実施：2018 年 12 月 18 日 (火曜) 14:50-16:20, 4-203 室

A3 size

2018 年度　後期　中間試験　(問題 兼 解答用紙)

開講学部	表評点	裏評点
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 6　火曜 4 時限, 教科書：Original	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 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, 退出は開始 60 分後の時点の一回限りとする.

1 (10 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. **2.10**

$\alpha=\sqrt{2}+\sqrt{5}$ が答の 1 つ.
なぜなら $\dfrac{1}{3\alpha}=\sqrt{5}-\sqrt{2}\in\mathbb{Q}(\sqrt{2},\sqrt{5})$,
ゆゑに $\sqrt{5}=\dfrac{1}{2}\left(\alpha+\dfrac{1}{3\alpha}\right)\in\mathbb{Q}(\sqrt{2},\sqrt{5})$, $\sqrt{2}=\dfrac{1}{2}\left(\alpha-\dfrac{1}{3\alpha}\right)\in\mathbb{Q}(\sqrt{2},\sqrt{5})$.
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 (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 $[M(\alpha):M]\le[K(\alpha):K]$ であることを示せ.

解. **5.19**

$\mathrm{irr}\,(\alpha,M,x)\,|\,\mathrm{irr}\,(\alpha,M,x)$ であるから

$$\deg\mathrm{irr}\,(\alpha,M,x)\le\deg\mathrm{irr}\,(\alpha,K,x).$$

ゆゑに,

$$[M(\alpha):M]=\deg\mathrm{irr}\,(\alpha,M,x)\le\deg\mathrm{irr}\,(\alpha,K,x)\le[K(\alpha):K].$$

3 (15 点)　体の拡大 L/K があり, $\alpha,\beta\in L$ とせよ. $[K(\alpha):K]=m$, $[K(\beta):K]=n$, $\gcd(m,n)=1$ ならば, $[K(\alpha,\beta):K]=mn$ であることを示せ. (**2** を使ふ)

解. **5.21**

$$[K(\alpha,\beta):K]=[K(\alpha,\beta):K(\alpha)][K(\alpha):K]\quad\cdots\cdots①$$

である.
これにより $[K(\alpha,\beta):K]$ は $m=[K(\alpha):K]$ の倍数である. 同様に

$$[K(\alpha,\beta):K]=[K(\alpha,\beta):K(\beta)][K(\beta):K]$$

であるから, これにより $[K(\alpha,\beta):K]$ は $n=[K(\beta):K]$ の倍数である.
$\gcd(m,n)=1$ なので, $[K(\alpha,\beta):K]$ は mn の倍数である. $\cdots\cdots$ ②
ここで **2** の M を $K(\alpha)$ とすれば $[K(\alpha,\beta):K(\alpha)]\le[K(\beta):K]$ だから, 等式 ① と合はせて

$$[K(\alpha,\beta):K]\le[K(\beta):K][K(\alpha):K]=mn.\quad\cdots\cdots③$$

② と ③ より

$$[K(\alpha,\beta):K]=mn$$

でなければならない.

4 (15 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 $\mathbb{Q}\subset\mathbb{Q}(\sqrt{2})\subset\mathbb{Q}(\sqrt[4]{2})$ 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.

解. **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. $\mathrm{irr}\,(\alpha,K,x)=x^2+bx+c$ とすれば, α の共役は $b-\alpha\in L$ 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. $\mathrm{irr}\,(\sqrt[4]{2},\mathbb{Q},x)=x^4-2$ であるが, これの根のうち $\sqrt[4]{2}i$, $-\sqrt[4]{2}i$ の 2 つは $\mathbb{Q}(\sqrt[4]{2})$ に属さないから, $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ は正規拡大ではない.

5 (15 点) 拡大 L/K の 2 元 α, β は K 上代数的であるとせよ. $f(x) = \mathrm{irr}\,(\alpha, K, x)$, $g(x) = \mathrm{irr}\,(\beta, K, x)$ とおく. このとき $f(x)$ が $K(\beta)$ 上で既約でないならば $g(x)$ は $K(\alpha)$ 上で既約でないことを示せ.
(Hint : $[K(\alpha,\beta) : K]$ を考へよ.)

解説 **10.7**
まづ,

$$\begin{aligned}[K(\alpha,\beta) : K] &= [K(\alpha,\beta) : K(\alpha)][K(\alpha) : K] \\ &= [K(\alpha,\beta) : K(\alpha)] \deg f(x) \\ &= \deg \mathrm{irr}\,(\beta, K(\alpha), x) \deg f(x).\end{aligned}$$

同様に

$$\begin{aligned}[K(\alpha,\beta) : K] &= [K(\alpha,\beta) : K(\beta)][K(\beta) : K] \\ &= [K(\alpha,\beta) : K(\beta)] \deg g(x) \\ &= \deg \mathrm{irr}\,(\alpha, K(\beta), x) \deg g(x)\end{aligned}$$

であるから,

$$\deg \mathrm{irr}\,(\beta, K(\alpha), x) \deg f(x) = \deg \mathrm{irr}\,(\alpha, K(\beta), x) \deg g(x) \quad \cdots \quad ①$$

いま, $g(x)$ が $K(\alpha)$ 上既約であるとする. これは $\mathrm{irr}\,(\beta, K(\alpha), x) = g(x)$ であることに同値であるから, ① は

$$\deg g(x) \deg f(x) = \deg \mathrm{irr}\,(\alpha, K(\beta), x) \deg g(x)$$

と書ける. つまり

$$\deg f(x) = \deg \mathrm{irr}\,(\alpha, K(\beta), x)$$

となる. $\mathrm{irr}\,(\alpha, K(\beta), x) \mid f(x)$ であるから

$$f(x) = \mathrm{irr}\,(\alpha, K(\beta), x)$$

でなければならない. つまり $f(x)$ は $K(\beta)$ 上でも既約. これで主張が証明された.

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

(1) $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ (2) $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$
(3) $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ (4) $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$ (5) $\mathbb{F}_5(t)/\mathbb{F}_5(t^4)$

略解. **11.7** はまだ有効とします.
(1) $\sqrt{2}$ の共役 $-\sqrt{2}$ は $\mathbb{Q}(\sqrt{2})$ の元なので, 正規拡大.
(2) $\sqrt{2}$ 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.
(3) $\sqrt[3]{2}$ 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.
(4) $\sqrt[3]{2}$ 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.
(5) $\mathrm{irr}\,(t, \mathbb{F}_5(t^4), x) = x^4 - t^4$ 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.

学籍番号	

7 (5 点) M, M' が代数的拡大 L/K の中間体であるとき, 次のことを示せ. M/K が分離的ならば, MM'/M' も分離的. (即ち, 拡大の分離性は持ち上げによつて保たれる.)
(Hint : 任意の $\alpha \in MM'$ に対し, 有限個の $\beta_1, \cdots, \beta_n \in M$ が存在して, $\alpha \in M'(\beta_1, \cdots, \beta_n)$ となる.)

略解. **12.16** はまだ有効とします.
MM' の任意の元が M' 上に分離的であることを示せばよい.
任意の $\alpha \in MM'$ は, M と M' の有限個の元の有理式であるから,
有限個の $\beta_1, \cdots, \beta_n \in M$ が存在して, $\alpha \in M'(\beta_1, \cdots, \beta_n)$ となる.
仮定により $\beta_1, \cdots, \beta_n$ は K 上分離的.
しかるに

$$\mathrm{irr}\,(\beta_j, M', x) \mid \mathrm{irr}\,(\beta_j, K, x)$$

であるから, $\beta_1, \cdots, \beta_n$ は M 上でも分離的.
M 上分離的な元から生成される体は M 上分離的であるから
$M'(\beta_1, \cdots, \beta_n)/M$ は分離的である.
ゆゑに $\alpha \in M'(\beta_1, \cdots, \beta_n)$ は M 上分離的である.

8 (15 点) 代数的拡大 L/K の 2 つの真の部分体 M_1, M_2 で, 互ひに包含関係がなく, $[M_1M_2 : M_1] < [M_2 : K]$ であり, $[M_1M_2 : M_1] = [M_2 : M_1 \cap M_2]$ となる例を挙げよ.

解説 **7.4**
$K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$, $M_1 = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, $M_2 = \mathbb{Q}(\sqrt{2}, \sqrt{5})$
とすると, $M_1M_2 = L$ になり,

$$[M_1M_2 : M_1] = 2, \quad [M_2 : K] = 4.$$

一方

$$[M_2 : M_1 \cap M_2] = [\mathbb{Q}(\sqrt{2}, \sqrt{5}) : \mathbb{Q}(\sqrt{2})] = 2$$

であるから, これは所望の例である.

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.　$\omega = \frac{-1+\sqrt{3}i}{2}$.

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 $\alpha_1, \cdots, \alpha_n \in L$ に対し, K のすべての元と $\alpha_1, \cdots, \alpha_n$ をすべてを含む最小の体を $K(\alpha_1, \cdots, \alpha_n)$ と記す. これは K に係数をもつ様な $\alpha_1, \cdots, \alpha_n$ 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 $\operatorname{char} K$ 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 1 つ存在し, それを α の 最小多項式 と呼んで $\operatorname{irr}(\alpha, K, x)$ 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 $\overline{K}$ 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 次式のみの積に分解する, 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. 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.
(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 $\overline{K}$ への中への K 上の同型の個数を $[L:K]_s$ と記す. $\operatorname{char} K = p > 0$ 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 $G = \operatorname{Gal}(L/K)$ について, $\mathscr{F}(L/K)$ を L/K の中間体の全体, $\mathscr{G}(G)$ を G の部分群の全体とせよ. 各 $H \in \mathscr{G}(G)$ に対し $L^H = \{\, \alpha \in L \,|\, \alpha^\sigma = \alpha \ (\forall \sigma \in H) \,\}$, 各 $M \in \mathscr{F}(L/K)$ に対し $G^M = \{\, \sigma \in G \,|\, \alpha^\sigma = \alpha \ (\forall \alpha \in M) \,\}$ と記す. このとき $G^M = \operatorname{Gal}(L/M)$ である.
(21) Galois の基本定理 1
(20) の状況下で, $\varphi : H \mapsto L^H$ は $\mathscr{G}(G)$ から $\mathscr{F}(L/K)$ 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 $x^3+y^3+z^3-3xyz = (x+y+z)(x+y\omega+z\omega^2)(x+y\omega^2+z\omega)$ 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 $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m} \iff n|m$. 有限体の拡大は常に Galois 拡大であり, $\operatorname{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ は位数 n の巡回群である.