応用楕円曲線論　プリント No.5

情報科学科　金子　晃

第５章　割り算多項式と捻れ群の構造

この章では，楕円曲線の群演算をより詳細に見るとき必要となる割り算多項式の解説をし，それを用いて前章で証明を保留した捻れ群の構造に関する諸定理を導きます．

§5.1 割り算多項式の定義

割り算多項式とは，楕円曲線上の有限点 (x,y) の n 倍点の座標を x,y の有理函数で表したときに分母に現れる多項式のことです．その零点が n-捻れ点に対応することが直感的には明らかなので，これが捻れ群を調べるときに重要であることが理解できるでしょう．

【標数が $2,3$ 以外の場合の割り算多項式】　まず，簡単のため体 $\boldsymbol{F}_q$ の標数 $p \neq 2,3$ とし，標準形 $y^2 = x^3 + ax + b$ で与えられた $\boldsymbol{F}_q$ 上の楕円曲線について計算を行います．まず，

$$
\begin{aligned}
&\Psi_0(x,y) = 0,\\
&\Psi_1(x,y) = 1,\\
&\Psi_2(x,y) = 2y,\\
&\Psi_3(x,y) = 3x^4 + 6ax^2 + 12bx - a^2,\\
&\Psi_4(x,y) = 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3),\\
&\quad\vdots\\
&\Psi_{2n+1}(x,y) = \Psi_{n+2}\Psi_n^3 - \Psi_{n+1}^3\Psi_{n-1}, \quad (n \geq 2),\\
&\Psi_{2n}(x,y) = \Psi_n(\Psi_{n+2}\Psi_{n-1}^2 - \Psi_{n-2}\Psi_{n+1}^2)/2y, \quad (n \geq 3)
\end{aligned}
\tag{5.1}
$$

と置きます．$n = 5$ から先は猛烈にややこしくなってゆきます．Risa/Asir で計算した結果は

$$
\begin{aligned}
\Psi_5(x,y) =& -27x^{12} - 162ax^{10} - 324bx^9 - 297a^2x^8 - 1296abx^7 + (32y^4 - 108a^3 - 1296b^2)x^6\\
&- 1080a^2bx^5 + (160ay^4 + 99a^4 - 2592ab^2)x^4 + (640by^4 + 432a^3b - 1728b^3)x^3\\
&+ (-160a^2y^4 - 18a^5 + 432a^2b^2)x^2 + (-128aby^4 - 36a^4b)x + (-32a^3 - 256b^2)y^4 + a^6,\\
\Psi_6(x,y) =& \{-93x^{16} - 792ax^{14} - 1824bx^{13} - 2252a^2x^{12} - 11520abx^{11} + (96y^4 - 1640a^3 - 14304b^2)x^{10}\\
&- 16544a^2bx^9 + (672ay^4 + 1074a^4 - 46656ab^2)x^8 + (2304by^4 + 3840a^3b - 35328b^3)x^7\\
&+ (448a^2y^4 - 40a^5 - 8256a^2b^2)x^6 + (5376aby^4 + 2976a^4b - 23040ab^3)x^5\\
&+ ((-1216a^3 + 6912b^2)y^4 - 396a^6 + 6912a^3b^2 - 6144b^4)x^4\\
&+ (-3328a^2by^4 - 1536a^5b - 512a^2b^3)x^3\\
&+ ((-32a^4 - 3072ab^2)y^4 + 40a^7 - 1248a^4b^2 - 4608ab^4)x^2\\
&+ ((-256a^3b - 3072b^3)y^4 + 32ba^6 - 512a^3b^3 - 3072b^5)x + (32a^5 + 256a^2b^2)y^4\\
&+ 3a^8 + 64a^5b^2 + 256a^2b^4\} \times 2y
\end{aligned}
$$

補題 5.1　$\Psi_n(x,y)$ は n が奇数のとき，x, y^2 の整係数多項式，n が偶数のときは，x, y^2 の整係数多項式に $2y$ を掛けた形をしている．

証明 帰納法により示す．$n \le 4$ までは定義により成り立つ．そこで，$m \ge 2$ に対し，$n \le 2m$ まで成立しているとして，$n = 2m+1,$ でも成立することを示し，それを用いて更に $2m+2$ でも成立することを示そう．$m \ge 2$ なので，Ψ_{2m+1} の帰納的定義における右辺の $m+2 \le 2m$ となるので，右辺の各項には帰納法の仮定が使える．m が奇数のときは, 第１項の $\Psi_{m+2}\Psi_m^3$ については問題なく x と y^2 の Z 係数多項式となる．第２項 の $-\Psi_{m+1}^3\Psi_{m-1}$ については，$n \pm 1$ は偶数となるが，因子の数が 4 個なので $(2y)^4$ が生じ，やはり x と y^2 の Z 係数多項式となる．m が偶数のときも同様である．次に Ψ_{2m+2} の定義式の右辺を考察する．Ψ_{2m+1} では既に済んでいるので，この右辺に現れる最大の添え字 $(m+1)+2 \le 2m+1$ では成り立っており，帰納法の仮定が使える．$n = m+1$ として，n が偶数のときは，右辺の因子 Ψ_n，および括弧内の $\Psi_{n\pm2}$ からそれぞれ因子 $2y$ が生ずるので，$2y$ で割った後も因子 $2y$ が一つ残る．n が奇数のときも，同様に括弧内の $\Psi_{n\pm1}$ から $(2y)^2$ が出るので，同じ結論を得る．□

上の補題から，$\Psi_n(x,y)$ の中の y^2 を x^3+ax+b で次々に置き換えると，これは n が奇数なら そのまま，また n が偶数なら $2y$ を取り除いたものは，x のみの多項式となることが分かります．これらを $f_n(x)$ で表すと，次のことが成り立ちます：

定理 5.2 $P = (\overline{x}, \overline{y})$ を E の有限点とする.
(1) $P \in E[n] \iff \Psi_n(\overline{x}, \overline{y}) = 0.$
(2) $P \notin E[2]$ のときは，更に，$P \in E[n] \iff f_n(\overline{x}) = 0.$
(3) $P \notin E[n]$ なら，

$$nP = \Big(\overline{x} - \frac{\Psi_{n-1}\Psi_{n+1}}{\Psi_n^2}, \frac{\Psi_{n+2}\Psi_{n-1}^2 - \Psi_{n-2}\Psi_{n+1}^2}{4\overline{y}\Psi_n^3}\Big) \tag{5.2}$$

ここに，Ψ_n 等は $(\overline{x}, \overline{y})$ における値を表す．

証明 最後の公式は直接計算により示せる．あるいは，この形が体の標数に依らないことから，複素数体の場合にトーラスによる表現 $(\wp, \wp') : E \to \boldsymbol{T}^2 \simeq \boldsymbol{C}/\boldsymbol{Z}^2$ を用いて解析的に証明することもできる． ここでは，手計算と数式処理を混ぜた初等的な証明を試みる.

まず $n = 2$ のとき, 上の公式の右辺は

$$\begin{aligned}
&\Big(\overline{x} - \frac{3\overline{x}^4 + 6a\overline{x}^2 + 12b\overline{x} - a^2}{(2\overline{y})^2}, \frac{4\overline{y}(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3}{4\overline{y}(2\overline{y})^3}\Big) \\
=&\Big(\overline{x} - \frac{3\overline{x}^4 + 6a\overline{x}^2 + 12b\overline{x} - a^2)}{(2\overline{y})^2}, \frac{x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3}{(2\overline{y})^3}\Big)
\end{aligned}$$

を与えるが, 他方左辺は, ２倍公式より

$$\begin{aligned}
2P &= \Big((\frac{3\overline{x}^2 + a}{2\overline{y}})^2 - 2\overline{x}, -\frac{3\overline{x}^2 + a}{2\overline{y}}\big((\frac{3\overline{x}^2 + a}{2\overline{y}})^2 - 3\overline{x}\big) - \overline{y}\Big), \\
&= \Big(\overline{x} - \frac{12\overline{x}(\overline{x}^3 + a\overline{x} + b) - (3\overline{x}^2 + a)^2}{4\overline{y}^2}, \\
&\qquad \frac{(3\overline{x}^2 + a)\{12\overline{x}(\overline{x}^3 + a\overline{x} + b) - (3\overline{x}^2 + a)^2\} - 8(\overline{x}^3 + a\overline{x} + b)^2}{(2\overline{y})^3}\Big) \\
&= \Big(\overline{x} - \frac{3\overline{x}^4 + 6a\overline{x}^2 + 12b\overline{x} - a^2}{4\overline{y}^2}, \frac{\overline{x}^6 + 5a\overline{x}^4 + 20b\overline{x}^3 - 5a^2\overline{x}^2 - 4ab\overline{x} - a^3 - 8b^2}{(2\overline{y})^3}\Big)
\end{aligned}$$

よって一致する. 同様にして (5.2) が $n = 3, 4$ に対しても正しいことが数式処理ソフトを用いると確認できる.

今 (5.2) がある $n \ge 4$ まで正しいとする. $n = 2m$ が偶数のときは, $P_{n+1} = P_{2m+1} = P_m + P_{m+1}$ と見て, 帰納法の仮定と加法公式より

$$(2m+1)P = (\lambda^2 - (mP)_x - ((m+1)P)_x, \lambda((mP)_x - (\lambda^2 - (mP)_x - ((m+1)P)_x)) - \overline{y})$$

ここに,

$$\begin{aligned}\lambda &= \frac{(mP)_y - ((m+1)P)_y}{(mP)_x - ((m+1)P)_x} \\ &= \Big(\frac{\Psi_{m+2}\Psi_{m-1}^2 - \Psi_{m-2}\Psi_{m+1}^2}{4\overline{y}\Psi_m^3} - \frac{\Psi_{m+3}\Psi_m^2 - \Psi_{m-1}\Psi_{m+2}^2}{4\overline{y}\Psi_{m+1}^3}\Big) \Big/ \Big(\frac{\Psi_m\Psi_{m+2}}{\Psi_{m+1}^2} - \frac{\Psi_{m-1}\Psi_{m+1}}{\Psi_m^2}\Big) \\ &= \frac{\Psi_{m+1}^3(\Psi_{m+2}\Psi_{m-1}^2 - \Psi_{m-2}\Psi_{m+1}^2) - \Psi_m^3(\Psi_{m+3}\Psi_m^2 - \Psi_{m-1}\Psi_{m+2}^2)}{4\overline{y}\Psi_m\Psi_{m+1}(\Psi_m^3\Psi_{m+2} - \Psi_{m-1}\Psi_{m+1}^3)}\end{aligned}$$

よって

$$\begin{aligned}((2m+1)P)_x &= \Big(\frac{\Psi_{m+1}^3(\Psi_{m+2}\Psi_{m-1}^2 - \Psi_{m-2}\Psi_{m+1}^2) - \Psi_m^3(\Psi_{m+3}\Psi_m^2 - \Psi_{m-1}\Psi_{m+2}^2)}{4\overline{y}\Psi_m\Psi_{m+1}(\Psi_m^3\Psi_{m+2} - \Psi_{m-1}\Psi_{m+1}^3)}\Big)^2 \\ &\qquad - 2\overline{x} + \frac{\Psi_{m-1}\Psi_{m+1}}{\Psi_m^2} + \frac{\Psi_m\Psi_{m+2}}{\Psi_{m+1}^2} \\ &= \overline{x} - \frac{1}{16\overline{y}^2\Psi_m^2\Psi_{m+1}^2(\Psi_m^3\Psi_{m+2} - \Psi_{m-1}\Psi_{m+1}^3)^2} \\ &\qquad \times \Big(\{\Psi_{m+1}^3(\Psi_{m+2}\Psi_{m-1}^2 - \Psi_{m-2}\Psi_{m+1}^2) - \Psi_m^3(\Psi_{m+3}\Psi_m^2 - \Psi_{m-1}\Psi_{m+2}^2)\}^2 \\ &\qquad\quad - 48\overline{xy}^2\Psi_m^2\Psi_{m+1}^2(\Psi_m^3\Psi_{m+2} - \Psi_{m-1}\Psi_{m+1}^3)^2 \\ &\qquad\quad + 16\overline{y}^2(\Psi_{m-1}\Psi_{m+1}^3 + \Psi_m^3\Psi_{m+2})(\Psi_m^3\Psi_{m+2} - \Psi_{m-1}\Psi_{m+1}^3)^2\Big)\end{aligned}$$

他方, (5.2) の右辺は $n = 2m+1$ に対して,

$$\begin{aligned}((2m+1)P)_x &= \overline{x} - \frac{\Psi_{2m}\Psi_{2m+2}}{\Psi_{2m+1}^2} \\ &= \overline{x} - \frac{\Psi_m(\Psi_{m+2}\Psi_{m-1}^2 - \Psi_{m-2}\Psi_{m+1}^2)\Psi_{m+1}(\Psi_{m+3}\Psi_m^2 - \Psi_{m-1}\Psi_{m+2}^2)}{(\Psi_{m+2}\Psi_m^3 - \Psi_{m+1}^3\Psi_{m-1})^2}\end{aligned}$$

これらが一致することは, (5.2) の座標が楕円曲線の方程式を満たすという等式を用いて不要な $\overline{x}, \overline{y}$ を消去すれば確かめられる. y 座標の方は更に面倒だが, 数式処理ソフトの助けを借りれば遂行できる. $n+1 = 2m$ となるときも, 同様に $(n+1)P = 2(mP)$ と考えて帰納法に持ち込めばよい. 詳細は略す.

この公式を仮定すると，もし $\Psi_n(\overline{x}, \overline{y}) \neq 0$ なら，nP がアフィン有限点として定まるので，対偶を取れば，$(\overline{x}, \overline{y}) \in E[n]$ なら $\Psi_n(\overline{x}, \overline{y}) = 0$ でなければならない．(補題 5.1 により，nP の y 座標成分の分母の y は分子を割り切っていることに注意.) $n \neq 2$ のときは, $\overline{y} \neq 0$ なので，$\Psi_n(x, y)$ から更に $2y$ を括り出した $f_n(x)$ で判定できる．□

上の公式における nP の x 座標の分母の $\Psi_n(x,y)^2$ は，n が奇数のときはそのまま，また n が偶数のときも，因子 y が y^2 にまとまるので，いずれの場合も楕円曲線の方程式 $r(x,y) = 0$ を用いて x のみの多項式に書き換えられます．よって以下これを $\Psi_n^2(x)$ で表すことにします[1)]．また，nP の x 座標を通分したものの分子

$$x\Psi_n(x,y)^2 - \Psi_{n-1}(x,y)\Psi_{n+1}(x,y)$$

も，同じく n の偶奇に拘らず因子 y がすべて y^2 にまとまるので，x の多項式となることが容易に分かります．よって以下これを $\Phi_n(x)$ で表します．

補題 5.3 $\Phi_n(x)$, $\Psi_n^2(x)$ の最高次の項は次の形をしている：

$$\Phi_n(x) = x^{n^2} + \text{低階項}, \qquad \Psi_n^2(x) = n^2 x^{n^2-1} + \text{低階項}$$

[1)] この記号は紛らわしいが, $\Psi_n^2(x)$ は y^2 に x の 3 次式を代入した結果なので, x の多項式としては完全平方ではない.

証明　まず, n **に関する帰納法で次が初等的に示せる：**

$$\Psi_n(x)=\begin{cases} y(nx^{(n^2-4)/2}+\cdots), & n \text{ が偶数のとき},\\ nx^{(n^2-1)/2}+\cdots, & n \text{ が奇数のとき}. \end{cases}$$

実際，これらは (5.1) **を見ると** $n\le 4$ **までは成り立っている．そこで今，**$n\le 2m$, $m\ge 2$ **で上が成り立っていると仮定し，**$2m+1$, $2m+2$ **のときにも成り立つことを示そう．**m **が偶数のとき**

$$\begin{aligned}
\Psi_{2m+1}(x,y)&=\Psi_{m+2}\Psi_m^3-\Psi_{m+1}^3\Psi_{m-1}\\
&=y((m+2)x^{((m+2)^2-4)/2}+\cdots)\{y(mx^{(m^2-4)/2}+\cdots)\}^3\\
&\quad-\{(m+1)x^{((m+1)^2-1)/2}+\cdots\}^3\{(m-1)x^{((m-1)^2-1)/2}+\cdots\}\\
&=m^3(m+2)(x^3+\cdots)^2(x^{2m^2+2m-6}+\cdots)-(m+1)^3(m-1)(x^{2m^2+2m}+\cdots)\\
&=(2m+1)(x^{2m^2+2m}+\cdots)=(2m+1)x^{((2m+1)^2-1)/2}+\cdots,\\
\Psi_{2m+2}(x,y)&=\Psi_{m+1}(\Psi_{m+3}\Psi_m^2-\Psi_{m-1}\Psi_{m+2}^2)/2y\\
&=(m+1)(x^{((m+1)^2-1)/2}+\cdots)[(m+3)(x^{((m+3)^2-1)/2}+\cdots)\{y(mx^{(m^2-4)/2}+\cdots)\}^2\\
&\qquad-(m-1)(x^{((m-1)^2-1)/2}+\cdots)\{y((m+2)x^{((m+2)^2-4)/2}+\cdots)\}^2]/2y\\
&=\frac{y}{2}(m+1)(x^{(m^2+2m)/2}+\cdots)\\
&\quad\{(m+3)m^2(x^{(3m^2+6m)/2}+\cdots)-(m-1)(m+2)^2(x^{(3m^2+6m)/2}+\cdots)\}\\
&=y((2m+2)x^{(2m+2)^2-4)/2}+\cdots)
\end{aligned}$$

m **が奇数のとき**,

$$\begin{aligned}
\Psi_{2m+1}(x,y)&=\Psi_{m+2}\Psi_m^3-\Psi_{m+1}^3\Psi_{m-1}\\
&=((m+2)x^{((m+2)^2-1)/2}+\cdots)\{(mx^{(m^2-1)/2}+\cdots)\}^3\\
&\quad-\{y(m+1)x^(m+1)^2-4)/2+\cdots\}^3\{y(m-1)x^(m-1)^2-4)/2+\cdots\}\\
&=m^3(m+2)(x^{2m^2+2m}+\cdots)-(m+1)^3(m-1)(x^3+\cdots)^2(x^{2m^2+2m-6}+\cdots)\\
&=(2m+1)(x^{2m^2+2m}+\cdots)=(2m+1)x^{((2m+1)^2-1)/2}+\cdots\\
\Psi_{2m+2}(x,y)&=\Psi_{m+1}(\Psi_{m+3}\Psi_m^2-\Psi_{m-1}\Psi_{m+2}^2)/2y\\
&=y\{(m+1)x^{((m+1)^2-4)/2}+\cdots\}[y\{(m+3)x^{((m+3)^2-4)/2}+\cdots\}\{mx^{(m^2-1)/2}+\cdots\}^2\\
&\quad-y\{(m-1)x^{((m-1)^2-4)/2}+\cdots\}\{(m+2)x^{((m+2)^2-1)/2}+\cdots\}^2]/2y\\
&=\frac{y}{2}\{(m+1)x^{((m+1)^2-4)/2}+\cdots\}[\{(m+3)m^2-(m-1)(m+2)^2\}x^{3(m+1)^2/2}+\cdots]\\
&=2y((m+1)x^{2(m+1)^2-2}+\cdots)=y((2m+2)x^{((2m+2)^2-4)/2}+\cdots)
\end{aligned}$$

これらから Ψ_n^2 **の表現は直ちに出る．**Φ_n **についても，**n **が奇数のときは，**

$$\begin{aligned}
&x\Psi_n(x,y)^2-\Psi_{n-1}(x,y)\Psi_{n+1}(x,y)\\
&=x\{n^2x^{(n^2-1)}+\cdots\}-y^2\{(n+1)(n-1)x^{(n^2+2n-3+n^2-2n-3)/2}+\cdots\}\\
&=n^2x^{n^2}+\cdots-(x^3+\cdots)\{(n^2-1)x^{n^2-3}+\cdots\}=x^{n^2}+\cdots
\end{aligned}$$

また，n **が偶数のときは，**

$$\begin{aligned}
&x\Psi_n(x,y)^2-\Psi_{n-1}(x,y)\Psi_{n+1}(x,y)\\
&=xy^2n^2\{x^{n^2-4}+\cdots\}-\{(n+1)(n-1)x^{(n^2+2n+n^2-2n)/2}+\cdots\}\\
&=\{x^3+\cdots\}n^2x\{x^{n^2-4}+\cdots\}-(n^2-1)x^{n^2}+\cdots=x^{n^2}+\cdots
\end{aligned}$$

□

補題 5.4 有限体 $K = \boldsymbol{F}_q$ 上定義された楕円曲線 $E : y^2 = x^3 + ax + b$ の群の準同型写像 α は

$$(x, y) \in E \text{ に対し } \alpha(x, y) = (r_1(x), yr_2(x)) \tag{5.3}$$

の形をしている．ここに，$r_1(x)$, $r_2(x)$ は x の有理函数である．$r_1'(x) \not\equiv 0$ のとき α は分離的と呼ばれる．この条件は $r_1(x) = \dfrac{p(x)}{q(x)}$ と既約分数で表したとき，$p'(x)$, $q'(x)$ の少なくとも一方が 0 多項式とならないことと同値である．

証明 群準同型は有理写像なので，

$$\alpha(x, y) = \Big(\frac{f_1(x, y)}{g_1(x, y)}, \frac{f_2(x, y)}{g_2(x, y)}\Big)$$

と書ける．ここで，多項式 f_j, g_j は E の方程式 $r(x, y) = y^2 - x^3 - ax - b = 0$ を用いて, それぞれ $v_j(x) + y\widetilde{v}_j(x)$, $w_j(x) + y\widetilde{w}_j(x)$ の形に書き直せるが，更に，いわゆる“ 分母の有理化 ”技法で

$$\frac{v_1(x) + y\widetilde{v}_1(x)}{w_1(x) + y\widetilde{w}_1(x)} = \frac{(v_1(x) + y\widetilde{v}_1(x))(w_1(x) - y\widetilde{w}_1(x))}{w_1(x)^2 - y^2\widetilde{w}_1(x)^2}$$

とし，再び $r(x, y) = 0$ を用いて y^2 を x の多項式に書き換えると，結局

$$\alpha(x, y) = (r_1(x) + ys_1(x), s_2(x) + yr_2(x))$$

の形に帰着できる．ここに，r_j, s_j は x の有理函数である．(記号の使い方が対称でないのは, 最後まで残る方に文字 r を割り当てたからである.) ここで α が群の準同型であることを用いると，

$$\alpha(x, -y) = \alpha[-(x, y)] = -\alpha(x, y),$$

従って

$$(r_1(x) - ys_1(x), s_2(x) - yr_2(x)) = (r_1(x) + ys_1(x), -s_2(x) - yr_2(x))$$

これから，$s_1(x) \equiv 0$, $s_2(x) \equiv 0$ が得られ，上の形となる．

最後に，$r_1(x) = \dfrac{p(x)}{q(x)}$ とすれば，

$$r_1'(x) = \frac{p'(x)q(x) - p(x)q'(x)}{q(x)^2} \equiv 0$$

とすると，もし $q'(x) \not\equiv 0$ なら，$\dfrac{p(x)}{q(x)} = \dfrac{p'(x)}{q'(x)}$ となり，$\deg p' < \deg p$, $\deg q' < \deg q$ なので，この表現が既約分数であったことに反する．また，$q'(x) \equiv 0$ なら，$q(x) \not\equiv 0$ により上の式から $p'(x) \equiv 0$ でなければならない．よって対偶を取れば上が成り立つ．□

命題 5.5 楕円曲線 $E = E(\overline{K})$ の非自明な自己準同型は必ず全射となる.

証明 $\alpha = (r_1(x), yr_2(x)) : E \to E$ を群の準同型とする. $\alpha(\mathcal{O}) = \mathcal{O}$ は確かに α の像に入るので, $E \ni \forall P(x_1, y_1) \neq \mathcal{O}$ をとる. $r_1(x) = \dfrac{p(x)}{q(x)}$ とする。もし $p(x) - x_1q(x)$ が定数でなければ, 根 x_0 を持つ. p, q は互いに素としているので, $q(x_0) \neq 0$ である. よって, $r_1(x) = \dfrac{p(x)}{q(x)} = x_1$ の根 x_0 が求まった. $yr_2(x_0)$ から直接 y を求めるには $r_2(x_0) \neq 0$ の情報が必要となるので, $y^2 = x_0^3 + ax_0 + b$ から y_0 を求めると, $(x_0, y_0) \in E$ なので, $\alpha(x_0, y_0) = (x_1, y_2) \in E$ なる y_2 が有り, $y_2^2 = x_1^3 + ax_1 + b = y_1^2$. $y_2 = y_1$ なら逆像が求まった. $y_2 = -y_1$ のときは, $\alpha(x_0, -y_0) = -\alpha(x_0, y_0) = -(x_1.y_2) = (x_1, -y_2) = (x_1, y_1)$ により, やはり逆像が求まる.

最後に, $p(x) - x_1q(x)$ が定数となるときを考える. $\operatorname{Ker}\alpha$ は高々有限個の点より成るので, 任意の点の逆像も高々有限個, 従って p, q のどちらか一方は定数ではない. このとき, 容易に分かるように,

$p(x)-x_1q(x)\equiv 0$ を満たすような定数は一つしかない．従って，x_1 以外の値 x_2 については既に示したように，$\forall(x_2,y_2)\in E$ は α の像となる．よって問題はただ $(x_1,\pm y_1)\in E$ が α の像となるかどうかだけである．E は無限個の点を含むので，$(x_2,y_2)\in E$ を $(x_1,\pm y_1)$ と異なり，かつ $(x_2,y_2)+(x_1,y_1)$ も $(x_1,\pm y_1)$ と異なるように選べる．仮定により $\alpha(P)=(x_2,y_2)$, $\alpha(Q)=(x_3,y_3)$ なる点は存在するから，(x_1,y_1) は群準同型 α による $Q-P$ の像となる．このとき $(x_1,-y_1)$ も $-(Q-P)$ の像となる．□

楕円曲線の射は，平行移動の分を取り去れば必ず群の準同型となることが知られているのでした．平行移動では全射性は変わらないので，このことから，非自明な射はすべて全射なことも分かります．

以後，E の群準同型 α を (5.3) の形に表現したとき，そこに現れる有理函数既約分数表示 $r_1=\dfrac{p(x)}{q(x)}$ を用いて

$$\deg\alpha=\deg r_1:=\max\{\deg p,\deg q\}$$

と定義し，α の次数と呼びます．($\deg r_1$ とも書きましたが，これは普通に使われる有理函数の次数 $\deg p-\deg q$ とは異なることに注意してください．)

命題 5.6 α を分離的な群の準同型とすれば，

$$\#\mathrm{Ker}\,\alpha=\deg\alpha.$$

また α が非分離的なら，

$$\#\mathrm{Ker}\,\alpha<\deg\alpha.$$

証明 まず分離的と仮定すると，その定義により $p'q-pq'\not\equiv 0$. そこで

$$S:=\{x\in\overline{K}\mid (p'(x)q(x)-p(x)q'(x))q(x)=0\}$$

と置けば，これは有限集合となる．今，$(x_0,y_0)\in E$ を

(1) $x_0\neq 0$, $y_0\neq 0$, $(x_0,y_0)\neq\mathcal{O}$.
(2) $\deg(p-x_0q)=\max\{\deg p,\deg q\}$.
(3) $x_0\notin r_1(S)$.
(4) $(x_0,y_0)\in\alpha(E)$.

となるように選ぶ．これが可能なことは，$r_1(\overline{K})$ が無限集合となることに注意すれば容易に分かる．

$\alpha(x,y)=(x_0,y_0)$ を満たす点 $(x,y)\in E$ がちょうど $\deg\alpha$ 個存在することを示そう．$(x_0,y_0)\neq\mathcal{O}$ より，$q(x)\neq 0$, また $(x,y)\neq\mathcal{O}$ である．方程式

$$\frac{p(x)}{q(x)}=x_0,\qquad yr_2(x)=y_0$$

において，x が決まれば，$y_0\neq 0$ より y は第２式から一意に決まるので[2)]，第１の方程式の x に関する解の個数を数えればよい．すなわち，$p(x)-x_0q(x)=0$ の根の個数を調べればよい．仮定の (2) により根は重複度を込めてちょうど $\deg\alpha$ 個なので，重根が無いことを言えばよいが，それには，

$$p'(x)-x_0q'(x)=0$$

と連立させて矛盾を出せばよい．この二つから

$$0=p'(x)-\frac{p(x)}{q(x)}q'(x)=\frac{p'(x)q(x)-p(x)q'(x)}{q(x)}$$

となるが，これは $x\in S$, 従って $x_0=r_1(x)\in r_1(S)$ を意味し，仮定の (3) に矛盾する．

[2)] $r_2(x)=0$ となると，(x_0,y_0) が α の像に入らないという結論になりそうにも見えるが，前命題により全射が証明されているのでそれはない．

以上により，少なくともある点の逆像がちょうど $\deg\alpha$ 点より成ることが分かったが，α は群の準同型なので，$\mathrm{Ker}\,\alpha$, すなわち $\mathcal{O}$ の逆像も結局同じ個数の点よりなる．

次に, 分離的でない場合は，上と同じ証明で，$p'(x)-x_0q'(x)\equiv 0$, 従って方程式 $p(x)-x_0q(x)=0$ は必ず重根を持つので, $\mathrm{Ker}\,\alpha$ の元の個数は $\deg\alpha$ よりも真に小さくなる． □

補題 5.7 楕円曲線 $E: y^2=x^3+ax+b$ の n 倍写像は次数 n^2 となる．

証明 補題 5.3 と命題 5.6 の直前に与えた次数の定義により，$\dfrac{\Phi(x)}{\Psi^2(x)}$ が既約なことを言えば, この写像の次数は $\max\{\deg\Phi(x),\Psi^2(x)\}=\deg\Phi(x)=n^2$ となる．(このことは $p\mid n$ のときも成り立つことに注意.) 既約性の証明は, 初等的だが大変長いので, 詳細は略す.

系 5.8 n が体の標数 p と互いに素なら，$E[n]=\boldsymbol{Z}_n\oplus\boldsymbol{Z}_n$.

証明 補題 5.3 と仮定により，$\Phi'(x)$ は最高次の係数 n^2 が零でないので, 零多項式ではない. よって n 倍写像は分離的となり, 命題 5.6 と前補題より $\#E[n]=n^2$, また，Abel 群の一般構造定理により，

$$E[n]=\boldsymbol{Z}_{n_1}\oplus\boldsymbol{Z}_{n_2}\oplus\cdots\oplus\boldsymbol{Z}_{n_s},\qquad \text{ここに}\ \ n_1\mid n_2\mid\cdots\mid n_s$$

と書けていた．従って $n_1n_2\cdots n_s=n^2$. ここで，$\ell\mid n_1$ を任意の素因子とすれば，$\ell\mid\forall n_i$, よって $\ell^s\mid n^2$. 特に, $\ell\mid n^2$, 従って $E[\ell]\subset E[n]$ なので，上の式から

$$E[\ell]=E[n][\ell]=(\boldsymbol{Z}_{n_1}\oplus\boldsymbol{Z}_{n_2}\oplus\cdots\oplus\boldsymbol{Z}_{n_s})[\ell],\quad \text{また}\ \ \#E[\ell]=\ell^2.$$

ところで，一般に $\ell\mid m$ のとき，$\boldsymbol{Z}_m[\ell]\simeq\boldsymbol{Z}_\ell$ が成り立つことに注意しよう．実際，$m=k\ell$ とすれば，$\boldsymbol{Z}_m$ の位数 ℓ を持つ元は $0,\,k,\,2k,\,\ldots,\,(\ell-1)k$ で尽くされる．よって，上の式の右辺は $\boldsymbol{Z}_\ell^s$ に同型となり，位数 ℓ^s となるから，$s=2$ と結論できる．よって $E[n]\simeq\boldsymbol{Z}_{n_1}\oplus\boldsymbol{Z}_{n_2}$. しかし，$E[n]$ の元はいずれも位数が n の約数なので，$n_2\mid n$ でなければならず，これと $n_1n_2=n^2$ とから $n_1=n_2=n$ と結論される． □

$E[n]$ の構造が定まったところでこの節の主目標は達せられましたが, 後に必要となる性質を若干用意しておきましょう.

補題 5.9 (u,v) を定数と見て, E 上の加法の意味で $(x,y)+(u,v)=(f(x,y),g(x,y))$ と有理函数で表すとき,

$$\frac{\frac{d}{dx}f(x,y)}{g(x,y)}=\frac{1}{y}$$

が成り立つ. ここで $\dfrac{d}{dx}$ は y が $y^2=x^3+ax+b$ により x に従属しているとみなした常微分である.

証明 具体的計算による.

$$f(x,y)=\Big(\frac{y-v}{x-u}\Big)^2-x-u,\ \ g(x,y)=\frac{-(y-v)^3+x(y-v)(x-u)^2+2u(y-v)(x-u)^2-v(x-u)^3}{(x-u)^3}$$

より, $2y\dfrac{dy}{dx}=3x^2+a$, 及び $y^2-v^2=x^3-u^3+a(x-u)$ に注意して,

$$\begin{aligned}
\frac{d}{dx}f(x,y)&=2\frac{y-v}{x-u}\frac{\frac{dy}{dx}(x-u)-(y-v)}{(x-u)^2}-1\\
&=\frac{y-v}{y(x-u)^3}(3x^2+a)(x-u)-2\frac{(y-v)^2}{(x-u)^3}-1\\
&=\frac{y-v}{y(x-u)^3}\Big(3x^2(x-u)+y^2-v^2-x^3+u^3)\Big)-2\frac{(y-v)^2}{(x-u)^3}-1\\
&=\frac{y-v}{y(x-u)^3}\Big((x-u)(2x^2-ux-u^2)+(y-v)^2+2v(y-v)-2y(y-v)\Big)-1\\
&=\frac{(y-v)\{-(y-v)^2+(x-u)^2(2x+u)\}-y(x-u)^3}{y(x-u)^3}=\frac{g(x,y)}{y}
\end{aligned}$$

$\mathbb{Q}$ 上の主張は $\dfrac{dx}{y}$ が楕円曲線の平行移動で不変な微分形式であることを意味します．このことは，複素数体上の楕円曲線のときには，$x=\wp(z)$, $y=\wp'(z)$ という変換で $\boldsymbol{C}/(\boldsymbol{Z}\omega_1+\boldsymbol{Z}\omega_2)$ の上に移してみたとき，

$$\frac{dx}{y}=\frac{d\wp(z)}{\wp'(z)}=\frac{\wp'(z)dz}{\wp'(z)}=dz$$

となることから理解できます．

補題 5.10 $\alpha_j, j=1,2,3$ を E の準同型で，$\alpha_3=\alpha_1+\alpha_2$, かつ，それぞれ有理函数により $(r_j(x), ys_j(x))$ と表現されているとする．もし $\dfrac{r_j'}{s_j}=c_j$, $j=1,2$ が定数なら，$\dfrac{r_3'}{s_3}=c_1+c_2$ となる．

証明 $(x,y)\in E$ とし $\alpha_j(x,y)=(x_j,y_j)$ と置くと，前補題より

$$\frac{\partial x_3}{\partial x_1}=\frac{y_3}{y_1},\qquad \frac{\partial x_3}{\partial x_2}=\frac{y_3}{y_2}$$

(ここで偏微分はそれぞれ x_2 あるいは x_1 を定数とみなすものである.) 仮定により

$$\frac{\partial x_j}{\partial x}=c_j\frac{y_j}{y},\quad j=1,2.$$

よって合成函数の偏微分公式により

$$\frac{dx_3}{dx}=\frac{\partial x_3}{\partial x_1}\frac{\partial x_1}{\partial x_1}+\frac{\partial x_3}{\partial x_2}\frac{\partial x_2}{\partial x_1}=\frac{y_3}{y_1}c_1\frac{y_1}{y}+\frac{y_3}{y_2}c_2\frac{y_2}{y}=(c_1+c_2)\frac{y_3}{y}=(c_1+c_2)s_3.\qquad\square$$

補題 5.11 E の n 倍写像の有理函数による表現を $(r_n(x), ys_n(x))$ とすれば，$\dfrac{r_n'(x)}{s_n(x)}=n$ が成り立つ．よって，n 倍写像は $p\nmid n$ のとき，かつそのときに限り分離的である．

証明 n 倍写像は群の準同型なので $-nP=n(-P)$, 従って $r_{-n}(x)=r_n(x)$, $s_{-n}(x)=-s_n(x)$ を満たす．よって $\dfrac{r_{-n}'(x)}{s_{-n}(x)}=-\dfrac{r_n'(x)}{s_n(x)}$ だから，$n>0$ のときに言えばよい．$n=1$ のときは $r_1(x)=x$, $s_1(x)=1$ なので明らかである．よって，前補題により $2=1+1$ 以下，帰納的にすべての n で成り立つ．$\square$

さて，E の勝手な準同型 α は $T\in E[n]$ に対して $n\alpha(T)=\alpha(nT)=\alpha(\mathcal{O})=\mathcal{O}$ により，$E[n]$ に作用しますが，系 5.8 により，そこでの作用は $\boldsymbol{Z}_n\oplus\boldsymbol{Z}_n$ の生成元の対 T_1,T_2 を一つ決めると２次の行列で表されます：実際，$\alpha(T_1)=aT_1+cT_2$, $\alpha(T_2)=bT_1+dT_2$ なので，

$$\alpha([T_1,T_2]\begin{pmatrix}x\\y\end{pmatrix})=\alpha(xT_1+yT_2)=x\alpha(T_1)+y\alpha(T_2)=[T_1,T_2]\begin{pmatrix}a&b\\c&d\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}$$

以下，生成元の対を言葉の乱用で単に基底と呼ぶことにします．この行列の性質を調べるため，Weil ペアリングを使う必要があります．そこで次の節でその定義と基本性質を導入します．

§5.2 Weil ペアリング

Weil ペアリングは楕円曲線の暗号への応用上常に重要な役割を果たしてきました．ここでは概念を定義し，その簡単な性質を調べて，楕円曲線の群構造の解明に用います．

E を $K=\boldsymbol{F}_q$ 上の楕円曲線とし，K の標数 p と互いに素な正整数 n を取ります．まず，有理函数 $f\in\overline{K}(E)^\times$ の因子 $D=\sum n_P(P)$ における値を

$$f(D)=\prod_{P\in\operatorname{supp}D}f(P)^{n_P}$$

で定義します. これは (f) と D の台が交わらないとき, 0 でない有限の値を持ちます. D が次数 0 の因子, すなわち $\sum n_P = 0$ のときは, 上の値は f をその非零定数倍と取り換えても不変なことに注意しましょう.

次に,

$$\mu_n := \{x \in \overline{K} \mid x^n = 1\}$$

は, $\mathrm{GCD}\,(n,p) = 1$ より, n 個の異なる元より成ります. 巡回群 $\overline{K}^\times$ の部分群として, μ_n も巡回群となり, 従って生成元 ζ_n が存在します. これがいわゆる 1 の原始 n 乗根です.

$P, Q \in E[n]$ に対し,0 次の因子 A, B を $A \sim (P) - (\mathcal{O})$, $B \sim (Q) - (\mathcal{O})$, かつ台が交わらないように任意選びます. (このことは $P = Q$ の場合も可能なことに注意しましょう.) 仮定により $nP = \mathcal{O}$, $nQ = \mathcal{O}$ なので, $nA = n(P) - n(\mathcal{O})$ から, $nP - n\mathcal{O} = \mathcal{O} - \mathcal{O} = \mathcal{O}$ 等となり, nA, nB は定理 4.2 の条件を満たし, 従って

$$(f_A) = nA, \quad (f_B) = nB$$

なる有理函数 $f_A, f_B \in \overline{K}(E)$ が存在します. (f_A) と B, (f_B) と A も台は交わらないことに注意しましょう. 以上により, $\dfrac{f_A(B)}{f_B(A)}$ という値を考えることができますが, 以下で示すようにこの値は 1 の n 乗根となり, かつ A, B の選び方によりません. よって

$$\begin{array}{rccc} e_n: & E[n] \times E[n] & \longrightarrow & \mu_n \\ & \cup & & \cup \\ & (P,Q) & \mapsto & \dfrac{f_A(B)}{f_B(A)} \end{array}$$

という写像が考えられます.

補題と定義 5.12 上の e_n は確定した写像となる. これを $E[n]$ の Weil ペアリングと呼ぶ.

証明 B は同じにして, 別の $A' \sim (P) - (\mathcal{O})$ を取ったときに一致を言えば十分である. $(f_{A'}) \sim nA'$ なる $f_{A'} \in \overline{K}(E)^\times$ を取ると, $A - A' \sim 0$ より $\exists g \in \overline{K}(E)^\times$ s.t. $A - A' = (g)$. よって $nA - nA' = (g^n)$ となるから, $(f_A) - (f_{A'}) = nA - nA' = (g^n)$. すなわち $f_A/f_{A'} = kg^n$, $k \in \overline{K}^\times$, となる. $\overline{K}$ は代数閉体なので k の n 乗根を g に繰り込んで, $f_A/f_{A'} = g^n$ と仮定してよい. このとき, $\mathrm{supp}\,(g) \cap \mathrm{supp}\,B = \emptyset$ であって,

$$\frac{f_A(B)}{f_B(A)} = \frac{f_{A'}(B)g^n(B)}{f_B(A)} = \frac{f_{A'}(B)g^n(B)}{f_B(A')f_B((g))} = \frac{f_{A'}(B)}{f_B(A')}\frac{g(nB)}{f_B((g))} = \frac{f_{A'}(B)}{f_B(A')}\frac{g((f_B))}{f_B((g))}$$

よって一般に, 二つの有理函数 f, g に対して

$$\mathrm{supp}\,(f) \cap \mathrm{supp}\,(g) = \emptyset \ \text{ ならば } \ \frac{f((g))}{g((f))} = 1 \tag{5.4}$$

を言えばよい. これは後で示す.

最後に e_n の像が 1 の n 乗根となることは, 同じく (5.4) から

$$\Big(\frac{f_A(B)}{f_B(A)}\Big)^n = \frac{f_A(nB)}{f_B(nA)} = \frac{f_A((f_B))}{f_B((f_A))} = 1$$

最後に (5.4) を示す. $\mathrm{supp}\,(f) = \{a_1, \ldots, a_M\}$, $\mathrm{supp}\,(g) = \{b_1, \ldots, b_N\}$ とし, まず簡単のためこれらに $\mathcal{O}$ は含まれないとする. これらの和集合は有限集合なので, 1次函数 $u = \lambda x + \mu y$ をうまく選んで, その適当な平行移動がこの集合上で E の局所パラメータとして使えるようにできる. このとき, これらの点をすべて含むあるアフィン Zariski 開集合 ($\lambda x + \mu y = c$ の形の直線が E と接する点はある代数方程式を満たすので, その零点の補集合をとればよい) の上で

$$(f) = c_f \prod_{j=1}^{M} (u - a_j)^{m_j}, \qquad (g) = c_g \prod_{k=1}^{N} (u - b_k)^{n_k}, \qquad \sum_{j=1}^{M} m_j = \sum_{k=1}^{N} n_k = 0$$

と書け, 従って,

$$\frac{f((g))}{g((f))} = \frac{\prod_{k=1}^{N}\left(c_f\prod_{j=1}^{M}(b_k-a_j)^{m_j}\right)^{n_k}}{\prod_{j=1}^{M}\left(c_g\prod_{k=1}^{N}(a_j-b_k)^{n_k}\right)^{m_j}} = \frac{\prod_{k=1}^{N}c_f^{n_k}}{\prod_{j=1}^{M}c_g^{m_j}}(-1)^{\sum_{j=1}^{M}\sum_{k=1}^{N}m_jn_k} = \frac{c_f^0}{c_g^0}(-1)^0 = 1$$

以上は $\mathcal{O}$ が因子の台に含まれていないと仮定したが, もし含まれていれば, 局所座標を定義する函数として $\lambda x+\mu y$ の代わりに $u=\dfrac{\lambda x}{y}$ を用いれば全く同様の議論が可能である. □

以下, Weil ペアリングの性質を調べるための必要から, ペアリングの具体的な計算法に立ち入ろう. まず, 次数 0 の因子 D に対する正準形

$$D=(P)-(\mathcal{O})+(f)$$

を定義しよう. ここに $f\in\overline{K}(E)^\times$ であり, 定数因子 $\in\overline{K}^\times$ を除いて一意に定まることは明らかである. 次に, 二つの正準形の因子 $D_1=(P_1)-(\mathcal{O})+(f_1)$, $D_2=(P_2)-(\mathcal{O})+(f_2)$ の和の正準形表現は, これらが主因子でないとき，すなわち $P_i\neq\mathcal{O}$ のとき，

$$D_1+D_2=(P_3)-(\mathcal{O})+(f_1f_2f_3),\quad \text{ここに}$$
$$P_3=P_1+P_2,\quad f_3=\frac{\ell}{v},\quad \ell \text{ は } P_1P_2 \text{ を通る直線，} v \text{ は } P_3 \text{ を通る垂直線}$$

となる. ただし $P_3=\mathcal{O}$ となるときは $v=1$ とする. 実際, $(f_1f_2f_3)=(f_1)+(f_2)+(f_3)$ であり，

$$(f_3)=(\ell)-(v)=\{(P_1)+(P_2)+(-P_3)-3(\mathcal{O})\}-\{(P_3)+(-P_3)-2(\mathcal{O})\}=(P_1)+(P_2)-(P_3)-(\mathcal{O})$$

もし $P_j\in E(K)$, すなわち, ともに K-有理点で, かつ $f_j\in K(E)$ なら, $P_3\in E(K)$, $f_3\in K(E)$ となることは明らかであろう. また f_3 は (約分しない段階では) $\pm P_3$ で定義されず, $1/f_3$ は $P_1,P_2,-P_3$ で定義されない. しかし $(f_3)=(P_1)+(P_2)-(P_3)-(\mathcal{O})$ なので, f_3 が (有理函数として) 真に定義されないのは P_3 と $\mathcal{O}$ だけである.

以上の操作と全く同様にして, $P\in E[n]$ なる因子 $(P)-(\mathcal{O})$ が与えられたとき, $S\in E[n]$ を任意に選んで, 楕円曲線の加法の意味で $T=P+S$ となる点 $S\in E[n]$ をとれば,

$$(T)-(S)=(P)-(\mathcal{O})-\{(P)+(S)+(-T)-3(\mathcal{O})\}+\{(T)+(-T)-2(\mathcal{O})\}=(P)-(\mathcal{O})+(v)-(\ell)$$

ここに ℓ は点 $P,S,-(P+S)$ を通る直線の方程式, v は点 $\pm T$ と $\mathcal{O}$ を通る直線の方程式, となる. すなわち $A=(P+S)-(S)$ は e_n を計算するのに使える. 同様に, $Q\in E[n]$ に対しても $U\in E[n]$ を選んで, $\{P+S,S\}$ と $\{Q+U,U\}$ が共通点を持たないようにすれば, $B=(Q+U)-(U)$ と取れ, 従って

$$e_n(P,Q)=\frac{f_{(P+S)-(S)}(Q+U)}{f_{(P+S)-(S)}(U)}\frac{f_{(Q+U)-(U)}(S)}{f_{(Q+U)-(U)}(P+S)}$$

と簡単になる. 特に, もし $P\in E(K)$ なら, $S\in E(K)$ に選べば $P+S\in E[n]$ となり, 従って A は K 上定義されることに注意せよ. よって, 主因子の加法に関して上に注意したことを反復適用すれば, nA の計算結果として定まる $(nP)-(\mathcal{O})+(f_A)=(f_A)$ における f_A も K 上定義された有理函数に取れることが分かる. 以上により, $P,Q\in E(K)$ なら $e_n(P,Q)\in K$ となることが分かる.

定理 5.13 Weil ペアリングは以下の性質を持つ.

(1) (単位性) $\forall P\in E[n]$ に対し $e_n(P,P)=1$.
(2) (交代性) $\forall P,Q\in E[n]$ に対し $e_n(Q,P)=e_n(P,Q)^{-1}$.
(3) (双線型性) $\forall P,Q,R\in E[n]$ に対し
$e_n(P,Q+R)=e_n(P,Q)e_n(P,R)$, $e_n(P+Q,R)=e_n(P,Q)e_n(Q,R)$.
(4) 非退化性 $\forall P\in E[n]$ に対し $e_n(P,\mathcal{O})=1$. 逆に, $\forall P\in E[n]$ に対し $e_n(P,Q)=1$ なら, $Q=\mathcal{O}$.

(5) $E[n] \subset E(K)$ なら $\forall P, Q \in E[n]$ に対し $e_n(P,Q) \in K$. 従って $\mu_n \subset K$. 逆に $\mu_n \subset K$ なら $E[n] \subset E(K)$.
(6) 両立性 $P \in E[n]$, $Q \in E[nm]$ なら, $e_{nm}(P,Q) = e_n(P, mQ)$.

証明 (1) これは当り前のように見えるがそれほど自明ではない. A, B および f_A, f_B に同じものを取ってしまっては, 台が交わらないという条件を満たさないからである. しかし $A \sim (P) - (\mathcal{O})$, $B \sim (P) - (\mathcal{O})$ を, 台が交わらないように選べば, $A - B \sim 0$ は主因子となるので, ある有理函数により $A - B = (g)$ と書ける. すると, $(f_A) - (f_B) = nA - nB = (g^n)$ となり, かつ f_A と f_B は台が交わらない. 今, $\operatorname{supp} A \cup \operatorname{supp} B = \operatorname{supp}(g)$ を含むアフィン Zariski 開集合で $u = \lambda x + \mu y$ の平行移動が E の局所座標と成り得るものを選べば,

$$g(u) = g_A(u) g_B(u), \qquad g_A(u) = \prod_{P \in \operatorname{supp} A} (u - P)^{m_P}, \quad g_B(u) = \prod_{P \in \operatorname{supp} B} (u - P)^{m_P}$$

と分解され, 従って, $(g_A) = A$, $(g_B) = B$ となるので, $\operatorname{supp}\{(f_A) - (g_A^n)\} = \operatorname{supp}\{(f_B) - (g_B^n)\} = \emptyset$. よって, 非零定数因子を調節して $f_A = g_A^n$, $f_B = g_B^n$. これから (5.4) により

$$\frac{f_A(B)}{f_B(A)} = \Big(\frac{g_A((g_B))}{g_B((g_A))}\Big)^n = 1.$$

(2) これは自明.
(3) $A = (P) - (\mathcal{O}) + (f)$, $B = (Q) - (\mathcal{O}) + (g)$, $C = (R) - (\mathcal{O}) + (h)$ を $\operatorname{supp} A \cap \operatorname{supp} C = \operatorname{supp} B \cap \operatorname{supp} C = \emptyset$ となるように選ぶと, 上で論じたように, $A + B = (P + Q) - (\mathcal{O}) + (fg\frac{\ell}{v})$ となり, かつ $n(A + B) = nA + nB \sim (f_A) + (f_B) = (f_A f_B)$ となるので, $f_{A+B} = f_A f_B$ はペアリング $e_n(P + Q, R)$ を計算するのに使え,

$$e_n(P + Q, R) = \frac{f_{A+B}(C)}{f_C(A + B)} = \frac{f_A(C) f_B(C)}{f_C(A) f_C(B)} = e_n(P, R) e_n(Q, R).$$

(4) $B \sim (\mathcal{O}) - (\mathcal{O})$ なら, $f_B = 1$ ととれる. $f_A((1)) = 1$, $1((f_A)) = 1$ は規約のようなものであるから, $e_n(P, \mathcal{O}) = 1$ となる. 逆に, +++++
(5) 前半は定理の直前で既に注意した. 後半は+++++
(6) $A \sim (P) - (\mathcal{O})$, $B \sim (Q) - (\mathcal{O})$ とすれば, $(f_A) = nA$, $(f_B) = nmB$ なる有理函数 f_A, f_B がある. $mQ \in E[n]$ であるが, $B = (Q) - (\mathcal{O}) + (g_B)$ とすれば, 上に述べた構成法を反復して用いれば, $mB = (mQ) - (\mathcal{O}) + (g_B h)$ なる有理函数 h が存在する. よって $e_n(P, mQ)$ を計算するときの因子として mB が使え, しかも $n \cdot mB = (f_B)$ なので, f_B は e_n を計算するための f_{mB} としても使える. 他方, $P \in E[n]$ は自然に $\in E[mn]$ ともみなせ, $(f_A) = nA$ なので, $(f_A^m) = mnA$, よって f_A^m は $e_{nm}(P, Q)$ を計算するときの f_A として使える. 以上により

$$e_n(P, mQ) = \frac{f_A(mB)}{f_B(A)} = \frac{f_A(B)^m}{f_B(A)} = \frac{f_A^m(B)}{f_B(A)} = e_{nm}(P, Q). \qquad \square$$

系 5.14 T_1, T_2 を $E[n] = \boldsymbol{Z}_n \oplus \boldsymbol{Z}_n$ の任意の基底とするとき, $\zeta = e_n(T_1, T_2)$ は 1 の原始 n 乗根となる.

証明 $\zeta^d = 1$ とせよ. このとき $e_n(T_1, dT_2) = e_n(T_1, T_2)^d = \zeta^d = 1$ となり, また明らかに $e_n(T_2, dT_2) = e_n(T_2, T_2)^d = 1$ でもある. $E[n]$ の任意の元 S は $S = aT_1 + bT_2$ の形に書けるので, $e_n(S, dT_2) = e_n(aT_1 + bT_2, dT_2) = e_n(T_1, dT_2)^a e_n(T_2, dT_2)^b = 1$. よって 定理 5.13 の (4) により $dT_2 = \mathcal{O}$. よって $n \mid d$ となるから, ζ は 1 の原始 n 乗根である. □

定理 5.15 E の準同型 α は分離的とする. このとき $\forall S, T \in E[n]$ に対し

$$e_n(\alpha(S), \alpha(T)) = e_n(S, T)^{\deg \alpha} \tag{5.5}$$

が成り立つ.

証明 +++++

☺ 実は上の定理の結論は任意の準同型について正しいことが知られているが, その証明は面倒なので, 以下の我々に必要な場合に限って証明した. なお, 後で非分離的な一つの写像についてもこの定理を証明し, 結果を利用するので, 以下に述べるこの定理の帰結は, やや回りくどいが, 定理の結論に相当する主張を仮定にした形で述べておく.

系 5.16 n は体の標数と互いに素とするとき, 上の定理の結論を成り立たせるような E の準同型 α に対して, その $E[n]$ への作用を (ある基底について) 表現する行列を α_n とするとき,

$$\det \alpha_n \equiv \deg \alpha \bmod n.$$

証明 $\alpha_n = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ とする. 基底 T_1, T_2 に対して, 系 5.14 により $\zeta = e_n(T_1, T_2)$ は 1 の原始 n 乗根を与えたので, (5.5) により,

$$\begin{aligned} \zeta^{\deg \alpha} &= e_n(\alpha(T_1), \alpha(T_2)) = e_n(aT_1 + cT_2, bT_1 + dT_2) \\ &= e_n(T_1, T_1)^{ab} e_n(T_1, T_2)^{ad} e_n(T_2, T_1)^{cb} e_n(T_2, T_2)^{bd} \\ &= 1 \cdot e_n(T_1, T_2)^{ad} e_n(T_1, T_2)^{-bc} \cdot 1 = \zeta^{ad-bc}. \end{aligned}$$

ζ が 1 の原始 n 乗根なので, これから $\deg \alpha \equiv ad - bc = \det \alpha_n \bmod n$ を得る. □

命題 5.17 α, β を E の準同型とし, a, b を整定数とする. 準同型 $a\alpha + b\beta$ を

$$(a\alpha + b\beta)(P) = a\alpha(P) + b\beta(P)$$

で定めるとき, もし $\alpha, \beta, \alpha + \beta, a\alpha + b\beta$ に対して (5.5) が成立していれば,

$$\deg(a\alpha + b\beta) = a^2 \deg \alpha + b^2 \deg \beta + ab(\deg(\alpha + \beta) - \deg \alpha - \deg \beta). \tag{5.6}$$

証明 n を K の標数と互いに素な任意の正整数とし, $E[n]$ の基底を一つ決めて α, β の $E[n]$ への作用を行列 α_n, β_n で表すとき, まず $a\alpha + b\beta$ の同じ基底による表現行列が $a\alpha_n + b\beta_n$ となることに注意せよ. 2 次行列の直接計算により

$$\det(a\alpha_n + b\beta_n) = a^2 \det \alpha_n + b^2 \det \beta_n + ab(\det(\alpha_n + \beta_n) - \det \alpha_n - \det \beta_n) \tag{5.7}$$

が示せるので, (5.6) は両辺の $\bmod n$ を取れば系 5.16 により成り立つ. n をこの式に現れるすべての項より大きく, かつ p と互いに素に選べるので, この式は真の等号となる.

さて (5.7) は $\alpha_n = (\boldsymbol{u}_1, \boldsymbol{u}_2)$, $\beta_n = (\boldsymbol{v}_1, \boldsymbol{v}_2)$ とそれぞれを列ベクトルで表すとき, 行列式の列に関する多重線型性により

$$\begin{aligned} \det(a\alpha_n + b\beta_n) &= \det(a\boldsymbol{u}_1 + b\boldsymbol{v}_1, a\boldsymbol{u}_2 + b\boldsymbol{v}_2) \\ &= \det(a\boldsymbol{u}_1, a\boldsymbol{u}_2) + \det(a\boldsymbol{u}_1, b\boldsymbol{v}_2) + \det(b\boldsymbol{v}_1, a\boldsymbol{u}_2) + \det(b\boldsymbol{v}_1, b\boldsymbol{v}_2) \\ &= a^2 \det \alpha_n + ab\{\det(\boldsymbol{u}_1, \boldsymbol{v}_2) + \det(\boldsymbol{v}_1, \boldsymbol{u}_2)\} + b^2 \det \beta_n \\ &= a^2 \det \alpha_n + ab\{\det(\boldsymbol{u}_1 + \boldsymbol{v}_1, \boldsymbol{u}_2 + \boldsymbol{v}_2) - \det(\boldsymbol{u}_1, \boldsymbol{u}_2) - \det(\boldsymbol{v}_1, \boldsymbol{v}_2)\} + b^2 \det \beta_n \\ &= a^2 \det \alpha_n + ab\{\det(\alpha_n + \beta_n) - \det \alpha_n - \det \beta_n\} + b^2 \det \beta_n. \qquad \square \end{aligned}$$

§5.3 Frobenius 写像

一般に標数 p の有限体 $K = \boldsymbol{F}_q$ $(q = p^m)$ の代数的閉包 $\overline{K}$ には, Frobenius 写像と呼ばれる独特な写像

$$\begin{array}{ccccc} \varphi_q & \overline{K} & \longrightarrow & \overline{K} \\ & \cup & & \cup \\ & \alpha & \mapsto & \alpha^p \end{array}$$

が働きます. 特に, $m = 1$ のときは $\varphi_p : x \mapsto x^p$ で, 写像の合成の意味で $\varphi_q = \varphi_p^m$ となっています. φ_q は定義により積を積に写しますが標数のいたずらで，加法も加法に対応させ，従って体の同型となります．実際, このことは φ_p について見れば十分ですが, 中間の２項係数がすべて p を因子に持つことから,

$$(x+y)^p = x^p + px^{p-1}y + \cdots + \frac{p!}{k!(p-k)!}x^k y^{p-k} + \cdots + y^p = x^p + y^p.$$

定理 2.1 で注意したように, 一般に $\boldsymbol{F}_q$ の元は $x^q - x = 0$ のすべての根と一致しているので, $\overline{K}$ の中で写像 φ_q で不変な元が，ちょうど $\boldsymbol{F}_q$ の元に対応しています．

Frobenius 写像 φ_q は, 座標への作用 $(x, y) \mapsto (x^q, y^q)$ を通して $\boldsymbol{F}_q$ 上の楕円曲線 E にも作用します. この像が再び楕円曲線 E 上の点となることは, 方程式

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

の両辺を q 乗してみれば, 係数 a_j が $a_j^q = a_j$ を満たすことと, クロスタームが消えること, および指数法則により

$$(y^q)^2 + a_1(x^q)(y^q) + a_3(y^q) = (x^q)^3 + a_2(x^q)^2 + a_4(x^q) + a_6$$

となるからです.

命題 5.18 E を $\boldsymbol{F}_q$ 上の楕円曲線とするとき, Frobenius 写像 φ_q は E の自己同型を与える. φ_q の次数は q であり, $\mathrm{Ker}\,\varphi_q$ は $\mathcal{O}$ のみより成り, φ_q は非分離的である.

証明 φ_q が $E \to E$ という写像を定めることは上に見た通りである. これから一般論により φ_q は群の準同型となるが, 準同型性は直接初等的に示すこともできる. すなわち, 加法 $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$ を定める公式には, これらの点の座標以外には $\boldsymbol{F}_q$ の元しか現れないので, 両辺を q 乗すると体の同型ということから, そのまま $(x_3^q, y_3^q) = (x_1^q, y_1^q) + (x_2^q, y_2^q)$ の公式となる.

φ_q は有理写像どころか多項式写像であり, 次数は明らかに q に等しい. また写像の第一成分 x^q の導函数 qx^{q-1} は恒等的に零となるので, 非分離的である. あるいは, $\mathrm{Ker}\,\varphi_q$ は定義により $\mathcal{O}$ のみで, 位数 $q > \#\mathrm{Ker}\,\varphi_q = 1$ となることより, 命題 5.6 の対偶としても得られる. □

補題 5.19 j, k を整数とするとき $j\varphi_q + k$ が分離的となるためには $p \nmid k$ が必要かつ十分である. 特に, $\varphi_q - 1$ は分離的で $\mathrm{Ker}\,(\varphi_q - 1) = E(\boldsymbol{F}_q)$, 従ってその次数 $\deg(\varphi_q - 1)$ は $\#E(\boldsymbol{F}_q)$ に等しい.

証明 j 倍写像の表現を $(r_j(x), ys_j(x))$ とすると, 合成写像 $j\varphi_q$ の表現は

$$(r_{j\varphi_q}(x), ys_{j\varphi_q}(x)) = (r_j(x^q), y^q s_j(x^q)) = (r_j(x)^q, y \cdot (x^3 + ax + b)^{(q-1)/2} s_j(x)^q)$$

を満たすはずである. よって,

$$c_{j\varphi_q} := \frac{r_{j\varphi_q}(x)'}{s_{j\varphi_q}(x)} = \frac{qr_j(x)^{q-1}r_j'(x)}{s_{j\varphi_q}(x)} = 0$$

となる. 他方, 補題 5.11 により $c_k := \dfrac{r_k'(x)}{s_k(x)} = k$ なので, 補題 5.10 によりこれらの和は

$$\frac{r'_{j\varphi_q+k}}{s_{j\varphi_q+k}} =: c_{j\varphi_q+k} = 0 + k = k$$

を満たす. 故に $r'_{j\varphi_q+k} \not\equiv 0 \iff p \nmid k$.

$\mathrm{Ker}\,(\varphi_q - 1) = E(\boldsymbol{F}_q)$ は Frobenius 写像の定義より明らか. $\varphi_q - 1$ は前半の主張より分離的なので, 命題 5.6 より次数は核の位数である $\#E(\boldsymbol{F}_q)$ と一致する. □

系 5.20 E を $\boldsymbol{F}_q$ 上の楕円曲線とし $n \geq 1$ を整数とする. このとき Frobenius 写像 φ_q について次が成り立つ.
(1) $\mathrm{Ker}\,(\varphi_q^n - 1) = E(\boldsymbol{F}_{q^n})$.
(2) $\varphi_q^n - 1$ は分離的な写像である. 従って $\#E(\boldsymbol{E}_{q^n}) = \deg(\varphi_q^n - 1)$.

証明 $\varphi_q^n = \varphi_{q^n}$ なので, (1), (2) ともに前補題に含まれる. □

補題 5.21 n は p と互いに素な整数とし, E は $\boldsymbol{F}_q$ 上定義された楕円曲線とする. このとき, $\alpha = \varphi_q$ に対しても定理 5.15 の結論 (5.5) が成立する.

証明 +++++

次の性質は Hasse の定理の証明で使われます：

補題 5.22 j, k を整数とし, k は p と素とする. $\#E(\boldsymbol{F}_q) = q + 1 - t$ とするとき,

$$\deg(j\varphi_q - k) = j^2 q + k^2 - jkt.$$

証明 前補題により, 定理 5.15 の結論 (5.5) が φ_q に対して成り立つことが示された. 他方, (-1) 倍は明らかに分離的な準同型であり, $\varphi_q - 1$, $j\varphi_q - k$ は補題 5.19 により分離的である. よって $\deg(j\varphi_q - k)$ の計算に $\alpha = \varphi_q$, $\beta = -1$ として命題 5.17 の公式が使える. $\deg \varphi_q = q$, また $-(x, y) = (x, -y)$ より, $\deg(-1) = \deg x = 1$ 及び $\deg(-\varphi_q) = q$ に注意すると,

$$\deg(j\varphi_q - k) = j^2 \deg \varphi_q + k^2 \deg(-1) + jk(\deg(\varphi_q - 1) - \deg \varphi_q - \deg(-1)) = j^2 q + k^2 - jk\{\deg(\varphi_q - 1) - q - 1\}.$$

ここで命題 5.19 により $\deg(\varphi_q - 1) = \#E(\boldsymbol{F}_q) = q + 1 - t$ なので, 上の値は $j^2 q + k^2 - jkt$ に等しい. □

§5.4 捩れ群の構造定理の証明

この節では今まで準備してきた結果を用いて, 第３章で証明無しに紹介した楕円曲線の点の個数 (位数), および捩れ部分群の位数と群構造に関する諸定理に証明を与えます. 有理点の個数と群構造の解明は更なる準備が必要なので, 後の章に回します.

定理 3.8bis (Hasse の定理) $\#E(\boldsymbol{F}_q) = q + 1 - t$ と置くとき, $|t| \leq 2\sqrt{q}$.

証明 $\deg(j\varphi_q - k) \geq 0$ なので, 補題 5.22 から $p \nmid k$ なる任意の k について,

$$j^2 q + k^2 - jkt \geq 0, \qquad \text{すなわち}, \qquad qx^2 - tx + 1 \geq 0 \quad (x = \frac{j}{k})$$

ここで, $p \nmid k$ なる k を分母に持つ有理数は実数全体の中で稠密に存在する (例えば, 今は $p \neq 2$ なので, 二進有限小数の全体をとればよい.) よって初等数学の定理から, 判別式 $t^2 - 4q \leq 0$, すなわち $|t| \leq 2\sqrt{q}$ でなければならない. □

定理 5.23 E を $\boldsymbol{F}_q$ 上定義された楕円曲線とし, $\#E(\boldsymbol{F}_q) = q + 1 - t$ とする. このとき Frobenius 写像 φ_q は E の自己準同型写像として

$$\varphi_q^2 - t\varphi_q + q = 0$$

を満たす. また, t は φ_q が E の自己準同型写像として満たす

$$\varphi_q^2 - k\varphi_q + q = 0$$

の形の関係式の係数 k として一意に定まる.

証明 $\varphi_q^2 - k\varphi_q + q$ **が零準同型でなければ**, **その核は有限集合となる**. **よって核が無限集合となることを示そう**.

正整数 n **を** q **と互いに素に選び**, φ_q **の** $E[n]$ **における表現行列を** $(\varphi_q)_n = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ **とすると**, **命題** 5.19 **と系** 5.16 **より**, I **を２次の単位行列として**

$$\#\mathrm{Ker}\,(\varphi_q - 1) = \deg(\varphi_q - 1) \equiv \det((\varphi_q)_n - I) = ad - bc - (a+d) + 1 \mod n$$

となる. **同じく系** 5.16 **により**, $ad - bc = \det \varphi_q \equiv \deg \varphi_q = q \bmod n$. **よって命題** 5.19 **より**

$$q + 1 - t = \#E(\boldsymbol{F}_q) = \#\mathrm{Ker}\,(\varphi_q - 1) \equiv q - \mathrm{tr}\,(\varphi_q)_n + 1 \mod n. \qquad \therefore\ \mathrm{tr}\,(\varphi_q)_n \equiv t \bmod n.$$

となる. **よって** Cayley-Hamilton **の定理により**

$$O = (\varphi_q)_n^2 - \mathrm{tr}\,(\varphi_q)_n(\varphi_q)_n + \det(\varphi_q)_n I \equiv (\varphi_q)_n^2 - t(\varphi_q)_n + qI \mod n.$$

ここに O **は２次の零行列を表す**. **得られた式は**, **準同型** $\varphi_q^2 - t\varphi_q + q$ **が** $E[n]$ **の上では恒等的に零となることを意味する**. $p \nmid n$ **なる** n **は無限に存在するので**, **これから** $\varphi_q^2 - t\varphi_q + q$ **の核が無限集合であることが従い**, **最初に述べたように** $\varphi_q^2 - t\varphi_q + q$ **が示された**.

最後に, $\varphi_q^2 - t'\varphi_q + q = 0$ **とすれば**, **引き算して** $(t - t')\varphi_q = 0$. φ_q **は全射なので**, $t - t'$ **は** E **のすべての元を** $\mathcal{O}$ **に写し**, **従って零写像となる**. **しかしこれから整数として** $t - t' = 0$ **が従うかどうかはまだ証明していなかったので**, **もう少し議論が必要である**. $t - t'$ **は任意の正整数** m **について** $E[m]$ **を零化するが**, $p \nmid m$ **のとき** $E[m]$ **は位数** m **の元を含むので**, $m \mid t - t'$. **これが無限に多くの** m **について成り立つので** $t - t' = 0$. □

定理 3.16 bis (Weil) E **を** $\boldsymbol{F}_q$ **上定義された楕円曲線で，**$\#E(\boldsymbol{F}_q) = q + 1 - t$ **とする．このとき，**$\#E(\boldsymbol{F}_{q^k}) = q + 1 - \alpha^k - \beta^k$ **と書ける．ここに，**$\alpha.\beta$ **は** $T^2 - tT + q = 0$ **の２根として定まる複素数である．**

証明 **まず**, $\alpha^k + \beta^k$ **は整数であり**, **かつ** $\alpha + \beta = t$ **で割り切れることに注意しよう**. **実際**,

$$\alpha^k + \beta^k = (\alpha + \beta)^k - \alpha\beta\chi(\alpha, \beta)$$

という式が成り立つ. **ここで** $\chi(\alpha, \beta)$ **は** α, β **のある対称多項式である**. **よってそれは** $\alpha + \beta = t$ **と** $\alpha\beta = q$ **の多項式として**, **ある整数** m **に等しく**, **上の全体は** $= t^k - qm$ **に等しい**.

さて, $\#E(\boldsymbol{F}_{q^k}) = q^k + 1 - t_k$ **と置けば**, $\varphi_{q^k} = \varphi_q^k$ **であって**, **定理** 5.23 **により**

$$(\varphi_q^k)^2 - t_k\varphi_q^k + q^k = 0.$$

しかるに, x **の多項式**

$$x^{2k} - (t^k - qm)x^k + q^k = x^{2k} - (\alpha^k + \beta^k)x^k + \alpha^k\beta^k = (x^k - \alpha^k)(x^k - \beta^k)$$

は, **明らかに** $(x - \alpha)(x - \beta) = x^2 - tx + q$ **で割り切れるので**, **これに** $x = \varphi_q$ **を代入したものも定理** 5.23 **により** 0 **となる：**

$$(\varphi_q^k)^2 - (\alpha^k + \beta^k)\varphi_q^k + q^k = 0.$$

よって, **定理** 5.23 **の最後の主張により** $t_k = \alpha^k + \beta^k$ **わ得る**. □

以上の準備の下に, **捻れ群の構造定理の証明を完成できます**.

命題 3.17 bis (1) n **が体の標数** p **と互いに素なら，**$E[n] = \boldsymbol{Z}_n \oplus \boldsymbol{Z}_n$.
(2) E **が超特異のとき，**$E[p^e] = \mathcal{O}$, **そうでないとき，**$E[p^e] = \boldsymbol{Z}_{p^e}$.

証明 (1) **の方は系** 5.8 **で既に示した**.

(2) $E[p]$ **が自明なら**, **任意の** k **について** $E[p^k]$ **も自明となることは明らか**. **実際**, $P \in E[p^k]$ **が単位元以外の元なら**, $pP, p^2P, \ldots$ **のどれかは自明でない** $E[p]$ **の元となる**. **そこで** $E[p]$ **が自明でない**

とすると, その位数は p 冪で, 命題 5.6 により p^2 より真に小さいから, p でなければならない. すなわち $E[p] \simeq \boldsymbol{Z}_p$. このとき $E[p^k] \simeq \boldsymbol{Z}_{p^k}$ となることを示そう. $P_1 \in E[p]$ を生成元とすれば, 命題 5.5 により $pP_2 = P_1$ なる P_2 が有り, これは明らかに位数 p^2 の元となる. 以下同様にして, 位数 p^k の元 P_k が存在する. 故に $E[p^k]$ は巡回群 $\boldsymbol{Z}_{p^k}$ を含む. これが一致することは, k に関する帰納法で示せる. 実際, $k = 1$ のときは既に示した. 今, $E[p^{k-1}] \simeq \boldsymbol{Z}_{p^{k-1}}$ だったとすると, p 倍写像 $E \to E$ は核 $E[p]$ が p 個の元より成ることから, 任意の点 P の逆像は p 個の元より成る. $P \in E[p^{k-1}]$ のとき, 逆像はすべて $E[p^k]$ に含まれることは明らかで, かつ $pE[p^k] \subset E[p^{k-1}]$ も明らかなので, 結局 $E[p^k] = p^{-1}E[p^{k-1}]$ であり, その元の総数は $p \times |E[p^{k-1}]| = p \times p^{k-1} = p^k$.

最後に, E が超特異なら, $E[\boldsymbol{F}_q]$ の位数は $q - t + 1$, $p \mid t$ なので, p と互いに素. 従って, 位数 p の元は $E[\boldsymbol{F}_q]$ には含まれない. 更に, Weil の定理 3.16 により任意の拡大体 $\boldsymbol{F}_{q^k}$ において $\#E(\boldsymbol{F}_{q^k}) = q + 1 - (\alpha^k + \beta^k)$ となり, ここで $\alpha + \beta = t$, $\alpha\beta = q$ であり, Weil の定理の証明の冒頭で示したように, $\alpha^k + \beta^k$ は $\alpha + \beta = t$ で割り切れる整数となり, 従って必ず p の倍数となる. 故に $\#E(\boldsymbol{F}_{q^k})$ は p と互いに素で有り続けるので, 位数が p の元はいつまで経っても現れない. 故に $E[p] = \mathcal{O}$ である. 逆に, E が超特異でないとき, ある k に対して $\#E(\boldsymbol{F}_{q^k}) = q + 1 - \alpha^k - \beta^k$ が, 従って $\alpha^k + \beta^k - 1$ が, p で割り切れることを言えば, $E(\boldsymbol{F}_{q^k})[p] \neq \mathcal{O}$, 従って $E[p] \neq \mathcal{O}$ が分かる. Weil の定理の証明の冒頭で示したように, $\alpha^k + \beta^k = (\alpha + \beta)^k - \alpha\beta\chi(\alpha, \beta) = t^k - qm$ と書け, 仮定により t は p と互いに素なので, $k = p - 1$ に対して $t^k \equiv 1 \bmod p$ が成り立つ. よってこのような k について $\alpha^k + \beta^k \equiv 1 \bmod p$ となる. □

補題 5.24 $\mathrm{GCD}\,(m, n) = 1$ なら, $E[mn] = E[m] \oplus E[n]$.

証明 $E[m] \oplus E[n] \subset E[mn]$ は明らか. 逆に, $P \in E[mn]$ なら, $(nP, mP) \in E[m] \oplus E[n]$ となるが, この対応は単射である. 実際 $nP = mP = \mathcal{O}$ から拡張 Euclid 互除法で $an + bm = 1$ なる a, b に対し, $P = anP + bmP = a\mathcal{O} + b\mathcal{O} = \mathcal{O}$ となる. 両者は有限集合だから, これより元の個数が一致し, 従って集合として一致する. □

定理 3.12 bis $E(\boldsymbol{F}_q)$ は巡回群か, 型 (n_1, n_2) の群となる. 後者の場合は $n_1 \mid n_2$ のみならず, $n_1 \mid q - 1$ となる.

証明 系 5.8 の証明と同様に論ずる. Abel 群の基本定理により,

$$E(\boldsymbol{F}_q) = \boldsymbol{Z}_{n_1} \oplus \boldsymbol{Z}_{n_2} \oplus \cdots \oplus \boldsymbol{Z}_{n_s}, \qquad \text{ここに} \quad n_1 \mid n_2 \mid \cdots \mid n_s$$

と書けるが, n_1 の各既約因子 ℓ について,

$$E(\boldsymbol{F}_q)[\ell] = \boldsymbol{Z}_\ell^s \subset E[\ell]$$

となり, $E[\ell]$ は命題 3.17 により一つまたは二つの因子の直和なので, $s \leq 2$ でなければならない. よって $E(\boldsymbol{F}_q) = \boldsymbol{Z}_{n_1} \oplus \boldsymbol{Z}_{n_2}$ で, $n_1 \mid n_2$. ($n_1 = 1$ の場合も含む.) 最後に $n_1 \mid q - 1$ となることは, まだ証明できないので留保しておく.