_1 \ldots \alpha_n)) = \sigma(F)(\sigma(\alpha_1)\ldots \sigma(\alpha_n))$

$\{\sigma(\alpha_1)\ldots \sigma(\alpha_n)\} = \{\alpha_1 \ldots \alpha_n\}$ $\quad = F(\alpha_1, \ldots, \alpha_n)$

(2) $\Rightarrow$ (3) Suppose $p\in F[x]$ irreducible, has a root β in E, $p(\beta)=0$.

$\Rightarrow \exists$ extension K/E $\quad p$ factors in K $\quad p = c\prod_j (x-\beta_j)$ $(*)$ $\quad \underline{\beta=\beta_1}$

$\forall_j$ $\exists$ an isomorphism $\psi: F(\beta_1)\to F(\beta_j)\subset K$.

ψ extends to $\sigma: E \to L$,

$\sigma(a) = \psi(a)$ $\forall a\in F(\beta_1)$

by (2), $\sigma(E)=E$

$\Rightarrow \beta_j \in E$ $\forall j$ $\Rightarrow p$ factors as $(*)$ in E

$$\begin{tikzcd} E \arrow[r, dashed, "\sigma"] \arrow[d, no head] & L \arrow[d, no head] \\ F(\beta_1) \arrow[r, "\psi"] \arrow[dr, no head] & F(\beta_j) \arrow[d, no head] \\ & F \end{tikzcd}$$

$$\begin{tikzcd} & L \arrow[d, no head] \\ & K \arrow[d, no head] \\ F(\beta_1)\subset & E \arrow[d, no head] \\ & F \arrow[ul, no head] \end{tikzcd}$$

(3) $\Rightarrow$ (1) E/F finite ext $\Rightarrow \exists\, \alpha_1 \dots \alpha_n \in E$, $E = F(\alpha_1, \dots \alpha_n)$.

Let $p_i(x) = \operatorname{irr}(\alpha_i, F, x)$. p_i irr. w/ root in F.

by (3), p_i factors in E. Let $f(x) = p_1(x) \dots p_n(x)$.

$\Rightarrow f$ fully factors in E. $\Rightarrow E$ is the splitting field of f.

A splitting field extension is also called a normal extension

Examples 1) $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ – not normal, $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$ – normal, splitting field of $x^3 - 2$

$\omega = e^{2\pi i/3}$ cube root of 1

2) Any quadratic extension is normal (exercise)

1') $\mathbb{F}_p \subset \mathbb{F}_q$ normal ($x^q - x$)

3) $F = \mathbb{F}_p(t)$ $E = \mathbb{F}_p(u)$ $u^p = t$ $u = \sqrt[p]{t}$ splitting field of $x^p - t = (x - \sqrt[p]{t})^p$

not separable, normal

irr. in F only one root in splitting field

Prop (Friedman, Corollary 3.8 on p.20).

Let E/F be a finite extension. TFAE:

(1) E is a separable extension of F (always if char $F = 0$ or F is finite) or perfect

(2) $|\operatorname{Gal}(E/F)| = [E:F]$

Read proof in Friedman, straightforward.

Def A finite extension E/F is called Galois iff $|\operatorname{Gal}(E/F)| = [E:F]$

E/F is Galois iff E is both normal & separable extension of F.

Example 1) Splitting field of x^4-2 / $\mathbb{Q}$ $\qquad F=\mathbb{Q}$, $E=\mathbb{Q}(\sqrt[4]{2}, i)\subset\mathbb{C}$.

$\sqrt[4]{2},\ i\sqrt[4]{2},\ -\sqrt[4]{2},\ -i\sqrt[4]{2} \Rightarrow i\in E$, $\underset{\substack{\uparrow\\ \text{complex}}}{i} \notin \underset{\text{real}}{\mathbb{Q}(\sqrt[4]{2})}$ $\qquad$ separable, normal

$E \underset{\substack{\uparrow\\ \deg 2}}{\supset} \mathbb{Q}(\sqrt[4]{2}) \overset{\text{degree } 4}{\supset} \mathbb{Q}$ $\qquad \Rightarrow [E:\mathbb{Q}]=8 \Rightarrow \left|\underset{\substack{\shortparallel\\ G}}{\mathrm{Gal}(E/\mathbb{Q})}\right| = 8.$

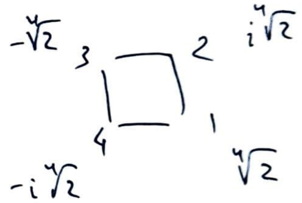
$G\subset S_4$ = permutations $(\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2})$ $\qquad E \overset{4}{\supset} \mathbb{Q}(i) \overset{2}{\supset} \mathbb{Q}$

Acts transitively, since x^4-2 is irreducible / $\mathbb{Q}$. $\qquad \Rightarrow x^4-2$ is irr / $\mathbb{Q}(i)$

$\sigma\in G$ $\qquad \sigma(\sqrt[4]{2})$ 4 choices, $\sigma(i)\in\{\pm i\}$ 2 choices

$\Rightarrow \sigma$ is determined by $\sigma(\sqrt[4]{2})$, $\sigma(i)$ and all choices are realized

$\sigma(i\sqrt[4]{2}) = \sigma(i)\sigma(\sqrt[4]{2})\ldots$



$G\simeq D_4$ dihedral group

$(24):\ \sigma(\sqrt[4]{2})=\sqrt[4]{2},\ \sigma(i)=-i$

$(1234):\ \sigma(\sqrt[4]{2})=i\sqrt[4]{2},\ \sigma(i)=i$

2) $\quad x^3-2$ / $\mathbb{Q}$ $\qquad E=\mathbb{Q}(\sqrt[3]{2},\omega)$ - all permutations of roots are in $G=\mathrm{Gal}(E/\mathbb{Q})$

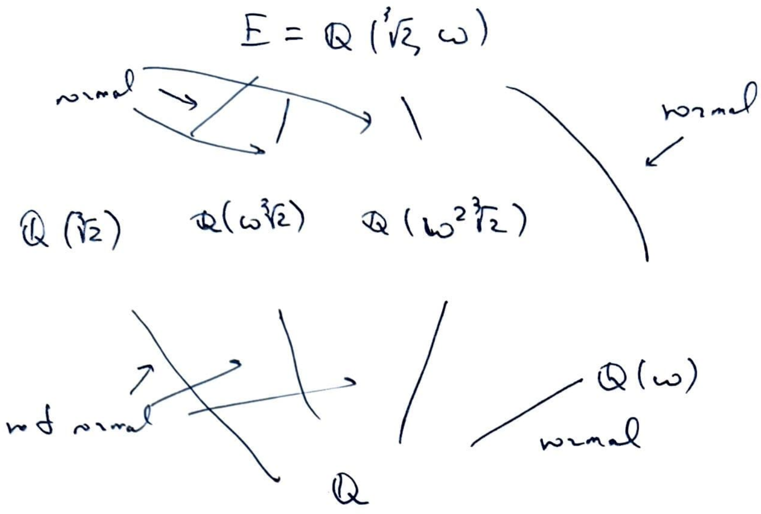
$G\simeq S_3$

3) $\mathbb{F}_p\subset\mathbb{F}_q$ $\quad q=p^n$ $\qquad \exists$ irred of deg n f $\qquad \mathbb{F}_q = E$ splitting field of x^q-x,

x^q-x redundancy. $\qquad \forall f(x)$ irr, deg n

$G=\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)\simeq C_n$ gen. by σ_p Frobenius.

In this example, f has n distinct roots, $\underset{\substack{\shortparallel\\ C_n}}{G}\subset S_n$ cyclic group.



<u>Prop</u> $F \subset K \subset E$. E/F normal $\Rightarrow$ E/K normal

<u>Proof</u> use the same polynomial for E/K as for E/F.

but K/F may not be normal $\qquad$ $\mathbb{Q} \subset \overbrace{\mathbb{Q}(\sqrt[3]{2}) \subset E}^{\text{normal}}$

$\qquad\qquad$ not normal $\qquad$ normal

Also possible: $F \subset K \subset E$ $\qquad$ $F \subset E$ not normal

$\qquad$ normal $\quad$ normal

$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$, $\qquad$ $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2})$ not normal.

normal

Thm (primitive element theorem)

Suppose F is a characteristic 0 field and E/F finite extension. Then $\exists\, \alpha \in E$, $E = F(\alpha)$

E can be generated by a single element / F.

Also works when char $F = p$ and F is perfect ($F = F^p$ $\sqrt[p]{\ }$ exists in F)

<u>Proof</u> By induction, enough to show $F(\alpha, \beta) = F(\gamma)$ for some $\gamma \in F(\alpha, \beta)$

Let $f(x) = \mathrm{irr}(\alpha, F, x)$, $g(x) = \mathrm{irr}(\beta, F, x)$.

They factor in some extension $L / F(\alpha, \beta)$

$f(x) = (x - \alpha_1) \dots (x - \alpha_n)$ $\qquad g(x) = (x - \beta_1) \dots (x - \beta_m)$ $\qquad \alpha = \alpha_1$, $\beta = \beta_1$

Look at linear combinations of α and β.

$\gamma = \alpha - c\beta$, $\quad c \in F$ generic

then $\gamma + cx = \alpha - c\beta + cx = \alpha + c(x - \beta)$

Define $h(x) = f(\underbrace{\gamma}_{\in F(\gamma)} + \underbrace{c}_{\in F} x) = f(\underbrace{\alpha}_{=\alpha_1} + c(x - \underbrace{\beta}_{=\beta_1}))$ $\qquad$ set $x = \beta$, get $h(\beta) = f(\alpha) = 0$

$\Rightarrow h(x) \in F(\gamma)[x]$ has coefficients in $F(\gamma)$

β is a root of h. Choose c generic so that no other β_j is a root of h

$h(\beta_j) = f(\alpha + c(\beta_j - \beta)) = 0$ iff $\alpha + c(\beta_j - \beta) = \alpha_i$ some i $\quad f(\alpha_i) = 0$

$c = \dfrac{\alpha_i - \alpha}{\beta_j - \beta}$, $c \in F$

bad values of c, avoid them

$\Rightarrow \gcd(h(x), g(x)) = x - \beta$.

$g(x) \in F[x] \Rightarrow \gcd$ is in $F(\gamma)[x]$.

$\Rightarrow \beta \in F(\gamma) \Rightarrow \alpha \in F(\gamma)$

choose $c \in F \setminus \left\{ \dfrac{\alpha_i - \alpha}{\beta_j - \beta} \right\}_{i,j}$

<u>done</u> γ generates $F(\alpha, \beta)$ $\square$

when generalizing to other fields, there is a problem if β is multiple root (inseparable case). F - finite $\to$ know that γ exists.

$\mathbb{F}_p(s,t) \subset \mathbb{F}_p(\sqrt[p]{s}, \sqrt[p]{t})$
$(x^p - s)(x^p - t)$
splitting field

Galois = normal (splitting field) + separable.

E/F Galois $\iff |Gal(E/F)| = [E:F]$.

If E/F - finite extension $\rightsquigarrow G = Gal(E/F)$.

smaller group, bigger subfield

if $H \subset G$ subgroup $\rightsquigarrow$ fixed field $E^H = \{\alpha \in E \mid \sigma(\alpha) = \alpha \ \forall \sigma \in H\}$.

If K intermediate field, $F \subset K \subset E$ $\to$ get a subgroup

$H = Gal(E/K) \subset Gal(E/F) = G$

symmetries that fix K elementwise

Thm (Main theorem of Galois theory, Friedman 4.1 p 23 I).
Let E/F be Galois. Then

(1) $\exists$ a one-to-one correspondence between subgroups of $Gal(E/F)$ and intermediate fields K, $F \subset K \subset E$.

$H \subset Gal(E/F) \longrightarrow$ fixed field E^H

$Gal(E/K) \longleftarrow$ K - intermediate field $F \subset K \subset E$

Mutually-inverse constructions

$$Gal(E/E^H) = H$$

$$E^{Gal(E/K)} = K$$

In particular, the fixed field of $Gal(E/F)$ is F,

largest group $\longrightarrow$ $E^{Gal(E/F)} = F$ $\qquad E^{\{1\}} = E$.

smallest int. field

(G_2: $\exists$ only fin. many intermediate fields).

(ii) this correspondence is order-reversing w.r.t. inclusion

(iii) $\forall H \subset G$, $[E : E^H] = |H|$, $[E^H : F] = (G : H)$ index.

$|Gal(E/K)| = [E : K]$.

(iv). for K , $F \subset K \subset E$, K is a normal extension of F iff

$Gal(E/K) \triangleleft \underset{\overset{\shortparallel}{G}}{Gal(E/F)}$ normal. then

K/F Galois and $Gal(K/F) = Gal(E/F) / Gal(E/K)$.

Example 1) $F=\mathbb{Q}$ $E=\mathbb{Q}(\sqrt{2},\sqrt{3})$ $G=Gal(E/\mathbb{Q})$

$(x^2-2)(x^2-3)$

$\sqrt{2}\ \ -\sqrt{2}$ $\quad\sqrt{3}\ \ -\sqrt{3}$

σ_1 fixes $\sqrt{3},-\sqrt{3}$ $\quad \sigma_2$ fixes $\pm\sqrt{2}$

$G \simeq C_2\times C_2$ Klein V_4 group.

5 subgroups $\quad G \quad \langle\sigma_1\rangle \quad \langle\sigma_2\rangle \quad \langle\sigma_1\sigma_2\rangle \quad \{1\}$.

$\sigma_1\sigma_2$: fixes $\sqrt{6}$.

H is one of these 5

Subfields $\quad E$

$\mathbb{Q}(\sqrt{2}) \quad \mathbb{Q}(\sqrt{3}) \quad \mathbb{Q}(\sqrt{6})$.

$\mathbb{Q}$

$E=E^{\{1\}}$

$\mathbb{Q}(\sqrt{2})=E^{\langle\sigma_2\rangle}$ $\quad \mathbb{Q}(\sqrt{6})=E^{\langle\sigma_1\sigma_2\rangle}$

$\mathbb{Q}(\sqrt{3})=E^{\langle\sigma_1\rangle}$

$\mathbb{Q}=E^{C_2\times C_2}$

No other subfields !

Corollary: any $\alpha=a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$, $\alpha\notin \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{6})$

$\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$ basis in E

generates E

$E=\mathbb{Q}(\alpha)$

simple extension.

$irr(\alpha,\mathbb{Q})$ has degree 4. Get lots of irreps, f.

E is a splitting field of any of these irreps.

$f(x)$ has 4 roots in E.

Often easier to build E using intermediate fields.

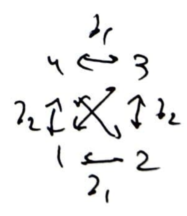
$\alpha=\sqrt{2}+\sqrt{3}$ root of $x^4-10x+1$ ← 4 roots

$\alpha=\beta_1=\sqrt{2}+\sqrt{3}$, $\beta_2=-\sqrt{2}+\sqrt{3}$, $\beta_3=\sqrt{2}-\sqrt{3}$, $\beta_4=-\sqrt{2}-\sqrt{3}$.

then $\sigma_1: \beta_1\leftrightarrow\beta_2, \beta_3\leftrightarrow\beta_4$, $\quad\sigma_2: \beta_1\leftrightarrow\beta_3, \beta_2\leftrightarrow\beta_4$, $\quad \sigma_3: \beta_1\leftrightarrow\beta_4, \beta_2\leftrightarrow\beta_3$.

$\sigma_1: (12)(34)$ $\quad \sigma_2: (13)(24)$ $\quad \sigma_3: (14)(23)$

this is a different embedding of $C_2\times C_2\subset S_4$.



$E^{\langle\sigma_1\rangle}$: $\underbrace{\beta_1+\beta_2}_{2\sqrt{3}}$ σ_1-invariant $\quad E^{\langle\sigma_2\rangle}$ $\beta_1+\beta_3=2\sqrt{2}$

$= \mathbb{Q}(\sqrt{3})$ $\quad = \mathbb{Q}(\sqrt{2})$

σ_3: $\beta_1+\beta_4=0$ does not help $\sigma_3(\beta_1)=-\beta_1 \Rightarrow \sigma_3(\beta_1^2)=\beta_1^2=5+2\sqrt{6}. \Rightarrow E^{\langle\sigma_3\rangle}=\mathbb{Q}(\sqrt{6})$.