③ Let K be a field:

Prove $K[x]$ has infinitely many maximal ideals

K field $\Rightarrow$ $K[x]$ is a PID

Ideal is max in PID iff it is generated by an irred. element

Suppose we have finitely many irred. elements $p_1, \dots, p_n$

Consider $q := p_1 \cdots p_n + 1$, $p_i \nmid q$ and q does not factor into a product of p_is, hence we miss irreducibles

④ V = finite dim vector space over $\mathbb{C}$

$\mathbb{C}$-linear maps $A_1, \dots, A_n : V \to V$ s.t. $\forall i, j$

$A_i \circ A_j = A_j \circ A_i$

Show: $\exists$ nonzero vector in V that is simultaneously an eigenvector for each $A_1, \dots, A_n$ (with possibly different eigenvalues)

Pf (Induction on n) ($\mathbb{C}$ alg. closed)

$n=1$ $A_1 : V \to V$ over $\mathbb{C}$ must have a root in $\mathbb{C}$, $\therefore$ characteristic poly of A which is an eigenvalue λ of $A \Rightarrow$ we obtain an eigenvector

Suppose this holds for k linear maps.

To Show: It holds for $k+1$ linear maps

Consider $A_1, \dots, A_{k+1}$ linear maps that pairwise commute

subspace

By I+1, consider $U \subset V$ of vectors that are eigenvectors for all $A_1, \dots, A_k$

$U \neq (0)$ by Induct. Hyp.

Take a basis $\{e_1, \dots, e_r\}$ of U,

and λ_{ij} s.t. $A_i e_j = \lambda_{ij} e_j$

<u>Claim</u> $A_{k+1} \cdot e_j \in U$.

Pf: Each A_i,

$$A_i A_{k+1} e_j = A_{k+1} A_i e_j = A_{k+1} \lambda_{ij} e_j$$

$$= \lambda_{ij} \underbrace{A_{k+1} e_j}_{\text{eigenvector of } \lambda_{ij}}$$

$$B_j := A_{k+1} e_j$$

$$\Rightarrow B_m = \sum_{j=1}^{r} \alpha_{ij} e_j \quad , \quad 1 \leq m \leq r$$

$$\alpha = (\alpha_{ij})$$

$\longrightarrow$ α must have some eigenvalue λ w. eigenvector v

$$\therefore \quad \alpha_{i1} v_1 + \alpha_{i2} v_2 + \cdots + \alpha_{ir} v_r = \lambda v_i$$

$\forall i = 1, \ldots, r$

Consider $d = v_1 e_1 + \cdots + v_r e_r$

<u>Claim</u>: This is an eigenvector for $A_1, \ldots, A_{k+1}$

Note, $d \neq 0$ b/c it is a linear comb. of lin. indep. elts, where at least one $v_i \neq 0$, and

d is an eigenvector for $A_1, \ldots, A_k$ b/c $\{e_1, \ldots, e_r\}$ is a basis of U

<u>WTS</u> d is an eigenvector of A_{k+1}

$$A_{k+1} d =$$

$$= A_{k+1}(v_1 e_1 + \cdots + v_r e_r)$$

$$= v_1 A_{k+1} e_1 + \cdots + v_r A_{k+1} e_r$$

$$= v_1 B_1 + \cdots + v_r B_r$$

$$= v_1 \sum_j \alpha_{j1} e_j + \cdots + v_r \sum_j \alpha_{jr} e_j$$

$$\begin{pmatrix} v_1 \alpha_{11} & v_2 \alpha_{21} & \cdots & v_r \alpha_{r1} \\ v_2 \alpha_{12} & v_2 \alpha_{22} & \cdots & \vdots \\ \vdots & \vdots & & \vdots \\ v_r \alpha_{1r} & v_2 \alpha_{2r} & \cdots & v_r \alpha_{rr} \end{pmatrix}$$

$$= \overbrace{\left(\sum_{j=1}^{r} \alpha_{kj} \cdot v_j \right)}^{\lambda v_1} e_1 + \cdots + \overbrace{\left(\sum_{j=1}^{r} \alpha_{rj} v_j \right)}^{\lambda v_r} e_r$$

$$= \lambda v_1 e_1 + \cdots + \lambda v_r e_r$$

$$= \lambda \underbrace{(v_1 e_1 + \cdots + v_r e_r)}_{\text{eigenvector of all } A_1, \ldots, A_{k+1}}$$

---

(5) R comm. ring

$I, J \subseteq R$ ideals

$\varphi : R \to R/I \otimes_R R/J$ be the function def.

by $\varphi(r) = r(\bar{1} \otimes \bar{1})$ $\forall r \in R$

(a) φ is a surjective R-mod hom

φ is well-def ✓

φ surjective: If $\bar{a} \otimes \bar{b} \in R/I \otimes_R R/J$,

note $\varphi(ab) = ab(\bar{1}\otimes\bar{1})$
$= a(b\cdot\bar{1}\otimes\bar{1}) = a(\bar{1}\otimes\bar{b})$
$= \bar{a}\otimes\bar{b}$

<u>R-mod hom</u>

$$\varphi(r+s) = (r+s)(\bar{1}\otimes\bar{1})$$
$$= (\bar{r}+\bar{s})\otimes\bar{1} = \bar{r}\otimes\bar{1} + \bar{s}\otimes\bar{1}$$
$$= r(\bar{1}\otimes\bar{1}) + s(\bar{1}\otimes\bar{1})$$
$$= \varphi(r) + \varphi(s)$$

$$\varphi(r\cdot s) = rs(\bar{1}\otimes\bar{1}) = r\left(s(\bar{1}\otimes\bar{1})\right)$$
$$= r\varphi(s)$$

(b) <u>$\ker\varphi = I + J$</u>

$$\varphi : R \to R/I \otimes_R R/J$$

$$\begin{tikzcd}
R/I \times R/J \arrow[rr, "f"] \arrow[dr, "\otimes"'] & \circlearrowleft & R/_{I+J} \\
& R/I \otimes_R R/J \arrow[ur, "\bar{f}"'] &
\end{tikzcd}$$

$f(\bar{r},\bar{s}) = \overline{rs}$

$r \in \ker\varphi \Rightarrow \varphi(r) = 0 \in R/I \otimes_R R/J$

$\Rightarrow \underbrace{\bar{f}(\varphi(r))}_{\bar{r}} = 0 \quad \Big| \Rightarrow r \in I + J$

$\underline{\ker\varphi \subseteq I + J}$

$\underline{I + J \subseteq \ker\varphi}$

$a \in I,\ b \in J$

$\varphi(a+b) = (a+b)(\bar{1} \otimes \bar{1})$

$= \bar{a} \otimes \bar{1} + \bar{b} \otimes \bar{1} = \bar{0}$

6. R comm. ring

P, F left R-mods

$\mathrm{Hom}_R(P,F) = \{ f : P \to F \mid f \text{ R-mod hom} \}$

(a) $\forall r \in R,\ f \in \mathrm{Hom}_R(P,F)$

<u>Show</u> $rf : P \to F$ is an R-mod hom
$x \mapsto f(rx)$

i.e., $(rf)(x) = f(rx)$

Pf $(rf)(x+y) = f(r(x+y))$

$= f(rx+ry) = f(rx) + f(ry)$

$s \in R$ $= (rf)(x) + (rf)(y)$

$(rf)(s \cdot x) = f(r \cdot sx) = f(srx)$

$= sf(rx) = s(rf)(x)$

$\mathrm{Hom}_R(P,F)$ is well-dfy R-mod

- $\mathrm{Hom}_R(P,F)$ abel gp. w. function addition,

- module action

$r(f+g) \overset{?}{=} rf + rg$

$r(f+g)(x) = r(f(x)+g(x))$

$= rf(x) + rg(x)$

$(r+s)f(x) = rf(x) + sf(x)$

$r(sf(x)) = (rs)f(x) = .$

$1 \cdot f(x) = f(x)$

(b) P, F finitely gen. as R-mods.

P projective, F free R-mod

Prove: $\mathrm{Hom}_R(P, F)$ is a projective R-mod

$P = \langle a_1, \ldots, a_n \rangle_R$

$F = \langle b_1, \ldots, b_m \rangle_R$

wlog, make it to a basis b/c F is free

P projective $\Rightarrow$ $P \oplus Q$ free

Take $\mathrm{Hom}_R(P \oplus Q, F) \cong \mathrm{Hom}_R(P, F) \oplus \mathrm{Hom}_R(Q, F)$

P f.g.

$P \oplus Q$ free $\Rightarrow$ $P \oplus Q \underset{\wedge}{\overset{\text{f.g.}}{\cong}} \bigoplus_{i \in I} R$ $\quad$ I finite

F free $\Rightarrow$ $F \cong \bigoplus_{j \in J} R$ $\quad$ $J = \{1, \ldots, m\}$

$\Rightarrow \mathrm{Hom}_R(P \oplus Q, F) \cong \bigoplus_{\substack{i \in I \\ j \in J}} R$ free

$\cong$

$\mathrm{Hom}_R(P,F) \oplus \mathrm{Hom}_R(Q,F)$ Hung IV.4.7

7 $\alpha = \sqrt{1+\sqrt{2}} \in \mathbb{R}$

a What is the irred polyn of α over $\mathbb{Q}$?

$$f = \left(x - \sqrt{1+\sqrt{2}}\right)\left(x + \sqrt{1+\sqrt{2}}\right) \cdot \left(x - \sqrt{1-\sqrt{2}}\right)\left(x + \sqrt{1-\sqrt{2}}\right)$$

roots r_1, r_2, r_3, r_4 not in $\mathbb{Q}$

$$f = x^4 - 2x^2 - 1$$

Note, $f(x+1)$ irred by Einsenstein

b Prove $\mathbb{Q}(\alpha)$ is <u>not</u> sp. field over $\mathbb{Q}$ of any polyn. in $\mathbb{Q}[x]$

Suppose it is, take $\left(\sqrt{1+\sqrt{2}}\right)\left(\sqrt{1-\sqrt{2}}\right) = i$

but $\mathbb{Q}(\alpha) \subset \mathbb{R}$ ↯

(8) $f = x^3 - 2 \in \mathbb{Q}[x]$, $g = x^2 - 2 \in \mathbb{Q}[x]$

K, L, M subfields of $\mathbb{C}$ st. K is the splitting field of f, L is the sp. f. of g, and M is sp. fld. of fg.

(a) Construct an automorphism $\beta \in \mathrm{Gal}(K/\mathbb{Q})$ st. $\beta(\sqrt[3]{2}) = \omega\sqrt[3]{2}$

$\beta(\omega) = \omega^2$

$\omega = e^{\frac{2\pi i}{3}} = -\frac{1}{2} + \frac{\sqrt{-3}}{2}$

Roots of $f = x^3 - 2$: $\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$

Compute K

$\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset K = \mathbb{Q}(\sqrt[3]{2})(\omega)$

$\frac{\omega\sqrt[3]{2}}{\sqrt[3]{2}} = \omega \in K$

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

$\Rightarrow [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$

$[K : \mathbb{Q}(\sqrt[3]{2})] = 2$

$\Longrightarrow [K : \mathbb{Q}] = 6$

Take a basis of K:

$$\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2, \omega, \omega\sqrt[3]{2}, \omega(\sqrt[3]{2})^2\}$$

Suppose $\beta(\sqrt[3]{2}) = \omega\sqrt[3]{2}$

$\beta(\omega) = \omega^2$

β again

$$\beta(1) = 1 \longrightarrow 1$$

$$\beta(\sqrt[3]{2}) = \omega\sqrt[3]{2} \longrightarrow \sqrt[3]{2}$$

$$\beta(\omega) = \omega^2 \longrightarrow \omega$$

$$\beta((\sqrt[3]{2})^2) = \omega^2\sqrt[3]{4} \longrightarrow (\sqrt[3]{2})^2$$

$$\beta(\omega\sqrt[3]{2}) = \sqrt[3]{2} \longrightarrow \omega\sqrt[3]{2}$$

$$\beta(\omega\sqrt[3]{4}) = \sqrt[3]{4} \longrightarrow \omega\sqrt[3]{4}$$

(b) What is the order of β?
what is the fixed field of the
subgroup generated by β?

$|\beta| = 2$

β keeps 1, $\omega^2\sqrt[3]{2}$, $\omega\sqrt[3]{4}$ fixed,

so span is

$\langle 1, \omega^2\sqrt[3]{2}, \omega\sqrt[3]{4} \rangle$

$(\omega^2\sqrt[3]{2})^2 = \omega^4\sqrt[3]{4}$

$= \omega\sqrt[3]{4}$

as a fixed field $\mathbb{Q}(\omega\sqrt[3]{4})$

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

(c) Determine $[M:\mathbb{Q}]$

M, split. fld of fg

<u>Show</u> $\sqrt{2} \notin K$

$\mathbb{Q}(\sqrt{2}) \neq \mathbb{Q}(\omega)$

$\Rightarrow \mathbb{Q}(\sqrt{2}) \not\subseteq K$

$\Rightarrow x^2-2$ is irred over K

so

$[M:K]=2$

Fund. Theor. of Gal. Theory

$|\mathrm{Gal}(K/\mathbb{Q})| = 6 \Rightarrow \exists!$ subgp. of order 3

Such subgp must correspond to a unique subfield of degree 2

$\mathbb{Q}(\omega)$ is our guy

$\Rightarrow [M:\mathbb{Q}] = 12$

(d) Construct an element $\rho \in Gal(M/\mathbb{Q})$ that has order 6, and determine its action on the roots of fg

ρ must on a root whose fixed field has deg. 3

Try: ω $\sqrt[3]{2}$

$\sqrt{2} \longmapsto -\sqrt{2}$

$\sqrt[3]{2} \longmapsto \omega\sqrt[3]{2}$

$\omega \longmapsto \omega$

$\Rightarrow \rho$ has order 6

Action on roots of fg

$$1 \mapsto 1$$

$$\omega \mapsto \omega$$

$$\omega^2 \mapsto \omega^2$$

$$\sqrt{2} \mapsto -\sqrt{2} \mapsto \sqrt{2}$$

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

$$\sqrt[3]{4} \mapsto \omega^2\sqrt[3]{4} \mapsto \omega\sqrt[3]{4} \mapsto \sqrt[3]{4}$$

$$\sqrt[3]{2}\sqrt{2} \mapsto -\omega\sqrt[3]{2}\sqrt{2} \mapsto \omega^2\sqrt[3]{2}\sqrt{2}$$
$$\mapsto -\sqrt[3]{2}\sqrt{2} \mapsto \omega\sqrt[3]{2}\sqrt{2}$$
$$\mapsto -\omega^2\sqrt[3]{2}\sqrt{2} \mapsto \sqrt[3]{2}\sqrt{2}$$

$$\sqrt[3]{4}\sqrt{2}$$

$$\mapsto -\omega^2\sqrt[3]{4}\sqrt{2} \mapsto \omega\sqrt[3]{4}\sqrt{2} \mapsto -\sqrt[3]{4}\sqrt{2}$$
$$\mapsto \omega\sqrt[3]{4}\sqrt{2} \mapsto -\omega^2\sqrt[3]{4}\sqrt{2} \mapsto \sqrt[3]{4}\sqrt{2}$$

(e) What is fixed field of sbgp generated by ρ?

anything fixed is

span $\{\omega, \omega^3\}$

fixed field: $\mathbb{Q}(\omega)$

---

check!

finite fields, cyclotomic polys