

2021 年度 後期 中間試験 (問題 兼 解答用紙)

開講学部	評点小計
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
2/1	有	なし	80分	代数学 5 <small>月曜 1 時間, 教科書: Original</small> (§§1-9)		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)  $p$  を素数とし,  $K$  は標数  $p$  の体とする. 任意の元  $a, b \in K$  に対し, 次が成り立つことを示せ.

**3.3(3)**

- (1)  $(a + b)^p = a^p + b^p$ .
- (2) 任意の  $n \in \mathbb{N} \cup \{0\}$  について  $(a + b)^{p^n} = a^{p^n} + b^{p^n}$ .

**3** (15 点) 次の体の間の包含関係を Hasse 図で示せ.

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

但し,  $i$  は虚数単位で  $\omega = \frac{-1+\sqrt{3}i}{2}$  で, 最後の括弧内は  $\sqrt[3]{2}$  と  $\sqrt{3}$  と  $i$  の積である. さらに, 隣接する体の間の拡大次数も求め書き入れよ.

**2.9, 5.20** の類題

**2** (15 点)  $f(x) = x^3 + 3x^2 + 2$  は  $\mathbb{F}_5[x]$  の既約多項式である. これの根の 1 つを  $\alpha$  とし  $K = \mathbb{F}_5(\alpha)$  とせよ. このとき,  $K$  における  $\alpha^2 + 1$  の逆数を  $\alpha$  の  $\mathbb{F}_5$  上の 2 次以下の多項式で表せ.

**4.13** の類題

**4** (10 点) 体の拡大  $L/K$  があり,  $M$  をその中間体とせよ.  $\alpha \in L$  が  $K$  上代数的であるとせよ. このとき  $[M(\alpha) : M] \leq [K(\alpha) : K]$  であることを示せ.

**5.21**

5 (10点) 体の拡大  $L/K$  と中間体  $M_1, M_2$  があつて  $[M_1 : K] = m_1$ ,  $[M_2 : K] = m_2$ ,  $\gcd(m_1, m_2) = 1$  とせよ. このとき  $M_1 \cap M_2 = K$  であることを示せ.

5.22

学籍番号 (9桁)	氏名

7 (10点) 代数的拡大  $L/K$  とその、互いに包含関係がない、2つの真の部分体  $M_1, M_2$  で次の様な例を挙げよ. もちろん、説明も付けること. 7.4

(1)  $[M_1 M_2 : M_1] < [M_2 : K]$  で  $[M_1 M_2 : M_1] = [M_2 : M_1 \cap M_2]$ .

(2)  $[M_1 M_2 : M_1] < [M_2 : M_1 \cap M_2]$ .

6 (10点) 2つの体の合成体の  $\mathbb{Q}$  上の基底と  $\mathbb{Q}$  上の拡大次数を求めよ.

(1)  $\mathbb{Q}(\sqrt{2})$  と  $\mathbb{Q}(\sqrt{3})$       (2)  $\mathbb{Q}(\sqrt[3]{5})$  と  $\mathbb{Q}(\sqrt[3]{5}i)$       7.2の類題

8 (10点) 体の同型について、以下の間に答へよ.

(1) 体  $\mathbb{Q}(\sqrt[3]{5})$  の自己同型をすべて求めよ.

(2) 体  $\mathbb{Q}(\sqrt[3]{5})$  から  $\mathbb{C}$  への中への同型をすべて求めよ.

9.1の類題

9 (10点)  $K$  を体,  $\alpha, \beta$  を  $K$  上代数的な元とする.  $\text{irr}(\alpha, K, x) = \text{irr}(\alpha, K(\beta), x) \iff \text{irr}(\beta, K, x) = \text{irr}(\beta, K(\alpha), x)$  を示せ.

9.9(1)

$\mathbb{N}$  … 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.  $\omega = \frac{-1+\sqrt{-3}}{2}$ .

### 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 体の拡大  $L/K$  と記す.
- (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  $[L : K] = [L : M][M : K]$ .
- (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  $K$  に係数をもつ線形  $\alpha_1, \dots, \alpha_n$  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, 後者の場合は素体は  $\mathbb{Q}$  である.
- (10) 拡大  $L/K$  と  $\alpha \in L$  について,  $\alpha$  を根とし, 最高次数が  $1$  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  $\alpha$  の 最小多項式 と呼んで  $\text{tr}(\alpha, K, x)$  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  $M_1 M_2$  または  $M_2 M_1$  と書いて,  $M_1$  と  $M_2$  の 合成体 と呼ぶ. また, 拡大  $M_1 M_2 / M_1$  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  $\Omega$  上に代数的拡大が存在しないとき,  $\Omega$  は 代数的閉体 といはれ, さらにもし,  $\Omega/K$  が代数的拡大であるならば  $\Omega$  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) 多項式  $f(x) \in K[x]$  のすべての根で  $K$  上される様な体を  $f(x)$  の 最小分解体 といふ.
- (14) 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,  $f(x)$  が  $L$  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.
- (15) 正規拡大の “底上げ” や持ち上げは正規拡大である. また  $K$  上の 2 つの正規拡大の合成体はまた  $K$  上の正規拡大である.
- (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  $\alpha$  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) 分離的拡大の持ち上げは分離的拡大である. また  $K$  上の 2 つの分離的拡大の合成体はまた  $K$  上の分離的拡大である.
- (18) 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 と呼ばれる. 標数が  $0$  である体や有限体は完全体である.
- (19) 代数的拡大  $L/K$  について,  $L$  から  $\bar{K}(\cap L)$  への中への  $K$  上の同型の個数を  $[L : K]_s$  と記す. さらに  $[L : K]_s = [L : K]/[L : K]_s$  と記す.  $\text{char } K = p > 0$  のとき, これは  $p$  の冪になる.
- (20) 分離的拡大は単純拡大である.
- (21) 正規かつ分離的な代数的拡大を Galois 拡大 と呼ぶ.
- (22) 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  $L^H = \{\alpha \in L \mid \alpha^g = \alpha \ (\forall g \in H)\}$ , 各  $M \in \mathcal{F}(L/K)$  に対し  $G^M = \{\sigma \in G \mid \sigma^g = \alpha \ (\forall \alpha \in M)\}$  と記す. このとき  $G^M = \text{Gal}(L/M)$  である.
- (23) Galois の基本定理 1  
 (22) 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.
- (24) Galois の基本定理 2  
 (22) の状況下で,  $M \in \mathcal{F}(L/K)$  について次が成り立つ.  
 (1)  $\tau \in \text{Gal}(L/K)$  に対し,  $\tau \text{Gal}(L/M)\tau^{-1} = \text{Gal}(L/M^\tau)$ .  
 (2)  $M$  は  $K$  の Galois 拡大  $\iff \text{Gal}(L/M) \triangleleft \text{Gal}(L/K)$ .  
 (3) (2) の両側が成り立つとき,  $\text{Gal}(M/K) \simeq \text{Gal}(L/K) / \text{Gal}(L/M)$  (群としての同型).
- (25) Galois 群が巡回群である様な拡大は, 巡回拡大 と呼ばれる.
- (26) Galois 群が Abelian 群である様な拡大は, Abelian 拡大 と呼ばれる.
- (27) 体  $K$  上の Abelian 拡大の合成体は  $K$  上の Abelian 拡大である.
- (28) 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,  $\text{Gal}(MM'/K) \simeq \text{Gal}(M/M \cap M') \times \text{Gal}(M'/M \cap M')$  が成り立つ. 左辺の  $\sigma$  に対して右辺の  $\sigma|_M$  が対応する.