lect 16, Nov 9.

Main ref: R. Friedman Notes G. Neeman I.

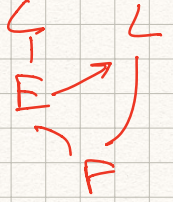
Thm (Friedman, Thm 3.5, part I, p. 18).
Let E/F be a finite extension. TFAE

(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 $\sigma: E \to L$, $\sigma|_F = id$, then $\sigma(E) = E$ & σ is an autom. of E.

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

(2): E is invariable rel. F

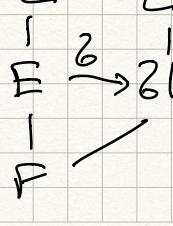


(3) implies E is split. field for pdys of polyn in $F(x)$:

take $\alpha_1 .. \alpha_n$ generate E. $\alpha_i \to f_i(x)$ irr(α_i, F, x)

E is spl. field of $\prod_{i=1}^{n} f_i(x)$

(1) $\Rightarrow$ (2) $E = F(\alpha_1 .. \alpha_n)$ $f = c(x-\alpha_1)..(x-\alpha_n)$

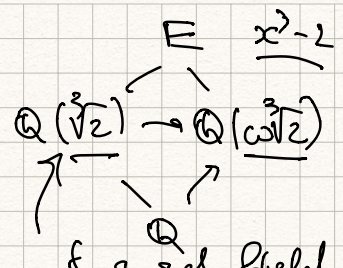


$\sigma(F) = F$ $\sigma(\alpha_i) = \alpha_j$

$\sigma(E) = \sigma(F(\alpha_1 .. \alpha_n)) =$

$= \sigma(F)(\sigma(\alpha_1) .. \sigma(\alpha_n)) =$

$= F(\alpha_1, \ldots, \alpha_n) = E$



(2) $\Rightarrow$ (3).

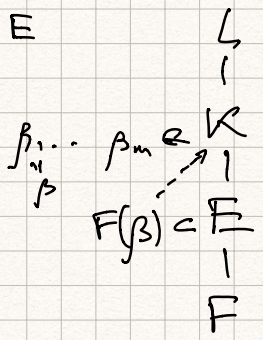
p - irr. in $F[x]$ has a root β in E

$p(\beta) = 0$.

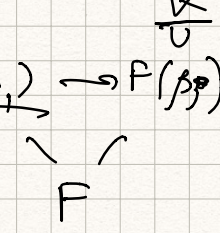
p factors in K

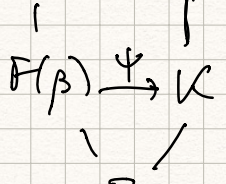
$\beta = \beta_1, \beta_2 \ldots \beta_m$ roots in K

$$p = c \prod_{j=1}^{m} (x - \beta_j)$$



$F(\beta_i) \cong F(\beta_j)$ $\exists$ a hom $\psi : F(\beta_1) \to F(\beta_j)$





ψ extends do σ.

but E is <u>invariable</u>

<u>$\sigma(E) = E$</u>

(don't need K, L after all)

$E \xrightarrow{\psi} E$

$\beta \xrightarrow{\psi} \beta_j^{\psi}$ $\Rightarrow \beta_j \in E \Rightarrow p$ factors in E.

Shows (2) $\Rightarrow$ (3)

(3) $\Rightarrow$ (1). E/F

E - chosen generators / F $\quad \alpha_1 \ldots \alpha_n \in E$

$p_i(x) = \text{irr}(\alpha_i, F, x)$. $\quad p_i$ - irr, root in E.

$p_i(\alpha_i) = 0$.

p_i - factors in E

$f(x) = p_1(x) \cdots p_n(x)$ $f(x)$ factors into q_i terms in E

E gen. by $\alpha_1 \ldots \alpha_n$, roots $\Rightarrow$ E splitting field. $\square$.

A splitting field extension E/F is also called a normal extension.

Ex 1) $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ – not normal

2) $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$ – normal
$x^3 - 2$

3) Any q. extension is normal.

4) $\mathbb{F}_p \subset \mathbb{F}_q$ normal $x^q - x$ $q = p^n$
$\exists$ many irr. / $\mathbb{F}_p$ of deg^n.

5) $F = \mathbb{F}_p(t)$ normal each such $f(x)$ $\mathbb{F}_q \simeq \mathbb{F}_p[x]/(f)$
rational f's

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

$x^p - t = (x-u)^p$

u ← has mult. p.

$F \subset E$, $[E:F] = p$

$|G| = |\langle p \rangle|$ $\mathrm{Gal}(E/F) = \{\}$.

Prop (Friedman, Corollary 3.8 on p. 20).
Let E/F be a finite extension. TFAE

(1) E is a separable extension of F, E is normal

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

See proof in Friedman.

$\forall\ |G| \le [E:F]$ — 2 obstructions do =

1) not separable
2) not all roots are in E_0

Def E/F finite is called Galois iff

$$|\mathrm{Gal}(E/F)| = [E:F].$$

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

Galois = normal + separable (*)

Ex Splitting field of x^4-2 / $\mathbb{Q}$ $\quad E \subset \mathbb{C}$

(x^4-2: Eisenstein.)

E

$\sqrt[4]{2},\ i\sqrt[4]{2},\ -\sqrt[4]{2},\ -i\sqrt[4]{2}$ roots $\quad i \notin \mathbb{Q}(\sqrt[4]{2})$

$E = \mathbb{Q}(\sqrt[4]{2}, i)$

x^2+1.

$\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2}) \subset E$

$4 \quad 2 \quad 2$

$i \notin \mathbb{Q}(\sqrt[4]{2})$, $i \in E$

$[E:\mathbb{Q}] = 8$., splitting field (normal), separable

$G = \mathrm{Gal}(E/\mathbb{Q})$ $\quad |G| = 8 = [E:\mathbb{Q}]$.

$G \subset S_4$ action of G is transitive on roots, since x^4-2 is irreducible (one orbit)

$\sigma \in G$ $\quad \sigma(\sqrt[4]{2})$ — 4 choices, any root.

determined by $\to \sigma(i)$ $\quad \sigma(i) \in \{\pm i\}$.

x^2+1 $\quad i$, $-i$ roots

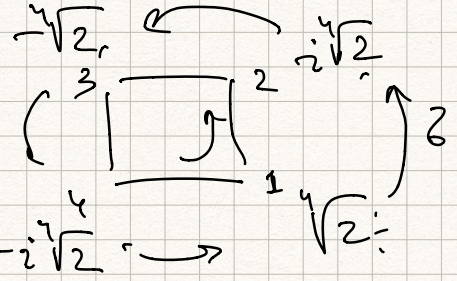
$\mathbb{Q}(\sqrt[4]{2}, i)$ For each $\sigma(\sqrt[4]{2})$, $\sigma(i)$ $\exists$ a unique symmetry σ.

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

$\pm i$ $\quad$ $\pm\sqrt[4]{2}$

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

$\sigma(i) = i$



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

$\sigma \leftrightarrow (1234) \in G \subset S_4$.

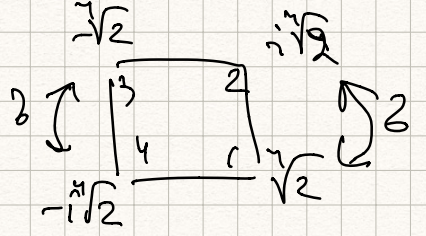
4 solutions

$\uparrow$

G

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

$\sigma(i) = -i$.

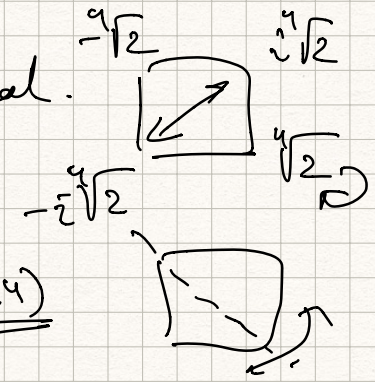


$\sigma(i\sqrt[4]{2}) = \sigma(i)\,\sigma(\sqrt[4]{2})$

$= -i\,i\sqrt[4]{2} = \sqrt[4]{2}$

$\sigma = (12)(34)$. reflection $\in G$.

$G = D_4 \subset S_4$ dihedral.



restrict complex conj to $E \subset \mathbb{Q}$

$[E : \mathbb{Q}] = 6$ 6-dim vect space/$\mathbb{Q}$ + multiplicative

$GL(n, F)$ V vs /F $\dim V = n$

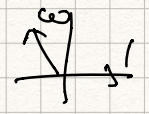
$GL(n, F) \cong$ Symmetries of v.s. V/F. of $\dim n$ $\quad$ invertible $n \times n$ matrices $\begin{pmatrix} & n & \\ & a_{ij} & \end{pmatrix}$ $a_{ij} \in F$

2) $x^3-2/\mathbb{Q}$ $\quad E=\mathbb{Q}(\sqrt[3]{2},\omega)$

$[E:\mathbb{Q}]=6$ $\quad G\cong S_3$

normal, Galois

$\omega=e^{2\pi i/3}=$

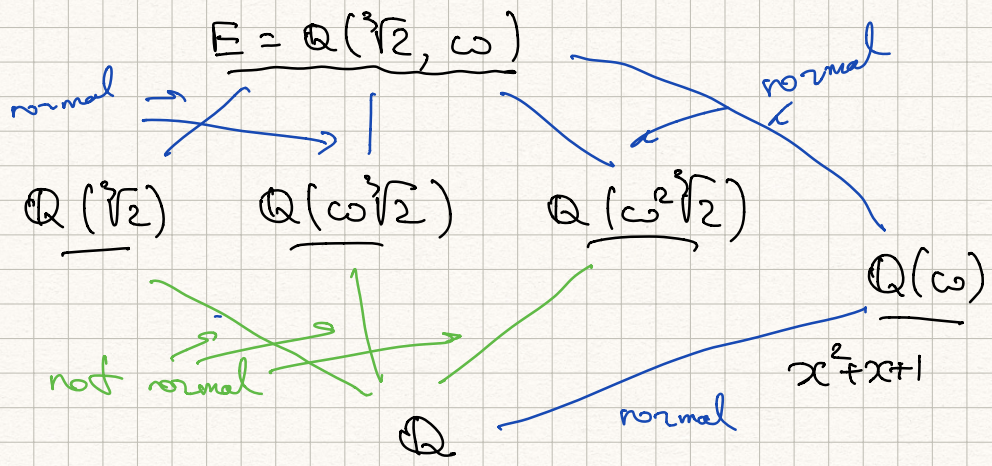


$=\frac{-1+\sqrt{-3}}{2}$

3) $\mathbb{F}_p\subset\mathbb{F}_q$ $\quad q=p^n$ $\quad$ normal, separable Galois

$\to \boxed{x^q-x}$

$\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)\cong C_n$ $\quad |C_n|=n=[\mathbb{F}_q:\mathbb{F}_p]$.



E - splitting field of f

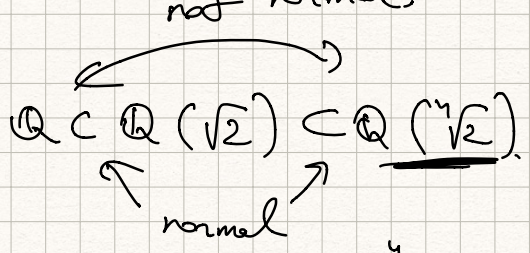
E ‖ normal

K $\quad f\in K[x]$ (normal)

F $\quad f\in F[x]$

$K\subset F\subset E$ — F may not be normal.

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 $\operatorname{char} F = p$ & F is perfect $F^p = F$ $\iff$ $\sqrt[p]{}$ exists in F.

Proof By induction, enough to show

$F(\alpha, \beta) = F(\gamma)$ for some $\gamma \in F(\alpha, \beta)$

$E = F(\alpha_1, \dots \alpha_m)$

$f(x) = \operatorname{irr}(\alpha, F, x)$

$g(x) = \operatorname{irr}(\beta, F, x)$.

$F(\alpha_1, \alpha_2) = F(\beta_1)$

$F(\alpha_1, \alpha_2, \alpha_3) = F(\beta_1, \alpha_3) = F(\beta_2)$

In some extension $L / F(\alpha, \beta)$ we can factor

$f(x) = (x - \alpha_1) \dots (x - \alpha_n)$ $\quad g(x) = (x - \beta_1) \dots (x - \beta_m)$

($\alpha_1 = \alpha$, $\beta_1 = \beta$)

$\boxed{\gamma = \alpha - c\beta}$ $\quad c \in F$ generic

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

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

$\gamma \in F(\gamma)$, F, x variable

$h(x) \in F(\gamma)[x]$

$h(\beta) = f(\alpha + c(\beta - \beta)) = f(\alpha) = 0$.

β is a root of h. $\beta = \beta_1$.

find c such that other β_j are not roots of $h(x)$

$\gcd(h(x), g(x))$

$h(\beta_j) = f(\alpha + c(\beta_j - \beta)) = 0$ ← avoid $\quad j \neq 1$. $\quad \beta = \beta_1$, $h(\beta_1) = 0$

$\alpha + c(\beta_j - \beta)$ not of α

$\alpha + c(\beta_j - \beta) = \alpha_i$ bad case

$c \neq \frac{\alpha_i - \alpha}{\beta_j - \beta}$, $j \neq 1$ $\quad i = 1 \ldots n$, $j = 2 \ldots m$ $\quad n(m-1)$.

$|F| > \infty$ can find such c.

Then β_1 is the only root of $h(x)$ in $\{\beta_1 \ldots \beta_m\}$ $\quad x - \beta_1 \mid h(x)$

$g(x) = (x - \beta_1) \ldots (x - \beta_m)$

$\gcd(h(x), g(x)) = x - \beta = x - \beta_1$

$F(\gamma)[x]$ $\quad F(x)$ $\quad F \subset F(\gamma)$

coeff of gcd are in $F(\gamma)$

$-\beta \in F(\gamma)$, $\beta \in F(\gamma)$

$\gamma = \alpha - c\beta$, $c \in F$. $\alpha = \gamma + c\beta \in F(\gamma)$

$\alpha, \beta \in F(\gamma)$ $\quad F(\gamma) = F(\alpha, \beta)$.

Friedman I.

Thm 2.5 on p. 13.

Rules-Compass (Rotman).

Midterm

II ⊂ I

III $\quad x^4 - 2$

IV.

D.