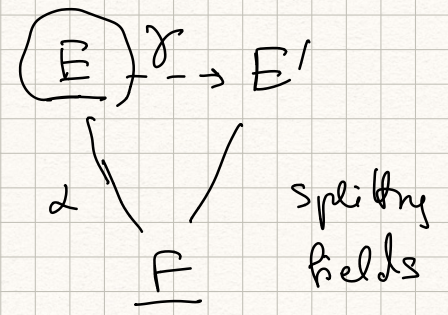
lecture 13

$f \in F[x]$



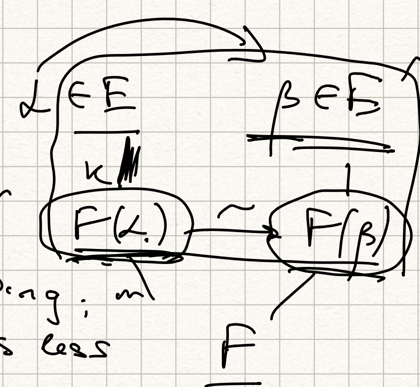
$f = f_1 \dots f_r$

irr. factors

γ - isomorphism

f_1 - irreducible factor

Any root in E generates a copy of field $F[x]/(f_1)$

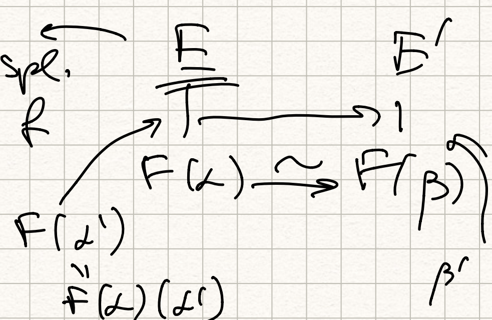


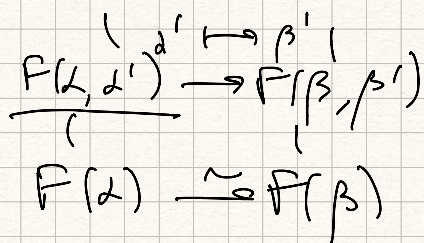
same f, more linear factors ← keep going; degree is less

$f = (X-\alpha)\dots\dots$

α' - root of irr. factor of f over $F(\alpha)$

still spl. field f





Thm $\forall$ two splitting fields of f

E, E' are isomorphic over F.

$\#$ isom $\leq [E:F]$.

if f is separable $/F$ then

$\#$ isom $= [E:F] = \dim_F E = [E':F]$

$f = f_1 \ldots f_r$ (irr) sep each f_i has only simple roots in any extension K/F. $\Rightarrow$

unusual in comparison to isom of rings

$\Leftrightarrow (f_i, Df_i) = 1 \Leftrightarrow Df_i \neq 0$

need char p & infinite F.

$E \xrightarrow{\gamma} E$ over F — γ is an automorphism

$$Gal(E/F) = \{ \gamma : E \to E \mid \gamma(a) = a \ \forall a \in F \}$$

$$\gamma|_F = id = id_F$$

γ takes a root to a root $\qquad f(x) \in F[x]$

$f = a_0 + a_1 x + \ldots + a_n x^n \qquad a_i \in F. \qquad \alpha \in E$

α - root $\quad f(\alpha) = 0 \quad a_0 + a_1\alpha + \ldots + a_n \alpha^n = 0$

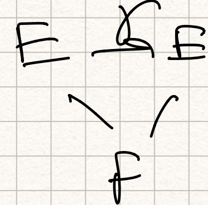
apply γ

$$\gamma(a_0)+\gamma(a_1)\gamma(\alpha)+\dots+\gamma(a_n)\gamma(\alpha)^n=0$$

$$a_0 + a_1\gamma(\alpha)+\dots+a_n\gamma(\alpha)^n=0$$

$\alpha \mapsto \gamma(\alpha)$

E | F fin. extension take $\alpha \in E$



$f(x)=\mathrm{Irr}(\alpha, F)$

$f(\alpha)=0$ $\underline{\gamma(\alpha)}$ also a root of f.

different α's $\to$ different polynomials

<u>Remark</u> If E split field of f.

$\alpha_1 \dots \alpha_n$ roots of f in F

γ $f = c(x-\alpha_1)\dots(x-\alpha_n)$

$g \in \mathrm{Gal}(E/F) = G$ $g(\alpha_i)=\alpha_j$ some j.

G acts on roots of f by permutations

$E = F(\alpha_1 \dots \alpha_n)$

$g \in G$ is determined by its action on $\alpha_1 \dots \alpha_n$

$G \longrightarrow \text{perm}(\alpha_1 \dots \alpha_n) = S_n$

this hom. is <u>injective</u>

$g(\alpha_i) = \alpha_j$

<u>Prop</u> if E spl. field of $f \in F[x]$,
$\alpha_1 \dots \alpha_n$ roots of f in E, hom.
<u>$\text{Gal}(E/F)$</u> $\to S_n = \text{perm}(\alpha_1 \dots \alpha_n)$
is <u>injective</u>.

change order of <u>roots</u>

Aut of $E \xrightarrow{g} E$ is determined by its values on roots

$$\begin{array}{c} E \\ | \\ F \end{array} \; f \qquad \alpha_1 \dots \alpha_n$$

random $\beta \in E$
has its own $m(\beta, F)$
$\uparrow$
not directly related to f.

E/F $\quad [E:F] = 2 \quad \alpha \in E/F$

$(1, \alpha)$ basis E $\quad a + b\alpha \quad a, b \in F$.

$\alpha^2 + b\alpha + c = 0$ some $b, c \in F$.

α is a root of $f(x) = x^2 + bx + c$.

if char $F \neq 2$

$$x^2 + bx + c = \left(x + \frac{b}{2}\right)^2 + c - \frac{b^2}{4} = \left(x + \frac{b}{2}\right)^2 - \left(\frac{b^2 - 4c}{4}\right) =$$

$\mathcal{D} = b^2 - 4c \in F$ discriminant of f.

$y = 2x + b$ $\quad x = \frac{y-b}{2}$ $\quad x, y$

$= \frac{1}{4}(y^2 - \mathcal{D})$ $\quad \operatorname{irr}(\beta, F) = x^2 - \mathcal{D}$. $\quad \alpha \mapsto \beta = 2\alpha + b$.

$$E \simeq F[x]/(x^2 + bx + c) \simeq F[y]/(y^2 - \mathcal{D})$$

$\forall$ Quadratic extension, char $F \neq 2$, reduces to

$E \simeq F[y]/(y^2 - \mathcal{D})$ $\quad \mathcal{D}$ not a square in F.

$y, -y$ roots of $x^2 - \mathcal{D}$ in E.

id, $\quad y \mapsto -y$. $\quad y \rightleftarrows -y$ $\quad g$

$g(y) = -y$, $g(-y) = y$

$g(a + by) = a - by$

Over $\mathbb{Q}$ can reduce $\mathcal{D}$

$\sqrt{\pm \frac{n}{m}} = \frac{1}{m}\sqrt{\pm nm}$ $\quad \sqrt{k} = p\sqrt{m}$

p^2 $\quad p^2$ $\quad k = p^2 m$

m - integer, ~~no~~ $\forall$ prime at most once

$m = \pm p_1 \ldots p_r$ at least 1 p if $m = p_1 \ldots p_r$

$x^2 - m$ irreducible $\quad x^2 - 1$

$x^2 - 2, x^2 - 3, x^2 - 5, x^2 - 6 \ldots \quad x^2 - 8$

x^2+1, x^2+3 . . .

get all quadratic extensions of $\mathbb{Q}$.

Galois group $E/\mathbb{Q}$ $E = \mathbb{Q}(\sqrt{D})$.

$G \simeq C_2$ $D = \pm p_1 \ldots p_r$

id

$\mathbb{Q} \overset{id}{\circlearrowleft}$ $\mathbb{Q} \circlearrowleft$ $\sqrt{D} \rightleftarrows -\sqrt{D}$

$\sqrt{D}$ $-\sqrt{D}$ "conjugates"

$F, f \rightarrow$ build splitting field E

$[E:F] \leq n!$ $n = \deg f$

$\forall \beta \in E \rightsquigarrow irr(\beta, F)$

$\mathbb{Q}(\sqrt{2}, \sqrt{3})$ $f = (x^2-2)(x^2-3)$

$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$

$\beta = \sqrt{2} + \sqrt{3}$ $x^4 - 10x^2 + 1 = irr(\sqrt{2}+\sqrt{3}, \mathbb{Q})$

$\gamma = 5\sqrt{2} - \frac{1}{2}\sqrt{3} + 51\sqrt{6} + \frac{71}{9}$ $irr(\gamma, \mathbb{Q})$.

(p. 4) $\mathbb{Q}[\alpha]/(\alpha^2+\alpha+1) \simeq \mathbb{Q}[y]/(y^2+3)$

α $\omega = e^{2\pi i/3}$ y

$\mathbb{C}$ $e^{2\pi i/3}$ $\pm\sqrt{-3}$.

$F = \mathbb{Q}$ $\quad E \quad$ $f(x) = x^3 - 2$ $\quad$ irr $\quad$ E. criterion, $p=2$

$E \subset \mathbb{C}$. $\quad \omega = e^{2\pi i/3}$

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

$\sqrt[3]{2} = \alpha_1$, $\sqrt[3]{2}\,\omega = \alpha_2$, $\sqrt[3]{2}\,\omega^2 = \alpha_3$

$\alpha_2, \alpha_3 \in \mathbb{C} \setminus \mathbb{R}$

$\mathbb{Q} \overset{3}{\subset} \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$

$\not\ni \alpha_2, \alpha_3$

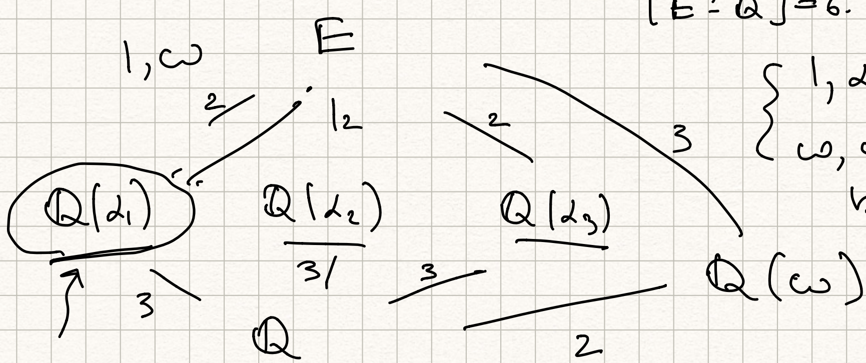
$$\mathbb{Q}(\alpha_i) \simeq \mathbb{Q}[x]/(x^3-2)$$

$$[\mathbb{Q}(\alpha_i) : \mathbb{Q}] = 3$$

basis $1, \alpha_i, \alpha_i^2$

$\alpha_i^3 = 2$

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



$$\left\{ \begin{matrix} 1, \alpha_1, \alpha_1^2 \\ \omega, \omega\alpha_1, \omega\alpha_1^2 \end{matrix} \right\}$$

basis of E.

$$x^3 - 2 = (x - \alpha_1)(x^2 + \alpha_1 x + \alpha_1^2)$$

$\alpha_1 = \sqrt[3]{2}$

$(x^2 + \alpha_1 x + \alpha_1^2)$ irr in $\mathbb{Q}(\alpha_1)$.

roots $\alpha_2, \alpha_3 \notin \mathbb{Q}(\alpha_1)$

$$[\underset{E}{\mathbb{Q}(\alpha_2, \alpha_1)} : \mathbb{Q}(\alpha_1)] = 2$$

$\omega^2 + \omega + 1 = 0$

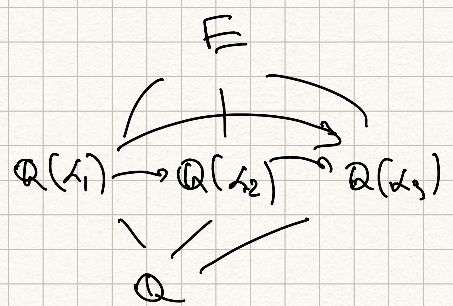
$\omega = e^{2\pi i/3}$

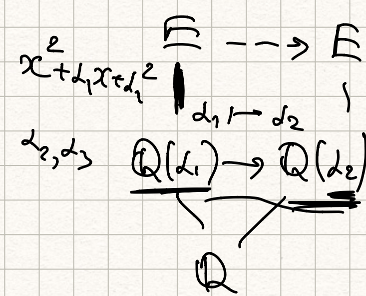
$$\omega = \frac{\alpha_2}{\alpha_1}$$

$\sqrt[3]{2} = \alpha_1 \quad \sqrt[3]{2}\,\omega = \alpha_2 \quad \sqrt[3]{2}\,\omega^2 = \alpha_3.$

$Gal(E/\mathbb{Q})$ permutes roots.

injective $\longrightarrow S_3$





$G = Gal(E/\mathbb{Q}) \qquad \underline{G \simeq S_3.}$

$|G| = [E:F]$

$|S_3| = 6 \qquad [E:F] = 6$

$\mathbb{F}_p \subset F \qquad |F| < \infty \Rightarrow |F| = p^n \quad n = [F:\mathbb{F}_p].$

<u>Remark</u> $\mathbb{F}_p \ni a$ a root of $\underline{x^p - x} =$

$x(x-1)\ldots(x-(p-1))$ F. little theorem

$\forall a \in \mathbb{F}_p^{\times} \quad a^{p-1} = 1 \Rightarrow \forall a \in \mathbb{F}_p \quad \underline{a^p = a}$

$q = p^n \quad f = x^q - x = x^{p^n} - x$

take splitting field $E/\mathbb{F}_p$ of f $\quad E$ finite.

__Ex__ if α, β are roots of f in $E \Rightarrow$

$\alpha+\beta$, $\alpha\beta$, α^{-1} (if $\alpha \neq 0$) are roots of f.

$(\alpha+\beta)^p = \alpha^p + \beta^p \Rightarrow (\alpha+\beta)^q = \alpha^q + \beta^q$.

$x^q - x$ $\quad \alpha^q - \alpha = 0$, $\beta^q - \beta = 0$

$(\alpha+\beta)^q - \alpha - \beta = \alpha^q + \beta^q - \alpha - \beta = 0$.

$(\alpha\beta)^q = \alpha^q \beta^q \overset{?}{=} \alpha\beta \Leftarrow \alpha^q = \alpha, \beta^q = \beta$

all roots of $x^q - x$ — all of E.

$0 \quad 0^q - 0 = 0$.

$\{$ roots of $x^q - x \}$ = splitting field E

$|E|$ = # of roots $\quad q$.

no repeated roots $\quad (f, Df) = 1$.

$Df = q x^{q-1} - 1 = 0 \cdot x^{q-1} - 1 = -1$.

$(f, -1) = 1$. all roots are simple (distinct).

$|E| = q = p^n \quad E \supset \mathbb{F}_p \quad \underline{x^p - x}$

q elements $\quad \Downarrow \quad a^p = a$

$a^q = a$ ⇓.

__Thm__ i) ∃ a field of order p^n, ∀ prime p, ∀ $n \geq 1$.

Splitting field of $x^{p^n} - x$, also consists of all roots of $x^{p^n} - x$.

$x^q - x$

2) $\forall$ two fields of cardinality p^n are isomorphic.

$\mathbb{F}_p \subset F \qquad |F| = p^n = q$

$\prod_{a \in F} (x - a) = x^q + \dots \qquad = x^q - x.$

↑ reducible into many terms.

$|F^*| = q - 1.$

$a \in F^* \quad a^{q-1} = 1 \Rightarrow a^q = a \quad \forall a \in F.$

$x^q - x.$

Example $\quad \mathbb{F}_4 = \mathbb{F}_2[\alpha] / (\alpha^2 + \alpha + 1). \qquad \begin{matrix} 1 & \alpha+1 \\ 0 & \alpha \end{matrix}$

Ex

$(x+0)(x+1)(x+\alpha)(x+\alpha+1) = x^4 - x$

($x+0$, $x+1$ ← $\mathbb{F}_2$; $x+\alpha$ ← α; $x+\alpha+1$ ← $\alpha+1$)

over $\mathbb{F}_2 \qquad x(x+1)(x^2+x+1) = x^4 - x.$

↑ irr / $\mathbb{F}_2$ $\qquad \alpha, \alpha+1$ 2 roots.

$\mathrm{Gal}(\mathbb{F}_4 / \mathbb{F}_2) \simeq C_2$

σ Frob $\quad \sigma(a) = a^p$

$\begin{matrix} \circlearrowleft 1 & \alpha+1 \\ \circlearrowleft 0 & \alpha \end{matrix}$ ($\alpha \leftrightarrow \alpha+1$)

$\mathbb{F}_8 \simeq \mathbb{F}_2[\alpha]/(\alpha^3+\alpha+1) \simeq \mathbb{F}_2[\beta]/(\beta^3+\beta^2+1)$

$x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$

linear ($\mathbb{F}_2$) — 3 roots — 3 roots.

$\mathbb{F}_p \subset F \qquad |F| = p^n$

$F^* \simeq C_{q-1}$ cyclic. take a gen α

$\{\alpha^n\}_{n \geq 0} = F^*$

$F = \mathbb{F}_p(\alpha)$

$E \,|\, F \qquad E \xrightarrow{\gamma} E \qquad \alpha^m \mapsto \beta^m$

$\alpha \in \xrightarrow{f} \beta = \gamma(\alpha)$ (f over F)

β also a root of f

$f(x) = a_0 + a_1 x + \dots + a_n x^n \qquad a_i \in F$

α root. $\quad$ # roots $\leq n$

$\gamma|_F = id \qquad \gamma(a_i) = a_i$

roots $f \to$ roots f

aut E/F (best we can)

$$|Gal(E/F)| \leq [E:F]$$

E/F split field $g \in Gal(E/F)$

$f = (x-\alpha_1)\dots(x-\alpha_n)$

$E = F(\alpha_1 \dots \alpha_n)$

root $\alpha_i \mapsto$ root α_j

$g \mapsto$ permutation of roots.

$\alpha_1 \mapsto \alpha_3$
$\alpha_2 \mapsto \alpha_4$ $\alpha_1^2 + a\alpha_2 \mapsto \alpha_3^2 + a\alpha_4$

$G \to S_n$ injective $G \subset S_n$

$x^3 - 2$ $\alpha_1 = \sqrt[3]{2}$ $\mathbb{Q}(\sqrt[3]{2})$

$g \in Gal(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{1\}$ $\mathbb{Q}$

α_1 $x^3 - 2$ $\sqrt[3]{2} = \alpha_1 \in \mathbb{Q}(\sqrt[3]{2})$ $g(\alpha_1)$ - root

$\alpha_2, \alpha_3 \notin \mathbb{Q}(\sqrt[3]{2})$ $g(\alpha_1) = \alpha_1$

$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. $|G| = 1 < 3$.

not a split. field, fewer automorphisms.