

数学入門公開講座

昭和60年7月24日(水)から8月1日(木)まで

日 時 間	7月 24日 (水)	25日 (木)	26日 (金)	27日 (土)	28日 (日)	29日 (月)	30日 (火)	31日 (水)	8月 1日 (木)
13:15~15:00	荒 木	一 松	一 松	荒 木	休 講	松 浦	松 浦	松 浦	松 浦
15:00~15:15	休 憩					休 憩			
15:15~17:00	一 松	一 松	荒 木	荒 木		笠 原	笠 原	笠 原	笠 原

主催 京都大学数理解析研究所

講師及び内容

1. 四元数の話 (7時間)

京都大学数理解析研究所教授 荒木不二洋

実数から複素数へという数の概念の拡大の延長線上にある四元数。

パスカルの定理の証明や剛体の回転などへの応用を解説する。

2. 四元数の整数論 (7時間)

京都大学数理解析研究所教授 一松 信

ハミルトン (Hamilton) が導入した四元数は, 当初期待された程には有用でなかった。しかしフルヴィッツ (Hurwitz) が考察した四元数整数は, 乗法が可換でないという点を除いて, 普通の整数とよく似た性質が多い。余り知られていないこの理論を紹介し, 整数の性質を反省するとともに, 幾つかの応用にも触れたい。

3. 金太郎飴と有平糖^{アルヘイトウ} (7時間)

京都大学数理解析研究所教授 松浦重武

上記表題のもとに, Brunn-Minkovski の不等式とその応用について述べる。

4. 磁針のずれの幾何学 (7時間)

京都大学教養部教授 笠原 皓司

北極と北磁極のずれを見込む角が一定である点の軌跡について考察する。

時間割

日 時 間	7月 24日 (水)	25日 (木)	26日 (金)	27日 (土)	28日 (日)	29日 (月)	30日 (火)	31日 (水)	8月 1日 (木)
13：15～15：00	荒 木	一 松	一 松	荒 木	休 講	松 浦	松 浦	松 浦	松 浦
15：00～15：15	休 憩					休 憩			
15：15～17：00	一 松	一 松	荒 木	荒 木		笠 原	笠 原	笠 原	笠 原

2. 四元数の整数論 (7 時間)

京都大学数理解析研究所教授 一 松 信

1985, JULY 24 15:15-17:00
JULY 25 13:15-15:00, 15:15-17:00
JULY 26 13:15-15:00

四元数の整数論

京都大学数理解析研究所 / 一松 信

目 次

0. 初めに	2
1. 四元数とは?	2
2. 四元数整数	5
3. 四元数体の自己同型変換	6
4. 二つの四元数の最大公約数	8
5. 四元数の偶数・奇数と代表数	11
6. 四元素数と素因数分解	14
7. Eulerの問題への応用	18
8. 八元数整数について	21

[参考文献]

- [1] W.R.Hamilton, The Elements of Quaternions, Dublin, 1866 (死後発行),
- [2] A.Hurwitz, Über die Zahlentheorie der Quaternionen,
Nachrichten Gesel. Wiss. Göttingen, Math-Phys., 1896, p.313-340 ;
全集 II, p.303-330 に再録
- [3] A.Hurwitz, Vorlesungen über die Zahlentheorie der Quaternionen,
Springer Verlag, 1918
- [4] H.S.M.Coxeter, Integral Cayley Numbers, Duke Math. J.13(1946), p.561-
578 ;
Coxeter, Twelve Geometric Essays, Southern Illinois Univ. Press, 1968,
p.22-39 に再録
- [5] 高木貞治 初等整数論講義、共立出版、新訂版、1966.

0. 初めに

Hamiltonが導入した四元数は、当初の期待ほどには有用ではなかった。しかし特別な四元数として、Hurwitz が研究した四元数整数は、乗法が交換可能でないという点を除けば、普通の整数とよく似た性質を数多く有する。

私がいささか専門の違うこの対象に興味をもったのは、正則格子による多重数値積分を研究したからである。4次元の D_4 格子の性質を調べているうちに、四元数整数として扱うと、色々の性質が統一的に理解できることを、筑波大学・内山三郎教授から教えて頂いた。([2], [3] 参照)

19世紀初めの Gauss の『整数論研究』は、二次体の整数、特にいわゆる Gauss の整数の研究が中心であった。その後今一つの複素整数である Eisenstein の整数も研究された。これら体系は、いずれも普通の整数と同様に互除法が可能であり、素因数分解の一意性が成立する。([5] 参照)

四元数整数は、乗法が交換可能でないという点に注意すれば、やはり普通の整数とよく似た性質が成立する。それらを学ぶことは、整数の性質に於いて、何が基本的なのかを反省するよい材料である。

今では忘れられたのに近いこの古い理論を講義しようという気になったのも、その辺に興味を感じたからである。

最後に時間があれば、八元数整数 (Cayley 整数) にも触れたい。([4] による)

1. 四元数とは？

複素数 $a+bi$ は永らく『虚数』とよばれて、幽霊のような存在と思われていた。

しかし19世紀初めに Gauss その他の人々によって、これが平面上に表わされ、実在の数と感ぜられるようになった。それではもっと次元の高い『多元数』が考えられないだろうか？

残念ながら、普通の数の計算規則をすべて保存しようとする、2次元より上に拡張することは出来ない。それはいわゆる『代数学の基本定理』による。

しかし計算規則のいくつかを諦めれば、もっと高次元の多元数が可能である。その典型例が、これから述べる四元数である。

複素数 $\alpha = a + bi$ が2個の実数 a, b から成立っているように、四元数は4個の基底からなる数である。基底を i_0, i_1, i_2, i_3 と書くのが便利だが、ここでは $1, i, j, k$ と書くことにする。従って四元数は a, b, c, d を実数として

$$\alpha = a + bi + cj + dk$$

の形の数である。 a, b, c, d をその成分という。それ同志の加法・減法は成分ごとに行う。乗法は次の規則による。

$$i^2 = j^2 = k^2 = ijk = -1, \quad (\text{基本関係})$$

しかしこれは要約した形である。Hamiltonが散歩の途中で発見し、運河に掛る橋に書残したと伝えられる式は、この形であった。但しこれから直に次の関係式が導かれる。

$$ij = k, \quad jk = i, \quad ki = j, \quad ji = -k, \quad kj = -i, \quad ik = -j.$$

従って2数 $\alpha = a + bi + cj + dk$ と $\beta = p + qi + rj + sk$ との積は次のようになる。

$$\alpha \cdot \beta = A + Bi + Cj + Dk, \quad \text{ここに}$$

$$A = ap - bq - cr - ds, \quad B = aq + bp + cs - dr, \quad C = ar - bs + cp + dq, \quad D = as + br - cq + dp.$$

α に対して、 $a^2 + b^2 + c^2 + d^2$ を $N(\alpha)$ と書き、ノルムとよぶ。その正の平方根を $\|\alpha\|$ と書き、絶対値という。これは0との距離を表す。なお関数解析学では、ノルムと絶対値とを同じ意味に使うことが多いが、整数論では平方根をとる前の数をノルムとよんで区別する習慣である。それは主として $N(\alpha)$ 自身が整数である数を扱うためである。

この積は、交換法則を満たさないが、結合法則・加法との分配法則を満たす。

定理 1. $N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$

系 m, n が4個の平方数の和で表されれば、積 mn も4個の平方数の和で表される。

証明は直接の計算でできる。練習の意味で一度はやってみる価値がある。但し以下に述べるように、計算しないでできる方法もある。

α に対して、 $\bar{\alpha} = a - bi - cj - dk$ をその共役四元数という。直接の計算により

$$\alpha \cdot \bar{\alpha} = N(\alpha) = \bar{\alpha} \cdot \alpha$$

がわかる。故に $\alpha \neq 0$ ならば、 α の逆数 α^{-1} は $\bar{\alpha} / N(\alpha)$ で与えられる。

逆数の一意性から、 $(\alpha\beta)^{-1} = \beta^{-1}\alpha^{-1}$ である。従って

$$\overline{(\alpha\beta)} = \overline{\beta\alpha}, \quad N(\alpha\beta) = \alpha\beta\overline{(\alpha\beta)} = \alpha\beta\overline{\beta}\overline{\alpha} = N(\beta)\alpha\overline{\alpha} = N(\alpha)N(\beta)$$

となって、定理1が証明された。

四元数 $\alpha = a+bi+cj+dk$ は $(a+bi)+(c+di)j$ と書けるから、二つの複素数

$$\sigma = a+bi, \quad \tau = c+di$$

を j で繋いだ組ともみられる。

また複素数 $a+bi$ を2次の行列

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

で表すことができる。これと同様に、上の四元数を行列

$$\begin{bmatrix} \sigma & \tau \\ -\overline{\tau} & \overline{\sigma} \end{bmatrix}$$

で表すことができる。実数行列ならば4次の行列で表すことができる。

行列表現とは、対応する行列

$$\alpha \rightarrow A, \quad \beta \rightarrow B$$

に対して、普通の行列の和・積 $A+B$, AB がそのままそれぞれ元の2数の和・積の表現になるという意味である。

$\beta \neq 0$ のとき、 $\gamma\beta = \alpha$, $\beta\delta = \alpha$ を満たす γ , δ をそれぞれ、 α の β による左商・右商という。これらはそれぞれ

$$\gamma = \alpha\beta^{-1}, \quad \delta = \beta^{-1}\alpha$$

で与えられる。これらをそれぞれ α/β , $\beta \setminus \alpha$ で表すこともある。

注意: 実数は任意の四元数と可換である。逆に任意の四元数との積が交換可能な四元数は、実数に限る。

2. 四元数整数

ちょっと考えると、四元数整数とは成分がすべて整数であるような四元数のこととすればよさそうである。このような数を仮に『丁数』とよぶことにする。

しかしこれだけでは足りない。

その理由を見るために、そもそも整数（正しくは整数全体のなす集合）がどのような性質をもつべきものであるかを考えてみよう。

1^o. 整数の集合は離散的である。すなわち一つの整数にいくらでも近い、異なる整数の無限列はありえない。

2^o. 整数同志で、加法・減法・乗法が自由にできる。しかし除法は必ずしもできない。

3^o. 整数同志で、除法は必ずしもできないが、次のような余りのある除法ができる。すなわち任意の二数 α, β ($\neq 0$) に対して、整数 γ をうまくとると、

$$\|\alpha - \beta \cdot \gamma\| < \|\beta\|$$

であるようにできる。ここに $\|\quad\|$ は、数の大きさ（絶対値）を表わす。

丁数だけでも、1^o, 2^oの性質は満たされるが、3^oの性質が成り立たない。 $\alpha = 1+i+j+k, \beta = 2$ とおくと、 γ をどうとっても、上の式の左辺は、右辺の値 2 よりも小さくならない。

これは丁数だけからなる4次元の単純立方格子が隙間だらけだからである。4次元の超立方体の対角線の長さは、その一辺の長さの丁度2倍であり、中心はどの頂点からも一辺と同じ距離にある。

従ってその中心に当る点をすべて補う。これを『半数』とよぶことにする。

この数は、その成分がすべて奇数の半分（これを半整数とよぶ）であるような数である。丁数と半数とを併せて、四元数整数またはHurwitzの整数という。

これ全体が上記の1^oの性質を持つことはすぐにわかる。2^o, 3^oの性質をも有することは後に示す。

これ以上増やせないこともわかる。もしこの他に数 λ があれば、 λ と 1 以下の距離にある四元数整数 α があり、その差の累乗を作ると、いくらでも 0 に近い整数の無限列ができてしまう。

2^c の性質を見るには、 $\rho = (1+i+j+k)/2$ と置いて、四元数整数を

$$h\rho + \varrho i + m j + n k, \quad h, \varrho, m, n \text{ は整数}$$

と表すとよい。ここで h が偶数か奇数かに応じて、丁数か半数かである。和・差は成分ごとに計算すればよい。積は次の関係式から確かめられる。

$$\rho^2 = \rho - 1 = i+j+k-\rho, \quad i\rho = \rho k = i+k-\rho, \quad j\rho = \rho i = i+j-\rho, \quad k\rho = \rho j = j+k-\rho,$$

$$\text{なお } \rho^3 = 1, \quad \bar{\rho} = \rho^{-1} = -\rho^2$$

3^c の性質は、後に 4 節でも述べるが、次のように考えてもよい。 α の β ($\neq 0$) による左商を作ると、丁数が作る立方格子のどこかの超立方体の内または周にある。その超立方体の頂点または中心のうち、それに最も近い点は必ずそれと 1 未満の距離にある。それを γ とすればよい。(4 節で再論する。)

Hurwitz の整数全体は、4 次元の 体心立方格子 をなす。0 に最も近いのは、ノルムが 1 である 24 個の次の数である。

$\pm 1, \pm i, \pm j, \pm k, (\pm 1 \pm i \pm j \pm k)/2$; 複号はすべての組合せをとる。

これらは 1 を割り切るから、すべての整数の約数である。これらを 単数 という。単数因子だけ違う 2 数を、互いに 同伴数 という。

整数の積に関する性質、例えば約数・素因数分解などを考えるときには、同伴数を同一の数とみなさなくてはならない。普通の整数では、符号の差に過ぎないが、複素整数を扱うときには、これを意識する必要がある。四元数整数の同伴数の内から代表数を選ぶ方法は、5 節で論ずる。

3. 四元数体の自己同型変換

0 で割ることを除いて、四則演算が自由にできる体系 $\overset{K}{\wedge}$ を 体 という。体 K から K の上への一対一写像で、和には和が、積には積が対応するものを、体の 自己同型変換 という。但し実数体を含む体では、対応の連続性をも仮定しておく。

定義から、0 には 0 が、1 には 1 が対応する。従って有理数は自分自身にうつる。連続性を仮定すれば、実数体の自己同型変換は恒等変換しかない。

複素数体では、虚数単位 i が $+i$ か $-i$ かに移るから、自己同型変換は、恒等変換かまたは共役複素数をとる写像に限る。

では4元数のときはどうか? このときには次のような変換がある。 任意の0でない4元数 λ に対して

$$T(\lambda) \cdot \alpha = \lambda \alpha \lambda^{-1}$$

と置くと、これは自己同型変換である。 しかも $\lambda = c\mu$ (c は0でない実数)のときには $T(\lambda) = T(\mu)$ である。(この像を α の“共役数”ということがある)

この他にあるか? 結果はそれだけである。 次の定理が成り立つ。

定理 2. 有理数を成分とする4元数全体のなす体の自己同型変換は、上に述べた $T(\lambda)$ に限る。 しかも $T(\lambda) = T(\mu)$ となるのは、 $\lambda = c\mu$, c は実数 のときに限る。

系 4元数整数の自己同型変換は、 $T(\lambda)$ であって、 $\lambda = \epsilon$ (単数) または $\lambda = \zeta = 1+i$ の同伴数 (ノルムが2の数) に限る。

証明 実数は自分自身に移るから、基底 i, j, k の像 i', j', k' を調べればよい。

これらは基本関係を満たす。 $\lambda = k-i'j$ と置くと、 $\lambda i = j+i'k = i' \lambda$ である。 但し $\lambda = 0$ のときには、 $i' = i$ だから、改めて $\lambda = 1$ と置く。

$T(\lambda^{-1})$ による i', j', k' の像を i'', j'', k'' と置く。 $i'' = i$ に注意する。

$\mu = -(j''j+1)i$ と置く。 但し $\mu = 0$ のときは、 $j'' = j$ なので、改めて $\mu = 1$ と置く。 いずれにしても

$$\mu i = i'' \mu, \quad \mu j = j'' \mu$$

が計算できる。 従って、 $T(\mu^{-1})$ による i'', j'', k'' の像はそれぞれ i, j, k になり、初めの変換は $T(\lambda\mu)$ に等しい。

後半は、 $\lambda^{-1}\mu = \nu$, $T(\nu) = T(1)$ とすると、 i, j に対する式から、 ν の i, j, k 成分がいずれも0になることからわかる。

系の証明 4元数整数の自己同型変換は、有理数係数4元数の自己同型変換に拡張される。 λ が単数ならば、整数の変換になるが、 ζ のときも

$$\zeta(a+bi+cj+dk)\zeta^{-1} = a+bi-dj+ck$$

により整数の変換になる。 ノルムが2の整数は全部で24個あり、すべて ζ の同伴数である。

さて四元数整数の変換は、実数を変えないので、 i, j, k は1と直交する単数に移る。それらは $\pm i, \pm j, \pm k$ のいずれかである。これらは3次元空間の正八面体を^{なし、それと}自分自身の上に移す変換である。それは全部で24個ある。

所がノルムが1, 2である整数はそれぞれ24個ずつ合計48個あり、それらは符号が違う組を除いて互いに比が実数ではない。従ってそれらは合計24個の相異なる変換を与える。故にその24個が24個の変換と一対一に対応し、それ以外にはない。(終)

付記 単数全体は、4次元の正24胞体とよばれる正多面体をなす。原点からこれらの頂点を結んだベクトル全体は、単純リー群の分類理論において D_4 とよばれるルート系なので、これによる格子を D_4 格子とよぶ。

この正24胞体は、一辺の長さが1の超立方体の上に、底が一辺1の立方体、高さが $\frac{1}{2}$ のピラミッド8個を合せた図形なので、その体積は2である。

ノルムが2の整数全体は、これを $\sqrt{2}$ 倍に拡大した正24胞体である。両者を合せた頂点を原点から結んだベクトルのなす図形は、例外単純リー群 F_4 のルート系とよばれるものである。

格子があるとき、その中の一点 O が最も近い点の集合を、 O の勢力域という。

四元数整数のなす格子に関する原点の勢力域は、ノルムが2の点のなす正24胞体を半分に縮めた図形である。その体積は $\frac{1}{2}$ である。

4. 二つの四元数の最大公約数

次の定理は2節でも述べたが、もう少し構造的な証明をしておく。

定理 3. 任意の四元数^{整数} α, β ($\neq 0$) に対して、

$$N(\alpha - \gamma\beta) < N(\beta), \quad N(\alpha - \beta\delta) < N(\beta)$$

を満たす γ, δ が(一意的とは限らないが)存在する。

(i) β が正の整数 p のときをまず示す。 証明

$$\alpha = h\rho + \mathfrak{q}i + mj + nk$$

に対して、整数 a, b, c, d を

$$|h - pa| \leq p/2, \quad |h + 2\mathfrak{q} - p(a + 2b)| \leq p, \quad |h + 2m - p(a + 2c)| \leq p, \quad |h + 2n - p(a + 2d)| \leq p$$

となるように定めることができる。ここで $\gamma = ap + bi + cj + dk$ と置くと

$$\alpha - \gamma p = [(h-pa) + (h+2q-p(a+2b))i + (h+2m-p(a+2c))j + (h+2n-p(a+2d))k] / 2$$

となる。この成分の絶対値はそれぞれ $p/4, p/2, p/2, p/2$ 以下なので、左辺のノルムは

$$\leq 13p^2 / 16 < p^2$$

である。なお上の a, b, c, d は原則として一意に定まるが、丁度中央に来たときには、二通りになることがある。

(ii) 一般のとき $\alpha \bar{\beta}$ [または $\bar{\beta} \alpha$] と $p = \beta \bar{\beta} = N(\beta)$ について (i) を適用すればよい。(終)

さて二つの 0 でない四元数整数 α, β が与えられたとき、

$$\alpha_1 = \alpha, \alpha_2 = \beta \text{ から順次 } \alpha_{i+1} = \alpha_i - \gamma_i \alpha_i, N(\alpha_{i+1}) < N(\alpha_i)$$

として、互除法ができる。同様に右商による互除法もできるが、差し当たり左商で考える。

正の整数であるノルムが真に減少するから、有限回の後に $\alpha_{p+1} = 0$ となる。

その1つ手前の $\alpha_p = \delta$ を、初めの2数の(右) 最大公約数 という。これは次の性質をもつ。

一般に $\alpha = \gamma \beta$ であるとき、 γ を α の左約数、 β を α の右約数 という。

定理 4. (i) $\delta = \alpha_p$ は、初めの2数の右約数である。(ii) 初めの2数の任意の右約数は、 δ の右約数でもある。

(iii) λ, μ をうまくとると $\lambda \alpha + \mu \beta = \delta$ が成立するようにできる。

証明 (i), (ii) は互除法の式から直接にわかる。(iii) は、まず

$$\lambda_1 = 1, \mu_1 = 0, \lambda_2 = 0, \mu_2 = 1$$

と置き、以下順次互除法の商 γ_i を使って

$$\lambda_{i+1} = \lambda_{i-1} - \gamma_i \lambda_i, \mu_{i+1} = \mu_{i-1} - \gamma_i \mu_i$$

と置くと、各 $i=1, 2, \dots$ について $\lambda_i \alpha + \mu_i \beta = \alpha_i$ が成立するから、

$\lambda_p = \lambda, \mu_p = \mu$ と置けばよい。(終)

この定理により、普通の整数と似た性質を色々と導くことができる。

四元数整数全体 H は、加法・減法・乗法が自由にできる体系である。数学の用語では、これを『環』という。

注意 環は Ring の直訳語である。原語には、ものの集りという意味もある。輪とは関係ない。

H の部分集合 J で、加法・減法について閉じており、さらに J の要素に任意の四元数整数を左[右]から掛けた積も J に含まれる、という性質をもつものを、 H の イデアル という。(正しいのは 左[右]イデアル)

注意 この奇妙な名前は、Kummer の理想数を、Dedekind が整理したときに付けた歴史的な由来による。強いて訳せば『理想系』とでもいう所か？

イデアルの典型例は、ある定数 α に左から四元数整数を掛けて出来る数全体である。これを α から生成される (左) 単項イデアル という。

定理 5. H のイデアルは、すべてある定数から生成される単項イデアルである。

証明 J が 0 だけならば、0 から生成される。そうでなければ、 J の 0 でない要素の内、ノルムが最小のもの一つ α をとる。

J の任意の数 β に対して、 $\beta - \gamma \alpha = \lambda$ のノルムが $N(\alpha)$ 未満にできる。

定義により λ は J に含まれるから、0 でなければ、 α のノルムが最小という仮定に反する。故に J のすべての要素は、 α に左から 四元数 整数を掛けてえられる数である。(終)

定理 6. 四元数整数 α と、普通の整数 p に対して、両者のノルムが互いに素なことと、両者の右及び左最大公約数がいずれも単数であることとは、同値である。このとき両者は『互いに素』という。

証明 右または左の最大公約数が、単数でなければ、両者のノルムは 1 でない公約数をもつ。逆に右最大公約数が単数ならば、

$$\lambda \alpha + \mu p = 1$$

を満たす λ, μ がある。そのとき

$$N(\lambda) \cdot N(\alpha) = N(1 - \mu p) = 1 + N(\mu) p^2 - (\mu + \bar{\mu}) p$$

となる。もしも $N(\alpha)$ と p^2 とに 1 でない公約素数 q があれば、 q は p の約数なので、1 を割り切ることになって矛盾である。左最大公約数も同様である。(終)

なおこの証明は、 p が実の整数でなくても、実質的にすべての四元数整数と交換可能な整数、即ち単数 ϵ またはノルムが2の整数 ϵ についても、適用できる。従ってこれらの整数については、左約数・右約数の区別なしに、互いに素、及びそれを法として合同という概念を使うことができる。

5. 四元数の偶数・奇数と代表数

四元数整数 α について

ノルムが偶数 $\longleftrightarrow \alpha$ が ϵ で割り切れる

ノルムが奇数 $\longleftrightarrow \alpha$ が ϵ と互いに素

という関係が成立する。前者を偶数、後者を奇数という。偶数はすべて丁数である。

丁数は、 ϵ を法として、0 か 1 と合同である。前者は偶数、後者は奇数である。

半数は、 ρ を引けば丁数になる。それが偶数か奇数かに応じて、第1種の半数・第2種の半数とよぶ。前者は ρ と、後者は ρ^2 と合同である。 ϵ で類別した四元数整数はの体系は、 $0, 1, \rho, \rho^2 (\equiv \rho + 1)$ で代表される。これは4個の要素からなる標数2の有限体 $GF(4)$ と同じものである。

ノルムが偶数である四元数整数 α について、 $N(\alpha)$ が2の r 乗で割り切れるが、それ以上では割り切れないとすると、 $\alpha = \epsilon^r \cdot \beta$, β は奇数 と書ける。

2 を法とする合同式の代表としては、単数の内の半分

$$1, i, j, k, (1 \pm i \pm j \pm k)/2$$

と $0, 1+i, 1+j, 1+k$ との合計16個である。

このうち12個の単数は、奇数を2で割った剰余系全体をなす。従って、任意の奇数 β に対して、

$$\beta \epsilon \equiv \epsilon' \beta \equiv 1 \pmod{2}$$

を満たす単数 ϵ, ϵ' が、符号を除いて一意的に定まる。他方2を法として1と合同な整数は、2 ϵ を法としたときには、 $1, -1, 1+2\rho, -1-2\rho$ のいずれかと合同になる。

ノルムが奇数の

四元数整数の内、2を法としたとき、1または $1+2\rho$ に合同な数を、代表数(primary number)とよぶ。

注意 Primary number は重要な数といった感じの語である。ふつうこの術語は『準素数』と訳することが多いが、この場合には感じが違う。代表数とは、仮の意識である。

ノルムが奇数である

任意の四元数整数 α について、それに左[右]から単数を掛けた24個の同伴数のうち、常に一つだけ代表数がある。なお代表数はすべて丁数である。2個の代表数の積は、やはり代表数である。また α が代表数のとき、2を法として1と合同か $1+2\rho$ と合同かに応じて、 $\bar{\alpha}$ または $-\bar{\alpha}$ も代表数である。(例はp.16)

以下では、ノルムが奇数 p である四元数整数の構造を調べる。

$\text{mod } p$ の体系の代表としては、 a, b, c, d を $0, 1, \dots, p-1$ のいずれかとして

$$\alpha = a + bi + cj + dk$$

という p^4 個の数をとってよい。

他方 $\text{mod } p$ の整数を係数とする2次元の一次変換は

$$S: \quad y_1 = sx_1 + tx_2, \quad y_2 = ux_1 + vx_2 \pmod{p}$$

という形で、全部で p^4 個ある。この両者の間には、次のような密接な関係がある。

定理 7. 上の p^4 個の四元数 q と、 p^4 個の一次変換 S との間に一対一の対応をつけて、積 $\alpha\alpha'$ が変換の合成 SS' に対応し、さらに $N(\alpha) \equiv sv - tu \pmod{p}$ であるようにできる。

この証明には、まず次のLagrangeの定理が、補助定理として必要である。

補助定理 奇数 p に対して、 $1 + m^2 + n^2 \equiv 0 \pmod{p}$ を満たす整数 m, n がある。

補助定理の証明 (Serret による) (i) p が素数のとき。 -1 が平方剰余ならば、 m をその平方根、 $n = 0$ とすればよい。そうでなければ、 $p-1, p-2, \dots$ の内初めて平方剰余になる数を b とすると、 $a = b+1$ は平方非剰余だから、 $b = m^2, -a = n^2$ を満たす整数があり、それらが求めるものである。

(ii) 一般のとき。 p を素因数分解して、それぞれについて m, n を作る。それから各因数の累乗に対する解ができ、その積に対する解を孫氏剰余定理で作

ることができる。

定理 7 の証明 $1+m+n^2 \equiv 0 \pmod{p}$ ならば、

$$a^2 + b^2 + c^2 + d^2 \equiv [a^2 - (mc+nd)^2] - [(nc-md)^2 - b^2] \pmod{p}$$

である。従って $\pmod{p}$ で

$$s \equiv a - mc - nd, \quad v \equiv a + mc + nd, \quad t \equiv b - nc + md, \quad u \equiv -b - nc + md$$

と置くと、逆に $\pmod{p}$ で

$$2a \equiv s + v, \quad 2b \equiv t - u, \quad 2c \equiv m(s - v) + n(t + u), \quad 2d \equiv n(s - v) - m(t + u)$$

と解くことができる。この対応で、 $N(a+bi+cj+dk) \equiv sv - tu \pmod{p}$ である。

ここでさらに

$$\xi = 1 + mj + nk, \quad \eta = i + nj - mk = \xi i = \overline{i \xi}$$

と置くと、 $2\alpha \equiv s\xi + t\eta - u\overline{i\xi} + v\overline{\xi} \pmod{p}$ である。このような数と変換との対応を作る。他の組と掛け合わせると、丁度数の積に変換の合成が対応している。(終)

a, b, c, d の最大公約数が p と互いに素な数を 原始的 (primitive) という。ノルムが p の倍数になる原始的な数は、 $sv - tu$ が p の倍数になる組に対応する。

p が素数ならば、そのような組は全部で

$$(p^2 - 1)(p + 1) = p^3 (1 - 1/p^2)(1 + 1/p)$$

個ある。一般の奇数 p では、素因数分解して掛けると、合計

$$p^3 \prod (1 - 1/q^2)(1 + 1/q) \text{ 個, 積は } p \text{ のすべての素因数 } q \text{ にわたる}$$

である。同様にノルムが $\pmod{p}$ で 1 と合同な数は

$$N = p^3 \prod (1 - 1/q^2) \text{ 個}$$

ある。そのような数全体は群をなし、それは $\pmod{p}$ に関する整数係数の一次変換群と同型である。

例えば $p=3$ のときには、 $N=24$ である。24 個の単数は、3 (一般に 2 より大きい整数) について、互いに合同でないから、これは単数全体が乗法で作る群である。それは同次四面体群と同型である。

6. 四元素数と素因数分解

単数でない

四元数整数 κ が、もしも2個の四元数整数の積 $\alpha\beta$ と表されたならば、因数のどちらかが単数でなければならないという性質を満たすとき、四元素数という。

複素整数については、普通の素数の内、素数のままでいるものと素数でなくなるものがある。Gaussの整数についていえば、2と $4n+1$ 型の素数が素数でなくなる。Eisensteinの整数についていえば、3と $6n+1$ 型の素数が素数でなくなる。

四元数整数では、 a, b を普通の整数とすると、

$a+bi$ 全体が Gaussの整数; $a+b\rho$ 全体がEisensteinの整数に対応するから、上述の数は素数ではない。しかし四元数整数では、普通の整数はすべて四元素数ではない。

その理由は、Lagrangeが示した通り、任意の正の整数 m は、必ず4個以下の平方数の和

$$m = a^2 + b^2 + c^2 + d^2$$

に表されるので、 $m = (a+bi+cj+dk)(a-bi-cj-dk)$ と分解されるからである。

四元素数には、次のような明解な判定条件がある。

定理 8. κ が四元素数であるための必要十分条件は、そのノルム n が普通の素数であることである。

証明 十分性は明らかである。もしも κ のノルムが素数であり、 $\kappa = \alpha\beta$ ならば、積 $N(\alpha) \cdot N(\beta)$ が素数だから、どちらかが1でなければならない。

次に必要性を示す。 κ のノルムを n とし、 n の一つの素因数を p とし、 $n = pq$ と置く。 p を四元数整数とみなして、 κ との最大公約数 δ をとる。 δ は κ の約数だから、単数かまたは κ の同伴数である。もしもこれが単数ならば、1としてよく、 λ, μ をとって

$$\lambda \kappa + \mu p = 1$$

とできる。これから

$$pqN(\lambda) = N(\lambda\kappa) = N(1 - \mu p) = 1 + N(\mu)p^2 - (\mu + \bar{\mu})p$$

となり、1が p の約数となって矛盾である。故に $\delta = \kappa$ である。つまり p は κ で割り切れる。その商のノルムを r とすれば、ノルムをとって

$$p^2 = pqr \quad \text{つまり} \quad p = qr$$

をうる。 p は素数だから、 $q=1$ か $r=1$ かである。 もしも後者をとると、 p は κ の同伴数になるが、前に述べた通り、普通の整数 p は四元素数ではないから矛盾である。 故に前者であり、 κ のノルム n は素数 p に等しい。(終)

ノルムが2の数は、 $1+i$ の同伴数合計24個である。 以下、3以上の素数 p を固定し、ノルムがそれに等しい代表数の個数を求めよう。

前節で述べた通り、 $\text{mod } p$ での剰余類は p 個あり、そのうちノルムが p の倍数であるものは、0以外に

$$(p^2 - 1)(p + 1)$$

個ある。 そのような数を代表的に $\theta = a+bi+cj+dk$ と書く。 ここで $N(\theta)$ が p では割り切れるが、 p^2 では割り切れないと仮定してよい。 何故なら

$$(a+sp)^2 + (b+tp)^2 + (c+up)^2 + (d+vp)^2 \equiv N(\theta) + 2p(as+bt+cu+dv) \pmod{p^2}$$

だから、 $as+bt+cu+dv$ が p の倍数でないようにとって、 $s+ti+uj+vk$ の p 倍を加えればよいからである。

定理 9. 奇素数 p に対して、ノルムが p である代表数は、丁度 $p+1$ 個ある。

系. ノルムが奇素数 p に等しい四元数整数は、合計 $24(p+1)$ 個ある。

証明 上のような θ と p との最大公約数 δ を作る。 定理8の証明と同様にし、 δ は単数ではないことがわかる。 それを代表数としてよい。 そのノルムは p である。 逆に、ノルムが p の代表数 δ に対して、 $\theta \equiv \delta \pmod{p}$ を満たす θ がある。

それは $\theta = \alpha \delta$ 、 $p = \bar{\delta} \delta$ という関係式を満たすものである。 ここで θ と θ' とが同じ δ に対応する条件を考える。 その必要十分条件は、 $\text{mod } p$ で一方が他方の右約数になること： $\theta' \equiv \beta \theta$ である。

これを証明しよう。 仮定により $\theta = \alpha \delta$ 、 $\theta' = \alpha' \delta$ であり、 α 、 α' のノルムは p と互いに素である。 故に $\beta \alpha \equiv \alpha' \pmod{p}$ である β をとることができる。 逆にそうなら

$$\theta' = (\beta \alpha + \alpha' \bar{\delta}) \delta$$

である。 このような β は、実質的に p^2 個ある。 それは $\beta \theta \equiv 0 \pmod{p}$ の解が p^2 個だからである。

0を除いて、丁度 p^2-1 個ずつが同じ代表数に対応するので、代表数の個数は $p+1$ 個になる。(終)

例 代表数を具体的に求めるのには、次の事実に注意するとよい。

- 1°. 代表数は、成分の和が $4n+1$ の形の数になる丁数である。
- 2°. p が $4m+1$ の型か、 $4m-1$ の型かに応じて、それぞれ 1 か $1+2p$ かに合同になる。
(ノルム) 前者では実部が奇数で虚部が偶数、後者では実部が偶数で虚部が奇数である。

p	代表数	個数
3	$-i-j-k, i+j-k, i-j+k, -i+j+k$	4個
5	$-1 \pm 2i, -1 \pm 2j, -1 \pm 2k$	6個
7	$\pm 2+i+j+k, \pm 2+i-j-k, \pm 2-i+j-k, \pm 2-i-j+k$	8個
9	$-3, 1 \pm 2(i \pm j), 1 \pm 2(i \pm k), 1 \pm 2(j \pm k)$ (複号はすべての組合せをとる)	13個
11	$3i \pm (j+k), -3i \pm (j-k), 3j \pm (i+k), -3j \pm (k-i), 3k \pm (i+j), -3k \pm (i-j)$	12個
13	$3 \pm 2i, 3 \pm 2j, 3 \pm 2k, 1 \pm 2i \pm 2j \pm 2k$ (すべての組合せ)	14個

さて任意の四元数整数は、 $\gamma \cdot \beta$, β は奇数 という形に表される。従って素因数分解は、奇数の代表数のみを考えればよい。更にその成分に実の公約数があればくりだしてよいから、原始的 (成分の間に公約数がない) としてよい。

定理 10. 原始的な奇数の四元数整数 α があるとき、ノルムを (代表数)

$$N(\alpha) = p_1 \cdots p_s$$

と素因数分解する。但し p_i には同じものがあってもよいが、積の順序を定めておく。このとき各 i に対して、ノルムが p_i であるような代表数である四元素数 κ_i が一意的に定まり

$$\alpha = \kappa_1 \cdots \kappa_s$$

と表される。

証明 α と p_1 との最大公約数 κ_1 をとる。定理 8 と同様に、 κ_1 は単数でなく、ノルムが p_1 である。 $\alpha = \kappa_1 \alpha_1$ とすると、 α_1 も原始的で、そのノルムは $p_2 \cdots p_s$ である。これを繰返せばよい。

一意性 も、この操作がすべて一意的に定まることと、逆にそのような κ_i があれば、左から順に上の操作で定まることからわかる。(終)

注意 交換可能でないため、素因数分解そのものは、必ずしも一意的ではない。

定理 11. 任意の奇数 m に対して、ノルムが m である代表数の個数は、 m の約数の総和

$$\psi(m) = m \prod_i (1 + 1/p_i), \quad m = \prod_i p_i^{r_i}$$

に等しい。

系 正の整数 n に対して、ノルムが n である四元数整数の個数は、 n の奇数の約数全体の和の24倍に等しい。

証明 m を $p_1^{r_1} p_2^{r_2} \cdots$ と素因数分解して、この順に定理10を適用すると、ノルムが m である代表数は、

$$\pi_1 \cdots \pi_{r_1} \cdot \kappa_1 \cdots \kappa_{r_2} \cdots$$

と表される。ここで π_{r_1} はノルムが p_1 の代表数である素数、 κ_{r_2} はノルムが p_2 である代表数である素数... である。この積はすべて相異なる代表数であり、逆にノルムが m の代表数はそれで尽くされる。相異なる素因数に対する部分は、独立な積になる。

同一のノルムをもつ項については、相隣る項が互いに共役(変換 $T(\lambda)$ で移る数)でないときに原始的である。このことは項数の帰納法により、証明できる。

すなわちもしも $\pi_1 \pi_2 \cdots \pi_{r_1} = \pi_1 \alpha$ が原始的でなければ、

$$\overline{\pi_1} \pi_1 \alpha = N(\pi_1) \alpha \equiv 0 \pmod{p}$$

であり、 $\pi_1 \cdots \pi_{r_1} = p \beta = \pi_1 \overline{\pi_1} \beta$, 即ち $\alpha = \overline{\pi_1} \beta$ となる。分解の一意性から、

$$\pi_2 = \pm \overline{\pi_1}$$

となり、互いに共約な2数が隣合うことになる。

このことから、ノルムが p^{r_1} のとき、相異なる代表数は、合計 $\frac{p^{r_1+1}-1}{p-1} = \psi(p)$ 個あることがわかる。

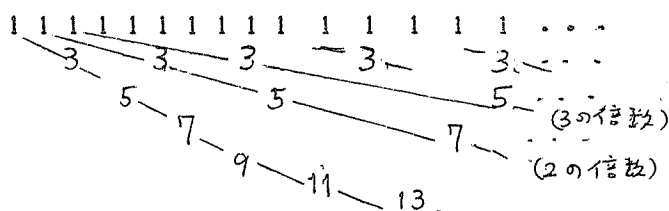
系は、とをくりだしたあと、ノルムが奇数の整数の個数を求めればよい。(12)

なおノルムが偶数の整数は、すべて丁数である。ノルムが奇数の整数は、代表数がすべて丁数であり、単数の内 8個が丁数、16個が半数であることから、半数が丁数の2倍だけあることがわかる。このことから、次のJacobiが証明した定理もわかる。

定理 12. 正の整数 n を 4 個の平方数の和に表す方法の数は、項の順序を問題とし、さらに正・負の数を区別するならば、 n の奇数の約数の総和を d とするとき、 n が奇数なら $8d$, n が偶数なら $24d$ に等しい。

系 正の整数 m を 4 個の正の三角数の和に表す方法の数は、順序を問題にすると、 $2m+1$ の約数の和に等しい。

さて四元数整数全体のなす D_4 格子の勢力域、及び 4 次元単位超球の体積をそれぞれ v , w とする。十分大きい半径 $\sqrt{n}$ の超球内の格子点の個数を評価しよう。ノルムが $1, 2, \dots$ の整数の個数の $1/24$ の和は



の形の和である。 $1+3+5+\dots+n$ はほぼ $n^2/4$ であるから、この和を斜めに足すと、ほぼ

$$\left[n^2 + (n/2)^2 + (n/3)^2 + \dots \right] / 4$$

となる。 $s = \sum (1/k^2)$ と置くと、この和はほぼ $s n^2/4$ である。これだけの個数の勢力域の和が、ほぼ半径 $\sqrt{n}$ の超球になるから、

$$24 v s n^2 / 4 \sim w n^2$$

n^2 で割って
である。 $\wedge n$ を ∞ にすると、低次の項が 0 に近づき、等式

$$6 v s = w$$

をうる。 実際の値は

$$v = 1/2, w = \pi^2/2, s = \pi^2/6$$

であって、当然成立している。これらはすべて直接に計算できる。しかしこの関係により、この内二つがわかれば、第三の値も自動的にわかる。思い掛けない量が、互いに結び付いていると感ずるのではなかろうか。

7. Eulerの問題への応用

Eulerの問題とは、現代流にいうと次のようになる。

普通の整数を成分とする 4 次の直交行列 A で、 AA^T が単位行列の定数倍になるものをすべて求めよ。 (A^T は A の転置行列)

もしも2次ならば、直接に求めることができる。その答は、複素整数の表現に当る

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

か、またはこの行を入換えたものである。行列式を正と限れば、前者だけになる。

4次のときにも、4元~~数~~整数を使うとうまく解ける。 $x_0, x_1, x_2, x_3; y_0, y_1, y_2, y_3$ を成分とする縦ベクトルを、それぞれ x, y とし、 $y = Ax$ と置く。またこれらを成分とする四元数をそれぞれ ξ, η として、これらをベクトル x, y の表現とみなす。このとき

定理 13. $AA^T = cI$ を満たす行列 A は、0でない四元数 α, β により、

$$\eta = \alpha \xi \beta$$

という関係で作られる。特に行列式が1の A は、 α, β がノルム1の数で作られる。

証明 この形で作られる変換行列は、行列式の値が $[N(\alpha\beta)]^2$ に等しい直交行列である。逆にそのような行列があるとして、成分を

$$A = [a_{\ell m}] \quad (\ell, m=0, 1, 2, 3)$$

と置くと、 $1, i, j, k$ をそれぞれ i_0, i_1, i_2, i_3 と書いて

$$\eta = \sum \lambda_{\ell} i_{\ell}, \quad \lambda_{\ell} = \sum_m a_{\ell m} i_m \quad (\text{和は0から3})$$

であり、所要の条件は $\alpha i_{\ell} \beta = \lambda_{\ell}$ である。 α, β の成分をそれぞれ a_{ℓ}, b_{ℓ} とする。また u_{ℓ}, v_{ℓ} ($\ell=0, 1, 2, 3$)を未知数とし、これらを成分とする四元数をそれぞれ v, ω とすると、求める条件は

$$4(\sum a_{\ell} u_{\ell})(\sum b_{\ell} v_{\ell}) = \text{Re}[\theta \cdot \bar{\omega}], \quad \theta = \overline{v} \lambda_0 - \sum_{m=1}^3 i_m \overline{v} \lambda_m$$

である。これらは u_{ℓ}, v_{ℓ} に関する双一次形式であり、その係数は A の成分である。この式は行列変換が $\eta = \alpha \xi \beta$ で与えられることを意味する。

行列式が1のときには、 $\alpha\beta = 1$ になるので、両者は逆数にとってよい。実数倍すれば、ともにノルム1としてよい。(13)

Eulerの問題の一般解は、この形に実の有理数を掛たもので与えられる。それをもう少し整理してみよう。

$y = r \alpha x \beta$, α, β は四元数整数、 r は実の有理数。

r の分子は必要なら α に掛^けてよいから、1 としてよい。このとき実は $r=1$ または $\frac{1}{2}$ である。その証明を述べる。

r の分母に奇数の素数因子 p があれば、 α, β の成分を a_ℓ, b_ℓ とするとき

$$4 \sum_{\ell} a_{\ell} u_{\ell} \cdot \sum_{\ell} b_{\ell} v_{\ell} \equiv 0 \pmod{p}$$

となるが、これは a_ℓ または b_ℓ がすべて p で割り切れなければ成立せず、原始的な数をとったことに反する。ただし $p=2$ のときには、 α も β も 2 で割り切れなければ、共に 2 で割り切れる場合がある。このときには

$$y = \alpha x' \beta, \quad x' = \zeta x \cdot \zeta / 2 = -x_1 + x_0 i_1 + x_2 i_2 + x_3 i_3.$$

と書ける。そして $\alpha \beta$ は丁数でなければならない。結局 Euler の問題の一般解は

$\alpha \beta$ が丁数である四元数整数 α, β に対して

$$y = \alpha x \beta \quad \text{または} \quad y = \alpha x' \beta$$

である。特に α, β が丁数であり、 $\alpha \beta$ かまたは $\alpha \beta - 1$ のノルムが普通の偶数ならばよい。

例 $y = (5+5i+9j)x(6-4i-2j+3k)$

とすると、条件が満たされる。このとき行列は次のようになる。これは Euler 自身が求め、後に Legendre が『整数論』で裏付けをしている歴史的な例である。

$$\begin{bmatrix} 68 & 17 & -59 & 11 \\ 37 & 32 & 61 & 49 \\ 29 & 31 & 28 & -77 \\ 41 & -79 & 23 & -8 \end{bmatrix}$$

8. 八元数整数について

乗法の交換法則を犠牲にしても、実数は四元数以上には拡張できない。しかし乗法の結合法則をも緩めれば、さらに拡張して、八元数ができる。これは普通Cayley数とよばれる。

Cayley数の表し方は、色々の流儀がある。ここでは [4] に倣って、次のように約束する。

$$\alpha = \sum a_\ell e_\ell, \ell=0, 1, \dots, 7; e_0=1$$

$$e_\ell^2 = e_1 e_2 e_4 = e_2 e_3 e_5 = e_3 e_4 e_6 = e_4 e_5 e_7 = e_5 e_6 e_1 = e_6 e_7 e_2 = e_7 e_1 e_3 = -1$$

和は成分ごとに行う。 e 同志の2個の積は、1節と同様に解釈する。 e_ℓ の三つ組の内、次の番号の組は結合法則を満たす。

$$1\ 2\ 4, 2\ 3\ 5, 3\ 4\ 6, 4\ 5\ 7, 5\ 6\ 1, 6\ 7\ 2, 7\ 1\ 3$$

これは『七人の夜警』の問題の1つの解である。 — それは、7人のメンバーの内毎晩3人ずつが勤務し、7日で一回りするとき、どの2人も丁度1回ずつ同じ晩に勤務するように組合せよという問題である。

この関係は、 $1, \dots, 7$ の巡回的置換と、互換の積 $(1\ 2)(3\ 6)$ によって不変であり、番号の付け方は、理論上 480通りが可能である。

なお m, n の内に同じものがあるときには、積 $e_\ell e_m e_n$ について結合法則が成立することも、注意する価値がある。

α に対して、 a_0 以外の成分の符号をすべて変えた数を $\bar{\alpha}$ と書いて、 α の共役数という。四元数のときと同様に、

$$\text{ノルム } N(\alpha) = \sum a_\ell^2 = \alpha \bar{\alpha} = \bar{\alpha} \alpha$$

であり、 $\alpha \neq 0$ ならば、 $\alpha^{-1} = \bar{\alpha} / N(\alpha)$ である。

このとき、定理 1 に相当する公式は、8個の平方数の和の2組の積が、8個の平方数の和で書けるという公式になる。これは Deganの公式とよばれるが、直接展開して計算するのはかなりしんどい。

さて八元数整数には、すべての成分が整数の数と、それがすべて半整数の数とだけではなお足りない。4個の成分が整数、残りの4個の成分が半整数である『混合型』の数をも許す必要がある。ただしそのすべてを加えては多過ぎる。

特定の組だけを、うまく選び出さなければならない。

その条件は、 $\{0, 1, \dots, 7\}$ の内の4個の要素からなる部分集合の組で、任意の2組をとったとき、両者の共通部分が空であるか、または丁度2個の要素からなるようなものを、出来るだけ沢山とることである。

このような組は、14個より多く作ることはできないが、うまく作れば最大の個数にできる。その一例は、前出の7人の夜警問題の解に0を付け加えた7組と、その補集合の合計14組をとればよい。これは誤り訂正符号系の、極く簡単な一例である。

番号を付け変えれば、これらの組は次のような簡単な規則で構成できる。0 ~ 7を二進法で3桁の数に表す。各桁ごとに桁上げしない加法(排他的論理和)で加える演算を考える。4個の番号 i, j, k, l の二進和が000になるような組 $\{i, j, k, l\}$ を採ると、所要の14組になる。

そのような組に属する番号のみ整数、他は半整数の成分をもつ八元数全体を採ると、2節の3条件を満たす系ができる。これを八元数整数という。

このような体系を初めて研究したのは、J.Kirmse(1924)であった。しかし不幸にして、彼の論文には計算誤りがあり、彼の提示した系は乗法について閉じていなかった。もっとも後に、番号をうまく付け変えと、正しい八元数整数になることが確かめられた。

この系で、ノルムが1の単数は合計240個ある。それらは例外単純リー群 E_8 のルート系をなすので、八元数整数全体のなす8次元格子を、 E_8 格子という。その基本勢力域は、ノルムが2の数合計2160個のなす図形を半分に縮小したもので、体積は $1/16$ である。

E_8 格子そのものは、これを2倍に拡大して回転してできる、次の形の方が扱い易い。この形にすると、ノルム(原点からの距離の2乗)はすべて偶数になる。

成分がすべて整数である点(丁点)と、成分がすべて半整数である点(半点)のうち、成分の和が偶数であるもの全体をとる。

この形にするとき、ノルムが偶数 $2n$ である丁点の個数 M と半点の個数 N との間に、次のような著しい関係がある。暇があったら、マイコンで n が小さいとき

を試してみると面白い。

$$M + N = 240 \sum \{d^3; d \mid n\}, M - N = 16 \sum \{(-1)^{d/3} d^3; d \mid n\}$$

ただし $d \mid n$ は、 d が n の約数であることを表し、和は n のすべての約数 d にわたる。特に n が奇数ならば、 $M : N = 7 : 8$ である。

このことから、6節末の議論と同様にして、8次元単位超球の体積 w 、 E_8 格子の基本勢力域の体積 v と、級数の和

$$s = \sum_{k=1}^{\infty} (1/k^4)$$

との間に関係式

$$(240/4) v s = w$$

が成立することがわかる。実際の値は

$$w = \pi^4/24, v = 1/16, s = \pi^4/90$$

であって、もちろん丁度合っているが、前と同様にこの内の二者から、第三の値が計算できる。

八元数整数については、他にも多くの事実が知られている。しかし概して、組合せ的な性質や、図形との関係はわかっているが、整数としての性質はほとんどわかっていないといってよい。その原因は、結合法則が成立しないために、古典的な整数論の方法がほとんど使えないためである。例えば互除法はできても、それが最大公約数と結びつかないのである。

また八元数は結合法則が成立しないので、その上に座標幾何学を作ろうとしても、Desargueの定理が成立せず、従って3次元以上の幾何学はできない。僅かに可能な1,2次元の幾何学が、5種の例外単純リー群と関連している。

ところで私が興味をもった元の問題は、高次元の正則格子であった。8次元より上では、もはや整数として研究することはできない。そして8次元の次にくる極めて密な格子は、16次元ではなくて、24次元の Leech格子である。この話題に触れる暇がないが、その研究にはある種の誤り訂正符号が基本的であり、 E_8 格子がよい見本になる。

この種の話は、現代の数学の第一線というよりも、静かな裏通りといった感じであるが、思い掛けない事実が交錯しているところに、私自身の興味があつた。