中間試験返却の前に、

特別演習 (答案提出):

$x = \sqrt{10+\sqrt{2}} \in \overline{\mathbb{Q}}$ **について、**

(1) x **の** $\mathbb{Q}$ **上の最小多項式**
$f(X) := \mathrm{Irr}(x;\mathbb{Q})(X) \in \mathbb{Q}[X]$ **を求めよ。**

(2) x **の** $\mathbb{Q}$ **上の共役をすべて挙げよ。**

(3) $K := \mathbb{Q}(x)$ **の** $\mathbb{Q}$ **上の正規閉包** $\widetilde{K}$**、**
及びその拡大次数 $[\widetilde{K}:\mathbb{Q}]$ **を求めよ。**

中間試験総評:

- **丁寧に書け**
  (答案は人に読まれる／読ませるもの)
- **日本語として意味の通るように書け**
  (答案は数式交じりの文章である)
- **論理の急所をしっかり押さえて書け**
  (突っ込みに答えることを書いておく)

体の拡大の理論としての Galois 理論

体拡大 L/K の様子を、

自己同型群 $\mathrm{Aut}(L/K)$ で統制する

$$\boxed{\begin{array}{c}\textbf{Galois 理論の基本定理}\\ \| \\ \textbf{中間体と部分群との対応}\end{array}}$$

有限次代数拡大の基本的な不等式 (再掲)

L/K: 有限次 (代数) 拡大

$K \subset L \subset \Omega$: 代数閉体

$$\#\mathrm{Aut}(L/K) \leq \#\mathrm{Emb}_K(L,\Omega) \leq [L:K]$$

左の等号 $\iff L/K$: 正規

右の等号 $\iff L/K$: 分離

$\mathrm{Aut}(L/K)$ が望む限り大きくなるのは、
L/K が**正規**かつ**分離的**のとき

体の拡大の理論としての Galois 理論

“Galois 拡大” とは、

“$\mathrm{Aut}(L/K)$ が充分大きく、
体拡大 L/K を統制できる拡大”

実際の所、

L/K が正規かつ分離的、

即ち、$\#\mathrm{Aut}(L/K) = [L:K]$ であることが、

Galois 理論 (中間体と部分群との対応)
が機能するのに重要

体の拡大の理論としての Galois 理論

L/K : **体の拡大**

$$G := \mathrm{Aut}(L/K) = \{\sigma \in \mathrm{Aut}(L) | \sigma|_K = \mathrm{id}\}$$

- $H \subset G$: **部分群に対し、**
  $L^H := \{x \in L \big| \forall \sigma \in H : \sigma(x) = x\}$
  : H **の固定体 (fixed field)**

- M : L/K **の中間体に対し、**
  $\mathrm{Aut}(L/M) = \{\sigma \in G | \forall x \in M : \sigma(x) = x\}$
  : L **の** M **上の自己同型群**

体の拡大の理論としての Galois 理論

自明に

$$\mathrm{Aut}(L/L^H) \supset H, \quad L^{\mathrm{Aut}(L/M)} \supset M$$

ここで $=$ が成り立つか？

一般には成り立たないが、Galois 拡大なら OK

体の拡大の理論としての Galois 理論

自明に

$$\mathrm{Aut}(L/L^H) \supset H, \quad L^{\mathrm{Aut}(L/M)} \supset M$$

ここで $=$ が成り立つか ?

一般には成り立たないが、Galois 拡大なら OK

体の有限次拡大 L/K が Galois 拡大

$$\Updownarrow$$

$$L^{\mathrm{Aut}(L/K)} = K$$

$$\Updownarrow$$

$$\#\mathrm{Aut}(L/K) = [L:K]$$

$$\Updownarrow$$

L/K **: 正規拡大 かつ 分離拡大**

この時、$\mathrm{Aut}(L/K) = \mathrm{Gal}(L/K)$ **と書き、**
L/K **の Galois 群 と呼ぶ。**

Galois 理論の基本定理

L/K: **Galois 拡大、**$G := \mathrm{Gal}(L/K)$: **Galois 群**

$\mathcal{H}_G := \{H | G$ **の部分群**$\}$

$\mathcal{M}_{L/K} := \{M \big| L/K$ **の中間体**$\}$

$$\begin{array}{ccc} & \Phi & \\ M & \longmapsto & \mathrm{Aut}(L/M) \\ & \longrightarrow & \\ \mathcal{M}_{L/K} & & \mathcal{H}_G \\ & \longleftarrow & \\ L^H & \longleftarrow\!\shortmid & H \\ & \Psi & \end{array}$$

Galois 理論の基本定理

- Φ, Ψ : **共に全単射で、互いに逆写像**
  ($\Phi \circ \Psi = \mathrm{id}_{\mathcal{H}_G}, \Psi \circ \Phi = \mathrm{id}_{\mathcal{M}_{L/K}}$**)**
- Φ, Ψ : **共に包含に関して順序逆同型**
  ($H_i \leftrightsquigarrow M_i$ **のとき、**$H_1 \subset H_2 \Leftrightarrow M_1 \supset M_2$**)**

"中間体と部分群とが一対一対応"

Galois 対応
(Galois correspondence)