

2017 年度 後期 中間試験 (問題 兼 解答用紙)

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 6	<small>大層 4 時間, 教科書: Original</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				

開講学部	表評点	裏評点
理工学部		

評 点

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 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。

注意 3. 試験場の静粛を保つために, 退場は開始 60 分後の時点の一回限りとする。

注意 4. **5a** **5b** は選択問題である。どちらか 1 問選んで解答せよ。

1 (15 点) 拡大 $\mathbb{Q}(\sqrt{2}, \sqrt{5})/\mathbb{Q}$ を単純拡大として生成する元を 1 つ求めよ。

解.

$\alpha = \sqrt{2} + \sqrt{5}$ が答の 1 つ.

なぜなら $\frac{1}{3\alpha} = \sqrt{5} - \sqrt{2} \in \mathbb{Q}(\sqrt{2}, \sqrt{5})$,

ゆえに $\sqrt{5} = \frac{1}{2}(\alpha + \frac{1}{3\alpha}) \in \mathbb{Q}(\sqrt{2}, \sqrt{5})$, $\sqrt{2} = \frac{1}{2}(\alpha - \frac{1}{3\alpha}) \in \mathbb{Q}(\sqrt{2}, \sqrt{5})$.

これより

$\mathbb{Q}(\sqrt{2}, \sqrt{5}) \subset \mathbb{Q}(\sqrt{2} + \sqrt{5})$.

$\mathbb{Q}(\sqrt{2}, \sqrt{5}) \supset \mathbb{Q}(\sqrt{2} + \sqrt{5})$ は明らか.

2 (15 点) 代数的拡大 L/K に対し, $L \supset R \supset K$ なる環 R は体であることを示せ.

解. 代数学 5 の中間試験の解説を参照せよ.

3 (20 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) 有理数体 \mathbb{Q} の拡大列 $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[3]{2})$ において, $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ はともに正規拡大であるが, $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ は正規拡大ではない。

解.

問 11.5

(1) 拡大 L/K を 2 次拡大とする。この拡大の基底を $1, \alpha \in L$ と取れるから, $L = K(\alpha)$ とおける。 $\text{irr}(\alpha, K, x) = x^2 + bx + c$ とすれば, $\alpha = \frac{-b + \sqrt{b^2 - 4c}}{2}$ としてよい。このとき,

α の共役についても $\frac{-b - \sqrt{b^2 - 4c}}{2} = -b - \alpha \in L$ であるから L/K は正規拡大である。

(2) 前半は (1) よりわかる。 $\text{irr}(\sqrt[3]{2}, \mathbb{Q}, x) = x^3 - 2$ であるが, これの根のうち $\sqrt[3]{2}i$, $-\sqrt[3]{2}i$ の 2 つは $\mathbb{Q}(\sqrt[3]{2})$ に属さないから, $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ は正規拡大ではない。

4 (20 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 $\omega = \frac{-1 + \sqrt{-3}}{2}$ で, t は不定元とする。

(1) $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$

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

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

(4) $\mathbb{F}_5(t)/\mathbb{F}_5(t^4)$

略解.

(1) $\sqrt{2}$ と $\sqrt{3}$ の共役 $-\sqrt{2}$ と $-\sqrt{3}$ は $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ の元なので, 正規拡大。

(2) $\sqrt[3]{2}$ の共役 $\sqrt[3]{2}\omega$ と $\sqrt[3]{2}\omega^2$ が $\mathbb{Q}(\sqrt[3]{2})$ の元でないので, 正規拡大でない。

(3) $\sqrt[3]{2}$ の共役 $\sqrt[3]{2}\omega$ と $\sqrt[3]{2}\omega^2$ および ω の共役 ω^2 は $\mathbb{Q}(\sqrt[3]{2}, \omega)$ の元なので, 正規拡大。

(4) $\text{irr}(t, \mathbb{F}_5(t^4), x) = x^4 - t^4$ であるが, $x^4 - t^4 = (x - t)(x - 2t)(x - 3t)(x - 4t)$ で $2t, 3t, 4t \in \mathbb{F}_5(t)$ なので, $\mathbb{F}_5(t)/\mathbb{F}_5(t^4)$ は正規拡大である。

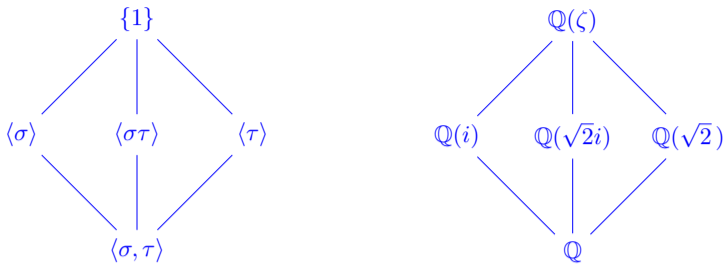
5a (15点) ζ を 1 の原始 8 乗根とせよ. $G = \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ とその部分群, および, それらに対応する $\mathbb{Q}(\zeta)$ の部分体を求めよ.

略解.
 G は

$$\sigma : \sqrt{2} \mapsto -\sqrt{2}, i \mapsto i \text{ および}$$

$$\tau : \sqrt{2} \mapsto \sqrt{2}, i \mapsto -i$$

によつて生成される Abel 群である.



5b (15点) $f(x) = x^3 - 6x + 2$ とおく.

- (1) $f(x) = 0$ の解を $\omega = \frac{-1+\sqrt{3}i}{2}$, 平方根号 $\sqrt{\quad}$, 3 乗根号 $\sqrt[3]{\quad}$, および四則演算のみで表せ.
 (2) $f(x)$ の最小分解体を L とし $K = \mathbb{Q}(\omega)$ とおく. $\text{Gal}(L/K)$ とその部分群, および, そのそれぞれに対応する中間体を図示せよ.

略解. (1) 恒等式 $x^3 + y^3 + z^3 - 3xyz = (x+y+z)(x+\omega y + \omega^2 z)(x + \omega^2 y + \omega z)$ を使ふ.

$$\begin{cases} y^3 + z^3 = 2 \\ -3yz = -6 \end{cases}$$

を解く. これから

$$\begin{cases} y^3 + z^3 = 2 \\ y^3 z^3 = 8 \end{cases}$$

と得るので, y^3 と z^3 は t の 2 次方程式 $t^2 - 2t + 8 = 0$ の 2 根

$$1 \pm \sqrt{-7}$$

である. ここで, y と z は入れ替へてもよいことと, $yz = 2$ を勘案すると

$$(y, z) = \left(\sqrt[3]{1+\sqrt{-7}}, \sqrt[3]{1-\sqrt{-7}} \right),$$

$$\left(\sqrt[3]{1+\sqrt{-7}}\omega, \sqrt[3]{1-\sqrt{-7}}\omega^2 \right),$$

$$\left(\sqrt[3]{1+\sqrt{-7}}\omega^2, \sqrt[3]{1-\sqrt{-7}}\omega \right)$$

ですべての場合を尽してゐる. したがつて求める解は

$$x = -\sqrt[3]{1+\sqrt{-7}} - \sqrt[3]{1-\sqrt{-7}},$$

$$-\sqrt[3]{1+\sqrt{-7}}\omega - \sqrt[3]{1-\sqrt{-7}}\omega^2,$$

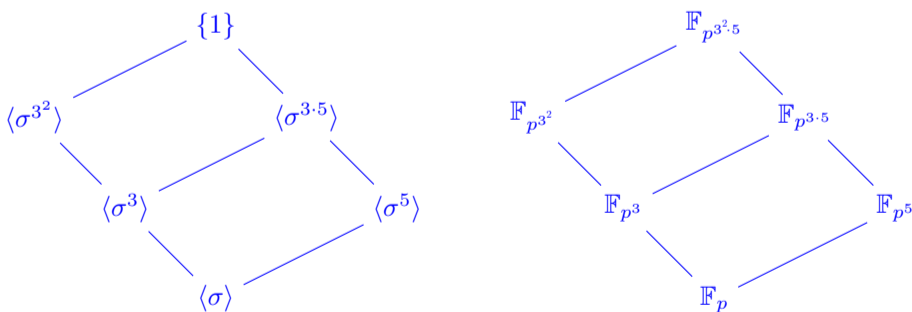
$$-\sqrt[3]{1+\sqrt{-7}}\omega^2 - \sqrt[3]{1-\sqrt{-7}}\omega.$$

(2) Text 16.12 にある図を参照されたい.

6 (15点) p を素数, $n = 3^2 \cdot 5$ とする. $G = \text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ の構造を記せ. また G の部分群とそれらに対応する拡大 $\mathbb{F}_{p^n}/\mathbb{F}_p$ の中間体の様子を図示せよ.

解.

G は位数 $3^2 \cdot 5$ の巡回群であるから, $G = \langle \sigma \rangle$ (但し $\text{ord } \sigma = 3^2 \cdot 5$) とおく.



8 (20点) K を体とし, $a \in K$ について $b = 1 + a^2 \in K$ が K の元の平方ではないとする. このとき $\text{char } K \neq 2$ で $\text{Gal}(K(\sqrt{b+\sqrt{b}})/K)$ は 4 次の巡回群であることを示せ.

(Hint: $\beta = \sqrt{b+\sqrt{b}}$ とおく. $[K(\beta):K] = 4$ が確かめられれば, $\beta^\sigma = -\sqrt{b-\sqrt{b}}$ なる $\text{Gal}(K(\beta)/K)$ の元 σ が存在する. このとき $\beta^{\sigma^2}, \beta^{\sigma^3}$ を調べよ.)

解.

16.11

Hint の記号を使ふ. $a = \sqrt{b-1}$ としてよい. $\beta^2 = b + \sqrt{b}$ で, $(\beta^2)^\sigma = (\beta^\sigma)^2 = b - \sqrt{b}$ なので $\sqrt{b}^\sigma = -\sqrt{b}$. $\beta\beta^\sigma = -\sqrt{b^2-b} = -a\sqrt{b}$ ゆゑ $\beta^\sigma\beta^{\sigma^2} = a\sqrt{b}$. よつて

$$\beta^{\sigma^2} = \frac{a\sqrt{b}}{-\sqrt{b}-\sqrt{b}} = \frac{\sqrt{b+\sqrt{b}}\sqrt{b-\sqrt{b}}}{-\sqrt{b}-\sqrt{b}} = -\sqrt{b+\sqrt{b}} = -\beta,$$

$$\beta^{\sigma^3} = -\beta^\sigma = \sqrt{b-\sqrt{b}},$$

$$\beta^{\sigma^4} = -\beta^{\sigma^2} = \beta$$

$K(\sqrt{b+\sqrt{b}})/K$ が高々 4 次拡大であることは明らかだから, $\text{Gal}(K(\sqrt{b+\sqrt{b}})/K)$ は 4 次の巡回群 $\langle \sigma \rangle$ でなくてはならない.

7 (20点) 下の間に答へよ. 但し

$$\alpha = \sqrt{6+3\sqrt{2}+2\sqrt{3}+2\sqrt{6}}, \quad \alpha_1 = \sqrt{6-3\sqrt{2}+2\sqrt{3}-2\sqrt{6}},$$

$$\alpha_2 = \sqrt{6+3\sqrt{2}-2\sqrt{3}-2\sqrt{6}}, \quad \alpha_3 = \sqrt{6-3\sqrt{2}-2\sqrt{3}+2\sqrt{6}}.$$

- (1) $\alpha\alpha_1 = \sqrt{6}$, $\alpha\alpha_2 = (1+\sqrt{2})\sqrt{6}$, $\alpha\alpha_3 = 3\sqrt{2}+2\sqrt{3}$ であることを示せ.
 (2) $\mathbb{Q}(\alpha)/\mathbb{Q}$ が Galois 拡大であることを示せ.
 (3) $[\mathbb{Q}(\alpha):\mathbb{Q}] = 8$ を既知として, $G = \text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ に属する 2 つの元

$$\sigma : \alpha \mapsto \alpha_1, \quad \tau : \alpha \mapsto \alpha_2$$

を用いて G のすべての元とそれらの演算規則を記述せよ.

- (4) (3) の記号の下で, $\{1, \sigma^2\} < G$ に Galois の基本定理で対応する部分体を求めよ.

略解. (教科書も参照されたい.)

16.10

- (1) 計算だけなので省略.

- (2) まづ $\sqrt{2}, \sqrt{3}, \sqrt{6} \in \mathbb{Q}(\alpha)$ を示せる (略).

よつて (1) により, α の共役 $\pm\alpha, \pm\alpha_1, \pm\alpha_2, \pm\alpha_3$ がすべて α の有理式で $\mathbb{Q}(\alpha)$ の元であることがわかる. よつて $\mathbb{Q}(\alpha)/\mathbb{Q}$ は Galois 拡大である.

- (3) $G = \{1, \sigma, \sigma^2 (= \tau^2), \sigma^3 (= \tau^2\sigma = \sigma\tau^2), \tau, \tau\sigma, \tau^3 (= \tau\sigma^2), \tau\sigma^3\}$. 演算規則は $\sigma\tau = \tau\sigma^3$ だけで定まる (詳細は省略).

- (4) $\sigma^2(\alpha) = \sigma(\alpha_1) = \sigma(\sqrt{6}/\alpha) = -\sqrt{6}/\alpha_1 = -\alpha$ である. これより対応する不変体は $\mathbb{Q}(\alpha^2) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ である. (詳細は略).

★赤字で で囲んだ番号の付いた教科書の問/演習問題は、以後、成績評価に関する report の成果の勘定に入れないので、ご注意下さい。

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. $\omega = \frac{-1 \pm \sqrt{3}i}{2}$.

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 基底 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 をいくつ加へても 0 にならない場合は, 標数は 0 であるといふ. K 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/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 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) 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, といふ性質を持つとき, L/K は 正規拡大 であるといはれる.
- (15) 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.
- (16) 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.
- (17) 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.
- (18) 分離的拡大は単純拡大である.
- (19) 正規かつ分離的な代数的拡大を Galois 拡大 と呼ぶ.
- (20) 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 $L^H = \{\alpha \in L \mid \alpha^g = \alpha (\forall \sigma \in H)\}$, 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.
- (21) Galois の基本定理¹
(20) 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 $\varphi^{-1}(M) = G^M$ で与へられる.
- (22) 3次方程式の解は, 恒等式 $x^3 + y^3 + z^3 - 3xyz = (x+y+z)(x+y+\omega z)(x+y\omega^2+z\omega)$ を使へば, 根号と四則演算のみで記述できる.
- (23) 有限体の元の個数はある素数 p の冪になり, 元の個数が同じ有限体はすべて同型である. また $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m} \iff n|m$.