大学入試の背景を探る ―― 共役の話 ――

宮川 幸隆（みやかわ ゆきたか）

本稿では，まず東京大学の '97 年前期の問題

> a，b は実数で $a^2+b^2=16$，$a^3+b^3=44$ を満たしている．このとき，
> (1) 省略
> (2) n を 2 以上の整数とするとき，a^n+b^n は 4 で割り切れる整数であることを示せ．

の背景を探ります．

(1)は実は「$a+b$ の値を求めよ．」というものであり，$a+b=2$ と求められます．そして，この結果を用いて，

$$a^{k+2}+b^{k+2}=(a+b)(a^{k+1}+b^{k+1})-ab(a^k+b^k)$$
$$=2(a^{k+1}+b^{k+1})+6(a^k+b^k)$$

により帰納法で(2)は解決されますが，**帰納法のような初等的な解法**に頼っていては，この問題の背景は全然見えてきません．

この問題の背景は K.F. Gauss が「**数学の女王**」と歎じた「整数論」です．特に，K.F. Gauss の最晩年の弟子 R. Dedekind による「二次体の整数論」の中の「**ideal 論**」です．

幸い，日本には，「日本の K.F. Gauss」ともいうべき高木貞治博士が居られました．そして高木博士は，Gauss の高弟 Dirichlet と Dedekind による「整数論講義」に匹敵する「初等整数論講義」という名著を遺して下さいました．そこで，まず，「初等整数論講義」(<参考文献>[1]) の中の二次体のイデヤルの解説から始めることにします：

§1. 二次体 $K(\sqrt{m})$ の整数

m を平方因数（もちろん 1 以外の）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，**二次体**と呼ばれ，$K(\sqrt{m})$ という記号で表されます．

二次体 $K(\sqrt{m})$ 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．

$K(\sqrt{m})$ の特別な要素として，$K(\sqrt{m})$ の "整数" なるものを定義することを考えます．"整数" の定義を二次体 $K(\sqrt{m})$ 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 $K(\sqrt{m})$ 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．そして，(I)～(III)の条件を満たす最大の部分集合 $[\subseteqq K(\sqrt{m})]$ の要素を $K(\sqrt{m})$ 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 $K(\sqrt{m})$ の "整数" は，
> $m\equiv 2,\ 3\ (\mathrm{mod}.\ 4)$ ならば $x+y\sqrt{m}$
> [ここに，x，y は有理整数]，
> $m\equiv 1\ (\mathrm{mod}.\ 4)$ ならば $\dfrac{x+y\sqrt{m}}{2}$
> [ここに，x，y は $x\equiv y\ (\mathrm{mod}.\ 2)$ なる有理整数].

さて，話を簡単にするために $m\equiv 2, 3\ (\mathrm{mod}.\ 4)$ とします．すると二次体 $K(\sqrt{m})$ の "整数" は，x，y を有理整数として，

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

と表されます．$\alpha'=x-y\sqrt{m}$ 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：

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

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

$$x^2+ax+b=0$$

の解であるということで特徴づけられます（x^2 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** な代数方程式と呼ぶ）．有理整数 a 自身は有理整係数の monic な1次方程式

$$x-a=0$$

の解です！

$\sqrt{m}=\omega$ とおくと，$\mathsf{K}(\sqrt{m})$ の整数は有理整係数 x，y をもって

$$x+y\omega$$

の形に表されます．x，y は各整数に関して一意的に定まります．このように $\mathsf{K}(\sqrt{m})$ の整数は適当な2つの整数 ω_1，ω_2（例えば上記の 1，ω）によって，有理整係数 x，y をもって一意的に

$$x\omega_1+y\omega_2$$

の形で表されます．このような2つの整数の組

$$[\omega_1,\ \omega_2]$$

を $\mathsf{K}(\sqrt{m})$ の**整数の底**（あるいは略して $\mathsf{K}(\sqrt{m})$ の**底**）といいます．上記 $[1,\ \omega]$ を**標準的の底**ともいいます．

二次体 $\mathsf{K}(\sqrt{m})$ の整数に対しても，有理整数の場合と同様に，整除の定義を行なうことができます．すなわち，$\mathsf{K}(\sqrt{m})$ の整数 α，β の商 $\frac{\alpha}{\beta}=\gamma$ が再び整数であるとき，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．

§2. 二次体のイデヤル

二次体 $\mathsf{K}(\sqrt{m})$ の整数の集合が次の i），ii）の性質を有するとき，その集合を1つのイデヤルという：

i）この集合に属する任意の2つの整数 α，β の和および差は，やはりこの集合に属する．

ii）この集合に属する整数 α の任意の倍数 $\lambda\alpha$ はやはり，この集合に属する．

この定義によれば，与えられた整数 α のすべての倍数 $\alpha\xi$ の集合はイデヤルの一例です．それを (α) と記します．このようなイデヤルを α から生ずる**単項イデヤル**と呼びます．また，α_1，α_2……，α_n を与えられた整数，ξ_1，ξ_2，……ξ_n を任意の整数とすれば，$\alpha_1\xi_1+\alpha_2\xi_2+\cdots\cdots+\alpha_n\xi_n$ の形に表される整数全部の集合は1つのイデヤルです．このイデヤルを

$$(\alpha_1,\ \alpha_2,\ \cdots\cdots,\ \alpha_n)$$

と記し，それを $\alpha_1\alpha_2$，……，α_n **から生ずるイデヤル**と呼びます．

任意のイデヤル A はある有理整数を含む．例えば A が α を含むならば，A は $\alpha\alpha'$ を含み（α' は α の共役！よって α' は整数であるから），$\alpha\alpha'$ は有理整数であるからです．A が既に1つの有理整数を含むならば，またそのすべての有理整数倍を含みます．

このように A に含まれるすべての有理整数は，その中の最小の正の数（それを a とする）の倍数です．なぜなら，b が A に含まれるとき，$b=qa+a'$，$0\leqq a'<a$ とすれば，b も qa も A に含まれるから，$b-qa=a'$ も A に含まれます．

ゆえに $a'=0$ でなければなりません．ただし，以上の議論においては，A は0のみから成るものとは考えていません．0のみから成る集合もイデヤルの定義にあてはまる（所謂**零イデヤル**）が，本稿では，それはイデヤルの中にいれないことにします．

さて，$\omega=\sqrt{m}$ とするときイデヤル A は

$x+y\omega$，$y\neq 0$；x，y：有理整数；

のような数を含まなければなりません（例えば $a\omega$ は A に含まれるから．ただし a は上記の有理整数）．いま A に含まれるこのような整数の中で，ω の係数なる有理整数が最小の正の値を有するものを $b+c\omega$ とします．しからば A に含まれる任意の整数 $x+y\omega$ において，係数 y は c の倍数でなければなりません．なぜならば，$y=qc+r$，$0\leqq r<c$ とすれば，$x+y\omega-q(b+c\omega)=(x-qb)+r\omega\in\mathsf{A}$ であるから，仮定によって $r=0$，したがって $y=qc$．

このとき，$x-qb\in\mathsf{A}$ ですが，$x-qb$ は有理整数ですから，a の倍数です．

よって

$$x-qb=pa$$

とおくと

$$x+y\omega=pa+q(b+c\omega)\qquad(1)$$

ここで $x+y\omega$ は A に属する任意の整数で，a は A に属する最小の正の有理整数，また $b+c\omega$ は A に属する整数の中で ω の係数が最小の正の有理整数であるものです．p，q はもちろん有理整数です．

$$pa+q(b+c\omega) \qquad (1')$$

のような形の数がAに属することは明らかですが，上記の考察によってAに属する任意の整数が(1')のような形に表されることが確定したのです．よって a と $b+c\omega$ とをイデヤルAの**底**と呼びます．

イデヤルの定義によれば

$$\mathsf{A}=(a,\ b+c\omega)$$

です．それはAは $a\xi+(b+c\omega)\eta$ のような数の集合であるというのですが，Aに属する任意の整数は既に a と $b+c\omega$ との有理整数倍の和に等しいのです．

a と $b+c\omega$ とがAの底であることを特別に明示するためには次の記法を用います．

$$\mathsf{A}=[a,\ b+c\omega] \qquad (2)$$

一般にイデヤルAに含まれるすべての数が任意の有理整係数 x，y をもって $\alpha_1x+\alpha_2y$ の形に表されるとき，α_1，α_2 をAの**底**といい，

$$\mathsf{A}=[\alpha_1,\ \alpha_2]$$

と記します．上記(2)のような底を**標準的底**と呼びます．標準的底(2)において a，b は c の倍数です．なぜならば $a\omega\in\mathsf{A}$ ですから a は c で割り切れます．また $(b+c\omega)\omega=cm+b\omega\in\mathsf{A}$ ですから b も c で割り切れます．

ゆえに $a=ca_0$，$b=cb_0$ とおくならば，(1)によってイデヤルAに含まれるすべての整数は

$$c(pa_0+q(b_0+\omega))$$

のような形の数です．

イデヤルAの各数が c で割り切れるならば，各数を c で割った商の集合は明らかに1つのイデヤルです．それを A_0 と名づけて

$$\mathsf{A}=c\mathsf{A}_0$$

と記せば，

$$\mathsf{A}_0=[a_0,\ b_0+\omega].$$

このイデヤル A_0 においてはそれが含むすべての整数に共通の有理約数はありません．このようなイデヤルを**原始イデヤル**と呼びます．

しからば，すべてのイデヤルは原始イデヤルの各数に一定の有理整数を乗ずることによって得られるもので，以上を要約して次の定理を得ます：

定理2　イデヤルAを標準的底をもって

$$\mathsf{A}=[a,\ b+c\omega]=c[a_0,\ b_0+\omega]\quad(a>0,\ c>0)$$

の形に表すことを得る．c はAの各数に共通な最大の有理約数，$a=ca_0$ はAに含まれる最小の有理整数である．

§3. イデヤルの積

イデヤル $\mathsf{A}=(\alpha_1,\ \alpha_2,\ \cdots\cdots,\ \alpha_m)$ と $\mathsf{B}=(\beta_1,\ \beta_2,\ \cdots\cdots,\ \beta_n)$ との**積**とは，イデヤル

$$\mathsf{AB}=(\alpha_1\beta_1,\ \cdots\cdots,\ \alpha_\mu\beta_\nu,\ \cdots\cdots\alpha_m\beta_n)$$

をいいます．すなわち積ABはA，Bに属する任意の整数 α，β の積なる $\alpha\beta$ およびそれらの有限和 $\sum\alpha\beta$ の集合です．実際

$$\alpha\beta=\left(\sum_{\mu=1}^{m}\xi_\mu\alpha_\mu\right)\left(\sum_{\nu=1}^{n}\eta_\nu\beta_\nu\right)$$

$$=\sum_{\mu,\nu}(\xi_\mu\eta_\nu)\cdot(\alpha_\mu\beta_\nu),$$

また，

$$\sum_{\mu,\nu}\xi_{\mu\nu}\cdot\alpha_\mu\beta_\nu=\sum_{\nu}\left(\sum_{\mu}\xi_{\mu\nu}\alpha_\mu\right)\beta_\nu=\sum\alpha\beta.$$

定理3　イデヤルAに属するすべての数の共役の集合は1つのイデヤルである．

それをAの**共役イデヤル**と呼び，通例A'で表します．

証明　$\mathsf{A}=(\alpha_1,\ \alpha_2,\ \cdots\cdots,\ \alpha_n)$ とすればAに属する数 $\alpha_1\xi_1+\alpha_2\xi_2+\cdots\cdots+\alpha_n\xi_n$ の共役なる $\alpha_1'\xi_1'+\alpha_2'\xi_2'+\cdots\cdots+\alpha_n'\xi_n'$ は $(\alpha_1',\ \alpha_2',\ \cdots\cdots,\ \alpha'_n)$ に属する．逆も明白である．すなわち

$$\mathsf{A}'=(\alpha_1',\ \alpha_2',\ \cdots\cdots,\ \alpha'_n).$$ ■

定理4　互いに共役な2つのイデヤルの積は1つの有理整数から生ずる単項イデヤルに等しい．

証明　イデヤル $\mathsf{A}=(\alpha)$ が単項イデヤルのときには，$\mathsf{A}'=(\alpha')$，したがって $\mathsf{AA}'=(\alpha\alpha')$ で，$\alpha\alpha'$ は有理整数であるから，定理は明白である．

一般の場合にイデヤルAは2つの整数(例えばその底)から生ずるものと見ることができる(定理2)から，

$$\mathsf{A}=(\alpha,\ \beta),\ \mathsf{A}'=(\alpha',\ \beta')$$

とすれば，

$$\mathsf{AA}'=(\alpha\alpha',\ \alpha\beta',\ \beta\alpha',\ \beta\beta')$$

いま

$$\alpha\alpha'=a,\ \alpha\beta'+\beta\alpha'=b,\ \beta\beta'=c$$

とおけば，a，b，c は AA' に属する有理整数である．それらの最大公約数を n とすれば，n を有理整数 x，y，z をもって

$$n=ax+by+cz$$

の形に表し得るから，$n\in AA'$ である．しかるに，$\alpha\beta'$，$\alpha'\beta$ は n で割り切れる．なぜならば

$$\frac{\alpha\beta'}{n}+\frac{\alpha'\beta}{n}=\frac{b}{n}\ (=p\ \text{とする}),$$

$$\frac{\alpha\beta'}{n}\cdot\frac{\alpha'\beta}{n}=\frac{ac}{n^2}\ (=q\ \text{とする})$$

はともに有理整数であるから，$\frac{\alpha\beta'}{n}$，$\frac{\alpha'\beta}{n}$ は monic な 2 次方程式 $x^2-px+q=0$ の解，したがって整数である．

このように $\alpha\alpha'$，$\alpha\beta'$，$\alpha'\beta$，$\beta\beta'$ がいずれも n で割り切れるから，AA' に含まれる数はすべて n で割り切れるが，n 自身が既に AA' に含まれているのだから $AA'=(n)$． ■

§4. 冒頭の入試問題の(2)の証明

$a+b=2$，$ab=-6$ から a，b は 2 次方程式

$$x^2-2x-6=0$$

の 2 つの解ですので，$\{a,\ b\}=\{1\pm\sqrt{7}\}$ となります．$7\equiv 3\ (\mathrm{mod}.\ 4)$ ですから，二次体 $K(\sqrt{7})$ は上の考察の対象であったわけで，$K(\sqrt{7})$ のイデヤル

$$A=(a^2,\ b^2)$$

の共役イデヤルは $A=(b^2,\ a^2)$ 自身ですから，

$$A^2=(a^2b^2,\ a^4,\ b^4,\ b^2a^2)$$

です．a^n+b^n は a，b の対称式ですから，

$$a=1+\sqrt{7},\ b=1-\sqrt{7}$$

として一般性を失いません．さて，

$$a^2b^2=(1+\sqrt{7})^2(1-\sqrt{7})^2=(1-7)^2=36=4\times 9,$$

$$\begin{aligned}a^4+b^4&=(1+\sqrt{7})^4+(1-\sqrt{7})^4\\&=(8+2\sqrt{7})^2+(8-2\sqrt{7})^2\\&=2\times(8^2+2^2\times 7)=8\times(16+7)=8\times 23\end{aligned}$$

ですから，a^2b^2，a^4+b^4，b^2a^2 の最大公約数は 4 です．

$$4=4\times 46-4\times 45=a^4+b^4-5a^2b^2$$

ですから，$4\in A^2$ です．しかるに，

$$a^4=(8+2\sqrt{7})^2=8^2+2^2\times 7+2\times 8\times 2\sqrt{7},$$

$$b^4=(8-2\sqrt{7})^2=8^2+2^2\times 7-2\times 8\times 2\sqrt{7}$$

は 4 で割り切れるから，a^2b^2，a^4，b^4 がいずれも 4 で割り切れることになって，A^2 に含まれる数はすべて 4 で割り切れますが，4 自身が既に A^2 に含まれているのだから，$A^2=(4)$ です．

さて，a，b は二次体 $K(\sqrt{7})$ の整数ですから，

$$a^4+b^4,$$

$$a^5+b^5=a^4\cdot a+b^4\cdot b,$$

$$a^6+b^6=a^4\cdot a^2+b^4\cdot b^2,$$

$$\vdots$$

はすべて A^2 に属する有理整数です．そして $A^2=(4)$ から，これらはすべて 4 で割り切れる有理整数であるのです．

§5. 他の入試問題との関連

(1) 2 次方程式 $x^2+ax+b=0$ が相異なる 2 つの解 α，β をもつとき，定数 p，q に対し，

$x_0=p+q$，$x_n=p\alpha^n+q\beta^n$ $(n=1,\ 2,\ 3,\ \cdots\cdots)$

とおく．このとき次の等式が成り立つことを示せ．$x_{n+2}+ax_{n+1}+bx_n=0$ $(n=0,\ 1,\ 2,\ \cdots\cdots)$

(2) $x_0=2$，$x_1=3$，$x_{n+2}=x_{n+1}+x_n$ $(n=0,\ 1,\ 2,\ \cdots\cdots)$ で与えられる数列の一般項は

$$x_n=\frac{2+\sqrt{5}}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n+\frac{-2+\sqrt{5}}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$$

で与えられることを示せ． ('97年東北大・前期)

(1)で，$a=-2$，$b=-6$，$p=q=1$ のときが，前の東大の問題と関係があり，このとき

$$x_n\ (n\geqq 2)$$

はすべて 4 の倍数だったわけです．

(2)は所謂フィボナッチ数列の一般項に関する問題で，$a=b=-1$，$p=\frac{2+\sqrt{5}}{\sqrt{5}}$，$q=\frac{-2+\sqrt{5}}{\sqrt{5}}$ の場合ですが，$x^2-x-1=0$ の 2 解が二次体 $K(\sqrt{5})$ の共役な 2 つの整数

$$\frac{1\pm\sqrt{5}}{2}$$

です．この場合

$$p=\frac{5+2\sqrt{5}}{5},\ q=\frac{5-2\sqrt{5}}{5}$$

ですから，p，q は二次体 $K(\sqrt{5})$ に属する互いに共役な 2 つの数である訳です．

さて，

$$\alpha=\frac{1+\sqrt{5}}{2},\ \beta=\frac{1-\sqrt{5}}{2}$$

とおくと，$\alpha^2=\frac{3+\sqrt{5}}{2}$，

$$4\alpha^3=(1+\sqrt{5})(3+\sqrt{5})=8+4\sqrt{5}$$

ですから，$p=\frac{\alpha^3}{\sqrt{5}}$．

同様にして

$$\beta^3=2-\sqrt{5},$$

$$q=-\frac{\beta^3}{\sqrt{5}}$$

です．よって　$x_n=\frac{1}{\sqrt{5}}(\alpha^{n+3}-\beta^{n+3})$

そして，α^{n+3} と β^{n+3} とは二次体 $K(\sqrt{5})$ の互いに共役な2つの整数ですから，

$$\alpha^{n+3}-\beta^{n+3}$$

は $\sqrt{5}$ の有理整数倍となり，x_n が有理整数となることがうなづけます．

数列 $\{x_n\}$，$n=1, 2, 3, \cdots\cdots$ を，$x_1=2$，$x_2=6$ と，漸化式 $x_n=2x_{n-1}+x_{n-2}$，$n=3, 4, 5, \cdots\cdots$ で定める．この数列の一般項はある定数 A，B (ただし，$A<B$ とする) を用いて $x_n=A^n+B^n$ と表すことができる．$A=$［ア］，$B=$［イ］である．　('97年慶應義塾大・医学部)

この問題は，前の東北大の問題で $a=-2$，$b=-1$，$p=q=1$ の場合であり，A，B は2次方程式

$$x^2-2x-1=0$$

の2解であるから，

$$A=1-\sqrt{2},\quad B=1+\sqrt{2}$$

となります［$\because$ $A<B$］

数列 $\{a_n\}$ を初項1，公比 r の等比数列とし，数列 $\{b_n\}$ を初項1，公比 s の等比数列とする．
第 n 項が

$$x_n=a_n+b_n\ (n=1, 2, 3, \cdots\cdots)$$

で与えられる数列 $\{x_n\}$ を考える．

$x_2=2$，$x_4=14$ のとき，次の問いに答えよ．

(1)　r，s を求めよ．ただし $r>s$ とする．

(2)　すべての自然数 n について，

$$x_{n+2}=2x_{n+1}+x_n$$

が成り立つことを示せ．　('97年大阪大・前期)

この問題は

$$x_n=r^{n-1}+s^{n-1}=y_{n-1}$$

とおくと，前の東北大の問題で $a=-2$，$b=-1$，$p=q=1$ の場合であり，r，s は2次方程式

$$x^2-2x-1=0$$

の2解であるから，

$$r=1+\sqrt{2},\quad s=1-\sqrt{2}$$

となります［$\because$ $r>s$］．

$$y_1=x_2=2,$$

$$y_2=(1+\sqrt{2})^2+(1-\sqrt{2})^2=6,$$

ですから，左の慶應大の問題と全く同じ問題です．

$$rs=-1$$

で，r，s はどちらも二次体 $K(\sqrt{2})$ の整数ですから r も s も1の約数です．このような整数を**単数**と呼びます．

二次体 $K(\sqrt{m})$ に属する数 α のノルムを $N\alpha$ と書くことにすれば，単数 α とは $N\alpha=\pm1$ を満たすものに他なりません．よって，$K(\sqrt{2})$ の単数全体の集合は

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

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．

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

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

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

$\therefore$　$a-b\sqrt{2}>-1$ ……②　かつ

$-1<b\sqrt{2}-a$ ……③

したがって，①+②，①+③ 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①を満たすから　$\varepsilon_0=1+\sqrt{2}=r$．

実は，二次体 $K(\sqrt{2})$ の1より大なる任意の単数は，

$$r^n(n：\text{自然数})$$

の形に表されることが知られています．したがってこの問題の数列 $\{x_n\}$ の第 n 項 $(n\geqq2)$ は，二次体 $K(\sqrt{2})$ の1より大なる単数とその共役の和であるということになります．よって，もちろん，その各項は有理整数です．

§6. おわりに

冒頭で，高木貞治先生のことを「日本のGauss」と申し上げましたが，「日本のRiemann」は岡潔先生，「日本のAbelもしくはGalois」は谷山豊先生でしょう．

<参　考　文　献>

［1］　高木貞治　初等整数論講義　共立出版

(静岡県立三島北高等学校)