岐阜大学教育学部研究報告（自然科学）第41巻, 19-26, 2017年 3 月
Sci. Rep. Fac. Educ. Gifu Univ.（Nat. Sci.）41, 19-26, March 2017

任意の整域における最大公約元と最小公倍元について

On G.C.D. and L.C.M. in Any Integral Domain

畑田 一幸（Kazuyuki HATADA）

岐阜大学教育学部数学教室
〒５０１－１１９３　岐阜県岐阜市柳戸１－１
Gifu University,　Department of Mathematics, Faculty of Education,
1-1, Yanagido, Gifu City, GIFU 501-1193, Japan

MSC Numbers:　13A05, 11A05.
Key words and phrases:　G.C.D.,　L.C.M.,　integral domain.

要旨． A を任意の整域とし，　K で A の商体を表す。n を任意の正整数とし，　$a_1, a_2, \ldots, a_n$ で $\prod_{j=1}^{n} a_j \neq 0$ を満たす，　K の n 個の任意の元達を表す。本論文で与える主要な結果をここに記す。

「$a_1, a_2, \ldots, a_n$ の A に関する最大公約元 G.C.D.$(a_1, a_2, \ldots, a_n)$が存在する」と

「$a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1}$ の A に関する最小公倍元 L.C.M.$(a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1})$が存在する」は互いに必要かつ十分である。

$a_1, a_2, \ldots, a_n$ の A に関する最大公約元 G.C.D.$(a_1, a_2, \ldots, a_n)$が存在すれば，

(G.C.D.$(a_1, a_2, \ldots, a_n)$)(L.C.M.$(a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1})$)$=1_A$　が成立する。

λ を　$0 \neq \lambda \in K$ を満たす任意の元とする。G.C.D.$(a_1, a_2, \ldots, a_n)$　が存在するならば，

G.C.D.$(\lambda a_1, \lambda a_2, \ldots, \lambda a_n) = \lambda$ (G.C.D.$(a_1, a_2, \ldots, a_n)$) が成立する。L.C.M.$(a_1, a_2, \ldots, a_n)$ が存在するならば，　L.C.M.$(\lambda a_1, \lambda a_2, \ldots, \lambda a_n) = \lambda$ (L.C.M.$(a_1, a_2, \ldots, a_n)$) が成立する。

Abstract. Let A denote any integral domain. Let K denote the quotient field of A. Let n be any positive integer and let $a_1, a_2, \ldots, a_n$ denote arbitrary elements of K with $\prod_{j=1}^{n} a_j \neq 0$. Our main results in this paper are the following.

That "there exists G.C.D.$(a_1, a_2, \ldots, a_n)$ with respect to A" is equivalent to that "there exists L.C.M.$(a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1})$ with respect to A."

If there exists G.C.D.$(a_1, a_2, \ldots, a_n)$ with respect to A, then we have (G.C.D.$(a_1, a_2, \ldots, a_n)$)(L.C.M.$(a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1})$)$=1_A$.

Let λ satisfy $0 \neq \lambda \in K$. If there exists G.C.D.$(a_1, a_2, \ldots, a_n)$ with respect to A, then we have G.C.D.$(\lambda a_1, \lambda a_2, \ldots, \lambda a_n) = \lambda$ (G.C.D.$(a_1, a_2, \ldots, a_n)$). If there exists L.C.M.$(a_1, a_2, \ldots, a_n)$, then we have L.C.M.$(\lambda a_1, \lambda a_2, \ldots, \lambda a_n) = \lambda$ (L.C.M.$(a_1, a_2, \ldots, a_n)$).

本論文ではAを任意の整域とし，1_AでAの乗法の単位元，0_AでAの加法の単位元を表す。簡単に記すため，$1 = 1_A$かつ$0 = 0_A$と書く。KでAの商体を表す。(KがAから，定義なしに自然に，生まれてくることは，[2]と[3]に書いた。) 本論文では，nを任意の正整数とし，$a_1, a_2, \ldots, a_n$で$\prod_{j=1}^{n} a_j \neq 0$を満たす，$K$の$n$個の任意の元達を表す。

Aが一意分解整域のときは，$a_1, a_2, \ldots, a_n$の最小公倍元や最大公約元について，代数学の通常の教本（例えば[1], [5]）で扱われている。

本論文では，任意の整域Aで最小公倍元と最大公約元を扱う。

$x(\neq 0) \in K$と$y(\neq 0) \in K$に対し，Aに関して$x \mid y$を

$$x \mid y \quad \Leftrightarrow \quad \exists c \in A\,(y = cx)$$

により定義する。($x \mid y$のこの定義は[6, p. 13]に書かれている。) このとき直ちに$x^{-1} = cy^{-1}$

が得られ，　$x \mid y \quad \Leftrightarrow \quad y^{-1} \mid x^{-1}$　が分かる。

定義１．　$a_1, a_2, \ldots, a_n$の，　Aに関する最大公約元（G.C.D.）．

$\alpha(\neq 0) \in K$で次の条件①と②を満たすものを　$a_1, a_2, \ldots, a_n$の，　Aに関する最大公約元（G.C.D.）と呼ぶ。

①　　$\alpha \mid a_j \quad (1 \leq \forall j \leq n)$　である。

②　　$s \in K$が$s \mid a_j \quad (1 \leq \forall j \leq n)$　を満たすならば，　$s \mid \alpha$である。

注１．　$a_1, a_2, \ldots, a_n$の，　Aに関する最大公約元（G.C.D.）は，　必ずしも存在するとは限らない。

定義２．　$a_1, a_2, \ldots, a_n$の，　Aに関する最小公倍元（L.C.M.）．

$\beta(\neq 0) \in K$で次の条件③と④を満たすものを　$a_1, a_2, \ldots, a_n$の，　Aに関する最小公倍元（L.C.M.）と呼ぶ。

③　　$a_j \mid \beta \quad (1 \leq \forall j \leq n)$　である。

④　　$0 \neq t \in K$が$a_j \mid t \quad (1 \leq \forall j \leq n)$　を満たすならば，　$\beta \mid t$である。

注２．　$a_1, a_2, \ldots, a_n$の，　Aに関する最小公倍元（L.C.M.）は，　必ずしも存在するとは限らない。

この定義１と２は，　$\{a_1, a_2, \ldots, a_n\} \subset A$の場合，　[1, p.101]に書かれている。この定義１は，　$n = 2$で$\{a_1, a_2\} \subset A$のとき　[5, p.111]　にも書かれている。

しかし，　[6, pp. 14-15]では，　Aが単項イデアル整域の場合のみに，　最大公約元と最小

公倍元が扱われている。[6]では，一般の整域 A に関しては，最大公約元と最小公倍元が扱われていない。

定義１（resp. ２）により次が分かる。G.C.D.$(a_1, a_2, \dots, a_n)$ (resp. L.C.M.$(a_1, a_2, \dots, a_n)$) が存在すれば，A の単数倍を除いてそれは一意的に決定する。

本論文で与える結果は次の定理１，定理２，命題３である。

定理１． A を任意の整域とする。

(1) $a_1, a_2, \dots, a_n$ の A に関する最大公約元 G.C.D.$(a_1, a_2, \dots, a_n)$が存在すれば，

$a_1^{-1}, a_2^{-1}, \dots, a_n^{-1}$ の A に関する最小公倍元 L.C.M.$(a_1^{-1}, a_2^{-1}, \dots, a_n^{-1})$が存在する。

(2) $a_1, a_2, \dots, a_n$ の A に関する最小公倍元 L.C.M.$(a_1, a_2, \dots, a_n)$が存在すれば，

$a_1^{-1}, a_2^{-1}, \dots, a_n^{-1}$ の A に関する最大公約元 G.C.D. $(a_1^{-1}, a_2^{-1}, \dots, a_n^{-1})$が存在する。

定理１の(1)の証明． G.C.D.$(a_1, a_2, \dots, a_n)$を α と書く。定義１より

$$\alpha \mid a_j \quad (1 \le \forall j \le n) \tag{1.1}$$

かつ

$$\text{If} \quad \xi \in K \quad \text{and} \quad \xi \mid a_j \ \ (1 \le \forall j \le n), \quad \text{then} \ \ \xi \mid \alpha \tag{1.2}$$

が成立する。

(1.1) $\Leftrightarrow$ $a_j^{-1} \mid \alpha^{-1}$ $\quad (1 \le \forall j \le n)$ であり

(1.2) $\Leftrightarrow$ (If $\quad \xi \in K$ and $\quad a_j^{-1} \mid \xi^{-1}$ $\ (1 \le \forall j \le n)$, then $\ \alpha^{-1} \mid \xi^{-1}$) である。

即ち $\quad \alpha^{-1} = \text{L.C.M.}(a_1^{-1}, a_2^{-1}, \dots, a_n^{-1})$ $\quad$ を得た。

定理１の(2)の証明.　L.C.M.$(a_1, a_2, \ldots, a_n)$をβと書く。定義２より

$$a_j \mid \beta \qquad (1 \le \forall j \le n) \tag{2.1}$$

かつ

$$\text{If} \quad 0 \neq \eta \in K \quad \text{and} \quad a_j \mid \eta \quad (1 \le \forall j \le n), \quad \text{then} \quad \beta \mid \eta \tag{2.2}$$

が成立する。

(2.1) $\Leftrightarrow$ $\beta^{-1} \mid a_j^{-1}$　$(1 \le \forall j \le n)$　であり

(2.2) $\Leftrightarrow$ (If　$0 \neq \eta \in K$　and　$\eta^{-1} \mid a_j^{-1}$　$(1 \le \forall j \le n)$,　then　$\eta^{-1} \mid \beta^{-1}$)　である。

即ち　$\beta^{-1} = \text{G.C.D.}(a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1})$　を得た。

定理 2.　Aを任意の整域とする。　$a_1, a_2, \ldots, a_n$のAに関する最大公約元

G.C.D.$(a_1, a_2, \ldots, a_n)$が存在すれば,

$$(\text{G.C.D.}(a_1, a_2, \ldots, a_n))(\text{L.C.M.}(a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1}))=1$$

が成立する。

定理２の証明.　定理１の(1)の証明において，G.C.D.$(a_1, a_2, \ldots, a_n)$をαと書くとき

$\alpha^{-1} = \text{L.C.M.}(a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1})$　となることを示した。$\alpha\alpha^{-1} = 1$なので定理２が得られた。

Aが単項イデアル整域（よってAは一意分解整域となる）でかつ$n = 2$の場合のみに，[6]において，最小公倍元と最大公約元の定義が書かれており，定理２の$n = 2$のときの結果も言及されているがその証明は書かれていない。(P. Samuel はその証明を[6]の読者に任せている。）本論文では，Aを任意の整域とし，定理１，定理２，命題３を与えた。

命題３． Aを任意の整域とする。 λを $0\neq\lambda\in K$を満たす任意の元とする。

(i) G.C.D.$(a_1,a_2,\ldots,a_n)$ が存在するならば， G.C.D.$(\lambda a_1,\lambda a_2,\ldots,\lambda a_n)$も存在し

G.C.D.$(\lambda a_1,\lambda a_2,\ldots,\lambda a_n)=\lambda$(G.C.D.$(a_1,a_2,\ldots,a_n)$) が成立する。

(ii) L.C.M.$(a_1,a_2,\ldots,a_n)$ が存在するならば， L.C.M.$(\lambda a_1,\lambda a_2,\ldots,\lambda a_n)$も存在し

L.C.M.$(\lambda a_1,\lambda a_2,\ldots,\lambda a_n)=\lambda$(L.C.M.$(a_1,a_2,\ldots,a_n)$) が成立する。

命題３の(i)の証明． G.C.D.$(a_1,a_2,\ldots,a_n)$をαと書く。

(1.1)より $(\lambda\alpha)|(\lambda a_j)\quad(1\leq\forall j\leq n)$ が成立する。

さて$\rho\in K$が $\rho|(\lambda a_j)\ (1\leq\forall j\leq n)$ を満たすと仮定する。即ち， $\rho x_j=\lambda a_j$を満たす$x_j\in A$が各々の$j\in[1,n]\bigcap\mathbb{Z}$に対して存在すると仮定する。よって$\lambda^{-1}\rho x_j=a_j$を満たす$x_j\in A$が各々の$j\in[1,n]\bigcap\mathbb{Z}$に対して存在する。即ち $(\lambda^{-1}\rho)|a_j\ (1\leq\forall j\leq n)$となる。G.C.D.$(a_1,a_2,\ldots,a_n)=\alpha$であったから$(\lambda^{-1}\rho)|\alpha$である。即ち $\rho|(\lambda\alpha)$である。

以上より$\lambda\alpha=$G.C.D.$(\lambda a_1,\lambda a_2,\ldots,\lambda a_n)$を得た。

命題３の(ii)の証明． L.C.M.$(a_1,a_2,\ldots,a_n)$をβと書く。

(2.1)より $(\lambda a_j)|(\lambda\beta)\quad(1\leq\forall j\leq n)$ が成立する。

さて$0\neq\varphi\in K$が $(\lambda a_j)|\varphi\ (1\leq\forall j\leq n)$ を満たすと仮定する。即ち， $0\neq\varphi\in K$で$\varphi=(\lambda a_j)y_j$を満たす$y_j\in A$が各々の$j\in[1,n]\bigcap\mathbb{Z}$に対して存在すると仮定する。よって$0\neq\varphi\in K$で$\lambda^{-1}\varphi=a_jy_j$を満たす$y_j\in A$が各々の$j\in[1,n]\bigcap\mathbb{Z}$に対して存在する。即ち

$a_j \mid (\lambda^{-1}\varphi)$ $(1 \le \forall j \le n)$ かつ $\varphi \neq 0$ を得る。(2.2)が成立して，そして

$\beta = \text{L.C.M.}(a_1, a_2, \ldots, a_n)$であったから，$\beta \mid (\lambda^{-1}\varphi)$ を得る。即ち$\lambda^{-1}\varphi = \beta z$を満たす $z \in A$が存在する。よって$\varphi = \lambda\beta z$を満たす$z \in A$が存在する。即ち$(\lambda\beta) \mid \varphi$が成立する。

以上より $\lambda\beta = \text{L.C.M.}(\lambda a_1, \lambda a_2, \ldots, \lambda a_n)$を得た。$\beta = \text{L.C.M.}(a_1, a_2, \ldots, a_n)$であったから命題３の(ii)が証明された。

命題３と定理２により次の系を得る。

系１． λを $0 \neq \lambda \in K$を満たす任意の元とする。

(i) $\text{G.C.D.}(a_1, a_2, \ldots, a_n)$ が存在するならば，

$$\lambda = (\text{G.C.D.}(a_1, a_2, \ldots, a_n))(\text{L.C.M.}(\lambda a_1^{-1}, \lambda a_2^{-1}, \ldots, \lambda a_n^{-1}))$$

が成立する。

(ii) $\text{L.C.M.}(a_1, a_2, \ldots, a_n)$ が存在するならば，

$$\lambda = (\text{L.C.M.}(a_1, a_2, \ldots, a_n))(\text{G.C.D.}(\lambda a_1^{-1}, \lambda a_2^{-1}, \ldots, \lambda a_n^{-1}))$$

が成立する。

系２． 系１で$\lambda = \prod_{j=1}^{n} a_j$とおく。 次の(i)と(ii)を得る。

(i) $\text{G.C.D.}(a_1, a_2, \ldots, a_n)$ が存在するならば，

$$\prod_{j=1}^{n} a_j = (\text{G.C.D.}(a_1, a_2, \ldots, a_n))(\text{L.C.M.}(\frac{\lambda}{a_1}, \frac{\lambda}{a_2}, \ldots, \frac{\lambda}{a_n}))$$

が成立する。

(ii) $\text{L.C.M.}(a_1, a_2, \ldots, a_n)$ が存在するならば，

$$\prod_{j=1}^{n} a_j = (\text{L.C.M.}(a_1, a_2, \ldots, a_n))(\text{G.C.D.}(\frac{\lambda}{a_1}, \frac{\lambda}{a_2}, \ldots, \frac{\lambda}{a_n}))$$

が成立する。

注３．Aを有理整数環$\mathbb{Z}$で$\{a_1, a_2, \ldots, a_n\} \subset \mathbb{Z}$のとき，系２の結果はよく知られている（例えば[4, p. 9, exercise 2]参照）。その証明方法は，各a_jを素因数分解しておいて，等式の左辺の数と右辺の数の素因数分解が一致することを示すものである。（$\Leftarrow \mathbb{Z}$が一意分解整域であることは非常に良く知られている。）本論文で畑田が使った方法は素元分解を用いない方法であり，[4]とは証明方法が全く異なっている。

文献

[1] 永尾汎，代数学，朝倉書店，東京，1983.

[2] K. Hatada, On the reason why the product of two negative integers must be positive, In: Geometry, Analysis and Mechanics, John M. Rassias, ed., World Scientific Pub., Singapore, New Jersey, London, 1994, pp. 113-120 and the sheet of corrections of misprints enclosed in the book.

[3] K. Hatada, The source of the rational numbers $\mathbb{Q}$ and rings of fractions $S^{-1}A$, JP Journal of Algebra, Number Theory and Applications, Vol. 14, Number 1, (2009), pp. 97-119.

[4] L. Hua, Introduction to Number Theory, Springer, Berlin, Heidelberg, New York, 1982.

[5] S. Lang, Algebra, 3rd edition, Springer, Berlin, Heidelberg, New York, 2002.

[6] P. Samuel, Algebraic Theory of Numbers, (Translated from the French by A. Silberger), Hermann, Paris, 1971.