数理解析研究所講究録 第2104巻 2019年 24-28

計算機科学から視た2次代数 $\mathbf{Z}_p[\sqrt{q}]$
A Point of View from Computer Sciences of Quadratic Algebras $\mathbf{Z}_p[\sqrt{q}]$

神谷徳昭　　森　和好
Noriaki KAMIYA　　Kazuyoshi MORI
会津大学　　会津大学
Univ. of Aizu *　　Univ. of Aizu †

Abstract

In this note, by a computer science's method we study a property of quadratic algebra $\mathbf{Z}_p[\sqrt{q}]$, $2 \leq q < p$, (p, q are prime numbers).

1　はじめに

この小論では $p, q(p > q)$ を素数とする2次代数 $m + n\sqrt{q} \in \mathbf{Z}_p[\sqrt{q}]$, $m, n \in \mathbf{Z}_p = \mathbf{Z}/(p)$ についての性質を, 計算機科学からの結果に基ずいて具体例をもとにして, $\mathbf{Z}_p[q]$ が体になるかならないか等のある判定条件と具体例を考察したいと思います.

特に $\mathbf{Z}_3[\sqrt{2}]$ を考えると, これは9個の元 $\{0, 1, 2, \sqrt{2}, 2\sqrt{2}, 1+\sqrt{2}, 1+2\sqrt{2}, 2+\sqrt{2}, 2+2\sqrt{2}\}$ から成る体であり, $m + n\sqrt{2} \in \mathbf{Z}_3[\sqrt{2}]$ の時、$m^2 - n^2 q = 1$ となる $(m.n)$ の対は, $(m, n) = (1, 0), (2, 0), (0, 1), (0, 2)$ なる4個存在します. 勿論 $mod\ p$ で考えます.

・$\mathbf{Z}_5[\sqrt{2}]$ は6個存在し, 体となります.

・$\mathbf{Z}_7[\sqrt{2}]$ は6個存在し, 体ではないです.

$1 + 2\sqrt{2}$ と $1 + 5\sqrt{2}$ が零因子で2個以上存在します.

・$\mathbf{Z}_{11}[\sqrt{2}]$ は12個存在し体となります

又, $\mathbf{Z}_{11}[\sqrt{3}]$ は10個存在し, 体ではないです. $5 + \sqrt{3}$, $5 + 10\sqrt{3}$ が零因子の一部です.

注 ここでは平方剰余の概念なしで考えたいと思います。

2　主要な結果

$M_2(p, q) = \{ \begin{pmatrix} m & nq \\ n & m \end{pmatrix} | m, n \in \mathbf{Z}_p \}$ とおく。

命題 1

$\mathbf{Z_p}[\sqrt{\mathbf{q}}] \cong \mathbf{M_2(p, q)}$ ($\mathbf{Z_p}$ 上の代数として同型)

*nskamiya@opal.ocn.ne.jp
†k-mori@u-aizu.ac.jp

補題 2
$\mathbf{Z}_p[\sqrt{q}]$ が体である．$_{iff} \Longleftrightarrow \forall x = m + n\sqrt{q}(\neq 0)$ に関して $m^2 - n^2 q \neq 0$.

命題 3
次は同値.
1) $\mathbf{Z_p}[\sqrt{\mathbf{q}}]$ が体である.
2) $M_2(p.q)$ が行列の積において群である.

次に

$$GL(M_2(p,q)) = \{A \in M_2(p,q) | \det\ A \neq 0\},$$

$$SL(M_2(p,q)) = \{A \in M_2(p,q) | \det\ A = 1\}.$$

として $GL(M_2(p,q))$ と $SL(M_2(p,q))$ を定義する.

注意 1

$\begin{pmatrix} m & nq \\ n & m \end{pmatrix}$ の表示は, 複素数 $a + \sqrt{-1}b$ を $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ と表した記号の一般化です.

以上をまとめると,

定理 4
1) $M_2(p,q) \cong \mathbf{Z}_p[\sqrt{q}]$ *(as an algebra)*
2) *If* $\mathbf{Z_p}[\sqrt{\mathbf{q}}]$ が体ならば,

$$GL(M_2(p,q)) \cong \mathbf{Z}_p[\sqrt{q}]^{\times} \quad \text{(as a group of multiplication)}$$

3) $SL(M_2(p,q))$ は $GL(M_2(p,q))$ の正規部分郡である.

次に, $\overline{x} = m - n\sqrt{q}$ (if $x = m + n\sqrt{q}$) と共役を定義すると, $x\overline{x} = m^2 - n^2 q$ となります.
$< x, y >= \frac{1}{2}(x\overline{y} + \overline{x}y)$ と内積を定義すると, $< x, x >= m^2 - n^2 q$ と成り, Norm の性質を持ち, $\det \begin{pmatrix} m & nq \\ n & m \end{pmatrix} = m^2 - n^2 q$ より $< xy, xy >=< x, x >< y, y >$ が成立し, 合成代数の性質をもちます。$\det(AB) = (\det\ A)(\det B)$ です. ただし $A, B \in GL(M_2(p,q))$. しかし, $< x, y >$ は非退化ではないです. 簡単なので証明は省略させていただきます. 大事なのはノルと行列式が同じ概念ということです。
次に,

$$N(p,q) = \ ^{\sharp}\{(m,n) | m^2 - n^2 q = 1,\ m, n \in \mathbf{Z}_p\}$$

と (m,n) の個数を定義する. 実例として $N(3,2) = 4,\ N(5,2) = 6,\ N(7,2) = 6$ 等を表します.

3 計算機による結果

$\mathbf{Z}_p[\sqrt{q}]$ における $m^2 - n^2 q = 1$ の対 (m,n) の個数を考えます。
$N(p,q)$ の表（一部の実例）と零因子の一例.
$\mathbf{Z}_3[\sqrt{2}]$
$(m,n) = (1,0), (2,0), (0,1), (0,2)$.
$\mathbf{Z}_5[\sqrt{3}]$

$(m,n)=(1,0),(2,1),(2,4),(3,1),(3,4),(4,0).$

$\mathbf{Z}_7[\sqrt{5}]$

$(m,n)=(0,2),(0,5),(1,0),(2,3),(2,4),(5,3),(5,4),(6,0).$

$\mathbf{Z}_{11}[\sqrt{7}]$

$(m,n)=(0,50,(0,6),(1,0),(3,3),(3,8),(5,4),(5,7),(6,4),(6,7),$
$(8,3),(8,8),(10,0).$

$\mathbf{Z}_{13}[\sqrt{11}]$

$(1,0),(3,3),(3,10),(4,5),(4,8),(5,1),(12,0),(5,12),(8,1),$
$(8,12),(9,5),(9,8),(10,3),(10,10).$

・$N(p,2)$ に関して

$N(3,2)=4$

$N(5,2)=6$

$N(7,2)=6$　零因子 $1+2\sqrt{2},\ 1+5\sqrt{2},$

$N(11,2)=12$

$N(13,2)=14$

$N(17,2)=16$　零因子 $6+\sqrt{2},\ 6+16\sqrt{2},$

$\vdots$

$N(97,2)=96$　零因子 $13+6\sqrt{2},\ 13+91\sqrt{2},$

・$N(p,3)$ に関して

$N(5,3)=6$

$N(7,3)=8$

$N(11,3)=10,$　零因子 $5+\sqrt{3},\ 5+10\sqrt{3},$

$\vdots$

$N(97,3)=96,$　零因子 $10+\sqrt{3},\ 10+96\sqrt{3},$

・$N(p,5)$ に関して

$N(7,5)=8$

$N(11,5)=10$　零因子 $1+3\sqrt{5},\ 1+8\sqrt{5},$

$\vdots$

$N(97,5)=98,$

・$N(p,7)$ に関して

$N(11,7)=12$

$N(13,7)=14$

$N(17,7)=18$

$N(19,7)=18$　零因子 $3+2\sqrt{7},\ 3+17\sqrt{2},$

$\vdots$

$N(97,7)=98,$

・$N(p,11)$ に関して

$N(13,11)=14,$

$N(17,11)=18,$

$N(19,11)=18$　零因子 $7+\sqrt{11},\ 7+18\sqrt{11}$,

$\vdots$

$N(97,11)=96$,　零因子 $9+5\sqrt{11},\ 9+92\sqrt{11}$.

4　まとめ

Conjecture 1

(判定条件と具体化) p,q が十分小さい時,

$N(p,q)=p+1$　*if* $\mathbf{Z}_p[\sqrt{q}]$ が体.

$N(p,q)=p-1$　*if* $\mathbf{Z}_p[\sqrt{q}]$ が体でない.

以上のことが, 計算機科学の結果より予想されます. つまり $N(p,q)$ によって体を判定することが可能であり. 以下の例にみられますように (m,n) を具体的に求めることが可能です。

注意 2

$\mathbf{Z}_p[\sqrt{q}]$ が体ならば, 零因子を持ちませんから, 零因子を一つでも見つければ体でないことが確かめられます.

$\mathbf{Z}_p[\sqrt{q}]$ の零因子の個数は 0 か 2 個以上いくつ存在するのかそして具体的に求めることが可能です.

(m,n) を具体的に見つける方法は計算機科学の手法が必要と考えますので以下その例を 2 つ挙げておきます。p,q が大きくなると計算するのに手計算では時間が非常にかかると思います。

例 1

$\mathbf{Z}_{83}[\sqrt{2}]$ *(体)* における　(m,n) *satisfying* $m^2-2n^2=1$, (m,n)*:*

$(1,0)$, $(82,0)$, $(13,1)$, $(70,1)$, $(3,2)$, $(80,2)$, $(38,4)$, $(45,4)$, $(36,5)$, $(47,5)$, $(4,7)$, $(79,7)$, $(34,11)$, $(49,11)$, $(17,12)$, $(66,12)$, $(16,13)$, $(67,13)$, $(12,14)$, $(71,14)$, $(6,15)$, $(77,15)$, $(9,17)$, $(74,17)$, $(20,18)$, $(63,18)$, $(15,19)$, $(68,19)$, $(35,23)$, $(48,23)$, $(5,26)$, $(78,26)$, $(31,27)$, $(52,27)$, $(18,28)$, $(65,28)$, $(40,29)$, $(43,29)$, $(41,33)$, $(42,33)$, $(25,35)$, $(58,35)$, $(0,37)$, $(0,46)$, $(25,48)$, $(58,48)$, $(41,50)$, $(42,50)$, $(40,54)$, $(43,54)$, $(18,55)$, $(65,55)$, $(31,56)$, $(52,56)$, $(5,57)$, $(78,57)$, $(35,60)$, $(48,60)$, $(15,64)$, $(68,64)$, $(20,65)$, $(63,65)$, $(9,66)$, $(74,66)$, $(6,68)$, $(77,68)$, $(12,69)$, $(71,69)$, $(16,70)$, $(67,70)$, $(17,71)$, $(66,71)$, $(34,72)$, $(49,72)$, $(4,76)$, $(79,76)$, $(36,78)$, $(47,78)$, $(38,79)$, $(45,79)$, $(3,81)$, $(80,81)$, $(13,82)$, $(70,82)$,

以上 *84* 個です.

$\mathbf{Z}_{97}[\sqrt{3}]$ *(体でない)* における　(m,n) *satisfying* $m^2-3n^2=1$, (m,n)*:*

$(0,41)$, $(0,56)$, $(1,0)$, $(2,1)$, $(2,96)$, $(3,36)$, $(3,61)$, $(5,28)$, $(5,69)$, $(6,23)$, $(6,74)$, $(7,4)$, $(7,93)$, $(10,18)$, $(10,79)$, $(14,29)$, $(14,68)$, $(16,45)$, $(16,52)$, $(17,22)$, $(17,75)$, $(18,25)$, $(18,72)$, $(20,6)$, $(20,91)$, $(22,8)$, $(22,89)$, $(23,46)$, $(23,51)$, $(26,15)$, $(26,82)$, $(27,9)$, $(27,88)$, $(29,38)$, $(29,59)$, $(32,27)$, $(32,70)$, $(34,26)$, $(34,71)$, $(38,44)$, $(38,53)$, $(39,32)$, $(39,65)$, $(40,40)$, $(40,57)$, $(41,47)$, $(41,50)$, $(48,11)$, $(48,86)$, $(49,11)$, $(49,86)$, $(56,47)$, $(56,50)$, $(57,40)$, $(57,57)$, $(58,32)$, $(58,65)$, $(59,44)$, $(59,53)$, $(63,26)$, $(63,71)$, $(65,27)$, $(65,70)$, $(68,38)$, $(68,59)$, $(70,9)$, $(70,88)$, $(71,15)$, $(71,82)$, $(74,46)$, $(74,51)$, $(75,8)$, $(75,89)$, $(77,6)$, $(77,91)$, $(79,25)$, $(79,72)$, $(80,22)$, $(80,75)$, $(81,45)$, $(81,52)$, $(83,29)$, $(83,68)$, $(87,18)$, $(87,79)$, $(90,4)$, $(90,93)$, $(91,23)$, $(91,74)$, $(92,28)$, $(92,69)$, $(94,36)$, $(94,61)$, $(95,1)$, $(95,96)$, $(96,0)$,

以上 *96* 個です.

追記

最近上の定理は数学的にもう少し一般的に証明できましたが, それは又別の機会に述べたいと思います. この様に計算機科学によって数学の数値を具体的に求めることと得られた結果（予想）を基ににして, 数学理論がさらに発展するのではないかと考えています。簡単な計算の結果ですが具体的事柄については計算機科学が役に立つのではないかとここに提供させていただきました。

5　今後の展開

$\mathbf{Z}_p[\sqrt{q}]$ を拡張した

$$A = \mathbf{Z}_p[\sqrt{q}, \sqrt{r}]$$

が 2 次代数であるかどうかの判定条件を考える

A が 2 次代数とは $1, x, x^2, \forall x \in A$ が 1 次従属を意味します。

$m^2 - n^2q - l^2r = 0, 1, 2, \cdot$ をみたす $m + n\sqrt{q} + l\sqrt{r}$ の元たちの具体化とそれをもとにした理論を作ること。

$\mathbf{Z}_7[\sqrt{3}, \sqrt{5}]$, $\mathbf{Z}_{13}[\sqrt{2}, \sqrt{7}]$ $\mathbf{Z}_{17}[\sqrt{3}, \sqrt{7}]$ は 2 次代数の一例です。

また　四元数の変形である標数 p の体上の基底　i, j, k、 ただし $i^2 = j^2 = k^2 = -1$, $ij = k$ をもつ非可換代数 $\mathbf{Z}_p[i, j, k]$　について具体的に正則元、零因子　等を求めるときにも計算機が有用ではないでしょうか。

このように具体例をもとにして予想を立て自己同型群の拡張の実例を計算したいと考えています。非結合的代数系理論への計算機科学からの利用の理論形成のために萌芽的アイデアの側面としてこのような考え方が役にたつのではないかと信じています。

更なる発展として Gell-Mann の Symmetry of Mesons and Baryons　の論文に出現する pseudo octonion algebra の analogous として標数 p の体上で考えそこでの性質を研究したいのでそのための第一歩としてこのような事柄を述べさせていただきました。

最後に　この note を執筆するにあたり筑波大学の増岡彰氏には多大な貴重な有益な advice をいただきました、ここに感謝の言葉を述べたいと思います。

文献については, 簡単な事柄（予備知識をあまり必要としないので）だけを用いましたので, 省略させていただきます.

Acknowledgment

This work was supported by the Research Institute for Mathematical Sciences, a Joint Usage/Research Center located Kyoto University.