lect 15.

Principle: Fields are rigid objects and automorphisms of fields are few (informal remark).

Automorphisms of rngs $\underline{\mathrm{Aut}(R)}$

$\underline{\sigma : R \to R}$ bijective, respects rng structure

σ^{-1} $\quad \sigma(1)=1 \quad \sigma(ab)=\sigma(a)\sigma(b)$

$\sigma(a+b)=\sigma(a)+\sigma(b)$

$\Rightarrow \sigma(0)=0$

$\mathrm{Aut}(\mathbb{Z}) = \{1\}$ (rng; $1 \mapsto$ id.)

$\mathbb{Z} \to$ rng

$\swarrow$ ab. group $\simeq C_\infty$

$\mathrm{Aut}(\mathbb{Z}) = 1$ (rng)

$\mathrm{Aut}(\mathbb{Z}) = \{\pm 1\}$ (group)

$\hookrightarrow$ permutation

$R \times R \quad (a,b) \to (b,a) \quad C_2 \subset \mathrm{Aut}(R \times R)$

$\mathrm{Aut}(\underline{\mathbb{Z} \times \mathbb{Z}}) \simeq C_2$ (rng)

$\mathrm{Aut}(\mathbb{Z} \times \mathbb{Q}) \simeq \{1\}$

$\mathbb{Z} \oplus \mathbb{Z}$ ab. group $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ $a,b,c,d \in \mathbb{Z}$

$\mathrm{Aut}(\underline{\mathbb{Z} \oplus \mathbb{Z}}) = GL(2,\mathbb{Z})$ (ab. group)

$\det A = \{\pm 1\}$

non-comm. R. R^* – invertible elements. group.

$c \in R^*$ acts on R by conjugation

$a \longmapsto cac^{-1}$, $a \in R$.

a^{-1} to go back

interesting if R non-commutative

$\underline{R^*} \xrightarrow{\varphi} \underline{Aut(R)}$ $\quad cac^{-1} = acc^{-1}ca$ if comm

homom.

$c \longmapsto \varphi_c$ $\quad \varphi_c(a) = cac^{-1}$

$\underline{Z(R)}$ – center $\quad Z(R) = \{ a \mid ab = ba \ \forall b \in R \}$

$\uparrow$ comm. ring.

Hw due Friday instead of today.

Comm ring $\longleftrightarrow$ geometry

functions on X $\longleftrightarrow$ X-space

$Fun(X)$

comm. ring.

Commutative rings $\longleftrightarrow$ Spaces

non-comm. ring $\longleftrightarrow$?

$\mathrm{Fun}(\mathbb{R})$

$f(a)=0$

$\longrightarrow \mathbb{R}$.

a

an ideal.

points of X $\longleftrightarrow$ (maximal) ideals of $\mathrm{Fun}(X)$.

$I \subset \mathrm{Fun}(\mathbb{R})$

$\uparrow$ Grothendieck

$I = \{ f \mid f(a)=0 \}$. ← max. ideal

$\mathrm{Fun}(\mathbb{R})/I \simeq \mathbb{R}$ ← field

$g(x) \longmapsto g(a)$

$R^* \xrightarrow{\varphi} \mathrm{Aut}(R)$

$c \longmapsto \varphi_c$

$\varphi_c(a) = cac^{-1}$

Ex $\ker\varphi$ =

$\{ c \mid cac^{-1} = a \ \forall a \in R \}$

$c \in Z(R)$.

$\ker\varphi = R^* \cap Z(R)$.

Ex $S = M_n(R)$ A - invertible

$B \longmapsto ABA^{-1}$ aut. of $M_n(R)$.

$R = \mathbb{R}, \mathbb{C}$.

$M_n(\mathbb{R})^* \xrightarrow{\varphi} \mathrm{Aut}(S)$.

Ex $\ker\varphi = \left\{ \begin{pmatrix} a & & 0 \\ & \ddots & \\ 0 & & a \end{pmatrix} \quad a \in R^* \cap Z(R) \right\}$

$R = \mathbb{R}$ $\quad \ker\varphi = \{ a \cdot I \mid a \in \mathbb{R}^* \}$.

Principle Easier to work with rings that are defined over a field.

F - field

Def An F-algebra R is a ring with a homomorphism $F \xrightarrow{\gamma} R$, γ is injective

$1 \longmapsto 1$

$F \cong \gamma(F)$ $\quad F \subset R$ field ring $\quad$ R - vect. space/F.

Example $R = E$ E/F, $\quad$ F-alg

$F[x]$, $F[x,y]$, $R/I \leftarrow$ F alg.

$F[x]/I \cong F[x]/(f(x))$.

f - irreducible $\to$ $F[x]/(f)$ is a field

f - reducible $F[x]/(f)$ F - alg. vect space/F.

Example $R = F[x]/(x^2)$ inf.

$x \cdot x = 0$ $x \neq 0$ $\quad x^2 = 0$ $\quad x$

$\mathrm{Aut}(R) \supset \mathrm{Aut}(R/F)$ $\quad \delta(a) = a$ $\forall a \in F$

$\delta(a + bx) = \delta(a) + \delta(b)\delta(x) =$ $\quad (1, x)$ $\quad F \circlearrowleft$

$\gamma : F \to F$

$\gamma(x) = x$

$= a + b\,\delta(x)$.

$y^2 = 0$ $\quad y = \lambda x$ $\quad \lambda \in F$. $\quad x^2 = 0$, $(\delta(x))^2 = 0$, $\lambda \in F^*$

$x \longmapsto \lambda x$

$\delta(x) = \lambda x$ an aut.

$\delta^{-1}(x) = \lambda^{-1} x$.

$\mathrm{Aut}(R/F) \simeq F^*$ $\quad$ more flexible than for field extensions

$\delta_\lambda \longleftrightarrow \lambda$

$\delta_\lambda(x) = \lambda x$

$R = F[x]/(x^3)$ $\quad a + bx + cx^2$ $\quad \mathrm{Aut}(R/F)$

$y = \delta(x)$ $\quad x^3 = 0$ $\quad \delta(x)^3 = 0$.

$y = bx + cx^2$

$y^3 = 0$.

$y^3 = (bx + cx^2)^3 =$

$= b^3 x^3 + \ldots x^4 \ldots = 0$

$\delta(x) = bx + cx^2$ a homomorphism

$\delta(x^2) = \delta(x)^2 = (bx + cx^2)^2 = b^2 x^2 + \ldots = b^2 x^2$

	1	x	x^2
1	1	0	0
x	0	b	0
x^2	0	c	b^2

δ is a homomorphism

δ bijective $\to$ δ is an automorphism

$b \neq 0$

$\forall b, c \in F \quad b \neq 0 \qquad \sigma(x) = bx + cx^2$

↳ invert

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & b^{-1} & 0 \\ 0 & u & b^{-2} \end{pmatrix}$$

$\sigma^{-1}(x) = b^{-1}x - b^{-3}cx^2$ $\qquad ub + b^{-2}c = 0$, $u = -b^{-3}c$

for field extensions $F \subset E$

if $[E:F] = 2$ $\qquad Aut(E/F) = Gal(E/F)$

$= \{1\}$ or C_2.

$E/F \qquad \sigma \in Gal(E/F)$

α alg. $/F$

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

root of $f(x) = a_0 + a_1x + \dots + a_nx^n$

$$\begin{array}{ccc} E & \xrightarrow{\sigma} & E \\ & \nwarrow \quad \nearrow_{\sigma(\alpha)} & \\ & F & \end{array}$$

α also a root of same polynomial

$a_i \in F \qquad \sigma|_F = id$

at most n roots in E. $\qquad$ at most n choices for images of α.

$$\begin{array}{ccc} E & \xrightarrow{\sigma} & K \\ & \nwarrow \quad \nearrow & \\ & F & \end{array}$$

at most n homomorphisms $F(\alpha) \xrightarrow{\sigma} F$ s.t. $\sigma|_F = id$

since $\exists$ at most n roots of f in K.

get a bound on # of hom $F(\alpha) \to K$

$[F(\alpha) : F] = n = \deg f$

E/F at most $\deg F(\alpha)/F$ hom. into K

$$\begin{array}{ccc} F(\alpha_1,\alpha_2) & \xrightarrow{\beta_2} & K \\ \Big\uparrow n_2 & & \| \\ F(\alpha_1) & \xrightarrow{\beta_1} & K \\ \Big\uparrow n_1 & & \nearrow \\ F & & \end{array}$$

at most β_2 hom. given β_1

at most n_1 hom β_1

at most $n_1 n_2$ hom $F(\alpha_1,\alpha_2) \to K$.

& so on

# of hom $E \to K$ that extend identity $\leq [E:F]$.

$$[F(\alpha_1,\alpha_2) : F] = [F(\alpha_1,\alpha_2) : F(\alpha_1)]\,[F(\alpha_1) : F]$$

$n_2 \qquad\qquad n_1$

to have $=$, need separability (always true on char 0)

+ K must contain all roots $f_1 \ldots$

must contain suitable field.

Special case $E = K \Rightarrow$

$E \xrightarrow{\beta} E$ hom. is an aut-

F

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

$=$ if E is "suff. large"

E is a splitting field of f

separable

fails for rings $F[x]/(x^2)$ $\supset F$

E be a field, $\sigma \in Aut(E)$.

Def $E^\sigma \subset E$ fixed field of σ

$E^\sigma = \{a \in E \mid \sigma(a) = a\}$. Ex E^σ is a subfield.

E_0 - prime subfield

$\mathbb{F}_p, \mathbb{Q}$

$X \subset Aut(E)$.

$E^X = \{a \in E \mid \sigma(a) = a \ \forall \sigma \in X\}$

$E^X \subset E$ a subfield $E^X = \bigcap_{\sigma \in X} E^\sigma$

$X \longrightarrow \langle X \rangle \subset Aut(E)$

smallest subgroup that contains X.

$E^X = E^{\langle X \rangle}$

$H \subset Aut(E)$ subgroup $E^H \subset E$ subfield

Principle : In nice cases, will have a bijection

subgroups H of symmetries of E $\longleftrightarrow$ subfields $K \subset E$

$H \longmapsto E^H$.

symmetries fix K. $\longleftarrow$ K

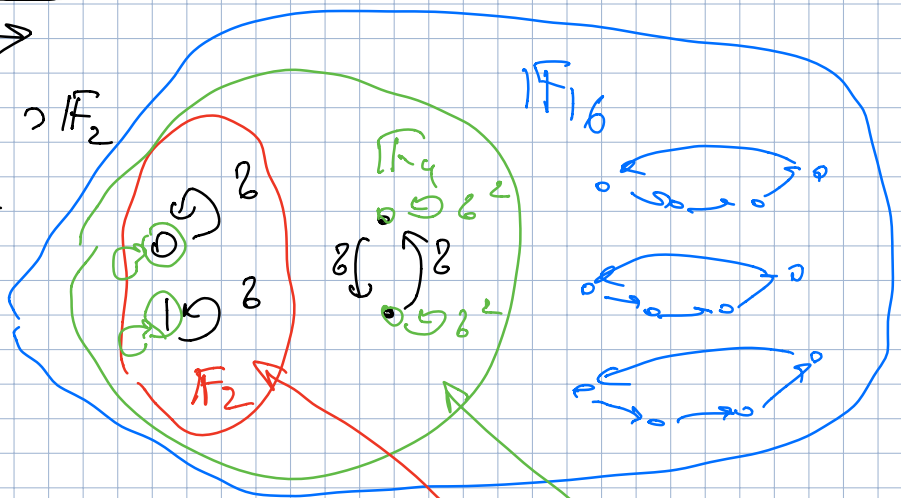
not many symm, not many subfield

reverses the size.

$H_1 \subset H_2 \Rightarrow E^{H_2} \subset E^{H_1}$

$\mathbb{F}_{16} \supset \mathbb{F}_4 \supset \mathbb{F}_2$

$\sigma(a) = a^2$



$\mathrm{Aut}(\mathbb{F}_{16}) = \mathrm{Gal}(\mathbb{F}_{16}/\mathbb{F}_2)$

$\{1, \sigma, \sigma^2, \sigma^3\} \simeq C_4$

$C_4 \supset C_2 \supset C_1$

$\{1, \sigma^2\}$ $\{1\}$

$\mathbb{F}_{16}^{C_2} \simeq \mathbb{F}_4$ bigger $\mathbb{F}_{16}^{C_4} = \mathbb{F}_2$ smaller

$\mathbb{F}_{16} \simeq \mathbb{F}_{16}^{C_1}$

$\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ - trivial symm

$\sqrt[3]{2}$ $\quad$ $\mathbb{C}$

Friedman, Gr. 1.B

E/F $\quad f \in F[x]$ $\quad \alpha_1 .. \alpha_n$ - distinct roots of f in E.

$Gal(E/F)$ acts on $\{\alpha_1 .. \alpha_n\}$ & there is a homomorphism

ρ: $Gal(E/F) \longrightarrow S_n$.

If also $E = F(\alpha_1 .. \alpha_n)$ then ρ is injective and $Gal(E/F) \subset S_n$.

$E \xrightarrow{\sigma} E$ $\quad \sigma$ permutes the roots.

F $\quad \sigma \longmapsto$ permutation in S_n (choose order of roots)

$Gal(E/F) \subset S_n$

$|Gal(E/F)| \mid n!$

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

4 roots in splitting field $\quad E \subset \mathbb{C}$.

$\pm\sqrt{2}, \pm\sqrt{3}$.

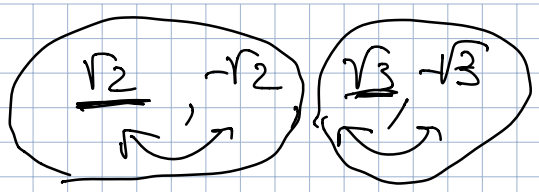
$\sqrt{3}$

$E \supset \mathbb{Q}(\sqrt{2}) \supset \mathbb{Q}$

$2 \quad\quad 2$

$G = \mathrm{Gal}(E/\mathbb{Q})$

$G \longrightarrow S_4$ injective



4 symmetries.

$$\begin{array}{ccc} E & \xrightarrow{\tau} & E \\ | & & | \\ \mathbb{Q}(\sqrt{2}) & \xrightarrow{\tau_1} & \mathbb{Q}(\sqrt{2}) \\ | & & | \\ \mathbb{Q} & = & \mathbb{Q} \end{array}$$

$\sqrt{3}$

$\tau(\sqrt{3}) = \sqrt{3}$ or $-\sqrt{3}$.

$\tau_1(\sqrt{2}) = \sqrt{2}$ or $-\sqrt{2}$

$G \cong C_2 \times C_2$

$[E:\mathbb{Q}] = |G| = 4$.

$x^4 - 2$

irred.

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

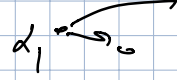
Prop If E/F is a splitting field of irreducible $f \in F[x] \Rightarrow$

$\mathrm{Gal}(E/F)$ acts transitively on roots of f in E.

$$\begin{array}{ccc} E & \xrightarrow{\sigma} & E \\ | & & | \\ F(\alpha_1) & \xrightarrow{\simeq} & F(\alpha_i) \\ & \searrow \quad \swarrow & \\ & F & \end{array}$$

$\alpha_1 \mapsto \alpha_i$

$\alpha_1 \longrightarrow \alpha_i$



$F(\alpha_i) \cong F[x]/(f)$

$f = (x - \alpha_1) h(x)$

$\uparrow$

$F(\alpha_1)[x]$