体とガロア理論

ああああ

2025 年 3 月 4 日

目次

0　はじめに

代数学 Ⅲ 体とガロア理論 (桂利行) の勉強ノートを tex で書いていきます．演習問題や証明で少しでもつまったところについてメモを書いていこうと思います．

1　体の理論

■定理 1.5.16　$E^* = \langle\theta\rangle$ から $E = F(\theta)$ となるのはなぜか．$\because$ 明らかに，$E \supset F[\theta]$ である．$0 \in F[\theta]$ かつ，$\theta^i \in F[\theta]$ より，$E \subset F[\theta]$．以上より，$E = F[\theta] = F(\theta)$.

■有限次拡大について　E/F を有限次拡大とする．E を F 上のベクトル空間として見たときの基底を $\{a_1, \cdots, a_n\}$ とすれば，$E = F[a_1, \cdots, a_n] = F(a_1, \cdots, a_n)$ と書ける (当たり前) ．つまり，E/F が有限次拡大なら，$a_i \in E$ が取れて，$E = F(a_1, \cdots, a_n)$ と書ける．

■分離拡大の中間体　$E/K, K/F$ を体の拡大とする．E/F が分離拡大であることの必要十分条件は，$E/K, K/F$ が分離拡大であることである．$\because$ まず，必要性を示す．$\alpha \in E$ の F 上の最小多項式を $p(X)$ とおき，K 上の最小多項式を $q(X)$ とおく．仮定から，p は重解をもたない．$K[X]$ において，$q(X) \mid p(X)$ であるから，q も重解をもたない．K/F のほうは明らか．十分性は命題 1.6.7 .

■定理 1.5.16　s に関する帰納法の $s > 2$ について．

$$E = F(\theta_1, \cdots, \theta_s) \supset F(\theta_1, \cdots, \theta_{s-1}) \supset F$$

であり，$F(\theta_1, \cdots, \theta_{s-1})/F$ は有限次分離拡大であるから，仮定より，$\alpha \in E$ がとれて，$F(\theta_1, \cdots, \theta_{s-1}) = F(\alpha)$ をみたす．よって，$E = F(\alpha, \theta_s)$ となり，$s = 2$ に帰着する．

■F 上の準同型写像 $E \to \bar{E}$　E/F を代数的拡大とする．$\sigma : E \to \bar{E}$ を F 上の準同型写像とする．このときに，$\sigma(E) = E$ とは限らない．常に，$\sigma(E) = E$ となるのは，E/F が正規拡大であるような時のみに限る．

■超越基底の存在について　E/F が代数拡大でないとする．(代数拡大なら，超越基底は空集合とすればいい．) 定理 1.8.4 より，空でない S がとれ，$T = E$ をとれば，$T_0 \subset T$ がとれて，$S \cup T_0$ は超越基底となる．空集合に対して代数的に独立というのが定義されていないように読めたので，代数拡大でないという仮定を入れた．

■代数的拡大の保存　体の拡大 $E \supset K \subset F$ について，K/F は代数的拡大であるとする．任意の $S \subset E$ について，$K(S)/F(S)$ は代数的拡大である．$\because$ 代数的な数全体は体をなすから，K の元と，S の元が F 上代数的であることを言えばよく，これは明らか．

章末問題

(1.1) R を F 上のベクトル空間として見たときの基底を $\{a_1, \cdots, a_n\}$ とおく．n に関する帰納法で示す．$n = 1$ であれば，明らかに $R = F$ となり，R は体となる．$n \geq 2$ のとき，$a_i \notin F$ がとれる．番号を付け替えて，この a_i を a_1 とおく．$\dim_F F(a_1) > 1$ である．R は $F(a_1)$ 上のベクトル空間とし

て見れる．R をこのように見たときの基底を $\{b_1, \cdots, b_m\}$ とおく．定理 1.1.12 と同様の証明により，$m = n/\dim_F F(a_1) < n$ だから，帰納法の仮定より，R は体である．

(1.2) 体から体の環の準同型は零写像でないかぎり単位元を単位元に写す．単位元のみから素体を作ることができるから，$\mathrm{Aut}(E)$ の元は P 上で同型となる．

(1.3) E 上で $X^n - 1$ の根は n 個以下である．すなわち，E^* の元であって，位数が n であるようなものは n 個以下である．よって，E^* は巡回群である．

(1.4)
$$\mathbf{Q}[X]/(X^2 - 2) \simeq \mathbf{Q}[\sqrt{2}] = \mathbf{Q}(\sqrt{2}).$$

(1.5) $\mathbf{R}[X]/(f(X))$ が体であることと，$(f(X))$ が極大イデアルであることは同値であるから，$(f(X))$ が極大イデアルつまり $f(x)$ が $\mathbf{R}$ 上既約であるとき，$\mathbf{R}[X]/(f(X))$ は体となり，そうでないときは体とならない．f が異なる実数解をのみを持つ場合，$\mathbf{R} \oplus \mathbf{R}$ と同型．これは体でない ($1 \oplus 0$ とか．)．実数根が重根である場合，$\mathbf{R}[X]/(f(X))$ は二乗して初めて 0 になる数を添加してできるベクトル空間と同型で，これは体でない．

(1.6) 同様.

(1.7) $1 + \sqrt{-1}$ は $\mathbf{Z}[\sqrt{-1}]$ の素元だから，$\mathbf{Z}[\sqrt{-1}]/(1 + \sqrt{-1})$ は有限位数の整域である．章末 1.1 より，$\mathbf{Z}[\sqrt{-1}]/(1 + \sqrt{-1})$ は体である．位数は 2 であるから，
$$\mathbf{Z}[X]/(1 + \sqrt{-1}) \simeq \mathbf{F}_2.$$

(1.8) F が標数 0 なら，$f(X) - g(X)$ は 0 に等しいから，$f(X) = g(x)$．標数が $p > 0$ なら，$f(X) - g(X) = X^p - X$ などできるので，$f(X) \neq g(X)$ となる場合がある．

(1.9) $p_1, \cdots, p_n$ を相異なる素数する．いま，$\sqrt{p_1}, \cdots, \sqrt{p_n}$ が $\mathbf{Q}$ 上で線形独立であることを示せばいい．もっと言えば，$\mathbf{Q}(\sqrt{p_1}, \cdots, \sqrt{p_n})$ は $1, \sqrt{p_1}, \cdots, \sqrt{p_n}, \sqrt{p_1 p_2}, \cdots, \sqrt{p_1 \cdots p_n}$ で生成されるから，$[\mathbf{Q}(\sqrt{p_1}, \cdots, \sqrt{p_n}) : \mathbf{Q}] = 2^n$ を示せばいい．n についての帰納法で示す．$n = 0, 1$ の時は自明である．$K = \mathbf{Q}(\sqrt{p_1}, \cdots, \sqrt{p_{n-1}})$ とおく．$\sqrt{p_{n+1}} \in K(\sqrt{p_n})$ と仮定する．すると，$a, b \in K$ が取れて，
$$\sqrt{p_{n+1}} = a + b\sqrt{p_n}$$
と書ける．両辺を二乗して，
$$p_{n+1} = a^2 + b^2 p_n + 2ab\sqrt{p_n}.$$
よって，$ab = 0$ を得る．$a = 0$ なら，$b = \sqrt{p_{n+1}}/\sqrt{p_n} = \sqrt{p_n p_{n+1}}/p_n$ となる．つまり，$\sqrt{p_n p_{n+1}} \in K$ を得る．ここで，$p_1, \cdots, p_n$ がそれぞれ無平方かつどの二つも互いに素であるとしても同様の議論が行え，そうすると $\sqrt{p_n p_{n+1}} \in K$ は矛盾する．$b = 0$ なら，$a = \sqrt{p_{n+1}} \in K$ となり，矛盾．以上より，
$$2^{n+1} = [K(\sqrt{p_n}, \sqrt{p_{n+1}}) : K(\sqrt{p_n})][K(\sqrt{p_n}) : K][K : \mathbf{Q}] = [\mathbf{Q}(\sqrt{p_1}, \cdots, \sqrt{p_{n+1}}) : \mathbf{Q}].$$

(1.10)

(1.10.1) 既約.

(1.10.2) $X^3 + X^2 + X + 1 = (X + 1)^3$

(1.10.3) $X^6 - 1 = (X + 1)^2(X^2 + X + 1)^2$

(1.11)

(1.11.1) $X^2+X+1=(X-1)^2$

(1.11.2) $X^3+X+2=(X+1)(X^2-X-1)$

(1.11.3) $X^4+X^3+X+1=(X+1)^4$

(1.12)

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

である．f が $F(\beta)$ 上で既約であることは，$\deg f=[F(\alpha,\beta):F(\beta)]$ であることと同値であり，

$$[F(\alpha,\beta):F(\alpha)]=[F(\alpha,\beta):F(\beta)]\deg g/\deg f$$

だから，$[F(\alpha,\beta):F(\beta)]=\deg g$ つまり，g が $F(\alpha)$ 上で既約であることと同値である．

(1.13) $f\circ g$ の根 α を任意にとる．f が F 上既約であるから，$\deg f=[F(g(\alpha)):F]$．また，$F(\alpha)\supset F(g(\alpha))$ であるから，

$$[F(\alpha):F]=[F(\alpha):F(g(\alpha))][F(g(\alpha)):F]\Longrightarrow \deg f\mid[F(\alpha):F].$$

$[F(\alpha):F]$ は α の F 上の最小多項式の次数であり，$f\circ g$ の既約因子の次数である．

(1.14) 対偶を示す．$a\in K^p$ であるとする．すると，$b\in K$ がとれて，$a=b^p$．

$$X^p-a=X^p-b^p=(X-b)^p$$

となるから，X^p-a は K 上可約である．逆に，X^p-a が F 上で可約であるとする．このとき，$b\in\bar{K}$ がとれて，$X^p-a=(X-b)^p$ と書ける．$(X-b)^i\in K[X]$ $(1\leq i<p)$ だから，

$$(X-b)^i=\sum_{j=0}^{i}\binom{i}{j}X^{i-j}b^j\in K[X].$$

X^{i-1} の係数を計算すれば，$b\in K$ である（ここで，$1\leq i<p$ であることを使っている．）．よって，$a=b^p\in K^p$．

(1.15) D が可換なら，$\mathbf{C}$ は代数的閉包だから，$\mathbf{C}\supset D\supset\mathbf{R}$．$D\simeq\mathbf{R},\mathbf{C}$．次に，$D$ を非可換とする．$a\in D\setminus\mathbf{R}$ をとり，$\mathbf{R}[a]$ を考える．$D\supset\mathbf{R}[a]$ だから，$\mathbf{R}[a]$ は整域で章末 1.1 より，$\mathbf{R}[a]$ は体である．特に，$\mathbf{R}[a]\simeq\mathbf{C}$．このことから，$D\setminus\mathbf{R}$ の元は $\mathbf{R}$ 上二次元である．いま，$u^2=-1$ なる D の元がとれ，$\mathbf{R}[u]=\mathbf{R}+\mathbf{R}u$．また，$v^2=-1$ なる $v\in D\setminus\mathbf{R}[a]$ がとれ，$1,u,v,uv$ は $\mathbf{R}$ 上で線形独立である．実際に，

$$a+bu+cv+duv=0\ (a,b,c,d\in\mathbf{R})$$

と書けたとすると，

$$(a+bu)+(c+du)v=0$$

とみれば，$a+bu=c+du=0$ となり，$a=b=c=d=0$ である．$u+v,uv\in D\setminus\mathbf{R}$ だから，

$$(u+v)^2+a(u+v)+b=0,(uv)^2+c(uv)+d=0\ (a,b,c,d\in\mathbf{R}).$$

$vu=-uv-c$ を得る．$D\neq\mathbf{R}+\mathbf{R}u+\mathbf{R}v+\mathbf{R}uv$ だと仮定する．$w^2=-1$ なる $w\in D\setminus\mathbf{R}[u,v]$ がとれ，$1,u,v,uv,w,uw,vw,uvw$ は $\mathbf{R}$ 上で線形独立である．同様にして，$wu=-uw-e,wv=-vw-f$ $(e,f\in\mathbf{R})$ となり，

$$(uvw)^2+g(uvw)+h=0\ (g,h\in\mathbf{R})$$

を計算すると，$h=-1, c=0, f=-e$ を得る．uwv についても考えると，$e=f=0$ を得る．同様に $z^2=-1$ なる $z\in D$ 対して，$uz=-zu, vz=-zv$．$z=(u+v)/\sqrt{2}$ をとれば，$z^2=-1$ であるが，$vz+zv=-\sqrt{2}$ となり矛盾する．$\therefore D\simeq \mathbf{R}+\mathbf{R}u+\mathbf{R}v+\mathbf{R}uv$．同型写像は，$u\mapsto i, v\mapsto (c/2)i+\sqrt{1-c^2/4}j$．ちなみに，$(uv)^2+c(uv)+1=0$ であるから，$c^2-4<0$.

(1.16)

(1.16.1) $[F(\sqrt{2},\sqrt{3},\sqrt{5}):F]=8$.

(1.16.2) $[F(\sqrt{2},\sqrt{3},\sqrt{5}):F(\sqrt{2})]=4$.

(1.16.3) $E=\mathbf{Q}(\sqrt[6]{2})$ だから，$[E:F]=6$.

(1.16.4) $E=\mathbf{Q}(\sqrt[12]{2})$ だから，$[E:F]=12$.

(1.16.5) $E=\mathbf{Q}(\sqrt{2},\sqrt[4]{2})=\mathbf{Q}(\sqrt[4]{2})$ だから，$[E:F]=4$.

(1.17)

(1.17.1) X^4-10X^2+1.

(1.17.2) X^3-3X^2+3X-3.

(1.17.3) X^4+1.

(1.17.4) $X^9-15X^6-87X^3-125$.

(1.18) $(1+\theta^2)^{-1}=-\theta^2-\theta$.

(1.19) $q\in\mathbf{Q}$ に対して，$q\mapsto q$ だから，$\sqrt{2}\mapsto\pm\sqrt{2}$ であることを考えると，$\pm\sqrt{2}\notin\mathbf{Q}(\sqrt{3})$ なので同型写像にはなりえない．

(1.20) なりえない．章末 1.19 と同様．

(1.21) 不可能．章末 1.19 と同様．

(1.22) $\sqrt[3]{2}\omega\mapsto\sqrt[3]{2}$ 一つだけが，$\mathbf{Q}(\sqrt[3]{2}\omega)$ から $\mathbf{R}$ の中への同型写像となる．また，$\mathbf{Q}(\sqrt[3]{2},\omega)$ から $\mathbf{C}$ の中への同型写像は，$\omega\mapsto\omega$ もしくは $\omega\mapsto\bar{\omega}$ の二種類があり，それぞれの時，$\sqrt[3]{2}\mapsto\sqrt[3]{2}\bar{\omega}$，$\sqrt[3]{2}\mapsto\sqrt[3]{2}\omega$.

(1.23) $\mathbf{Q}(\sqrt[3]{2},\sqrt[5]{3})$ の $\mathbf{Q}$ 上の自己同型写像を f とおく．$f(\sqrt[3]{2})^3=2$ であり，$f(\sqrt[3]{2})\in\mathbf{R}$ に注意すると，$f(\sqrt[3]{2})=\sqrt[3]{2}$．同様にして，$f(\sqrt[5]{3})=\sqrt[5]{3}$．よって，$f=id$.

(1.24) $k(X)$ の $k(X^p)$ 上の自己同型写像を f とおく．

$$f(X)^p=f(X^p)=X^p\Longleftrightarrow(f(X)-X)^p=0\Longleftrightarrow f(X)=X.$$

よって，$f=id$.

(1.25) $\mathbf{Q}(\sqrt{m})\simeq\mathbf{Q}(\sqrt{n})$ だとする．m,n のいずれかが平方数なら，もう片方も平方数である必要がある．m,n のどちらも平方数でないと仮定すると，$\sqrt{m}\in\mathbf{Q}(\sqrt{n})$ である必要がある．つまり，$\sqrt{m}=a+b\sqrt{n}$ $(a,b\in\mathbf{Q})$ と書ける．両辺を二乗すると，$m=a^2+nb^2+2ab\sqrt{n}$ で $ab=0$ を得る．$b=0$ なら $\sqrt{m}\in\mathbf{Q}$ となり矛盾．よって，$a=0$ を得る．つまり，$\sqrt{m/n}\in\mathbf{Q}$ が必要．逆に，$\sqrt{m/n}=q\in\mathbf{Q}$ とおくと，$\sqrt{m}\mapsto q\sqrt{n}$ は $\mathbf{Q}(\sqrt{m})$ から $\mathbf{Q}(\sqrt{n})$ への同型写像となる．

(1.26)

$$X^4-X^2+4=(X^2+2)^2-5X^2=\prod_{\varepsilon_1,\varepsilon_2\in\{1,-1\}}\left(X-\frac{\varepsilon_1\sqrt{5}+\varepsilon_2\sqrt{-3}}{2}\right)$$

よって，X^4-X^2+4 の $\mathbf{Q}$ 上の最小分解体は $\mathbf{Q}(\sqrt{5},\sqrt{-3})$.

(1.27) n についての帰納法で示す．$n=1$ の時は自明である．f の根の一つを α とおく．$F(\alpha)$ 上の $f(X)/(X-\alpha)$ の最小分解体と，F 上の $f(X)$ の最小分解体は一致する．帰納法の仮定より，$[E:$

$F(\alpha)] \leq (n-1)!$. よって，

$$[E:F] = [E:F(\alpha)][F(\alpha):F] \leq (n-1)! \cdot n = n!$$

(1.28) $\mathbf{Q}(\sqrt[3]{2}+\omega)$.

(1.29) $\mathbf{Q}(\sqrt{2},\sqrt{3},\sqrt{5}) = \mathbf{Q}(\sqrt{2}+\sqrt{3}+\sqrt{5})$.

(1.30) $[\mathbf{F}_2(\zeta_2,\zeta_3):\mathbf{F}_2] = 6$ だから，$\mathbf{F}_2(\zeta_2,\zeta_3) \simeq \mathbf{F}_{2^6}$．$\mathbf{F}_{2^6}^{\times} = \langle\theta\rangle$ とおくと，$\mathbf{F}_2(\theta) = \mathbf{F}_{2^6}$.

(1.31) $|F| < \infty$ なら，α が分離的である仮定を除いてもよい．$F(\alpha,\beta)$ は有限体となるから，$F(\alpha,\beta)^{\times}$ の生成元 θ をとれば，$F(\alpha,\beta) = F(\theta)$ となる．$|F| = \infty$ の時を考える．F 上の α の最小多項式を f，β の最小多項式を g とおく．$\bar{F}$ 上で

$$f(X) = \prod_{i=1}^{n}(X-\alpha_i), \qquad (\alpha = \alpha_1)$$

$$g(X) = \prod_{j=1}^{m}(X-\beta_j), \qquad (\beta = \beta_1)$$

と書けたとする．α が分離的であるから，$\alpha_i - \alpha_j \neq 0$ $(i \neq j)$ となり，

$$\frac{\beta_\mu - \beta_\nu}{\alpha_i - \alpha_j}\ (1 \leq \mu,\nu \leq m, 1 \leq i,j \leq n, i \neq j)$$

という値を考えることができる．この値は有限個の値しかとらないから，これらのいずれでもない $c \in F$ をとることができる（ここで，$|F| = \infty$ を使っている．）．$\theta = c\alpha + \beta$ とおく．明らかに $F(\theta) \subset F(\alpha,\beta)$ である．逆の包含関係について示す．

$$g(\theta - cX) = \prod_{j=1}^{m}(\theta - cX - \beta_j) \in F(\theta)[X]$$

について考える（$g(\theta-cX) \in F(\theta)[X]$ を言うのに，$c \in F$ を使っている．）．θ の定義より，α は $g(\theta-cX)$ の根である：

$$\theta - c\alpha - \beta_1 = \theta - c\alpha - \beta = 0.$$

また，$i \geq 2$ に対して，

$$\theta - c\alpha_i - \beta_j = (\alpha - \alpha_i)\left(c - \frac{\beta_j - \beta}{\alpha - \alpha_i}\right) \neq 0$$

であるから，α_i は $g(\theta-cX)$ の根ではない．f が分離多項式であるから，$f(X)$ と $g(\theta-cX)$ の gcd は $X - \alpha \in F(\theta)[X]$ である．よって，$\alpha \in F(\theta)$．また，$\beta = \theta - c\alpha \in F(\theta)$．よって，$F(\alpha,\beta) \subset F(\theta)$．以上より，$F(\alpha,\beta) = F(\theta)$.

(1.32) E/F は有限次分離拡大であるから，$\theta \in E$ がとれて，$F(\theta) = E$．θ の F 上の最小多項式を p とおく．E/F の中間体 K 上の θ の最小多項式を p_K とおく．このとき，$E = K(\theta)$ である．E/F の中間体 M であって，$p_M = p_K$ とすると，$p_M = p_{M\cap K}$ であるから，

$$\begin{aligned}
&\deg p_M \cdot [M : M\cap K] = [E:M][M:M\cap K] = [E:M\cap K] = \deg p_{M\cap K} \\
&\Longrightarrow [M:M\cap K] = 1 \\
&\Longrightarrow M = M\cap K \\
&\Longrightarrow M \subset K.
\end{aligned}$$

同様に，$K \subset M$ が言えて，$M = K$．E/F の中間体から，p の既約因子のいくつかの積全体への単射を得る．これの値域の元はいずれも $(X - \theta)$ で割り切れるから，E/F の中間体の総数は 2^{n-1} 以下．

(1.33) 必要性は章末 1.32 から言える．十分性をを示す．E/F の中間体が有限個しかないと仮定する．$|F| < \infty$ なら章末 1.31 の結果から明らかなので $|F| = \infty$ とする．E における F の分離閉包 E_s を考える．E_s/F は有限次分離拡大であるから，$\alpha \in E_s$ が取れて，$F(\alpha) = E_s$ となる．r が最小となるような $E_s(\beta_1, \cdots, \beta_r) = E$ をとる．$r = 1$ なら，$F(\alpha, \beta_1)/F$ は章末 1.31 より単純拡大である．次に，$r \geq 2$ の時を考える．異なる $c \in E_s$ が異なる中間体 $E_s(\beta_1 + c\beta_2, \beta_3, \cdots, \beta_r)$ を与えるとすると，これは中間体が有限であることに反する．よって，$c, d \in E_s$ が取れて，

$$E_s(\beta_1 + c\beta_2, \beta_3, \cdots, \beta_r) = E_s(\beta_1 + d\beta_2, \beta_3, \cdots, \beta_r)$$

をみたす．

$$[(\beta_1 + c\beta_2) - (\beta_1 + d\beta_2)](c - d)^{-1} = \beta_2 \in E_s(\beta_1 + c\beta_2, \beta_3, \cdots, \beta_r),$$
$$(\beta_1 + c\beta_2) - c\beta_2 = \beta_1 \in E_s(\beta_1 + c\beta_2, \beta_3, \cdots, \beta_r),$$

より，$E = E_s(\beta_1 + c\beta_2, \beta_3, \cdots, \beta_r) = E_s(\beta_1, \cdots, \beta_r)$ となるが，これは r の最小性に反する．

(1.34) 対偶を示す．a が F 上分離的でないと仮定する，a の F 上最小多項式を $p(X)$ をとる．仮定より，$q(X) \in F[X]$ が存在して，$p(X) = q(X^p)$．$p \mid \deg p(X)$ であるから，$a \notin F(a^p)$．つまり，$F(a) \neq F(a^p)$ (線形独立性から，$a \in F(a^p)$ だとすると，$\exists i, (a^p)^i = a.$)．逆に $F(a) \neq F(a^p)$ だと仮定する．$a \notin F(a^p)$ であるから，$(X - a)^p$ は a の $F(a^p)$ 上の最小多項式である．よって，a は F 上分離的でない．

(1.35) E から E の F 上の準同型写像は F 上の線形写像として見れるから，全射なら単射でもある．

(1.36) $\mathbf{C}$ の $\mathbf{Q}$ 上の超越基底 S をとる．S が無限集合である．S が有限集合とすると，$\mathbf{Q}$ と $\mathbf{C}$ の濃度が同じになって矛盾する．$x \in S$ をとり，$\varphi : S \to S \setminus \{x\}$ なる全単射を考える．この φ は $\mathbf{Q}(S)$ から $\mathbf{Q}(S)$ の中への同型写像を与える．これの延長 $\psi : \mathbf{C} = \overline{\mathbf{Q}(S)} \to \overline{\mathbf{Q}(S \setminus \{x\})} \subset \mathbf{C}$ は $\mathbf{C}$ から $\mathbf{C}$ への全射でない単射準同型である．

(1.37) $\mathbf{C}/\mathbf{Q}$ の超越基底 S をとる．S から S の全単射 φ を与える．φ は同型 $\mathbf{Q}(S) \to \mathbf{Q}(S)$ を引き起こし，すなわち $\mathbf{C}$ の自己同型写像 $\tilde{\varphi}$ を引き起こす．$\tilde{\varphi}$ は φ ごとに異なり，φ は無数に取れるから，$\mathbf{C}$ の自己同型群は無限群である．

(1.38) f を $F[X]$ 上の既約多項式とし，$E[X]$ で，

$$f(X) = g_1(X) \cdots g_n(X)$$

と既約因子分解できたとする．簡単のため，f, g_i はすべて monic であると仮定する．また，$\bar{F}$ で

$$f(X) = (X - \alpha_1) \cdots (X - \alpha_m)$$

と書けたとする．番号を付け替えることで，α_1 は g_1 の根だと仮定してよい．$\bar{F}$ の F 上の自己同型写像であって，$\alpha_1 \mapsto \alpha_i$ とするようなものを σ_i とおく．このような σ_i は，命題 1.3.6, 定理 1.4.7 よりとれることが保証される．まず，$E^{\sigma_i} = \{a^{\sigma_i} : a \in E\} \subset E$ であることを示す．$a \in E$ を任意にとる．a^{σ_i} と a は F 上共役であるから，正規拡大の定義から，$a^{\sigma_i} \in E$ である．$\alpha_1^{\sigma_i} = \alpha_i$ の E 上の最小多項式を p と置けば，$g_1^{\sigma_i} = p$ である．なぜなら，$g_1^{\sigma_i}$ は monic かつ E 係数で，α_i を根に持つからである．p は j が存在して，$g_j = p$ と書け，つまり $g_1^{\sigma_i} = g_j$ である．特に，$\deg g_1 = \deg g_j$．i を 1 から m を動かしていくと，対応する j は 1 から n の値をすべて動くので，g_i たちの次数は相等しい．

(1.39)

(1.39.1) はい.

(1.39.2) いいえ.

(1.39.3) はい.

(1.39.4) はい.

(1.40) $a \in E_1 \cap E_2$ をとる．a の F 上共役元は E_1 にも E_2 にも含まれるから，$a \in E_1 \cap E_2$．よって，$E_1 \cap E_2$ は F の正規拡大.

(1.41)

(1.41.1) $F^G = \mathbf{Q}(\sqrt{-1})$

(1.41.2) $F^G = \mathbf{Q}(\sqrt[3]{2}\omega^2)$

(1.41.3) $F^G = \mathbf{Q}(\sqrt[3]{2})$

(1.41.4) $F^G = \mathbf{Q}(\zeta_8^2)$

(1.41.5) $F^G = \mathbf{Q}(X^2, Y^2, XY)$

(1.41.6) $F^G = \mathbf{Q}(t + 1/t)$

(1.42) $x \in S$ を任意にとる．$1/x \in F$ であるから，$a_0, \cdots, a_{n-1} \in S$ が存在して，

$$(1/x)^n + a_{n-1}(1/x)^{n-1} + \cdots + a_0 = 0$$

をみたす．これの両辺に x^{n-1} をかけると，

$$1/x = -(a_{n-1} + \cdots + a_0 x^{n-1}) \in S.$$

(1.43) $F = R[a_1, \cdots, a_n]$ と書けたとする．n についての帰納法で示す．$n = 1$ の時，$a_1 = a$ とおく.

$$\frac{1}{a} = b_0 + b_1 a + \cdots + b_m a^m \quad (b_i \in R)$$

とすると，

$$b_m a^{m+1} + \cdots + b_0 a - 1 = 0$$

であるから，$1, a, a^2, \cdots$ は R 上線形従属である．$1, \cdots, a^k$ は線形独立で，$1, \cdots, , a^k, a^{k+1}$ は線形従属であるとする．$x \in R$ に対して，

$$\frac{1}{x} = c_0 + c_1 a^1 + \cdots + c_k a^k \quad (c_i \in R)$$

とすると，

$$1 = c_0 x + c_1 x a + \cdots + c_k x a^k$$

で，$c_i x \in R$ であるから，$x^{-1} = c_0 \in R$. よって，R は体. $n \geq 2$ であるときは，$F = R[a_1][a_2, \cdots, a_n]$ と考えれば良い.

(1.44) 任意の $a \in R$ について，

$$f_a(X) = \prod_{\sigma \in G} (X - a^\sigma) \in R^G[X]$$

であり，$f_a(X)$ は monic で，$f_a(a) = 0$. 実際に，任意の $\sigma \in G$ に対して，$f_a(X) = f_a^\sigma(X)$ である.

(1.45) X^iY^j についてだけ考えれば良い．$X^iY^j = k(i-j)X^iYj$ が任意の k について成り立てば，$X^iY^j \in \mathbf{C}[X,Y]^G$ である．

$$\forall k, \quad 1 = \zeta^{k(i-j)} \quad \Longleftrightarrow \quad i \equiv j \pmod{n}$$

であるから，$\mathbf{C}[X,Y]^G = \mathbf{C}[XY, X^n, Y^n]$.

(1.46) $\mathbf{Q}$．明らかに，$\mathbf{Q} \subset \mathbf{C}^G$．$\mathbf{C}/\mathbf{Q}$ の超越基底 S をとる．$x \in \mathbf{Q}(S) \setminus \mathbf{Q}$ は，$Q(S)$ の自己同型写像で，x に含まれる基底を x に含まれない基底に移すようなものを考え，これを $\mathbf{C}$ に延長すれば，$x \notin \mathbf{C}^G$．$x \in \mathbf{C} \setminus \mathbf{Q}(S)$ については，$\mathbf{C}/\mathbf{Q}(S)$ が分離拡大であるから，別のものに移すことができるので，$x \notin \mathbf{C}^G$.

(1.47) $E^p \supset k^p = k$．K/L が有限次拡大で，K, L は正標数 p であるとき，$[K:L] = [K^p : L^p]$ である．これを示すには，K を L 上の有限ベクトル空間として見たときの基底を $\{\omega_1, \cdots, \omega_m\}$ としたとき，K^p を L^p のベクトル空間として見たときの基底は $\{\omega_1^p, \cdots, \omega_m^p\}$ であることを言えば十分である．任意の $y \in K^p$ について，$x \in K$ がとれて，$y = x^p$ をみたす．

$$x = \sum_{i=1}^{m} a_i\omega_i \quad \Longrightarrow \quad y = x^p = \sum_{i=1}^{m} a_i^p\omega_i^p$$

より，$K^p = L^p(\omega_1^p, \cdots, \omega_m^p)$．また，

$$a_1^p\omega_1^p + \cdots + a_m^p\omega_m^p = 0 \quad \Longleftrightarrow \quad a_1\omega_1 + \cdots + a_m\omega_m = 0$$

であるから，$\{\omega_1^p, \cdots, \omega_m^p\}$ は L^p 上線形独立．E/k の超越基底を $\{x_1, \cdots, x_n\}$ とする．$[k(x_1, \cdots, x_n) : k(x_1^p, \cdots, x_n^p)] = p^n$, $[E : k(x_1, \cdots, x_n)] = [E^p : k(x_1^p, \cdots, x_n^p)]$ に注意すると，

$$\begin{aligned}[E : k(x_1^p, \cdots, x_n^p)] &= [E : k(x_1, \cdots, x_n)][k(x_1, \cdots, x_n) : k(x_1^p, \cdots, x_n^p)] \\ &= [E : E^p][E^p : k(x_1^p, \cdots, x_n^p)] \\ \Longrightarrow\ [E : E^p] &= p^n.\end{aligned}$$

(1.48) $g(X)Y - f(X) \in k[X,Y]$ は Y が一次で，$k[X,Y]$ が一意分解整域であることから既約である．y は k 上超越的なので，$g(X)y - f(X) \in k(y)[X]$ は既約多項式である．

(1.49) $y \in k(X) \setminus k$ をとる．$X \mapsto y$ が $k(X)$ の自己同型写像であることは，$k(X) = k(y)$ であること同値である．章末 1.48 より，互いに素な $f(X), g(X) \in k(X)$ をとって，$y = f(X)/g(X)$ と書けば，$k(X) = k(y)$ と $\max(\deg f, \deg g) = 1$ と同値である．つまり，$k(X)$ の k 上の自己同型写像は，$X \mapsto (aX+b)/(cX+d) \quad (a,b,c,d \in k,\ ab \neq 0,\ (aX+b, cX+d) = 1)$ である．

(1.50) x の K における最小多項式を $p(X) = a_0 + a_1X + \cdots + X^n$ とおく．a_i の最小公倍数を $l(x) \in k[x]$ として，$q(x,X) = p(X)l(x) = b_0 + b_1X + \cdots + b_nX^n \in k[x,X]$ とおく．$a_i \notin K$ なる i をとる．互いに素な $f(x), g(x) \in k[x]$ をとって，$a_i = f(x)/g(x)$ と書けたとする．$f(x)g(X) - f(X)g(x)$ は X の多項式として，根に x を持つから，$r(x,X) \in k[x,X]$ が取れて，

$$f(x)g(X) - f(X)g(x) = r(x,X)q(x,X).$$

両辺の x の多項式としての次数は $f(x)g(X) - f(X)g(x)$ が，$q(x,X)$ より大きくなることはないので，$r(x,X)$ は X だけに依存する．また，右辺は X を因子として含まないから，$r(x,X)$ は定数である．$k(a_i) \subset K$, $[E:K] = [E:k(a_i)]$ より，$K = k(a_i)$.