目 次

第1章　Galois理論入門

1.1　環とその準同型写像

R が環 ($ring$) であるとは, まず R は空でない集合であって, その上 R には 2 つの演算 $+,\times$ が定められていて次の条件 (公理) をみたすことをいう.

(1) $(R,+)$ は加法群をなし
(2) R の元 a,b に対し $(ab)c=a(bc)$ が成り立つ. (結合法則)
(3) a,b,c を R の元とすれば等式 $a(b+c)=ab+ac$, $(a+b)c=ac+bc$ が成立する. (分配法則)
(4) R 内に次の条件をみたす特殊な元 1 が存在する; $a1=1a=a$, $^\forall a\in R$.

ここで条件 (4) において $1\in R$ は R 内にただ一つしか存在しないのでこれを環 R の単位元 ($the\ identity$) という. 環 R の加法についての単位元は 0 で表し, 元 $a\in R$ の逆元は $-a$ で表す. そして, 任意の元 $a,b\in R$ に対して $a-b:=a+(-b)$ によって減法を定義しよう.

さて, しばらくは, 集合 R は環であるとしよう. このとき次が正しい.

Lemma 1.1.1. 次の主張がすべて成立する.

(1) a は環 R の元とすれば等式 $a0=0a=0$ が正しい.
(2) 元 $a,b\in R$ に対して等式 $(-a)b=a(-b)=-ab$ が成立する.
(3) 更に $-a=(-1)a$, $(-a)(-b)=ab$,
(4) $a(b-c)=ab-ac$, $(a-b)c=ac-bc$ も成立する.

Proof. 環 R 内では $0+0=0$ である. 従って, 等式 $a0=a(0+0)=a0+a0$ が成立することから $a0=0$ が従う. 同様にして, 等式 $0a=0$ を得る. 後は, 読者に委ねることとしよう. □

このことからわかるように, もし環 R 内で等式 $1=0$ が成り立つならば全ての元 $a\in R$ に対して $a=a1=a0=0$ が従い, $R=\{0\}$ となる. この様な環のことを零環と呼ぶのだが, 以下の議論では特に断らないときは

$$1\neq 0$$

であると仮定しよう. つまり, これから考える環は, 特に断らない限り, 零環ではないことを仮定しよう.

Example 1.1.2. 環の例を 3 つあげる. 一つは整数全体の集合 $\mathbb{Z}$ である. もう一つは, 整数 $n\geq 1$ を取り, 集合 $\mathrm{M}_n(\mathbb{R})=\{A|A$ は n 次の実正方行列 $\}$ である. 整数環 $\mathbb{Z}$ 内では等式 $ab=ba$ が 任意の元 $a,b\in\mathbb{Z}$ について成り立つが, $n>1$ であるときの $\mathrm{M}_n(\mathbb{R})$ では一般に成立しない.

$$\begin{pmatrix}0&1\\0&0\end{pmatrix}\begin{pmatrix}1&0\\0&0\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix},\qquad \begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}0&1\\0&0\end{pmatrix}=\begin{pmatrix}0&1\\0&0\end{pmatrix}$$

を見よ. 整数環 $\mathbb{Z}$ のように次の条件

$$(5)\ ab = ba, \quad {}^{\forall}a, b \in R$$

が成立する様な環 R のことを可換環 (*commutative ring*) という. $n > 1$ としたときの $\mathrm{M}_n(\mathbb{R})$ は非可換な環である. ここで, もう一つの可換環の例をあげよう.

$$\begin{aligned} R &= \mathbb{Z} \ltimes \mathbb{Q} \\ &= \{(a, x) | a \in \mathbb{Z},\ x \in \mathbb{Q}\} \end{aligned}$$

とし集合 R 上に $+$ と $\times$ を

$$\begin{aligned} (a, x) + (b, y) &= (a + b, x + y) \\ (a, x) \cdot (b, y) &= (ab, ax + by) \end{aligned}$$

によって定めると, R はこの和と積を演算にして可換環となる.

上の環 $R\ (= \mathbb{Z} \ltimes \mathbb{Q})$ 内では $\mathbb{Q}$ の元 x, y に対して, 次の等式 $(0, x) \cdot (0, y) = (0, 0)$ が成立している. そして写像 f, p を

$$\begin{array}{ccccc} \mathbb{Z} & \xrightarrow{f} & R & \xrightarrow{p} & \mathbb{Z} \\ \cup & & \cup & & \cup \\ a & \longmapsto & (a, 0) & & \\ & & (a, x) & \longmapsto & a \end{array}$$

によって定めると, この f, p は次の性質を持つ.

$$\begin{array}{ll} {}^{\forall}a, b \in \mathbb{Z} \text{ に対して} & \begin{cases} f(a + b) = f(a) + f(b) \\ f(ab) = f(a) f(b) \\ f(1) = 1, \end{cases} \\ {}^{\forall}\alpha, \beta \in R \text{ に対して} & \begin{cases} p(\alpha + \beta) = p(\alpha) + p(\beta) \\ p(ab) = p(\alpha) p(\beta) \\ p(1) = 1. \end{cases} \end{array}$$

このような性質をみたす写像を環の準同型写像という. すなわち

Definition 1. 写像 φ は環 R から環 S への写像とする. このとき, 写像 φ が環の準同型写像 (*homomorphism of rings*) であるとは, R の元 α, β に対して, 等式 $\varphi(\alpha + \beta) = \varphi(\alpha) + \varphi(\beta)$, $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$ が成立し, しかも $\varphi(1) = 1$ である, という条件を写像 φ が全て満たしていることをいう.

写像 $\varphi : R \to S$ が環の準同型写像であるならば, 加法的に見ると, φ は群の準同型写像であるので 2 つの等式 $\varphi(0) = 0$, $\varphi(-a) = -\varphi(a)$, ${}^{\forall}a \in R$ が成立する. 故に, 全ての元 $a, b \in R$ について $\varphi(a - b) = \varphi(a) - \varphi(b)$ が正しい. このことから φ が単射であることと, 集合 $\mathrm{Ker}\,\varphi = \{a \in R | \varphi(a) = 0\}$ について等式 $\mathrm{Ker}\,\varphi = \{0\}$ が成立することは同値である. 上の例 ($R = \mathbb{Z} \ltimes \mathbb{Q}$) においては, 写像 f は単射ではあるが写像 p については $\mathrm{Ker}\,p = \{(0, x) | x \in \mathbb{Q}\}$ であるので単射ではない.

Example 1.1.3.

(1) 複素数体 $\mathbb{C}$ は可換環である. 今, 写像 $\varphi : \mathbb{C} \to \mathbb{C}$ を, $\varphi(a+bi) = a-bi$ によって定めると, 写像 φ は環の準同型写像である.

(2) 実数体 $\mathbb{R}$ から 2 次の実行列環 $\mathrm{M}_2(\mathbb{R})$ への写像 $\varphi : \mathbb{R} \to \mathrm{M}_2(\mathbb{R})$ を, $\varphi(a) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ によって定めると, この写像 φ は環の準同型写像である.

Exercise 1. 実数体から実数体への環の準同型写像は, 恒等写像しか存在しない.

Proof. $\mathbb{R}$ から $\mathbb{R}$ への環の準同型写像を $f : \mathbb{R} \to \mathbb{R}$ とおく. $f(1) = 1$ であるから全ての整数 n に対して, 等式 $f(n) = n$ が成り立つ. 次に全ての有理数 $q \in \mathbb{Q}$ は $a, b \in \mathbb{Z}$ を $a \neq 0$ にとり $q = \frac{b}{a}$ と表すことができるから $f(q) = q$ が従う. 今, 正の数 $0 < a \in \mathbb{R}$ を取り $a = b^2$ とかくと $f(a) = f(b^2) = f(b)^2$ である. 一方で, $1 = f(1) = f(a\frac{1}{a}) = f(a)f(\frac{1}{a})$ より $f(a) \neq 0$ であるから $f(a) > 0$ であることが確かめられる. 故に, $a, b \in R$ を $b > a$ となるように取れば, 必ず次の式 $f(b) > f(a)$ が従う. さて, 任意の実数 $a \in R$ をとる. $f(a) = a$ を証明したいので $f(a) \neq a$ としてみよう. このとき $f(a) < a$ であるか, もしくは $f(a) > a$ であるが, もし $f(a) < a$ を仮定すれば, 有理数 $x \in \mathbb{Q}$ を, $f(a) < x < a$ を満たす様に取ることができ, $f(a) < x = f(x) < f(a)$ という結果が従う. 同様にして $f(a) > a$ を仮定しても矛盾が生じるので等式 $f(a) = a$ が成立する. □

Lemma 1.1.4. 写像 $f : R \to S$ と $g : S \to T$ は環の準同型写像であると仮定すれば, 合成写像 $g \cdot f : R \to T$ も環の準同型写像である.

Definition 2. 写像 $f : R \to S$ は環の準同型写像とする. この f が全単射であるとき, f は環の同型写像 (*isomorphism of rings*) であるという.

Definition 3. R と S は環としよう. R と S が環の同型であるとは, 少なくとも一つは R から S への環の同型写像が存在することをいう. これを $R \cong S$ とかく. この環の同型写像 f をとおして R と S は本質的に同じものとみることができる.

Lemma 1.1.5. 写像 $\varphi : R \to S$ が環の同型写像であれば, 逆写像 $\varphi^{-1} : S \to R$ も環の同型写像である.

Proof. 全ての元 $a, b \in S$ に対して, 等式 $\varphi\left(\varphi^{-1}(a) + \varphi^{-1}(b)\right) = \varphi\left(\varphi^{-1}(a)\right) + \varphi\left(\varphi^{-1}(b)\right) = a + b$, $\varphi\left(\varphi^{-1}(a+b)\right) = a + b$ が成立する. 同様にして, 等式 $\varphi^{-1}(ab) = \varphi^{-1}(a)\varphi^{-1}(b)$, $\varphi^{-1}(1) = 1$ も容易に確かめられる. □

Exercise 2. 環の同型 $\cong$ は同値関係である.

Definition 4. S を環とする. R が S の部分環であるとは,

(1) $\emptyset \neq R \subseteq S$
(2) 元 $a, b \in R$ について, 等式 $a \pm b, ab, -a \in R$ が成立し,
(3) $1 \in R$

をすべて満たすことをいう. よって, 集合 S は環 S の部分環である.

Lemma 1.1.6. 集合 R が環 S の部分環ならば, R は環 S の和と積を演算に環である.

たとえば, 写像 $\varphi : R \to S$ を環の準同型写像であると仮定すれば, 集合 $\varphi(R)$ は環 S の部分環であって, 従って $\varphi(R)$ はそれ自身で環であり, ここで, 写像 $f : R \to \varphi(R)$ を $f(a) = \varphi(a)$ によって定めると, f は環の準同型写像であって全射となる.

Example 1.1.7. 複素数体 $\mathbb{C}$ の部分集合 R, S を $R = \{a + b\,i | a, b \in \mathbb{Z}\},\ S = \{a + b\,i | a, b \in \mathbb{Q}\}$ とおくと, R と S は $\mathbb{C}$ の部分環であって, 更に R は S の部分環でもある.

集合 $A = \{a + \sqrt{2}\,b | a, b \in \mathbb{Q}\}$ とおくと, A は実数体 $\mathbb{R}$ の部分環である.

Example 1.1.8.

$$R = \begin{pmatrix} \mathbb{Q} & \mathbb{Q} \\ 0 & \mathbb{Z} \end{pmatrix} = \left\{ \begin{pmatrix} x & y \\ 0 & a \end{pmatrix} \middle| x, y \in \mathbb{Q},\ a \in \mathbb{Z} \right\} \subset \mathrm{M}_2(\mathbb{Q})$$

としよう. R は $\mathrm{M}_2(\mathbb{Q})$ の部分環である. この R は可換環ではない. そして, *Right noetherian* であるが *Left noetherian* ではない.

$$\begin{array}{ccccc} R & \xrightarrow{p_1} & \mathbb{Q} & \qquad R & \xrightarrow{p_2} & \mathbb{Z} \\ \cup & & \cup & \qquad \cup & & \cup \\ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} & \longmapsto & a & \qquad \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} & \longmapsto & c \end{array}$$

は環の準同型写像で全射となっている. この R も実に奇妙な性質をもつ.

1.2 Ideals

以下, R は環 $(1 \neq 0)$ とする.

Definition 5. I が R の *ideal* であるとは,

(1) $\emptyset \neq I \subseteq R$
(2) $^\forall x, y \in I$, $^\forall a \in R$ について $x + y, ax \in I$

が成立していることをいう. R, $\{0\}$ は自明な R の *ideal* である. 又, I が R の *ideal* であれば $I < R$ であって $(-x = (-1)x)$, $I = R \Leftrightarrow 1 \in I$ が成り立つ.

Lemma 1.2.1. $\varphi : R \to S$ を環の準同型写像とすれば, $\mathrm{Ker}\,\varphi$ は R の *ideal* であって, $1 \notin \mathrm{Ker}\,\varphi$ となっている.

Proof. $\varphi(1) = 1 \neq 0$ からである. □

Definition 6. I を R の *ideal* で, $I \subsetneq R$ であるとする. このとき *an abel group* R/I は次の積を演算にして再び環になる.

$$\overline{a} \cdot \overline{b} := \overline{ab}$$

この R/I を R の I による剰余環 (*factor ring*) という. R が可換であれば R/I も可換である.

Proof. 大切なことは, 2 つの定義が well-defined であることにある. $\overline{a} = \overline{a_1}, \overline{b} = \overline{b_1}$ とすると $a-a_1, b-b_1 \in I$ であるから $a - a_1 = i,\ b - b_1 = j$ とおくと $ab = (i + a_1)(j + b_1) = ij + ib_1 + a_1j + a_1b_1$. $\therefore ab - a_1b_1 \in I$ であるから $\overline{ab} = \overline{a_1b_1}$. □

$R/I = \{\overline{a}|a \in R\}$, $\overline{a} = a + I = \{a + i|i \in I\}$ $\therefore \overline{a} = \overline{b} \Leftrightarrow a - b \in I$ に注意すること. $1 = \overline{1}$, $0 = \overline{0}$ であるから $\overline{1} \neq \overline{0}$. ($\because \overline{1} = \overline{0} \Rightarrow 1 = 1 - 0 \in R.\ R = I.$)

$\varepsilon : R \to R/I,\ a \mapsto \overline{a}$ は環の準同型写像であり, ε は全射であって, $\mathrm{Ker}\,\varepsilon = I$ が成り立つ. この ε を自然な全射という.

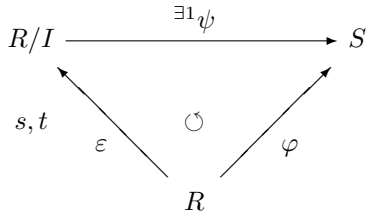
Example 1.2.2. $R = \mathbb{Z}$ とし $2 \leq n \in \mathbb{Z}$ をとり $I = \{na|n \in \mathbb{Z}\}$ とおく. すると I は R の *ideal* であって $1 \notin I$. $\therefore R/I$ が得られる. $^\forall a \in \mathbb{Z}$, $a = qn + r$ $(q, r \in \mathbb{Z},\ 0 \leq n < n)$ と表すと

$$\overline{a} = \overline{qn + r} = \overline{qn} + \overline{r} = \overline{r}$$

$\therefore R/I = \left\{\overline{a}|\overline{0},\ \overline{1}, \cdots, \overline{n-1}\right\}$ となる. もちろん, $0 \leq i, j < n$ のとき $\overline{i} = \overline{j} \Rightarrow i - j \in I$. $\therefore n|i - j$ であるので $i = j$. よって, $\#R/I = n$ である. もし $n \in \mathbb{Z}$ が素元 (素数) であれば, $^\forall a \in \mathbb{Z}$; $0 < a < n$ についても $n \nmid a$. $\therefore (n, a) = 1$. $\therefore xn + ya = 1$ *for some* $x, y \in \mathbb{Z}$. $\therefore \overline{ay} = 1$. 従って $0 \neq {}^\forall\alpha \in R/I$ であれば $^\exists\beta \in R/I$ s,t $\alpha\beta = \beta\alpha = 1$. とくに $n = 2$ であれば $R/I = \left\{\overline{0},\ \overline{1}\right\}$, $n = 3$ ならば $R/I = \left\{\overline{0},\ \overline{1},\ \overline{2}\right\}$ である. $n = 2$ であるときの R/I は最も単純な環であって, 暗号理論の主要な道具となっている.

与えられた環の中にどのような ideal が含まれているかは, 極めて重大な問題である.

Theorem 1.2.3. $\varphi : R \to S$ を環の準同型写像とするとき, R の *ideal* I がもし $I \subseteq \mathrm{Ker}\,\varphi$ であれば,



Proof. $\overline{a} = \overline{b} \Rightarrow a - b \in I \subseteq \mathrm{Ker}\,\varphi$. $\therefore 0 = \varphi(a - b) = \varphi(a) - \varphi(b)$. $\therefore \varphi(a) = \varphi(b)$. これで well-defined になる. あとは自明に近いことのみである. □

Exercise 3. R, S を環とし $\varphi : R \to S$ を環の準同型写像で全射であるとせよ. このとき, $I := \mathrm{Ker}\,\varphi$ とおくと

$$S \cong R/I$$

である.

Exercise 4. $R = \mathrm{M}_n(\mathbb{R})$ $(n > 1)$ 内には *ideal* は R と $\{0\}$ だけである. 従って, $^\forall(R \to S)$ 環の準同型写像は単射である.

1.3　整域と体

さてこれからは, 単に環といえば, R 可換環で $1 \neq 0$ とする.

Definition 7. $a \in R$ のとき, a が R の単元であるとは, ${}^{\exists}x \in R\ s,t\ ax = xa = 1$ が成立することをいう. このとき x は a に対して唯一に定まるので a の逆元と呼び a^{-1} とかく. a が R の単元であれば $a \neq 0$, また $1 \in R$ は単元であって

$$\mathrm{U}(R) = \{u \in R | u \text{ は } R \text{ の単元 }\}$$

とおく.

Lemma 1.3.1. $\mathrm{U}(R)$ は R の $\times$ を演算にして $(able)$ 群をなす.

Proof. $1 \in \mathrm{U}(R)$. $\therefore \emptyset \neq \mathrm{U}(R) \subseteq R$. ${}^{\forall}u, v \in \mathrm{U}(R)$ をとると, $(uv)(v^{-1}u^{-1}) = 1$. $\therefore uv \in \mathrm{U}(R)$. $u \in \mathrm{U}(R)$ であれば $u^{-1} \in \mathrm{U}(R)$ である. よって, $\mathrm{U}(R)$ は群をなす. □

R が S の部分環ならば, $u \in \mathrm{U}(R)$ は $u \in \mathrm{U}(S)$ であって, $\mathrm{U}(R)$ は $\mathrm{U}(S)$ の部分群である.

Definition 8. $a \in R$ が *NZD; non-zerodivisor* (非零因子) であるとは

$$x \in R \text{ について, もし } ax = 0 \text{ ならば } x = 0 \text{ である}$$

が成立することをいう. $a \in R$ が *ZD* であるとは, a は R の *NZD* ではない, つまり

$$0 \neq {}^{\exists}x \in R\ s,t\ ax = 0$$

が成立することである.

Lemma 1.3.2.
(1) $u \in \mathrm{U}(R)$ は $R - nzd$ である, (とくに $1 \in R$ は nzd である.)
(2) $0 \in R$ は *ZD* である.
(3) $R = \mathbb{Z} \ltimes \mathbb{Q}$ とおくと $x \in \mathbb{Q}$ に対して $(0, x) \in R$ は *ZD* である.

Proof. $u \in \mathrm{U}(R)$ をとり $x \in R$ について $ux = 0$ とする. $0 = u^{-1}(ux) = (u^{-1}u)x = x$. □

Definition 9. $0 \neq {}^{\forall}x \in R$ が $R - nzd$ であるとき R を *an integral domain* であるという. $0 \neq a \in R$, $a \in \mathrm{U}(R)$ であるとき R を体という. ($\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ は体であり, $\mathbb{Z}$ は *domain* である.)

Proposition 1.3.3.
(1) 体は整域である.
(2) 整域の部分環は整域である.
(3) よって, 体の部分環は整域である.

Proof. $0 \neq {}^{\forall}a \in R$, a は $\mathrm{U}(R)$ であるから $R - nzd$ である. $R \subseteq S$ として $a, b \in R$ について $ab = 0$ in R ならば $ab = 0$ in S. $\therefore a = 0$ or $b = 0$ in S. $\therefore a = 0$ or $b = 0$ in R. そして (3) は自明. □

一般には, 整域は必ずしも体ではない. $\mathbb{Z}$ がその例である. しかしながら

Proposition 1.3.4. 有限整域は体である.

Proof. $0 \neq {}^{\forall}a \in R$, $\widehat{a} : R \to R$ は injection. $\therefore \widehat{a}$ は bijection. ${}^{\exists}x \in R$ s,t $ax = 1$. □

F を体とし $R \subseteq F$ が部分環であるとき, $0 \neq {}^{\forall}a \in R$ は $0 \neq a \in F$ であるから $a^{-1} \in F$ を取れる. (ただし, $a^{-1} \in R$ であるとは限らない.) そこで

$$K := \left\{ \frac{a}{s} \;\middle|\; a \in R,\ s \in R\backslash\{0\} \right\} \subseteq F$$

とおく. 但し $\dfrac{a}{s} = as^{-1}$ のことであって $s\dfrac{a}{s} = a$ が成立する. $x \in F$ について $a, s \in R$, $s \neq 0$ をとり $sx = a$ であれば $x = \dfrac{a}{s}$ である. $\dfrac{0}{s} = 0s^{-1} = 0$ である.

Lemma 1.3.5.
(1) K は F の部分環で体をなし, R を含む. (この K を R の商体と呼び, $\mathbb{Q}(R)$ とかく.)
(2) L が F の部分環で体であるとし, かつ $R \subseteq L \Rightarrow K \subseteq L$.

Proof. $\dfrac{a}{1} = a$ ${}^{\forall}a \in R$. $\therefore R \subseteq K \subseteq L$. $s, t \in R\backslash\{0\}$, $a, b \in R$ とせよ. すると $st \neq 0$ で

$$\frac{a}{s} + \frac{b}{t} = \frac{ta + sb}{st}\ , \quad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$$

が成立する. また $-\dfrac{a}{s} = \dfrac{-a}{s}$, $1 = \dfrac{1}{1} = \dfrac{s}{s}$ が成立する. 実際,

$$\begin{aligned}
&(st)\left(\frac{a}{s} + \frac{b}{t}\right) = (st)\frac{a}{s} + (st)\frac{b}{t} = ta + sb, \\
&(st)\left(\frac{a}{s} \cdot \frac{b}{t}\right) = ab, \\
&\frac{a}{s} + \frac{-a}{s} = \frac{sa + s(-a)}{s^2} = \frac{0}{s^2} = 0,
\end{aligned}$$

を見よ. そして $0 \neq {}^{\forall}x \in K$, $x = \dfrac{a}{s}$ とかくと $a, s \in L$ であるから $a, s^{-1} \in L$. $\therefore as^{-1} \in L$, $K \subseteq L$. 一方で, $a \neq 0$ なので $\dfrac{a}{s} \in K$; $\dfrac{a}{s} \cdot \dfrac{s}{a} = 1$. $\therefore K$ は L の部分環で体をなし, $R \subseteq K$. □

少し Example を見よう. $\mathbb{C}$ 内で $R = \{a + b\,i |\ a, b \in \mathbb{Z}\}$ とすると, R は $\mathbb{C}$ の部分環であって $K = \{a + b\,i |\ a, b \in \mathbb{Q}\}$ となる.

Proof. まず K は F の部分環であって体をなす. 実際 $0 \neq {}^{\forall}x = a + b\,i \in K$ をとると $(a + b\,i)(a - b\,i) = a^2 + b^2 \neq 0$, であるから ${}^{\exists}(a + b\,i)^{-1} = \dfrac{a}{a^2 + b^2} - i\dfrac{b}{a^2 + b^2} \in K$.

($0 \neq x \in F$ であるから ${}^{\exists}x^{-1} \in F$ であって, 実は $x^{-1} = \dfrac{a}{a^2 + b^2} - i\dfrac{b}{a^2 + b^2}$ であった. ところが K の定義をみると $x^{-1} \in K$, $xx^{-1} = x^{-1}x = 1$ in K. $\therefore x$ は K 内でも単元.)

$\therefore K$ は体である. $R \subseteq K$.
一方で, $R \subseteq L$ が F の部分環で体をなすならば, $0 \neq {}^{\forall}x = a + b\,i \in R$, $0 \neq x \in L$. $\therefore {}^{\exists}x^{-1} \in L$. ${}^{\forall}a, s \in R$; $s \neq 0$, $\frac{a}{s} = as^{-1} \in L$. $\therefore K \subseteq L$. K_0 を R の商体とおくと $K \subseteq K_0$ である. $\therefore K = K_0$. □

Definition 10. F を体とする.
K が F の部分環でかつ体をなすとき, F は K の拡大体, K は F の部分体であるという.
このとき, $0 \neq {}^{\forall}x \in K$ について x の K での逆元は $x^{-1} \in L$ に等しい. 従って

$$\begin{aligned} K \text{ は } L \text{ の部分体である} \quad \Leftrightarrow \quad & K \text{ は } L \text{ の部分環であってかつ} \\ & 0 \neq {}^{\forall}x \in K \text{ について } x^{-1} \in L \text{ をとると } x^{-1} \in K \text{ である} \end{aligned}$$

が成立する.

Proposition 1.3.6. F を体とする. $\{K_\alpha\}_{\alpha\in\Lambda}$ を F の部分体の族とすれば $\bigcap_{\alpha\in\Lambda} K_\alpha$ は F の部分体である.

Exercise 5. $\mathbb{C} \supseteq R := \left\{a + b\sqrt{2} | a, b \in \mathbb{Z}\right\}$ とするとき, $\mathbb{Q}(R) = \left\{a + b\sqrt{2} | a, b \in \mathbb{Q}\right\}$ であることを確かめよ.

1.4　埋め込みの原理について

この Lemma を認めて使う.

Lemma 1.4.1. *X, Y を空でない集合とすれば, ${}^{\exists}(Z, \varphi)$ where Z は空でない集合であって $\varphi : X \to Z$ 全単射, $Y \cap Z = \emptyset$.*

これを証明するには, 集合論を多少必要とする. これと次の Lemma 証明は Exercise としよう.

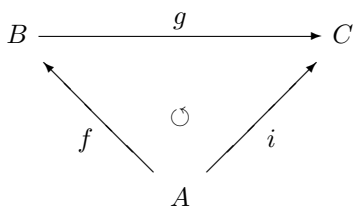
Lemma 1.4.2. R を環とする. X は空でない集合で $f : R \to X$ は全単射とする. このとき, ${}^{\forall}a, b \in X$ について

$$\begin{aligned} a + b &:= f\left(f^{-1}(a) + f^{-1}(b)\right) \\ a \cdot b &:= f\left(f^{-1}(a) f^{-1}(b)\right) \end{aligned}$$

と定めると, この和と積を演算にして X は環になる. このとき, f は環の同型写像であって, もし R が体ならば X も体となる.

Theorem 1.4.3. *$f : A \to B$ が環の準同型写像で単射ならば, ${}^{\exists}(C, g)$ where $g : B \to C$ は環の同型写像であって*

s, t *A は C の部分環,*



もし, B が体であれば C も体である.

Proof. $B = f(A)$ であれば $C = A$ とするとよい. $B \neq f(A)$ としてよい. $\varphi : B \backslash f(A) \xrightarrow{\sim} X$, $X \cap A = \emptyset$ となる (X, φ) を見つけ g をつくり $C = X \cup A$ に環構造をいれよ. ${}^{\forall}a \in A$, $g(f(a)) = a = i(a)$, $\therefore A$ は C

の部分環である.

$$\begin{array}{ccccc} g & : & B & \longrightarrow & C \\ & & \cup & & \cup \\ & & b & \longmapsto & \begin{cases} a & b = f(a) \in f(A) \\ \varphi(b) & b \notin f(A) \end{cases} \end{array}$$

□

1.5 多項式環とその性質

さて, ここでも R は可換環で $1 \neq 0$ とする.

Definition 11. S は環で R は S の部分環とする. $X \in S$ について, X が R 上超越的 (*transcendental*) であるとは,

$$0 \leq n \in \mathbb{Z};\ a_0,\ a_1, \cdots, a_n \in R \text{ について } a_0 + a_1X + \cdots + a_nX^n = 0 \text{ であるなら } a_i = 0 \quad {}^{\forall}i$$

が成立することをいう. 一方, X が R 上 *transcendental* でないときは, X は R 上代数的 (*algebraic*) であるという. 解析学が示すように, $e,\ \pi \in \mathbb{R}$ は $\mathbb{Q}$ 上 *transcendental* であるし, 又すぐわかるように, $i \in \mathbb{C}$ は $\mathbb{R}$ 上 *algebraic* である. ($x^2 + 1 = 0$ をみよ.) e は $\mathbb{Q}$ 上では *transcendental* であるが, R 上では *algebraic* ($e + (-1)e = 0$) である.

transcendental かどうかは必ず "相対的" な概念である. さて, この §5 で示したいことは, 次の定理である.

Theorem 1.5.1. R を環とすれば, 次のような *pair* (S, X) が少なくとも一つは存在する.

(1) S は R を部分環に含むような環である.
(2) X は R 上 *transcendental* である.
(3) ${}^{\forall}f \in S$ は, $n \geq 0;\ a_0, a_1, \cdots, a_n \in R$ をとり $f = a_0 + a_1X + \cdots + a_nX^n$ と表せる.

Remark 1.5.2. $0 \neq f \in S$ のとき (3) の表現は, $a_n \neq 0$ にとると n を含めて必ず一意になる. このときの n を f の次数とよび $\deg f$ とかく. このような環 S を R 上 X を変数にもつ多項式環とよび $S = R[X]$ と表す. 上の定理の証明は後回しにして $S = R[X]$ の大切な性質を一つ述べておく. A を 加法群として $\{a_i\}_{i \in I}$ ($I \neq \emptyset;\ a\ set$) を A の元の *a family* としたとき, $a_i = 0$ *for almost all* $i \in I$ であるとは, $\#\{i \in I | a_i \neq 0\} < \infty$ であることをいう. すなわち, $\emptyset \neq {}^{\exists}J \subset I;\ \#J < \infty,\ i \in I$ がもし $i \notin J$ ならば $a_i = 0$, が成り立つ. このとき,

$$\sum_{i \in I} a_i = \sum_{i \in J} a_i$$

と定める. この定義は J の取り方によらないことに注意せよ. $\therefore -\sum_{i \in I} a_i = \sum_{i \in I}(-a_i)$ である. 勿論, $\{b_i\}_{i \in I}$ が A の元の *a family* であって, $b_i = 0$ *for almost all* $i \in I$ であるならば

$$\sum_{i \in I} a_i + \sum_{i \in I} b_i = \sum_{i \in I}(a_i + b_i)$$

が成り立つ.

Theorem 1.5.3 (代入原理). $S = R[X]$ が環 R 上変数 X をもつ多項式環とする. $\psi : R \to T$ を環の準同型写像とし, $t \in T$ とせよ. すると

$$
\begin{array}{l}
{}^{\exists 1}\varphi : S \longrightarrow T \quad \text{環の準同型写像} \\
s, t \\
\begin{cases}
(1)\ {}^{\forall}a \in R,\ \varphi(a) = \psi(a) \\
(2)\ \varphi(X) = t
\end{cases}
\end{array}
\qquad
\left(
\begin{array}{ccc}
S & \xrightarrow{\quad\varphi\quad} & T \\
& {\scriptstyle i}\nwarrow \quad \circlearrowleft \quad \nearrow{\scriptstyle \psi} & \\
& R &
\end{array}
\right)
$$

${}^{\forall}f \in S$ に対して $\varphi(f)$ を単に $f(t)$ と書く.

Proof. $I = \{0, 1, 2, \cdots\}$ とおくと ${}^{\forall}f \in S$, $f = \sum_{i \in I} a_i X^i$ となる R の元の族 $\{a_i\}_{i \in I}$; $a_i = 0$ for almost all $i \in I$ が f に対して唯一通りに定まる. $\varphi(f) = \sum_{i \in I} \psi(a_i) t^i$ と定める. すると, ${}^{\forall}f, g \in S$,

$$
{}^{\exists 1}\{a_i\}_{i \in I},\ \{b_i\}_{i \in I};\ R \text{ の元の族 } where\ f = \sum_{i \in I} a_i X^i\ , \quad g = \sum_{i \in I} b_i X^i
$$

と表すと,

$$
\varphi(f + g) = \sum_{i \in I} \psi(a_i + b_i) t^i = \sum_{i \in I} \psi(a_i) t^i + \sum_{i \in I} \psi(b_i) t^i = \varphi(f) + \varphi(g)\ ;
$$

となり, 一方で, 積については

$$
\varphi(fg) = \varphi\left(\sum_{n \in I} \left(\sum_{\substack{(i,j) \in I \times I \\ i+j=n}} (a_i b_j) \right) t^n \right)\ ;
$$

となるが, additivity を用いて $f = aX^i$, $g = bX^j$ のときだけを見れば十分. 又, ${}^{\forall}a \in R$, $\varphi(a) = \psi(a)$ は自明であるから $\varphi(1) = 1$ をうる. $\therefore \varphi(X) = t$ であって, 一意性はやさしい. □

Corollary 1.5.4. 多項式環は互いに *R-algebra* として同型である.

Corollary 1.5.5. 多項式は函数ではない.

Proof. $R = \mathbb{Z}/(2)$, $f = X(X-1) \in S = R[X]$ をみよ. □

多項式環の構成の方法.
$C = \{(a_0, a_1, \cdots) | a_i \in R\}$ として $f, g \in C$ をとり $f = (a_0, a_1, \cdots)$, $g = (b_0, b_1, \cdots)$ と表し, 和と積を

$$
\begin{aligned}
f + g &= (a_0 + b_0, a_1 + b_1, \cdots, a_n + b_n, \cdots) \\
f \cdot g &= (a_0 b_0, a_0 b_1 + a_1 b_0, \cdots, \sum_{i+j=n} a_i b_j, \cdots)
\end{aligned}
$$

で定めると, $1_C = (1, 0, 0 \cdots)$, $-f = (-a_0, -a_1, \cdots, -a_n, \cdots)$, $0_C = (0, 0, \cdots)$ をもつような可換環になる. $S \subseteq C$ を

$$
S = \left\{ f \in C | a_i = 0,\ \ {}^{\forall}i \gg 0 \right\}
$$

とおくと S は C の部分環であって, $X = (0, 1, 0, 0, \cdots)$ とおくとよい. □

Definition 12. $n > 0$, $I = \{(\alpha_1, \cdots, \alpha_n) | 0 < \alpha_i \in \mathbb{Z}\}$ とする. R を環とすれば, 次のような組 $(S, \{X_i\})$ が少なくとも一つは存在する.

(1) S は R を部分環に含むような環である.
(2) $X_1, \cdots, X_n$ は R 上 *transcendental* である.
(3) $^\forall f \in S$ は, $\{a_\alpha\}_{\alpha \in I}$ を $a_\alpha = 0$ *for almost all* $\alpha \in I$ となるようにとり $f = \sum_{\alpha \in I} a_\alpha X^\alpha$ と表せる.

ただし, X^α は $\alpha = (\alpha_1, \cdots, \alpha_n)$ としたとき $X^\alpha := X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ を表すものとする. そのような可換環 S を $R = [X_1, \cdots, X_n]$ と表す.

$R[X_1, \cdots, X_n]$ については次が正しい.

Proposition 1.5.6. $S = R[X_1, \cdots, X_n]$ とすると, $\{X^\alpha := X_1^{\alpha_1} \cdots X_n^{\alpha_n}\}$ は S の *an R-free basis* であって, $\psi : R \to T$ 環の準同型写像と $t_1, \cdots, t_n \in T$ を与えれば
$^{\exists 1}\varphi : R[X_1, \cdots, X_n] \to T$ 環の準同型写像 *s,t* $\varphi(a) = \psi(a)$ *for* $^\forall a \in R$, $\varphi(X_i) = t_i$ $(1 \leq {}^\forall i \leq n)$
が成り立つ. S は *a $\mathbb{Z}^n$-graded ring* である.

従って, $^\forall \sigma \in \mathfrak{S}_n$ をとり, $\varphi : R[X_1, \cdots, X_n] \to R[X_1, \cdots, X_n]$, $X_i \mapsto X_{\sigma(i)}$ と定めると, φ は $\varphi(a) = a$ $(^\forall a \in R)$ をみたすような環の同型写像であることがわかる. これは, $\{X_{\sigma(1)}^{\alpha'_1} \cdots X_{\sigma(n)}^{\alpha'_n}\}$ が S の R-代数としての generator としてとることができることをいっている. $\therefore R[X_1, \cdots, X_n] = R[X_{\sigma(1)}, \cdots, X_{\sigma(n)}]$ をうる. これは, subalgebra の議論を持ち込めばもっとよい説明ができるが, ここではこのくらいにしておく.

Lemma 1.5.7. $S = R[X] \ni f \neq 0, g \neq 0$ とし $\deg f = m$, $\deg g = n$ とする. f の m 次の項の係数 a が *R-nzd* であるならば $fg \neq 0$, $\deg(fg) = \deg f + \deg g$ が正しい. よって, R が *domain* ならば $S = R[X]$ も *domain* である. ($S = R[X]$ は必ずしも体ではない.)

Corollary 1.5.8. k が体ならば $k[X_1, \cdots, X_n]$ は *domain* である.

1.6 体上の一変数の多項式環 $k[X]$ とその性質

ここでは簡単のため, 体 k (例えば $\mathbb{Z}/(p)$, $\mathbb{Q}$ などであるが.) を一つ固定し, $k[X]$ によって k 上一変数多項式環を表す. 次が全てを支配している.

Lemma 1.6.1 (Euclid). $f, g \in k[X]$ で $g \neq 0$ とすると $^{\exists 1}(q, r)$ *where* $q, r \in k[X]$; $f = qg + r$ であって, もし $r \neq 0$ であれば $\deg r < \deg g$.

Proof. $n = \deg g$ とおく.
(existance) もし正しくないならば $f \neq 0$, しかも $\deg f = m \geq n$ のはずである. そこでこのような反例から m を最小にとる. すると

$$f = aX^m + (\textit{lower terms}) , \qquad g = bX^n + (\textit{lower terms})$$

と表せている. $b \neq 0$ であるから $h = f - b^{-1}gX^{m-n}$ とおくと $h \neq 0$, $\deg h < m$. $\therefore m$ についての induction により $^\exists(q', r')$ where $q', r' \in k[X]$, $h = q'g + r'$ であって $r' \neq 0$ であれば $\deg r' < m$. よって,

$f = \left(b^{-1}X^{m-n} + q'\right)g + r'$ と表せ矛盾である.
(uniqueness) 上のような $k[X]$ の元の pair (q, r) と (q_1, r_1) をとる. すると

$$f = qg + r = q_1 g + r_1$$

であるから $(q - q_1)g = r_1 - r$ となり, 両辺の次数をみて $q = q_1$, $r = r_1$ をうる. □

Corollary 1.6.2 (剰余の定理). $f \in k[X]$, $\alpha \in k$ とするとき

$$f(\alpha) = 0 \Leftrightarrow f = (X - \alpha)q \quad for\ {}^{\exists}q \in k[X].$$

Proof. $\Rightarrow$ のみ. $g = X - \alpha$ とみると $f = (X - \alpha)q + r$ where $q, r \in k[X]$ であって $r \neq 0$ ならば $1 = \deg(X - \alpha) > \deg r = 0$. $\therefore r \neq 0$ ならば $0 \neq r \in k$ である. 今, $f(\alpha) = 0$ を仮定しているので $f(\alpha) = (\alpha - \alpha)q + r = r$. 従って, $r = 0$ である. □

Corollary 1.6.3. $f \in k[X]$ で ${}^{\forall}\alpha \in k$, $f(\alpha) = 0$ とする.

$$|k| = \infty \Rightarrow f = 0.$$

Proof. $f \neq 0$ ならば $n = \deg f$ とおく. $\alpha_1, \cdots, \alpha_n, \alpha_{n+1} \in k$ を互いに異なるようにとると, ${}^{\forall}i$ について $f(\alpha_i) = 0$ であるから $(X - \alpha_i)|f$. $\therefore \deg f \geq n + 1$. (矛盾) □

さて, 少し notation を作ることにしよう.

Definition 13. R を環とする. $n \geq 1$; $a_1, \cdots, a_n \in R$ が与えられたとき

$$I = \{c_1 a_1 + \cdots + c_n a_n | c_i \in R\}$$

とおくと I は R の *ideal* であって, $a_1, \cdots, a_n \in I$ である. (勿論, この I は $a_1, \cdots, a_n$を含む R の *ideal* で最小である.) この I を, $a_1, \cdots, a_n$ で生成された R の *ideal* とよび, $(a_1, \cdots, a_n)$ とかく. 例えば, $n = 1$ ならば $(a) = \{ca | c \in R\}$ であって, このとき (a) のことを単項 *ideal* (*principal ideal*) とよぶ. $a, b \in R$ ならば, $(a, b) = \{xa + yb | x, y \in R\}$ となり, $(1) = R$, $(0) = \{0\}$ である. $a \in R$ については, $a \in \mathrm{U}(R) \Leftrightarrow (a) = R$ が成立する. そして, $b \in (a)$ であることを $a|b$ (*in* R) と書くこともある.

Corollary 1.6.4. $k[X]$ は, *PID* (*Principal ideal domain*) である. つまり, ${}^{\forall}I \subseteq k[X]$; *ideal* は $I = (g)$ *for some* $g \in I$ とかける.

Proof. $I \neq (0)$, $k[X]$ としてよい. ${}^{\exists}g \in I$ s,t $\deg g = \min\{\deg f | 0 \neq f \in I\}$. このとき $(g) \subseteq I$ は自明. ${}^{\forall}f \in I$ をとると $f = qg + r$ for some $q, r \in k[X]$; $r \neq 0$ ならば $\deg r < \deg g$. $\therefore r = f - qg \in I$ であるから g の次数の最小性をみて $r = 0$ をうる. $\therefore f = qg \in (g)$. $\therefore I = (g)$. □

Definition 14. R を環とする. $0 \neq f \in R$ が *irreducible* であるとは

(1) $f \notin \mathrm{U}(R)$ であって,
(2) $g, h \in R$ をとり, $f = gh$ であれば $g \in \mathrm{U}(R)$ *or* $h \in \mathrm{U}(R)$ となる.

をみたすことをいう. 今, $\mathrm{U}(k[X]) = \{c \in k | c \neq 0\}$ であるから $0 \neq f \in k[X]$ がもし, $f \notin k$ であって, 且つ

$$g, h \in k[X] \text{ をとり } f = gh \text{ とかけているならば } g \in k \text{ or } h \in k$$

をみたすとき, この $f \in k[X]$ は *irreducible* である.

Lemma 1.6.5. $0 \neq f \in k[X]$ が *irreducible* であるとき, $(f) \subsetneq I \subseteq k[X]$ となる *ideal* は $k[X]$ のみである.

Proof. $I = (p)$ とかくと, $f \in (p)$ であるから $f = pg$ for some $g \in k[X]$. もし $p \notin \mathrm{U}(k[X])$ ならば $(f) = (p) = I$ となり矛盾である. $\therefore p \in \mathrm{U}(k[X])$. □

以前にも述べたように, $f, g \in k[X]$ について

$$f|g \Leftrightarrow g = fh \quad for\ some\ h \in k[X] \Leftrightarrow g \in (f)$$

とさだめる.

Theorem 1.6.6. $0 \neq f \in k[X]$ が *irreducible* であれば, $g, h \in k[X]$ について

$$f|gh \Rightarrow f|g \quad or \quad f|h$$

が成り立つ.

Proof. $gh \in (f)$ であって, さらに $g, h \notin (f)$ とすれば $(f) \subsetneq (f, g)$, $(f) \subsetneq (f, h)$ であるから $1 = \alpha f + \beta g = \alpha' f + \beta' h$ for some $\alpha, \beta, \alpha', \beta' \in k[X]$ とかける. $\therefore (f) \ni 1 = (\alpha f + \beta g)(\alpha' f + \beta' h) = \alpha\alpha' f^2 + \alpha\beta' fh + \alpha'\beta fg + \beta\beta' gh$. $\therefore gh \notin (f)$. (矛盾) □

Corollary 1.6.7. $f \in k[X]$ で $f \notin k$ とすると,

$$f \text{ は } irreducible \text{ である} \Leftrightarrow k[X]/(f) \text{ は体である}$$

が成り立つ.

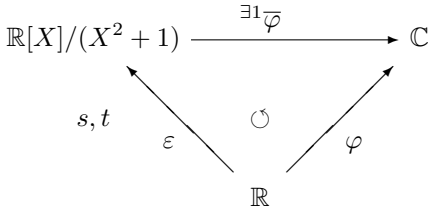
Proof. ($\Rightarrow$) $0 \neq \alpha \in k[X]/(f)$ をとると $\alpha = \overline{g}$ for some $g \in k[X]$. このとき $g \notin (f)$ であるから $\xi, \lambda \in k[X]$ をとり $1 = \alpha f + \beta g$ とかける. $\therefore \overline{1} = \overline{\xi f} + \overline{\lambda g} = \overline{\lambda}\alpha$.
($\Leftarrow$) $g, h \in k[X]$ が, もし $f = gh$ であるならば, $0 = \overline{g}\overline{h}$. $\therefore g \in (f)$ or $h \in (f)$. 今, $g \in (f)$ とすれば $g = \xi f$ ($\xi \in k[X]$) であるから $f = (\xi f)h = (\xi h)f$. $f \neq 0$ であるから $1 = \xi h$ である. □

たとえば, $k = \mathbb{R}$ のとき $f = X^2 + 1 \in \mathbb{R}[X]$ は irreducible である. 実際, $f \notin \mathbb{R}$ であることは自明であって, もし $g, h \in \mathbb{R}[X]$ をとり $X^2 + 1 = gh$ と表せ, $g, h \notin \mathbb{R}$ であるならば, $\deg(X^2 + 1) = 2$ なので $\deg g = \deg h = 1$ である. $\therefore a, b \in \mathbb{R}$ をとり $g = X + a$, $h = X + b$ とかける. $\therefore gh = X^2 + (a + b)X + ab$ であるから, $a + b = 0$ かつ $ab = 1$ を満たさなければならないが, これは実数体 $\mathbb{R}$ の内では不可能であるので, $f = X^2 + 1$ は $\mathbb{R}$ 内では irreducible である. 従って, $\mathbb{R}[X]/(X^2 + 1)$ は体をなす.

Exercise 6. $\mathbb{R}[X]/(X^2 + 1)$ は $\mathbb{C}$ と同型であることを確かめよ. これは, $\mathbb{C}$ の構成の仕方の一つである. もう一つは, 行列を用いる ($\mathrm{M}_2(\mathbb{R})$ の部分体として構成する.) のが有名である.

$$\left\{ \begin{pmatrix} x & y \\ -y & x \end{pmatrix} \middle| x, y \in \mathbb{R} \right\} \subseteq \mathrm{M}_2(\mathbb{R}).$$

Proof. $\varphi : \mathbb{R}[X] \to \mathbb{C}$ を $X \mapsto i$ を代入する代入射とすると, φ は環の準同型写像であって, さらに全射である. $I = \mathrm{Ker}\,\varphi$ とおくと $X^2+1 \in I$. $\therefore \mathbb{R}[X] \supsetneq I \supseteq (X^2+1)$ より $I = (X^2+1)$. 従って, 準同型定理より



この $\overline{\varphi}$ は, 勿論, 全単射である. □

Corollary 1.6.8 (因数分解). $f \in k[X]$ が $f \notin k$ であるならば,

$$f = p_1 p_2 \cdots p_\ell \qquad (\ \ell \geq 1;\ \ p_i \in k[X] \text{ は } \textit{irreducible}\ )$$

の形に表せる. この表現の仕方は, 定数の違いと順序をのぞいて唯一に定まる.

Proof. まず表せることを示そう. 表せないとして, そのような $f \notin k$ のうち $\deg f$ が最小になるものをとると, 少なくとも f は irreducible ではないので $f = gh$; $g, h \notin k$ となるはず. このとき, $\deg g, \deg h < \deg f$ であるから $g, h \in k[X]$ は表現をもつので, はじめの仮定は矛盾である.

さて, $f \in k[X]$ を $f = p_1 p_2 \cdots p_\ell = q_1 q_2 \cdots q_n$ と表す. 但し, $p_i, q_j \in k[X]$ は irreducible とする. これから示したいことは, $\ell = n$, $p_i = c_i q_i$ ($1 \leq {}^\forall i \leq \ell$; $c_i \in k$) である. ℓ についての induction を用いる. $\ell = 1$ ならば $f = p_1$ は irreducible. $\therefore n = 1$ であって $q_1 = p_1$ をうる. $\ell > 1$ で $\ell - 1$ まで正しいとする. 勿論, $n > 1$ である. $p_1 | q_1 q_2 \cdots q_n$ より $p_1 | q_1$ としてよい. $q_1 = \xi_1 p_1$ とかくと q_1 は irreducible, $p_1 \notin k$ なので $\xi_1 \in k$. すると $\xi_1 q_2$ は, やはり irreducible であるから

$$p_2 p_3 \cdots p_\ell = (\xi_1 q_2) q_3 \cdots q_n$$

となり, induction の仮定より $\ell = n$ であって $p_2 = \xi_2 q_2$, $p_3 = \xi_3 q_3, \cdots$, $p_\ell = \xi_\ell q_\ell$ for some $\xi_i \in k$. □

さて, K/k を体の拡大とする. $K[X]$ の内で

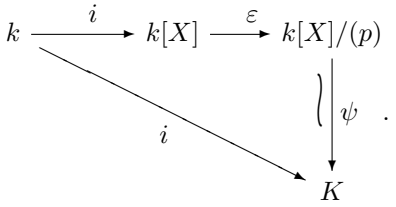
$$k[X] = \{a_0 + a_1 X + \cdots + a_n X^n | n \geq 0,\ \ a_i \in k\} \subseteq K[X]$$

としても, k 上の多項式環がえられる. ($k[X] \to K[X]$ 代入射の像とみてもよい.) 通常は, 必ずこのようにして $k[X] \subseteq K[X]$ を部分環とみなす. 次の定理は, 非常に重要である.

Theorem 1.6.9 (Kronecker). $f \in k[X]$ が $f \notin k$ ならば

$$^\exists(K/k) :\ \text{体の拡大}\ \ s, t\ f \text{ は } K \text{ 内に少なくとも一つの根をもつ.}$$

Proof. $f = p_1 p_2 \cdots p_\ell$ と表して $p = p_1$ とすると $k[X]/(p)$ は体である.



$k \to k[X] \to k[X]/(p)$ は必ず単射になるので, 埋め込みの原理より (K, ψ) を作ると K は体である. $\psi\left(\overline{X}\right) =: \alpha$ とすると $k[X] \to K, \xi \mapsto \xi(\alpha)$ という代入射がつくれ, $p(\alpha) = 0$. これは, $p = c_0 + c_1X + \cdots + c_nX^n$ と表しておくと $0 = \overline{p} = \overline{c_0} + \overline{c_1}\overline{X} + \cdots + \overline{c_n}\overline{X}^n$.

$$\begin{aligned} \therefore \quad 0 &= \psi\left(\overline{c_0}\right) + \psi\left(\overline{c_1}\right)\alpha + \cdots + \psi\left(\overline{c_n}\right)\alpha^n \\ &= c_0 + c_1\alpha + \cdots + c_n\alpha^n = p(\alpha). \end{aligned}$$

$\therefore f(\alpha) = p_1(\alpha)p_2(\alpha)\cdots p_n(\alpha) = 0$ in K. □

Corollary 1.6.10. $f \in k[X]$, $f \notin k$ とせよ. このとき $^{\exists}K/k$; 体の拡大があって $f \in K[X]$ とみたとき f は $K[X]$ 内で一次式の積に分解する.

Proof. $n = \deg f$ についての induction で証明する. K_1/k を f が K_1 内で根 α_1 をもつようにとると $f = (X - \alpha_1)f_1$ $^{\exists}f_1 \in K_1[X]$. ここで, $\deg f_1 = n - 1$ となるので induction の仮定より f_1 について K/K_1 を用いて $f_1 = (X - \alpha_2)(X - \alpha_3)\cdots(X - \alpha_n)$ in $K[X]$ と分解する. $\therefore f = (X - \alpha_1)(X - \alpha_2)\cdots(X - \alpha_n)$ in $K[X]$. □

ある多項式が irreducible であるかどうかは, 考えている体の大きさによるのである. 又, 同じ理由で irreducible であるかどうかの判定は勿論, 因数分解を具体的に行うことは computer を駆使しても, 依然容易いなことではない.

Exercise 7. $k = \mathbb{Z}/(2)$ とするとき $X^2 + X + 1$ は *irreducible* である. $^{\forall}n \geq 1$ に対して n 次の *irreducible* 多項式が $k[X]$ 内に少なくとも一つは存在することを証明せよ. $k = \mathbb{Z}/(3)$ についても考えよ.

1.7 Eisenstein の既約判定法

示したいことは次の定理である.

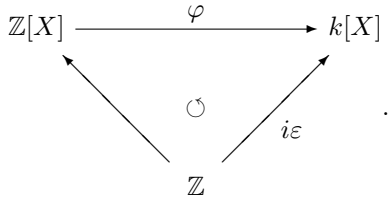
Theorem 1.7.1 (Eisenstein の既約判定法). $n > 0$ とし $a_0, a_1, \cdots, a_n \in \mathbb{Z}$, $2 \leq p \in \mathbb{Z}$ を素数とする. このとき $f = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Q}[X]$ が次の条件をすべてみたすとき $\mathbb{Q}$ 内で既約である.

$$(1)\ a_0, \cdots, a_{n-1} \in (p), \quad (2)\ a_n \notin (p), \quad (3)\ a_0 \notin (p^2).$$

これを証明するには次の 2 つの補題を必要とする.

Lemma 1.7.2. $I = \{pf | f \in \mathbb{Z}[X]\}$ とする. この I は $\mathbb{Z}[X]$ の *prime ideal* である.

Proof. $k = \mathbb{Z}/(p)$ とし $k[X]$ を k 上の多項式環とする. $\mathbb{Z} \xrightarrow{\varepsilon} k \hookrightarrow k[X]$ によって $^{\exists 1}\varphi : \mathbb{Z}[X] \to k[X]$ the $\mathbb{Z}$-algebra map s,t



このとき $\operatorname{Ker}\varphi = I$ であるから $\mathbb{Z}[X]/I \cong k[X]$. $\therefore I \in \operatorname{Spec}\mathbb{Z}[X]$. □

Lemma 1.7.3. $f \in \mathbb{Z}[X]$, $\varphi, \psi \in \mathbb{Q}[X]\backslash\mathbb{Q}$ とせよ. もし $f = \varphi\psi$ であれば $^{\exists}g, h \in \mathbb{Z}[X]$ s,t $f = gh$ であってかつ $\deg g = \deg\varphi$, $\deg h = \deg\psi$.

Proof. $0 < a, b \in \mathbb{Z}$ を $a\varphi, b\psi \in \mathbb{Z}[X]$ にとり, $c = ab$ とせよ. $0 \neq cf = (a\varphi)(b\psi)$. $a\varphi, b\psi$ は $\deg\varphi = \deg a\varphi$, $\deg\psi = \deg b\psi$. $\therefore 0 < {}^{\exists}c \in \mathbb{Z}$; $cf = gh$ where $g, h \in \mathbb{Z}[X]$ であって $\deg g = \deg\varphi$, $\deg h = \deg\psi$. ここで, このような c を最小にとる. もし $c \neq 1$ なら $c \in (p)$ となる正の素数 p をとり $P = \{pf | f \in \mathbb{Z}[X]\} \in \mathrm{Spec}\,\mathbb{Z}[X]$ とおくと $gh = cf \in P$ であるから $g \in P$ or $g \in P$ をみたす. もし $g \in P$ なら $^{\exists}g_1 \in \mathbb{Z}[X]$ s,t $g = pg_1$ であるから $\dfrac{c}{p}f = g_1 h$ となり矛盾である. $\therefore c = 1$. □

さて, 定理の証明をしよう.

Proof of theorem. $f \in \mathbb{Z}[X]$ が (1),(2),(3) をみたすが $\mathbb{Q}$ 内で既約でないなら $^{\exists}\varphi, \psi \in \mathbb{Q}[X]\backslash\mathbb{Q}$ s,t $f = \varphi\psi$. $\therefore f = gh$ for some $g, h \in \mathbb{Z}[X]\backslash\mathbb{Z}$. $I = \{pf | f \in \mathbb{Z}[X]\}$ とおくとき $\overline{\varphi} : \mathbb{Z}[X]/I \xrightarrow{\sim} k[X]$, $f = gh \mapsto \varphi(f) = \varphi(g)\varphi(h) = \overline{a_n}X^n \neq 0$. ここで $\deg g = \ell$, $\deg h = m$ とおくと $\ell + m = n$, $\ell, m > 0$. そして $g = bX^\ell + (lower\ terms)$, $h = cX^m + (lower\ terms)$ とかくと $bc = a_n$ であって $bc \notin (p)$.
$\therefore b \notin (p)$ かつ $c \notin (p)$. 従って $\deg\overline{g} = \ell$, $\deg\overline{h} = m$ であるから $\deg\varphi(g) = \ell > 0$, $\deg\varphi(h) = m > 0$. 今, $g = b_\ell X^\ell + \cdots + b_0$, $h = c_m X^m + \cdots + c_0$ $(b = b_\ell, c = c_m)$ と表すと $b_0 \in (p)$ or $c_0 \in (p)$ である. $b_0 \in (p)$ とする. もし $c_0 \notin (p)$ ならば $b_1 c_0 + c_1 b_0 \in (p)$ より $b_1 c_0 \in (p)$, $b_1 \in (p)$. 次に f の 2 次をみて $b_2 \in (p)$ となり, これを繰り返して $b = b_\ell \in (p)$ となるので矛盾である. $\therefore b_0, c_0 \in (p)$, $a_0 = b_0 c_0 \in (p^2)$. (矛盾) □

Corollary 1.7.4. $a \in \mathbb{Z}$, $2 \leq p \in \mathbb{Z}$ 素数とする. $n > 0$ としたとき, $a \in (p)\backslash(p^2)$ ならば $X^n + a$ は $\mathbb{Q}$ 内で既約である.

Exercise 8. 素数 p に対して $f = X^{p-1} + X^{p-2} + \cdots + X + 1$ は *irreducible in* $\mathbb{Q}$ であることを確かめよ.

($\because X \mapsto X + 1$ を比べて $X^p - 1 = (X - 1)f$ をみよ.)

1.8　体の代数拡大

議論をはじめる前に次を注意しておく.

Lemma 1.8.1. R, S を環とせよ.

(1) $R \cong S$ のときは, R が体 (*resp. domain.*) であることの必要十分条件は S が体 (*resp. domain.*) である.
(2) $\sigma : R \to S$ を環の準同型写像とするとき, $^{\exists 1}\varphi : R[X] \to S[X]$ *a ring homom* s,t $\varphi(X) = X$, $\varphi(a) = \sigma(a)$ *for* $^{\forall}a \in R$. このとき $\varphi(a_0 + a_1 X + \cdots + a_n X^n) = \sigma(a_0) + \sigma(a_1)X + \cdots + \sigma(a_n)X$ となっている.

さて, 以下 K/k を体の拡大とする. $[K : k]$ によって K を k 上の vector s.p とみたときの次元 $\dim_k K$ を表すことにする.

Notation. $n > 0$; $\alpha_i \in K$ $(^{\forall}i = 1, \cdots, n)$, R を K の部分環としたとき

$$R[\alpha_1, \cdots, \alpha_n] := \{f(\alpha_1, \cdots, \alpha_n) | f \in R[X_1, \cdots, X_n]\}$$

と定める. $R[\alpha_1,\cdots,\alpha_n]$ は代入射 $\varphi : R[X_1,\cdots,X_n] \to K$ の像であるから K の部分環である.

次が正しい.

Lemma 1.8.2.
(1) $R \subseteq R[\alpha_1,\cdots,\alpha_n]$.
(2) $\alpha_1,\cdots,\alpha_n \in R[\alpha_1,\cdots,\alpha_n]$.
(3) L を K の部分環とせよ. もし L が R と $\alpha_1,\cdots,\alpha_n$ をすべて含むならば $R[\alpha_1,\cdots,\alpha_n] \subseteq L$ である.

Corollary 1.8.3. $R[\alpha_1,\cdots,\alpha_n] = (R[\alpha_1,\cdots,\alpha_{n-1}])\,[\alpha_n]$ *if* $n \geq 2$.

Notation. $\alpha_1,\cdots,\alpha_n \in K$ $(n \geq 1)$ に対して

$$k(\alpha_1,\cdots,\alpha_n) := K \text{ 内で考えた } k[\alpha_1,\cdots,\alpha_n] \text{ の商体}$$

とおく. $k(\alpha_1,\cdots,\alpha_n)$ は K の部分体であって次の補題をみたしている. ただし, $k(\alpha_1,\cdots,\alpha_n)$ は必ずしも $k[\alpha_1,\cdots,\alpha_n]$ と一致するとは限らないことに注意する.

Lemma 1.8.4.
(1) $k \subseteq k(\alpha_1,\cdots,\alpha_n)$.
(2) $\alpha_1,\cdots,\alpha_n \in k(\alpha_1,\cdots,\alpha_n)$.
(3) L を K の部分体とせよ. もし L が k と $\alpha_1,\cdots,\alpha_n$ をすべて含むならば $k(\alpha_1,\cdots,\alpha_n) \subseteq L$ である.

Corollary 1.8.5. $k(\alpha_1,\cdots,\alpha_n) = (k(\alpha_1,\cdots,\alpha_{n-1}))\,(\alpha_n)$ *if* $n \geq 2$.

さて, $\alpha \in K$ としよう.

Definition 15. α が k 上代数的 (*algebraic over* k) であるとは, $0 \neq {}^{\exists}f \in k[X]$ *s,t* $f(\alpha) = 0$ *in* K をみたすことをいう. この条件は, α を代入する代入射 $\varphi : k[X] \to K$ が単射でないことと同値である.

Theorem 1.8.6. $\alpha \in K$; *algebraic over* k として, $\varphi : k[X] \to K$ を代入射とせよ. このとき $k[X]$ が *a PID* であるから $\operatorname{Ker}\varphi = (f)$ *for some* $0 \neq f \in k[X]$; *monic* と表せる. この f については次が成立する.

(1) f は *irreducible in* k である.
(2) $g \in k[X]$ について, $g(\alpha) = 0$ であるための必要十分条件は $g = hf$ となる $h \in k[X]$ が存在することである.
(3) f は $k[X]$ の元で α を根にもつ多項式の内で次数が最小なものである.

この f のことを α の k 上の最小多項式という.

Proof. (1) のみ. $f = gh$ $(g,h \in k[X])$ とせよ. $f \neq 0$ より $g,h \neq 0$ であるから $\deg f = \deg g + \deg h$ をみるに, もし f が既約でないならば $g,h \in k[X]$ で $\deg g > 0$, $\deg h > 0$ であって更に $f = gh$ をみたすものがとれるが, これは f の次数の最小性に反する. $\therefore f$ は irreducible. □

Corollary 1.8.7. $\alpha \in K$ とする. $k[\alpha]$ が体であることと, α が *algebraic over* k であることは同値である. このとき f を α の *the minimal polynomial,* $n = \deg f$ とすれば $\{1,\alpha,\cdots,\alpha^{n-1}\}$ が $k[\alpha]$ の *k-basis* であるから $\big[k[\alpha]:k\big] = n$ になる.

Proof. α が k 上代数的であるとしよう. $k[\alpha] \cong k[X]/I$, $k[X]/I$ は体であるから $k[\alpha]$ は体である. 逆に, $k[\alpha]$ が体ならば $\mathrm{Ker}\,\varphi \neq (0)$. 最後の等式を示そう. $\deg f = n$ とせよ. $n \geq 1$ である. $c_i \in k$ をとり $f = c_0 + c_1X + \cdots + c_{n-1}X^{n-1} + X^n$ とかくと $^\forall g \in k[X]$ に対して $g = qf + r$ ($^{\exists 1}q, r \in k[X]$; $r \neq 0$ ならば $\deg r < n$.) であるから $g(\alpha) = r(\alpha)$. $\therefore g(\alpha) \in k + k\alpha + \cdots + k\alpha^{n-1}$. 一方で, $\{1, \alpha, \cdots, \alpha^{n-1}\}$ は $k-free$ であるからこれは basis である. $\therefore \big[k[\alpha]:k\big] = n$ をうる. □

Corollary 1.8.8. $n > 0$; $\alpha_1, \cdots, \alpha_n \in K$ とせよ. α_i がすべて *algrbraic over* k ならば $k[\alpha_1, \cdots, \alpha_n]$ は体をなし, $\big[k[\alpha_1, \cdots, \alpha_n]:k\big] < \infty$ である.

Proof. n についての induction に従う. □

Definition 16. K/k が *algebraic* であるとは $^\forall\alpha \in K$ が k 上 *algebraic* であることをいう.

Corollary 1.8.9. $\alpha_1, \cdots, \alpha_n \in K$ が k 上 *algebraic* であれば, 体拡大 $k(\alpha_1, \cdots, \alpha_n)/k$ は代数拡大である.

Proof. $k[\alpha_1, \cdots, \alpha_n]$ は体である. $\therefore k[\alpha_1, \cdots, \alpha_n] = k(\alpha_1, \cdots, \alpha_n)$. $^\forall\alpha \in k(\alpha_1, \cdots, \alpha_n)$ とすると $\big[k[\alpha]:k\big] = n < \infty$. よって, α の代入射 $\varphi : k[X] \to k[\alpha]$ は単射ではない. $\therefore \alpha$ は k 上代数的である. □

Remark 1.8.10. この証明からわかるように, $\alpha \in K$ について, α が *algebraic over* k であることと $\big[k[\alpha]:k\big] < \infty$ は同値である. とくに $[K:k] < \infty$ ならば K/k は必ず代数拡大である.

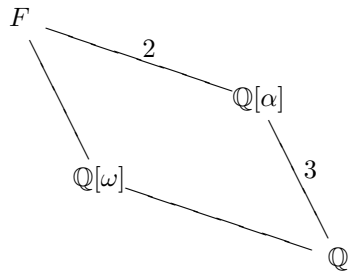
Corollary 1.8.11. K/k は代数拡大とせよ. $^\forall\alpha_1, \cdots, \alpha_n \in K$ に対して $k[\alpha_1, \cdots, \alpha_n] = k(\alpha_1, \cdots, \alpha_n)$ であってかつ $\big[k(\alpha_1, \cdots, \alpha_n):k\big] < \infty$ である. ただし $[K:k] < \infty$ とは限らない.

次の例はこれからよく用いるであろうから, ここでは以下, *Basic Example* と呼ぶことにする.

Example 1.8.12. $f = X^3 - 2 \in \mathbb{Q}[X]$ は $\mathbb{Q}$ で既約である. 一方で, 代数学の基本定理によれば f は $\mathbb{C}[X]$ 内で一次式の積に分解する. それを $f = (X-\alpha)(X-\beta)(X-\gamma)$ とかくことにする. 実際には, $\alpha = \sqrt[3]{2}$ ととると $\omega^2 + \omega + 1 = 0$ となる $\omega \left(= \dfrac{-1 \pm i\sqrt{3}}{2}\right)$ を一つとれば $\beta = \alpha\omega$, $\gamma = \alpha\omega^2$ である. このとき $F = \mathbb{Q}[\alpha, \beta, \gamma]$ は $\mathbb{C}$ の部分体をなし $F = \mathbb{Q}[\alpha, \omega]$ が成立する.

Proof. $F \ni \alpha, \alpha\omega, \alpha\omega^2$ より $\alpha, \omega \in F$. $\therefore F \supseteq \mathbb{Q}[\alpha, \omega]$. α, ω は $\mathbb{Q}$ 上で代数的であるから $\mathbb{Q}[\alpha, \omega]$ は $\mathbb{C}$ の部分体であって, $\alpha, \beta, \gamma \in \mathbb{Q}[\alpha, \omega]$. $\therefore F = \mathbb{Q}[\alpha, \omega]$.

そして $\omega^2 + \omega + 1 = 0$ より ω は $\mathbb{Q}[\alpha]$ 上 $X^2 + X + 1$ の根. $\mathbb{Q}[\alpha] \subseteq \mathbb{R}$ ので $\omega \notin \mathbb{Q}[\alpha]$. $\therefore \big[F:\mathbb{Q}[\alpha]\big] = 2$. $\big[\mathbb{Q}[\alpha]:\mathbb{Q}\big] = 3$ であることは上と同様にして求まり, 従って $[F:\mathbb{Q}] = 6$ となる.



もちろん, $^\forall\theta \in F$ は $\mathbb{Q}$ 上代数的であって, その最小多項式を f, $\deg f = n$ とおくと, $n|6$ であるから $n = 1, 2, 3, 6$ となる. ($\mathrm{Gal}(F/\mathbb{Q}) \cong \mathrm{S}_3$ であって *abel* 群ではない.) □

Proposition 1.8.13. $k \subseteq K \subseteq L$ を体拡大とする. このとき L/k; *algebraic* であることの必要十分条件は L/K, K/k; *algebraic* である.

Proof. $\Leftarrow$ のみで十分. $^{\forall}\alpha \in L$ をとると α は K 上 algebraic. よって $f = c_0 + c_1X + \cdots + c_nX^n$ を α の K 上の最小多項式とすると $E = k[c_0, \cdots, c_n]$ は体で, E 上で α は algebraic である. $\therefore E[\alpha]$ は体をなし, $\big[E[\alpha] : E\big] < \infty$. 一方で, $[E : k] < \infty$ であるから $\big[E[\alpha] : k\big] < \infty$. 従って, α は k 上 algebraic である. □

Definition 17. k を体とする. k が代数閉体 (*algebraic closed field*) であるとは, $^{\forall}(K/k)$; 体の拡大で *algebraic* について $K = k$ が成り立つことをいう. これを, $k = \overline{k}$ と表すこともある.

Example 1.8.14. 複素数体 $\mathbb{C}$ は *an algebraic closed field* である. 代数学の基本定理はこれを保証しているが, その証明は解析的に行われる. 但し, *Galois* 理論を用いた証明にはのちにふれる予定である.

Lemma 1.8.15. k を体とするとき次は同値である.

(1) k は代数閉体である.
(2) $f \in k[X]$ が $f \notin k$ ならば, f は $k[X]$ 内で 1 次式の積に分解する.
(3) $^{\forall}k[X]\backslash k$ は少なくとも一つの根をもつ.

Proof. (1)⇒(3) $f \in k[X]\backslash k$ をとると $^{\exists}K/k$; 体拡大 s,t f の根を一つは K が含む. その根を $\alpha \in K$ とかく. すると $k[\alpha]$ は体であって k 上代数拡大であるから $\alpha \in k[\alpha] = k$.
(3)⇒(2) 自明.
(2)⇒(1) K/k を代数拡大, $\alpha \in K$ とすると α の k 上最小多項式は irreducible. よって, それは 1 次式であって $\alpha \in k$. □

一般には次が知られていてる. その証明は $Exercise$ とするが非常に難しい.

Theorem 1.8.16. k を体とすると $^{\exists}K/k$ 体の拡大 *s,t* K は代数閉体であって K/k は *algebraic.*

1.9 分解体とその一意性について

はじめに次の補題から入る. K/k, K'/k' は体の拡大で $\sigma : k \to k'$ は環の同型とする. すると σ によって多項式環の同型 $\widetilde{\sigma} : k[X] \to k'[X]$, $\sum_{i\in I} a_iX^i \mapsto \sum_{i\in I} \sigma(a_i)X^i$ where $I = \{0, 1, 2, \cdots\}$ が induce される. この記号の下に,

Lemma 1.9.1. $\alpha \in K$, $\alpha' \in K'$ とする. α は k 上 *algebraic,* α' は k' 上 *algebraic* とせよ. このとき, もし α の k 上の最小多項式 $\phi(X)$ の $\widetilde{\sigma}$ による像 $\widetilde{\sigma}(\phi(X))$ が α' の k' 上の最小多項式であったならば

$$
\begin{array}{lccc}
^{\exists 1}\tau : & k[\alpha] & \longrightarrow & k'[\alpha'] \quad a\ ring\ homom \\
s,t & \uparrow & \circlearrowleft & \uparrow \quad , \ \tau(\alpha) = \alpha' \quad . \\
k & & \xrightarrow{\sigma} & k'
\end{array}
$$

Proof. 一意性は自明. 存在は

$$\begin{array}{ccccc} (p) & \longrightarrow & k[X] & \xrightarrow{\varphi} & k[\alpha] \quad \subseteq K \\ & & \Big\downarrow \widetilde{\sigma} & \circlearrowleft & \Big\downarrow {}^{\exists 1}\tau \\ (p') & \longrightarrow & k'[X] & \xrightarrow{\varphi'} & k'[\alpha'] \ \subseteq K' \end{array}$$

をみるに, 環の準同型によって τ が unique にある. この τ は onto であって $\sigma = \tau|_k$, $\tau(\alpha) = \alpha'$ をみたす. もちろん τ は単射でもある. □

Definition 18. K/k を体の拡大とし $f \in k[X]\backslash k$ とする. このとき K と k の中間体 E (E は K の部分体であって, 更に k を部分体として含む,) が f の K 内で考えた k 上の分解体であるとは

(1) $f = c(X-\alpha_1)\cdots(X-\alpha_n)$ *where* $0 \neq c \in k$; $n = \deg f \geq 1$; $\alpha_1, \cdots, \alpha_n \in K$ と表せる.
(2) $E = k[\alpha_1, \cdots, \alpha_n]$.

が成り立つことをいう. もちろん K 内には E の他に f の k 上の分解体は含まれない. *Kronecker* の定理によると, k 体とし $f \in k[X]\backslash k$ であれば必ず f の k 上の分解体が存在する. 次の主張はそのような分解体の一意性を述べたものである.

Theorem 1.9.2. 上の *Lemma* と同じ仮定の下に, $f \in k[X]\backslash k$ の $\widetilde{\sigma}$ による像を $f'(X)$ とする. ここで f は K 内で, f' は K' 内でそれぞれ 1 次式に分解していると仮定せよ. f の K 内で考えた k 上の分解体を E, f' の K' 内で考えた k' 上の分解体を E' とすると,

$$\begin{array}{ccc} K & & K' \\ | & & | \\ E & \xrightarrow{{}^{\exists}\tau} & E' \ a\ ring\ homom \\ \uparrow & \circlearrowleft & \uparrow \\ k & \longrightarrow & k' \end{array}$$

.

Proof. $f = c(X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_n)$ where $0 \neq c \in k$; $n = \deg f > 0$, $\alpha_i \in K$ とする. $m = \#\{1 \leq i \leq n | \alpha_i \notin k\}$ とおき, m についての induction で示す. $m = 0$ であれば $1 \leq {}^{\forall} i \leq n$, $\alpha_i \in k$.
$\therefore k = E$. 一方で, $f' = \widetilde{\sigma}(f) = \sigma(c)(X-\sigma(\alpha_1))\cdots(X-\sigma(\alpha_n))$, $E' = k'$. $m > 0$ として $m-1$ 以下で正しいとせよ. 適当に並び替えをして $\alpha = \alpha_1 \notin k$ としてよいであろう. すると α の k 上の最小多項式を p とすると $f = pg$, ${}^{\exists} g \in k[X]$. $\therefore f' = p'g'$ where $p' = \widetilde{\sigma}(p)$, $g' = \widetilde{\sigma}(g)$. このとき p' は irreducible in k' であって, f' が $K'[X]$ 内で 1 次式の積に分解しているので, p' は $K'[X]$ 内で 1 次式に分解している. 今, $\alpha' \in K'$ を p' の K' 内での根とすれば $f'(\alpha') = 0$ であって, α' の k' 上の最小多項式は p' に他ならない. よって, $k_1 = k[\alpha]$, $k_1' = k'[\alpha']$ とおくと Lemma より

$$\begin{array}{ccc} K & & K' \\ | & & | \\ k_1 & \xrightarrow{{}^{\exists 1}\tau} & k_1' \quad s,t \ \ \tau(\alpha) = \alpha'. \\ \uparrow & \circlearrowleft & \uparrow \\ k & \xrightarrow[\sigma]{} & k' \end{array}$$

ここで $f \in k_1 = k[\alpha]$ をみると, E は K 内で k_1 上考えた f の分解体であるから $\#\{1 \leq i \leq n | \alpha_i \notin k_1\} < m$. よって m についての induction より次のような環の同型射 ρ が得られそれが求めるものである.

$$\begin{array}{ccc} E & \xrightarrow{{}^{\exists}\rho} & E' \\ \uparrow & \circlearrowleft & \uparrow \\ k_1 & \longrightarrow & k_1' \end{array} .$$

□

Corollary 1.9.3. k を体, $f \in k[X]\backslash k$ とする. そして K/k, K'/k を体の拡大としよう. f は K 内でも K' 内でも 1 次式に分解していると仮定し, E と E' をそれぞれ K, K' 内での k 上で考えた f の分解体とすると

$$\begin{array}{lccc} {}^{\exists 1}\tau : & E & \longrightarrow & E' \\ s,t & & \overset{i}{\nwarrow}\ \circlearrowleft\ \overset{i}{\nearrow} & \\ & & k & \end{array} \quad ;\ a\ ring\ isomorphism \quad .$$

Proof. $k = k'$, $\sigma = 1_k$ とせよ. □

1.10 群指標

$(G, \times)$ は群, k を体として $k^* = k\backslash\{0\} = \mathrm{U}(k)$ とせよ. 群の射 $\sigma : G \to k^*$ を G の k 上の指標 (*charactor*) という. $\widehat{G} := \{\sigma | \sigma : G \to k^* \ \ a\ group\ homomorphism\}$ とおく.

Lemma 1.10.1. $\sigma_1, \cdots, \sigma_n \in \widehat{G}$ $(n > 0)$ で *distinct* と仮定せよ. このとき, $c_1, \cdots, c_n \in k$ について $\sum_{i=1}^{n} c_i\sigma_i(x) = 0$ *for* ${}^{\forall}x \in G$ ならば $c_1 = \cdots = c_n = 0$ である.

Proof. n についての induction で示す. $n = 1$ ならば $x = e$ をとって自明. $n > 1$ で $n-1$ 以下で正しいとせよ. $\sigma_1 \neq \sigma_n$ ので ${}^{\exists}\alpha \in G$ s,t $\sigma_1(\alpha) \neq \sigma_n(\alpha)$. $\therefore {}^{\forall}\alpha, x \in G$ について $0 = \sum_{i=1}^{n} c_i\sigma_i(\alpha x) = \sum_{i=1}^{n} c_i\sigma_i(\alpha)\sigma_i(x)$.

一方で, ${}^{\forall}x \in G$, $0 = \sigma_n(\alpha)\left(\sum_{i=1}^{n} c_i\sigma_i(x)\right)$.

$$\therefore \quad \sum_{i=1}^{n-1}\Big(c_i\big(\sigma_i(\alpha) - \sigma_n(\alpha)\big)\Big)\sigma_i(x) = 0.$$

induction の仮定より ${}^{\forall}i = 1, \cdots, n-1$ について $c_i\big(\sigma_i(\alpha) - \sigma_n(\alpha)\big) = 0$ である. 今, $i = 1$ をみるに $\sigma_1(\alpha) \neq \sigma_n(\alpha)$ であるから $c_1 = 0$. よって ${}^{\forall}x \in G$, $\sum_{i=2}^{n} c_i\sigma_i(x) = 0$ をうるが, もう一度 induction を用いて $c_2 = \cdots = c_n = 0$ をうる. □

さて, E, E' を体とし $\sigma_i : E \to E'$ を環の準同型写像 $(i = 1, \cdots, n;\ n > 0)$ とする. このとき $L = \big\{x \in E | \sigma_i(x) = \sigma_j(x),\ 1 \leq {}^{\forall}i, j \leq n\big\}$ とする.

Lemma 1.10.2. L は E の部分体である.

Proof. $1 \in E$ は $^{\forall}i$ に対して $\sigma_i(1) = 1$ であるから $1 \in L$. $\therefore L \neq \emptyset$. $^{\forall}x, y \in L$ をとると $1 \leq {}^{\forall}i, j \leq n$ について $\sigma_i(x+y) = \sigma_i(x) + \sigma_i(y) = \sigma_j(x) + \sigma_j(y) = \sigma_j(x+y)$; $\sigma_i(xy) = \sigma_i(x)\sigma_i(y) = \sigma_j(x)\sigma_j(y) = \sigma_j(xy)$; $\sigma_i(-x) = -\sigma_i(x) = -\sigma_j(x) = \sigma_j(-x)$ である. $\therefore x+y, xy, -x \in L$, L は部分環である. $0 \neq {}^{\forall}x \in L$ に対して $^{\exists}x^{-1} \in E$. よって i をとって, $1 = \sigma_i(1) = \sigma_i(xx^{-1}) = \sigma_i(x)\sigma_i(x^{-1})$ $\therefore \sigma_i(x^{-1}) = \sigma_i(x)^{-1}$ in E. 従って, $\sigma_i(x^{-1}) = \sigma_i(x)^{-1} = \sigma_j(x)^{-1} = \sigma_j(x^{-1})$ をみて $x^{-1} \in L$ が確かめられる. $\therefore K/L$ は体の拡大となっている. □

Corollary 1.10.3. 上の $\sigma_1, \cdots, \sigma_n$ が *distinct* であれば, $c_1, \cdots, c_n \in E'$ について, $\displaystyle\sum_{i=1}^{n} c_i\sigma_i(x) = 0$ *for* $^{\forall}x \in E$ ならば $c_1 = \cdots = c_n = 0$ である.

Proof. $G = E\backslash\{0\}$ とすることに従う. □

示したいことは次である.

Theorem 1.10.4. $\sigma_1, \cdots, \sigma_n$ が *distinct* ならば $[E : L] \geq n$ である.

Proof. $r = [E : L]$ とおき $r < n$ として矛盾をみちびく. もちろん, $1 \leq r < n$ である. E の L 上の basis を一組とってこれを $\{\omega_1, \cdots, \omega_r\}$ とする. このとき

$$A = \begin{bmatrix} \sigma_1(\omega_1) & \cdot & \cdot & \cdot & \sigma_n(\omega_1) \\ \vdots & & \ddots & & \vdots \\ \sigma_1(\omega_r) & \cdot & \cdot & \cdot & \sigma_n(\omega_r) \end{bmatrix} \quad \in \mathrm{M}_{rn}(E)$$

をみると, $A : E^{(n)} \to E^{(r)}$ は $r < n$ としているので決して単射ではない. $\therefore 0 \neq {}^{\exists}x = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \in E^{(n)}$

s,t $Ax = [0]$. $\therefore 1 \leq {}^{\forall}i \leq r$, $\displaystyle\sum_{j=1}^{n} \sigma_j(\omega_i)x_j = 0$ in E'. そこで $^{\forall}\alpha \in E$ をとるとき $\{\omega_1, \cdots, \omega_r\}$ は E の $L - basis$ であるから $\displaystyle\alpha = \sum_{i=1}^{r} a_i\omega_i$ $(a_i \in L)$ と表せて, $1 \leq {}^{\forall}i \leq r$ に対して

$$0 = \sigma_i(a_i) \cdot \sum_{j=1}^{n} \sigma_j(\omega_i)x_j = \sum_{j=1}^{n} \sigma_i(a_i)\sigma_j(\omega_i)x_j = \sum_{j=1}^{n} \sigma_j(a_i)\sigma_j(\omega_i)x_j = \sum_{j=1}^{n} \sigma_j(a_i\omega_i)x_j.$$

$$\therefore \quad 0 = \sum_{i=1}^{r} \left(\sum_{j=1}^{n} \sigma_j(a_i\omega_i)x_j \right) = \sum_{j=1}^{n} \left(\sum_{i=1}^{r} \sigma_j(a_i\omega_i)x_j \right) = \sum_{j=1}^{n} \sigma_j(\alpha)x_j.$$

ここで Corollary をみると $x_1 = \cdots = x_n = 0$ となり単射であることに矛盾する. $\therefore [E : L] \geq n$. □

以上を用いてこれから *Galois* 拡大の理論をつくる. さて, やはり E は体とする.

$$\mathrm{Aut}\, E = \{\alpha | \alpha : E \to E \ \ a\ ring\ isomorphism\}$$

とすると, $\mathrm{Aut}\, E$ は写像の合成を演算に群をなす. (*Exercise*) $\emptyset \neq {}^{\forall}G \subseteq \mathrm{Aut}\, E$ に対して

$$E^G = \left\{x \in E | \sigma(x) = x,\ {}^{\forall}\sigma \in G\right\}$$

とおくと, E^G は E の部分体となる. (*Exercise*) このとき, 更に次が正しい.

Corollary 1.10.5. $|G| < \infty$ ならば $\left[E : E^G\right] \geq |G|$ である.

Proof. $1_E \in G$ であれば E^G は上の記号で L に他ならない. $1_E \notin G$ であれば $G' = G \cup \{1_E\}$ とすると $E^G \subseteq E^{G'}$, $E^{G'} = L$ であるから $\left[E : E^G\right] \geq \left[E : E^{G'}\right] \geq |G'| > |G|$. □

K を E の部分体とする. $\mathrm{Gal}(E/K) = \left\{\alpha \in \mathrm{Aut}\, E | \alpha(x) = x,\ {}^{\forall}x \in K\right\}$ とおく. このとき $\mathrm{Gal}(E/K)$ は $\mathrm{Aut}\, E$ の部分群である. (*Exercise*) $G := \mathrm{Gal}(E/K)$ とすると $K \subseteq E^G$, $[E : K] \geq |G|$ が成り立つ. 中間体と $\mathrm{Aut}\, E$ の subgroup については, ある整った関係がある.

Exercise 9. *Basis Example* において $\mathrm{Aut}\, F$ を決定せよ. S_3 のはずである.

1.11 体の Galois 拡大について

E を体とし G を $\mathrm{Aut}\, E$ の a finite subgroup とせよ. $n = |G|$ とおく. そして $K = E^G$ とせよ. すると次の驚くべき等式

Theorem 1.11.1. $[E : K] = |G|$.

が成り立つ.

Proof. $[E : K] \geq n = |G|$ であった. $n \geq [E : K]$ を示せばよい. ${}^{\forall}\omega_1, \cdots, \omega_n, \omega_{n+1} \in E$ をとると連立方程式 $\sigma \in G$,

$$\sigma^{-1}(\omega_1)x_1 + \sigma^{-1}(\omega_2) + \cdots + \sigma^{-1}(\omega_n)x_n + \sigma^{-1}(\omega_{n+1}) = 0$$

は非自明な解 $0 \neq \begin{bmatrix} x_1 \\ \vdots \\ x_{n+1} \end{bmatrix} \in E^{n+1}$ をもつ. $\therefore {}^{\forall}\sigma \in G$ について $\displaystyle\sum_{j=1}^{n+1} \sigma^{-1}(\omega_j)x_j = 0$. $\therefore \displaystyle\sum_{j=1}^{n+1} \sigma(x_j)\omega_j = 0$.

$$\therefore \quad \sum_{\sigma \in G} \left(\sum_{j=1}^{n+1} \sigma(x_j)\omega_j \right) = \sum_{j=1}^{n+1} \omega_j \left(\sum_{\sigma \in G} \sigma(x_j) \right) = 0.$$

そこで, $T : E \to K$, $x \mapsto \displaystyle\sum_{\sigma \in G} \sigma(x)$ をみるに, T は a K-linear かつ, 指標の独立性から $T(x) \neq 0$ ${}^{\exists}x \in E$. この notation を用いると $\displaystyle\sum_{j=1}^{n+1} T(x_j)\omega_j = 0$. 一方, $T(x) \neq 0$ となる $x \in E$ をとると, $x_j \neq 0$ ならば $\dfrac{x}{x_j}$ 倍することによって x_j を x に置き換えて $x = x_j$ となる非自明な解がとれる. $\therefore T(x_j) \neq 0$. よって $\{\omega_1, \cdots, \omega_{n+1}\}$ は一次独立ではないので $[E : K] \leq n$ をうる. □

この定理より

Corollary 1.11.2. $\mathrm{Gal}(E/K) = G$.

Proof. $G \subseteq \mathrm{Gal}(E/K)$ は自明. $^{\exists}\sigma \in \mathrm{Gal}(E/K)\backslash G$ とすると $K = E^{G\cup\{\sigma\}}$ であるから $[E : K] \geq |G \cup \{\sigma\}| > n$ となり矛盾. $\therefore G = \mathrm{Gal}(E/K)$. □

Corollary 1.11.3. G_1, G_2 を $\mathrm{Aut}\, E$ の *finite subgroups* とすると, $G_1 = G_2$ であるための必要十分条件は $E^{G_1} = E^{G_2}$ である.

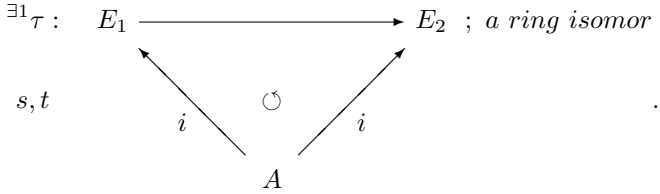
Definition 19. E/K を体の拡大とせよ. E/K が *Galois* 拡大であるとは, $^{\exists}G \subseteq \mathrm{Aut}\, E$ *s,t* $E^G = K$ をみたすことをいう. このとき $G = \mathrm{Gal}(E/K)$ となるので G の取り方は *unique* に定まる.

例えば *Basis Example* をみるに $E = \mathbb{Q}[\alpha, \omega]$ とすると, $\mathrm{Aut}\, E \cong \mathrm{S}_3$. $\mathrm{Aut}\, F = G$ とすると $\mathbb{Q} \subseteq E^G$, $[E : \mathbb{Q}] = 6$ より $E^G = \mathbb{Q}$ である. よって $E/\mathbb{Q}$ は典型的な *Galois* 拡大の例である.

Lemma 1.11.4. K を体とする. $f \in K[X]\backslash K$ をとる. このとき次は同値である.

(1) f は $^{\forall}(E/K)$ 体の拡大をとっても, 決して E 内で重根をもたない. つまり, $^{\forall}\alpha \in E$ に対して $f \notin \left((X-\alpha)^2\right)$ *in* $E[X]$ である.
(2) $^{\exists}(E/K)$ 体の拡大 *s,t* f は $E[X]$ 内で 1 次式の積に分解して, かつ E 内で重根を持たない.

Proof. (1)⇒(2) は自明なので (2)⇒(1) だけを示す. F/K を体の拡大とする. F をさらに拡大して, (それを L とおく.) L 内では f が 1 次式に分解したとする. E 内での f の分解体を E_1, L 内での f の分解体を E_2 とおくと,



$\therefore f = c(X-\alpha_1)\cdots(X-\alpha_n)$ where $0 \neq c \in K$; $n = \deg f > 0$; $\alpha_i \in E_1$ と表すと, τ の induce する環の同型 $\tilde{\tau} : E_1[X] \to E_2[X]$ によって $f = \tilde{\tau}(f) = \tau(c)(X - \tau(\alpha_1))\cdots(X - \tau(\alpha_n)) \in E_2[X]$. 従って f は E 内でも重根をもつことはない. $\therefore f$ が F 内で重根をもつことはない. □

Theorem 1.11.5. E/K は *Galois* 拡大で $G = \mathrm{Gal}(E/K)$ とせよ. このとき $^{\forall}\alpha \in E$ について α の K 上の最小多項式は E 内で 1 次式の積に分解していて, しかも重根をもつことはない.

Proof. $^{\forall}\alpha \in E$ をとって $t = \#\{\sigma(\alpha)|\sigma \in G\}$ とし $\{\sigma(\alpha)|\sigma \in G\} = \{\alpha_1, \cdots, \alpha_t\}$ とかく. $f = \prod_{i=1}^{t}(X - \alpha_i) \in E[X]$ とする. $^{\forall}\sigma \in G$, $\tilde{\sigma} : E[X] \xrightarrow{\sim} E[X]$ を σ が induce する環の同型写像とすれば, $\tilde{\sigma}(f) = \prod_{i=1}^{t}(X - \sigma(\alpha_i)) = f$. $\therefore f \in K[X]$, $f(\alpha) = 0$. $g \in K[X]$ が $g(\alpha) = 0$ をみたすならば $g = (X-\alpha)h$ $^{\exists}h \in K[X]$. $\therefore {}^{\forall}\sigma \in G$, $g = \tilde{\sigma}(g) = (X - \sigma(\alpha))\tilde{\sigma}(h)$. $\therefore g(\sigma(\alpha)) = 0$. $\therefore g(\alpha_i) = 0$ for $^{\forall}i = 1, \cdots, t$.
$\therefore g = f\xi$ $^{\exists}\xi \in K[X]$. $^{\forall}\sigma \in G$, $\tilde{\sigma}(g) = \tilde{\sigma}(f)\tilde{\sigma}(\xi)$ より $g = f\tilde{\sigma}(\xi)$. 従って, $\tilde{\sigma}(\xi) = \xi$ $(^{\forall}\sigma \in G)$ であるから $\xi \in K[X]$ をうる. よって f は α の K 上の最小多項式であることがわかる. □

Theorem 1.11.6. E/K は *Galois* 拡大で, $G = \mathrm{Gal}(E/K)$ とする. このとき $K \subseteq {}^{\forall}B \subseteq E$; 中間体, $U = \mathrm{Gal}(E/B)$ とすると, U は G の部分群であって $B = E^U$ が成り立つ. 従って, E/B も *Galois* 拡大である.

Proof. もちろん $U < G$ である. $B \subseteq E^U$ は自明であるので $B \supseteq E^U$ を示す. $s = [G : U]$ とおき $\{\sigma U | \sigma \in G\} \left(= \overline{\sigma}\right)$ の完全代表系を $\sigma_1 (= 1), \sigma_2, \cdots, \sigma_s$ とすると, $\tau_1, \tau_2 \in G$ のとき, $\tau_1^{-1}\tau_2 \in U$ (i, e; $\tau_1 U = \tau_2 U$) であることと, ${}^{\forall}b \in B$ について $\tau_1(b) = \tau_2(b)$ は同値である. 従って, $\{\sigma_i\}_{1 \leq i \leq s}$ の取り方をみると $\tau_i := \sigma_i|_B : B \to E$ はすべて異なる写像を定める. $\therefore K = \left\{b \in B | \tau_i(b) = \tau_j(b),\ 1 \leq {}^{\forall}i, j \leq s\right\}$ であるので $[B : K] \geq s$ をうる. よって, $[E : B][B : K] = |G|$ より $[E : B] \leq \dfrac{|G|}{s} = |U| = \left[E : E^U\right]$ である. $\therefore E \supseteq E^U \supseteq B$ より $[E : B] = \left[E : E^U\right]$. $\therefore B = E^U$. □

Theorem 1.11.7 (Galois の基本定理). E/K を *Galois* 拡大, $G = \mathrm{Gal}(E/K)$ とすると

$$\begin{array}{ccc} \{B | K \subseteq B \subseteq E,\ \text{中間体}\} & \longleftrightarrow & \{U | U < G\} \\ B & \longmapsto & \mathrm{Gal}(E/B)\ . \\ E^U & \longmapsfrom & U \end{array}$$

$K \subseteq B \subseteq E$; 中間体について, B/K が *Galois* であることと U が G の正規部分群であることは同値であり, このとき $\mathrm{Gal}(B/K) \cong G/U$ が正しい. より詳しくは,

$$\begin{array}{ccccccccc} 1 & \longrightarrow & U & \longrightarrow & G & \longrightarrow & \mathrm{Gal}(B/K) & \longrightarrow & 1 \\ & & & & \cup & & \cup & & \\ & & & & \sigma & \longmapsto & \sigma|_B & & \end{array}$$

という群の完全列が存在する.

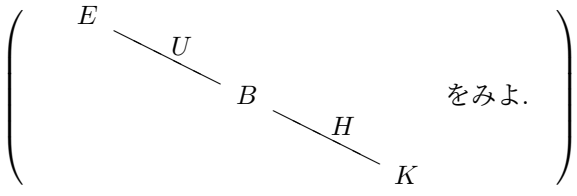
Proof. 最後の主張のみを示す. B を任意の中間体とし ${}^{\forall}\sigma \in G$ をとるとき $\sigma(B)$ も中間体である. $U = \mathrm{Gal}(E/B)$ としたとき $\mathrm{Gal}(E/\sigma(B)) = \sigma U \sigma^{-1}$ となることが次のようにして確かめられる.

$V = \mathrm{Gal}(E/\sigma(B))$ とするとき $\tau \in G$ について

$$\begin{aligned} \tau \in U &\Leftrightarrow \tau(\sigma(b)) = \sigma(b),\ {}^{\forall}b \in B \\ &\Leftrightarrow \left(\sigma^{-1}\tau\sigma\right)(b) = b,\ {}^{\forall}b \in B \\ &\Leftrightarrow \sigma^{-1}\tau \in U \\ &\Leftrightarrow \tau \in \sigma U \sigma^{-1}. \end{aligned}$$

$\therefore V = \sigma U \sigma^{-1}$. よって $\sigma(B) = B\ {}^{\forall}\sigma \in G$ であることは, $U \triangleleft G$ であることと同値である. そして $U \triangleleft G$ として $H = \{\sigma|_B | \sigma \in G\}$ とおくと $H < \mathrm{Aut}\, B$; a finite subgroup であって $\varphi : G \to H,\ \sigma \mapsto \sigma|_B$ の *Kernel* は U に他ならないので $H \cong G/U$. 一方で, $B^H = K$. $\therefore B/K$ は Galois 拡大である.

逆に, B/K は Galois 拡大であるならば $H = \mathrm{Gal}(B/K)$ として $s = |H|$ とすれば $s = [G : U]$ であって



そして $\sigma_1(=1), \sigma_2, \cdots, \sigma_s$ を $\{\sigma U | \sigma \in G\}$ の一組の完全代表系とすると $\sigma_i|_B : B \to E$ は distinct であるのでこれが $B \to E$ 全ての $K-algebra\ maps$ を動く．実際, $\rho : B \to E$ を a $K-algebra\ map$ で $^\forall i$, $\rho \neq \sigma_i|_B$ とするとき $K = B^{\{\sigma_i|_B | 1 \leq i \leq s\} \cup \{\rho\}}$. $\therefore [B:K] \geq s+1$ となり矛盾．一方で, $^\forall h \in H$ に対して $B \xrightarrow{h} B \xrightarrow{i} E$ は $distinct\ K-algebra\ maps$ s 個を定める．これより $1 \leq {}^\forall i \leq s$, $\sigma(B) = B$ が得られる．$\therefore {}^\forall \sigma \in G$, $\sigma(B) = B$. $\therefore U \triangleleft G$. □

Exercise 10. *Basis Example* で $\mathrm{Aut}\, E$ の部分群とそれに対応する中間体を全て求めよ．

しかし真の問題は, "いつ *Galois* 拡大になっているか " を判断する簡単な方法を求めることにある．次回はそのことについて述べることにしよう．

1.12　分離拡大

示したい定理は唯一つ．次の結果である．

Theorem 1.12.1. E/K を体の拡大とする．このとき次の条件は同値である．

(1) 体拡大 E/K は *Galois* 拡大である．
(2) E は f の K 上の分解体であって, 更に *separable* である元 $f \in K[X]\backslash K$ が存在する．

"*separable*"という言葉の定義は後にすることとして, 今は k は体として, 元 $f \in k[X]\backslash k$ を取る．この元 f が重根を持つとは, 適当な体拡大 K/k を取ると f は K 内では重根を持つ, 即ち, $f \in \left((X-\alpha)^2\right) K[X]$ を満たす元 $\alpha \in K$ が存在することをいう．

Lemma 1.12.2. $f \in k[X]\backslash k$ とすると, 次の条件は同値である．

(1) f は重根を持つ．
(2) f' によって f の形式的微分を表すと, $(f, f') \neq k[X]$ が成立する．
(3) $f(\theta) = f'(\theta) = 0$ を満たす元 θ を含むような, k の拡大体 K が取れる．

Proof. (1)⇒(3) K/k を体拡大で, $\theta \in K$ が $f(\theta) = 0$ の重根であったとする．この時, f は $K[X]$ 内で $f = (X-\theta)^2 g$ という分解を持つ．すると, $f' = 2(X-\theta) + (X-\theta)^2 g'$ となるので $f'(\theta) = 0$ が従う．

(3)⇒(2) $1 \in (f, f')$ であるならば $g, h \in k[X]$ を, 等式 $fg + f'h = 1$ を満たすように取ることができる．故に, $f(\theta)g(\theta) + f'(\theta)h(\theta) = 1$ という結果が得られる．

(2)⇒(1) $(f, f') = (g)$ とすると $f = gh$, $f' = g\ell$ と表す $g\ell \in k[X]$ を取ることができる．$g \notin k$ を仮定しているので, $g(\theta) = 0$ となる θ を含む拡大体 K を取り, $f = (X-\theta)\xi$ と表す．すると, $f' = \xi + (X-\theta)\xi'$ より等式 $g(\theta)\ell(\theta) = f'(\theta) = \xi(\theta) = 0$ が得られ, 故に, $\xi \in (X-\theta)$, $f = (\theta)\xi \in \left((X-\theta)^2\right)$ が従う．□

Corollary 1.12.3. $f \in k[X]\backslash k$ は k 内で *irreducible* であると仮定せよ．この時, f が重根を持たないことと, $f' \neq 0$ が成り立つことは同値である．

Proof. $f' \neq 0$ であると仮定しよう．もし, f が重根を持つならば $(f, f') \neq k[X]$ である．しかしながら f は既約であって, かつ $(f) \subseteq (f, f')$ より $f' \in (f)$ であることが従う．ここで degree に注目すれば $f' = 0$ となる．

逆に, f は重根を持たないと仮定しよう. 上の補題によって等式 $(f, f') = k[X]$ が従うので, $f' \neq 0$ という結果が得られる. □

Definition 20. 環の準同型写像 $\varphi : \mathbb{Z} \to k$ を $\varphi(n) = n \cdot 1$ によって定める. この時, 0 又は正の整数 p を取って $\operatorname{Ker}\varphi = (p)$ と表すことができる. この p のことを, 体 k の標数と呼び, $p = \operatorname{char} k$ と表す. $\operatorname{char} k$ は 0 か又は素数である.

Corollary 1.12.4. 体 k がもし, $\operatorname{char} k = 0$ であるならば, 任意の既約多項式 $f \in k[X]$ は決して重根を持つことはない.

Definition 21. $k[X]$ の元 f が分離的 (*separable*) であるとは, $f \notin k$ であって更に $f = p_1 p_2 \cdots p_n$ を $k[X]$ 内の既約分解とした時 p_i が全て重根を持たないことをいう. 従って, $\operatorname{char} k = 0$ ならば $k[X]$ 内の既約多項式は全て分離的である.

さて, 定理を証明して, その幾つかの応用を述べてみよう.

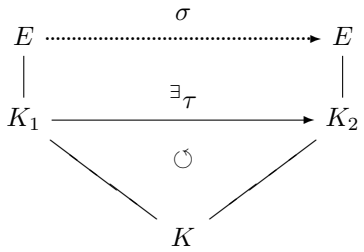
Proof of theorem. (1)⇒(2) $E = \sum_{i=1}^{\ell} K\alpha_i$ と表し, p_i によって α_i の K 上の最小多項式を表す. すると, p_i は E 内で 1 次式の積に分解していて, しかも決して重根を持たない. 従って, $f = p_1 p_2 \cdots p_\ell$ とすると E は K 上 f の分解体となっている.

(2)⇒(1) $f = c(X - \alpha_1)(X - \alpha_2)\cdots(X - \alpha_n)$ と表す. 但し, $n > 0$; $0 \neq c \in k$ であって $\alpha_i \in E$ とする. この時, 等式 $E = K[\alpha_1, \alpha_2, \cdots, \alpha_n]$ が成立する. さて, $t = \#\{1 \leq i \leq n | \alpha_i \notin K\}$ として, t についての induction によって, E/K が Galois 拡大であることを証明をしよう. $t = 0$ の時は, 全ての i について $\alpha_i \in K$ である. よって, $E = K$ で確かに E/K は Galois 拡大である. $t > 0$ で $t - 1$ 以下で正しいと仮定せよ. $\alpha = \alpha_1 \notin K$ としてよい. 今, $K_1 = K[\alpha]$ とおく時

$$\begin{array}{c} E \\ | \\ K_1 \\ | \\ K \end{array}$$

という体の拡大が得られ, E は K_1 上 f の分解体であって, q が K_1 上 f の irreducible component であれば $q|p$ であることから q は重根を持つことはない. 但し, p は K 上 f の irreducible component とする. 故に, f は K_1 上でも separable である. 勿論, $\#\{1 \leq i \leq n | \alpha_i \notin K_1\} < t$ より, t についての仮定から E/K_1 は Galois 拡大である. さて, $G = \operatorname{Gal}(E/K)$ とおく. $\operatorname{Gal}(E/K_1) \subseteq G$ であるので $K \subseteq E^G \subseteq E^{\operatorname{Gal}(E/K_1)} = K_1$ が従う. 今, $E^G \subseteq K$ を証明するために, 任意の元 $\theta \in E^G$ を取る. $\theta \in K_1$ であるから $\theta = \sum_{i=0}^{d-1} c_i \alpha_i$ と表せる. 但し, $d = [K_1 : K] > 1$, $c_i \in K$ である. そこで, α の K 上の最小多項式を p とおくと $p|f$ を満たすので, p は E 内で 1 次式の積に分解している. それを $p = (X - \beta_1)(X - \beta_2)\cdots(X - \beta_d)$ $(\beta_j \in E)$ と表す. 全ての

j について, β_j の K 上の最小多項式は p のままであるから, $\beta = \beta_j$ として $K_2 = K[\beta]$ とすると



但し, τ は環の準同型写像で全単射であって $\tau(\alpha) = \beta$ をみたす. $f \in K[X]$ より $f \in K_2[X]$ であって, f は E 内で 1 次式の積に分解していて, 更に, E は f の K_2 上の分解体でもある. よって, 分解体の一意性に従うと, τ は $\sigma \in \mathrm{Aut}\, E$ (実は $\sigma \in G$) に拡大される. 従って, 等式 $\theta = \sigma(\theta) = \sum_{i=0}^{d-1} c_i \beta^i$ が成り立ち, 故に, 多項式 $(c_0 - \theta) + c_1 X + c_2 X^2 + \cdots + c_{d-1} X^{d-1} = \xi(X) \in E[X]$ は, $\beta_1, \beta_2, \cdots, \beta_d$ を全て根に持つが, $\{\beta_j\}$ は distinct であるために, 等式 $\xi = 0$ が従う. 従って, $c_0 = \theta \in K$ となり, $E^G = K$ であって, E/K は Galois 拡大である. □

Definition 22. *E/K は体の拡大とする. E の元 α について, α は K 上代数的であって, 更に α の K 上の最小多項式が重根を持たない時, この α は K 上 separable であるという. そして, E の全ての元が K 上 separable である時, E/K は separable 拡大であるという.*

次の補題は非常に大切である.

Lemma 1.12.5. *E/K を体の拡大とする. $n > 0$ として, E の元 $\alpha_1, \alpha_2, \cdots, \alpha_n$ が全て K 上 separable であるならば, $K[\alpha_1, \alpha_2, \cdots, \alpha_n]$ は K 上 separable である. 実際, $K[\alpha_1, \alpha_2, \cdots, \alpha_n]$ を含む K の Galois 拡大体 F が存在する. 従って, $K[\alpha_1, \alpha_2, \cdots, \alpha_n]$ と K の間には中間体は有限個しか含まれていない.*

Proof. α_i の K 上の最小多項式を p_i として, 元 $f = p_1 p_2 \cdots p_n$ とおく. □