大学入試の背景を探る

—— 代数的整数の話 ——

宮川（みやかわ） 幸隆（ゆきたか）

本稿では，次の問題の背景を探ります．

> a，b を整数，u，v を有理数とする．
> $u+v\sqrt{3}$ が $x^2+ax+b=0$ の解であるならば，u と v は共に整数であることを示せ．ただし $\sqrt{3}$ が無理数であることは使ってよい．
> （1999年・京都大・後期・理系）

§1．二次体$\mathbb{Q}(\sqrt{3})$の整数

集合$\mathbb{Q}(\sqrt{3})=\{u+v\sqrt{3}\,|\,u,\ v$ は有理数$\}$ は**二次体**と呼ばれます．

二次体$\mathbb{Q}(\sqrt{3})$に属する２つの数

$$\alpha=u+v\sqrt{3},\quad \alpha'=u-v\sqrt{3}$$

を互いに**共役**であるといいます．

$\mathbb{Q}(\sqrt{3})$の特別な要素として，$\mathbb{Q}(\sqrt{3})$の〝整数〟なるものを定義することを考えます．〝整数〟の定義を二次体$\mathbb{Q}(\sqrt{3})$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

$$a+b\sqrt{3}$$

のような形の数を$\mathbb{Q}(\sqrt{3})$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．そして，（Ｉ）〜（III）の条件を満たす最大の部分集合$[\subseteqq\mathbb{Q}(\sqrt{3})]$の要素を$\mathbb{Q}(\sqrt{3})$の〝整数〟と改めて定義すると，次の定理が成り立ちます：

> **定理１** 二次体$\mathbb{Q}(\sqrt{3})$の〝整数〟は，
> $x+y\sqrt{3}$（ここに，x，y は有理整数）
> なる形の数に限る．

この定理によると，二次体$\mathbb{Q}(\sqrt{3})$の〝整数〟は，x，y を有理整数として，

$$\alpha=x+y\sqrt{3}$$

と表されます．$\alpha'=x-y\sqrt{3}$ とすると，α と α' とは互いに共役であり，これらの和と積は有理整数です．

$$\alpha+\alpha'=2x,\quad \alpha\alpha'=x^2-3y^2$$

これらを α または α' の**スプール**および**ノルム**と呼びます．そして解と係数の関係により，〝整数〟α は有理整係数の２次方程式

$$t^2+at+b=0,\qquad (1)$$
$$a=-2x,\quad b=x^2-3y^2,$$

の解となります（最高次の項の係数が１であることに注意！ このような代数方程式を ***monic*** な有理整係数代数方程式と呼ぶ）．有理整数 a 自身は *monic* な有理整係数１次方程式

$$t-a=0$$

の解です！

§2．代数的数

２次体$\mathbb{Q}(\sqrt{3})$の整数 α は *monic* な有理整係数２次方程式(1)の解であるということで特徴づけられます． このことを証明することが本稿の目標なのですが，そのために大きく間合いをとって，代数的数の説明から始めます：

代数的数とは，有理数を係数とする代数方程式の解のことをいいます．このとき，次が成立します：

> **定理 2**　二つの代数的数の和，差，積，商は，再び代数的数である．

［**証**］　二つの代数的数を α，βとし，それぞれ

$$x^m+a_1x^{m-1}+\cdots\cdots+a_m=0 \qquad ①$$

$$x^n+b_1x^{n-1}+\cdots\cdots+b_n=0 \qquad ②$$

の解として，まず $\zeta=\alpha+\beta$ を考察する．α，β の巾の積

$$\alpha^\mu\beta^\nu\,(\mu=0,\ 1,\ \cdots,\ m-1\,;\ \nu=0,\ 1,\ \cdots,\ n-1) \qquad ③$$

を任意の順序で

$$\omega_1,\ \omega_2,\ \cdots\cdots,\ \omega_l \quad (l=mn)$$

と書けば，

$$\zeta\omega_i=(\alpha+\beta)\alpha^\mu\beta^\nu=\alpha^{\mu+1}\beta^\nu+\alpha^\mu\beta^{\nu+1}$$

において，$\mu+1<m$，$\nu+1<n$ ならば，$\zeta\omega_i$ は③の二つの数の和に等しい．また，もし $\mu+1=m$ または $\nu+1=n$ ならば，

$$\alpha^m=-a_1\alpha^{m-1}-\cdots\cdots-a_m$$

または　$$\beta^n=-b_1\beta^{n-1}-\cdots\cdots-b_n$$

を代入して

$$\zeta\omega_i=C_{i1}\omega_1+C_{i2}\omega_2+\cdots+C_{il}\omega_l \qquad ④$$

を得る．すなわち $\zeta\omega_i$ は有理係数を以っての ω_1，ω_2，$\cdots$，ω_l の一次式として表される．④はすべての $i=1,\ 2,\ \cdots,\ l$ に関して成り立つから，

$$\begin{vmatrix} C_{11}-\zeta & C_{12} & \cdots\cdots & C_{1l} \\ C_{21} & C_{22}-\zeta & \cdots\cdots & C_{2l} \\ \cdots & \cdots & \cdots & \cdots \\ C_{l1} & C_{l2} & \cdots\cdots & C_{ll}-\zeta \end{vmatrix}=0$$

左辺を展開すれば

$$\zeta^l+C_1\zeta^{l-1}+\cdots\cdots+C_l=0 \qquad ⑤$$

を得るが，係数 C_i は C_{ij} の整式として有理数である．すなわち $\zeta=\alpha+\beta$ は代数的数である．

$\alpha-\beta$，$\alpha\beta$ に関しても同様の証明ができる．α/β に関しては，$\beta\neq0$ だから，②において $b_n\neq0$ と仮定してよく，$1/\beta$ は

$$b_nx^n+b_{n-1}x^{n-1}+\cdots\cdots+1=0$$

の解である．従って $\alpha/\beta=\alpha\ (1/\beta)$ は代数的数である．　終

代数的数 θ を解とするような有理数を係数とする代数方程式の中で，次数の最も低いものを

$$f(x)=x^n+a_1x^{n-1}+\cdots\cdots+a_n=0$$

とすれば，$f(x)$ は有理的には**既約**です．すなわち有理数を係数とする二つの低次の因数の積の形に，$f(x)$ が因数分解されることはありません．

有理数を係数とする多項式 $F(x)$ が θ を解とするならば，$F(x)$ は $f(x)$ で割り切れます —— もしも割り切れないと仮定して，$F(x)=f(x)Q(x)+f_1(x)$ とするならば，剰余 $f_1(x)$ は有理数を係数とし，$f(x)$ よりも低次で，かつ $f_1(\theta)=0$ となって矛盾が生じるからです．

θ が満たす既約方程式 $f(x)=0$ が n 次ならば，θ を ***n* 次の代数的数**と呼び，$f(x)=0$ の解 θ，θ'，$\cdots\cdots$，$\theta^{(n-1)}$ を互いに**共役**といいます．

例 1　$\alpha=u+v\sqrt{3}$（u，v は有理数，$v\neq0$）は有理的に既約な（有理数を係数とする）2 次方程式

$$(x-u-v\sqrt{3})(x-u+v\sqrt{3})=0$$

すなわち，

$$x^2-2ux+u^2-3v^2=0$$

を満たすから，2 次の代数的数であり，

$$\alpha=u+v\sqrt{3} \quad と \quad \alpha'=u-v\sqrt{3}$$

とは互いに共役です．　終

θ および θ と共役なる数の対称式の中で，和と積とがしばしば用いられるので，和を θ 達の**スプール**（*Spur*，記号 S），積を θ 達の**ノルム**（*Norm*，記号 N）と呼びます．この二つはどちらも有理数です．

$$S\theta=S\theta'=\cdots\cdots=\theta+\theta'+\cdots\cdots+\theta^{(n-1)}=-a_1,$$

$$N\theta=N\theta'=\cdots\cdots=\theta\theta'\cdots\cdots\theta^{(n-1)}=(-1)^na_n$$

§3．有限代数体

本稿では有限代数体のみを取り扱うのですが，それの代数学的理論は既知と見なさなければなりません．今後引用する必要があろうと思われる事柄の概要だけを，ここで述べて置くことにします：

体（数体）とは複素数の集合 k で，$\alpha\in k$，$\beta\in k$ なるとき $\alpha\pm\beta\in k$，$\alpha\beta\in k$，$\alpha/\beta\in k\ (\beta\neq0)$ なるもののことをいいます．

この定義によれば，0 なる一つの数だけでも体が組成されますが，便宜上それを除外します．しからば k は $\alpha\neq0$ なる数を含み，従って $\alpha/\alpha=1$ を含むから，1 から四則によって生ずるすべての有理数を含まねばなりません．しかるに，有理数全体の集合

$\mathbb{Q}$は，上記の定義から既に一つの体を成すので，それを**有理数体**と呼びます．有理数体は最小範囲の体です．

一つの体 k に含まれる数がすべて他の体 K に含まれるとき，k を K の**部分体**，K を k の**拡大体**と呼び，記号では $\boldsymbol{k} \subset \mathrm{K}$ と表します．

体 k と，k に含まれない数 α とが与えられたとき，k に含まれる数を係数とする有理式を一般的に $\varphi(x)$ で表すならば，すべての $\varphi(\alpha)$ の集合は一つの体を成します．それは k の拡大体であり，しかも k と α とを含む最小範囲の体となります．それを **k に α を添加して生ずる体**と呼び，$\boldsymbol{k(\alpha)}$ という記号で表します．$k(\alpha, \beta)$ 等も同様です．ただし，β が既に $k(\alpha)$ に含まれているならば，$k(\alpha, \beta)=k(\alpha)$，含まれてなければ，$k(\alpha, \beta)=k(\alpha)(\beta)$ 等々です．

θ を n 次の代数的数とすれば，有理数体$\mathbb{Q}$に θ を添加して生ずる体$\mathbb{Q}(\theta)$ のことを **n 次の代数体**と呼びます．$\mathbb{Q}(\theta)$に属する数 $\omega=\varphi(\theta)$ は θ の $(n-1)$ 次以下の**有理数**係数多項式として，**一意的に**次の形に表されます．

$$\omega=C_0+C_1\theta+C_2\theta^2+\cdots\cdots+C_{n-1}\theta^{n-1} \qquad (2)$$

実際，θ が満たす n 次の既約方程式を $f(x)=0$ とし

$$\omega=\frac{g(\theta)}{h(\theta)},\quad h(\theta)\neq 0$$

と置けば，$f(x)$ で $g(x)$ 等を割ることによって，
上記 $g(x)$，$h(x)$ は $(n-1)$ 次以下と見て差し支えなく，$h(x)$ の次数が 1 以上ならば，割り算をして

$$f(x)=Q(x)h(x)+h_1(x)$$

とすれば，$f(x)$ は既約なので，剰余 $h_1(x)$ は 0 ではありません．そうして

$$h_1(\theta)=-Q(\theta)h(\theta),\quad Q(\theta)\neq 0.$$

従って

$$\omega=\frac{-Q(\theta)g(\theta)}{h_1(\theta)}$$

となり，$-Q(\theta)g(\theta)$ は θ の $(n-1)$ 次以下の多項式と考えてよいことになります．$h_1(x)$ は $h(x)$ よりも低次ですから，この操作を繰り返すことによって，(2)の形に達します．

(2)の表現の一意性は明らかでしょう —— もしも

$$\omega=C_0+C_1\theta+\cdots\cdots+C_{n-1}\theta^{n-1}$$
$$=C'_0+C'_1\theta+\cdots\cdots+C'_{n-1}\theta^{n-1}$$

ならば

$$(C_0-C'_0)+(C_1-C'_1)\theta+\cdots\cdots+(C_{n-1}-C'_{n-1})\theta^{n-1}=0$$

となって，

$$(C_0-C'_0),\ (C_1-C'_1),\ \cdots\cdots,\ (C_{n-1}-C'_{n-1})$$

のうちに 0 でないものが存在するならば，θ は $(n-1)$ 次以下の代数的数となって矛盾を生ずるからです．

§4. 代数的整数

monic な有理整係数代数方程式の解を**代数的整数**と呼びます．

定理 3　二つの代数的整数の和，差，積は，再び代数的整数である．

[証]　定理 2 の証明の記号を用いるならば，この場合，係数 a，b が整数だから，⑤における係数 C_i も整数であり，$\alpha+\beta$ も代数的整数となる．

$\alpha-\beta$，$\alpha\beta$ に関しても同様である．　終

定理 4　有理数が代数的整数ならば，それは有理整数である．

[証]　有理数 $\alpha=p/q\neq 0$，$(p,\ q)=1$，が代数的整数ならば

$$\left(\frac{p}{q}\right)^n+a_1\left(\frac{p}{q}\right)^{n-1}+\cdots\cdots+a_n=0$$

すなわち

$$p^n=-q(a_1p^{n-1}+\cdots\cdots+a_nq^{n-1})$$

よって，q は p^n を割り切る．
しかるに　$(p,\ q)=1$
ゆえに　　$q=\pm 1$　終

2 次体$\mathbb{Q}(\sqrt{3})$ の数 α で，*monic* な有理整係数 2 次方程式(1)の解であるようなもの全体の集合を S とすると，定理 3，定理 4 によって，

(I′)　$\alpha,\ \beta\in \mathrm{S} \Longrightarrow \alpha\pm\beta,\ \alpha\beta\in \mathrm{S}$

(II′)　$\alpha=x+y\sqrt{3}\in \mathrm{S}$,

$$(x+y\sqrt{3})^2+a(x+y\sqrt{3})+b=0$$
$$\Longrightarrow x^2+3y^2+ax+b+\sqrt{3}(2xy+ay)=0$$
$$\Longrightarrow x^2+3y^2+ax+b-\sqrt{3}(2xy+ay)=0$$
$$\Longrightarrow (x-y\sqrt{3})^2+a(x-y\sqrt{3})+b=0$$
$$\Longrightarrow \alpha'=x-y\sqrt{3}\in \mathrm{S}$$

(III′)　$\mathrm{S}\cap\mathbb{Q}=\mathbb{Z}$

が成り立つので，Sの各要素は2次体$\mathbb{Q}(\sqrt{3})$の整数となります．実はSは2次体$\mathbb{Q}(\sqrt{3})$の整数全体の集合に他ならず，本稿の目標が達成されました．

さて，上の京都大の問題に戻ると，2次体$\mathbb{Q}(\sqrt{3})$の数 $\alpha=u+v\sqrt{3}$ は *monic* な有理整係数2次方程式 $x^2+ax+b=0$ の解ですから，$\alpha\in$Sであり，αは2次体$\mathbb{Q}(\sqrt{3})$の整数となって，定理1から，uとvは共に整数(有理整数)とならねばならないのです．

§5. 補　足

有理整係数の多項式

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots\cdots+a_1x+a_0$$

に対して，a_0，a_1，……，a_{n-1}，a_nの最大公約数が1に等しいとき，$f(x)$のことを**原始多項式**と呼びます．このとき，次の補助定理が成り立ちます：

> **補助定理**　2つの原始多項式の積は，また原始多項式である．

[証]　$f(x)=a_0+a_1x+\cdots\cdots$,

$g(x)=b_0+b_1x+\cdots\cdots$

を原始多項式とし，$f(x)g(x)$のすべての係数を割り切るような素数pが存在したと仮定する．a_rをpで割り切れない$f(x)$の最初の係数とし，b_sをpで割り切れない$g(x)$の最初の係数とする．

$f(x)g(x)$のx^{r+s}の係数は

$$a_rb_s+a_{r+1}b_{s-1}+a_{r+2}b_{s-2}+\cdots\cdots$$
$$+a_{r-1}b_{s+1}+a_{r-2}b_{s+2}+\cdots\cdots$$

であり，この和全体はpで割り切れ，最初の項を除いた残りの項もすべてpで割り切れるから，最初の項　a_rb_s

もpで割り切れる．よって，a_rまたはb_sがpで割り切れることになって，矛盾する．　終

さて，有理数を係数とする多項式$\varphi(x)$は，有理整係数多項式$F(x)$と有理整数bを用いて

$$\varphi(x)=\frac{F(x)}{b}$$

の形に表せますが，更に$F(x)$は，原始多項式$f(x)$と有理整数aを用いて $F(x)=af(x)$ の形に表せます．すなわち，

$$\varphi(x)=\frac{a}{b}f(x) \qquad (3)$$

の形に表せます．このとき次の定理が成立します：

> **定理5**　(3)の原始多項式$f(x)$は，±1を除けば，$\varphi(x)$から一意に定まる．このように各有理数係数多項式$\varphi(x)$に，原始多項式$f(x)$を対応させると，2つの有理数係数多項式$\varphi_1(x)$，$\varphi_2(x)$の積には，±1を除いて，それぞれの原始多項式の積が対応する．すなわち，$\varphi(x)$が2つの有理数係数多項式$\varphi_1(x)$，$\varphi_2(x)$の積に等しいならば，$\varphi(x)$，$\varphi_1(x)$，$\varphi_2(x)$に対応する原始多項式を，それぞれ$f(x)$，$f_1(x)$，$f_2(x)$とするとき，
> $f(x)=\pm f_1(x)f_2(x)$ となる．

[証]　$\varphi(x)$に2つの原始多項式$f(x)$，$g(x)$が対応したと仮定すると，有理整数a，b，c，dを用いて，$\varphi(x)=\frac{a}{b}f(x)=\frac{c}{d}g(x)$ と書ける．

よって，$daf(x)=bcg(x)$ であり，

$da=\pm bc$　〔∵　f，g：原始多項式〕．

$\therefore\quad \pm bcf(x)=bcg(x)$，$\therefore\quad \pm f(x)=g(x)$．

次に，$\varphi_1(x)=\frac{a_1}{b_1}f_1(x)$，$\varphi_2(x)=\frac{a_2}{b_2}f_2(x)$

とすると，

$$\varphi(x)=\varphi_1(x)\varphi_2(x)=\frac{a_1a_2}{b_1b_2}f_1(x)f_2(x)$$

であって，補助定理から$f_1(x)f_2(x)$も原始多項式であるから，$f(x)=\pm f_1(x)f_2(x)$ である．　終

さて，§4の(I′)に戻りましょう：

定理2の証明によれば，$\alpha\pm\beta$，$\alpha\beta$の満たす有理整係数代数方程式は*monic*な4次方程式 $\varphi(x)=0$ となります．しかるに，$\alpha\pm\beta$，$\alpha\beta\in\mathbb{Q}(\sqrt{3})$ですから，例えば，

$$\alpha+\beta=u+v\sqrt{3}\ (u,\ v\text{ は有理数})$$

の形に表され，$\alpha+\beta$は*monic*で既約な2次の有理数係数多項式$\varphi_1(x)$に対して，

$$\varphi_1(\alpha+\beta)=0 \qquad (4)$$

を満たします．よって，$\varphi(x)$は

$$\varphi(x)=\varphi_1(x)\varphi_2(x)\ (\varphi_2\text{ は有理数係数多項式})$$

の形に因数分解されます．そこで，$\varphi(x)$を(3)の形に表すと，$\varphi(x)$がそもそも*monic*で有理整係数なので，$f(x)=\varphi(x)$，$a=b$ となります．そして定理5から，

$$\varphi(x)=f(x)=\pm f_1(x)f_2(x), \qquad (5)$$

ここに，f_iはφ_iに対応する原始多項式となり，$f_1(\alpha+\beta)=0$〔∵(4)〕となりますが，$f_1(x)$は*monic*であると仮定しても一般性を失いません〔∵(5)〕．

〈参　考　文　献〉

［1］高木貞治著，初等整数論講義　第2版，共立出版
［2］高木貞治著，代数的整数論，岩波書店
［3］van der Waerden著，銀林浩訳，現代代数学1，東京図書

(静岡県立三島北高等学校)