lect 12 Quiz 1 average 17.7/20

1) +(0)

$\underset{\text{field}}{\mathbb{F}_4} \not\cong \mathbb{F}_2 \times \mathbb{F}_2$ $(0,1), (1,0)$ $e^2 = e$ $e \neq 0, 1.$

not an ID, not a field $e(1-e) = 0$

both comm. rings, 4 elements each

other such comm. rings? $\mathbb{Z}/4$,

$\mathbb{F}_2[x]/(x^2)$ $a + bx$ $a, b \in \mathbb{F}_2$ $x x = 0$

$\mathbb{F}_4$, $\mathbb{F}_2 \times \mathbb{F}_2$, $\mathbb{Z}/4$, $\mathbb{F}_2[x]/(x^2)$ $0, (2), \mathbb{Z}/4$

only with additional idempotents 3 ideals each $0, (x)$, whole ring.

2) Frobenius $\delta_p : F \to F$ $x \mapsto x^p$.

homomorphism (endomorphism). always injective

isomorphism if F is finite. $\boxed{\text{char } F = p \text{, } F \text{ a field}}$

$a \mapsto a^p$ homomorphism

$\forall$ map $f : X \to X$ $|X| < \infty$

f injective $\Rightarrow$ f is surj, f isom. of sets.

isom = aut

3) $D : F[x] \to F[x]$ F-linear

not a homomorphism

$D(x^p) = p x^{p-1} = 0$ char p

$D(x^{np}) = 0$

$C_2 \times C_2$ not cyclic

$\cap$

$G \subset F^\times$ finite $\Rightarrow$ G is cyclic $C_4 \times C_6$

$\mathbb{F}_{25}^{*} = C_{24} \not\cong C_4 \times C_6 = \underline{\underline{C_4 \times C_2}} \times C_3$

$\cong \underline{\underline{C_8}} \times C_3$

7) fin $[E:F] = n < \infty \Rightarrow \forall\, \alpha \in E$ is alg /F

$1, \alpha, \ldots \alpha^n$ lin dep.

$\mathbb{Q}(\underbrace{\sqrt{2}, \sqrt{3}, \sqrt{5}, \ldots}\ )$ ext alg. but not f.d.

$F \subset B \subset E$ $\boxed{[E:F] = [E:B]\ [B:F]}$

$\underline{\text{inf} \quad \text{fin}}$

∞

$B = E$ $F \subset E \subset E$

17.7/20.

Def A splitting field of $f(x) \in F[x]$ is an extension E/F when f splits into linear factors, but f does not fully split into any proper subfield of E.

$f = c(x - \alpha_1) \ldots (x - \alpha_n)$ $F \subset E'$

In E', take $E = F(\alpha_1, \ldots \alpha_n)$
splitting field

$x^2+1 \in \mathbb{Q}[x]$ splits in $\mathbb{C}$, splitting field

$\mathbb{Q}(i) \subset \mathbb{C}$ $\qquad (x-i)(x+i)$

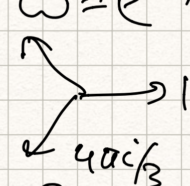
$\mathbb{Q}(i,-i) = \mathbb{Q}(i)$.

$x^3-1 \in \mathbb{Q}[x]$ splits in $\mathbb{C}$.

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

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

$= (x-1)(x-\omega)(x-\omega^2)$.



$\omega^2 = e^{4\pi i/3}$

splitting field $\mathbb{Q}(\omega)$ $\qquad \omega^2+\omega+1=0$

$[\mathbb{Q}(\omega):\mathbb{Q}] = 2$

Def An extension $F \subset E$ is *simple* if $\exists\, \alpha \in E$ $\quad E = F(\alpha)$

Separable polynomials

Def Irred $f(x) \in F[x]$ is *separable* if $f(x)$ does not have repeated roots in any extension of F.

$D f(x) = f'(x)$

if $f'(x) \neq 0$ $\qquad \deg f' < \deg f$

$\gcd(f', f) = 1$ since f is irreducible.

$\Rightarrow f$ has no repeated roots in any E/F.

$f = (x-\alpha)^2 \dots \qquad x-\alpha \mid f(x), f'(x).$

Only examples of $\underline{\text{irr.}}$ inseparable (not separable) is when $f'(x)=0$

$\underline{\text{char } F = p} \qquad f(x) = \underbrace{a_0 + a_1 x^p + a_2 x^{2p} + \dots + a_n x^{pn}}$

$D(x^{np}) = n\underline{p}\, x^{np-1} = 0$ in $F[x]$ $\qquad f$ irreducible.

not possible if $|F|<\infty$. $\quad \mathbb{F}_p$.

$\underline{(b+c)^p = b^p + c^p}$ $\qquad \dfrac{\alpha \mapsto \alpha^p}{F \to F}$ bijection

$\forall a \in F \ \exists b$ $\qquad$ finite

$\underline{b^p} = a$

$b_0^p = a_0, \ b_1^p = a_1.$

$\underset{F}{a_0} + \underset{F}{a_1} x^p \qquad |F| = p^n$

$\underline{a_0} + \underline{a_1} x^p = b_0^p + b_1^p x^p = b_0^p + (b_1 x)^p = \underline{(b_0 + b_1 x)^p}$

$$\begin{cases} a_0 + a_1 x^p + \dots + a_n x^{pn} = \\ (b_0 + b_1 x + \dots + b_n x^n)^p \end{cases} \qquad a_i = b_i^p$$

$(\underbrace{c_1 + c_2}_{} \dots + c_n)^p = c_1^p + \dots + c_n^p$

$(c_1 + c_2 + c_3)^p = ((\underbrace{c_1 + c_2}_{}) + \underbrace{c_3}_{})^p = (\underbrace{c_1 + c_2}_{})^p + c_3^p =$
$= c_1^p + c_2^p + c_3^p$

For bad examples (inseparable f) need to start with F, char $F = p$, not all el's of

F have p-th roots $\sqrt[p]{a}$ $\quad b^p = a.$

<u>example</u> $\mathbb{F}_p(t)$ rational functions in t

$$\frac{f(t)}{g(t)} \qquad a \mapsto a^p \qquad t \to t^p$$

$$\left(\frac{f}{g}\right)^p = \frac{f^p}{g^p} \qquad \sqrt[p]{t} = \frac{f}{g}.$$

$x^p - t$ is inseparable $\underline{\mathbb{F}_p(t)}$.

simplest such example.

Say a field char p is <u>perfect</u> if $\forall a$ has p-th root $\exists b$ $b^p = a$.

$\forall$ finite field is perfect, $\mathbb{F}_p(t)$ is not.

$f \in F[x]$ is <u>separable</u> if each irreducible factor of f is separable.

$f = f_1(x) \dots f_r(x)$ $\qquad$ if $F \supset \mathbb{Q}$, $\forall$ pol is separable.

over fin field, any polyn is separable.

An irred. polyn $f \in F[x]$ has exactly $\deg f = n$ $\quad n$ roots in its splitting field.

$F \subset E$ $\qquad f = (x - \alpha_1) \dots (x - \alpha_n)$

all $\alpha_1 \dots \alpha_n$ are distinct - $\underline{\exists\, n \text{ of them}}$

$F \subset E$ ← splitting field

take one root α_i

$\underline{F} \subset \underline{F(\alpha_i)} \subset \underline{E}$. α_i - root, f irreducible, separable, $n = \deg f$

$F(\alpha_i) \simeq F[x]/\underline{(f(x))}$

$$\begin{array}{ccccc} & \subset E & & & \\ F(\alpha_1) & \leftrightarrows & F(\alpha_2) \;\dots & \leftrightarrow & F(\alpha_n) \\ \alpha_1 \mapsfrom x \;\; \wr & & \wr & & \wr \;\; x \mapsto \alpha_n \\ & & \underline{F[x]/(f(x))} & & \end{array}$$

$F(\alpha_i) \simeq F(\alpha_j)$ $f = (x-\alpha_1)\dots$

$\underline{n \text{ roots}}$

$F \subset F(\alpha_i)$ n

In $\underline{\text{separable case}}$ E has automorphisms

~~$\#$~~ $|\underline{\mathrm{Aut}(E/F)}| = \underline{[E:F]}$

$\underline{\text{Thm}}$ $\sigma: F \to F'$ be an isom. of fields.

$\underline{f(x)} \in F[x]$ and $F[x] \xrightarrow{\sigma} F'[x]$

$\underline{f^\sigma(x)} = \sigma(f(x)) \in F'[x]$. $f \longmapsto \sigma(f) = f^\sigma$

Let E/F a splitting field of f in F. related coefficients $a_i \mapsto \sigma(a_i) \in F'$

E'/F' spl. field of f^σ in F'

1) There is an isomorphism $\tilde{\sigma} : \underline{E} \to \underline{E}'$ extending σ

2) if $f(x)$ is separable then σ has exactly $\underline{[E:F]}$ extensions

$\#$ of $\hat{\sigma}$ is the degree of $[E:F]$.

$$\begin{tikzcd} E \arrow[r, dashed, "\hat{\sigma}"] \arrow[d, dash] & E' \arrow[d, dash, "f^{\sigma}"] \\ F \arrow[r, "\sigma"] & F' \end{tikzcd}$$

__Proof__ Induction on $\underline{[E:F]}$.

$F \subset B \subset E$ $\quad$ $\underline{E}$ is splitting field of f over B.

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

1) $[E:F] = 1$ $\quad E = F$ $\quad f$ fully factors,

f^{σ} fully factors $\quad E' = F' \quad \hat{\sigma} = \sigma$

2) Ind. step. choose irreducible factor

$p(x) \mid f(x)$, $\deg p \geq 2$. $\quad (\deg p = m)$

$$\begin{tikzcd} E \arrow[d, dash] & E' \arrow[d, dash] \\ F \arrow[r, "\sigma"] & F' \end{tikzcd}$$

$\underline{p(x)}, f(x) \rightsquigarrow p^{\sigma}(x), f^{\sigma}(x)$.

p^{σ} irred

copy of p: $\underline{p^{\sigma}(x)}$

Choose a root β of $\underline{p(x)}$ in E.

$$\begin{tikzcd} E \arrow[d, dash] & & E' \\ F(\beta) \arrow[d, dash] & F(\beta) \simeq F[y]/(p(y)) & \\ F & & F' \end{tikzcd}$$

$p^\sigma(x)$ has a root in E', has $\overset{m}{\overset{\shortparallel}{\deg p}}$ roots if p is separable.

$$\begin{tikzcd} E \arrow[d, dash] & & E' \arrow[d, dash] \\ F(\beta) \arrow[rr, dashed, "\tilde{\sigma}"] \arrow[d, dash, "m"'] & & F'(\beta_i) \arrow[d, dash, "m"] \\ F \arrow[rr, "\sigma"] & & F' \end{tikzcd}$$

$p(x)$ factors $\nearrow E$; $\uparrow p^\sigma$ factors

m roots $\underline{\underline{\beta_1 \ldots \beta_m}}$ of p^σ in E'

choose β_i $1 \le i \le m$.

$F(\beta) \simeq F[x]/(p(x))$ $\qquad$ $F(\beta_i) \simeq F'[x]/\underline{(p^\sigma(x))}$

$\tilde{\sigma}(\beta) = \beta_i$ $\qquad \simeq$ extends σ.

$F \xrightarrow{\sigma} F'$ $\qquad x \longmapsto x$

$p(x) \longmapsto p^\sigma(x)$.

$$\begin{tikzcd} E \arrow[d, dash] & E' \arrow[d, dash] \\ F(\beta) \arrow[r, "\tilde{\sigma}"] \arrow[d, dash, "m"'] & F'(\beta_i) \arrow[d, dash, "m"] \\ F \arrow[r, "\sigma"] & F' \end{tikzcd}$$

m extensions, $m = \deg p$

$$[E:F(\beta)] = \frac{[E:F]}{\underset{\overset{\shortparallel}{[F(\beta):F]}}{m}}$$

$$\begin{tikzcd} E \arrow[r, dashed, "\hat{\sigma}"] & E' \\ F(\beta) \arrow[u, dash, "k"] \arrow[r, "\tilde{\sigma}"] & F'(\beta_i) \arrow[u, dash, "k"'] \end{tikzcd}$$

By induction, $\hat{\sigma}$ exists and, if f is separable, # of such $\hat{\sigma}$ is the degree

$[E : F(\beta)]$.

$$[E:F] = [E:F(\beta)][F(\beta):F].$$

$$\begin{array}{c} E \\ | \\ F \end{array}$$

$$\begin{array}{ccc} E & \dashrightarrow & E' \\ {\scriptstyle k}| & & | \\ F(\beta) & \xrightarrow{\hat{\tau}} & F(\beta_i) \\ {\scriptstyle m}| & & | \\ F & \xrightarrow{\tau} & F' \end{array}$$

m extensions

by induction, for each $\hat{\tau}$ there are k extensions

Rotman Thm 51, p. 56.

extensions exist, # of ext. is the degree (separable f)

<u>Corollary</u> if E/F is a splitting field of a separable polynomial f, then $[E:F] = $ # of automorphisms of E/F

$$\begin{array}{ccc} E & \xrightarrow{\tilde{\tau}} & E \\ & \diagdown \quad \diagup & \\ & F & \end{array}$$

$\tilde{\tau}$ is aut. of E

$\tilde{\tau}$ is identity on F

$\tilde{\tau}(a) = a \quad \forall a \in F$.

$$\boxed{\begin{array}{c}[E:F] = |\mathrm{Aut}(E/F)| \\ \text{degree} = \text{\# of symmetries}\end{array}}$$

if E is splitting f. of a separable polynomial.

Aut(E/F) Galois group

$\parallel$

Gal(E/F)

x^2-2 / $\mathbb{Q}$ $\quad \pm\sqrt{2} \quad \alpha_1=\sqrt{2}$

$\mathbb{Q}$ $\quad \alpha_2=-\sqrt{2}=-\alpha_1$

$x^2-2=(x-\sqrt{2})(x+\sqrt{2}) \quad \alpha_1 \to -\alpha_1$

$\mathbb{Q}(\alpha_1)\simeq \mathbb{Q}(\sqrt{2}) \quad [\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$

$\{1,\sqrt{2}\}$ 2 symmetries: identity 1, id

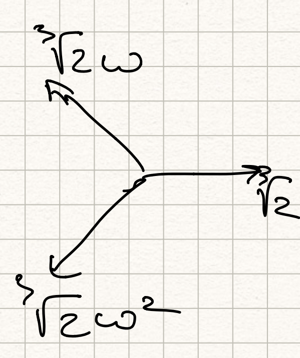
$\alpha_1 \to -\alpha_1$

$\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})=C_2$

$f=\underline{x^3-2}$ / $\mathbb{Q}$ irred by Eisenstein criterio.

$\mathbb{Q}\subset\mathbb{C}$ splitting field

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



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

$\underbrace{\mathbb{Q} \overset{3}{\subset} \mathbb{Q}(\sqrt[3]{2})}_{\cong} \overset{2}{\subset} \mathbb{Q}(\underline{\sqrt[3]{2}},\underline{\omega})=\underline{E}.$

$\underline{\mathbb{Q}[x]}/\underline{(x^3-2)} \quad 1, x, x^2$

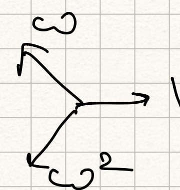
$\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ basis $/\mathbb{Q}$.

$\mathbb{Q}(\sqrt[3]{2}) \not\ni \omega$ - not really

$\cap$

$\mathbb{R}$

$$\underline{\omega^2+\omega+1=0}$$



$\underline{\mathbb{Q}(\sqrt[3]{2})}[y] \Big/ \underset{\text{irr}}{(y^2+y+1)}$ - field $\cong E$.

$$E \overset{2}{\supset} \underline{\mathbb{Q}(\sqrt[3]{2})} \overset{3}{\supset} \underline{\mathbb{Q}}$$

$[E:\mathbb{Q}] = 2\cdot 3 = 6$.

<u>basis of $E/\mathbb{Q}$</u>

$\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ basis of $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$

basis of $E/\mathbb{Q}(\sqrt[3]{2})$ $\{1, \omega\}$ $\omega^2 = -\omega - 1$ in E, in $\mathbb{C}$.

ba $\{1, \sqrt[3]{2}, \sqrt[3]{4}, \omega, \omega\sqrt[3]{2}, \omega\sqrt[3]{4}\}$

$\dim_{\mathbb{Q}} E = 6$.

roots in E.

$$x^2+x+1 = (x-\omega)(x-\omega^2)$$

x^3-2 roots $\underline{\sqrt[3]{2}}$, $\underline{\sqrt[3]{2}\,\omega}$, $\underline{\sqrt[3]{2}\,\omega^2}$

E

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

$\mathbb{Q}$

$\cong \quad \cong \quad \cong$

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

E

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

$$\mathbb{Q}(\underline{\sqrt[3]{2}\,\omega})$$

fix
isom

$$\underline{E} \longrightarrow E$$

$\underline{\omega}$ $\qquad \omega$

$$\underline{\mathbb{Q}(\sqrt[3]{2})} \longrightarrow \underline{\mathbb{Q}(\sqrt[3]{2}\,\omega)}$$

$\mathbb{Q}$

$\omega \quad x^2+x+1$

$$\sqrt[3]{2} \longrightarrow \sqrt[3]{2}\,\omega.$$

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

$$\omega \longrightarrow \omega$$

$$\omega \longrightarrow \omega^2$$

$$\sqrt[3]{2},\ \sqrt[3]{2}\,\omega,\ \sqrt[3]{2}\,\omega^2$$

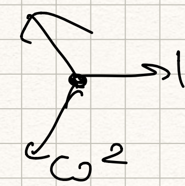
$\underline{6}$ aut. of E

$$[E:\mathbb{Q}]=6=|\mathrm{Aut}(E/\mathbb{Q})|$$

$\omega^3 = 1$, $\omega^6 = 1$ $\quad \underline{\underline{\omega^2}}$

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

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



$\overline{\omega} = \omega^2$

$x^n - 1$ are n-th roots of unity.

$\mathbb{C} \to \mathbb{C}$ $\quad x^2 + ax + b \quad \cancel{\sqrt{D}\in}$

$z \mapsto \bar{z}$ $\quad \quad D < 0$.

has 2 roots

$(x-\lambda)(x-\bar{\lambda})$ $\quad \lambda, \bar{\lambda}$

$\sqrt[3]{2}\,\omega^2$

$a + b\lambda \mapsto a + b\bar{\lambda}$

$\sqrt[3]{2}, \sqrt[3]{2}\,\omega, \sqrt[3]{2}\,\omega^2$ $\quad \sqrt[3]{2} \to \sqrt[3]{2}\,\omega$

$\mathbb{C}$ field + topology

$\mathbb{R}, \mathbb{C}$. $\quad \mathbb{R} \to \mathbb{R}$, $\quad \mathbb{C} \to \mathbb{C}$.

$\mathbb{R}$ as field, forget distance, top.

$\Rightarrow$ many automorphisms of $\mathbb{R}$.

$\mathbb{Q} \subset E$ $\quad [E : \mathbb{Q}] < \infty$.

$\mathbb{R}/\mathbb{Q}$ ← cannot explicitly write a basis of $\mathbb{R}$ over $\mathbb{Q}$.