鲁东大学学报(自然科学版)
Journal of Ludong University(Natural Science Edition)　2020,36(4):305—311

关于欧氏环中最大公因子与最小公倍的统一求法

陈灵香,谭宜家

(福州大学　数学与计算机科学学院,福州 350108)

摘要:研究了欧氏环中元素的最大公因子与最小公倍,利用矩阵的初等变换,给出了欧氏环中多个元素的最大公因子与最小公倍的统一求法。

关键词:最大公因子;最小公倍;矩阵;欧氏环
中图分类号:O153.5　文献标志码:A　文章编号:1673-8020(2020)04-0305-07

欧氏环中元素的最大公因子与最小公倍是欧氏环的一个基本内容。计算欧氏环中元素的最大公因子与最小公倍(包括整数和多项式的最大公因子与最小公倍)的一个常用方法是矩阵的初等变换法。文献[1—3]利用矩阵的初等变换求整数或多项式的最大公因子;文献[4]和文献[5—6]分别求出整数的最小公倍数和多项式的最小公因式;进一步,文献[7]和文献[8]在欧氏环中分别给出元素的最大公因子和最小公倍的矩阵方法。与此同时,文献[9]利用整数矩阵的初等变换,在一个整数矩阵上同时求出两个整数的最大公因数和最小公倍数;而文献[10-13]将这一方法应用在域上的多项式环,给出求两个多项式最大公因式和最小公倍式的统一方法;文献[14]将这一方法拓广到欧氏环上,通过对欧氏环上矩阵的讨论,给出欧氏环中两个元素的最大公因子与最小公倍的统一求法,该方法对整数环 Z 和多项式环 $F[x]$ 中问题的解决具有指导意义。

本文在文献[14]的基础上进一步探讨欧氏环中元素的最大公因子和最小公倍,利用欧氏环上矩阵的初等变换,同时求出多个元素的最大公因子和最小公倍,并将最大公因子表为这些元素的组合。所得结果拓广了文献[14]中的重要结论。

1　基本概念与引理

本文中,R 表示一个含有单位元 1 的交换环。

设 $a \in R$,如果存在 $b \in R$ 使得 $ab = ba = 1$,则称 a 是 R 中的一个可逆元。本文用 $U(R)$ 表示 R 中所有可逆元组成的集合。对于任意 $a,b \in R$,如果 $a = bc$,则称 b 为 a 的一个因子(或称 b 整除 a),记为 $b|a$。如果 $a \in U(R)$,则有 $aa^{-1} = a^{-1}a = 1$,所以 a 可逆当且仅当 $a|1$。

设 R 是一个环。R 称为一个整环,如果 $\forall a,b \in R$,由 $ab = 0$ 可推出 $a = 0$ 或 $b = 0$,这里 0 表示环 R 中的零元。显然,如果 R 为整环,那么 $\forall a,b,c \in R$,当 $a \neq 0$ 时,由 $ab = ac$(或 $ba = ca$)可推出 $b = c$。对于 R 中的任意元 a,b,如果存在 $\varepsilon \in U(R)$ 使得 $b = \varepsilon a$,则称 a 与 b 在 R 中相伴,记为 $a \sim b$。显然,相伴关系"~"是 R 上的一个等价关系。

设 R 是一个交换整环,$a_1,a_2,\cdots,a_n \in R$,$d,m \in R$。d 称为 $a_1,a_2,\cdots,a_n$ 的一个最大公因子,如果 $d|a_1,d|a_2,\cdots,d|a_n$,并且 $\forall c \in R$,由 $c|a_1,c|a_2,\cdots,c|a_n$ 可推出 $c|d$。用 $(a_1,a_2,\cdots,a_n)$ 表示 $a_1,a_2,\cdots,a_n$ 的任一个最大公因子。对偶地,m 称为 $a_1,a_2,\cdots,a_n$ 的一个最小公倍,如果 $a_1|m,a_2|m,\cdots,a_n|m$,并且 $\forall l$

收稿日期:2020-09-03;修回日期:2020-09-15
基金项目:福建省自然科学基金面上项目(2016J01012)
第一作者简介:陈灵香(1996—),女,福建宁德人,研究方向为应用数学。E-mail:444520828@qq.com
通信作者简介:谭宜家(1962—),男,湖北咸宁人,教授,硕士研究生导师,硕士,研究方向为矩阵代数及其应用。E-mail:yjtan62@126.com

$\in R$,由 $a_1 | l, a_2 | l, \cdots, a_n | l$ 可推出 $m | l$。用 $[a_1, a_2, \cdots, a_n]$ 表示 $a_1, a_2, \cdots, a_n$ 的任一个最小公倍。

一个交换整环 R 称为欧氏环[5],如果存在 R 到非负整数集 $\mathbf{N}$ 的一个映射 $\delta: R \to \mathbf{N}, a| \to \delta(a)$,满足:$\forall a, b \in R, b \neq 0$,存在 $q, r \in R$,使得 $a = bq + r$,且 $\delta(r) < \delta(b)$。

显然,整数环、域上的多项式环都是特殊的欧氏环。

设 R 是一个交换环。$\boldsymbol{M}_{m,n}(R)$ 表示 R 上所有 $m \times n$ 矩阵组成的集合,特别地,用 $\boldsymbol{M}_n(R)$ 表示 R 上所有 n 阶矩阵组成的集合。对于任意 $\boldsymbol{A} \in \boldsymbol{M}_{m,n}(R)$,用 a_{ij} 表示矩阵 $\boldsymbol{A}$ 的第 i 行第 j 列交叉处的元素;$\boldsymbol{E}_n$ 表示 R 上的 n 阶单位矩阵,$\boldsymbol{E}_{ij}$ 表示 R 上第 i 行第 j 列交叉处元素为 1,其余元素为 0 的 n 阶矩阵;用 $\boldsymbol{O}$ 表示零矩阵。

对于任意 $\boldsymbol{A} \in \boldsymbol{M}_{m,n}(R)$,下列三种变换称为矩阵 $\boldsymbol{A}$ 的行(列)初等变换[5]:

a) 将矩阵 $\boldsymbol{A}$ 的某一行(某一列)乘以 R 中的某一元素加到 $\boldsymbol{A}$ 的另一行(另一列),其余行(列)不变;

b) 将矩阵 $\boldsymbol{A}$ 中某一行(某一列)乘以 R 中的一个可逆元,其余行(列)不变;

c) 交换矩阵 $\boldsymbol{A}$ 中两行(两列)的位置,其余行(列)不变。

由单位矩阵 $\boldsymbol{E}_n$ 经过一次初等变换得到的矩阵称为初等矩阵[5]。

显然,每一个初等变换都有一个与之相对应的初等矩阵。具体地,将 $\boldsymbol{E}_n$ 的第 j 行乘以 $b(b \in R)$,加到 $\boldsymbol{E}_n$ 的第 i 行,得 $\boldsymbol{P}(i, j(b)) = \boldsymbol{E}_n + b\boldsymbol{E}_{ij}$;用 R 中的可逆元 u 乘以 $\boldsymbol{E}_n$ 的第 i 行,得 $\boldsymbol{P}(i(u)) = \boldsymbol{E}_n + (u - 1)\boldsymbol{E}_{ii}$;交换矩阵 $\boldsymbol{E}_n$ 的第 i 行与第 j 行的位置,得 $\boldsymbol{P}(i, j) = \boldsymbol{E}_n - \boldsymbol{E}_{ii} - \boldsymbol{E}_{jj} + \boldsymbol{E}_{ij} + \boldsymbol{E}_{ji}$。不难验证,矩阵 $\boldsymbol{P}(i, j(b))$,$\boldsymbol{P}(i(u))$ 和 $\boldsymbol{P}(i, j)$ 都是可逆的。

同样可以得到与列初等变换相对应的初等矩阵。不难看出,对单位矩阵作一次列初等变换得到的矩阵也包含在上面列举的三类矩阵之中。因此,这三类矩阵是全部的初等矩阵。

在交换环 R 中,下列结论成立[5]:

a) 欧氏环中任意有限个元素都有最大公因子和最小公倍。

b) 设 $\boldsymbol{A} \in \boldsymbol{M}_{m,n}(R)$,则对 $\boldsymbol{A}$ 施行一次行初等变换,相当于对 $\boldsymbol{A}$ 左乘上一个相对应的初等矩阵;对 $\boldsymbol{A}$ 施行一次列初等变换,相当于对 $\boldsymbol{A}$ 右乘上一个相对应的初等矩阵。

引理 1 设 R 是一个欧氏环,$a_1, a_2, \cdots, a_n, b \in R$,那么

(i) $(a_1, a_2)[a_1, a_2] \sim a_1 a_2$;

(ii) $((a_1, a_2, \cdots, a_{n-1}), a_n) \sim (a_1, a_2, \cdots, a_{n-1}, a_n)$,$[[a_1, a_2, \cdots, a_{n-1}], a_n] \sim [a_1, a_2, \cdots, a_{n-1}, a_n]$;

(iii) $b(a_1, a_2, \cdots, a_n) \sim (ba_1, ba_2, \cdots, ba_n)$。

证明 从略。

定义 1 设 $\boldsymbol{A}, \boldsymbol{B} \in \boldsymbol{M}_{m,n}(R)$,若存在可逆矩阵 $\boldsymbol{U} \in \boldsymbol{M}_m(R)$ 和 $\boldsymbol{V} \in \boldsymbol{M}_n(R)$,使得 $\boldsymbol{B} = \boldsymbol{UAV}$,则称 $\boldsymbol{A}$ 与 $\boldsymbol{B}$ 等价,记为 $\boldsymbol{A} \sim \boldsymbol{B}$。

引理 2[5] 设 R 是一个交换环,那么矩阵 $\boldsymbol{A} \in \boldsymbol{M}_n(R)$ 是可逆的当且仅当 $\boldsymbol{A}$ 的行列式 $|\boldsymbol{A}|$ 在 R 中是可逆的。

引理 3 设 R 是一个欧氏环,$\boldsymbol{A} \in \boldsymbol{M}_{m,n}(R)$。那么 $\boldsymbol{A}$ 等价于矩阵 $\boldsymbol{B} = \begin{bmatrix} \boldsymbol{D}_r & \boldsymbol{O} \\ \boldsymbol{O} & \boldsymbol{O} \end{bmatrix}$,这里 $\boldsymbol{D}_r = \mathrm{diag}(d_1, d_2, \cdots, d_r)$,$d_i \neq 0$,且当 $i \leqslant j$ 时,$d_i | d_j$。

证明 由文献[5]中的定理 3.8 可得。

引理 3 中的矩阵 $\boldsymbol{B}$ 称为矩阵 $\boldsymbol{A}$ 的等价标准形,$d_1, d_2, \cdots, d_r$ 称为 $\boldsymbol{A}$ 的不变因子。从文献[5]中定理 3.8 的证明可以看出,对欧氏环上矩阵 $\boldsymbol{A}$ 施行有限次初等变换后,可得到 $\boldsymbol{A}$ 的等价标准形。又因为初等矩阵是可逆的,所以由引理 3,得下列结论:

推论 1 欧氏环 R 上 n 阶矩阵是可逆的,当且仅当该矩阵可表为一些初等矩阵的乘积。

引理 4 设 R 是一个欧氏环,$\boldsymbol{A} \in \boldsymbol{M}_{m,n}(R)$,$\boldsymbol{A}$ 的秩为 r,不变因子为 $d_1, d_2, \cdots, d_r$,$\forall i \in \{1, 2, \cdots, r\}$,记 Δ_i 为 $\boldsymbol{A}$ 的所有 i 阶子式的最大公因子。那么

$$d_1 \sim \Delta_1, \Delta_2 \sim d_2\Delta_1, \cdots, \Delta_r \sim d_r\Delta_{r-1}。$$

证明　由文献[5]中的定理 3.9 可得。

2　主要结论

定理 1　设 R 是一个欧氏环，$a_1, a_2, \cdots, a_n$ 是 R 中的非零元，作矩阵

$$\boldsymbol{A} = \begin{bmatrix} a_1 & 0 & 0 & \cdots & 0 & 0 \\ a_2 & a_2 & 0 & \cdots & 0 & 0 \\ a_3 & 0 & a_3 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_n & 0 & 0 & \cdots & 0 & a_n \end{bmatrix},$$

则有下列结论成立：

1）$\boldsymbol{A}$ 的等价标准形具有形式 $\boldsymbol{B} = \mathrm{diag}(d_1, d_2, \cdots, d_n)$，即存在可逆矩阵 $\boldsymbol{U}, \boldsymbol{V} \in \boldsymbol{M}_n(R)$，使得 $\boldsymbol{UAV} = \boldsymbol{B}$，其中 $d_i \neq 0 (1 \leqslant i \leqslant n)$，且当 $i \leqslant j$ 时，$d_i | d_j$；

2）$d_1 \sim (a_1, a_2, \cdots, a_n)$，$d_n \sim [a_1, a_2, \cdots, a_n]$；

3）$d_1 = u_{11}v_{11}a_1 + u_{12}(v_{11} + v_{21})a_2 + \cdots + u_{1n}(v_{11} + v_{n1})a_n$，其中 $u_{11}, u_{12}, \cdots, u_{1n}$ 和 $v_{11}, v_{21}, \cdots, v_{n1}$ 分别为矩阵 $\boldsymbol{U}$ 和 $\boldsymbol{V}$ 的第一行和第一列的元素。

证明　1）因为 $a_1, a_2, \cdots, a_n$ 是 R 中的非零元，所以 $\boldsymbol{A}$ 的行列式 $|\boldsymbol{A}| = a_1a_2\cdots a_n \neq 0$。由引理 3，可设 $\boldsymbol{B} = \mathrm{diag}(d_1, d_2, \cdots, d_r, 0, \cdots, 0) \in \boldsymbol{M}_n(R)$ 是 $\boldsymbol{A}$ 的等价标准形，其中 $d_i \neq 0 (1 \leqslant i \leqslant r, r \leqslant n)$，当 $i \leqslant j$ 时，$d_i | d_j$。而由 $\boldsymbol{UAV} = \boldsymbol{B}$，得 $|\boldsymbol{B}| = |\boldsymbol{U}| \cdot |\boldsymbol{A}| \cdot |\boldsymbol{V}| \neq 0$（根据引理 2），因此 $r = n$。

2）由引理 4 知，$d_1 \sim \Delta_1 = (a_1, a_2, \cdots, a_n)$。下证 $d_n \sim [a_1, a_2, \cdots, a_n]$。

首先，不难得到，$\Delta_{n-1} = (a_2a_3\cdots a_n, a_1a_3\cdots a_n, \cdots, a_1a_2\cdots a_{n-1})$，$\Delta_n = a_1a_2\cdots a_n$。为了证明 $d_n \sim [a_1, a_2, \cdots, a_n]$，下面用归纳法证明

$$(a_2a_3\cdots a_n, a_1a_3\cdots a_n, \cdots, a_1a_2\cdots a_{n-1})[a_1, a_2, \cdots, a_n] \sim a_1a_2\cdots a_n。\tag{1}$$

当 $n = 2$ 时，由引理 1(i) 知，式(1) 左边 $= (a_2, a_1)[a_1, a_2] \sim a_1a_2 =$ 右边，故式(1) 成立。假设对于 $n - 1 (n \geqslant 3)$，式(1) 成立。那么对于 n，有

$$\begin{aligned}
&(a_2a_3\cdots a_n, a_1a_3\cdots a_n, \cdots, a_1a_2\cdots a_{n-1})[a_1, a_2, \cdots, a_n]([a_1, \cdots, a_{n-1}], a_n) \sim \\
&(a_2a_3\cdots a_n, a_1a_3\cdots a_n, \cdots, a_1a_2\cdots a_{n-1})[[a_1, \cdots, a_{n-1}], a_n]([a_1, \cdots, a_{n-1}], a_n)（根据引理 1(\mathrm{ii})）\sim \\
&(a_2a_3\cdots a_n, a_1a_3\cdots a_n, \cdots, a_1a_2\cdots a_{n-1})[a_1, a_2, \cdots, a_{n-1}]a_n（根据引理 1(\mathrm{i})）\sim \\
&((a_2a_3\cdots a_n, a_1a_3\cdots a_n, \cdots, a_1a_2\cdots a_{n-2}a_n), a_1a_2\cdots a_{n-1})[a_1, a_2, \cdots, a_{n-1}]a_n（根据引理 1(\mathrm{ii})）\sim \\
&((a_2a_3\cdots a_{n-1}, a_1a_3\cdots a_{n-1}, \cdots, a_1a_2\cdots a_{n-2})a_n, a_1a_2\cdots a_{n-1})[a_1, a_2, \cdots, a_{n-1}]a_n（根据引理 1(\mathrm{iii})）\sim \\
&((a_2a_3\cdots a_{n-1}, a_1a_3\cdots a_{n-1}, \cdots, a_1a_2\cdots a_{n-2})[a_1, a_2, \cdots, a_{n-1}]a_n, a_1a_2\cdots a_{n-1}[a_1, a_2, \cdots, a_{n-1}])a_n（根据引理 1(\mathrm{iii})）\sim \\
&(a_1a_2\cdots a_{n-1}a_n, a_1a_2\cdots a_{n-1}[a_1, a_2, \cdots, a_{n-1}])a_n（根据归纳假设）\sim \\
&a_1a_2\cdots a_{n-1}(a_n, [a_1, a_2, \cdots, a_{n-1}])a_n（根据引理 1(\mathrm{iii})）= \\
&a_1a_2\cdots a_{n-1}a_n(a_n, [a_1, a_2, \cdots, a_{n-1}]),
\end{aligned}$$

所以得到

$$\begin{aligned}
&(a_2a_3\cdots a_n, a_1a_3\cdots a_n, \cdots, a_1a_2\cdots a_{n-1})[a_1, a_2, \cdots, a_n]([a_1, \cdots, a_{n-1}], a_n) \sim \\
&a_1a_2\cdots a_{n-1}a_n(a_n, [a_1, a_2, \cdots, a_{n-1}])。
\end{aligned}$$

由于 $([a_1, \cdots, a_{n-1}], a_n) \neq 0$，所以 $(a_2a_3\cdots a_n, a_1a_3\cdots a_n, \cdots, a_1a_2\cdots a_{n-1})[a_1, a_2, \cdots, a_n] \sim a_1a_2\cdots a_n$，即式(1) 成立，故 $\Delta_{n-1}[a_1, a_2, \cdots, a_n] \sim \Delta_n$。结合 1) 及引理 4 知 $\Delta_{n-1}d_n \sim \Delta_n$，进而得到 $\Delta_{n-1}[a_1, a_2, \cdots, a_n] \sim \Delta_{n-1}d_n$。而 $\Delta_{n-1} \neq 0$，所以，$d_n \sim [a_1, a_2, \cdots, a_n]$。

3）由 $\boldsymbol{B} = \boldsymbol{UAV}$ 知

$$d_1 = b_{11} = \sum_{i,j=1}^{n} u_{1i}a_{ij}v_{j1} = u_{11}v_{11}a_1 + u_{12}(v_{11}+v_{21})a_2 + \cdots + u_{1n}(v_{11}+v_{n1})a_n。$$

证毕。

注1:在定理1中,当 $n=2$ 时,有 $d_1 \sim (a_1,a_2)$,$d_2 \sim [a_1,a_2]$,即存在 $\varepsilon_1,\varepsilon_2 \in U(R)$,使得 $d_1 = \varepsilon_1(a_1,a_2)$,$d_2 = \varepsilon_2[a_1,a_2]$。

根据定理1,给出具体求欧氏环中多个元素的最大公因子、最小公倍以及将最大公因子表为这些元素组合的统一方法。

对于定理1中的矩阵 A,存在 R 上的可逆矩阵 $\boldsymbol{U},\boldsymbol{V}$,使得 $\boldsymbol{UAV}=\boldsymbol{B}$,其中 $\boldsymbol{B}$ 是 A 的等价标准形。由推论1知,存在 R 上的初等矩阵 $\boldsymbol{P}_1,\boldsymbol{P}_2,\cdots,\boldsymbol{P}_s$;$\boldsymbol{Q}_1,\boldsymbol{Q}_2,\cdots,\boldsymbol{Q}_t$ 使得 $\boldsymbol{P}_s\cdots\boldsymbol{P}_2\boldsymbol{P}_1=\boldsymbol{U}$,$\boldsymbol{Q}_1\boldsymbol{Q}_2\cdots\boldsymbol{Q}_t=\boldsymbol{V}$。于是,$\boldsymbol{P}_s\cdots\boldsymbol{P}_2\boldsymbol{P}_1\boldsymbol{A}\boldsymbol{Q}_1\boldsymbol{Q}_2\cdots\boldsymbol{Q}_t=\boldsymbol{B}$。

现将矩阵 $\boldsymbol{A},\boldsymbol{E}_n,\boldsymbol{E}_n,\boldsymbol{O}$ 凑成一个 $2n$ 阶矩阵 $\begin{bmatrix}\boldsymbol{A} & \boldsymbol{E}_n\\ \boldsymbol{E}_n & \boldsymbol{O}\end{bmatrix}$,按矩阵的分块乘法规则,可得

$$\begin{bmatrix}\boldsymbol{P}_s & \boldsymbol{O}\\ \boldsymbol{O} & \boldsymbol{E}_n\end{bmatrix}\cdots\begin{bmatrix}\boldsymbol{P}_2 & \boldsymbol{O}\\ \boldsymbol{O} & \boldsymbol{E}_n\end{bmatrix}\begin{bmatrix}\boldsymbol{P}_1 & \boldsymbol{O}\\ \boldsymbol{O} & \boldsymbol{E}_n\end{bmatrix}\begin{bmatrix}\boldsymbol{A} & \boldsymbol{E}_n\\ \boldsymbol{E}_n & \boldsymbol{O}\end{bmatrix}\begin{bmatrix}\boldsymbol{Q}_1 & \boldsymbol{O}\\ \boldsymbol{O} & \boldsymbol{E}_n\end{bmatrix}\begin{bmatrix}\boldsymbol{Q}_2 & \boldsymbol{O}\\ \boldsymbol{O} & \boldsymbol{E}_n\end{bmatrix}\cdots\begin{bmatrix}\boldsymbol{Q}_t & \boldsymbol{O}\\ \boldsymbol{O} & \boldsymbol{E}_n\end{bmatrix}=$$

$$\begin{bmatrix}\boldsymbol{P}_s\cdots\boldsymbol{P}_2\boldsymbol{P}_1\boldsymbol{A}\boldsymbol{Q}_1\boldsymbol{Q}_2\cdots\boldsymbol{Q}_t & \boldsymbol{P}_s\cdots\boldsymbol{P}_2\boldsymbol{P}_1\\ \boldsymbol{Q}_1\boldsymbol{Q}_2\cdots\boldsymbol{Q}_t & O\end{bmatrix}=\begin{bmatrix}\boldsymbol{UAV} & \boldsymbol{U}\\ \boldsymbol{V} & \boldsymbol{O}\end{bmatrix}=\begin{bmatrix}\boldsymbol{B} & \boldsymbol{U}\\ \boldsymbol{V} & \boldsymbol{O}\end{bmatrix} \tag{2}$$

式(2)表明,只要对 $2n$ 阶矩阵 $\begin{bmatrix}\boldsymbol{A} & \boldsymbol{E}_n\\ \boldsymbol{E}_n & \boldsymbol{O}\end{bmatrix}$ 的前 n 行和前 n 列分别作行初等变换和列初等变换,把 $\boldsymbol{A}$ 变为它的等价标准形 $\boldsymbol{B}$,那么该矩阵的右上角和左下角的单位矩阵 E_n 分别变成可逆矩阵 $\boldsymbol{U}$ 和 $\boldsymbol{V}$。通过定理1,可得到这些元素的最大公因子和最小公倍,并将最大公因子表为这些元素的组合。

例1 设 $a=231$,$b=273$,$c=429$,求 a,b,c 的最大公因数 (a,b,c) 和最小公倍数 $[a,b,c]$,并将 (a,b,c) 表为元素 a,b,c 的一个组合。

解 作6阶矩阵

$$\boldsymbol{C}=\begin{bmatrix}231 & 0 & 0 & 1 & 0 & 0\\ 273 & 273 & 0 & 0 & 1 & 0\\ 429 & 0 & 429 & 0 & 0 & 1\\ 1 & 0 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 0 & 0\end{bmatrix},$$

并在整数环 Z 上对矩阵 $\boldsymbol{C}$ 的前三行和前三列分别作行初等变换和列初等变换,则有下列式子成立:

$$\boldsymbol{C}\xrightarrow{r_2+(-1)r_1,\,r_3+(-1)r_1}\begin{bmatrix}231 & 0 & 0 & 1 & 0 & 0\\ 42 & 273 & 0 & -1 & 1 & 0\\ 198 & 0 & 429 & -1 & 0 & 1\\ 1 & 0 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 0 & 0\end{bmatrix}\xrightarrow{r_1+(-5)r_2,\,r_3+(-4)r_2}$$

$$\begin{bmatrix}21 & -1365 & 0 & 6 & -5 & 0\\ 42 & 273 & 0 & -1 & 1 & 0\\ 30 & -1092 & 429 & 3 & -4 & 1\\ 1 & 0 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 0 & 0\end{bmatrix}\xrightarrow{r_2+(-2)r_1,\,r_3+(-1)r_1}\begin{bmatrix}21 & -1365 & 0 & 6 & -5 & 0\\ 0 & 3003 & 0 & -13 & 11 & 0\\ 9 & 273 & 429 & -3 & 1 & 1\\ 1 & 0 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 0 & 0\end{bmatrix}\xrightarrow{r_1+(-2)r_3}$$

$$\begin{bmatrix} 3 & -1911 & -858 & 12 & -7 & -2 \\ 0 & 3003 & 0 & -13 & 11 & 0 \\ 9 & 273 & 429 & -3 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix} \xrightarrow{r_3+(-3)r_1} \begin{bmatrix} 3 & -1911 & -858 & 12 & -7 & -2 \\ 0 & 3003 & 0 & -13 & 11 & 0 \\ 0 & 6006 & 3003 & -39 & 22 & 7 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ & & & & & \end{bmatrix} \xrightarrow{c_2+637c_1,c_3+286c_1}$$

$$\begin{bmatrix} 3 & 0 & 0 & 12 & -7 & -2 \\ 0 & 3003 & 0 & -13 & 11 & 0 \\ 0 & 6006 & 3003 & -39 & 22 & 7 \\ 1 & 637 & 286 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix} \xrightarrow{r_3+(-2)r_2} \begin{bmatrix} 3 & 0 & 0 & 12 & -7 & -2 \\ 0 & 3003 & 0 & -13 & 11 & 0 \\ 0 & 0 & 3003 & -13 & 0 & 7 \\ 1 & 637 & 286 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}。$$

可以得到，$(a,b,c)=3$，$[a,b,c]=3003$，以及

$$\boldsymbol{U}=\begin{bmatrix} 12 & -7 & -2 \\ -13 & 11 & 0 \\ -13 & 0 & 7 \end{bmatrix},\boldsymbol{V}=\begin{bmatrix} 1 & 637 & 286 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}。$$

所以 $u_{11}=12$，$u_{12}=-7$，$u_{13}=-2$，$v_{11}=1$，$v_{21}=v_{31}=0$。于是，$u_{11}v_{11}=12$，$u_{12}(v_{11}+v_{21})=-7$，$u_{13}(v_{11}+v_{31})=-2$，则有 $3=12\times 231+(-7)\times 273+(-2)\times 429$。

例 2　设 $f(x)=x^3+3x^2+2x$，$g(x)=x^3+x^2-2x$，$h(x)=x^3+2x^2-x-2\in F[x]$，求 $(f(x),g(x),h(x))$ 与 $[f(x),g(x),h(x)]$，并将 $(f(x),g(x),h(x))$ 表为多项式 $f(x),g(x),h(x)$ 的一个组合，这里 $F[x]$ 是数域 F 上的多项式环。

解　作 6 阶矩阵

$$\boldsymbol{C}=\begin{bmatrix} x^3+3x^2+2x & 0 & 0 & 1 & 0 & 0 \\ x^3+x^2-2x & x^3+x^2-2x & 0 & 0 & 1 & 0 \\ x^3+2x^2-x-2 & 0 & x^3+2x^2-x-2 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}。$$

在 $F[x]$ 上，对矩阵 C 的前三行和前三列分别作行初等变换和列初等变换：

$$\boldsymbol{C}\xrightarrow{r_2+(-1)r_1,r_3+(-1)r_1} \begin{bmatrix} x^3+3x^2+2x & 0 & 0 & 1 & 0 & 0 \\ -2x^2-4x & x^3+x^2-2x & 0 & -1 & 1 & 0 \\ -x^2-3x-2 & 0 & x^3+2x^2-x-2 & -1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix} \xrightarrow{r_1+(\frac{1}{2}x+\frac{1}{2})r_2,r_3+(-\frac{1}{2})r_2}$$

$$\begin{bmatrix} 0 & \frac{1}{2}x^4+x^3-\frac{1}{2}x^2-x & 0 & -\frac{1}{2}x+\frac{1}{2} & \frac{1}{2}x+\frac{1}{2} & 0 \\ -2x^2-4x & x^3+x^2-2x & 0 & -1 & 1 & 0 \\ -x-2 & -\frac{1}{2}x^3-\frac{1}{2}x^2+x & x^3+2x^2-x-2 & -\frac{1}{2} & -\frac{1}{2} & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix} \xrightarrow{r_2+(-2x)r_3}$$

$$\begin{bmatrix} 0 & \frac{1}{2}x^4+x^3-\frac{1}{2}x^2-x & 0 & -\frac{1}{2}x+\frac{1}{2} & \frac{1}{2}x+\frac{1}{2} & 0 \\ 0 & x^4+2x^3-x^2-2x & -2x^4-4x^3+2x^2+4x & x-1 & x+1 & -2x \\ -x-2 & -\frac{1}{2}x^3-\frac{1}{2}x^2+x & x^3+2x^2-x-2 & -\frac{1}{2} & -\frac{1}{2} & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix} \xrightarrow{c_2+\frac{1}{2}(-x^2+x)c_1,\, c_3+(x^2-1)c_1}$$

$$\begin{bmatrix} 0 & \frac{1}{2}x^4+x^3-\frac{1}{2}x^2-x & 0 & -\frac{1}{2}x+\frac{1}{2} & \frac{1}{2}x+\frac{1}{2} & 0 \\ 0 & x^4+2x^3-x^2-2x & -2x^4-4x^3+2x^2+4x & x-1 & x+1 & -2x \\ -x-2 & 0 & 0 & -\frac{1}{2} & -\frac{1}{2} & 1 \\ 1 & \frac{1}{2}(-x^2+x) & x^2-1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix} \xrightarrow{r_1 \leftrightarrow r_3}$$

$$\begin{bmatrix} -x-2 & 0 & 0 & -\frac{1}{2} & -\frac{1}{2} & 1 \\ 0 & x^4+2x^3-x^2-2x & -2x^4-4x^3+2x^2+4x & x-1 & x+1 & -2x \\ 0 & \frac{1}{2}x^4+x^3-\frac{1}{2}x^2-x & 0 & -\frac{1}{2}x+\frac{1}{2} & \frac{1}{2}x+\frac{1}{2} & 0 \\ 1 & \frac{1}{2}(-x^2+x) & x^2-1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix} \xrightarrow{(-1)r_1,\, r_3+(-\frac{1}{2})r_2}$$

$$\begin{bmatrix} x+2 & 0 & 0 & \frac{1}{2} & \frac{1}{2} & -1 \\ 0 & x^4+2x^3-x^2-2x & -2x^4-4x^3+2x^2+4x & x-1 & x+1 & -2x \\ 0 & 0 & x^4+2x^3-x^2-2x & -x+1 & 0 & x \\ 1 & \frac{1}{2}(-x^2+x) & x^2-1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix} \xrightarrow{r_2+2r_3}$$

$$\begin{bmatrix} x+2 & 0 & 0 & \frac{1}{2} & \frac{1}{2} & -1 \\ 0 & x^4+2x^3-x^2-2x & 0 & -x+1 & x+1 & 0 \\ 0 & 0 & x^4+2x^3-x^2-2x & -x+1 & 0 & x \\ 1 & \frac{1}{2}(-x^2+x) & x^2-1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}。$$

所以 $(f(x), g(x), h(x)) = x+2$, $[f(x), g(x), h(x)] = x^4+2x^3-x^2-2x$，以及

$$\boldsymbol{U} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} & -1 \\ -x+1 & x+1 & 0 \\ -x+1 & 0 & x \end{bmatrix}, \boldsymbol{V} = \begin{bmatrix} 1 & \frac{1}{2}(-x^2+x) & x^2-1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

所以 $u_{11}=\frac{1}{2}$，$u_{12}=\frac{1}{2}$，$u_{13}=-1$，$v_{11}=1$，$v_{21}=v_{31}=0$，于是 $u_{11}v_{11}=\frac{1}{2}$，$u_{12}(v_{11}+v_{21})=\frac{1}{2}$，$u_{13}(v_{11}+v_{31})=-1$，则有 $x+2=\frac{1}{2}(x^3+3x^2+2x)+\frac{1}{2}(x^3+x^2-2x)+(-1)(x^3+2x^2-x-2)$。

注 2: 例 1、2 中 $r_i+br_j(c_i+bc_j)$ 表示将矩阵的第 j 行(第 j 列) 乘以 b 加到第 i 行(第 i 列); $ur_i(uc_i)$ 表示将矩阵的第 i 行(第 i 列) 乘以 u; $r_i\leftrightarrow r_j(c_i\leftrightarrow c_j)$ 表示将矩阵的第 i 行(第 i 列) 与第 j 行(第 j 列) 互换。

3　结语

本文探讨了欧氏环中元素的最大公因子和最小公倍，利用欧氏环上矩阵的初等变换同时求出多个元素的最大公因子和最小公倍，并将最大公因子表为这些元素的组合。这一方法对整数环 Z 和多项式环 $F[x]$ 中相应问题的解决具有指导意义。

参考文献:

[1] 陈祥恩，杨永保，程辉，等. 最大公因数的一种新求法[J]. 西北师范大学学报(自然科学版)，2002，38(4): 23 - 25.
[2] 刘汝臣. 求多项式最大公因式的矩阵方法[J]. 沈阳工业学院学报，2000，19(1): 89 - 94.
[3] 周立仁. n 个一元多项式的最大公因式的矩阵求法[J]. 湖南理工学院学报(自然科学版)，2004，17(4): 8 - 11.
[4] 张建奎. 多个整数的最小公倍数的矩阵求法[J]. 山东师范大学学报(自然科学版)，2006，21(6): 18 - 21.
[5] 王新民，孙霞. 多个多项式最小公倍式的一个实用求法[J]. 山东大学学报(理学版)，2007，42(10): 76 - 79.
[6] 高丽，任芳玲. 最小公倍式矩阵求法的推广[J]. 天津师范大学学报(自然科学版)，2008，28(1): 48 - 50.
[7] 张景晓. 欧式环上矩阵的广义初等变换及应用[J]. 重庆理工大学学报(自然科学版)，2010，24(8): 100 - 103.
[8] 王新民. 欧式环中多个元素的最小公倍子[J]. 烟台师范学院学报(自然科学版)，2003，19(2): 148 - 152.
[9] 王新民. 最大公因数与最小公倍数的矩阵求法[J]. 潍坊学院学报，2002，2(6): 42 - 44.
[10] 扎洛. 多项式的最大公因式和最小公倍式的矩阵求法[J]. 青海师范大学民族师范学院学报，2002，13(1): 50.
[11] 张建黛，王新民. 关于最小公倍式的矩阵求法[J]. 山东师范大学学报(自然科学版)，2003，18(4): 87 - 88.
[12] 李立. 求最小公倍式的矩阵变换法[J]. 齐齐哈尔大学学报，2010，26(2): 89 - 91.
[13] 苗嘉兴. 关于最小公倍式求法的讨论[J]. 理论数学，2019，9(4): 486 - 491.
[14] 王新民. 欧氏环中最大公因子与最小公倍子的统一求法[J]. 烟台师范学院学报(自然科学版)，2002，18(20): 141 - 144.
[15] JACOBSON N. Basic algebra I[M]. New York: W H Freeman and Company，1985.

A United Method for Findng Greatest Common Divisor and Least Common Multiple in a Euclidean Domain

CHEN Lingxiang，TAN Yijia

(College of Mathematics and Computer Science，Fuzhou University，Fuzhou 350108，China)

Abstract: The greatest common divisor and the least common multiple of a finite set of elements in a Euclidean domain were studied in this paper. With the elementary transformations on matrices，a unified method for finding the greatest common divisor and the least common multiple of a finite set of elements in a Euclidean domain was obtained.

Keywords: greatest common divisor; least common multiple; matrix; Euclidean domain

(责任编辑　顾建忠)