Automorphisms of fields is a rigid situation (not many automorphisms).

Automorphisms of rings $\text{Aut}(R)$

$\sigma: R \longrightarrow R$ bijective, respects ring structure

$\sigma(1)=1 \quad \sigma(a+b)=\sigma(a)+\sigma(b)$
$\sigma(ab)=\sigma(a)\sigma(b)$
$\Downarrow$
$\sigma(0)=0$

<u>Example</u> $\text{Aut}(\mathbb{Z}) = \{1\}$ identity autom. only

$\uparrow$ ring

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

$\uparrow$ abelian group

$\mathbb{Z}$ is both a ring & ab. group, specify which structure you consider

<u>Exercise</u> 1) $\text{Aut}(\mathbb{Z}\times\mathbb{Z}) \cong C_2$ id, permute terms.

$\uparrow$ direct product of rings

If consider $\mathbb{Z}\times\mathbb{Z}$ as abelian group $\mathbb{Z}\oplus\mathbb{Z}$, it has many automorphisms

$\text{Aut}(\mathbb{Z}\oplus\mathbb{Z}) = GL(2,\mathbb{Z})$

invertible 2×2 matrices with integer coeff.

2) $\text{Aut}(\mathbb{Z}\times\mathbb{Q}) = \{id\}$ check that $\sigma(e)=e$ if e is an idempotent.

classify idempotents in $\mathbb{Z}\times\mathbb{Q}$.

$(1,0), (0,1), (0,0), (1,1)$

prove any autom. fixes each of them ?

$(0,0)$: zero; $(1,1)$: identity.

Consider group R^* of invertible elements of R.

Suppose R is a <u>non-commutative</u> ring

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

$a \longmapsto cac^{-1}, \quad a\in R.$ Check this is a homomorphism

Get a homomorphism $R^* \xrightarrow{\varphi} \text{Aut}(R)$ $(*)$

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

<u>Remark</u> Center of R, denoted $Z(R)$, is $\{a \mid ab=ba \ \forall b\in R\}$

<u>Exercise</u> $Z(R)$ is a commutative ring, $Z(R) \subset R$ a subring

$Z(R)=R$ iff R is commutative.

Check that $\ker\varphi = R^* \cap Z(R)$ φ is given by $(*)$

normal subgroup of R^*

Exercise. Let $M_n(R)$ be the matrix algebra, R commutative.

then $Z(M_n(R)) \simeq R \cdot Id$ ← multiples of identity matrix

For general, noncommutative, R, $Z(M_n(R)) \simeq Z(R)$.

Often consider F-algebras, F a field. (assume $R \neq 0$)

Def An F-algebra R is a ring R with a homomorphism

$F \xrightarrow{\gamma} R$.. γ is injective, field F is a subring of R.

R acquires a structure of F-vector space, can do linear algebra, convenient

Examples $R = F$, $R = E/F$ - field that contains F, $F[x]$, $F[x,y]$, ...

R/I, where I is any ideal, R an F-algebra

$F[x]/I \simeq F[x]/(f(x))$, some polynomial $f(x)$.

If f is reducible, $R = F[x]/(f)$ is not a field.

Example $R = F[x]/(x^2)$. $Aut(R/F)$ - autom that fix all el's of F

not a field

$a+bx$, $a,b \in F$ $\qquad \sigma \in Aut(R/F)$

$\sigma(a+bx) = a + b\sigma(x)$. $\qquad \sigma(x)$ satisfies $(\sigma(x))^2 = \sigma(x^2) = 0$.

$\Rightarrow \sigma(x) = \lambda x$, $\lambda \in F^*$ $\qquad \lambda = 0$ not an automorphism.

$\Rightarrow Aut(R/F) \simeq F^*$ $\qquad$ if $|F| = \infty$, get ∞-many automorphisms.

but $\qquad$ fields are more rigid, this cannot happen

$\dim_F R = 2$ $\qquad [E:F] = 2 \Rightarrow Gal(E/F) = C_2$ or $\{1\}$ trivial

not a field

Exercise Let $R = F[x]/(x^3)$. $\qquad \sigma(x)$ must satisfy $\sigma(x)^3 = \sigma(x^3) = 0$.

$a + bx + cx^2$ $\qquad \Rightarrow \sigma(x) = ux + vx^2$, $u,v \in F$, $u \in F^*$ ← otherwise σ is not an automorphism

get a large group of automorphisms of R → and compositions $\begin{cases} x \mapsto ux & u \neq 0 \text{ ok} \\ x \mapsto x + vx^2 & \text{ok} \end{cases}$

Reminder E/F field extension $\sigma \in Gal(E/F)$,

take algebraic $\alpha \in E$, $a_0 + a_1\alpha + \dots + a_n\alpha^n = 0$ $a_i \in F$, $f(\alpha) = 0$

$f(x) = Irr(\alpha, F) = a_n x^n + \dots + a_0$

$$\begin{tikzcd} E \arrow[r, "\sigma"] & E \\ & F \arrow[ul] \arrow[u] \end{tikzcd}$$

$\alpha \in E$, $\sigma(\alpha) \in E$

$\sigma(\alpha)$ has the same irreducible polynomial

$Irr(\sigma(\alpha), F) = Irr(\alpha, F) = f(x)$.

f has at most n roots $\alpha_1, \dots, \alpha_m$ $m \leq n$ in $E \Rightarrow$

at most n choices for $\sigma(\alpha) \in \{\alpha_1 \dots \alpha_m\}$.

if $E = E(\alpha)$, look at homomorphisms into any K/F

$$\begin{tikzcd} F(\alpha) = E \arrow[r, "?"] & K \\ & F \arrow[ul] \arrow[u] \end{tikzcd}$$

$\sigma(E) \subset K$ subfield, $\sigma(E) \supset F$

$\sigma|_F = id \Rightarrow$ at most m homomorphisms, where $m \leq n$ is the # of roots of f in K

$E \xrightarrow{\sigma} K$, $\sigma|_F = id$

$$\boxed{\text{such homomorphisms, if } E = F(\alpha), \text{ are in a bijection with roots of } f(x) \text{ in } K.}$$

$\Downarrow$

get a bound on # of homomorphisms, at most $n = \deg f$.

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

Can iterate, if have

$$\begin{tikzcd} E = F(\alpha_1, \alpha_2) \arrow[r, dashed, "\sigma_2"] & K \\ F(\alpha_1) \arrow[u, dash, "n_2"] \arrow[r, dashed, "\sigma_1"] & K \arrow[u, equal] \\ F \arrow[u, dash, "n_1"] \arrow[ur, dash] & \end{tikzcd}$$

K field

at most $[F(\alpha_1) : F] = n_1$ homomorphisms (extensions) σ_1

Fix σ_1, at most $n_2 = [F(\alpha_1, \alpha_2) : F(\alpha_1)]$ extensions to σ_2

$f_1 = Irr(\alpha_1, F)$ $\deg f_1 = n_1$

$f_2 = Irr(\alpha_2, F(\alpha_1))$ $\deg f_2 = n_2$

$\Rightarrow$ at most $n_1 n_2$ extensions to $E = F(\alpha_1, \alpha_2)$

$n_1 n_2 = [F(\alpha_1, \alpha_2) : F(\alpha_1)][F(\alpha_1) : F] = [F(\alpha_1, \alpha_2) : F] = [E : F]$ if $E = F(\alpha_1, \alpha_2)$. Otherwise repeat.

To make the argument rigorous, phrase it as

$$\begin{tikzcd} E \arrow[r, dashed, "\sigma"] \arrow[d, dash] & K \arrow[d, dash] \\ F \arrow[r, "\sigma_0"'] & F_1 \end{tikzcd}$$

E/F, K/F_1 field extensions

$\sigma_0 : F \xrightarrow{\cong} F_1$ isomorphism of fields

# of extension $\sigma : E \to K$ homomorphisms, $\sigma|_F = \sigma_0$ is at most $[E:F]$.

# of extensions is the degree $[E:F]$ in favorable circumstances: $K = E$ is a splitting field of $f(x) \in F[x]$, f is separable (always so in char 0)

E - field, $\sigma \in Aut(E)$ an automorphism

<u>Def</u> $E^\sigma \subset E$ is the fixed field of σ

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

Exercise: E^σ is a subfield of E. E^σ always contains the prime subfield F_0 of E (either $\mathbb{Q}$ or $\mathbb{F}_p$)

If $X \subset Aut(E)$ a subset $\quad E^X := \{ a \in E \mid \sigma(a) = a \ \forall \sigma \in X \}$

$E^X \subset E$ is a subfield, $E^X = \bigcap_{\sigma \in X} E^\sigma$ intersection of subfields.

Let $H = \langle X \rangle$ be the subgroup of $Aut(E)$ generated by X. (smallest subgroup that contains X).

H consists of arbitrary products of el's of X and their inverses.

Then $E^X = E^H$ - subfield, el's fixed by all automorphisms in H.

<u>Note</u> As H gets bigger, E^H becomes smaller

$$H_1 \subset H_2 \Rightarrow \underset{\substack{\uparrow \\ \text{smaller}}}{E^{H_2}} \subset \underset{\substack{\uparrow \\ \text{bigger}}}{E^{H_1}}$$

$H = \{1\}$ smallest $\quad E^{\{1\}} = E$.

Example(s) 1) subgroups of S_3

Index is written on edges.

$$
\begin{tikzcd}
 & & S_3 \arrow[dll, dash, "3"'] \arrow[dl, dash, "3"] \arrow[d, dash, "3"] \arrow[dr, dash, "2"] & \\
\{1,(12)\} \arrow[drr, dash, "2"'] & \{1,(13)\} \arrow[dr, dash, "2"] & \{1,(23)\} \arrow[d, dash, "2"] & \{1,(123),(132)\} = A_3 \arrow[dl, dash, "3"] \\
 & & \{1\} &
\end{tikzcd}
$$

2) subgroups of $C_{12} \simeq (g \mid g^{12}=1) \simeq (\mathbb{Z}/12, +)$

$C_k \subset C_n \quad k \mid n$

$C_n / C_k \simeq C_{n/k}$

$$
\begin{tikzcd}
 & & (g) = C_{12} \arrow[dl, dash, "2"'] \arrow[dr, dash, "3"] & \\
 & (g^2) \arrow[dl, dash, "2"'] \arrow[dr, dash, "3"] & & (g^3) = \{1, g^3, g^6, g^9\} \arrow[dl, dash, "2"] \\
\{1, g^4, g^8\} = (g^4) \arrow[dr, dash, "3"'] & & (g^6) \arrow[dl, dash, "2"] & \\
 & \{1\} & &
\end{tikzcd}
$$

$E/F \rightsquigarrow \mathrm{Gal}(E/F)$.

If $H \subset \mathrm{Gal}(E/F)$, get a subfield E^H, $F \subset E^H \subset E$

If $F \subset K \subset E$ (subfield), have a subgroup $\mathrm{Gal}(E/K)$ - autom of E that fix each element of K

In favorable circumstances get a bijection:

intermediate subfields K $F \subset K \subset E$ $\longleftrightarrow$ subgroups $H \subset \mathrm{Gal}(E/F)$
$H = \mathrm{Gal}(E/K)$, $K = E^H$.

<u>Reminder</u>: (Friedman, Corollary 1.8) Notes on Galois Theory I, p. 5

Let E be an extension field of F, $f(x) \in F[x]$. Let $\alpha_1, \dots, \alpha_n$ be distinct roots of f in E.

$$\{\alpha_1, \dots, \alpha_n\} = \{\alpha : E : f(\alpha) = 0\}. \qquad \alpha_i \neq \alpha_j \quad i \neq j.$$

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

$$\rho : \mathrm{Gal}(E/F) \longrightarrow S_n \qquad S_n \text{ - symmetric group}$$

If, in addition, $E = F(\alpha_1 \dots \alpha_n)$, then ρ is <u>injective</u> and $\mathrm{Gal}(E/F) \subset S_n$. Then also $|\mathrm{Gal}(E/F)| \leq n!$ and the order is a divisor of $n!$

<u>Prop</u> If E/F is a finite extension, then $|\mathrm{Gal}(E/F)|$ is finite,

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

<u>Proof</u> Use our techniques on extending field homomorphisms.

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

$G = \mathrm{Gal}(E/\mathbb{Q}) = \mathrm{Aut}(E)$ $\qquad \{\pm\sqrt{2}, \pm\sqrt{3}\}$ roots of f

$\uparrow$ prime field

$$\begin{array}{cccc} \sqrt{2}, & -\sqrt{2}, & \sqrt{3}, & -\sqrt{3} \\ 1, & 2, & 3, & 4. \end{array}$$ label roots

$G \xrightarrow{\gamma} S_4 =$ permutations (4 roots) is injective, since roots generate F.

what's the image $\mathrm{im}(\gamma)$ in S_4?

$$E \underset{2}{\supset} \mathbb{Q}(\sqrt{2}) \underset{2}{\supset} \mathbb{Q} \qquad \sqrt{3} \notin \mathbb{Q}(\sqrt{2}).$$

$$\begin{tikzcd} E \arrow[r, dashed] \arrow[d, no head] & E \arrow[d, no head] \\ \mathbb{Q}(\sqrt{2}) \arrow[r, "\delta"] \arrow[d, no head] & \mathbb{Q}(\sqrt{2}) \arrow[d, no head] \\ \mathbb{Q} \arrow[r, phantom, "="] & \mathbb{Q} \end{tikzcd}$$

2 automorphisms: $\delta(\sqrt{2}) \mapsto \sqrt{2}$ & $\sqrt{2} \mapsto -\sqrt{2}$

both extend to aut. of E

$\sqrt{3} \notin \mathbb{Q}(\sqrt{2}) \Rightarrow \mathrm{Gal}(E/\mathbb{Q}(\sqrt{2})) \simeq C_2$

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

identity & $\sqrt{3} \mapsto -\sqrt{3}$

$\sqrt{2} \to \sqrt{2}$, $\sqrt{2} \to -\sqrt{2}$ $\quad$ independently $\quad \sqrt{3} \to \sqrt{3}$, $\sqrt{3} \to -\sqrt{3}$

$$\mathrm{im}(\gamma) \simeq \{1, (12)\} \times \{1, (34)\} = C_2 \times C_2$$

$$G \simeq \{1, (12), (34), (12)(34)\} \quad \text{Klein 4 group}$$

This is a special case

$$\begin{tikzcd} & E \arrow[dl, no head] \arrow[dr, no head] & \\ \mathbb{Q}(\sqrt{2}) \arrow[dr, no head] & & \mathbb{Q}(\sqrt{3}) \arrow[dl, no head] \\ & \mathbb{Q} & \end{tikzcd}$$

both fields are fixed by el's of G

$$\mathrm{Gal}(E/\mathbb{Q}) \simeq \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\sqrt{3})/\mathbb{Q})$$
$$\simeq C_2 \times C_2$$

$f = x^4 - 2$ $\quad f \in \mathbb{Q}[x]$ irreducible (Eisenstein)

splitting field $E \subset \mathbb{C}$, roots $\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}$

$G = \mathrm{Gal}(E/\mathbb{Q}) \longrightarrow S_4$ permutations, injective map

subgroup

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

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

Proof $f(x) = c(x-\alpha_1)\dots(x-\alpha_n)$ (separable case; in inseparable case terms are $(x-\alpha_i)^{p^m}$)

distinct $\alpha_1 \dots \alpha_n$

$$\begin{tikzcd} E \arrow[d, dash] & E \arrow[d, dash] \\ F(\alpha_1) \arrow[r, "\sigma"] \arrow[d, dash] & F(\alpha_i) \arrow[d, dash] \\ F \arrow[r, equal] & F \end{tikzcd}$$

σ is an isomorphism. σ extend to an automorphism

$\tau : E \longrightarrow E, \ \tau \in \mathrm{Gal}(E/F)$

Back to example

$G \to S_4$, action on roots is transitive

$$\begin{array}{c} E \\ \mid \ 2, \text{ add } i \\ \mathbb{Q}(\sqrt[4]{2}) \\ \mid \ 4, \text{ add } \sqrt[4]{2} \\ \mathbb{Q} \end{array}$$

Complex conjugation restricts to automorphism of E

$$\begin{tikzcd} & i\sqrt[4]{2} \arrow[dd, leftrightarrow] & \\ \sqrt[4]{2} \arrow[loop left] & & -\sqrt[4]{2} \arrow[loop right] \\ & -i\sqrt[4]{2} & \end{tikzcd}$$

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

$1 \quad 2 \quad 3 \quad 4$

conjugation

$[E : \mathbb{Q}] = 8$,

separable extension,

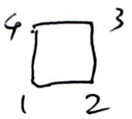
E is splitting field $\Rightarrow$

$|\mathrm{Gal}(E/\mathbb{Q})| = 8$

Exercise: if $H \subset S_4$, $|H| = 8$, $H \ni (2,4)$

& H acts transitively on $\{1,2,3,4\} \Rightarrow$

H is the Dihedral group $D_4 \subset S_4$



$\Downarrow$

$\mathrm{Aut}(E) \cong \mathrm{Gal}(E/\mathbb{Q}) \cong D_4.$

<u>Remark</u> Automorphisms of E do not come from "nice" automorphisms of $\mathbb{C}$

($\mathbb{C}$ has "topology" and has only two symmetries that preserve its topology: identity & complex conjugation).

$\mathbb{Q} \subset E \subset \mathbb{C}$. Forget about $\mathbb{C}$, think of E as extension of $\mathbb{Q}$

degree 8: E is a vect. space $/\mathbb{Q}$ of dimension 8, basis

$$\{\underbrace{1, \sqrt[4]{2}, \sqrt{2}, \sqrt[4]{8}}_{\substack{\uparrow \\ \text{basis for } E \cap \mathbb{R} = \mathbb{Q}(\sqrt[4]{2})}}, i, \sqrt[4]{2}i, \sqrt{2}i, \sqrt[4]{8}i\}$$

+ multiplication

$E \times E \to E$

$a, b \mapsto ab$.

$\boxed{\text{Most symmetries of } E \text{ extend to "bad" symmetries of } \mathbb{C} \text{ that do not respect distance or topology in } \mathbb{C} \text{ and cannot be written down explicitly.}}$

We only use embedding in $\mathbb{C}$ to get partial information about E.

Think of E as an 8-dimensional v.s $/\mathbb{Q}$ with multiplication

$E \simeq \mathbb{Q}^8$ + extra structure (multiplication $\rightsquigarrow$ group G of symmetries).