実施：2020 年 1 月 22 日 (水曜) 13:10-14:40, H-102 室

B4 size

2019 年度　**後期　定期試験**　(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　水曜 3 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．

注意 4. **9a** **9b** は選択問題である．どちらか 1 問選んで解答せよ．

1 (10 点) 拡大 $\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q}$ を単純拡大として生成する元を 1 つ求めよ．

2 (10 点) 体 K 上の代数的な元 α と $\alpha+1$ が K 上共役であれば, $\mathrm{char}\, K \neq 0$ であることを示せ．

(Hint：$f(x) = \mathrm{irr}\,(\alpha, K, x)$ とおくとき, $f(x+1) = \mathrm{irr}\,(\alpha, K, x)$ でもあることを示せ．このことより $\alpha, \alpha+1, \cdots$ のすべてが互ひに共役であることがわかる．)

3 (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) 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．

4 (15 点) 次の多項式 $f(x) \in \mathbb{Q}[x]$ について $f(x)$ の $\mathbb{Q}$ 上の最小分解体 L, および $[L:\mathbb{Q}]$ を求めよ．

(1) $f(x) = x^3 - 8$.

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

(3) $f(x) = x^5 - 1$.

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

学 籍 番 号 (9 桁)	氏 名

学籍番号	

$\boxed{\mathbf{5}}$ (10 点)　拡大 L/K の 2 元 $\alpha,\ \beta$ 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 $K(\beta)$ 上で既約であることと $g(x)$ が $K(\alpha)$ 上で既約であることは同値であることを示せ. (Hint : $[\,K(\alpha,\beta) : K\,]$ を考へよ.)

$\boxed{\mathbf{6}}$ (10 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) $\mathbb{F}_5(t)/\mathbb{F}_5(t^4)$

$\boxed{\mathbf{7}}$ (10 点)　t を不定元とし, $L = \mathbb{F}_5(t)$ とする. $t \in L$ と, 次に挙げる部分体 $K \subset L$ について $\mathrm{irr}\,(t, K, x)$ とその L 上での因数分解を求めよ.

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

$\boxed{\mathbf{8}}$ (15 点)　$L = \mathbb{Q}(\sqrt[3]{2}, \omega)$ (但し $\omega = \frac{-1+\sqrt{-3}}{2}$) と $K = \mathbb{Q}$ について,

(1) L/K が Galois 拡大であることを示せ.

(2) 以下 $G = \mathrm{Gal}(L/K)$ とおく. G の要素をすべて記述せよ.

(3) $M_0 = \mathbb{Q}(\sqrt[3]{2}\,),\ M_1 = \mathbb{Q}(\sqrt[3]{2}\,\omega),\ M_2 = \mathbb{Q}(\sqrt[3]{2}\,\omega^2)$ について $G^{M_0},\ G^{M_1},\ G^{M_2}$ を求めよ.

(4) $\sigma \in G$ を $\sqrt[3]{2} \longmapsto \sqrt[3]{2}\,\omega,\ \omega \longmapsto \omega$ で定まる元とし, H を σ で生成される G の部分群とせよ : $H = \langle\sigma\rangle$.　このとき L^H を求めよ.
(Hint : L/K の基底として $\{\omega, \omega^2, \sqrt[3]{2}\,\omega, \sqrt[3]{2}\,\omega^2, \sqrt[3]{2}^2\omega, \sqrt[3]{2}^2\omega^2\}$ が取れることを利用せよ.)

(5) $\tau \in G$ を $\sqrt[3]{2} \longmapsto \sqrt[3]{2},\ \omega \longmapsto \omega^2$ で定まる元とし, D を τ で生成される G の部分群とせよ : $D = \langle\tau\rangle$.　このとき L^D を求めよ.
(Hint : L/K の基底として $\{1, \sqrt[3]{2}, \sqrt[3]{2}^2, \omega, \sqrt[3]{2}\,\omega, \sqrt[3]{2}^2\omega\}$ が取れることを利用せよ.)

学 籍 番 号 (9 桁)	氏　　名

9a (5 点) $L = \mathbb{Q}\big(\exp(2\pi \boldsymbol{i}/7)\big)$, $\alpha = \exp(2\pi \boldsymbol{i}/7) + \exp(-2\pi \boldsymbol{i}/7)$ とする. 次の問に答へよ.

(1) $\mathrm{irr}\,(\alpha, \mathbb{Q}, x) = x^3 + x^2 - 2x - 1$ であることを示せ.

(2) $[L : \mathbb{Q}(\alpha)]$ および $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ はいくつか.

(3) $\exp(2\pi \boldsymbol{i}/7) \mapsto \exp(4\pi \boldsymbol{i}/7)$ 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.

(4) (3) の $\mathbb{Q}(\alpha)$ の自己同型を σ とおく. α^σ を α の有理式で書け. それを $\varphi(\alpha)$ とするとき, $\alpha^{\sigma^2} = \varphi(\varphi(\alpha))$, $\sigma^3 = \mathrm{id}$ であることを示せ.

(5) 拡大 $\mathbb{Q}(\alpha)/\mathbb{Q}$ が Galois 拡大であり, $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ は位数 3 の巡回群であることを示せ.

9b (5 点) p を素数, $n = 2^2 \cdot 3^3 \cdot 5$ とする. $G = \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ を求め, その構造を記せ. G の部分群とそれらに対応する拡大 $\mathbb{F}_{p^n}/\mathbb{F}_p$ の中間体を求めよ.

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.　$\omega = \frac{-1+\sqrt{3}i}{2}$.

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<u>部分体</u>, あるいは L は K の拡大といひ, この状況を<u>体の拡大</u> 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<u>代数的拡大</u>と呼ぶ.

(4) 体の拡大 L/K について, $[L:K] < \infty$ のとき, これを<u>有限次拡大</u>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<u>中間体</u>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<u>単純拡大</u>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<u>素体</u>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<u>標数</u>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<u>最小多項式</u>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<u>合成体</u>と呼ぶ. また, 拡大 M_1M_2/M_1 を拡大 M_2/K の M_1 による<u>持ち上げ</u>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<u>代数的閉体</u>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<u>代数的閉包</u>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) 体 K 上代数的な 2 元 α, α' に対して, 次の 2 つの同値は同値であり, これらが成り立つとき, 2 元 α, α' は K 上で<u>共役</u>であるといはれる.
(1) $\operatorname{irr}(\alpha, K, x) = \operatorname{irr}(\alpha', K, x)$.
(2) K 上の同型 $\sigma : K(\alpha) \to K(\alpha')$ 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 上される様な体を $f(x)$ の<u>最小分解体</u>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, $f(x)$ 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<u>正規拡大</u>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<u>分離的</u>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<u>分離的</u>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<u>分離的拡大</u>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<u>完全体</u>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 $\overline{K}(\supset L)$ への中への K 上の同型の個数を $[L:K]_s$ と記す. さらに $[L:K]_i = [L:K]/[L:K]_s$ と記す. $\operatorname{char} K = p > 0$ のとき, これは p の冪になる.

(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 <u>Galois 拡大</u>と呼ぶ.

(21) 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.

(22) <u>Galois の基本定理 1</u>
(21) 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.

(23) 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.

(24) 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 $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^n} \iff n|m$. 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.