Proceedings of the 29th Summer Seminar on Lie Algebras and Related Topics

Held at Osaka Shoin Women's University,
August 23 – 24, 2013

Kashiba, Japan

Preface

The 29th Summer Seminar on Lie Algebras and Related Topics was held at Osaka Shoin Women's University, Sekiya Campus, on August 23 – 24, 2013.

The lectures cover various topics of Lie algebra, algebraic systems and their applications, and the normed spaces. We would like to thank the lecturers for their interesting talks and the preparation of their papers for this proceedings.

Manabu Matsuoka
Yasuyuki Hirano
Fujio Kubo

Contents

Proceedings of Summer Seminar on
Lie Algebras and Related Topics **29** (2013)

"Radical zero" forces a finite dimensional associative algebra to have a unity

Fujio Kubo

Abstract

We have many times faced to the situation in which we have to be careful of the existence of the unity. In this short article, it is not the case for finite dimensional associative algebras with a trivial Jacobson radical. Most of contents of this article are found in the B.Matej [1].

1 $\mathrm{Rad}\, A = 0 \Leftrightarrow A$ is semiprime

Throughout this paper, let $\mathbb{F}$ denote a field and let A be an associative algebra over $\mathbb{F}$.

Let us first remind the notions 'simple", 'semisimple", "prime" and "semiprime".

Definition 1.1 *Let A be an algebra.*

(1) A is simple if A has no notrivial two-sided idel of A and $AA \neq 0$.

(2) A is semisimple if A is a direct sum of simple ideals of A.

(3) A is prime if $aAb = 0$ implies $a = 0$ or $b = 0$.

(4) A is semiprime if $aAa = 0$ implies $a = 0$.

(5) A is of radical zero if A has no nilpotent ideal.

We state the relations among them. Let A be a finite dimensonal associative algebra.

(1) If A is simple then A is prime.

[Why?] Take any nonzero elements $a, b \in A$. Then $\mathbb{F}a + Aa + aA + AaA$ and $\mathbb{F}b + Ab + bA + AbA$ is nonzero ideal of A. We have $A = \mathbb{F}a + Aa + aA + AaA = \mathbb{F}b + Ab + bA + AbA$.Therefore $A = A^3 = (\mathbb{F}a + Aa + aA + AaA)A(\mathbb{F}b + Ab + bA + AbA) = (aA + AaA)(\mathbb{F}b + Ab + bA + AbA) = aAb + aAbA + AaAb + AaAbA$, which implies $aAb \neq 0$.

[Prime $\not\Rightarrow$ Simple] Let $A = \mathbb{F}[x]$ be an algebra of polynomials over $\mathbb{F}$. Then A is prime but not simple.

[When A is finite dimensional, Prime $\Rightarrow$ Simple]

Proposition 1.2 *Let A be an algebra. $RadA = 0$ if and only if A is semiprome*

Proof. Assume that A is semiprime. If I is a nonzero nilpotent with $I^n = 0$ and $I^{n-1} \neq 0$, one can take a nonzero $a \in I$. Then $aAa \subseteq I^{2n-2} \subseteq I^n = 0$. Since A is semiprime, $a = 0$ which is a contradiction. Therefore every nilpotent ideal of A is zero, in other words, $\mathrm{Rad}A = 0$.

Conversely assume that $\mathrm{Rad}A = 0$. Assuming that $aAa = 0$, let $I = ka + Aa + aA$. Since $(AaA)^2 = 0$ one has $AaA = 0$. Hence I is an ideal of A, and $I^3 = 0$. Therefore $I = 0$ and $a = 0$.

2 A nonzero finite dimensional semiprime algebra has a nonzero idempotent

Lemma 2.1 ([1]) *If A is a nonzero finite dimensional semiprime algebra, then there exists a nonzero idempotent $e \in A$ such that eAe is a division algebra.*

Proof. The proof will follow to that in [1] with some extra explanation. Take a nonozero left ideal L of minimal dimension. Let $0 \neq x \in L$. Since A is semiprime, there exist $a \in A$ such that $xax \neq 0$. They put $y = ax \in L$ and say that we have $x, y \in L$such that $xy \neq 0$, which implies that Ly is a nonzero left ideal containd in L. Hence $Ly = L$ and we can find $e \in L$ such that $ey = y$. Let $T = \{z \in L | zy = 0\}$, then $e^2 - e \in T$. Moreover T is a left ideal of A contained strictly in L because $x \notin L$, $T = 0$. Therefore $e^2 = e$ and e is an idempotent in A.

We will next show that eAe is a division algebra. Obviously $e = 1_{eAe}$. We must s how that any nonzero element eae with $a \in A$ has an inverse. We have $0 \neq Aeae \subseteq Ae = L$ and $Aeae = L$. Therefore there exists $b \in A$ such that $beae = e$, and hence $(ebe)(eae) = e^2 = e$. Applying the same argument to ebe, we can find $c \in A$ such that $(ece)(ebe) = e$. Then $ece = (ece)e = (ece)(ebe)(eae) = e(eae) = eae$ and $ebe = (eae)^{-1}$. ∎

3 Subalgebra $\widehat{A} = \{a - ae - ea + eae | a \in A\}$ of A

Let e be a nontrivial idempotent, i.e., $e \neq 1_A$ and $e \neq 0$. Consider the subspace $\widehat{A} = \{a - ae - ea + eae | a \in A\}$ of A and denote by

$$\widehat{a} = a - ae - ea + eae.$$

Then we easily have the following formulas

$$\widehat{a} + \hat{b} = \widehat{a+b} \quad (1)$$
$$\widehat{a}\widehat{b} = \widehat{ab} - \widehat{aeb} \quad (2)$$
$$\widehat{a}e = e\widehat{a} = 0 \quad (3)$$

If $e \in \widehat{A}$ with $e = \widehat{a}\,(a \in A)$, then $e^2 = e\widehat{a} = 0$ by (3), a contradiction. Hence $e \notin \widehat{A}$. Therefore $\widehat{A}$ is a subalgebra by the formulas (1) and (2) such that $e \notin \widehat{A}$.

Lemma 3.1 ([1]) *Let A be a finite dimensional prime algebra and let e be a nontrivial idempotent in A. Then $\widehat{A}$ is a prime algebra with $e \notin \widehat{A}$.*

Proof. The proof will also follow to that in [1] with some extra explanation.

(1) We first state a simple formula

$$(a - ae)b(c - ec) = \widehat{a}\widehat{b}\widehat{c}. \tag{4}$$

(2) We next prove that $\widehat{A} \neq 0$. Assume that $\widehat{A} = 0$. Then $(a-ae)A(c-ec) = 0$ for all $a, c \in A$ by (4). If there exits an $a \in A$ such that $a - ae \neq 0$, then by the primeness of A, one has $c - ec = 0$ for any $c \in A$. Hence

$$0 = a(c - ec) = (a - ae)c, \text{ and therefore, } (a - ae)A = 0.$$

The last equation leads to $(a-ae)A(a-ae) = 0$, which contradicts to $a-ae \neq 0$. Hence $\widehat{A} \neq 0$.

(3) The primeness of $\widehat{A}$ follows from the equation

$$\widehat{a}\widehat{b}\widehat{c} = \widehat{\widehat{a}\widehat{b}\widehat{c}}, \tag{5}$$

which is easily proved by $\widehat{a}(b - \widehat{b})\widehat{c} \in \widehat{a}(eA + Ae)\widehat{c}$ and (3). ∎

Lemma 3.2 **([1])** *Let A be a finite dimensional prime algebra and e be a nontrivial idempotent in A. If $\widehat{A}$ has a unity $1_{\widehat{A}}$, then A has a unity.*

Proof. Write $1_{\widehat{A}} = \widehat{f}$ for some $f \in A$. We shall prove that $e + \widehat{f}$ is a unity of A. Let a be any element of A. Since $\widehat{f}a\widehat{f} = \widehat{f}\widehat{a}\widehat{f}$ by (5), $\widehat{f}a\widehat{f} = \widehat{f}\widehat{a}\widehat{f} = 1_{\widehat{A}}\widehat{a}\widehat{f} = \widehat{a}\widehat{f} = (a-ae-ea+eae)\widehat{f} = (a-ea)\widehat{f}$ by (3). Hence $((e+\widehat{f})a-a)\widehat{f} = 0$ for any $a \in A$. Inserting $b \in A$ into the left, we have $((e + \widehat{f})a - a)b\widehat{f} = ((e + \widehat{f})ab - ab)\widehat{f} = 0$ and then $((e + \widehat{f})a - a)A\widehat{f} = 0$ which implies $(e + \widehat{f})a - a = 0$. Similarly we have $a(e + \widehat{f}) = a$. ∎

Theorem 3.3 *A nonzero finite dimensional prime algebra necessarily has a unity.*

Proof. We proceed by induction on $N = \dim_{\mathbb{F}} A$. As for the case $N = 1$, let $A = \mathbb{F}a$ $(a \in A)$ and $aa = \lambda a$ $(\lambda \neq 0)$. Then A has a unity $(1/\lambda)a$.

Let $N > 1$. A has a nonzero idempotent e by Lemma 2.1. If e is a unity of A, then we have done. If e is a nontrivial idempotent, then $\widehat{A}$ is a prime sugalgebra of A with $e \notin \widehat{A}$ (hence $\dim_{\mathbb{F}} \widehat{A} < N$) by Lemma 3.1. By induction hypothesis $\widehat{A}$ has a unity $1_{\widehat{A}}$. Therefore A has a unity by Lemma 3.2. ∎

4 A nonzero finite dimensional semiprime algebra has a unity

Theorem 4.1 *A nonzero finite dimensional semiprime algebra necessarily has a unity.*

Proof. Let A be a nonzero finite dimensional semiprime algebra. If A is prime, then A has a unity by Theorem 3.3. Assume that A is not prime. Let a, b be nonzero elements in A such that $aAb = 0$. Consider the subspace

$$I = \{x \in A | aAx = 0\} \neq 0.$$

Since $aA(AI) = aA(IA) = 0$, I is a ideal of A. Furthermore I is semiprime. In fact, if $x \in I$ satisfies that $xIx = 0$, then for any $y \in A$ we have $(xyx)A(xyx) \subseteq xIx = 0$ and then $xAx = 0$. This implies $x = 0$, which shows that I is semiprime. By the induction hypothesis I has a unity 1_I.

We next consider a "correspoinding" subspace

$$J = \{z - 1_I z | z \in A\}.$$

Let us show that 1) J is an ideal of A, 2) J is prime, 3) $A = I + J$ and 4) $I \cap J = 0$ as follows. 1): We use a simple formura $1_I z = z 1_I$ $(z \in A)$ which follows from $1_I z = (1_I z)1_I = 1_I(z 1_I) = z 1_I \cdots (\sharp)$. For $z - 1_I z \in J$ and $w \in A$, we have $(z - 1_I z)w = zw - 1_I(zw) \in J$ and $w(z - 1_I z) = wz - w(1_I z) = wz - (w 1_I)z = wz - (1_I w)z \in J$ by $(\sharp)$, which shows that J is an ideal of A. 2) It follows from the formula

$$(z - 1_I z)(w - 1_I w)(z - 1_I z) = (z - 1_I z)w(z - 1_I z)$$

$(z, w \in A)$ that $(z - 1_I z)J(z - 1_I z) = 0$ implies that $(z - 1_I z)A(z - 1_I z) = 0$ and $z - 1_I z = 0$. 3) follows from $z = 1_I z + z - 1_I z$ $(z \in A)$. 4): Take $z \in I \cap J$ and write $z = u - 1_I u$ $(u \in A)$. Then $z = 1_I z = 1_I u - 1_I(1_I u) = 0$.

By induction hypothesis, we have a unity 1_J of J. It is now easy to verify that $1_I + 1_J$ is a unity of $A = I + J$. ∎

References

[1] B.Matej, An elementary approach to Wedderburn's structure theory, Expo. Math.28(2010)79-83

Proceedings of Summer Seminar on
Lie Algebras and Related Topics **29** (2013)

加群の自己同型群と導分環

首藤 武史

1. 初めに

[2] で講演者は次のことを示している：代数的閉体 k 上の有限次元多元環 A の根基 R が 2-nilpotent のとき，A の自己同型群 $\mathrm{Aut}(A)$ のリー環 $\mathrm{L}(\mathrm{Aut}(A))$ は A の R を保つ導分全体のなすリー環 $\mathrm{der}(A)$ に一致する．その証明の方法は，以下に述べる性質をもつ R の 1 次変換のなす幾つかの空間の次元を調べるというものである．

$A=S+R$ を A の Wedderburn 分解とする．S は A の Wedderburn factor (A の半単純部分多元環) である．S および R の基底を併せて A の基底を構成するとき，A の自己同型 σ の表現行列は次のようになる：

$$\sigma=\begin{pmatrix}\alpha & 0\\ \delta & \gamma\end{pmatrix}$$

$\sigma\in\mathrm{Aut}(A)$ ということから，$\alpha\in\mathrm{Aut}(S)$ で，δ，γ は次の等式をみたす：

(1) $x,y\in S$ に対して，$\delta(xy)=\alpha(x)\delta(y)+\delta(x)\alpha(y)$,

(2) $\gamma\in\mathrm{GL}(R)$で，$x\in S$，$u\in R$ に対して，$\gamma(xu)=\alpha(x)\gamma(u)$，$\gamma(ux)=\gamma(u)\alpha(x)$.

A の導分 D で R を保つものも同様に

$$D=\begin{pmatrix}d & 0\\ \delta & \Delta\end{pmatrix}$$

と表すことができる．このとき，$d\in\mathrm{Der}(S)$ で，δ，Δ は次の等式をみたす：

(3) $x,y\in S$ に対して，$\delta(xy)=x\delta(y)+\delta(x)y$,

(4) $x\in S$，$u\in R$ に対して，$\Delta(xu)=x\Delta(u)+d(x)u$，$\Delta(ux)=\Delta(u)x+ud(x)$.

R は S-S 両側加群で，(1)～(4) はその上の作用であるが，S の包絡環 $S^e=S\otimes S^o$ を考えると，これらはすべて左 S^e 加群上の作用で表される．これらを一般化して考える．

2. α 自己同型と d 導分

k を任意の体，A を k 上の有限次元多元環，M を左 A 加群とする．$\alpha\in\mathrm{Aut}(A)$ に対して M に新しい A 加群の構造が決まる：

$$x \in A,\ m \in M \text{ に対して, } x \cdot m = \alpha(x)m$$

このようにして決まる A 加群を M^{α} で表す．単に M と書くときは初めに与えられた A 加群を表す．すなわち，$M^{id}=M$ である．

M の正則な 1 次変換 γ が M から M^{α} への A 加群としての同型であるとき，これを M の **α 自己同型**と呼ぶ．すなわち，任意の $x \in A$, $m \in M$ に対して，

$$\gamma(xm)=\alpha(x)\gamma(m)$$

が成り立つこと． 従って，§1, (2) は γ が S 加群 R の α 自己同型であることを示している．

A の導分 d に対して，M の 1 次変換 δ が，$x \in A$, $m \in M$ に対して

$$\delta(xm)=d(x)m+x\delta(m)$$

を満たすとき，δ を M の ***d* 導分**と呼ぶ．従って，§1, (4) は Δ が R の d 導分であることを示している．

命題 1． M は忠実な A 加群とする．したがって $A \subset \mathrm{E}(M)$ とみなす．

(1) γ が M の α 自己同型であれば，$\alpha(x)=\gamma x\gamma^{-1}$ $(x \in A)$.

(2) δ が M の d 導分であれば，$d(x)=[\delta, x]\,(=\delta x - x\delta)$ $(x \in A)$.

3. Normalizers, Centralizers

命題 1 は A のある種の自己同型 [resp. 導分] が $\mathrm{E}(M)$ の内部自己同型 [resp. 内部導分] から引き起こされることを示している．そこで A の‘正規化’を考える．

M を有限次元ベクトル空間とし，$G=\mathrm{GL}(M)$, $\mathfrak{g}=\mathfrak{gl}(M)$ とする．部分多元環 $A \subset \mathrm{E}(M)$ に対して，

$$\mathrm{N}_G(A)=\{\gamma \in G \mid \gamma A \gamma^{-1}=A\},$$

$$\mathfrak{n}_{\mathfrak{g}}(A)=\{\delta \in \mathfrak{g} \mid [\delta, A] \subset A\}$$

とおく．このとき，命題 1 より群の準同型 ω およびリー環の準同型 ω_* を得る：

$$\omega : \mathrm{N}_G(A) \longrightarrow \mathrm{Aut}(A),\quad \gamma \mapsto \mathrm{Int}(\gamma)|_A,$$

$$\omega_* : \mathfrak{n}_{\mathfrak{g}}(A) \longrightarrow \mathrm{Der}(A),\quad \delta \mapsto \mathrm{int}(\delta)|_A$$

これらの像，核をそれぞれ $\mathrm{Aut}(A; M)$, $\mathrm{C}_G(A)$, $\mathrm{Der}(A; M)$, $\mathfrak{c}_{\mathfrak{g}}(A)$ とおく．従って次の完全系列を得る：

(A) $$1 \longrightarrow \mathrm{C}_G(A) \longrightarrow \mathrm{N}_G(A) \xrightarrow{\omega} \mathrm{Aut}(A; M) \longrightarrow 1$$

(B) $$0 \longrightarrow \mathfrak{c}_\mathfrak{g}(A) \longrightarrow \mathfrak{n}_\mathfrak{g}(A) \xrightarrow{\omega_*} \mathrm{Der}(A; M) \longrightarrow 0.$$

$\mathrm{Aut}(A; M)$，$\mathrm{Der}(A; M)$ に関して，次のことが分かる．

命題 2. M が A の (左) 正則表現のとき，$\mathrm{Aut}(A; M) = \mathrm{Aut}(A)$，$\mathrm{Der}(A; M) = \mathrm{Der}(A)$．従って，$A$ の自己同型はすべて $\mathrm{E}(A)$ の内部自己同型から引き起こされ，A の導分はすべて $\mathrm{E}(A)$ の内部導分から引き起こされる．

例 3. A が 1 つのべき零元から生成されているとする．このとき，任意の (忠実な) A 加群 M に対して $\mathrm{Aut}(A; M) = \mathrm{Aut}(A)$ が成り立つ．しかし，$\mathrm{Der}(A; M) = \mathrm{Der}(A)$ は成り立たない場合がある．

H を $\mathrm{Aut}(A; M)$ の部分群とし，$\Gamma(H) = \omega^{-1}(H)$ とおけば，次の系列は群の完全系列である：

(a) $$1 \longrightarrow \mathrm{C}_G(A) \longrightarrow \Gamma(H) \xrightarrow{\omega} H \longrightarrow 1.$$

L を $\mathrm{Der}(A; M)$ の部分リー環とし，$\Delta(L) = \omega_*^{-1}(L)$ とおけば，リー環の完全系列を得る：

(b) $$0 \longrightarrow \mathfrak{c}_\mathfrak{g}(A) \longrightarrow \Delta(L) \xrightarrow{\omega_*} L \longrightarrow 0.$$

4. 代数群とリー環

この節では基礎体は代数的閉体とする．このとき，系列 (A) は代数群と準同型の完全系列である．また，H が $\mathrm{Aut}(A; M)$ の閉部分群のとき，系列 (a) も代数群と準同型の完全系列である．リー環と準同型の微分を考えると次のリー環の完全系列を得る：

(C') $$0 \longrightarrow \mathrm{L}(\mathrm{C}_G(A)) \longrightarrow \mathrm{L}(\mathrm{N}_G(A)) \xrightarrow{d\omega} \mathrm{L}(\mathrm{Aut}(A; M))$$

(c') $$0 \longrightarrow \mathrm{L}(\mathrm{C}_G(A)) \longrightarrow \mathrm{L}(\Gamma(H)) \xrightarrow{d\omega} \mathrm{L}(H)$$

(c') における $d\omega$ は (C) での $d\omega$ の $\mathrm{L}(\Gamma(H))$ への制限写像である．

代数群の表現の一般論より $\mathrm{L}(\mathrm{N}_G(A)) \subset \mathfrak{n}_{\mathfrak{g}}(A)$ で，$d\omega$ は ω_*の $\mathrm{L}(\mathrm{N}_G(A))$ への制限写像である．

Remark. 基礎体の標数が 0 の場合には $\mathrm{N}_G(A)$ のリー環は $\mathfrak{n}_{\mathfrak{g}}(A)$ であることが分かる([1]，§13)．この場合には，$\mathrm{L}(\mathrm{Aut}(A; M)) = \mathrm{Der}(A: M)$ が成り立つ．正標数の場合には一般に成り立たない．

例 4. 基礎体 k の標数は 3 であるとする．$A = k[X]/(X^3) = k[x]$ を考える．A の正則表現は忠実で，$1, x, x^2$ を基底に選ぶと，x, x^2 の表現行列はそれぞれ

$$x \mapsto \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad x^2 \mapsto \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

である. 正規化群 $\mathrm{N}_G(A)$ および中心化群 $\mathrm{C}_G(A)$ を計算すると, $\dim \mathrm{N}_G(A) = 5$, $\dim \mathrm{C}_G(A) = 3$ を得る．

一方，正規化環 $\mathfrak{n}_{\mathfrak{g}}(A)$，中心化環 $\mathfrak{c}_{\mathfrak{g}}(A)$ は $\dim \mathfrak{n}_{\mathfrak{g}}(A) = 6$，$\dim \mathfrak{c}_{\mathfrak{g}}(A) = 3$.
$\dim \mathrm{L}(\mathrm{N}_G(A)) = 5$ であるから，

$$\mathrm{L}(\mathrm{N}_G(A)) \subsetneq \mathfrak{n}_{\mathfrak{g}}(A)$$

となっている．

命題 5. $\mathfrak{c}_{\mathfrak{g}}(A)$ は $\mathrm{E}(M)$ の部分多元環で，この可逆元全体のなす群が $\mathrm{C}_G(A)$ である．とくに，$\mathrm{L}(\mathrm{C}_G(A)) = \mathfrak{c}_{\mathfrak{g}}(A)$.

(a) の完全性より，$\mathrm{C}_G(A) = \mathrm{Ker}\, \omega$，$\mathfrak{c}_{\mathfrak{g}}(A) = \mathrm{Ker}\, \omega_*$ であるから ω は分離的で，従って (c') での $d\omega$ は surjective である．とくに，(C') における $d\omega$ も surjective である．

これまでに得られた 6 個の完全系列を再掲する：

$$\begin{array}{lccccc}
\text{(A)} & 1 \longrightarrow \mathrm{C}_G(A) \longrightarrow & \mathrm{N}_G(A) & \xrightarrow{\omega} & \mathrm{Aut}(A; M) \longrightarrow 1 \\
\text{(B)} & 0 \longrightarrow \mathfrak{c}_{\mathfrak{g}}(A) \longrightarrow & \mathfrak{n}_{\mathfrak{g}}(A) & \xrightarrow{\omega_*} & \mathrm{Der}(A; M) \longrightarrow 0. \\
 & \qquad \| & \cup & & \cup \\
\text{(C)} & 0 \longrightarrow \mathrm{L}(\mathrm{C}_G(A)) \longrightarrow & \mathrm{L}(\mathrm{N}_G(A)) & \xrightarrow{d\omega} & \mathrm{L}(\mathrm{Aut}(A; M)) \longrightarrow 1
\end{array}$$

(a) $$1 \longrightarrow C_G(A) \longrightarrow \Gamma(H) \xrightarrow{\omega} H \longrightarrow 1.$$

(b) $$0 \longrightarrow \mathfrak{c}_{\mathfrak{g}}(A) \longrightarrow \Delta(L) \xrightarrow{\omega_*} L \longrightarrow 0.$$

(c) $$0 \longrightarrow \mathrm{L}(C_G(A)) \longrightarrow \mathrm{L}(\Gamma(H)) \xrightarrow{d\omega} \mathrm{L}(H) \longrightarrow 0$$

定理 6. H を $\mathrm{Aut}(A\colon M)$ の閉部分群，L を $\mathrm{Der}(A\colon M)$ の部分リー環とする．このとき，$\mathrm{L}(\Gamma(H)) = \Delta(L)$ であるための必要十分条件は $L = \mathrm{L}(H)$ であることである．

系 7. A の自己同型群 $\mathrm{Aut}(A)$ が連結であるための必要十分条件は，A を正則表現によって $\mathrm{E}(A)$ の部分多元環とみなすとき，$\mathrm{GL}(A)$ における $A^{\times}$ の正規化群が連結であることである．

参考文献

[1] Humphreys, J.E. : Linear Algebraic Groups, GTM **21**, Springer-Verlag, 1975.

[2] 首藤武史：Radical が 2-nilpotent である多元環の自己同型群と導分環，preprint.

Proceedings of Summer Seminar on
Lie Algebras and Related Topics **29** (2013)

Reflection spaces of an abelian group

Iwate University
Yoji Yoshii

We introduce a *reflection space* of an abelian group, which is a generalization of a subgroup.

Let $G = (G, +, 0)$ be an abelian group.

Definition 1 A subset E of G is called a **refection space** of G if

$$2x - y \in E \qquad (\text{or} \quad 2E - E \subset E) \tag{1}$$

for all $x, y \in E$. On the other hand, E is called a **symmetric reflection space** of G if

$$x - 2y \in E \qquad (\text{or} \quad E - 2E \subset E) \tag{2}$$

for all $x, y \in E$. Also, we say that E is **pointed** if $0 \in E$.

(See [LN], [NY], [Y1], [Y2] and [Y3]. In some references a symmetric reflection space is simply called a reflection space.)

For example, if $G = \mathbb{Z}$, then a symmetric reflection space of $\mathbb{Z}$ is just $m\mathbb{Z}$ or $m(2\mathbb{Z}+1)$. On the other hand, $m\mathbb{Z} + e$ for any $m, e \in \mathbb{Z}$ is a reflection space. In particular, any singleton $\{e\}$ is a reflection space.

Lemma 1 *Let E be a symmetric reflection space of G. Then $-E = E$.*
Hence $E + 2E \subset E$ and $2E - E \subset E$. Thus a symmetric reflection space is a reflection space.

Proof) For $x \in E$, we have $x - 2x = -x \in E$. Hence $-E \subset E$. Thus $E \subset -E$. □

Lemma 2 *Let E be a reflection space of G. Then*

$$E \textit{ is pointed} \Longrightarrow E \textit{ is a symmetric reflection space.}$$

Hence, a pointed reflection space is a pointed symmetric reflection space.

Proof) Since $0 \in E$, we get $-E \subset E$. Hence $E - 2E = -(2E - E) \subset E$. $\square$

Lemma 3 *Let E be a reflection space of G. Then $E - e$ for any $e \in E$ is a pointed reflection space.*

Proof) We have $2(E - e) - (E - e) = (2E - E) - e \subset E - e$, and so E is a reflection space. It is clear that $0 \in E - e$. $\square$

Lemma 4 *Let E be a subset of G. For any $e, e' \in E$, we have*

$$\langle E - e \rangle = \langle E - e' \rangle,$$

where the bracket $\langle A \rangle$ means the subgroup generated by a subset A of G.

Proof) For $x \in E$, we have $x - e, e' - e \in E - e$. Hence $x - e' = x - e - (e' - e) \in \langle E - e \rangle$, and so $\langle E - e' \rangle \subset \langle E - e \rangle$. Similarly, we have $\langle E - e \rangle \subset \langle E - e' \rangle$. $\square$

Lemma 5 *Let E be a pointed reflection space of G, and let $e \in E$. Then $\langle e \rangle \subset E$.*

Proof) Since $0 \in E$ (so E is symmetric), we have $\pm 2e = 0 \pm 2e \in E$ and $\pm 3e = \pm(e + 2e) \in E$. Similarly, we have $2me = 0 \pm (2e + \cdots + 2e) \in E$ and $(2m+1)e = e \pm (2e + \cdots + 2e) \in E$ for all $m \in \mathbb{Z}$. $\square$

More generally, we have:

Lemma 6 *Let E be a symmetric reflection space of G. Suppose that $\{e_i\}_{i \in \mathfrak{I}} \subset E$, where $\mathfrak{I}$ is any index set. Then $E + 2\langle e_i \rangle_{i \in \mathfrak{I}} \subset E$. Hence, $E + 2\langle E \rangle = E$.*

Proof) Let $x \in E + 2\langle e_i \rangle_{i \in \mathfrak{I}}$. Then $x = e + 2\sum_{j=1}^{n} \epsilon_j e_{i_j}$, where $\epsilon_j = 1$ or -1, and $e_{i_j} \in \{e_i\}_{i \in \mathfrak{I}}$. Thus $x = e + 2\epsilon_1 e_{i_1} + \cdots + 2\epsilon_n e_{i_n} \in E$, inductively. (Note that $-e_{i_j} \in E$ by Lemma 1). $\square$

Let us classify reflection spaces.

Proposition 1 *Let E be a subset of G. Then*

$$E \text{ is a symmetric reflection space} \iff E = \bigcup_{i=1}^{m} (2\langle E \rangle + e_i) \tag{3}$$

for some $1 \leq m \leq |\langle E \rangle / 2\langle E \rangle|$ and some $e_i \in E$, and if E is pointed, then some $e_i = 0$.

Moreover,

$$E \text{ is a reflection space} \iff E = \bigcup_{i=1}^{m} (2\langle E - e \rangle + x_i) \tag{4}$$

for any $e \in G$ (see Lemma 4), and some $x_i \in E$ and $1 \leq m \leq |\langle E - e \rangle / 2\langle E - e \rangle|$.

Proof) For (3), ($\Longleftarrow$) is clear. For the other implication, E contains $2\langle E\rangle$ by Lemma 6. Thus E is a union of cosets in $\langle E\rangle/2\langle E\rangle$.

For (4), ($\Longleftarrow$) is clear. For the other implication, note that $E-e$ for $e\in E$ is a pointed reflection space, by Lemma 3. Hence by (3), we have

$$E-e=\bigcup_{i=1}^{m}(2\langle E-e\rangle+g_i),$$

where $g_i\in E-e$. So letting $x_i:=g_i+e$, we obtain (4). $\square$

Example 1 A union of cosets in $(m_1\mathbb{Z}\times m_2\mathbb{Z})/(2m_1\mathbb{Z}\times 2m_2\mathbb{Z})$ plus some $(e_1,e_2)\in\mathbb{Z}^2$ for $m_1,m_2\in\mathbb{Z}$ is an example of reflection spaces of $\mathbb{Z}^2$. In particular, $(m_1\mathbb{Z}+e_1)\times(m_2\mathbb{Z}+e_2)$ is a reflection space of $\mathbb{Z}^2$.

Where can we find reflection spaces?

Let us recall *extended affine root systems.*

Definition 2 Let V be a finite-dimensional vector space over $\mathbb{Q}$ with a positive semidefinite symmetric bilinear form $(\cdot,\cdot)$. A subset $\mathfrak{R}$ of V is called an **extended affine root system** if $\mathfrak{R}$ satisfies the following:

(A1) $(\alpha,\alpha)\neq 0$ for all $\alpha\in\mathfrak{R}$, and $\mathfrak{R}$ spans V;

(A2) $\langle\alpha,\beta\rangle\in\mathbb{Z}$ for all $\alpha,\beta\in\mathfrak{R}$, where $\langle\alpha,\beta\rangle=\frac{2(\alpha,\beta)}{(\beta,\beta)}$;

(A3) $\sigma_\alpha(\beta)\in\mathfrak{R}$ for all $\alpha,\beta\in\mathfrak{R}$, where $\sigma_\alpha(\beta)=\beta-\langle\beta,\alpha\rangle\alpha$;

(A4) $\mathfrak{R}=\mathfrak{R}_1\cup\mathfrak{R}_2$ and $(\mathfrak{R}_1,\mathfrak{R}_2)=0$ imply $\mathfrak{R}_1=\emptyset$ or $\mathfrak{R}_2=\emptyset$ (irreducibillity)

(see [MY] and [Y2]).

One can show that if $(\cdot,\cdot)$ is positive definite, then $\mathfrak{R}$ is a **finite irreducible root system** (see [MY]).

Let

$$V^0:=\{x\in V\mid (x,y)=0 \text{ for all } y\in V\}$$

be the radical of the form, and

$$^{-}:V\longrightarrow V/V^0$$

the canonical surjection. Note that $\overline{\mathfrak{R}}$ is a finite irreducible root system.

For $\bar\alpha\in\overline{\mathfrak{R}}$, let $\dot\alpha\in V$ be an inverse image of $\bar\alpha$, i.e., $\overline{\dot\alpha}=\bar\alpha$. Let

$$S_{\dot\alpha}:=\{s\in V^0\mid \dot\alpha+s\in\mathfrak{R}\}.$$

Then we have

$$\sigma_{\dot\alpha+s}(\dot\alpha+s)=\dot\alpha+s-\langle\dot\alpha+s,\dot\alpha+s\rangle(\dot\alpha+s)=-\dot\alpha-s\in\mathfrak{R}.$$

Thus $-s \in S_{-\dot{\alpha}}$, and so $-S_{\dot{\alpha}} \subset S_{-\dot{\alpha}}$. Similarly, we have $-S_{-\dot{\alpha}} \subset S_{\dot{\alpha}}$, and hence

$$-S_{\dot{\alpha}} = S_{-\dot{\alpha}}. \tag{5}$$

Also, we have

$$\sigma_{\dot{\alpha}+t}(\dot{\alpha}+s) = \dot{\alpha}+s - \langle \dot{\alpha}+s, \dot{\alpha}+t\rangle(\dot{\alpha}+t) = -\dot{\alpha}+s-2t \in \mathfrak{R},$$

and hence $s - 2t \in S_{-\dot{\alpha}}$ for all $s, t \in S_{\dot{\alpha}}$. Thus $S_{\dot{\alpha}} - 2S_{\dot{\alpha}} \subset S_{-\dot{\alpha}}$, and by (5), we get

$$2S_{\dot{\alpha}} - S_{\dot{\alpha}} \subset S_{\dot{\alpha}},$$

for all $\alpha \in \mathfrak{R}$. Thus, $S_{\dot{\alpha}}$ is a reflection space of V^0. We note that if we take $\dot{\alpha} \in \mathfrak{R}$, e.g. $\dot{\alpha} = \alpha$, then $0 \in S_{\dot{\alpha}}$, and so $S_{\dot{\alpha}}$ is a pointed reflection space (see Lemma 2).

Reflection spaces are important not only for root systems but also for Lie algebras. Let us give one simple example. Let F be a field of characteristic $\neq 2$.

Let $\{e, f, h\}$ be a standard basis of the Lie algebra $\mathrm{sl}_2(F)$ so that $[e, f] = h$, $[h, e] = 2e$ and $[h, f] = -2f$, having the root system $\{\pm\alpha\}$ relative to Fh, i.e., α is the linear form of Fh such that $\alpha(h) = 2$. Let

$$L := \mathrm{sl}_2(F[t^{\pm 1}]) = \mathrm{sl}_2(F) \otimes F[t^{\pm 1}]$$

be the loop algebra, which is a $(\mathbb{Z}\alpha \times \mathbb{Z})$-graded Lie algebra, defining

$$L_\alpha^n = Fe \otimes t^n, \quad L_{-\alpha}^n = Ff \otimes t^n \quad \text{and} \quad L_0^n = Fh \otimes t^n$$

for all $n \in \mathbb{Z}$, and all the other homogeneous spaces are 0, i.e., $L_{k\alpha}^n = 0$ for $k \neq \pm 1, 0$. Let

$$M := (e \otimes t^r F[t^{\pm p}]) \oplus (f \otimes t^{-r} F[t^{\pm p}]) \oplus (h \otimes F[t^{\pm p}])$$

be the homogeneous subalgebra of L generated by $e \otimes t^r$, $f \otimes t^{-r}$ and $h \otimes t^{\pm p}$ for $p, r \in \mathbb{Z}$. Let

$$S_{\pm\alpha} := \mathrm{supp}_{\pm\alpha} M = \{n \in \mathbb{Z} \mid M \cap L_{\pm\alpha}^n \neq 0\}$$

be subsets of $\mathbb{Z}$. For $m, k \in S_\alpha$, since

$$[e \otimes t^m, [e \otimes t^m, f \otimes t^{-k}]] \neq 0,$$

we have $2m - k \in S_\alpha$. Thus S_α is a reflection space of $\mathbb{Z}$. Similarly, $S_{-\alpha}$ is a reflection space of $\mathbb{Z}$. Moreover, one can easily see that

$$S_\alpha = p\mathbb{Z} + r \quad \text{and} \quad S_{-\alpha} = p\mathbb{Z} - r.$$

Thus reflection spaces naturally appear in supports of graded subalgebras of a loop algebra (see [Y3] for more general examples).

References

[A] S. Azam, *Extended affine root systems*, J. Lie Theory, no. 2, **12** (2002), 515–527.

[A-P] B. Allison, S. Azam, S. Berman, Y. Gao and A. Pianzola, *Extended affine Lie algebras and their root systems*, Mem. Amer. Math. Soc. 126 (1997), no. 603.

[AF] B. Allison and J. Faulkner, *Isotopy for extended affine Lie algebras and Lie tori*, Prog. Math., **288** (2008), 3-43.

[LN] O. Loos, E. Neher, *Reflections systems and partial root systems*, Forum Math., Vol 23(2), 349–411 (2011).

[M] M. Macdonald, *Affine root systems and Dedekind's η-functions*, J. Invent. Math., **15** (1972), 91–143.

[MY] J. Morita and Y. Yoshii, *Locally extended affine Lie algebras*, J. Algebra 301 (2006), 59–81.

[N] K. Naoi, *Multiloop Lie algebras and the construction of extended affine Lie algebras*, J. Algebra 323 (2010), 2103–2129.

[NY] E. Neher, Y. Yoshii, *Derivations and invariant forms of alternative or Jordan G-tori* Trans. Amer. Math. Soc. **355**(3) (2002), 1079–1108.

[S] K. Saito, *Extended affine root systems 1 (Coxeter transformations)*, RIMS., Kyoto Uviv. **21** (1985), 75–179.

[Y1] Y. Yoshii, *Root systems extended by an abelian group and their Lie algebras*, J. Lie Theory **14(2)** (2004), 371–394.

[Y2] Y. Yoshii, *Locally extended affine root systems*, Proc. on Quantum Affine Algebras, Extended Affine Lie Algebras and Applications, Contemp. Math., **508** (2010), 285–302.

[Y3] Y. Yoshii, *General Lie tori from Naoi tori*, preprint.

Proceedings of Summer Seminar on
Lie Algebras and Related Topics **29** (2013)

ノルム空間のある幾何的定数

池田敏春（九州工業大学大学院工学研究院）

ノルム空間 X の幾何的定数のなかでも von Neumann-Jordan 定数 $C_{\mathrm{NJ}}(X)$ および James 定数 $J(X)$ は最もよく知られ広く取り扱われている．これらを簡単に紹介するとともに最近得られた結果をいくつか述べる．

1 Absolute normalized ノルムと凸関数

$\mathbb{K}$ は実数体 $\mathbb{R}$ または複素数体 $\mathbb{C}$ とする．

Definition 1. $\mathbb{K}^n$ 上のノルム $\|\cdot\|$ が *absolute normalized* であるとは

(AN1) $\|(x_1, x_2, \cdots, x_n)\| = \|(|x_1|, |x_2|, \cdots, |x_n|)\| \qquad (x_i \in \mathbb{K})$,

(AN2) $\|e_1\| = \|e_2\| = \cdots = \|e_n\| = 1$

を満たすときをいい，その全体を $\mathcal{AN}_n$ で表す．

Example 1. 次の ℓ_p ノルム $\|\cdot\|_p$ $(1 \le p \le \infty)$

$$\|(x_1, \cdots, x_n)\|_p = \begin{cases} \left(\sum_{i=1}^n |x_i|^p\right)^{1/p} & (1 \le p < \infty), \\ \max\{|x_1|, \cdots, |x_n|\} & (p = \infty) \end{cases}$$

は absolute normalized ノルムであり，任意の $\|\cdot\| \in \mathcal{AN}_n$ に対して

$$\|\cdot\|_\infty \le \|\cdot\| \le \|\cdot\|_1$$

が成り立っている．

いま

$$\Delta_n = \left\{ s = (s_1, \cdots, s_{n-1}) \in \mathbb{R}^{n-1} \,:\, \sum_{j=1}^{n-1} s_j \le 1,\ \ s_j \ge 0\ (1 \le j \le n-1) \right\}$$

とし，次の $(A_0), (A_1), \cdots, (A_n)$ を満たす Δ_n 上の 連続凸関数 ψ の全体を Ψ_n で表す．

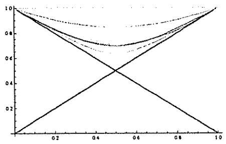
(A_0) $\psi(o) = \psi(e_1) = \cdots = \psi(e_{n-1}) = 1,$

(A_j) $\psi(s) \geq \left(1 - s_j\right)\psi\left(\dfrac{1}{1-s_j}(s_1, \cdots, \underset{j}{0}, \cdots, s_{n-1})\right)$ $(s \neq e_j;\ j = 1, \cdots, n-1),$

(A_n) $\psi(s) \geq \left(\sum_{j=1}^{n-1} s_j\right)\psi\left(\dfrac{1}{\sum_{j=1}^{n-1} s_j} s\right)$ $(s \neq o).$

とくに，$n = 2$ のときは，$\Delta_2 = [0, 1]$ であり，Ψ_2 の凸関数 ψ の条件は

$$\max\{1-t,\ t\} \leq \psi(t) \leq 1$$



となる．

次に，$\psi \in \Psi_n$ に対して $\mathbb{K}^n$ 上のノルム $\|\cdot\|_\psi$ を

$$\|(x_1, \cdots, x_n)\|_\psi = \begin{cases} \left(\sum_{j=1}^{n} |x_j|\right)\psi\left(\dfrac{1}{\sum_{j=1}^{n}|x_j|}(|x_2|, \cdots, |x_n|)\right) & (x \neq o), \\ 0 & (x = o) \end{cases}$$

により定義すると absolute normalized ノルムになり，この対応

$$\Psi_n \ni \psi \longleftrightarrow \|\cdot\|_\psi \in \mathcal{AN}_n$$

は全単射になっている．ℓ^2 ノルム $\|\cdot\|_2$ に対応する関数 ψ_2 は

$$\psi_2(x_1, \cdots, x_{n-1}) = \sqrt{2\sum_{j=1}^{n-1}(x_j^2 - x_j) + 2\sum_{i<j} x_i x_j + 1}$$

であり，$n = 2$ のとき，$\psi_2(t) = \sqrt{2t^2 - 2t + 1}$ である．

2 von Neumann-Jordan 定数

P. Jordan と J. von Neumann はノルム空間が内積空間であることを中線定理の成立することで特徴づけた．これに関連して J.A. Clarkson は次のような定数を導入した．

Definition 2. ノルム空間 X において

$$C_{\mathrm{NJ}}(X) = \sup\left\{\frac{\|x+y\|^2 + \|x-y\|^2}{2\left(\|x\|^2 + \|y\|^2\right)} \ :\ x, y \in X,\ \text{not both } o\right\}$$

を X の *von Neumann-Jordan* 定数という.

一般に $1 \leq C_{\mathrm{NJ}}(X) \leq 2$ であり, $C_{\mathrm{NJ}}(X) = 1 \iff X$: 内積空間 が成り立っている. また, ℓ_p ノルム $\|\cdot\|_p$ については

$$C_{\mathrm{NJ}}(\|\cdot\|_p) = 2^{|(2-p)/p|} \qquad (1 \leq p \leq \infty)$$

が知られている.

目標としていることは, $\psi \in \Psi_n$ に対応の $\|\cdot\|_\psi \in \mathcal{AN}_n$ に対して, $C_{\mathrm{NJ}}(\|\cdot\|_\psi)$ を求めることである. しかし, $n \geq 3$ のときの求め方は, ほとんど何も知られていないのが現状である. 以下では, $n = 2$ として, いくつかの結果を述べる.

まず, $\psi \in \Psi_2$, $M_1 = \max_{0\leq t\leq 1} \psi(t)/\psi_2(t)$, $M_2 = \max_{0\leq t\leq 1} \psi_2(t)/\psi(t)$ とするとき

$$\max\{M_1^2,\ M_2^2\} \leq C_{\mathrm{NJ}}(\|\cdot\|_\psi) \leq M_1^2\, M_2^2$$

の成り立つことがわかり, 次の Theorems A, B が知られている (cf. [5]).

Theorem A. $\psi \in \Psi_2$ が $t = 1/2$ に関して対称とし, $t = 1/2$ において, M_1 または M_2 の値をとるとする. このとき, 次が成り立つ.

$$C_{\mathrm{NJ}}(\|\cdot\|_\psi) = M_1^2\, M_2^2.$$

Theorem B. $\psi \in \Psi_2$ に対して, 次が成り立つ.

(i) $\psi \geq \psi_2 \implies C_{\mathrm{NJ}}(\|\cdot\|_\psi) = M_1^2$,

(ii) $\psi \leq \psi_2 \implies C_{\mathrm{NJ}}(\|\cdot\|_\psi) = M_2^2$.

Theorem A の条件のもとでは

$$C_{\mathrm{NJ}}(\|\cdot\|_\psi) = \max\{M_1^2\, M_2^2\} \iff \psi \geq \psi_2 \text{ or } \psi \leq \psi_2$$

であることがわかる. そこで次に, $C_{\mathrm{NJ}}(\|\cdot\|_\psi) = M_1^2\, M_2^2$ となるときについて考え, 次の結果が得られた ([1]).

Theorem 1. $\mathbb{K} = \mathbb{R}$ とする. $\psi \in \Psi_2$ が $t = 1/2$ に関して対称とし, $[0, 1/2]$ において M_1 (resp. M_2) の値をとる t は uniqude で t_1 (resp. t_2) とする. このとき, 次が成り立つ.

$$C_{\mathrm{NJ}}(\|\cdot\|_\psi) = M_1^2\, M_2^2 \iff t_1 t_2(1 - 2t_1)(1 - 2t_2) = 0 \text{ or } (1 - t_1)(1 - t_2) = 1/2.$$

Thorem 1 の 'if' part については，t_1，t_2 の unique 性や $\mathbb{K}=\mathbb{R}$ の仮定は要らないので，このことを踏まえ，次の corollary の成り立つことがわかる．

Corollary 1. $\psi \in \Psi_2$ とする．$M_1 = \max_{0\le t\le 1} \psi(t)/\psi_2(t)$ $\left(\text{resp. } M_2 = \max_{0\le t\le 1} \psi_2(t)/\psi(t)\right)$ の値をとる t の値 t_1 (resp. t_2) で次のいずれかを満たすものがあるとする．

(i) $t_1 t_2 = 0$,

(ii) ψ は $t = 1/2$ に関し対称で，$(1-2t_1)(1-2t_2) = 0$,

(iii) ψ は $t = 1/2$ に関し対称で，$(1-t_1)(1-t_2) = 1/2$.

このとき，$C_{\mathrm{NJ}}(\|\cdot\|_\psi) = M_1^2 M_2^2$ である．

3 James 定数

Definition 3. ノルム空間 X において

$$J(X) = \sup\{\min(\|\boldsymbol{x}+\boldsymbol{y}\|, \|\boldsymbol{x}-\boldsymbol{y}\|) \ : \ \boldsymbol{x},\boldsymbol{y}\in X,\ \|\boldsymbol{x}\| = \|\boldsymbol{y}\| = 1\}$$

を *James* 定数という．

一般に，$C_{\mathrm{NJ}}(X)$ との関係式として

$$1 \le J(X)^2/2 \le C_{\mathrm{NJ}}(X) \le J(X) \le 2$$

の成り立つことが知られている (cf. [3, 7])．このことから，$\psi \in \Psi_2$，$M_1 = \max_{0\le t\le 1} \psi(t)/\psi_2(t)$，$M_2 = \max_{0\le t\le 1} \psi_2(t)/\psi(t)$ とすると

$$\max\{M_1^2 M_2^2\} \le J(\|\cdot\|_\psi) \le \sqrt{2} M_1 M_2$$

が成り立つ．２節における $C_{\mathrm{NJ}}(\|\cdot\|_\psi)$ と同じように，この左右の等号成立条件を考え，以下の結果が得られた ([1]).

Proposition 1. $\psi \in \Psi_2$ に対して次が成り立つ．

$$J(\|\cdot\|_\psi) = \max\{M_1^2,\ M_2^2\} \iff \psi = \psi_1 \text{ or } \psi_\infty,$$

ここで，ψ_1，ψ_∞ はそれぞれ ℓ_1，ℓ_∞ ノルムに対応する関数である．

Theorem 2. $\mathbb{K} = \mathbb{R}$ とする．$\psi \in \Psi_2$ が $t = 1/2$ に関して対称とし，$M_1 = \max_{0\le t\le 1/2} \psi(t)/\psi_2(t)$，$M_2 = \max_{0\le t\le 1/2} \psi_2(t)/\psi(t)$ とする．このとき，次が成り立つ．

$$J(\|\cdot\|_\psi) = \sqrt{2}M_1 M_2 \quad \Longleftrightarrow$$

$$M_1 = \frac{\psi(t_1)}{\psi_2(t_1)},\ M_2 = \frac{\psi_2(t_2)}{\psi(t_2)},\ (1-t_1)(1-t_2) = \frac{1}{2}$$ を満たす $t_1, t_2 \in [0, 1/2]$ が存在.

Theorem 2 の 'if' part については，$\mathbb{K} = \mathbb{R}$ の仮定は不要であり，次の corollary が成り立つ.

Corollary 2. $\mathbb{K} = \mathbb{C}$ or $\mathbb{R}$ で，Theorem 2 の条件を満たすとき，次が成り立つ.

$$C_{\mathrm{NJ}}(\|\cdot\|_\psi) = C'_{\mathrm{NJ}}(\|\cdot\|_\psi) = C_{\mathrm{Z}}(\|\cdot\|_\psi) = C'_{\mathrm{Z}}(\|\cdot\|_\psi) = \frac{1}{2}J(\|\cdot\|_\psi)^2 = M_1^2 M_2^2,$$

ここで，$C_{\mathrm{Z}}(\|\cdot\|_\psi) = \sup\left\{\dfrac{\|\boldsymbol{x}+\boldsymbol{y}\|_\psi \|\boldsymbol{x}-\boldsymbol{y}\|_\psi}{\|\boldsymbol{x}\|_\psi^2 + \|\boldsymbol{y}\|_\psi^2} : (\boldsymbol{x}, \boldsymbol{y}) \neq (\boldsymbol{o}, \boldsymbol{o})\right\}$ (Zbăganu 定数) である．$C'_{\mathrm{NJ}}(\|\cdot\|_\psi)$, $C'_{\mathrm{Z}}(\|\cdot\|_\psi)$ は，それぞれ対応する定数の $\|\boldsymbol{x}\| = \|\boldsymbol{y}\| = 1$ の条件下での sup の値である.

4 Some examples

2 節，3 節の結果の使用例をいくつかあげる.

Examples 2. (cf. [2]) (i) Parabola norm: $0 < c \leq 1$ に対して

$$\psi_{par(c)} = ct^2 - ct + 1 \quad (0 \leq t \leq 1)$$

は放物線の一部で Ψ_2 の関数であり，対応するノルムは

$$\|(z, w)\|_{par(c)} = |z| + |w| - \frac{c|zw|}{|z| + |w|} \quad \text{for } (z, w) \neq \boldsymbol{o}$$

である．このとき

$$C_{\mathrm{NJ}}(\|\cdot\|_{par(c)}) = \frac{(4-c)^2}{8}, \quad J(\|\cdot\|_{par(c)}) = \frac{4-c}{2}$$

である.

(ii) Ellipse norm: $0 < a \leq 2\sqrt{c}$ に対して

$$\psi_{ell(a,c)}(t) = 1 + \sqrt{c} - \sqrt{-at^2 + at + c} \quad (0 \leq t \leq 1)$$

は楕円の一部で Ψ_2 の関数であり，対応するノルムは

$$\|(z, w)\|_{ell(a,c)} = (1 + \sqrt{c})(|z| + |w|) - \sqrt{c(|z| + |w|)^2 + a|zw|} \quad \text{for } (z, w) \neq \boldsymbol{o}$$

である．このとき

$$C_{\mathrm{NJ}}(\|\cdot\|_{ell(a,c)}) = 2\left(1 + \sqrt{c} - \sqrt{a+4c}/2\right)^2, \quad J(\|\cdot\|_{ell(a,c)}) = 2 + 2\sqrt{c} - \sqrt{a+4c}$$

である.

(iii) Hyperbola norm: $0 \le a,\ a^2 \le 4c$ に対して

$$\psi_{hyp(a,c)}(t) = \sqrt{at^2 - at + c} + 1 - \sqrt{c} \quad (0 \le t \le 1)$$

は双曲線の一部で Ψ_2 の関数であり，対応するノルムは

$$\|(z,w)\|_{hyp(a,c)} = (1 - |c|)(|z| + |w|) + \sqrt{c(|z|+|w|)^2 - a|zw|} \text{ for } (z,w) \neq \boldsymbol{o}$$

であり，とくに $\|\cdot\|_{hyp(2,1)}$ は ℓ^2 ノルム $\|\cdot\|_2$ である．このとき

$$C_{\mathrm{NJ}}(\|\cdot\|_{hyp(a,c)}) =$$

$$\begin{cases} \dfrac{1}{2}(\sqrt{4c-a} + 2 - 2\sqrt{c})^2 & \text{if } c \ge 1,\ 0 < a \le 2\sqrt{c} \\ & \text{or } 0 < c < 1,\ 0 < a \le \rho(c), \\ \dfrac{a(a+2-4\sqrt{c})}{2(a-2c)} & \text{if } 0 < c \le \dfrac{3-2\sqrt{2}}{2},\ \rho(c) < a < 4c \\ & \text{or } \dfrac{3-2\sqrt{2}}{2} < c < 1,\ \rho(c) < a \le \sigma(c), \\ \dfrac{a(a+2-4\sqrt{c})}{(a-2c)(\sqrt{4c-a}+2-2\sqrt{c})^2} & \text{if } \dfrac{3-2\sqrt{2}}{2} < c < \dfrac{1}{4},\ \sigma(c) < a < 4c \\ & \text{or } \dfrac{1}{4} \le c < 1,\ \sigma(c) < a < 2\sqrt{c}, \end{cases}$$

ここで，$\rho(c) = \frac{1}{2}\left\{3c + 2\sqrt{c} - 1 + (1-\sqrt{c})\sqrt{9c - 2\sqrt{c} + 1}\right\}$, $\sigma(c) = (8-4\sqrt{2})\sqrt{c} - 6 + 4\sqrt{2}$ である．

Example 3. $0 \le c \le 1$ とし，$\psi(t) = \max\left\{1 - ct,\ 1 - c + ct,\ 1 - \dfrac{c^2}{2}\right\}$ とすると，$\psi \in \Psi_2$ である．対応するノルムは

$$\|(z,w)\|_{tr(c)} = |z| + |w| - \min\left\{c|z|, c|w|, \tfrac{c^2}{2}(|z|+|w|)\right\}$$

であり，c の値によって

$$M_1 = \frac{\psi(1/2)}{\psi_2(1/2)} = \frac{2-c^2}{\sqrt{2}},\ M_2 = 1 \qquad \left(c \le -1 + \sqrt{3}\right),$$

$$M_1 = \frac{\psi(t_1)}{\psi_2(t_1)} = \sqrt{c^2 - 2c + 2},\ M_2 = \frac{\psi_2(t_2)}{\psi(t_2)} = \frac{\sqrt{2(c^2-2c+2)}}{2-c^2} \qquad \left(-1 + \sqrt{3} < c\right)$$

となる．ここで，$t_1 = (1-c)/(2-c)$, $t_2 = c/2$ であり，$(1-t_1)(1-t_2) = 1/2$ を満たす．よって，Theorem 2 などにより

$$J(\|\cdot\|_\psi) = \sqrt{2C_{NJ}(\|\cdot\|_\psi)} = \begin{cases} 2 - c^2 & \text{if } 0 \le c \le -1 + \sqrt{3}, \\ \dfrac{2(c^2-2c+2)}{2-c^2} & \text{if } -1 + \sqrt{3} < c \le 1. \end{cases}$$

References

[1] T. Ikeda and M. Kato, Notes on von Neumann-Jordan and James constants for absolute norms on $\mathbb{R}^2$, Mediterr. J. Math., to appear.

[2] T. Ikeda, S. Kai and M. Kato, Von Neumann-Jordan constant for the norms associated with conics, J. Nonlinear Convex Anal. **13** (2012), 807-820.

[3] M. Kato, L. Maligranda and Y. Takahashi, On James, Jordan-von Neumann constants and the normal structure coefficient of Banach spaces, Studia Math. **144** (2001), 275-295.

[4] K.-I. Mitani and K.-S. Saito, The James constant of absolute norms on $\mathbb{R}^2$, J. Nonlinear Convex Anal. **4** (2003), 399-410.

[5] K.-S. Saito, M. Kato and Y. Takahashi, Von Neumann-Jordan constant of absolute normalized norms on $\mathbb{C}^2$, J. Math. Anal. Appl. **244** (2000), 515-532.

[6] K.-S. Saito, M. Kato and Y. Takahashi, Absolute norms on $\mathbb{C}^n$, J. Math. Anal. Appl. **252** (2000), 879-905.

[7] Y. Takahashi and M. Kato, A simple inequality for the von Neumann-Jordan and James constants of a Banach space, J. Math. Anal. Appl. **359** (2009), 602-609.

Proceedings of Summer Seminar on
Lie Algebras and Related Topics **29** (2013)

行列環上の巡回符号について

大阪樟蔭女子大学・児童学部　松岡　学
Manabu Matsuoka
Faculty of Child Sciences,
Osaka Shoin Women's University

1　はじめに

有限体 $\mathbf{F}$ 上のベクトル空間 $\mathbf{F}^n = \{(a_0, \cdots, a_{n-1}) \mid a_i \in \mathbf{F}\}$ の部分空間 C のことを長さ n の線形符号という。線形符号 $C \subseteq \mathbf{F}^n$ が条件

$$(a_0, a_1, \cdots, a_{n-1}) \in C \text{ ならば } (a_{n-1}, a_0, a_1, \cdots, a_{n-2}) \in C$$

を満たすとき、巡回符号であるという。

J. A. Wood は有限フロベニウス環上の符号理論を [8] において確立した。また、M. Greferath と M. E. O'Sullivan は有限フロベニウス環上のブロック符号を [2]. において調べた。

本稿においては、有限 QF 環上の符号理論を構築することを考察する。

以後特に断らない限り、R は（必ずしも可換ではない）環、n は２以上の自然数、(g) は $g \in R[X]$ によって生成される両側イデアルを表すものとする。

2　QF 環

R を環とする。左 R-加群 P が射影加群であるとは、任意の全射 R-準同型写像 $g : M \to N$ と任意の R-準同型写像 $f : P \to N$ に対して、適当な R-準同型写像 $h : P \to M$ が存在して、$f = g \circ h$ が成り立つことをいう。任意の射影加群が自由加群に埋め込まれることはよく知られている。

左 R-加群 Q が入射加群であるとは、任意の単射 R-準同型写像 $g : N \to M$ と任意の R-準同型写像 $f : N \to Q$ に対して、適当な R-準同型写像 $h : M \to Q$ が存在して、$f = h \circ g$ が成り立つことをいう。任意の加群が入射加群に埋め込まれることはよく知られている。

環 R は R 自身が左（右）加群として入射的であるとき、左（右）自己入射環であるという。R が左自己入射であり、右自己入射でもあるとき、単に自己入射環であるという。

左 R-加群 M がアルチン加群 とは M が部分加群に関して降鎖条件を満たすことであるという。

環 R は R 自身が左（右）加群としてアルチン加群であるとき、 左（右）アルチン環であるという。R が左アルチンであり、右アルチンでもあるとき、単にアルチン環であるという。

降鎖条件の代わりに昇鎖条件にすることで、ネーター加群やネーター環を定義することができる。

有限環は明らかにアルチン環である。

M を左 R-加群とする。部分集合 $X \subseteq M$ に対して、X の annihilator を

$$\mathrm{ann}_l(X) = \{r \in R \mid 任意の\, x \in X \,に対して\, rx = 0\},$$

と定める。これは R の左イデアルとなる。. 右 R-加群の部分集合 X の annihilator $\mathrm{ann}_r(X)$ も同様に定義される。これはこれは R の右イデアルとなる。

定理 1. 任意の環 R に対して、次の条件は同値である。
(1) R は右アルチンかつ右自己入射環である。
(2) R は左アルチンかつ左自己入射環である。
(3) R は右ネーター環であり、次の条件を満たす。
(3a) 任意の右イデアル $A \subseteq R$ に対して $\mathrm{ann}_r(\mathrm{ann}_l A) = A$ が成り立つ。
(3b) 任意の左イデアル $I \subseteq R$ に対して $\mathrm{ann}_l(\mathrm{ann}_r I) = I$ が成り立つ。

定義 2. 定理 1 の条件を満たす環を QF (quasi-Frobenius) 環と呼ぶ。

QF (quasi-Frobenius) 環の定義は左右対称であることが分かる。

任意の左 R-加群 ${}_RM$ に対して、$M^* = \mathrm{Hom}_R({}_RM, {}_RR)$ は、右 R-加群になる。R の右からの作用は次のように定義される。

$$(f \cdot r)(m) = f(m) \cdot r$$

ここで、$r \in R$, $m \in M$, $f \in M^*$ である。

自然な準同型写像 $\xi : M \to M^{**}$ を次のように定義する。

$$\xi(m)(f) = f(m)$$

ここで、 $m \in M$, $f \in M^*$ である。

自然な準同型写像 $\xi : M \to M^{**}$ が単射であるとき、加群 M は torsionless と呼ばれる。自然な準同型写像 $\xi : M \to M^{**}$ が全単射であるとき、加群 M は reflexive と呼ばれる。

定理 3. R を *QF* 環とする。任意の有限生成 R-加群 M は *reflexive* である。

M の任意の部分加群 A に対して、$A^\circ = \{f \in M^* \mid f(A) = 0\}$ と定める。これは M^* の部分加群になる。

定理 4. R を *QF* 環、${}_RM$ を有限生成左 R-加群とする。M の任意の部分加群 A に対して、左 R-加群の同型 $A^{\circ\circ} \cong A$ が成り立つ。

3 環上の巡回符号

R を有限環とする。R^n の階数が k の左自由部分加群 $C \subseteq R^n$ を、R 上の左線形 $[n,k]$-符号とよぶ。n を線形符号 C の長さという。

R 上に次のような標準的な内積を定義する。
$x = (x_0, x_1, \cdots, x_{n-1})$, $y = (y_0, y_1, \cdots, y_{n-1}) \in R^n$ に対して

$$< x, y >= \sum_{i=0}^{n-1} x_i y_i$$

左線形符号 C の双対符号 $C^\perp$ を次のように定義する。

$$C^\perp = \{a \in R^n | \text{ 任意の } c \in C \text{ に対して } < c, a >= 0\}.$$

明らかに $C^\perp$ は R 上の右線形符号になる。

命題 5. 有限環 R の左線形符号 C に対して、右加群としての同型 $C^\perp \cong C^\circ$ が成り立つ。

定理 4 と命題 5 より、次のことが成り立つ。

定理 6. R を有限 QF 環、C を R^n の左線形符号とする。このとき、$(C^{\perp)\perp} = C$ が成り立つ。

双対符号 $C^\perp$ の階数に関しては、次が成り立つ。

定理 7. R を有限 QF 環、$C \subseteq R^n$ を有限階数の左自由部分加群とする。このとき、$C^\perp$ は有限階数の右自由加群であり、階数は、$\mathrm{rank} C^\perp = n - \mathrm{rank} C$ となる。

定理 5 と定理 6 に関しては、環 R が有限であるという条件は必要ない。
次に、巡回符号を定義する。

定義 8. C を R 上の長さが n の左線形符号とする。C が条件

$$(a_0, a_1, \cdots, a_{n-1}) \in C \text{ ならば } (a_{n-1}, a_0, a_1, \cdots, a_{n-2}) \in C$$

を満たすとき、巡回符号であるという。

巡回符号は多項式環の剰余環の左イデアルとみなすことができる。左 R-加群としての準同型写像 $\rho : R^n \to R[X]/(x^n - 1)$ を $a = (a_0, a_1, \cdots, a_{n-1})$ に対して、同値類 $\overline{a_{n-1}X^{n-1} + \cdots + a_1 X + a_0}$ を対応させる写像と定義する。このとき、R^n の巡回符号と $R[X]/(x^n - 1)$ の左イデアルを ρ を通して同一視することができる。

4 行列環の構成と巡回符号

歪多項式環を用いることで、行列環を構成する。

定義 9. R を環, θ をその自己準同型写像とする。S を $1, x, x^2, \cdots$ を基底とする左自由 R-加群とし、積を $x^i x^j = x^{i+j}$ と $xr = \theta(r)x$ により定める。ここで、$r \in R$ とする。このように構成された環 S を歪多項式環と呼び、記号 $R[x;\theta]$ で表わす。

位数が p の有限体を成分とする行列環を、歪多項式環を用いて構成する。

定理 10. $\mathbf{F}_{p^r}$ を位数が p^r の有限体とし、σ をそのフロベニウス写像とする。このとき、次の同型が成り立つ。

$$\mathbf{F}_{p^r}[x;\sigma] \cong M_r(\mathbf{F}_p).$$

行列環の巡回符号を具体的に求めるには、行列環を係数とする多項式環の剰余環の構造を決定する必要がある。

例 11. 行列環 $R = M_2(\mathbf{F}_2)$ に対して、中心は $Z = \mathbf{F}_2$ であり、次の同型が成り立つ。

$$R[x]/(x^3-1) \cong R \otimes_Z Z[x]/(x^3-1) \cong M_2(\mathbf{F}_2) \oplus M_2(\mathbf{F}_4).$$

今後は、行列環だけでなく、一般の QF 環の巡回符号を決定する方法を開発する必要がある。

参考文献

[1] D. Boucher and P. Solé, *Skew constacyclic codes over Galois rings*, Advances in Mathematics of Communications, Volume **2**, No. **3** (2008), 273–292.

[2] M. Greferath, M. E. O'Sullivan, *On bounds for codes over Frobenius rings under homogeneous weights*, Discrete Math, **289** (2004), 11–24.

[3] Y. Hirano, *On admissible rings*, Indag. Math. **8** (1997), 55–59.

[4] S. Ikehata, *On separable polynomials and Frobenius polynomials in skew polynomial rings*, Math. J. Okayama. Univ. **22** (1980), 115–129.

[5] T. Y. Lam, *Lectures on Modules and Rings, Graduate Texts in Mathematics*, Vol. 189, Springer-Verlag, New York, 1999.

[6] S. R. López-Permouth, B. R. Parra-Avila and S. Szabo, *Dual generalizations of the concept of cyclicity of codes*, Advances in Mathematics of Communications, Volume **3**, No. **3** (2009), 227–234.

[7] B. R. McDonald, *Finite Rings With Identity, Pure and Applied Mathematics*, Vol. 28, Marcel Dekker, Inc., New York, 1974.

[8] J. A. Wood, *Duality for modules over finite rings and applications to coding theory*, Amer. J. Math, **121** (1999), 555–575.

List of talks

Fujio Kubo	"Radical zero" forces a finite dimensional associative algebra to have a unity
Naoki Kawamoto	ある有理式環の微分代数について
Takefumi Shudo	加群の自己同型群と導分環
Yoji Yoshii	アーベル群の鏡映空間
Toshiharu Ikeda	ノルム空間の幾何的定数
Manabu Matsuoka	行列環上の巡回符号について