

2022 年度 後期 定期試験 (問題兼 解答用紙)

開講学部	評点 1	評点 2	評点 3	評点 4
理工学部				

評点

問題枚数	両面印刷	別紙解答用紙	試験時間	試験科目名		クラス	出題者
2/2	有	なし	80分	代数学 6 <small>金曜 2 時間, 教科書: Original §10 ~ §15</small>		A, B	大西 良博
持込許可物件	所属学部	所属学科	学年	学籍番号 (9 桁)		氏名	
なし	理工学部	数学科	年				

注意 1. 最終的な答に至る途中の説明をできるだけ詳しく書くこと。最終結果だけでは得点できない。
 注意 3. 試験場の静粛を保つために、退出は開始 60 分後の時点の一回限りとする。

注意 2. 学生証, 記名用のペン, 鉛筆またはシャープペンシル, 消しゴム以外は机の上に置かないこと。

1 (10 点) 拡大 $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$ を単純拡大として生成する元を 1 つ求めよ。但し i は虚数単位である。

3 (10 点) 拡大次数が 2 である拡大を 2 次拡大 といふ。次の事を示せ。

- (1) 2 次拡大は正規拡大である。
- (2) 体の拡大列 $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$ において, $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ はともに正規拡大であるが, $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ は正規拡大ではない。

2 (15 点) 次の多項式 $f(x) \in \mathbb{Q}[x]$ の \mathbb{Q} 上で可能な限り因数分解し, $f(x)$ の最小分解体とその \mathbb{Q} 上の拡大次数を求めよ。最小分解体はできるだけ簡潔な表示を求めよ。

- (1) $f(x) = x^4 - 5x^2 + 6$.
- (2) $f(x) = (x^2 + 3)(x^2 + x + 1)$.
- (3) $f(x) = x^4 + 3x^2 + 4$.

4 (10 点) 3 つの体からなる代数的拡大の列 $L/M/K$ において L/K は正規拡大であるとする。このとき L/M も正規拡大であることを示せ。

(Hint : 任意の $\alpha \in L$ について $\text{irr}(\alpha, M, x) \mid \text{irr}(\alpha, K, x)$ であることを利用する。)

学籍番号 (9桁)	氏名

5 (15点) 次の代数的拡大は正規であるか否かを理由を付して答へよ.
但し i は虚数単位, $\omega = \frac{-1+\sqrt{3}i}{2}$ とする.

- (1) $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ (2) $\mathbb{Q}(\sqrt{3}+\sqrt{5})/\mathbb{Q}$
(3) $\mathbb{Q}(\sqrt{3}\omega, \sqrt[3]{5})/\mathbb{Q}$ (4) $\mathbb{Q}(\sqrt[3]{3}i)/\mathbb{Q}$

6 (10点) t を不定元とする. 次の拡大は

(a) 正規拡大であるか否か, また (b) 分離拡大であるか否か,
それぞれ理由を付けて答へよ.

- (1) $\mathbb{F}_5(t)/\mathbb{F}_5(t^5)$ (2) $\mathbb{F}_5(t)/\mathbb{F}_5(t^4)$ (3) $\mathbb{F}_5(t)/\mathbb{F}_5(t^3)$

学籍番号 (9桁)	氏名

7 (10点) p を素数, $f(x) = x^p - x - 1 \in \mathbb{F}_p[x]$ とする.

- (1) $f(x) = 0$ の 1 つの根を α とせよ. このとき, $\text{Aut } \mathbb{F}_p(\alpha)/\mathbb{F}_p$ は $\alpha \mapsto \alpha + r$ ($r = 0, 1, \dots, p-1$) で尽されることを示せ.
- (2) 多項式 $f(x)$ は \mathbb{F}_p 上既約であること, および $\mathbb{F}_p(\alpha)/\mathbb{F}_p$ が Galois 拡大であることを示せ.

8 (10点) $\zeta = \exp(2\pi i/7)$ とおき, $L = \mathbb{Q}(\zeta)$, $\alpha = \zeta + \zeta^{-1}$ とする.

次の問に答へよ.

- (1) $\text{irr}(\zeta, \mathbb{Q}, x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ であることを示せ.
(Hint: (右辺) $= \frac{x^7-1}{x-1}$. $x = y+1$ とし, y の多項式として Eisenstein の判定法.)
- (2) $\sigma: \zeta \mapsto \zeta^3$ は L の \mathbb{Q} 上の自己同型を与へることを示せ. また, それが $\mathbb{Q}(\alpha)$ の自己同型を与へることを示せ.
- (3) $\text{irr}(\alpha, \mathbb{Q}, x) = x^3 + x^2 - 2x - 1$ であることを示せ.
- (4) $[L:\mathbb{Q}(\alpha)]$ および $[\mathbb{Q}(\alpha):\mathbb{Q}]$ はいくつか.
- (5) $\sigma(\alpha)$ を α の有理式で書け.

9 (10 点) 以下 i は虚数単位を表す. $\alpha = i\sqrt{5+\sqrt{2}}$, $\beta = i\sqrt{5-\sqrt{2}}$, $L = \mathbb{Q}(\alpha, \beta)$ とおく. もちろん $\pm\alpha$ と $\pm\beta$ は \mathbb{Q} 上共役である. このとき

$$\sigma : \alpha \mapsto \beta, \beta \mapsto -\alpha;$$

$$\tau : \alpha \mapsto -\alpha, \beta \mapsto \beta$$

はともに L の \mathbb{Q} 上の自己同型であることは既知として, 以下の間に答へよ.

- (1) $[L:\mathbb{Q}]$ を求めよ.
- (2) L/\mathbb{Q} が正規拡大 (従つて Galois 拡大) であることを示せ.
- (3) $\sigma^2, \sigma^3, \sigma^4, \tau^2, \sigma\tau, \sigma^2\tau, \tau\sigma$ を求め, 上の様に記せ.
- (4) $\text{Gal}(L/\mathbb{Q})$ を σ, τ で記述せよ.
- (5) $\text{Gal}(L/\mathbb{Q})$ のすべての部分群とそれらに対応する L/\mathbb{Q} の中間体を求め, 双方を互ひに対応する Hasse 図で記述せよ.

記号

\mathbb{N} … 自然数全体, \mathbb{Z} … 整数全体のなす環, \mathbb{Q} … 有理数全体のなす体,
 \mathbb{R} … 実数全体のなす体, \mathbb{C} … 複素数全体のなす体, i … 虚数単位, $\omega = \frac{-1+\sqrt{-3}}{2}$.

既習事項のまとめ

- (1) 体 L の部分集合 K が L の演算に関して体であるとき, K を L の 部分体, あるいは L は K の 拡大 といひ, この状況を L/K と記す. このとき L は K 上の vector 空間 である.
- (2) 体の拡大 L/K に対して K 上の vector 空間としての L の次元を L/K の 拡大次数 と呼び $[L:K]$ で表す. 3 つの体 $K \subset M \subset L$ について $[L:K] = [L:M][M:K]$ である. より詳しく, $\{\beta_j\}$ が L/M の基底で, $\{\alpha_i\}$ が M/K の基底のとき, $\{\alpha_i\beta_j\}$ が L/K の基底をなす.
- (3) 体の拡大 L/K について, 任意の $\alpha \in L$ がある $f(x) \in K[x]$ の根であるとき, L/K を 代数的拡大 と呼ぶ.
- (4) 体の拡大 L/K について, $[L:K] < \infty$ のとき, これを 有限次拡大 と呼ぶ.
- (5) 体 K が体 M の部分体で, M が体 L の部分体であるとき, M を L/K の 中間体 と呼ぶ.
- (6) 体 L とその部分体 K および $\alpha_1, \dots, \alpha_n \in L$ に対し, K のすべての元と $\alpha_1, \dots, \alpha_n$ をすべてを含む最小の体を $K(\alpha_1, \dots, \alpha_n)$ と記す. これは K に係数をもつ様な $\alpha_1, \dots, \alpha_n$ の有理式の全体に他ならない.
- (7) ある体 L がその部分体 K と $\alpha \in L$ によつて, 上の記法で $L = K(\alpha)$ と書けるとき, L は K の 単純拡大 であるといはれる.
- (8) 2 つの部分体の共通部分は再び体であるから, どんな体 K についても, それに含まれる最小の体が存在する. それを 素体 と呼ぶ. 素体は有理数体 \mathbb{Q} か p 元体 $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (p は素数) に同型である.
- (9) 体 K の積に関する単位元 1 をいくつか加へて 0 になるとき, その最小の個数は K の 標数 といはれ, それは素数である. 1 をいくつか加へても 0 にならない場合は, 標数は 0 であるといふ. K の標数を $\text{char } K$ と記す. 前者の場合は素体が \mathbb{F}_p であり, 後者の場合の素体は \mathbb{Q} である.
- (10) 拡大 L/K と $\alpha \in L$ について, α を根とし, 最高次係数が 1 であり, 次数が最小な多項式 $f(x) = K[x]$ が唯一つ存在し, それを α の 最小多項式 と呼んで $\text{irr}(\alpha, K, x)$ で表す.
- (11) 拡大 L/K と中間体 M_1, M_2 について, M_1 と M_2 を含む最小の部分体を M_1M_2 または M_2M_1 と書いて, M_1 と M_2 の 合成体 と呼ぶ; また, 拡大 M_1M_2/K を拡大 M_2/K の M_1 による 持ち上げ と呼ぶ.
- (12) 体 K を含む体 Ω 上に代数的拡大が存在しないとき, Ω は 代数的閉体 といはれ, さらにもし, Ω/K が代数的拡大であるならば Ω は K の 代数的閉包 といはれる. 任意の体 K に対し, その代数的閉包が存在し, すべて同型である. それを一般に \bar{K} と記す.
- (13) 体 K 上代数的な 2 元 α, α' に対して, 次の 2 つの主張は同値であり, これらが成り立つとき, 2 元 α, α' は K 上で 共役 であるといはれる.
 - (1) $\text{irr}(\alpha, K, x) = \text{irr}(\alpha', K, x)$.
 - (2) K 上の同型 $\sigma: K(\alpha) \rightarrow K(\alpha')$ で $\alpha^\sigma = \alpha'$ となるものがある.
- (14) 多項式 $f(x) \in K[x]$ のすべての根で K 上生成される様な体を $f(x)$ の 最小分解体 といふ.
- (15) 拡大 L/K が, どんな既約多項式 $f(x) \in K[x]$ も L 内に 1 つ根を持てば $f(x)$ は L 上 1 次式のみ積に分解する, という性質を持つとき, L/K は 正規拡大 であるといはれる. 体 K に, 1 つの多項式 $f(x) \in K[x]$ の根の全てを添加してできる拡大は, 正規拡大 である.
- (16) 多項式 $f(x) \in K[x]$ が重根を持たないとき, $f(x)$ は 分離的 であるといはれる. 拡大 L/K において, $\alpha \in L$ が K 上の分離的多項式の根であるとき α は K 上 分離的 であるといはれ, さらに, すべての $\alpha \in L$ が K 上分離的であるとき, L/K を 分離的拡大 と称する.
- (17) あらゆる代数的拡大 L/K が分離的である様な体 K は 完全体 であると呼ばれる. 標数が 0 である体や有限体は完全体である.
- (18) 代数的拡大 L/K について, L から \bar{K} への中への K 上の同型の個数を $[L:K]_s$ と記す. $\text{char } K = p > 0$ のとき, これは p の冪になる. さらに L 内の K 上分離的な元の全体を $K^{s,L}$ と書く. これは K 上分離的な L/K の最大の中間体であり, L/K における K の 分離閉包 と呼ばれる. また $[L:K]_i = [L:K]/[L:K]_s$ と定める.
 $[L:K]_s = [K^{s,L}:K]$, $[L:K]_i = [L:K^{s,L}]$ である.
- (19) 分離的拡大は単純拡大である.
- (20) 正規かつ分離的な代数的拡大を Galois 拡大 と呼ぶ.
- (21) 有限次 Galois 拡大 L/K とその Galois 群 $G = \text{Gal}(L/K)$ について, $\mathcal{F}(L/K)$ を L/K の中間体の全体, $\mathcal{G}(G)$ を G の部分群の全体とせよ. 各 $H \in \mathcal{G}(G)$ に対し $L^H = \{\alpha \in L \mid \alpha^\sigma = \alpha \ (\forall \sigma \in H)\}$, 各 $M \in \mathcal{F}(L/K)$ に対し $G^M = \{\sigma \in G \mid \alpha^\sigma = \alpha \ (\forall \alpha \in M)\}$ と記す. このとき $G^M = \text{Gal}(L/M)$ である.
- (22) Galois の基本定理 ¹
 - (21) の状況下で, $\varphi: H \rightarrow L^H$ は $\mathcal{G}(G)$ から $\mathcal{F}(L/K)$ への包含関係を逆転させる全単射であり, 逆写像は $\varphi^{-1}(M) = G^M$ で与えられる.
- (23) Galois 群が巡回群である様な拡大は, 巡回拡大 と呼ばれる.
- (24) Galois 群が Abel 群である様な拡大は, Abel 拡大 と呼ばれる.
- (25) 体 K 上の Abel 拡大の合成体は K 上の Abel 拡大である.
- (26) 拡大 L/K の部分体 M, M' について M/K と M'/K がともに Galois 拡大であれば, MM'/K も Galois 拡大であつて, $\text{Gal}(MM'/K) \simeq \text{Gal}(M/M) \times \text{Gal}(M'/M)$ が成り立つ. 左辺の σ に対して右辺の $\sigma|_M$ が対応する.