応用楕円曲線論　プリント No.4

情報科学科　金子　晃

第４章　有理函数体と因子

この章では，代数幾何の基本概念である，代数曲線上の有理函数体と，因子の話を，なるべく具体的に楕円曲線に特化して学びます．

§4.1 有理函数体と因子

因子の理論は，有理函数の零点と極を抽象化したもので，代数幾何学では非常に重要です．近頃は暗号への応用もあります．

$K = \boldsymbol{F}_q$ とし，K 上の楕円曲線 E を考えます (E の点は座標を K の閉体 $\overline{K}$ に持つのであったことに注意)．E の因子 (divisor) D とは，次のような形式和のことを言います．

$$D = \sum_{P \in E} n_P(P).$$

ここに，$n_P \in \boldsymbol{Z}$ で，かつ有限個を除き 0 とします．(代数幾何では，普通は (P) の代わりに単に P と書くのですが，ここでは後者を楕円曲線の成す群の元とみなしているので，区別するために因子の方を括弧で括っています.) 因子 D の台を

$$\operatorname{supp} D := \{P \in E \mid n_P \neq 0\}$$

で定義します．つまり，上の形式和に真に現れる点の全体で，これは因子の仮定により有限集合です．

因子の全体 $\boldsymbol{D}$ は自然な定義

$$\sum_{P \in E} n_P(P) + \sum_{P \in E} m_P(P) = \sum_{P \in E} (n_P + m_P)(P)$$

により，自由 Abel 群を成します．生成元は E の点が定める元 (P) の全体です．

因子 D の次数を

$$\deg D := \sum_{P \in E} n_P$$

で定義します．これは整数です．次数が 0 の因子の集合を $\boldsymbol{D}^0$ で表します．これは $\boldsymbol{D}$ の部分群となります．

E が標準形

$$r(x, y) := y^2 + a_1xy + a_3y - (x^3 + a_2x^2 + a_4x + a_6) = 0$$

で与えられているとき，E の K 上の座標環 (coordinate ring) を

$$K[E] := K[x, y]/(r(x, y))$$

で定義します．この記号は，２変数多項式環 $K[x, y]$ の $r(x, y)$ で生成されたイデアル $(r(x, y))$ による剰余環を表します．一言で言えは，この世界では，y^2 が出て来たら $r(x, y) = 0$ を使って $-a_1xy - a_3y + x^3 + a_2x^2 + a_4x + a_6$ で置き換えてしまうということです．$r(x, y)$ は既約なので，$(r(x, y))$ は素イデアルとなり，従って剰余環 $K[E]$ は整域となります．すなわち，零因子を持ちません．同様に

$$\overline{K}[E] := \overline{K}[x, y]/(r(x, y))$$

を定義します．上に注意したように y^2 を置き換える操作を続けると，遂には $K[E]$ の任意の元は

$$v(x) + yw(x)$$

の形の元で代表されることが分かります．

$K[E]$ の商体を $K(E)$ と記し，E の函数体 (function field) と呼びます．一般に，整域 I の商体は，I の二つの元 a, b, ただし $b \neq 0$ により，a/b と書かれるものの同値類の全体として定義されるのでした．同値関係は，小学生以来の約分規則で与えられます：

$$\frac{a_1}{b_1} = \frac{a_2}{b_2} \qquad \Longleftrightarrow \qquad a_1 b_2 = a_2 b_1.$$

演算の定義も通常の分数の場合と同じです．同様に, $\overline{K}[E]$ の商体 $\overline{K}(E)$ も定義されます．この元は E 上の有理函数と呼ばれます．$\overline{K}$ は $\overline{K}(E)$ の部分体となることに注意しましょう．これは, 定数値函数に相当します．

$f \in \overline{K}(E)^\times$ を零でない有理函数とし, $P \in E \setminus \{\mathcal{O}\}$ とします．f の表現 $g(x)/h(x)$, $g, h \in \overline{K}[E]$ で, $h(P) \neq 0$ となるものが存在するとき, f は P で定義されていると言い, $f(P) = g(P)/h(P)$ によりその値を定義します．この値は明らかに, f の分数としての (P で分母が零にならないような) 表現の選び方には依存しません．$f(P)$ が定義されていないときは, P は f の極であると言い，$f(P) = \infty$ と定めます．

例 4.1 標数が $2, 3$ のいずれでもない有限体 $K = \boldsymbol{F}_q$ 上の楕円曲線 $y^2 = x^3 - x$ を考える．$f = (x^2 - x)/y \in \overline{K}(E)$ と置く．$(1, 0)$ は E 上の点であるが，f を $\overline{K}^2$ 上の２変数有理函数とみなしたときは，f は点 P で $0/0$ の不定形となる．しかし，E 上の有理函数としては，

$$f = \frac{x^2 - x}{y} = \frac{(x^2 - x)y}{y^2} = \frac{(x^2 - x)y}{x^3 - x} = \frac{y}{x + 1}$$

と変形され，$f(P) = 0$ という確定した値を持つ．(一般に２次元以上の代数多様体上では，有理函数の値が $0/0$ の不定形になることは有るが，(特異点を持たない) 代数曲線上では，後述のように１次元の局所座標の存在が保証され，それによる表現から $0/0$ は有り得ないことが分かる．ただし，代数曲線でも特異点を持つと，例えば $y^2 = x^3$ 上の y/x のように，いくら表現を取り替えても $0/0$ から逃れられないものが存在する.)

次に，有理函数 f の無限遠点 $\mathcal{O}$ における値を定義するため，x に 2, y に 3 のウェイトを再び導入し，単項式の $\mathcal{O}$ における次数を

$$\mathrm{Deg}\, a x^i y^j = 2i + 3j$$

により，また，多項式 $g(x, y)$ の $\mathcal{O}$ における次数を f に含まれる各単項式の上の意味での次数の最大値と定めます．$f \in \overline{K}[E]$ は $v(x) + yw(x)$ の形に書き直されるので，これを用いると具体的に

$$\mathrm{Deg}(v(x) + yw(x)) = \max\{2 \deg v, 3 + 2 \deg w\}$$

と書くことができます．ただし，右辺の $\deg$ は１変数多項式としての通常の次数です．

さて，$f = g(x, y)/h(x, y) \in \overline{K}[x, y]/(r(x, y))$ に対し，$\mathrm{Deg}\, g > \mathrm{Deg}\, h$ なら $f(\mathcal{O}) = \infty$, $\mathrm{Deg}\, g < \mathrm{Deg}\, h$ なら $f(\mathcal{O}) = 0$ と定めます．$\mathrm{Deg}\, g = \mathrm{Deg}\, h$ のときは，両辺とも偶数か，両辺とも奇数であり，前者なら g, h の最高次の項は ax^d, bx^d の形，後者なら ayx^d, byx^d の形をしているので，いずれの場合も $f(\mathcal{O}) = a/b$ と定めます．これらの値は，実数体のときに無限遠点での極限値として定められた函数の値と同じものです．

例 4.2 楕円曲線 $y^2 = x^3 + ax + b$ 上の函数 $f = y$, $g = x/y$, $h = (x^2 - xy)/(1 + xy)$ に対しては，$f(\mathcal{O}) = \infty$, $g(\mathcal{O}) = 0$, また，$h(\mathcal{O}) = -1$ となる．

§4.2 局所パラメータ

楕円曲線 E 上の任意の点 P に対して，有理函数 $u \in \overline{K}(E)^\times$ で $u(P) = 0$ となるものを適当にとると，$\forall f \in \overline{K}(E)^\times$ が $f = u^d s$, $s(P) \neq 0, \infty$ の形に一意的に表されます．このような u を楕円曲線 E の点 P における一意化パラメータ，または，局所パラメータと呼びます．以下では簡単のため局所座標と呼ぶことにします．このような u の選び方は一意ではありませんが，それらのどれを用い

ても，任意の f について，上のように表現したときの d は f だけから一意的に定まります．実際，u と v をそのようなものとすれば，お互いに他方で表されなければならないので，$u = v^a s,\ v = u^b t,\ s(P) \neq 0,\ t(P) \neq 0$ となり，これより $u = u^{ab} s t^a$. u を u で表したときの表現の一意性から，$ab = 1$, 従って $a, b = \pm 1$ となりますが，$u(P) = v(P) = 0$ より $a = b = 1$ でなければならず，従って f を u，v のいずれで表しても冪指数は同じ値になります．

局所座標の存在証明は，次のように具体的に与えることができます．これは一般の代数曲線に対しても通用します：

定理 4.1 $P \in E$ を有限点とする．もし $u(x, y) := ax + by + c = 0$ が点 P を通り，かつ P における接線の方程式と一致しなければ，u は P における局所座標として使える．

証明 平行移動して $P(0, 0)$ としても一般性を失わない．(E の方程式は変化するが，$r(x, y) = y^2 + \cdots$ の形で，省略した部分が y の１次以下の式であることには変わりない.) このとき必然的に $c = 0$ となる．$r(x, y) = 0$ と $ax + by = u$ を連立させたとき，もし $b \neq 0$ ならば，後者を y について解いて前者に代入したものは $u = 0$ で $x = 0$ を単根に持つ (これが $u = 0$ が接線でないことと同値)．故に，

$$xg(x) + u^d\{h_0(x) + u^{d_1} h_1(x, u)\}, \qquad d \geq 1,\ \ d_1 \geq 1,\ \ g_0(0) \neq 0,\ \ h_0(x) \not\equiv 0$$

の形をしている．ここに，$h_1(x, 0) \not\equiv 0$ または $h_1(x, u) \equiv 0$ のいずれかである．従って，$h_0(0) \neq 0$ なら，

$$x = \Big\{ -\frac{h_0(x) + u^{d_1} h_1(x, u)}{g(x)} \Big\} u^d$$

で，$\{\ \}$ 内は $(0, 0)$ で零にならない x, y の有理函数となる．また，$h_0(0) = 0$ なら，$h_0(x) = x^e q_0(x)$, $e \geq 1$ と書け，従って，

$$x\{g(x) + x^{e-1} u^d q_0(x)\} + u^{d_1} h_1(x, u) = 0$$

となるが，このとき $h_1(x, u) \equiv 0$ だと，上の式より $(g(x) + x^{e-1} u^d q_0(x) \equiv 0$ では有り得ないから$)$ $x \equiv 0$ となり，不合理なので，$h_1(x, u) = h_1(x) + u^{d_2} h_2(x, u)$, $d_2 \geq 1$, $h_1(x) \not\equiv 0$ と分解される．よって，$h_1(0) \neq 0$ なら，

$$x\{g(x) + x^{e-1} u^d q_0(x)\} + u^{d+d_1}\{h_1(x) + u^{d_2} h_2(x, u))\} = 0$$

となり，x が P で零にならない函数 $\times\ u^{d+d_1}$ の形に書ける．もし $h_1(0) = 0$ なら上と同様, これを x で割った商を最初の項に繰り込むという操作を繰り返せば，$h(x, u)$ の u に関する展開が有限項で終わることから，必ず有限のステップで x が所与の形に表せる．これを $y = -\dfrac{u - ax}{b}$ に代入して同様に論ずれば，y も同じ形で表される．(今度は x を代入すると有理函数となるので, 打ち消しが起こって u のいくらでも高い冪が括り出せてしまう可能性が残るが, これは以下で一般の有理函数の表現を論ずるときに解決法が示される.)

そこで今，$x = u^d s,\ y = u^e t,\ d, e \geq 1,\ s(P) \neq 0,\ t(P) \neq 0$ と書けたとしよう. (d，e のどちらかは 1 に等しいことが $ax + by = u$ から分かるが，以下では特に使わない.) $\overline{K}[E]$ の元で, P において値が 0 となるものは, 明らかにイデアルを成し, その補集合, すなわち, P での値が $\neq 0$ のものの成す集合 S は，乗法的部分集合を成す．よって，S の元を分母に加える商環 $\overline{K}[E]_S$ が定義されるが，これを $\overline{K}[E]$ の P における局所化と呼ぶ．その理由は，こうして得られる環が，P での値が 0 となる元の成すイデアル I を唯一の極大イデアル，すなわち最大イデアルとして持つ，いわゆる局所環 (local ring) となるからである．有理函数が I に属するための必要十分条件は，それが $f(x, y)/g(x, y)$, $f(P) = 0$, $g(P) \neq 0$ という表示を持つとき，かつそのときに限るが，$f(P) = 0$ は，($P = (0, 0)$ としているので) x, y の定数項が無いこと，従って上の仮定により $f(x, y)$ がこの環の中で u で割り切れることである．よって，I は u で生成される $\overline{K}[E]_S$ のイデアルと一致する．以上により，$\overline{K}(E)$ の一般の元 $f(x, y)/g(x, y)$ について，$f = u^{d_1} c_1,\ g = u^{d_2} c_2,\ c_1(P) \neq 0,\ c_2(P) \neq 0$ と表示され，従って $f(x, y)/g(x, y) = u^{d_1 - d_2} c,\ c(P) = c_1(P)/c_2(P) \neq 0$ と表示される．ここで，$f(x, y) \not\equiv 0$ のとき，これが $\forall d > 0$ について u^d により環 $\overline{K}[E]_S$ の中で割り切れることが有ると (すなわち, 無限位の零点を持つものが有ると)，議論が破綻するが，これは形式的冪級数環を用いて解決する．以下その道筋を述べる．

一般に, 体 K 上の１変数 u の形式的冪級数環 $K[[u]]$ とは，

$$a_0 + a_1u + a_2u^2 + \cdots + a_iu^i + \cdots , \qquad a_i \in K$$

の形の形式和 (i.e. 収束は考慮しない；K が有限体のときは考慮の仕様も無い) に通常の加減乗算を導入して得られる環のことをいう．２変数の形式的冪級数環 $K[[x, y]]$ も

$$a_{00} + a_{10}x + a_{01}y + a_{20}x^2 + a_{11}xy + a_{02}y^2 + \cdots + a_{ij}x^iy^k + \cdots , \qquad a_{ij} \in K$$

で，同様に定義される．$\overline{K}[E]_S$ の元は，分母を等比級数展開することにより $\overline{K}[[x, y]]$ の部分環として埋め込める．例えば，

$$\frac{1}{1 + x + y^2} = 1 - (x + y^2) + (x + y^2)^2 - (x + y^2)^3 + \cdots = 1 - x + x^2 - y^2 - x^3 + 2xy^2 + \cdots$$

のように，各単項式の係数が下の方から順に定まってゆくので，形式的冪級数としては意味が付くのである．$x = u^ds$, $y = u^et$ は，$s, t \in \overline{K}[E]_S$ だったので，これに上の構成を適用すると，x, y の形式的冪級数として展開しては，出て来た x, y に $x = u^ds$, $y = u^et$ を代入するという操作を繰り返すと，遂には x, y が $\overline{K}[[u]]$ の元として表される．より詳しくは，$s, t \in \overline{K}[[u]]$ により $x = u^ds$, $y = u^et$ の形となる．以上により，$\overline{K}[E]_S \to \overline{K}[[u]]$ という写像が確定し，これは明らかに環の準同型となる．更に，前者のイデアル I には後者のイデアル (u) が対応する．後者においては，$\forall d > 0$ に対し u^d で割り切れるような元は，形式的冪級数のすべての係数が 0 となるので，定義により 0 となる．今もし，$f(x, y)$ について $f(x(u), y(u))$ が $\overline{K}[[u]]$ において 0 に等しいと，実は x, y の多項式として $f(x, y) \equiv 0 \mod r(x, y)$ でなければならないことが，次のようにして示せる (先に心配した y の表現可能性についても, 以下の議論の特別な例とみなせる)：上の条件を満たすような $f(x, y)$ の全体は $\overline{K}[x, y]$ の中でイデアル J を成す. $J \supset (r(x, y))$ であるが，この二つが一致することを言えばよい．もし一致しないと, 先の計算と同様, $\mod r$ で還元することにより, $v(x) + yw(x)$ の形の元がイデアル J に含まれることが言える. このとき, もし $w(x) \not\equiv 0$ なら, $r(x, y) = y^2 + Ay + B(x)$ とすれば，

$$\begin{aligned} &w(x)^2r(x, y) + (v(x) - yw(x) - Aw(x))(v(x) + yw(x)) \\ &= w(x)^2\{y^2 + Ay + B(x)\} - (w(x)^2y^2 - v(x)^2 - w(x)A(yw(x) + v(x)) \\ &= w(x)^2B(x)) + v(x)^2 - v(x)w(x) =: h(x) \end{aligned}$$

は x のみの多項式であるようなイデアル J の元となり、かつ r の既約性から, 恒等的に 0 とはなり得ない. しかし, このような元に対しては $h(x(u)) \equiv 0$ から $h(x) \equiv 0$ は容易に結論できる. 実際, $h(x) = x^ec(x)$, $c(0) \neq 0$ とすれば, $h(x(u)) = u^{de}c'(u)$, $c'(0) = s(0)^dc(0) \neq 0$ となることは明らかである. これは矛盾であるから．$J = (r(x, y))$, 従って $\overline{K}[E]_S \to \overline{K}[[u]]$ は単射なことが分かり，点 P での位数の定義が確定した．

最後に, $b = 0$ の場合を調べておこう. $ax = u$ となるが, $a \neq 0$ なので, 簡単のため u を取り換えて $x = u$ としよう. +++++

最後の議論は一般の平面代数曲線についても, 計算をもう少し抽象化すればほぼそのまま通用する. $u = ax + by$ において係数 $a \neq 0$ の場合も x と y の役割を入れ換えれば同様に議論できる. □

楕円曲線の場合は更に，次のように具体的に u の選び方を特定できます：

例 4.3 標数が $2, 3$ でない有限体 K 上の楕円曲線 $E : y^2 = x^3 + ax + b$ を考える．
$P = (c, d) \notin E[2]$ のとき P における E の接線は

$$(-3c^2 - a)(x - c) + 2d(y - d) = 0$$

ここで $d \neq 0$ なので，$u = x - c$ は接線ではないから，局所座標として使える．実際，$x - c = u$, また，$y^2 - d^2 = x^3 + ax + b - (c^3 + ac + b)$ より $y - d = \dfrac{x^2 + cx + c^2 + a}{y + d}u$ となる．

$P=(c,0)$ のとき　同じく P における E の接線は，$(-3c^2-a)(x-c)=0$ であり，従って $u=y$ が局所座標になる．このとき，非特異の仮定より $x=c$ は E の方程式の右辺の単根だから，E の方程式は $x=c$ の近くで $x-c=su^2,\ s(P)\neq 0,$ の形に解ける．

無限遠点における局所座標　同次座標に移行して考える：

$$Y^2Z=X^3+aXZ^2+Z^3$$

ここで，無限遠点では $Y\neq 0$ だから，Y^3 で両辺を割り，アフィン座標 $v=X/Y,\ w=Z/Y$ を導入すると

$$\frac{Z}{Y}=\Big(\frac{X}{Y}\Big)^3+a\frac{X}{Y}\Big(\frac{Z}{Y}\Big)^2+b\Big(\frac{Z}{Y}\Big)^3 \quad \therefore\ w=v^3+avw^2+w^3$$

無限遠点はこのアフィン座標で $(0,0)$ に対応する．そこでの接線（１次近似！）は上の方程式より，$w=0.$ 従って v は局所座標として採用できる．もとのアフィン座標では，$v=X/Y=x/y$ であり，無限遠点での重みが $3-2=1$ となっている．

$f\in\overline{K}(E)^\times,\ P\in E$ とし，P における局所座標 u を一つとるとき $f=u^ds,\ s(P)\neq 0$ となったとします．このとき f の P における位数は d であると言い，$\mathrm{ord}_P f=d$ で表します．P が f の零点となるのは $\mathrm{ord}_P f>0$ のとき，かつそのときに限り，この値が零点の位数となります．同様に，P が f の極となるのは $\mathrm{ord}_P f<0$ のとき，かつそのときに限り，この値の符号を変えたものが極の位数となります．有理函数は高々有限個の零点と極を持つので，f から因子

$$(f):=\sum_{P\in E}\mathrm{ord}_P f\cdot(P)$$

が定義されます．有理函数に関する基本事実は，この因子の次数が 0 となること，i.e. $(f)\in \boldsymbol{D}^0$ となることです．このことは一般の代数曲線で成り立つことですが，楕円曲線の場合には下の定理 4.2 で直接的に示します．

例 4.4　$K=\boldsymbol{F}_q,\ \mathrm{char}\,K\neq 2,3$ とし，K 上の楕円曲線 $E: y^2=x^3+ax+b$ を考える．

(i) $P=(c,d)\neq E[2]$ なら，

$$(x-c)=(P)+(-P)-2(\mathcal{O}).$$

実際，$\pm P$ では $u=x-c$ が局所座標としてとれ，また，$x-c$ は無限遠で２位の極を持つことが明らかです．

(ii) $P=(c,0)\in E[2]$ なら，

$$(x-c)=2(P)-2(\mathcal{O}).$$

この場合は $x-c$ は P で局所座標になりませんが，$u=y$ が局所座標となり，P は３重点ではないことから，$y^2=(x-c)g(x),\ g(c)\neq 0$ という表現より，$x-c=u^2/g(x)$ は P で位数２の 零点をもつことが分かります．無限遠では上と全く同じです．

(iii) $P_1,\ P_2,\ P_3$ を E の位数２の点のすべてとするとき，

$$(y)=(P_1)+(P_2)+(P_3)-3(\mathcal{O}).$$

実際，$y=0$ は位数２の点に対応しており，y は無限遠で３位の極を持っています．

(iv) より一般に，直線 $\lambda x+\mu y+\nu=0,\ \mu\neq 0$ が楕円曲線 E と３点 $P_1,\ P_2,\ P_3$ で交わるとき，

$$(\lambda x+\mu y+\nu)=(P_1)+(P_2)+(P_3)-3(\mathcal{O})$$

実際，これらの点では $u=\lambda x+\mu y+\nu$ が局所座標となります．この函数の無限遠点における極の位数は項 by の方で決まり，３です．

(v) $b\neq 0$ とし，$P_4=(0,\sqrt{b}),\ P_5=(0,-\sqrt{b})$ とすれば，

$$\Big(\frac{x}{y}\Big)=(P_4)+(P_5)+(\mathcal{O})-(P_1)-(P_2)-(P_3).$$

これは，分子の零点が P_4, P_5, 分母の y の零点が (ii) で与えられ，ここではそれらが極となることなどから分かります．

因子 $D \in \boldsymbol{D}^0$ は，ある $f \in \overline{K}(E)^\times$ について $D = (f)$ となるとき主因子 (principal divisor) であると言います．次の定理は楕円曲線上の因子について，それが主因子かどうかの便利な判定法を与えます，後の章で，主因子の f を見付ける効率的なアルゴリズムを与えます．

定理 4.2 $D = \sum_{P \in E} n_P(P)$ を因子とする．これが主因子であるための必要十分条件は，

$$\sum_{P \in E} n_P = 0, \qquad \sum_{P \in E} n_P P = \mathcal{O}. \tag{4.1}$$

一つ目の等式には、$\mathcal{O}$ の前の係数も関与しますが、二つ目の等式にはそれは無関係であることに注意しましょう.

証明 まず例 4.4 (iv) により x, y の１次式は上の２条件を満たしていることに注意せよ．一般に条件 (4.1) が必要なことを示すには，任意の主因子 (f) に含まれる因子から，$(P)+(Q)$ の形の対を選び出し，３点 P, Q, R で交わる直線 $l(x,y) = ax + by + c = 0$, $b \neq 0$ を取って，f を f/l で置き換えると，因子中の $(P)+(Q)$ が $-(R)+3(\mathcal{O})$ に減る．同様に，$(P)+(-P)$ の形の因子対は $x - c$ の形の因子で処理することにより $2(\mathcal{O})$ と取り換えることができる．この操作を繰り返すと，上の等式が二つとも成立するような有限個の１次因子 g_j を用いて，$(\frac{f}{\prod g_j}) = (P) + k(\mathcal{O})$, または $k(\mathcal{O})$ の形に帰着できる．ここに $k \in \boldsymbol{Z}$. しかし，楕円曲線上でこの形の主因子は存在しない. 実際，このような主因子 $(\frac{f}{g})$ が存在したとすると，もし $g \neq 1$ なら，代数的閉体 $\overline{K}$ において $r(x,y) = g(x,y) = 0$ の共通根が E のアフィン有限点に位数負の因子を生じさせ，上の形にはならないので，$g \equiv 1$. 次に，$r(x,y) = f(x,y) = 0$ の共通根が E のアフィン有限点に位数正の因子を生じさせるが．(厳密には Bézout の定理により) この共通根は，重複度を込めて少なくとも r の次数だけは存在するから，もし有限の台が P だけだと，P は３重点でなければならず，$3P$ の形でなければならない．よって，前者の形は有り得ず，後者の $k = 0$ の場合だけが可能性として残る．すなわち，$(f) = \sum(g_j)$ となり，(f) についても上の条件 (4.1) が成り立っていたことになる．

逆に，上の条件を満たす因子に対しては，同様に１次式の積で因子の対を取り崩してゆけば，主因子として実現できることが，(厳密には $\sum_{P \in E, P \neq \mathcal{O}} |n_P|$ に関する帰納法を用いて) 容易に示せる．□

上の定理の一般化として，どんな代数曲線上でも主因子の次数は 0 となることが知られています[1)]．従ってそれらは 0 と合わせて $\boldsymbol{D}^0$ の部分群 $\boldsymbol{D}^{pr}$ を成すことが容易に分かります．二つの因子 D_1, $D_2 \in \boldsymbol{D}^0$ は, ある $f \in \overline{K}(E)^\times$ により $D_1 = D_2 + (f)$ と書けるとき，同値であると言われ $D_1 \sim D_2$ と書かれます．同値類の集合は因子類群 (divisor class group) と呼ばれます．これは，商群 $\boldsymbol{D}^0/\boldsymbol{D}^{pr}$ に他なりません．これには Abel 多様体の構造が入ることが一般論で知られており，これを元の代数曲線の Jacobi 多様体と呼びます．

楕円曲線の場合には，因子類は E の点と一対一に対応します．すなわち，Jacobi 多様体が自分自身と同型です．実際，$\forall D = \sum_{P \in E} n_P(P) \in \boldsymbol{D}^0$ に対し，$Q = \sum_{P \in E} n_P P$ と置けば，$D - (Q) + (\mathcal{O})$ は上の定理の条件を満たし，従って主因子となるので，$D \sim (Q) - (\mathcal{O})$. また，もし $(Q) - (\mathcal{O}) \sim (Q') - (\mathcal{O})$ とすると，$(Q) - (Q') \sim 0$, 従って $(Q) - (Q')$ が主因子となってしまい，不合理です．(この証明も，上と同様，$(\frac{f}{g}) = (Q) - (Q')$ と置き，Bézout の定理を適用すれば，得られます.) よって，対応 $\sigma : D \mapsto Q$ は因子類群から楕円曲線への一対一対応となり，しかも明らかに Abel 群の準同型となります．

問題 4.1 有限体 $K = \boldsymbol{F}_7$ 上の楕円曲線 $y^2 = x^3 + 2$ 上の次の因子を計算せよ．また，同じ因子を１次函数の因子のみを用いて書け．

(1) $(x^2 - y)$ (2) $\dfrac{x^2 + y}{x^2 + y + 1}$ (3) $\dfrac{x^2 + x + 1}{x^2 + x + y}$

[1)] これは函数論でいわゆる偏角の原理を一般の Riemann 面に拡張したものに相当します.

【参考】 Bézout の定理　代数的閉体 K 上の m 次及び n 次の２変数多項式 $f(x,y)$, $g(x,y)$ が有るとき, これらの共通零点は重複度も込め, また無限遠点における交点も込めて mn 個存在する.
この定理の証明の概略は次の通り：

(0) **まず適当な射影変換で, 二つの曲線が無限遠点では交わらないように, また, それぞれが無限遠直線と有限個の点でしか交わらないようにする.**

(1) K^n **の適当なアフィン座標変換により, 両曲線とも** y **軸方向に無限遠点を持たないように, また** $f=0$ **は** x **軸方向に無限円点を持たず,** $g=0$ **の方は持つようにする. すると, 非零の定数因子の調節により, それぞれの方程式は,**

$$f(x,y)=y^m+a_1(x)y^{m-1}+\cdots+a_m(x),\qquad g(x,y)=y^n+b_1(x)y^{n-1}+\cdots+b_n(x)$$

の形にでき, ここで x **の多項式として**

$$\deg a_j\le j,\ j=1,\dots,m-1,\ \deg a_m<m,\ \deg b_j\le j,\ j=1,\dots,n-1,\ \deg b_n=n$$

となる. (実際, もし $\deg b_n<n$ **だと** x **軸方向の無限遠点が** $g=0$ **上に現れてしまうから.)**

(2) $f(x,y)=g(x,y)=0$ **を満たす点の** x **座標は, 終結式** $R(f,g)(x)$ **の根に他ならない. 上で仮定した形から,** $R(f,g)$ **の** x **の多項式としての次数はちょうど** mn **となることが,** $R(f,g)$ **の行列式による表現**

$$R(f,g)=\begin{vmatrix}
1 & a_1(x) & a_2(x) & \cdots & a_m(x) & 0 & \cdots & 0\\
0 & 1 & a_1(x) & a_2(x) & \cdots & a_m(x) & \ddots & \vdots\\
\vdots & \ddots & \ddots & \ddots & \ddots & & \ddots & 0\\
0 & \cdots & 0 & 1 & a_1(x) & a_2(x) & \cdots & a_m(x)\\
1 & b_1(x) & b_2(x) & \cdots & b_n(x) & 0 & \cdots & 0\\
0 & 1 & b_1(x) & b_2(x) & \cdots & b_n(x) & \ddots & \vdots\\
\vdots & \ddots & \ddots & \ddots & \ddots & & \ddots & 0\\
0 & \cdots & 0 & 1 & b_1(x) & b_2(x) & \cdots & b_n(x)
\end{vmatrix}$$

から容易に分かる.

(3) x_0 **が** $R(x,y)(x)=0$ **の** k **重根なら, 直線** $x=x_0$ **上には,** $f=0$, $g=0$ **の共通零点が重複度も込めてちょうど** k **個存在する. このことは, 終結式の元来の定義**

$$R(f,g)=\prod_{j=1}^{m}\prod_{k=1}^{n}(\alpha_j(x)-\beta_k(x))$$

から分かる. ここで $\alpha_j(x)$ **は** x **を固定したときの** $f(x,y)=0$ **の** y **に関する根を重複度だけ挙げたもの,** $\beta_k(x)$ **は同じく** $g(x,y)=0$ **のそれである.**

(1) **楕円曲線** $y^2=x^3+ax+b$ **と直線** $y=\lambda x+\mu$ **の交点は３個で** 3×1 **に等しい. 直線** $x=c$ **との交点は２個しか無いが, 残りの一つは無限遠点** $(0:1:0)$ **である.** (2) **実数体上, 二つの円** $x^2+y^2-x=0$ **と** $x^2+y^2+x=0$ **の交点は, アフィン平面内では円** $x^2+y^2-x=0$ **と直線** $x=0$ **の交点と同じで, 二つしかないが, 射影座標化すると** $x^2+y^2-xz=0$ **と** $x^2+y^2+xz=0$ **となり,** $x=0$ **の他に** $z=0$, $x^2+y^2=0$, **すなわち, 二つの無限遠虚点** $(1:\pm i:0)$ **が交点に含まれることが分かり, 総数は** $2\times2=4$ **と一致する. このように,** Bézout **の定理は, 代数的閉体でなければならないのはもちろんであるが, 射影平面にしないと成り立たない. 射影平面では位相幾何学における写像度の理論の特別な場合と解釈される. これは単独の１変数多項式の零点の個数についてもそうである.**