応用楕円曲線論　プリント No.3

情報科学科　金子　晃

第３章　楕円曲線入門

この章では，一般の体 K 上の楕円曲線の定義と性質のうちで，基本的なものを学びます．

§3.1 楕円曲線の定義

【有限体上の幾何学】　体 K 上の n 次元アフィン空間とは, K^n のこと，n 次元射影空間 $P^n(K)$ とは, $(K^{n+1}\setminus\{0,\dots,0\})/K^\times$ のことです．ここで，$K^\times := K\setminus\{0\}$ による商は，次の同値関係による商集合を表します

$$\lambda\in K^\times \text{ に対し } (X_0,X_1,\dots,X_n)\sim(\lambda X_0,\lambda X_1,\dots,\lambda X_n).$$

以下，この同値類の元を $(X:Y:Z)$ で表すことにします．これは，座標の比だけが点を区別するという直感的な意味にマッチした表現です．

【楕円曲線】　さて，体 $K=\boldsymbol{F}_q$ 上の (あるいは K 上で定義された) 楕円曲線とは，$a_1,\dots,a_6\in K$ により定義される集合

$$E=\{(X:Y:Z)\in P^n(\overline{K})\mid Y^2Z+a_1XYZ+a_3YZ^2=X^3+a_2X^2Z+a_4XZ^2+a_6Z^3\}$$

のことです．単に方程式だけ書いて

$$E:\quad Y^2Z+a_1XYZ+a_3YZ^2=X^3+a_2X^2Z+a_4XZ^2+a_6Z^3 \tag{3.1}$$

のことを楕円曲線と呼ぶこともあります．$(0:1:0)$ は常に E の点となります．これが楕円曲線の唯一の無限遠点で，$\mathcal{O}$ と書かれます．曲線上の点としては代数的閉包に座標を持つものも考えていることに注意しましょう．代数的閉体は必ず無限体なので，上の集合は無限集合になります．応用上は，それらのうちある有限部分体 $L\supset K$ に座標が含まれるようなものだけを考えます．これを楕円曲線 E の L-有理点と呼び，$E(L)$ で表します．特に係数体と同じ $L=K$ のとき，すなわち $E(K)$ が重要です．

楕円曲線のアフィン部分平面 $\overline{K}^2$ における形は，$Z\neq0$ で割り算した非同次座標 $x=X/Z, y=Y/Z$ により，

$$E:\quad y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6 \tag{3.2}$$

と書き直されます．同次方程式は面倒なので，普通は，こちらの表示で済ませてしまいます．

楕円曲線は，その上に特異点が無いとき，すなわち，その定義多項式

$$F(X,Y,Z)=Y^2Z+a_1XYZ+a_3YZ^2-X^3-a_2X^2Z-a_4XZ^2-a_6Z^3$$

の 1 階偏導函数

$$\frac{\partial F}{\partial X},\quad \frac{\partial F}{\partial Y},\quad \frac{\partial F}{\partial Z}$$

のどれかが 0 ではないとき，本当の楕円曲線となります．実際，これらを係数とする 1 次同次式

$$\frac{\partial F}{\partial X}\cdot X+\frac{\partial F}{\partial Y}\cdot Y+\frac{\partial F}{\partial Z}\cdot Z=0 \tag{3.3}$$

は，曲線上の点 $(X:Y:Z)$ における $F(X,Y,Z)=0$ の接線の方程式を表します．(接線とは一次近似なり！) このことは直感的には明らかで，実際にも実数体 $\boldsymbol{R}$ 上ではアフィン座標に書き直して確認できます．そのときは，陰函数定理から上の条件が曲線の見掛けの滑らかさを保証すること (滑ら

かな函数のグラフとして書けること) が示せるのでした．係数体が一般の体のときは (3.3) で接線を定義します．

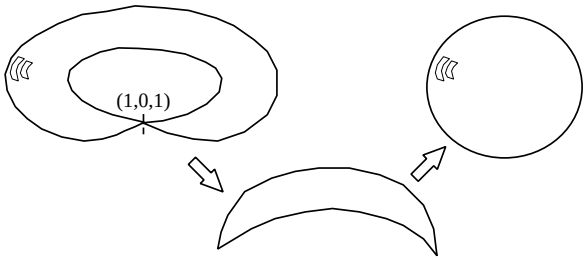
Q 上の接線の方程式は，射影直線なので，当然のことながら定数項はありませんが，アフィン幾何の場合のように，通る点の座標を方程式に含めなくても，偏微分係数を計算した曲線上の点をちゃんと通っているでしょうか？これは，同次函数の微分に関する Euler の恒等式より自然に従います．F の次数を m (今は $m=3$) とすれば, 接線の方程式の左辺の X, Y, Z に考えている点の座標を代入すると， Euler の恒等式により

$$\frac{\partial F}{\partial X}\cdot X+\frac{\partial F}{\partial Y}\cdot Y+\frac{\partial F}{\partial Z}\cdot Z=mF(X,Y,Z)=0$$

となるからです．ところで，上の偏微分係数のどれか一つが 0 でなければ，確かにこれらを係数として射影直線は定まりますが，もし最初の二つが 0 だと，アフィン直線ではなくなるので，心配になるかもしれません．しかし，そのとき接線の方程式は $Z=0$, すなわち無限遠直線を与え，従ってもとの点も始めから曲線の無限遠点であったことになるので，接線が有限点を通らなくても矛盾はありません．

特異点が有ると，楕円曲線の場合はそこで 2 重点を持ち，トーラスがくっついてしまいます．この結果，有理直線，すなわち Riemann 球面と同等なものに帰着してしまいます．複素数体上の場合は，幾何学的直感で次の図のようにこれを説明することができます．有限体上の場合はこれに相当することを代数的な計算で示すことになります．

例 3.1 アフィン代数曲線 $y^2=x(x-1)^2$ は, $(x,y)=(1,0)$ に特異点を持つ．



実際には, 下記の変換で 2 段階的にではなく一気に丸くなる．

双有理変換，すなわち，それ自身も逆変換も有理函数で書けるような座標変換を用いると，この変形は

$$\left\{\begin{array}{l} X=x,\\ Y=\dfrac{y}{x-1}\end{array}\right. \iff \left\{\begin{array}{l} x=X,\\ y=(X-1)Y\end{array}\right. \quad \text{により}\ \ Y^2=X\ \ \text{へ, 更に}$$

$$\left\{\begin{array}{l} \xi=X-Y^2,\\ \eta=Y\end{array}\right. \iff \left\{\begin{array}{l} X=\xi+\eta^2,\\ Y=\eta\end{array}\right. \quad \text{により}\ \ \xi=0\ \ \text{へ}$$

として計算により実現されます．$\{(\xi,\eta,\zeta)\in \boldsymbol{P}^2 \mid \xi=0\}\cong \boldsymbol{P}^1$ に注意しましょう．ここで用いた変換 $(x,y)\mapsto(X,Y)=(x,\dfrac{y}{x-1})$ は, $(1,0,1)$ において, $\boldsymbol{P}^2$ の変換としては $\dfrac{0}{0}$ 型となり, 不定です．つまり，双有理変換には, 定義されない点が有るのです．

【楕円曲線の同型類】 体 K 上定義された二つの楕円曲線 E_1 と E_2 が K 上同型 (isomorphic) とは，それが K 上の射影多様体として同型なことをいいます．同型の定義は，K 上定義された射 (morphism), すなわち，局所的に分母が消えない K 上の有理函数で表示されるような写像 (正則な双有理変換) $\varphi: E_1\to E_2$, $\psi: E_2\to E_1$ が存在して，$\varphi\circ\psi=id_{E_2}$, $\psi\circ\varphi=id_{E_1}$ が成り立つことをいいます．

定理 3.1 K 上定義された二つの楕円曲線

$$E_1:\ \ y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6,$$
$$E_2:\ \ y^2+b_1xy+b_3y=x^3+b_2x^2+b_4x+b_6$$

が K 上同型なためには，$u, r, s, t \in K$, $u \neq 0$ で定まる線型変換

$$(x, y) \mapsto (\xi, \eta) = (u^2 x + r, u^3 y + u^2 s x + t) \tag{3.4}$$

で，E_1 の方程式が E_2 の方程式に書き換えられることが必要かつ十分である．

証明 morphism はアフィン平面上の **Zariski 開集合**, すなわち, アフィン空間からある多項式の零点集合を除いたところ, で x, y の有理函数により定義された写像となる．無限遠点が無限遠点に対応していることから, 分母に零点が有ってはならない. 更に, 方程式の次数が変わらないためには，ξ, η は x, y の一次式でなければならず[1)]，かつ，ξ は y を含んではならない．よって

$$\xi = \lambda x + r, \quad \eta = \mu y + c x + t$$

と書ける．これを ξ, η 座標で表された E_1 の方程式に代入して，その結果が x, y 座標で書かれた E_2 の方程式と，0 でない定数倍を除いて一致するためには，まずは x^3 の係数と y^2 の係数が等しくならねばならないから，$\lambda^3 = \mu^2 \neq 0$ なるを要す．このとき，$\lambda, \mu \neq 0$ となり，自動的に逆変換

$$x = \frac{1}{\lambda}\xi - \frac{r}{\lambda}, \quad y = \frac{1}{\mu}\eta - \frac{c}{\lambda\mu}\xi + \frac{cr}{\lambda\mu} - \frac{t}{\mu}$$

が存在する．$u = \mu/\lambda$ と置けば，$u^2 = \mu^2/\lambda^2 = \lambda^3/\lambda^2 = \lambda$, $u^3 = \mu^3/\lambda^3 = \mu^3/\mu^2 = \mu$ であって，更に $s = c/\lambda = c/u^2$ と置けば，定理の主張する形となる．ちなみに，このとき逆変換は,

$$x = \frac{1}{u^2}\xi - \frac{r}{u^2}, \quad y = \frac{1}{u^3}\eta - \frac{s}{u^3}\xi + \frac{rs}{u^3} - \frac{t}{u^3} \tag{3.5}$$

と書け, $1/u$ を u だと思えば同じ形となっている．□

例によって，変換 (3.4) が曲線 E_1 の方程式を曲線 E_2 の方程式に写すのなら，変換 (3.5) が曲線 E_2 上の点を曲線 E_1 上の点に写します (contravariant).

実際に変換

$$\xi = u^2 x + r, \quad \eta = u^3 y + u^2 s x + t$$

を (ξ, η) 座標で書かれた E_1 の方程式に代入したとき，(x, y) 座標で書かれた E_2 の方程式が得られたとして，係数比較すると次が得られます：

定理 3.2 K 上定義された定理 3.1 の二つの楕円曲線が K 上同型なためには,

$$\begin{cases} u b_1 = a_1 + 2s, \\ u^2 b_2 = a_2 - s a_1 + 3r - s^2, \\ u^3 b_3 = a_3 + r a_1 + 2t, \\ u^4 b_4 = a_4 - s a_3 + 2r a_2 - (t + rs) a_1 + 3r^2 - 2st, \\ u^6 b_6 = a_6 + r a_4 + r^2 a_2 + r^3 - t a_3 - t^2 - rt a_1 \end{cases} \tag{3.6}$$

が成り立つような，K の元 $u \neq 0$, r, s, t が存在することが必要かつ十分である．

証明 代入した式を書いてみると

$$\begin{aligned} &(u^3 y + u^2 s x + t)^2 + a_1 (u^2 x + r)(u^3 y + u^2 s x + t) + a_3 (u^3 y + u^2 s x + t) \\ &\quad = (u^2 x + r)^3 + a_2 (u^2 x + r)^2 + a_4 (u^2 x + r) + a_6 \end{aligned}$$

この全体を u^6 で割り，E_2 の方程式と比較すると，$y2$ や x^3 の項はそのまま一致する．xy の項は

$$b_1 = \frac{1}{u}(a_1 + 2s).$$

[1)] 実は Frobenius 写像という特別なものが有りうるが, これは自己同型を与えるので方程式を変えないから, 今は無視する. 第 5 章参照.

以下同様に x^2. y, x, 定数項を比較してゆけば，上が得られる．□

§3.2 楕円曲線の群演算

第 1 章で歴史的背景とともに直感的に説明した楕円曲線の群構造を，ここでは一般の方程式で与えられた楕円曲線に対して定義します．ただし簡単のためアフィン表現を用いて説明します．E を方程式 (3.2) で与えられた体 $K = \boldsymbol{F}_q$ 上の楕円曲線とし，$\mathcal{O}$ を E の無限遠点とします．

定義 $\forall P, Q \in E$ に対し

(i) $\mathcal{O} + P = P + \mathcal{O} = P$ と定める．

(ii) $-\mathcal{O} = \mathcal{O}$ と定める．

(iii) $P = (x_1, y_1) \neq \mathcal{O}$ のとき，$-P = (x_1, -y_1 - a_1x_1 - a_3)$ と定める．

(iv) $Q = -P$ のとき $P + Q = \mathcal{O}$ と定める．

(v) $P \neq \mathcal{O}, Q \neq \mathcal{O}, Q \neq -P$ のとき，P, Q を通る直線 ($P = Q$ のときは，P における E の接線) と曲線 E との第 3 の交点を R とするとき，$P + Q = -R$ と定める．

$-P$ は P と無限遠点を通る直線，すなわち，$x = x_1$ と曲線との第 2 の交点です：

$$y^2 + a_1x_1y + a_3y = x_1^3 + a_2x_1^2 + a_4x_1 + a_6$$

から，方程式を解かなくても根と係数の関係 $y_1 + y_2 = -a_1x_1 - a_3$ から y_2 が得られます．第 1 章で説明したときは $a_1 = a_3 = 0$ だったので，単なる符号の変更でした．

問題 3.1 xy と y の項が有る一般のアフィン楕円曲線の正確な図を適当な係数を選んで計算機により描画してみよ．

定理 3.3 E は上に定義された演算で Abel 群となる．$E(K)$ はその部分群となる．

(v) の場合の加法の公式を具体的に与えておきましょう．まず，P, Q を通る直線 l の傾きは，

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & P \neq Q \text{ のとき,} \\ \dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, & P = Q \text{ のとき,} \end{cases} \tag{3.7}$$

l の方程式を $y = \lambda x + \nu$ と置き，第 3 の交点を求めるのですが，これを (3.2) に代入した x の 3 次方程式

$$(\lambda x + \nu)^2 + a_1x(\lambda x + \nu) + a_3 = x^3 + a_2x^2 + a_4x + a_6$$

から，根と係数の関係を用いて

$$x_1 + x_2 + x_3 = -a_2 + \lambda^2 + a_1\lambda \qquad \therefore\ x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$$

これを l の方程式に代入して，R の y 座標は $\lambda x_3 + \nu$ と求まります．よって $-R = P + Q$ の y 座標 y_3 は

$$y_3 = -(\lambda + a_1)x_3 - a_3 - \nu$$

ちなみに，ν は l の方程式に (x_1, y_1) を代入して

$$\nu = y_1 - \lambda x_1$$

と求まるので，

$$y_3 = \lambda(x_1 - x_3) - y_1 - a_1x_3 - a_3$$

よって (3.7) を用いると，(x_3, y_3) が (x_1, y_1) と (x_2, y_2) で完全に表されます．$P = Q$ のときは，上で $x_2 = x_1$ を代入したものを用います．

問題 3.2 この群演算の定義が結合律を満たすことを Risa/Asir などの数式処理ソフトで確かめよ．

命題 3.4 定理 3.1 で与えられた E_1 と E_2 の同型は群の同型ともなっている．

このことは楕円曲線については計算で初等的に確かめることができます．実は，一般に楕円曲線を一般化した概念である Abel 多様体 (代数多様体で，有理写像で表される可換な群演算を持つもの) の間の有理写像は，有理準同型写像と原点の平行移動の合成に限ることが知られています．上は単位元すなわち無限遠点を動かさないので，一般論から群の同型となっていることが分かるのです．

問題 3.3 命題 3.4 を Risa/Asir などの数式処理ソフトによる直接計算で確かめよ．

§3.3 判別式と j-不変量

E を非同次な標準型 (3.2) で表された楕円曲線とするとき，その係数を用いて次のような量を定義します．

$$\begin{aligned} d_2 &= a_1^2 + 4a_2, \\ d_4 &= 2a_4 + a_1a_3, \\ d_6 &= a_3^2 + 4a_6, \\ d_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\ c_4 &= d_2^2 - 24d_4, \\ \Delta &= -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6, \\ j(E) &= c_4^3/\Delta \end{aligned} \tag{3.8}$$

Q 1) 方程式 (3.2) において，x にウェイト 2, y にウェイト 3 を与えると，各単項のウェイトは，順に次のようになります：

y^2	a_1xy	a_3y	x^3	a_2x^2	a_4x	a_6
6	5	3	6	4	2	0

そこで，この次数を揃えるために，係数 a_i にウェイト i を与えると，すべての単項がウェイト 6 で揃います．このウェイトで上の量を眺めると，それぞれ，添え字に等しいウェイトを持つ量であることが分かります．添え字の無い量 Δ はウェイト 12, $j(E)$ はウェイト 0 となり，いかにも不変量 (invariant) っぽいですね．
2) 楕円曲線が Wierstrass の標準形 $y^2 = 4x^3 - g_2x - g_3$ で与えられたときは，次節で計算するように，判別式は $\Delta = g_2^3 - 27g_3^2$ で, $j(E) = g_2^3/(g_2^3 - 27g_3^2)$ という，古来よく知られた形になります．

定理 3.5 方程式 (3.2) が非特異，従って本当に楕円曲線を定めるための必要十分条件は $\Delta \neq 0$ である．

証明 (3.2) の左辺 $-$ 右辺を $f(x, y)$ と置けば，特異点の条件は

$$f(x,y) = 0, \qquad \frac{\partial f}{\partial x} = a_1y - 3x^2 - 2a_2x - a_4 = 0, \qquad \frac{\partial f}{\partial y} = 2y + a_1x + a_3 = 0.$$

第 3 の式を第 2 の式に代入して整理すれば，

$$\frac{a_1^2x + a_1a_3}{2} + 3x^2 + 2a_2x + a_4 = 0, \qquad \therefore\ 6x^2 + (a_1^2 + 4a_2)x + a_1a_3 + 2a_4 = 0$$

同じものを第 1 の式に代入すれば，

$$\frac{(a_1x + a_3)^2}{4} - a_1x\frac{a_1x + a_3}{2} - a_3\frac{a_1x + a_3}{2} - x^3 - a_2x^2 - a_4x - a_6 = 0,$$
$$\therefore\ 4x^3 + (a_1^2 + 4a_2)x^2 + (2a_1a_3 + 4a_4)x + a_3^2 + 4a_6 = 0$$

よって非特性の条件は x に関するこの二つの方程式が共通根を持たないことである．先に定義した d_i を用いてこれらを書き直せば,

$$6x^2 + d_2x + d_4 = 0, \qquad 4x^3 + d_2x^2 + 2d_4x + d_6 = 0$$

よって共通根を持たない条件は，終結式を用いて

$$\begin{vmatrix} 4 & d_2 & 2d_4 & d_6 & 0 \\ 0 & 4 & d_2 & 2d_4 & d_6 \\ 6 & d_2 & d_4 & 0 & 0 \\ 0 & 6 & d_2 & d_4 & 0 \\ 0 & 0 & 6 & d_2 & d_4 \end{vmatrix} \neq 0$$

と表される．この行列式を計算すると上で定義した Δ の -8 倍が得られる．

Q これを展開しても d_8 が出てこないので変だと思うかもしれないが, 実は d_8 は d_2, d_4, d_6 で表される：

$$d_8 = \frac{1}{4}(d_2d_6 - d_4^2)$$

以上の計算は標数 2, 3 のときには修正を要するが，結局上の公式で，これらの標数の場合に自明に消える項を省いたものが得られる．□

問題 3.4 上の行列式に関する主張を Risa/Asir などの数式処理ソフトを用いて確かめよ.

Q 上のアフィン座標による偏微分の計算と，先の同次座標による偏微分の計算との間には,

$$\frac{\partial}{\partial X} = \frac{\partial x}{\partial X}\frac{\partial}{\partial x} = \frac{1}{Z}\frac{\partial}{\partial x}, \qquad \frac{\partial}{\partial Y} = \frac{\partial y}{\partial Y}\frac{\partial}{\partial y} = \frac{1}{Z}\frac{\partial}{\partial y}$$

という関係があります．従って，有限の点 $Z \neq 0$ での非特異条件は (当然のことながら) アフィンで偏微分を計算すれば十分です．なお，楕円曲線は，無限遠点では決して特異点を持ちません．このことは同次方程式 (3.1) が $Z \sim 0$ を同次座標で偏微分するまでもなく，その方程式を Y で割り算して

$$\frac{Z}{Y} = -a_1\Big(\frac{Z}{Y}\Big)^2 + \Big(\frac{X}{Y}\Big)^3 + \cdots$$

の形になることから明らかです.

定理 3.6 K 上定義された二つの楕円曲線 E_1, E_2 が K 上同型ならば，$j(E_1) = j(E_2)$ となる．K が代数的閉体のときは，逆も成り立つ.

実際，同型が (3.6) により具体的に与えられているので，前半は代入して計算するだけで初等的に確かめられます．後半は，$a_1 \sim a_6$ から計算した $j(E_1)$ と $b_1 \sim b_6$ から計算した $j(E_2)$ が等しいという仮定の下で，(3.6) を満たすような u, r, s, t が求まることを言えばよいので，これも初等的に示せます．しかしこの計算はかなり面倒なので，次節以降で標数について分類して簡単化した標準形を用いてこれを確かめましょう．一般には，ここで方程式を解く必要があるため，K が代数的閉体という仮定をしたのです．実際，K が代数的閉体でない場合は，$j(E)$ が同じ値でも同型とは限りません.

例 3.2 後述の例 3.5 や 3.6 で，有限体上の楕円曲線の有理点の成す群が群として同型でないものの例が，それぞれ $j = 0$ あるいは $j = 1728$ の場合に示されますが，命題 3.4 によりこれらは，楕円曲線としても同型ではありません．標数 0 の例として，$y^2 = x^3 - 25x$ と $y^2 = x^3 - 4x$ は，ともに j-不変量が 1728 ですが，前者は $\boldsymbol{Q}$ 上点 $(-4, 6)$ を，従ってそれから生成される無限個の点を含むのに対し，後者の $\boldsymbol{Q}$-有理点は $\mathcal{O}$, $(0, 0)$, $(\pm 2, 0)$ の 4 点だけです．(後者の主張は，不定方程式に解が無いことを証明するために Fermat が発明した降下法 (method of descent) を用いて示すことができます.)

§3.4 標数が 2, 3 以外の場合の楕円曲線

$\mathrm{char}\, K \neq 2$ ならば，(3.1) は，変換

$$(x, y) \mapsto (x, y - \frac{a_1}{2}x - \frac{a_3}{2})$$

により，

$$y^2 = x^3 + b_2x^2 + b_4x + b_6$$

に帰着されます．更に，$\mathrm{char}\, K \neq 3$ でもあれば，変換

$$(x, y) \mapsto (x - \frac{b_2}{3}, y)$$

により，

$$y^2 = x^3 + ax + b \tag{3.9}$$

に帰着されます．このとき (3.8) は，

$$\begin{aligned}
d_2 &= 0,\\
d_4 &= 2a,\\
d_6 &= 4b,\\
d_8 &= -a^2,\\
c_4 &= d_2^2 - 24d_4 = -48a,\\
\Delta &= -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6 = -8(2a)^3 - 27(4b)^2 = -16(4a^3 + 27b^2)\\
j(E) &= c_4^3/\Delta = -1728\frac{(4a)^3}{\Delta} \quad \Big(= \frac{1728}{1 + \frac{27}{4}\frac{b^2}{a^3}} \quad (a \neq 0 \text{ のとき})\Big)
\end{aligned}$$

となります．従って，Δ は (3.9) の右辺の 3 次方程式としての判別式の 16 倍となっています．この場合は逆に，任意の j がある楕円曲線の j-不変量となることが，曲線

$$\begin{array}{ll}
y^2 = x^3 + \dfrac{3j}{1728 - j}x + \dfrac{2j}{1728 - j}, & j \neq 0, 1728 \text{ のとき},\\
y^2 = x^3 + 1, & j = 0 \text{ のとき},\\
y^2 = x^3 + x, & j = 1728 \text{ のとき}
\end{array}$$

から直接確かめられます．

Q Weierstrass の標準形 $y^2 = 4x^3 - g_2x - g_3$ の場合には，

$$\Big(\frac{y}{2}\Big)^2 = x^3 - \frac{g_2}{4} - \frac{g_3}{4}$$

と考えると，$a = g_2/4$, $b = g_3/4$ なので，

$$\Delta = g_2^3 - 27g_3^2, \qquad j(E) = \frac{1728g_2^3}{g_2^3 - 27g_3^2}$$

となります．

標準形 (3.9) に対しては，同型写像は

$$(x, y) \mapsto (u^2x, u^3y) \tag{3.10}$$

と簡単になり，この写像で二つの楕円曲線

$$E_1 : y^2 = x^3 + ax + b, \qquad E_2 : y^2 = x^3 + a'x + b' \tag{3.11}$$

が同型のとき，係数の間の関係式は

$$\begin{cases} u^4 a' = a, \\ u^6 b' = b \end{cases} \tag{3.12}$$

と簡単になります．このときは，両者の j-不変量が等しいとすると，

$$\frac{a^3}{4a^3+27b^2} = \frac{a'^3}{4a'^3+27b'^2}.$$

よって， $b^2/a^3 = b'^2/a'^3$, あるいは，$a^3/a'^3 = b^2/b'^2 = k$ となり，これより $a^3 = ka'^3$, $b^2 = kb'^2$. 従って，$b/b' = w$ と置けば，$k = w^2$ で，$a^3 = w^2 a'^3$, i.e. $w = (wa'/a)^3$. 従って $v = wa'/a$ と置けば，$w = v^3$. $k = v^6$ となり，$a = (w/v)a' = v^2 a'$, $b = wb' = v^3 b'$ となり，もし，$u^2 = v$ となる u が見付かれば，従って特に K が代数的閉体なら，両者は確かに同型です．なお，$a = 0$ または $b = 0$ のときは例外ですが，それぞれ，$u^6 = b/b'$, $u^4 = a/a'$ という代数方程式が解 u を持てば，変換が求まります．

以上をまとめると，

定理 3.7 $\operatorname{char} K \neq 2, 3$ のとき，K 上の楕円曲線は $y^2 = x^3 + ax + b$ の形に帰着される．二つの楕円曲線 (3.11) が K 上同型となるためには，(3.12) を満たす $u \in K$ が存在することが必要かつ十分であり，このとき同型は (3.10) で与えられる．

加法公式 一般の場合から係数が減り，標数 0 の場合に導いたのと同じ公式が得られます：まず，$P = (x_1, y_1)$ のとき $-P = (x_1, -y_1)$. 更に $Q = (x_2, y_2)$ で $Q \neq -P$ なら，$P+Q = (x_3, y_3)$, ここに，

$$x_3 = \lambda^2 - x_1 - x_2, \qquad y_3 = \lambda(x_1 - x_3) - y_1 = -\lambda^3 + 2\lambda x_1 + \lambda x_2 - y_1$$

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & P \neq Q \ \text{のとき}, \\ \dfrac{3x_1^2 + a}{2y_1}, & P = Q \ \text{のとき} \end{cases}$$

例 3.3 $\boldsymbol{F}_{11}$ 上で $y^2 = x^3 + x + 6$ を考えると，$\Delta = 4 \neq 0$ で，確かに楕円曲線を定める．E の $\boldsymbol{F}_{11}$-有理点は

$$E(\boldsymbol{F}_{11}) = \{\mathcal{O}, (2,4), (2,7), (3,5), (3,6), (5,2), (5,9), (7,2), (7,9), (8,3), (8,8), (10,2), (10,9)\}$$

加法の例としては，$(2,4) + (2,7) = \mathcal{O}$, $(2,4) + (3,5) = (7,2)$, $(2,4) + (2,4) = (5,9)$ など．

§3.5 標数が 2 の場合の楕円曲線

公式 (3.8) において 2 倍が掛かっている項を消すと，

$$\begin{aligned} d_2 &= a_1^2, \\ d_4 &= a_1 a_3, \\ d_6 &= a_3^2, \\ d_8 &= a_1^2 a_6 + a_1 a_3 a_4 + a_2 a_3^2 + a_4^2, \\ c_4 &= d_2^2 = a_1^4, \\ \Delta &= d_2^2 d_8 + d_6^2 + d_2 d_4 d_6 = a_1^6 a_6 + a_1^5 a_3 a_4 + a_1^4 a_2 a_3^2 + a_3^6 + a_1^4 a_4^2 + a_1^3 a_3^3, \\ j(E) &= a_1^{12}/\Delta \end{aligned}$$

そこで，まず，$j(E) \neq 0$, すなわち，$a_1 \neq 0$ のときは，

$$(x, y) \mapsto (a_1^2 x + \frac{a_3}{a_1}, a_1^3 y + \frac{a_1^2 a_4 + a_3^2}{a_1^3})$$

という変換で，x と y の 1 次の項を消し，xy の係数を 1 にすことができる．(その結果, 係数の添え字はもはや次数を表さなくなる.) すなわち，

$$y^2 + xy = x^3 + a_2x^2 + a_6 \tag{3.13}$$

という標準形に帰着される．このときは，$\Delta = a_6$, $j(E) = 1/a_6$ である．上の変換は記憶しなくても，

$$(x, y) \mapsto (\lambda^2 x + A, \lambda^3 y + B)$$

を代入して，x と y の係数が消え，かつ xy の係数が x^3, y^2 の係数と等しくなるようにすれば自然に求まる．標数 2 なのでクロス項が消え，計算は見掛けよりずっと楽である：定数項を省略すると，

$$\begin{aligned}
&(\lambda^6 y^2 + \cdots) + (a_1\lambda^5 xy + a_1\lambda^2 Bx + a_1\lambda^3 Ay + \cdots) + (a_3 y + \cdots) \\
&= (\lambda^6 x^3 + \lambda^4 Ax^2 + \lambda^2 A^2 x + \cdots) + a_2(\lambda^4 x^2 + \cdots) + a_4\lambda^2 x + \cdots \\
&\therefore \quad \lambda^6 = \lambda^5 a_1, \quad a_1 A + a_3 = 0, \quad a_1 B = A^2 + a_4
\end{aligned}$$

これから上の変換が定まる．

$j(E) = 0$ のときは，$a_1 = 0$ であり，このときは変換

$$(x, y) \mapsto (x + a_2, y)$$

により，x^2 の項を消せ，

$$y^2 + a_3 y = x^3 + a_4 x + a_6 \tag{3.14}$$

に帰着される．このときは $\Delta = a_3^4$, $j(E) = 0$ である．

加法公式; $j(E) \neq 0$ の標準形 (3.13) の場合： $P \neq Q$ なら，一般の場合の公式を標数 2 を考慮して書き直すと

$$\begin{cases} x_3 = \left(\dfrac{y_1 + y_2}{x_1 + x_2}\right)^2 + \dfrac{y_1 + y_2}{x_1 + x_2} + x_1 + x_2 + a_2, \\ y_3 = \left(\dfrac{y_1 + y_2}{x_1 + x_2}\right)(x_1 + x_3) + x_3 + y_1 \end{cases}$$

$P = Q$ の場合は，$\lambda = x_1 + \dfrac{y_1}{x_1}$ となるので，

$$\begin{cases} x_3 = x_1^2 + \dfrac{y_1^2}{x_1^2} + x_1 + \dfrac{y_1}{x_1} + a_2 = x_1^2 + \dfrac{y_1^2 + x_1 y_1 + x_1^3 + a_2 x_1^2}{x_1^2} = x_1^2 + \dfrac{a_6}{x_1^2} \\ y_3 = (x_1 + \dfrac{y_1}{x_1})(x_1 + x_3) + x_3 + y_1 = x_1^2 + (1 + x_1 + \dfrac{y_1}{x_1})x_3 \end{cases}$$

加法公式; $j(E) = 0$ の標準形 (3.14) の場合： $P \neq Q$ なら，同じく，

$$\begin{cases} x_3 = \left(\dfrac{y_1 + y_2}{x_1 + x_2}\right)^2 + x_1 + x_2, \\ y_3 = \left(\dfrac{y_1 + y_2}{x_1 + x_2}\right)(x_1 + x_3) + y_1 + a_3 \end{cases}$$

$P = Q$ なら，$\lambda = \dfrac{x_1^2 + a_4}{a_3}$ で，

$$\begin{cases} x_3 = \left(\dfrac{x_1^2 + a_4}{a_3}\right)^2 = \dfrac{x_1^4 + a_4^2}{a_3^2}, \\ y_3 = \left(\dfrac{x_1^2 + a_4}{a_3}\right)(x_1 + x_3) + y_1 + a_3 \end{cases}$$

標数が 2 のとき, 代数的閉体では $j(E)$ が等しいことが同型の条件であることは, それほど自明ではありません. このことは第 6 章で, 標数 2 の有限体上の楕円曲線の同型類の完全な分類をおこなうついでに示されます.

標数 3 の体は暗号ではほとんど使われないので，省略します.

§3.6 楕円曲線の群構造

E を体 $\boldsymbol{F}_q$, $q = p^m$ 上定義された楕円曲線とする．E の $\boldsymbol{F}_q$-有理点の個数 $\#E(\boldsymbol{F}_q)$ を考えよう．これはこの加法群の位数となり，これから作られる暗号の強度を左右する重要な量である．各 $x \in \boldsymbol{F}_q$ に対し，楕円曲線の方程式から定まる y の値は高々 2 個なので，無限遠点も込めて常に $\#E(\boldsymbol{F}_q) \leq 2q+1$ が成り立つ．しかし，$\boldsymbol{F}_q$ での平方剰余がちょうど半分であることから類推して，y の 2 次方程式が解を持つような x の値も確率的に約半分であろうと考えられるので，q が大きくなったときは，漸近的に $\#E(\boldsymbol{F}_q) \sim q$ と想像される．これは実際に正しい：

定理 3.8 (Hasse) $\#E(\boldsymbol{F}_q) = q + 1 - t$ と書くとき，$|t| \leq 2\sqrt{q}$ が成り立つ.

Q この評価は，Weil により一般化され, Serre による精密化を経て, 種数 g の平面代数曲線について 有理点の総数 $a + 1 - t$, $|t| \leq g\lfloor 2\sqrt{q} \rfloor$ という Hasse-Weil-Serre の限界式が知られています.

Hasse の定理の証明は後で与えることにし，この定理から得られる結論を示しておきましょう．まず，この定理から，与えられた楕円曲線上の点をランダムに選ぶための確率的多項式時間のアルゴリズムが得られます．実際，$x_1 \in \boldsymbol{F}_q$ をランダムに選んだとき，解くべき方程式は，体の標数が 2 でないとき $y^2 = C$，標数が 2 のとき $y^2 + a_3 y = C$ の形です．この根は後述のように (存否の判定も込めて) 多項式時間で見付けられるので，Hasse の評価が有れば，一回の成功確率は少なく見積もっても $P = \dfrac{1}{2} - \dfrac{1}{\sqrt{q}}$ は有ります．(x の座標の選び方は $\#\boldsymbol{F}_q = q$ 通りですが，楕円曲線の無限遠点を除いた有理点は少なくとも $q - 2\sqrt{q}$ 個は有り，それらは，三つ以上が同じ x 座標を持つことはないので，一番可能性が低くても，少なくとも半分の個数だけは有理点の x 座標の候補となります．よって割り算すれば上の確率が出て来ます.) 故に，k 回続けて失敗する確率は $(1-P)^k = \left(\dfrac{1}{2} + \dfrac{1}{\sqrt{q}}\right)^k$ で，これは急速に 0 に近付きます．実際に，成功するまでの回数 k の期待値をまじめに計算すれば

$$\sum_{k=1}^{\infty} k(1-P)^{k-1}P = P\sum_{k=0}^{\infty} k(1-P)^{k-1} = P \cdot \frac{1}{P^2} = \frac{1}{P}$$

ここで,

$$\sum_{k=0}^{\infty} kx^{k-1} = \Big(\sum_{k=0}^{\infty} x^k\Big)' = \Big(\frac{1}{1-x}\Big)' = \frac{1}{(1-x)^2}$$

を用いました．成功するまでの回数の期待値は q が大きいとほぼ 2 回です．解 y_1 が一つ求まったら，$y^2 = C$ の場合は y_1 か $-y_1$ を，$y^2 + a_3 y = C$ の場合は y_1 か $y_1 + a_3$ をランダムに選べばよい．この方法だと，楕円曲線上の位数が 2 のある点を選ぶ確率が，そうでないある点を選ぶ確率の 2 倍になるが，位数 2 の点は 2 倍公式における λ の分母が 0 となるような x に対応するので，全部で高々 3 個しか存在せず，従って全体として位数 2 の点を選んでしまう確率は限りなく小さい．(実数体上の楕円曲線でいうと，位数 2 の点は接線が y 軸に平行となる点なので，ちょうど 3 個存在することが幾何学的に明らかですが，有限体の場合には必ずしもそうではありません．特に，標数が 2 の場合には，上で導いた公式から分かるように，体を拡大しても 0 個または 1 個しかないことに注意しましょう.)

Hasse の評価式における t が取り得る値は，次のように細かく調べられています．基本的な結果ですが，その証明は構成法を与えているのではなく，いわゆる抽象的存在定理なので，応用の観点からは結果を信じておけばよいでしょう.

補題 3.9 (Waterhouse) $q = p^m$ のとき，$\boldsymbol{F}_q$ 上の楕円曲線で，$\boldsymbol{F}_q$- 有理点の個数が $q + 1 - t$ であるようなものが存在するための必要十分条件は t が次のいずれかを満たすことである：

(i) $t \not\equiv 0 (\mathrm{mod}\ p)$ かつ $t^2 \leq 4q$.
(ii) m は奇数で次のいずれかが成り立つ：

(1) $t = 0$
(2) $t^2 = 2q,\ \ p = 2$
(3) $t^2 = 3q,\ \ p = 3$

(iii) m は偶数で次のいずれかが成り立つ：

(1) $t^2 = 4q$
(2) $t^2 = q,\ \ p \not\equiv 1 (\mathrm{mod}\ 3)$
(3) $t = 0,\ \ p \not\equiv 1 (\mathrm{mod}\ 4)$

$q = p$ が素数のときは，$|t| \leq 2\sqrt{p}$ の範囲の t に対して $\#E(\boldsymbol{F}_p) = p + 1 - t$ となるような $\boldsymbol{F}_p$ 上の楕円曲線が必ず存在することが (i) から分かります．しかもその分布はほぼ一様であることが次の定理で保証されます．このことが Lenstra による楕円曲線を用いた素因数分解法の基礎になっているのです．

定理 3.10 実際に計算可能な正の定数 c_1, c_2 が存在し，任意の素数 $p \geq 5$, および任意の部分集合 $S \subset [p+1-\sqrt{p}, p+1+\sqrt{p}]$ に対し，勝手に選んだ対 $(a, b) \in \boldsymbol{F}_p \times \boldsymbol{F}_p$ から作った方程式 $y^2 = x^3 + ax + b$ が $\#E(\boldsymbol{F}_p) \in S$ なる楕円曲線を定める確率 r_S は

$$\frac{\#S - 2}{2\lfloor\sqrt{p}\rfloor + 1} \frac{c_1}{\log p} \leq r_S \leq \frac{\#S}{2\lfloor\sqrt{p}\rfloor + 1} c_2 (\log p)(\log\log p)^2.$$

楕円曲線 E は $p \mid t$ のとき (従って，E の有限有理点の総数が p の倍数のとき) **超特異 (supersingular)** と呼ばれます．補題 3.8 から，また次のことが分かります．

系 3.11 E を $\boldsymbol{F}_q$ 上定義された楕円曲線とするとき，E が超特異となるための必要十分条件は $t^2 = 0, q, 2q, 3q, 4q$ のいずれかとなることである．

$p \mid t$ というだけなら, まだいくらでも可能性が有るのに, こんなに制限されてしまうのは面白いですね. 更に, $p = 2$ または 3 のとき，E が超特異であるための必要十分条件は $j(E) = 0$ であることが良く知られています．

次に $E(\boldsymbol{F}_q)$ の群構造を調べます．位数 n の加法群を $\boldsymbol{Z}_n$ で表すと，有限 Abel 群の基本構造定理により，任意の有限 Abel 群 G は

$$G = \boldsymbol{Z}_{n_1} \oplus \boldsymbol{Z}_{n_2} \oplus \cdots \oplus \boldsymbol{Z}_{n_s}, \qquad \text{ここに}\ \ n_1 \mid n_2 \mid \cdots \mid n_s$$

の形に一意的に分解されます．これは $\boldsymbol{Z}$-係数の正方行列の標準形と密接に関連しているので，$n_1, \ldots, n_s$ は単因子と呼ばれることもあります．ここでは G が型 $(n_1, \ldots, n_k)$ の群であるということにします．(G の階数 (rank) が s という人も居ますが，Abel 群の階数は，それに含まれる自由因子 $\boldsymbol{Z}$ の個数の意味で使うことの方が多いので，ここでは使わないことにします.)

定理 3.12 $E(\boldsymbol{F}_q)$ 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．

後に，$E(\boldsymbol{F}_q)$ の群構造を計算するアルゴリズムを紹介しますが，E が超特異の場合は，群構造は次のように定まります：

補題 3.13 (Schoof) $\#E(\boldsymbol{F}_q) = q + 1 - t$ とする．
(i) $t^2 = q, 2q, 3q$ のとき，$E(\boldsymbol{F}_q)$ は巡回群となる．
(ii) $t^2 = 4q$ のとき，

(1) $t = 2\sqrt{q}$ なら $E(\boldsymbol{F}_q) \simeq \boldsymbol{Z}_{\sqrt{q}-1} \oplus \boldsymbol{Z}_{\sqrt{q}-1}$
(2) $t = -2\sqrt{q}$ なら $E(\boldsymbol{F}_q) \simeq \boldsymbol{Z}_{\sqrt{q}+1} \oplus \boldsymbol{Z}_{\sqrt{q}+1}$

(iii) $t=0$ のとき，

(1) $q \not\equiv 3 (\mathrm{mod}\ 4)$ なら $E(\boldsymbol{F}_q)$ は巡回群

(2) $q \equiv 3 (\mathrm{mod}\ 4)$ なら $E(\boldsymbol{F}_q)$ は巡回群か，$\boldsymbol{Z}_{(q+1)/2} \oplus \boldsymbol{Z}_2$ に同型となる．

この補題の主張の大半は補題 3.8 と定理 3.12 を仮定すると初等的に確認できます：

その粗筋 まず，定理 3.12 より，群 $E(\boldsymbol{F}_q)$ の位数は $n_1 n_2$ で，かつ $n_1 \mid n_2$, $n_1 \mid q-1$ でなければならないことに注意する．以下複号は各場合の証明中一貫して同順とする．

$t^2 = q$ のとき, 補題 3.8 により $q = p^{2k}$ の形で, かつ $p \not\equiv 1 \bmod 3$. 定理 3.12 より $n_1 n_2 = p^{2k} \mp p^k + 1$, $n_1 \mid p^{2k} - 1 = (p^k+1)(p^k-1)$. $p^k \pm 1$ の共通因子は 2 だけで, n_1 は奇数なので, n_1 はこれら二つの因子のいずれか一方を割り切る．以下複号同順で $n_1 \mid \pm p^k + 1$ と仮定しよう．すると, $n_1 \mid p^{2k} \mp p^k + 1 - (\pm p^k + 1) = p^k(p^k \mp 2)$. n_1 の素因子は p ではないから, 必ず $\pm p^k + 1$ の方を割らねばならない. 従って $n_1 \mid p^k \mp 2$. よって $n_1 \mid \pm p^k + 1 \mp (p^k \mp 2) = 3$. しかし, もし $n_1 = 3$ だと，$n_1 \mid n_2$ より，$n_1 n_2 = p^{2k} \mp p^k + 1$ は 9 で割り切れなければならなくなるが，$3 \mid p^k \mp 2$ より，$p^k \pm 1 \equiv 0 \bmod 3$, よって $(p^k \pm 1)^2 = p^{2k} \pm 2p^k + 1 \equiv 0 \bmod 9$ となるから，$p^{2k} \mp p^k + 1 = (p^k \pm 1)^2 \mp 3p^k$ は決して 9 で割り切れない．よって $n_1 = 1$ でなければならず，巡回群.

$t^2 = 2q$ のときは，補題 3.8 より $q = 2^{2k+1}$ の形であり，$n_1 n_2 = 2^{2k+1} \mp 2^{k+1} + 1$. これと $n_1 \mid q - 1 = 2^{2k+1} - 1$ とから，$n_1 \mid \mp 2^{k+1} + 2$. $n_1 \neq 2$ だから, これより $n_1 \mid \mp 2^k + 1$. よって $n_1 \mid n_1 n_2 \pm 2^{k+1}(\mp 2^k + 1) = 1$ となるから, 巡回群.

$t^2 = 3q$ のときは，同じく $q = 3^{2k+1}$ の形であり，$n_1 n_2 = 3^{2k+1} \mp 3^{k+1} + 1$. これと $n_1 \mid q - 1 = 3^{2k+1} - 1$ とから，$n_1 \mid \mp 3^{k+1} + 2$. よって $n_1 \mid n_1 n_2 \pm 3^k(\mp 3^{k+1} + 2) = \mp 3^k + 1$. これと $n_1 \mid \mp 3^{k+1} + 2 = 3(\mp 3^k + 1) - 1$ とから $n_1 \mid -1$, よって巡回群.

$t = 0$ のとき，$n_1 \mid q-1, n_1 \mid q+1$ となり，従って $n_1 \mid 2$ だから，$n_1 = 1$ または 2 である．$n_1 = 2$ だと $2 \mid n_2$, 従って $4 \mid q+1$, すなわち $q \equiv -1 \equiv 3 \bmod 4$ となるから，対偶を取って $q \not\equiv 3 \bmod 4$ なら $n_1 = 1$, すなわち巡回群と決定する．

$t^2 = 4q$ のとき，補題 3.8 により $q = p^{2k}$ であり，$n_1 n_2 = q \mp 2\sqrt{q} + 1 = (p^k \mp 1)^2$, および $n_1 \mid q - 1 = (p^k - 1)(p^k + 1)$. $p^k + 1$ と $p^k - 1$ に共通因子は 2 しか無いので，2 以外で n_1 を割り切る因子があれば，それは $p^k \pm 1$ の因子では有り得ない．このことから，$n_1 = \dfrac{p^k \mp 1}{A}$, $n_2 = (p^k \mp 1)A$, の形でなければならないことが分かる．ここに A は $p^k \mp 1$ の約数である．上の補題は，ここで更に $A = 1$ となることを主張しているが，これは定理 3.12 だけからは出て来ないので，ここで一旦中止しておく．

$v_l(N)$ により N に含まれる素因子 l の重複度を表します (v は valuation の頭文字で，この値はいわゆる l-進付値の原型です.) 定理 3.12 から，次のことが分かります．

系 3.14 $N = \#E(\boldsymbol{F}_q)$ と置けば，

$$E(\boldsymbol{F}_q) \simeq \boldsymbol{Z}_{p^{v_l(N)}} \oplus \bigoplus_{l \mid N, l \neq p} (\boldsymbol{Z}_{l^{a_l}} \oplus \boldsymbol{Z}_{l^{b_l}}) \tag{3.15}$$

ここに，$a_l \geq b_l$, $a_l + b_l = v_l(N)$, $b_l \leq v_l(q-1)$. 特に，$\mathrm{GCD}\,(N, q-1) = 1$ なら, $E(\boldsymbol{F}_q)$ は巡回群となる．N が異なる素数の積に分解されるときも，$E(\boldsymbol{F}_q)$ は巡回群となる．

この分解は, Abel 群に関する初等的な知識 $\mathrm{GCD}\,(n_1, n_2) = 1$ なら $\boldsymbol{Z}_{n_1 n_2} = \boldsymbol{Z}_{n_1} \oplus \boldsymbol{Z}_{n_2}$ を繰り返し適用すれば得られます. p の因子が一つしか出ないことも, 定理 3.12 より小さい方の直和因子における p の指数が $\leq v_p(q-1) = 0$ でなければならないことから分かります.

次の補題は超特異でないとき，上が $E(\boldsymbol{F}_q)$ の可能な群構造を尽くしていることを主張したものです．

補題 3.15 $N = q + 1 - t$, $t \not\equiv 0 (\mathrm{mod}\ p)$, $t^2 \leq 4q$ とし，更に，$l \mid N$, $l \neq p$ について a_l, b_l を $a_l \geq b_l$, $a_l + b_l = v_l(N)$, $b_l \leq v_l(q-1)$ となるように取る．このとき，$\boldsymbol{F}_q$ 上の超特異でない楕円曲線で， $E(\boldsymbol{F}_q)$ の群構造が (3.15) となるものが存在する．

$\boldsymbol{F}_q$ 上の楕円曲線 E は，拡大体 $\boldsymbol{F}_{q^k}$ 上の楕円曲線とみなせ，$E(\boldsymbol{F}_q)$ は $E(\boldsymbol{F}_{q^k})$ の部分群となります．拡大体での有理点の個数は，Hasse 1937 により次のように決定されています．ちなみに，Weil

1949 はこれを一般の代数曲線に一般化し，さらに一般の代数多様体でも正しいだろうと予想したのが，ゼータ函数の零点分布に関する Riemann 予想の代数的アナロジーである Weil 予想の核心部分で，約 20 年後に Deligne 1980 により解決されました．

定理 3.16 (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．

最後に，代数的閉包まで持ち上げた楕円曲線 $E := E(\overline{\boldsymbol{F}_q})$ の群構造の説明をします．E は捻れ群です．すなわち，$\forall P \in E$ に対し，$\exists k \in \boldsymbol{N}$ が存在して $kP = \mathcal{O}$ となります．このような k の最小値を P の位数と呼びます．逆に，正整数 n を先に指定したとき，E の n-捻れ点 (n-torsion point) とは，位数 $\mid n$ なる点，すなわち $nP = \mathcal{O}$ を満たす点 P のことです．$E(\boldsymbol{F}_q)$, E の n-捻れ点の全体をそれぞれ $E(\boldsymbol{F}_q)[n]$, $E[n]$ と書くことにします．これらはそれぞれの元の群の部分群を成します．

命題 3.17 (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，$E[p^e] = \boldsymbol{Z}_{p^e}$.

この証明も後でやります．

n-捻れ点の基本的な例を見ておきましょう．

例 3.4 $\operatorname{char} \boldsymbol{F}_q \neq 2,3$ とし，楕円曲線 $E/\boldsymbol{F}_q : \{y^2 = x^3+ax+b\}$ を考える．
(1) 点 $P = (x,y)$ が位数 2 となる条件は，$P = -P = (x,-y)$, i.e. $y = 0$ である．これは，$x^3+ax+b=0$ の 3 個の異なる根 x_1, x_2, x_3 により与えられる．これに，自明な 2-捻れ点である単位元を合わせて，

$$E[2] = \{\mathcal{O}, (x_1,0), (x_2,0), (x_3,0)\}.$$

これは $E[2] = \boldsymbol{Z}_2 \oplus \boldsymbol{Z}_2$ という，上の命題の (1) の場合の例となっている．ただし，これらがすべて $\boldsymbol{F}_q$ 有理点とは限らない．
(2) 点 $P = (x,y)$ が位数 3 となる条件は，$2P = -P$. これは実数体上では，P における接線が再び曲線と交わる点が P であることを意味し，いわゆる変曲点に相当する．実の図だけを見ると 2 点しか無いように見えるが，$2P = -P$ を座標で書くと，

$$\Big(\frac{3x^2+a}{2y}\Big)^2 - 2x = x \qquad \therefore\ (3x^2+a)^2 - 12x(x^3+ax+b) = 0$$
$$\text{i.e. } 3x^4+6ax^2+12bx-a^2 = 0$$

これは，x の 4 次方程式で 4 根を持つ，それぞれに y の値が正負二つずつ存在するので，合計 8 点，単位元と合わせて 9 点が 3-捻れ点のすべてである．(この方程式が重根を持たないことは，その判別式を計算すると $-6912(4a^3+27b^2)^2$ となり，括弧内が $\Delta(E)$ であることから分かる.)

例 3.5 $q \equiv 2 (\mathrm{mod}\ 3)$ とし，楕円曲線 $E/\boldsymbol{F}_q : \{y^2 = x^3+b\}$ を考える．ここに，$b \in \boldsymbol{F}_q^\times$. q に対する仮定から，写像 $x \mapsto x^3$, 従って $x \mapsto x^3+b$ は $\boldsymbol{F}_q$ 上一対一，すなわち，$\boldsymbol{F}_q$ の置換を引き起こす．$\because\ 0 \mapsto 0$ なので，$\boldsymbol{F}_q^\times$ 上で考えると，$x \mapsto x^3$ は乗法群の準同型なので，$x^3 = 1$ の根が 1 のみなら単射，従って全射，1 以外に存在すれば，3 個は存在するので 3 対 1 の写像となる．$x^3 = 1$ と $x^{q-1} = 1$ とから，$q = 3k+2$ なら，$1 = x^{q-1} = x^{3k+1} = x$. ちなみに，$q = 3k+1$ なら，$1 = x^{q-1} = x^{3k}$. ここで $k = \dfrac{q-1}{3} < q-1$ より，$x^k \neq 1$ なる x が必ず存在し，そのとき x^k は $x^3 = 1$ の 1 以外の根となるから．$x \mapsto x^3$ は 3 対 1 の写像となる．
以上により，$q \equiv 2 (\mathrm{mod}\ 3)$ のときは，x^3+b が $\boldsymbol{F}_q$ の零以外の平方剰余となるような x がちょうど $(q-1)/2$ 個有り，そのそれぞれに対して y が二つずつ求まる．これと $(\sqrt[3]{-b}, 0)$ および $\mathcal{O}$ を合わせて，有理点の総数は $q+1$ となる．すなわち，この曲線は超特異である．補題 3.13 (iii) により，この群の型は $(\dfrac{q+1}{2}, 2)$ か $(q+1)$ のいずれかであり，しかも前者が起こり得るのは $q \equiv 3 (\mathrm{mod}\ 4)$, 従って $\dfrac{q+1}{2}$ が偶数のときだけであるから，もしこちらなら，位数 2 の点が少なくとも 4 個は存在する．

しかし $E(\boldsymbol{F}_q)$ の 2-捻れ群は $\mathcal{O}$ と $(\sqrt[3]{-b}, 0)$ の 2 点のみより成るので，$(q+1)$ すなわち巡回群と定まる．

上の例中で示された次の事実は, 初等的だが有限体上の楕円曲線の議論でよく使われるので, 補題の形にしておきましょう.

補題 3.18 $\boldsymbol{F}_q$ における写像 $x \mapsto x^3$ は, $q \equiv 1 \bmod 3$ のとき 3 対 1 , それ以外のとき 1 対 1 となる.

$q \equiv 0 \bmod 3$ のときは上で出てきませんでしたが, これは後述 (第 6 章参照) の Frobenius 写像の特別な場合で, 体の同型となるので, もちろん 1 対 1 です.

例 3.6 q を奇素数冪で $q \equiv 3 (\bmod 4)$ を満たすものとし，$a \in \boldsymbol{F}_q^\times$ に対して楕円曲線 $E/\boldsymbol{F}_q : y^2 = x^3 + ax$ を考える．
$q \equiv 3 (\bmod 4)$ より -1 は平方剰余でない．(実際，$x^2 = -1$ だと，$1 = x^{q-1} = x^{2+4k} = -1$ となり，不合理.) これと $(-x)^3 + a(-x) = -(x^3 + ax)$ より，$x^3 + ax \neq 0$ なる各 x に対して x か $-x$ のどちらか一方，かつ一方のみが E の点の x 座標となり得る．(平方剰余元は $\boldsymbol{F}_q^\times$ において指数 2 の部分群を成すので，“a が平方剰余 $\Longleftrightarrow$ $-a$ が平方非剰余 ”に注意せよ.) 他方，$x^3 + ax = 0$ なる $x \neq 0$ がもし有れば，$(x, 0), (-x, 0)$ が E の点となる．よってこのとき, すなわち $-a$ が平方剰余，すなわち，a が平方非剰余のときは，これらに $(0, 0)$ と $\mathcal{O}$ を加えて E の位数は $\dfrac{q-3}{2} \times 2 + 2 + 1 + 1 = q + 1$ となる．すなわち，E は超特異である．a が平方剰余のときは，$x \neq 0$ は $x^3 + ax \neq 0$ を意味するので, E の位数は $\dfrac{q-1}{2} \times 2 + 1 + 1 = q + 1$ で，やはり超特異である．
位数 2 の点は $\mathcal{O}$, $(0, 0)$ 以外に有るとすれば $(\pm\sqrt{-a}, 0)$ なので，a が平方非剰余のときこれらは $\boldsymbol{F}_q$-有理点となって，群の型は $(\frac{q+1}{2}, 2)$ となり，a が平方剰余のときは $(q+1)$ となる．ここで扱った方程式を持つ楕円曲線は，j-不変量が必ず 1728 に等しいので，これから，代数的閉体でない場合に，j-不変量が同じでも同型にならない例が得られる．

上の例中で示された次の事実も, 補題の形にしておきましょう.

補題 3.19 $q \equiv 3 \bmod 4$ のとき -1 は $\boldsymbol{F}_q$ において平方非剰余であり, その他のときは平方剰余となる.

$q \equiv 1 \bmod 4$ のときは, 乗法群 $\boldsymbol{F}_q^\times$ の生成元を g とすると, $g^{(q-1)/2}$ は $x^2 = g^{q-1} = 1$ を満たすが 1 ではないので -1. 従って $g^{(q-1)/4}$ が $x^2 = -1$ の解となります. 今回は, 残った $q \equiv 0, 2 \bmod 4$ の場合は $-1 = 1$ となるので自明です.

問題 3.5 (1) 有限体 $\boldsymbol{F}_7$ 上，方程式 $y^2 = x^3 + 2$ で定義された楕円曲線の有理点が成す加法群の群構造を示せ．ただし無限遠点を $\mathcal{O}$ で表せ．
(2) 同じく $\boldsymbol{F}_{13}$ 上の方程式 $y^2 = x^3 + x + 2$ で定義された楕円曲線の有理点が成す加法群の群構造を示せ．

問題 3.6 (1) 有限体 $\boldsymbol{F}_{2^2}$ の演算を説明せよ．
(2) この体の上で方程式 $y^2 + y = x^3 + x + 1$ で定義された楕円曲線, および $y^2 + xy = x^3 + x^2 + 1$ で定義された楕円曲線について, すべての $\boldsymbol{F}_{2^2}$-有理点を挙げよ．また，これらの楕円曲線の群構造を示せ．