ミレニアム大学入試の背景を探る (1)

宮川 幸隆（みやかわ ゆきたか）

本稿では，まず2000年の大阪大学・理，工，基礎工学部(後期)の入試問題の背景を探ります．その問題とは次のようなものです：

> 数列 $\{a_n\}$, $\{b_n\}$ を $a_1=-2$, $b_1=3$,
> $a_{n+1}=3a_n+2b_n$, $b_{n+1}=4a_n+3b_n$ $(n=1, 2, 3, \cdots\cdots)$
> で定める．
> (1) すべての番号 n について $b_n^2-2a_n^2=1$ であることを示せ．
> (2) $c_n=\sqrt{2}\,a_n+b_n$ とするとき，c_n を n を用いて表せ．
> (3) b_n が最小となる番号 n を求めよ．
> (4) (3)で求められた n の値を m とするとき，$n\geqq m$ ならば $b_{n+1}\geqq b_n$ となることを示せ．

本問の背景は**実2次体の単数**です．筆者は「数研通信・数学 No.9, No.25, No.33」で，それを背景に持つ入試問題を取り上げましたが，No.9 等をお持ちでない方もいらっしゃるでしょうから，実2次体の単数について簡潔にまとめてみたいと思います．

m を1以外の平方因数をもたない整数とし，x, y を任意の有理数として

$$x+y\sqrt{m}$$

のような数全体の集合を考えます．このような集合は**2次体**と呼ばれ，$\mathrm{K}(\sqrt{m})$ という記号で表されます．特に $m>0$ のときは**実の**2次体と呼ばれます．

2次体 $\mathrm{K}(\sqrt{m})$ に属する2つの数

$$\alpha=x+y\sqrt{m},\quad \alpha'=x-y\sqrt{m}$$

を互いに**共役**であるといいます．

互いに共役な2数の和および積は有理数です：

$$\alpha+\alpha'=2x,\quad \alpha\alpha'=x^2-my^2$$

特に積 $\alpha\alpha'$ を α または α' の**ノルム**(記号 $N\alpha$)と呼びます．

$\mathrm{K}(\sqrt{m})$ の特別な要素として，$\mathrm{K}(\sqrt{m})$ の“整数”なるものを定義することを考えます．“整数”の定義を2次体 $\mathrm{K}(\sqrt{m})$ の数の上に拡張するに当たっては，次の条件を目標とします；

(I) α, β が“整数”ならば，$\alpha\pm\beta$, $\alpha\beta$ も“整数”である．

(II) α が“整数”ならば，それと共役な α' も“整数”である．

(III) $\{\alpha\,|\,\alpha$：“整数”かつ α：有理数$\}$
$=$(普通の整数全体の集合)

(IV) “整数”の範囲は上記3つの条件のもとにおいてできる限り広くする．

いま，a, b を普通の整数(**有理整数**と呼ぶ)として

$$a+b\sqrt{m}$$

のような形の数を $\mathrm{K}(\sqrt{m})$ の“整数”とすることにすれば，上記(I), (II), (III)の条件が満たされることは明らかですが，ここに特別の考慮を要するのは条件(IV)です．

さて，上記(I)～(III)の条件を満たすような，$\mathrm{K}(\sqrt{m})$ の，最大の部分集合の要素を改めて $\mathrm{K}(\sqrt{m})$ の“整数”と呼ぶことにすると，$m=2$ のとき，次の定理が成り立ちます．

> **定理1** 2次体 $\mathrm{K}(\sqrt{2})$ の“整数”は，
> $x+y\sqrt{2}$ (ここに x, y は有理整数)である．

2次体 $\mathrm{K}(\sqrt{m})$ の“整数”に対しても，有理整数の場合と同様に，整除の定義を行うことができます．すなわち，$\mathrm{K}(\sqrt{m})$ の“整数” α, β の商 $\frac{\alpha}{\beta}=\gamma$ が再び $\mathrm{K}(\sqrt{m})$ の“整数”であるとき，α は β で割り切れるといい，α を β の倍数，β を α の約数といいます．すべての“整数”の約数であるような“整数”を**単数**と呼びます．単数は1の約数に他なりません．

実2次体 $\mathrm{K}(\sqrt{m})$ の単数については，次の**著しい定理**が成り立ちます：

定理2　実2次体 $K(\sqrt{m})$ の1より大なる任意の単数は，そのような単数のうちの最小のもの ε_0 によって

$$\varepsilon_0^{\,n}\quad (n：自然数)$$

の形に表される．

また，2次体 $K(\sqrt{m})$ の“整数”のノルムについては，次の定理が成り立ちます：

定理3　α，β を同一の2次体の“整数”とする．α が β で割り切れるならば，有理整数 $N\alpha$ は有理整数 $N\beta$ で割り切れる．

証明　$\alpha=\beta\gamma$ で，γ は“整数”であるから，$N\gamma$ は有理整数で［∵ 左段の(I)，(II)，(III)による］，
$N\alpha=N\beta\cdot N\gamma$ (各自確かめて下さい)．

(証明終)

次に α を $K(\sqrt{m})$ の単数とすると，α は1の約数ですから

$$\alpha\beta=1 \quad\cdots\cdots ①$$

であるような $K(\sqrt{m})$ の“整数” β が存在します．
①により

$$N\alpha\cdot N\beta=N1=1$$

であるから，$N\alpha=\pm1$ となります．

このように，**2次体 $K(\sqrt{m})$ の単数 α は $N\alpha=\pm1$ を満たします．**

さて，大阪大の問題に戻りましょう：

まず，実2次体 $K(\sqrt{2})$ を考えます．

いま述べたばかりのことによって，$K(\sqrt{2})$ の単数全体の集合は

$G=\{x+y\sqrt{2}\,|\,x,\ y：有理整数,\ x^2-2y^2=\pm1\}$

です．

G の要素で，1より大なるもののうちの最小のもの ε_0 を求めることを考えましょう．

$\varepsilon_0=a+b\sqrt{2}>1 \quad\cdots\cdots ⑤$ とおくと

$$a^2-2b^2=\pm1$$

$$\therefore\quad |a-b\sqrt{2}|=\frac{1}{|a+b\sqrt{2}|}<1$$

$$\therefore\quad \begin{cases} a-b\sqrt{2}>-1 & \cdots\cdots ⑥ \\ -1<b\sqrt{2}-a & \cdots\cdots ⑦ \end{cases}$$

したがって，⑤+⑥，⑤+⑦から　$a>0$，$b>0$
これを満たす a，b のうちで，$a+b\sqrt{2}$ を最小にし $a^2-2b^2=\pm1$ を満たすものは　$(a,\ b)=(1,\ 1)$．
逆に，このとき⑤を満たすから　$\varepsilon_0=1+\sqrt{2}$．

さて，大阪大の連立漸化式は

$$\begin{pmatrix} b_{n+1} \\ a_{n+1} \end{pmatrix}=\begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} b_n \\ a_n \end{pmatrix}$$

と表されるので

$$A=\begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}$$

とおきます．数列 $\{a_n\}$，$\{b_n\}$ は

$$\begin{pmatrix} b_n \\ a_n \end{pmatrix}=A^{n-1}\begin{pmatrix} 3 \\ -2 \end{pmatrix}\quad (n=1,\ 2,\ \cdots\cdots)$$

によって定まるので，

$$A\begin{pmatrix} 3 \\ -2 \end{pmatrix}=\begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} 3 \\ -2 \end{pmatrix}=\begin{pmatrix} 1 \\ 0 \end{pmatrix},$$

$$A^2\begin{pmatrix} 3 \\ -2 \end{pmatrix}=\begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}=\begin{pmatrix} 3 \\ 2 \end{pmatrix}\iff 3+2\sqrt{2}=\varepsilon_0^2,$$

$$A^3\begin{pmatrix} 3 \\ -2 \end{pmatrix}=\begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} 3 \\ 2 \end{pmatrix}=\begin{pmatrix} 9+8 \\ 6+6 \end{pmatrix}=\begin{pmatrix} 17 \\ 12 \end{pmatrix}$$
$$\iff 17+12\sqrt{2}=(\varepsilon_0^2)^2,$$

……

という対応を考えると，任意の自然数 n に対して

$$\begin{pmatrix} b_{n+2} \\ a_{n+2} \end{pmatrix}=A^{n+1}\begin{pmatrix} 3 \\ -2 \end{pmatrix}$$
$$\iff (\varepsilon_0^2)^n=b_{n+2}+a_{n+2}\sqrt{2}$$

と対応していて(正確には帰納法による)，

$$\boldsymbol{b_{n+2}{}^2-2a_{n+2}{}^2=N(\varepsilon_0^{2n})=(N\varepsilon_0)^{2n}=1}$$

が任意の自然数 n に対して成り立つ．また，
$(b_1,\ a_1)=(3,\ -2)$，$(b_2,\ a_2)=(1,\ 0)$ であるから，

$$b_1{}^2-2a_1{}^2=b_2{}^2-2a_2{}^2=1$$

も成り立ち，大阪大の問題の(1)が示された．
また，上の考察によって

$$c_{n+2}=(\varepsilon_0^2)^n=(3+2\sqrt{2})^n\quad (n=1,\ 2,\ \cdots\cdots),$$

すなわち

$$c_n=(3+2\sqrt{2})^{n-2}\quad (n=3,\ 4,\ \cdots\cdots)$$

であるが，

$$c_2=\sqrt{2}\,a_2+b_2=1=(3+2\sqrt{2})^{2-2},$$

$$c_1=\sqrt{2}\,a_1+b_1=3-2\sqrt{2}=\frac{1}{3+2\sqrt{2}}$$

であるから，

$$\boldsymbol{c_n=(3+2\sqrt{2})^{n-2}\quad (n=1,\ 2,\ \cdots\cdots)}$$

これが大阪大の問題の(2)の答えである．更に，

$$\varepsilon_0'=1-\sqrt{2}$$

であり，任意の自然数 n に対して

$$\{(\varepsilon_0')^2\}^n=b_{n+2}-a_{n+2}\sqrt{2},$$

$$b_{n+2}=\frac{{\varepsilon_0}^{2n}+\{(\varepsilon_0')^2\}^n}{2} \quad \cdots\cdots ⑧$$

$$>\sqrt{(\varepsilon_0\varepsilon_0')^{2n}}=1 \quad \cdots\cdots ⑨$$

であるから，大阪大の問題の(3)の答は $\boldsymbol{n=2}$ となる．最後に，

$$n\geqq 2 \text{ ならば } b_{n+1}\geqq b_n$$

すなわち，

$$n\geqq 1 \text{ ならば } b_{n+2}\geqq b_{n+1} \quad \cdots\cdots ⑩$$

を示すのであるが，$n=1$ のときの⑩の成立は，⑨と $b_2=1$ とから明らかである．そこで $n\geqq 2$ とする．このとき⑧から，

$$b_{n+2}-b_{n+1}=\frac{{\varepsilon_0}^{2n}+(\varepsilon_0')^{2n}-{\varepsilon_0}^{2(n-1)}-(\varepsilon_0')^{2(n-1)}}{2}$$

$$=\frac{\{{\varepsilon_0}^{2n-1}+(\varepsilon_0')^{2n-1}\}(\varepsilon_0+\varepsilon_0')}{2}={\varepsilon_0}^{2n-1}+(\varepsilon_0')^{2n-1}$$

>0 $[\because\ {\varepsilon_0}^{2n-1}>1,\ |\varepsilon_0'|=\sqrt{2}-1<1]$

となり，大阪大の問題の(4)は $\boldsymbol{b_{n+1}\geqq b_n}$ を

$$\boldsymbol{b_{n+1}>b_n}$$

に替えても示された．

次に，2000年の東北大学・理系(前期)の入試問題の背景を探ります．その問題とは次のようなものです：

> 実数 a，b，c，d が $ad-bc\neq 0$ を満たすとき，関数 $f(x)=\dfrac{ax+b}{cx+d}$ について，次の問いに答えよ．
> (1) $f(x)$ の逆関数 $f^{-1}(x)$ を求めよ．
> (2) $f^{-1}(x)=f(x)$ を満たし，$f(x)\neq x$ となる a，b，c，d の関係式を求めよ．
> (3) $f^{-1}(x)=f(f(x))$ を満たし，$f(x)\neq x$ となる a，b，c，d の関係式を求めよ

$\mathbb{R}$ を実数全体の集合とし，実数を成分とする 2×2 型の行列全体の集合を $\mathrm{M}_2(\mathbb{R})$ で表す．行列 α の行列式を $\det(\alpha)$ で表し，

$$\mathrm{GL}_2(\mathbb{R})=\{\alpha\in\mathrm{M}_2(\mathbb{R})\,|\,\det(\alpha)\neq 0\}$$

とおく．また，$x(\in\mathbb{R})$ と

$\alpha=\begin{pmatrix}a & b\\ c & d\end{pmatrix}(\in\mathrm{GL}_2(\mathbb{R}))$ とに対し，$\alpha x=\dfrac{ax+b}{cx+d}$

と定める．このとき，

$$(\boldsymbol{\alpha\beta})\boldsymbol{x}=\boldsymbol{\alpha}(\boldsymbol{\beta x})\ (\boldsymbol{\alpha},\ \boldsymbol{\beta}\in\mathrm{GL}_2(\mathbb{R}),\ \boldsymbol{x}\in\mathbb{R})$$

が成り立つ．これによって，関数 $(\alpha^{-1})x$ は関数 αx の逆関数であるから，

(1) $f^{-1}(x)=\begin{pmatrix}a & b\\ c & d\end{pmatrix}^{-1}x=\boldsymbol{\dfrac{dx-b}{-cx+a}}$ である．

また，$f^{-1}(x)=f(x)\iff(\alpha^{-1})x=\alpha x$

$\iff(\alpha^2)x=x$

$\iff \alpha^2=kE$ $(k\neq 0,\ E$；単位行列$)$

$\iff\begin{pmatrix}a^2+bc & b(a+d)\\ c(a+d) & bc+d^2\end{pmatrix}=\begin{pmatrix}k & 0\\ 0 & k\end{pmatrix}$

であるから，(2)の a，b，c，d の関係式としては，

$$a=d \text{ or } a+d=0$$

が成り立つことが必要である．しかるに $a=d$ とすると，i) $b=0$ or $c=0$ のとき，

$ad-bc=a^2\neq 0$ から，$a\neq 0$ でなければならず

$b=c=0$ となって，$f(x)=x$ となってしまう．

ii) $b\neq 0$ かつ $c\neq 0$ のときは，$a+d=0$ となることが必要で，いずれにしても(2)の関係式としては $a+d=0$ が必要だが，これは十分でもあるので，(2)の答は $\boldsymbol{a+d=0}$ である．最後に，

$f^{-1}(x)=f(f(x))\iff(\alpha^{-1})x=(\alpha^2)x\iff(\alpha^3)x=x$

$$\iff\begin{pmatrix}a^3+2abc+bcd & b(a^2+ad+bc+d^2)\\ c(a^2+ad+bc+d^2) & abc+2bcd+d^3\end{pmatrix}=\begin{pmatrix}k & 0\\ 0 & k\end{pmatrix}$$

であるから，i) $b\neq 0$ or $c\neq 0$ のときは(3)の関係式として $a^2+ad+bc+d^2=0$ が必要である．

ii) $b=c=0$ のときは $a=d$ or $a^2+ad+d^2=0$ が必要であるが $a=d$ だとすると，$f(x)=x$ となってしまうから，このときも

$$a^2+ad+d^2=a^2+ad+bc+d^2=0$$

が必要で，いずれにしても(3)の関係式としては

$$a^2+ad+bc+d^2=0$$

が必要だが，これは十分でもある．

$[\because$ i) $b=0$ or $c=0$ のときは $a^3=d^3$ である．

ii) $b\neq 0$ かつ $c\neq 0$ のときは

$a^3-d^3+abc-bcd$

$=a(-ad-bc-d^2)+d(a^2+ad+bc)+abc-bcd$

$=-a^2d-abc-ad^2+a^2d+ad^2+bcd+abc-bcd$

$=0]$

したがって，(3)の答は $\boldsymbol{a^2+ad+bc+d^2=0}$ である．

(静岡県立三島高等学校)

ミレニアム大学入試の背景を探る (2)

宮川 幸隆（みやかわ ゆきたか）

§1. 実数体上の楕円曲線

$\mathbb{R}$ を**実数体**とする．

$a, b, c, d \in \mathbb{R}$；$a \neq 0$ であって，x の3次方程式

$$ax^3+bx^2+cx+d=0$$

が重解を持たないとき，曲線

$$E : y^2=ax^3+bx^2+cx+d$$

を $\mathbb{R}$ 上の**楕円曲線**と呼ぶ．集合，

$$E(\mathbb{R})=\{(x, y) ; y^2=ax^3+bx^2+cx+d\}\cup\{O\}$$

に**可換群**の構造を入れよう：

(I) Oを**単位元**とする：

$$P+O=O+P=P \quad (P\in E(\mathbb{R}))$$

(II) $P\neq O$ かつ $Q\neq O$ のとき $P+Q$ を定義するのであるが，$P=(x_1, y_1)$，$Q=(x_2, y_2)$ であるとし，まず

i) $x_1\neq x_2$ の場合を考える：

このとき，直線PQの方程式

$$(1)\quad y=\frac{y_2-y_1}{x_2-x_1}(x-x_1)+y_1$$

を E の方程式に代入して

$$ax^3+rx^2+sx+t=0 \quad (r, s, t\in\mathbb{R})$$

の形の3次方程式を得るが，左辺は

$$a(x-x_1)(x-x_2)(x-x_3) \quad (x_3\in\mathbb{R})$$

の形に因数分解される．(1)で $x=x_3$ とし，

$$-y_3=\frac{y_2-y_1}{x_2-x_1}(x_3-x_1)+y_1$$

として，$P+Q=(x_3, y_3)$ と定義する．このとき，

$$(2)\quad y_3=-\frac{y_2-y_1}{x_2-x_1}(x_3-x_1)-y_1,$$

$$(3)\quad x_3=\frac{1}{a}\left(\frac{y_2-y_1}{x_2-x_1}\right)^2-\frac{b}{a}-x_1-x_2$$

となる．(2)は明らかであるが，(3)は次のように証明される：

(1)を E の方程式に代入すると，

$$ax^3+bx^2+cx+d$$
$$=\left(\frac{y_2-y_1}{x_2-x_1}\right)^2(x-x_1)^2+2y_1\frac{y_2-y_1}{x_2-x_1}(x-x_1)+{y_1}^2$$

よって，$ax^3+bx^2+cx+d-{y_1}^2$ は $x-x_1$ で割り切れるから，

a	b	c	$d-{y_1}^2$	$\lfloor x_1$
	ax_1	$ax_1^2+bx_1$	$-d+{y_1}^2$	
a	ax_1+b	$ax_1^2+bx_1+c$	0	

よって，ax^3+rx^2+sx+t を $x-x_1$ で割ったときの商は

$$ax^2+(ax_1+b)x+(ax_1^2+bx_1+c)$$
$$-\left(\frac{y_2-y_1}{x_2-x_1}\right)^2(x-x_1)-2y_1\frac{y_2-y_1}{x_2-x_1}$$
$$=ax^2+\left\{ax_1+b-\left(\frac{y_2-y_1}{x_2-x_1}\right)^2\right\}x+\text{Const.}$$

であって，これは $x-x_2$ で割り切れるから，

a	$ax_1+b-\left(\frac{y_2-y_1}{x_2-x_1}\right)^2$	Const	$\lfloor x_2$
	ax_2	Const.	
a	$a(x_1+x_2)+b-\left(\frac{y_2-y_1}{x_2-x_1}\right)^2$	0	

これから

$$a(x-x_3)=a\left\{x+x_1+x_2+\frac{b}{a}-\frac{1}{a}\left(\frac{y_2-y_1}{x_2-x_1}\right)^2\right\}$$

となるから(3)を得る．

ii) $x_1=x_2$ の場合：

$y_1=-y_2$ ならば $P+Q=O$ と定義する．

$y_1\neq -y_2$ ならば $P=Q$ かつ $y_1\neq 0$ であって，E の方程式の両辺を x で微分すると，

$$2yy'=3ax^2+2bx+c$$

であるから，点Pにおける曲線 E の接線の方程式

$$(4)\quad y=\frac{3ax_1^2+2bx_1+c}{2y_1}(x-x_1)+y_1$$

を E の方程式に代入して

$$ax^3+rx^2+sx+t=0 \quad (r, s, t\in\mathbb{R})$$

を得るが，左辺は

$$a(x-x_1)^2(x-x_3) \quad (x_3\in\mathbb{R})$$

の形に因数分解される．(4)で $x=x_3$ とし，

$$-y_3=\frac{3ax_1^2+2bx_1+c}{2y_1}(x_3-x_1)+y_1$$

として，P+Q(=P+P=2P)=(x_3, y_3) と定義する．このとき

(5) $y_3=\dfrac{3ax_1^2+2bx_1+c}{2y_1}(x_1-x_3)-y_1$,

(6) $x_3=\dfrac{1}{a}\left(\dfrac{3ax_1^2+2bx_1+c}{2y_1}\right)^2-\dfrac{b}{a}-2x_1$

となる．(5)は明らかであるが，(6)は次のように証明される：(4)をEの方程式に代入すると，

$$ax^3+bx^2+cx+d$$
$$=\left(\frac{3ax_1^2+2bx_1+c}{2y_1}\right)^2(x-x_1)^2$$
$$+(3ax_1^2+2bx_1+c)(x-x_1)+y_1^2$$

よって，ax^3+rx^2+sx+t を $x-x_1$ で割ったときの商は，上と同様にして，

$ax^2+(ax_1+b)x+(ax_1^2+bx_1+c)$

$-\left(\dfrac{3ax_1^2+2bx_1+c}{2y_1}\right)^2(x-x_1)-(3ax_1^2+2bx_1+c)$

であって，これを $x-x_2=x-x_1$ で割ったときの商は，やはり上と同様にして，

$$ax+2ax_1+b-\left(\frac{3ax_1^2+2bx_1+c}{2y_1}\right)^2$$

であるから，やはり上と同様にして(6)を得る．

以上で**和** P+Q を定義したが，この和に関して E(ℝ) が**可換群**になっていることを示すことができる．(**結合法則**を示すのが大変なので深入りはしないが，徹底的に深入りして**代数幾何**または**代数函数論**を用いればエレガントに示される．)ちなみに**逆元**については次のようになる：

(iii) E(ℝ)∋P=(x, y)≠O に対して，

$$-P=(x, -y).$$

定理1 {P∈E(ℝ)；2P=O}
={O}∪{(x, y)(≠O)∈E(ℝ)；$y=0$}.

証明 O∈{P∈E(ℝ)；2P=O} は

$$O+O=O$$

により明らかである．

P=(x_1, y_1)(≠O)∈E(ℝ) かつ $y_1=0$ とする．

P=(x_2, y_2) でもあるとすると，

$x_1=x_2$ かつ $y_1=y_2=0$,

∴ $x_1=x_2$ かつ $y_1=0=-y_2$.

よって，上のii)から，2P=P+P=O.

したがって，⊇は成り立つ．

逆に，P=(x_1, y_1)(≠O)∈E(ℝ) かつ 2P=O かつ $y_1\neq 0$ とする．P=(x_2, y_2) でもあるとすると，

$x_1=x_2$ かつ $y_1=y_2\neq 0$,

∴ $x_1=x_2$ かつ $y_1\neq -y_2$.

よって，やはり上のii)から，2P≠O となり矛盾する．よって，⊆も成り立つ．　(証明終)

次に，可換群 E(ℝ) の単位元Oの意味を与えよう：

集合 $X=\{$比$(x:y:z)$；$x, y, z\in\mathbb{R}$ かつ $(x, y, z)\neq(0, 0, 0)$ かつ $y^2z=ax^3+bx^2z+cxz^2+dz^3\}$

を考え，写像

$$\begin{array}{ccc} E(\mathbb{R}) & \longrightarrow & X \\ \cup & & \cup \\ (x, y) & \longrightarrow & \text{比}(x:y:1) \\ O & \longrightarrow & \text{比}(0:1:0) \end{array}$$

によって E(ℝ) を X と同一視する．X においては，Oも他の点と同等な存在感を得ている．

X に自然な位相を与えれば，楕円曲線E上の点(x, y)がEのグラフの上方へ上方へと，あるいは下方へ下方へと無限の彼方へ向かうとき，

$$(x, y)=\text{比}(x:y:1)=\text{比}\left(\frac{x}{y}:1:\frac{1}{y}\right)$$

は実際に O=(0：1：0) に収束する．

§2. 東京理科大学・理学部のミレニアム入試問題

2000年の大学入試問題に，§1の「実数体上の楕円曲線」の内容を背景に持つ，東京理科大学・理学部の入試問題が現われました．その問題とは次のようなものです：

方程式 $y^2=x^3-x$ が表す曲線Cを考察する．

(1) 関数 $y=\sqrt{x^3-x}$ について，次を求めよ．

(a) xのとり得る値の範囲(定義域)

(b) この関数が極大となるxの値

(c) この関数のグラフの変曲点のx座標

(求める答えは，たとえば $\sqrt{\dfrac{5+3\sqrt{7}}{2}}$ のように，根号を二重に含む数である．)

(2) 曲線Cについて，次を求めよ．

(a) Cとx軸の交点の座標

(b) y軸に平行なCの接線

(3) 曲線Cの概形をかけ．

(4) 曲線C上の点$P(a,\ b)\ (b>0)$における接線をℓ_aで表し，ℓ_aとCの共有点を$P(a,\ b)$，$Q(r,\ s)$とする．ただしℓ_aとCの共有点が$P(a,\ b)$のみのときは，$P(a,\ b)=Q(r,\ s)$とする．このとき，rはaの関数となるので，$r=g(a)$とおく．

(a) $g(a)$を求めよ．(ヒント：ℓ_aとCの共有点のx座標が満たす方程式において，$x=a$は重解となっている．)

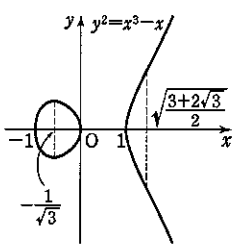
(b) 省略．

解説 (1)は普通に，微分法等を用いて解決します．ちなみに，(a)の答は $-1\leqq x\leqq 0,\ x\geqq 1$，(b)，(c)の答はそれぞれ $x=-\dfrac{1}{\sqrt{3}}$，$x=\sqrt{\dfrac{3+2\sqrt{3}}{3}}$ となります．(2)も普通に解決し，(a)の答は

$$(\pm 1,\ 0),\ (0,\ 0)$$

(b)の答は $x=\pm 1,\ 0$ となります．

(3)も普通に解決し，Cは $y=\sqrt{x^3-x}$ と $y=-\sqrt{x^3-x}$ を合わせたものとして，その概形は右のようになります：



さて，(4)の(a)の解説をするために§1の結果を用いましょう：まず

$$x^3-x=0$$

は重解を持たないので，Cは$\mathbb{R}$上の楕円曲線です．§1のii)の場合と逆元の定義(III)とから，

$$Q=-2P$$

ですから，§1の(6)とから，

$$r=\left(\frac{3a^2-1}{2b}\right)^2-2a$$

$$=\frac{9a^4-6a^2+1-8ab^2}{4b^2},$$

これと $b^2=a^3-a$ とから，

$$r=\frac{9a^4-6a^2+1-8a(a^3-a)}{4(a^3-a)}$$

$$=\frac{\boldsymbol{a^4+2a^2+1}}{\boldsymbol{4(a^3-a)}}$$

となり，これが(4)の(a)の背景です．もう少し言及しますと，ℓ_aとCの共有点が$P(a,\ b)$のみのときとは，PがCの**変曲点**であるときに他ならず，このときは，$a=\sqrt{\dfrac{3+2\sqrt{3}}{3}}$ で，

$$r=\frac{a^4+2a^2+1}{4(a^3-a)}=\frac{(a^2+1)^2}{4a(a^2-1)}$$

$$=\frac{\left(\dfrac{3+2\sqrt{3}}{3}+1\right)^2}{4\sqrt{\dfrac{3+2\sqrt{3}}{3}}\left(\dfrac{3+2\sqrt{3}}{3}-1\right)}$$

$$=\frac{\dfrac{2^2}{3^2}(3+\sqrt{3})^2}{\dfrac{2^3\sqrt{3}}{3}\sqrt{\dfrac{3+2\sqrt{3}}{3}}}=\frac{12+6\sqrt{3}}{6\sqrt{3+2\sqrt{3}}}$$

$$=\sqrt{\frac{(2+\sqrt{3})^2(2\sqrt{3}-3)}{12-9}}=\sqrt{\frac{3+2\sqrt{3}}{3}}$$

$$=a$$

と確かになっています．

最後に(2)の(a)，(b)についてですが，§1の定理1によれば，Cとx軸の交点をPとするとき，$2P=O$となります．このことは，Cとx軸の交点におけるCの接線がy軸に平行となることを意味しますが，逆に，y軸に平行なCの接線とCとの接点は，Cとx軸の交点であることも，§1の定理1が意味しているのです．このことが(2)の背景です(左のCのグラフも参照して下さい)．

〈参 考 文 献〉

岩波講座　現代数学の基礎，数論1 Fermat の夢，
加藤和也・黒川信重・斎藤毅 著，岩波書店

(静岡県立三島高等学校)