同余单矩阵半环

´ˇ˜´ˇ VITEZSLAV KALA、TOMAS KEPKA 和 MIROSLAV KORBELAR

Abstract. 众所周知，斜域上的全矩阵环是单环。我们将这一结论推广到半环的情形。对于矩阵半环 $\mathrm{M}_n(S)$（即半环 S 上所有 $n\times n$ 矩阵构成的半环），当 S 具有乘法吸收元，或 S 是交换且加法可消时，我们刻画其为同余单的条件。

arXiv:2303.06921v1 [math.RA] 13 Mar 2023

对那些在不存在任何非平凡同余意义下为单的代数结构进行分类，是代数的一项普遍目标。最著名的例子或许是有限单群的分类，而环的情形也已得到深入研究。韦德伯恩—阿廷定理从半单情形出发，以矩阵环的乘积刻画了这类结构。特别是众所周知，对于单环 R （无论是否含幺，但乘法非平凡），其全矩阵环 $\mathrm{M}_n(R)$（即环 R 上的方 $n\times n$ 矩阵构成的环）仍是单环。因此，例如，有理数 $\mathbb{Q}$ 上的全矩阵环是单环。

本文的总体目标是研究半环中的类似问题，即由两个结合运算 S 和 $+$ 组成的集合 $\cdot$，其中 $+$ 是交换的，且满足分配律。过去几十年来，半环日益受到关注，这尤其得益于它们在密码学和热带数学等领域的应用 [6, 9, 18, 19]。

对于乘法交换的情形，同余单半环的分类基本上已完成 [1], ，但正实数的子半环除外 $\mathbb{R}^+$。还值得简要指出的是，理想单的交换情形相当棘手 [11, 13]。

尽管已有一些部分结果 [2, 20]，非交换同余单半环 S 仍鲜为人知。特别是，一个基本分类定理 [2, 2.1] 表明， S 在加法下是可消去的、幂等的或幂零的（或者加法 $+$ 是平凡的），并且针对这些情形还有一些进一步的结果。尤其是，当 S 有限时，已知结果要多得多 [20]。不过，一般性的分类计划很可能极其困难，因此有必要先寻找种类广泛的例子和可能的构造。

矩阵半环再次展现出一类天然的单性候选对象。虽然半环上的矩阵的其他性质已有较为详细的研究（例如 [17, 22]），但与环的情形不同，我们尚未得到矩阵半环何时为单半环的刻画。即使对于 $\mathbb{Q}^+$——正有理数半环——的子半环，其相应的矩阵半环也尚未得到充分理解。

本文旨在填补这一空白。我们的主要结果是在以下假设下，刻画半环 $\mathrm{M}_n(S)$ 何时为同余单：

- S 有乘法吸收元（定理 2.5），或 - S 加法可消且向下有向（定理 4.6），或 - S 加法可消且交换（定理 4.7）。

我们的定理推广了 [14, 命题 5.5]，该命题讨论的是具有零元和单位元的半环情形。将讨论限制在同时具有这两个特殊元素的半环，通常可以得到类似于环情形的结果，例如韦德伯恩–阿廷定理 [14, 15] 的推广。此外，对于具有零元和单位元的半环，关于给定半环 T 何时同构于某个半环 S 上的全矩阵半环 $\mathrm{M}_n(S)$，也已有多种解答 [3, 7, 21] 。

Date: 2023年3月14日。2010 *Mathematics Subject Classification.* 06A12，16Y60，20M14。

Key words and phrases. 单半环，双吸收，半模，幂等，半格。第一作者获得捷克科学基金会（GAČR）项目 21-00420 M 以及查理大学研究中心计划 UNCE/SCI/022 的资助。第三作者感谢奥地利科学基金会（FWF）双边项目 I 4579-N 和捷克科学基金会（GAČR）项目 20-09869L“正交模性的诸多面向”提供的支持。

此外，半环 $\mathbf{M}_n(S)$ 与某个 S-半模的所有 S自同态之间众所周知的对应关系，恰好在这种情形下成立（参见例如命题 1.3）。

另一方面，这当然不是唯一值得关注的情形；没有零元或没有单位元的半环也值得研究（例如，$\mathbb{R}^+$ or 的子半环或某些格就说明了这一点）。本文的贡献主要针对这些更一般的半环情形。我们还给出了若干半环的例子（例 4.8），它们对应的矩阵半环是同余单的，但同时既没有零元也没有单位元。

1. 预备知识

本文所考虑的半环 S 是一个非空集合，配备两个结合的二元运算，通常记作加法 $+$ 和乘法 $\cdot$，其中加法满足交换律，乘法对加法满足左右分配律。

设 $S = S(+,\cdot)$ 是一个半环。对于 S 的子集 A, B，我们定义 $A + B = \{a + b \mid a \in A, b \in B\}$ 和 $AB = \{ab \mid a \in A, b \in B\}$。此外，我们将在 S 上使用标准拟序 $\leq_S$，其定义为：若 $a = b$，则 $a \leq_S b$；或者存在 $c \in S$ 使得 $a + c = b$。显然，$\leq_S$ 是传递的，并且相对于半环 S 的运算是稳定的。

I是 S的一个非空子集，若对任意 $a \in I, s \in S$，都有 $a + s, as, sa \in I$，则称其为 S的双理想。半环 S 上的同余是一个在加法和乘法下保持不变的等价关系。

半环 S 称为

若 S 恰有两个同余，则称其为• 同余单；
若 $|S| \geq 2$ 且对 S 的每个双理想 I，都有 $|I| = 1$ 或 $I = S$，则称其为• 双理想单；
若 $|S| \geq 2$ 且 S 的唯一双理想是其自身 S，则称其为• 双理想自由；
若半群 $S(\cdot)$ 是交换的，则称其为• 交换；
• 加法幂等，当且仅当 $a + a = a$ 对每个 $a \in S$；
• 加法可消，当且仅当 $a + c \neq b + c$对所有满足 $a \neq b$ 的 a、b、$c \in S$；
• 加法阿基米德，当且仅当对所有 a、$b \in S$，存在 $m \in \mathbb{N}$ 使得 $a \leq_S mb$；
• 加法（唯一）m-可除（对于 $m \in \mathbb{N}$），当且仅当对每个 $a \in S$，存在（唯一的）$b \in S$ 使得 $a = mb$。

元素 $w \in S$ 称为

• 乘法（分别为加法）吸收元，当且仅当对每个$a \in S$，$aw = w = wa$（分别为 $a + w = w$）；

• 若对每个 $a \in S$ 都有 $aw = a = wa$（分别为 $a + w = a$），则称其为单位元（加法中性元）；（单位元记作 1_S）；

• 若 w 同时是乘法吸收元和加法吸收元，则称其为双吸收元（这样的元素记作 o_S）；

• 若 w 是乘法吸收元且为加法中性元，则称其为零元（这样的元素记作 0_S）。

注意，元素 $w \in S$ 是双吸收元，当且仅当 $\{w\}$ 是双理想（因此 S 至多有一个平凡双理想）。

此外，对于 S 的每个双理想 I，关系 $(I \times I) \cup id_S$ 是 S 上的一个同余。因此，若 S 是同余单的，则 S 也是双理想单的。

关于半环的更多信息，参见例如 [8, 10]。

设 S 为半环且 $n \geq 1$。用 $\mathbf{M}_n(S)$ 表示由 S 中的元素构成的（方形）$n \times n$-矩阵在通常矩阵运算下形成的全矩阵半环：加法 $(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij})$ 和乘法 $(a_{ij})(b_{ij}) = (\sum_k a_{ik} b_{kj})$。

对于每个 $a \in S$，令 $\overline{a} = (a_{ij}) \in \mathbf{M}_n(S)$ 为满足对所有 i, j 均有 $a_{ij} = a$ 的矩阵。显然，$\overline{a} + \overline{b} = \overline{a + b}$ 且 $\overline{a}\,\overline{b} = n\overline{ab}$。因此，$\overline{S} = \{\overline{a} \mid a \in S\}$ 是 $\mathbf{M}_n(S)$ 的子半环。

首先，我们研究矩阵半环具有某些重要元素（单位元、零元、双吸收元或乘法吸收元）的情形。

命题 1.1. 设 S 为半环且 $n \geq 1$。那么对于 $T = \mathbf{M}_n(S)$，以下结论成立：

(i) $0_T \in T$ 当且仅当 $0_S \in S$。如果其中一个条件成立，那么 $0_T = \overline{0_S}$。(ii) $o_T \in T$ 当且仅当 $o_S \in S$。如果其中一个条件成立，那么 $o_T = \overline{o_S}$。

证明。(i) 设 $0_T = (\omega_{ij})$是 T中的一个零元。那么，对于每个 $A = (a_{ij})$， $\in T$都成立：$\omega_{ij} + a_{ij} = a_{ij}$ 对所有 i、j均成立。因此， $\omega_{ij} = \omega \in S$ 是 S中的一个加法中性元。

现在取 $b \in S$。由于 0_T 在 T中是乘法吸收的，因此对于每个满足 $b_{11} = b$ 且对所有 $(i, j) \neq (1, 1)$ 都有 $b_{ij} = \omega$ 的$B = (b_{ij}) \in T$，都有 $0_T \cdot B = 0_T$。于是 $\omega = \omega \cdot b + \omega \cdot \omega + \cdots + \omega \cdot \omega = \omega(b + \cdots + \omega) = \omega \cdot b$。通过对偶论证，我们得到对于每个 $b \in S$，都有 $\omega = b \cdot \omega$。因此， $\omega = 0_S$是 S中的零元。其余部分很容易。

(ii) 设 $o_T = (\omega_{ij}) \in T$。那么对于每个 $A = (a_{ij}) \in T$，对所有 i, j 都有 $\omega_{ij} + a_{ij} = \omega_{ij}$。因此，$\omega_{ij} = \omega \in S$ 在 S中是加法吸收的。

此外，对于每个 $b \in S$， $o_T \cdot \overline{b} = o_T$。因此 $\omega = \omega \cdot b + \cdots + \omega \cdot b = \omega(nb) = (n\omega) \cdot b = \omega \cdot b$。于是，$\omega$ 是左乘法吸收的。通过对偶论证，我们得到 ω 是右乘法吸收的。因此， $\omega = o_S$ 是 S 中的一个双吸收元。其余部分显而易见。□

P命题 1.2. 设 $n \geq 2$ 和 S 为半环。则下列条件等价：

(i) $\mathrm{M}_n(S)$ 有零元和单位元。(ii) $\mathrm{M}_n(S)$ 有单位元。(iii) S 有零元和单位元。

若其中一个条件成立，则 $T = \mathrm{M}_n(S)$ 的单位元 $1_T = (e_{ij})$ 具有如下形式： $e_{ii} = 1_S$，且 $e_{ij} = 0_S$ 对于 $i \neq j$。

证明。(i) 显然推出 (ii)，而由命题 1.1(i)，(iii) 推出 (i)。

(ii)⇒(iii)：设 $1_T = (e_{ij})$ 是一个单位元。对于 $1 \leq i \leq n$，令 $R_i = \{\sum_{j, j \neq i} e_{ij} a_j \mid a_j \in S\} \subseteq S$。显然，$R_i$ 是半环 S的右理想（即 $R_i \cdot S \subseteq R_i$ 且 $R_i + R_i \subseteq R_i$）。由于 1_T是 T的单位元，我们有：对于每个 i 以及所有 $a \in S$ 和 $u \in R_i$， $e_{ii}a + u = a$。因此，对于所有$a \in S$ 和 u， $a = e_{ii}a + u + v = a + v$， $v \in R_i$。于是， $w \in S$ 中存在一个加法中性元，且对于所有 i， $R_i = \{w\}$。因此， $\{w^2\} \subseteq wS = R_iS \subseteq R_i = \{w\}$，由此可得 $w^2 = w$ 和 $wS = \{w\}$。

同理， $L_j = \{\sum_{i, i \neq j} a_i e_{ij} \mid a_i \in S\}$是 S的左理想（即， $S \cdot L_j \subseteq L_j$且 $L_j + L_j \subseteq L_j$），通过对称论证可得，对于所有 j 和 $Sw = \{w\}$， $L_j = \{w\}$。这意味着 $w = 0_S$是 S中的零元。

最后，对于每个 i 以及所有 $a \in S$ 和 $v \in R_i = \{0_S\}$，有 $a = e_{ii}a + v$。因此， $a = e_{ii}a$。同理，$a = ae_{ii}$也成立。由此可得，对于每个 i， $e_{ii} = 1_S$ 都是 S 中的单位元。当然，对于 $i \neq j$，$e_{ij} = 0_S$。□

P命题 1.3. 设 $n \geq 2$ 和 S 为半环。则以下条件等价：

(i) 存在一个半环 R 和一个左 R-半模 ${}_RM$，使得半环 $\mathrm{End}({}_RM)$（由所有 ${}_RM$的R-自同态构成）与 $\mathrm{M}_n(S)$ 同构。 (ii) S 有零元和单位元。

证明。（i)⇒(ii)：由于半环 $\mathrm{End}({}_RM)$ 包含恒等映射 id_M，半环 $\mathrm{M}_n(S)$ 含有单位元。因此，根据命题 1.2， S 有零元和单位元。

(ii)⇒(i)：设 S 有零元和单位元。令 $R = S$ 和 $M = S \times \cdots \times S$（$n$ 次）。于是，左 S-半模 ${}_SM$是自由的，其自由基为 $e_1, \ldots, e_n$（具有标准形式）。因此，对于 ${}_SM$ 的每个 S-自同态 φ，都存在唯一的矩阵 $A \in \mathrm{M}_n(S)$，使得对于每个 $m \in {}_SM$， $\varphi(m) = m \cdot A$。由此可得 $\mathrm{End}({}_SM) \cong \mathrm{M}_n(S)$。□

命题 1.4。设 $n \geq 1$。则集合 $S_n = S + \cdots + S$（n 次）是 S 的一个双理想，且以下条件等价：

(i) $\mathrm{M}_n(S)$ 有乘法吸收元。(ii) S_n 有乘法吸收元（若 w 是这样的元素，则 $\overline{w}$ 是 $\mathrm{M}_n(S)$ 的乘法吸收元）。

此外，若 $S + S = S$，则 $S_n = S$ 及上述条件等价于条件

(iii) S 有乘法吸收元。

证明。(i)⇒(ii)：设 $W = (w_{ij})$ 是 $\mathrm{M}_n(S)$ 中的乘法吸收元。则对所有 a_1、.....、$a_n \in S$ 以及所有 i、j，都有 $w_{i1}a_1 + \cdots + w_{in}a_n = w_{ij}$。因此，对于 $k \neq j$，有 $w_{ik} = w_{i1}a_1 + \cdots + w_{in}a_n = w_{ij}$。于是， $w_{i1} = \cdots = w_{in} = w_i$且 $w_iS_n = \{w_i\}$。对偶地，对所有 i 以及 a_1、.....、$a_n \in S$，都有 $a_1w_1 + a_2w_2 + \cdots + a_nw_n = w_i$。因此， $w_1 = w_2 = \cdots = w$ 且 $wS_n = \{w\} = S_nw$。

其余蕴含关系都很容易证明。 □

2. Congruence-simple matrix semirings

本节将刻画含有乘法吸收元的同余单矩阵半环。这一结果将推广 [14, 命题 5.5]，其中假设半环同时具有零元和单位元。

我们先回顾一下文献 [2] 中关于同余单半环的基本性质。

引理 2.1。 [2, 引理 2.2] 设 S 是一个同余单半环，且满足 $|SS| \geq 2$。那么以下条件至少有一个成立：

(i) $|S| = 2$、 S 既是乘法幂等的，也是加法幂等的，并且 S 没有乘法吸收元。(ii) 对每个 a， $b \in S$ 满足 $a \neq b$，都存在 c、 $d \in S$，使得 $ca \neq cb$ 且 $ad \neq bd$。

命题 2.2。 [2, 命题 3.4] 设 S 是一个半环。若半环 $\mathrm{M}_n(S)$ 对某个 $n \geq 2$ 是同余单的，则：

(i) S 是同余单的。(ii) S 不含双吸收元。(iii) $|SS| \geq 2$。(iv) S 要么是加法幂等的，要么是加法可消的（因此 $|S + S| \geq 2$）。

定理 2.3。 [2, 定理 5.4] 设 S 是加法可消的同余单半环。

(i) 若 S 有加法中性元，则 S 是一个环。(ii) 若 S 有单位元，则 S 要么是一个环，要么 S 是交换的。

此外，以下引理很容易验证。

引理 2.4。设 S 是一个带零元 0_S 且 $n \geq 2$ 的半环。对于 i_0、 $j_0 \in \{1, \ldots, n\}$ 和 $a \in S$，我们用 $E_{i_0 j_0}(a) = (e_{ij}) \in \mathrm{M}_n(S)$ 表示一个矩阵，使得 $e_{i_0 j_0} = a$，且对于所有 $(i', j') \neq (i_0, j_0)$，都有 $e_{i'j'} = 0_S$。

以下结论对所有 $c, d \in S$, $i, j, k, \ell \in \{1, \ldots, n\}$ 和 $A = (a_{ef}) \in \mathrm{M}_n(S)$ 都成立：

(i) $E_{ij}(c) + E_{ij}(d) = E_{ij}(c + d)$。 (ii) $E_{ii}(c) \cdot E_{ij}(d) = E_{ij}(c \cdot d)$ 且 $E_{ij}(d) \cdot E_{jj}(c) = E_{ij}(d \cdot c)$。 (iii) $E_{ik}(c) \cdot A \cdot E_{\ell j}(d) = E_{ij}(c \cdot a_{k\ell} \cdot d)$。

现在给出我们的第一个结果。

定理 2.5. 设 S 为一个半环，并且对于某个 $k \geq 1$，半环 $\mathrm{M}_k(S)$ 有一个乘法吸收元。那么以下条件等价：

(i) 对每个 $n \geq 1$, $\mathrm{M}_n(S)$ 都是同余单的。 (ii) 至少存在一个 $n \geq 2$, 使得 $\mathrm{M}_n(S)$ 是同余单的。 (iii) S 是同余单的， S 不含双吸收元，并且 $|SS| \geq 2$。

如果满足这些条件之一，那么 S 有零元，并且 S 要么是环，要么是加法幂等的。

证明。 (i)⇒(ii)：显然。

(ii)⇒(iii)：利用命题 2.2。

(iii)⇒(i)：首先，我们证明 $|S + S| \geq 2$。反设 $S + S = \{u\}$ 对某个 $u \in S$成立。那么对每个 $a \in S$，都有 $au = a(u + u) = au + au = u$，类似地， $ua = u$也成立。因此， u 是一个双吸收元，矛盾。

因此， $|S + S| \geq 2$。现在，由于半环 S 是同余单的， S 也是双理想单的。由于集合 $S + S$ 是 S的一个非平凡双理想，故可得 $S + S = S$。根据命题 1.4，半环 S 有一个乘法吸收元 $w \in S$。

我们证明 w 是加法中性的。由于 w 是乘法吸收的，因此有 $w = w(w + w) = w^2 + w^2 = w + w$。显然， $S + w$ 是 S 和 $w = w + w \in S + w$ 的双理想。由于 S 是同余单的， S 也是双理想单的。因此，我们有 $S + w = S$ 或 $S + w = \{w\}$。后一种情况意味着 w 是双吸收的，由命题 2.2 可知， $S + w = S$ 成立。于是，对于每个 $a \in S$，都存在 $b \in S$ 使得 $a = b + w$。因此，对于每个 $a \in S$，都有 $a + w = b + w + w = b + w = a$，故 $w = 0_S$ 是零元。由命题 2.2， S 要么是加法可消的（因而由定理 2.3 可知是一个环），要么是加法幂等的。

现在设 ϱ 是 $T=\mathrm{M}_n(S)$ 的一个同余。在 S 上定义关系 σ：$(a,b)\in\sigma$ 当且仅当对于所有的对 (i,j)，都有 $(E_{ij}(a)\ E_{ij}(b))\in\varrho$。由引理 2.4(i) 和 (ii) 可容易推出，σ 是 S 上的一个半环同余。

现在假设 $\varrho\neq id_T$，即存在 A、$B\in T$，使得 $(A,B)\in\varrho$，并且对于某一对 (k,ℓ)，有 $a=a_{k\ell}\neq b_{k\ell}=b$。根据引理 2.1，存在 c、$d\in S$，使得 $cad\neq cbd$。现在，由引理 2.4 (iii)，可得

$$\big(E_{ij}(cad),E_{ij}(cbd)\big)=\big(E_{ik}(c)\cdot A\cdot E_{\ell j}(d),\ E_{ik}(c)\cdot B\cdot E_{\ell j}(d)\big)\in\varrho$$

对于所有的对 (i,j)。因此 $(cad,cbd)\in\sigma$，从而 $\sigma\neq id_S$。由于 S 是同余单的，我们得到 $\sigma=S\times S$。因此，对于 T 中所有的 $C=(c_{ij})$ 和 $D=(d_{ij})$，可得 $(C,D)=\Big(\sum_{i,j}E_{ij}(c_{ij})\sum_{i,j}E_{ij}(d_{ij})\Big)\in\varrho$，并由此得到 $\varrho=T\times T$。我们得出结论，T 是同余单的。□

在文献和应用中，带零元（并且可能带单位元）的半环十分常见。在这种情况下，定理 2.5 已完整给出了同余单矩阵半环的刻画。另一方面，不含此类特殊元素的半环（例如无界分配格或正实数的子半环）本身也很重要。

注 2.6. 带零元的同余单半环 S 不一定需要具有单位元。因此，定理 2.5 是对命题 5.5], 的恰当推广；后者假设零元和单位元都存在。

(i) 对于加法可消的情形（实际上就是环的情形），存在没有零因子且没有单位元的非交换单环（例如，参见 [4, 5]）。

（ii）对于加法幂等的情形，考虑如下情况。设 L 是一个半格，其最小元为 $\omega\in L$、最大元为 $\Omega\in L$，并且令 $|L|\geq 3$。设 $\mathrm{End}_\omega(L)$ 为所有保持 ω 的 L 自同态构成的半环。现在，半环 $S=\{\varphi\in\mathrm{End}_\omega(L)\mid \varphi(L)\text{ 是一个有限集}\}$，是 $\mathrm{End}_\omega(L)$ 的一个含零元的子半环。根据 [16, 命题 2. 7], ，半环 S 是同余单的，并且容易证明 S 含有零因子。

如果 L 是无限的，那么 S 不含单位元；如果 L 是有限的，那么 $S=\mathrm{End}_\omega(L)$ 有单位元，但存在没有（乘法）逆元的非零元。

根据命题 2.2，同余单矩阵半环分为两个互不相交且本质上不同的类别：一类是加法可消半环（即可嵌入环中的半环），另一类是加法幂等半环（例如见于逻辑、偏序结构或热带代数中）。

本文其余部分将致力于讨论前面提到的第一类情形——加法可消的情形。后一类情形将在后续文章中研究。

3. Bi-ideal-free matrix semirings

正如我们已经指出的，每个同余单半环都是双理想单的；事实上，关于同余单半环的性质往往可以利用其双理想单性推导出来。尤其是，在研究加法可消的同余单半环时，这一性质发挥着关键作用（见第 4 节）。本节从双理想单性（及双理想自由性）的角度，研究半环 S 与其矩阵半环 $\mathrm{M}_n(S)$之间的相互关系。

在本节中，设 S 为一个半环。

引理 3.1。设 I 是 $\mathrm{M}_n(S)$的一个双理想。则：

(i) $\overline{a}\in I$ 对至少一个 $a\in S$成立。(ii) 若 $a\in S$ 满足 $\overline{a}\in I$ 和 $a+S=S$，则 $I=\mathrm{M}_n(S)$。

证明. (i) 假设 $n\geq 2$，取 $A=(a_{ij})\in I$ 并令 $a=\sum_{i,j}a_{ij}$ 和 $b_{ij}=\sum_{(k,\ell)\neq(i,j)}a_{k\ell}$. 那么$A+B=\overline{a}$, 因此 $\overline{a}\in I$。

(ii) 若 $A=(a_{ij})\in I$，则对于某个 $b_{ij}\in S$，有 $a+b_{ij}=a_{ij}$。现在，$\overline{a}+B=A$，因此 $A\in I$。 □

引理 3.2. 设 $a\in S$。那么：

(i) 对所有 $C,D\in\mathrm{M}_n(S)$，存在 $c_1,\dots,c_n,d_1,\dots,d_n\in S$，使得 $(C\overline{a}D)_{ij}=c_iad_j$ 对所有 i, j 均成立。(ii) 设 $c_1,\dots,c_n,d_1,\dots,d_n\in S$，且 $F=(c_iad_j)\in\mathrm{M}_n(S)$。那么对于每个 $B\in\mathrm{M}_n(S)$, 存在$c'_1,\dots,c'_n,d'_1,\dots,d'_n\in S$，使得 $(BF)_{ij}=c'_iad_j$ 且 $(FB)_{ij}=c_iad'_j$ 对所有 i,j 均成立。

(iii) 此外，若 $S+S=S$，则对于所有 $c_1,\dots,c_n,d_1,\dots,d_n\in S$，存在 $C,D\in \mathbf{M}_n(S)$，使得 $(C\overline{a}D)_{ij}=c_iad_j$ 对所有 i,j 均成立。

证明. (i) 设 $C=(c_{ij})$ $D=(d_{ij})$ $\in \mathbf{M}_n(S)$。则 $(C\overline{a}D)_{ij}=\sum_{k,\ \ell}c_{ik}ad_{\ell j}=(\sum_k c_{ik})a(\sum_\ell d_{\ell j})=c_iad_j$ 对 $c_i=\sum_k c_{ik}$ 和 $d_j=\sum_\ell d_{\ell j}$。

(ii) 和 (iii)。设 $c_1,\dots,c_n,d_1,\dots,d_n\in S$ 和 $F=(c_iad_j)$ $\in \mathbf{M}_n(S)$。对于 $B=(b_{ij})$ $\in \mathbf{M}_n(S)$，令 $c'_i=\sum_k b_{ik}c_k$ 和 $d'_j=\sum_\ell d_\ell b_{\ell j}$。则 $(BF)_{ij}=\sum_k b_{ik}c_kad_j=(\sum_k b_{ik}c_k)ad_j=c'_iad_j$ 和 $(FB)_{ij}=\sum_\ell c_iad_\ell b_{\ell j}=c_ia(\sum_\ell d_\ell b_{\ell j})=c_iad'_j$。

此外，假设 $S+S=S$。那么，对于每个 $c_i\in S$，存在 $c_{ij}\in S$，使得 $c_i=\sum_j c_{ij}$。类似地，对于每个 $d_j\in S$，存在 $d_{ij}\in S$，使得 $d_j=\sum_i d_{ij}$。现在，对于 $C=(c_{ij})$ 和 $D=(d_{ij})$，有 $(C\overline{a}D)_{ij}=\sum_{k,\ \ell}c_{ik}ad_{\ell j}=(\sum_k c_{ik})a(\sum_\ell d_{\ell j})=c_iad_j$。□

现在，我们来引入并研究矩阵半环中某些重要双理想的性质。为此，令 $T=\mathbf{M}_n(S)$ 和 $a\in S$。我们设 $Q_a=T\cdot\overline{a}\cdot T+T$ 并

$$P_a=\{(a_{ij})\in T\mid \exists\, c_1,\dots,c_n,d_1,\dots,d_n\in S\ \ \forall i,j\ \ c_iad_j\le_S a_{ij}\}$$

我们用 R_a 表示由 $\overline{a}\in T$ 生成的 T 的双理想。

引理 3.3。令 $a\in S$。那么，$Q_a\subseteq P_a$ 和 $Q_a\subseteq R_a$，且集合 Q_a 和 P_a 是$T=\mathbf{M}_n(S)$ 的双理想。此外，若 $S+S=S$，则 $Q_a=P_a$。

证明。由引理 3.2(i)，$Q_a\subseteq P_a$。显然，$P_a+T\subseteq P_a$，并且由引理 3.2(ii)，$TP_a\subseteq P_a$ 和$P_aT\subseteq P_a$。因此，P_a 是 T的一个双理想。

假设 $S+S=S$，并令 $A=(a_{ij})\in P_a$。那么存在 $c_1,\dots,c_n,\ d_1,\dots,d_n\in S$，使得对所有 i,j，都有 $c_iad_j\le_S a_{ij}$。由于 $S+S=S$，存在 $e_1,\dots,e_n,f_1,\dots,f_n\in S$，使得对每个 i，都有 $c_i=e_i+f_i$。因此 $a_{ij}\ge_S c_iad_j=e_iad_j+f_iad_j$，从而存在 $M=(m_{ij})\in T$，使得对所有 i,j，都有$a_{ij}=e_iad_j+m_{ij}$。现在，由引理 3.2(iii)，存在 $E,D\in T$，使得$A=E\overline{a}D+M$。由此可得 $A\in Q_a$，进而得到 $Q_a=P_a$。□

引理 3.4. 设 $a\in S$。那么 $|Q_a|=1$ 当且仅当 S 有一个双吸收元 o_S，且 $S_naS_n+S=\{o_S\}$（见命题 1.4）。

证明。首先假设，对于某个 $W=(w_{ij})\in T=\mathbf{M}_n(S)$，有 $Q_a=\{W\}$。由于 Q_a 是 T 中基数为一的双理想，半环 T 有一个双吸收元。根据命题 1.1(ii)，半环 S 也有一个双吸收元 o_S，且对所有 i、j，都有 $w_{ij}=o_S$。现在，对 T 中所有的 $A=(a_{ij})$、$B=(b_{ij})$、$C=(c_{ij})$，都有 $A\overline{a}B+C=W$。因此可得，对所有 i、j，$o_S=w_{ij}=(\sum_k a_{ik})\ a\ (\sum_\ell b_{\ell j})+c_{ij}$。于是，$S_naS_n+S=\{o_S\}$。

逆命题很容易证明。□

现在我们可以转而关注 S 与 $\mathbf{M}_n(S)$ 中真双理想（不）存在之间的关系。

命题 3.5。假设 $n\ge 2$ 与 $\mathbf{M}_n(S)$ 是双理想单的。那么半环 S 是双理想自由的。

证明。设 I 是 S 的一个双理想。集合 $J=\{A=(a_{ij})\in T\mid a_{11}\in I\}$ 是 $T=\mathbf{M}_n(S)$ 的一个双理想。若$J=T$，则 $I=S$。若 $|J|=1$，则 $|I|=1, I=\{o_S\}$，其中 o_S 是双吸收的，并且由于 $n\ge 2$，我们有 $|S|=1$ 和 $S=\{o_S\}$。但这与 T 非平凡矛盾。□

命题 3.6。假设 S 是双理想自由的。那么：

(i) 若 I 是 $\mathbf{M}_n(S)$ 的双理想，则 $\overline{S}=\{\overline{b}\mid b\in S\}\subseteq I$。(ii) $\mathbf{M}_n(S)$ 存在最小双理想 J，且对于每个 $a\in S$，都有 $J=Q_a=R_a=P_a$。

证明。(i) 设 I 是 $\mathbf{M}_n(S)$ 的双理想。根据引理 3.1，$\overline{a}\in I$，其中 $a\in S$。令 $a'=n^2a$。集合 $Sa'S+S$ 是 S 的双理想，因此 $Sa'S+S=S$。若 $b\in S$ 是任意元素，则存在某些 c、d、$e\in S$，使得 $b=ca'd+e$。我们有 $\overline{b}=\overline{ca'd}+\overline{e}=\overline{n^2cad}+\overline{e}=n^2\overline{cad}+\overline{e}=\overline{c}\cdot\overline{a}\cdot\overline{d}+\overline{e}\in I$。由此证明了 $\overline{S}\subseteq I$。

(ii) 若 I 是 T的双理想，则由 (i) 可得 $\overline{S}\subseteq I$。因此，对每个 $a\in S$，都有 $R_a\subseteq I$ 和 $Q_a\subseteq I$。由于R_a 和 Q_a 都是双理想，因此对每个 $a\in S$，都有 $R_a=Q_a$，且此集合是T的最小双理想。最后，由于 S是双理想自由的，双理想 $S+S$ 等于 S。因此，根据引理 3.4，对每个 $a\in S$，都有 $Q_a=P_a$。□

命题 3.7。设 $n \geq 2$ 和 $|S| \geq 2$。则以下条件等价:

(i) 矩阵半环 $\mathrm{M}_n(S)$ 是双理想单的。(ii) 矩阵半环 $\mathrm{M}_n(S)$ 是双理想自由的。(iii) 对每个 $a \in S$, $Q_a = \mathrm{M}_n(S)$。(iv) $\forall\, a \in S\ \forall (a_{ij}) \in \mathrm{M}_n(S)\ \exists\, c_1, \ldots, c_n, d_1, \ldots, d_n \in S\ \ \forall i, j\ \ c_i a b_j \leq_S a_{ij}$。

若这些等价条件成立，则 S 是双理想自由的。

证明。(i)⇒(iii): 设 $a \in S$。若 $|Q_a| = 1$, 则根据引理 3.4, S 有一个双吸收元，这与命题 3.5 矛盾。现在, Q_a 是 T 的非平凡双理想，且 T 是双理想单的。因此，根据命题 3.5, $Q_a = T$，且 S 是双理想自由的。

(iii)⇒(ii): 设 I 是 T 的一个双理想。由引理 3.1, $\overline{a} \in I$ 对至少一个 $a \in S$ 成立。由于 I 是一个双理想，因此得到 $Q_a \subseteq I$。但这样一来, $I = T$。

(ii)⇒(i): 这是显然的。

(iii)⇒(iv): 由引理 3.3 立即可得。

(iv)⇒(iii): 设 $b \in S$，并考虑一个矩阵 $A = (a_{ij}) \in T$，使得 $a_{11} = b$。根据 (iv) 的假设，存在 c_1、$d_1 \in S$，使得 $c_1(b+b)d_1 \leq_S b$。因此 $b \in S+S$，从而可得 $S+S = S$。由于假设 (iv) 意味着对每个 $a \in S$，都有 $P_a = T$，由引理 3.3 可得，对每个 $a \in S$，都有 $Q_a = P_a = T$。□

推论 3.8. 设 n、k 为正整数，且 $n \geq k \geq 2$。若 $\mathrm{M}_n(S)$ 是双理想单的，则 $\mathrm{M}_k(S)$ 是双理想单的。

证明. 由命题 3.7(i) 和 (iv) 可立即得出。 □

可以注意到，命题 3.7 中的所有条件 (i)–(iv) 都取决于 n。但鉴于定理 2.5，自然会想到，对于所有 n，是否存在一个共同的等价条件。特别是，一个显而易见的问题随之而来：设 $n \geq 3$ 和 $\mathrm{M}_2(S)$ 都是双理想单的。那么 $\mathrm{M}_n(S)$ 是否也是双理想单的?

鉴于命题 3.5 以及紧接着的命题 3.9 和命题 3.10，很可能存在一个与命题 3.7 中条件 (i)–(iv) 等价的条件，其形式为

(v) S 是双理想自由的，并且对于所有 a、$b \in S$，都存在 $c \in S$，使得 $c \leq_S a$ 且 $c \leq_S b$。

以下命题对于证明我们在第 4 节中的主要结果至关重要。

命题 3.9. 设 S 是交换的，且对于某个 $n \geq 2$, $\mathrm{M}_n(S)$ 是双理想自由的。那么对于所有 a、$b \in S$，都存在 $c \in S$，使得 $c \leq_S a$ 且 $c \leq_S b$。

证明. 设 a、$b \in S$。根据引理 3.3，集合 P_{a+b} 是 $T = \mathrm{M}_n(S)$ 中的一个双理想。由于这个半环是双理想自由的，因此有 $P_{a+b} = T$。现在考虑一个矩阵 $A = (a_{ij}) \in T = P_{a+b}$，使得 $a_{11} = a_{22} = a$ 且 $a_{12} = a_{21} = b$。根据 P_{a+b} 的定义，存在 c_1、c_2、d_1、$d_2 \in S$，使得 $c_1(a+b)d_1 \leq_S a$、$c_2(a+b)d_2 \leq_S a$、$c_1(a+b)d_2 \leq_S b$ 且 $c_2(a+b)d_1 \leq_S b$。现在，令 $c = c_1c_2(a+b)d_1d_2$。由 S 的交换性可知, $c = c_1 \cdot c_2(a+b)d_2 \cdot d_1 \leq_S c_1 \cdot a \cdot d_1 \leq_S c_1(a+b)d_1 \leq_S a$，且 $c = c_1 \cdot c_2(a+b)d_1 \cdot d_2 \leq_S c_1 \cdot b \cdot d_2 \leq_S c_1(a+b)d_2 \leq_S b$。因此 $c \leq_S a$ 且 $c \leq_S b$。□

命题 3.10. 假设对所有的 $a, b \in S$，存在 $c \in S$，使得 $c \leq_S a$ 且 $c \leq_S b$。如果 S 是双理想自由的，那么 $\mathrm{M}_n(S)$ 是双理想自由的。

证明. 首先，集合 $S+S$ 是 S 的一个双理想。由于 S 是双理想自由的，因此 $S+S = S$。根据我们的假设，对所有的 $a, b \in S$，存在 $c \in S$，使得 $c \leq_S a$ 且 $c \leq_S b$。由于 $c \in S = S+S$，存在 $d, e \in S$，使得 $c = d+e$，因此 $a, b \in d+S$。通过归纳法，我们很容易得到，对于每个 $A \in T = \mathrm{M}_n(S)$，都存在 $d \in S$，使得 $A \in \overline{d} + T$。

现在，设 I 是 $\mathrm{M}_n(S)$ 的一个双理想。根据命题 3.6, $\overline{S} \subseteq I$。由证明的前一部分可知，对每个 $A \in T$，都存在 $d \in S$，使得 $A \in \overline{d} + T$。由此可得 $A \in \overline{d} + T \subseteq I$，因此$I = T$。所以 T 是双理想单的。□

命题 3.11. 设 S 是加法阿基米德的，并且对某个 $m \geq 2$, 加法上唯一 m-可除。那么对于所有 a、$b \in S$，存在 $c \in S$ 使得 $c \leq_S a$ 和 $c \leq_S b$。

证明。假设 S 满足这些条件。设 a、$b \in S$。取一个元素 $e \in S$。根据阿基米德性质，存在正整数 k_1 和 k_2，使得 $e \leq_S k_1 a$ 和 $e \leq_S k_2 b$。此外，存在 $\ell \geq 1$ 使得 $m^\ell \geq 1 + \max\{k_1, k_2\}$。因此，$e \leq_S k_1 a + a \leq m^\ell a$ 和 $e \leq_S k_2 b + b \leq_S m^\ell b$，并且存在 f_1、$f_2 \in S$ 使得 $e + f_1 = m^\ell a$ 和 $e + f_2 = m^\ell b$。

由于 S 是加法唯一 m可除的，变换 $\psi : x \mapsto m^\ell x$ 是 $S(+)$的一个自同构。因此，存在 c、d_1、$d_2 \in S$，使得 $m^\ell c = e$、$m^\ell d_1 = f_1$ 且 $m^\ell d_2 = f_2$。现在，等式 $m^\ell(c + d_1) = m^\ell a$ 和 $m^\ell(c + d_2) = m^\ell b$ 根据可除性唯一性可推出 $c + d_1 = a$ 和 $c + d_2 = b$。由此可得 $c \leq_S a$ 和 $c \leq_S b$。□

4. Congruence-simple matrix semirings – The additively cancellative case

回想一下，对于一个加法可消去半环 S，存在唯一的环 R（在同构意义下），它包含 S，且在具有这一性质的环中是最小的。这样的环称为差环，记作 $R = S - S$。注意，此时 $\mathbf{M}_n(S)$ 的差环是 $\mathbf{M}_n(R)$。

加法可消去半环 S 称为锥形的，若其差环 $R = S - S$ 是单的。
使用这一术语，可以表述如下重要的分类结果。

定理 4.1。 [2, 定理 5.1] 设 S 是加法可消去半环。那么，S 是同余单的，当且仅当满足以下三个条件：

(1) S 是锥形的，(2) S 是双理想单的，(3) S 是加法阿基米德的。

命题 4.2。设 S 是一个非环的同余单加法可消去半环。设 $R = S - S$ 是 S的差环。那么，在 R 上由 $r \leq s$ 定义的关系 $\leq$，对于 r、$s \in R$，当且仅当 $r = s$ 或 $s - r \in S$ 时成立，它是 R上的一个（偏）序。此外：

(i) $\leq$ 对 $S \times S$ 的限制为 $\leq_S$。(ii) 对所有 r、s、t、$u \in R$、$0 < u$，条件 $r \leq s$蕴含 $r + t \leq s + t$、$ru \leq su$和 $ur \leq us$。(iii) 对所有 r、$u \in R$、$0 < u$，存在 $n \in \mathbb{N}$ 使得 $r \leq nu$。

特别地，$(R, \leq)$ 是一个有序简单环。

证明。令 ϱ 表示标准拟序 $\leq_S$的核。也就是说，$(a, b) \in \varrho$ 当且仅当 $a = b$ 成立，或者 $a \in b + S$ 与 $b \in a + S$ 同时成立。显然，ϱ 是半环 S上的一个同余。若 $\varrho = S \times S$，则 S 是一个环，矛盾。因此 $\varrho \neq S \times S$，又由于 S 是同余单的，可得 $\varrho = id_S$，且拟序 $\leq_S$ 是半环 S上的一个序。因此，由序 $\leq_S$ 诱导的 R上的序 $\leq$ 具有如下形式：对于 r、$s \in R$，$r \leq s$ 当且仅当 $r = s$ 或 $s - r \in S$。由此，条件 (i) 和 (ii) 可由 $\leq_S$的性质轻易得出。最后，根据定理 4.1，条件 (iii) 由 S的阿基米德性质推出。□

注 4.3. 设 S 是一个非环的同余单加法可消去半环。令 $R = S - S$ 为 S 的差环，并取命题 4.2 中的序 $\leq$。注意，S 上的序 $\leq_S$ 总是向上有向的（因为有 $a, b \leq_S a + b$）。

现在，若假设对所有 $a, b \in S$，都存在 $c \in S$ 使得 $c \leq_S a$ 且 $c \leq_S b$（即，S 上的序 $\leq_S$ 是向下有向的），那么序 $\leq$ 在 R 上既向上有向又向下有向：

事实上，取 $r, s \in R$, $r = a - b$, $s = c - d$，其中 $a, b, c, d \in S$。则 $r, s \leq a + c$（$\in S$）。此外，$e \leq_S a, b$ 对某个 $e \in S$ 成立，因此 $t \leq r, s$，其中 $t = e -$（$b + d$）（$\in R$）。

接下来，我们来说明定理 4.1 中的性质在多大程度上适用于矩阵半环。

命题 4.4. 设 S 是一个半环。那么，矩阵半环 $\mathbf{M}_n(S)$ 是加法阿基米德的，当且仅当半环 S 也是如此。

证明. 若 S 是加法阿基米德的，且 $A, B \in T = \mathbf{M}_n(S)$，则存在 $c_{ij} \in S$ 和正整数 m_{ij}，使得 $a_{ij} + c_{ij} = m_{ij} b_{ij}$。令 $d_{ij} = c_{ij} + (m - m_{ij}) b_{ij}$，其中 $m = \max\{m_{ij} \mid i, j\} + 1$，则得到 $A + D = mB$。

反过来，若 T 是加法阿基米德的，且 $a, b \in S$，则对于某个正整数 k和矩阵 $C = (c_{ij})$，有 $\overline{a} + C = k\overline{b} \in T$。现在，$a + c_{ij} = kb$，因此 S是加法阿基米德的。□

命题 4.5. 设 S 是一个加法可消去半环。那么以下条件等价：

(i) 对每个 $n \geq 2$，$\mathrm{M}_n(S)$ 都是锥形的。
(ii) $\mathrm{M}_2(S)$ 是锥形的。(iii) S 是锥形的，
且 $|SS| \geq 2$。

证明。(i)⇒(ii)：显然。
(ii)⇒(iii)：假设条件 (ii) 成立。则差环 $\mathrm{M}_2(R) = \mathrm{M}_2(S) - \mathrm{M}_2(S)$ 是单的。由定理 2.5，差环 $R = S - S$ 是单的且 $RR \neq \{0_R\}$。因此，S 是锥形的，且$|SS| \geq 2$。

(iii)⇒(i)：假设条件 (iii) 成立。则差环 $R = S - S$ 是单的。若 $RR = \{0_R\}$，则 R 是有限的素数阶，因此 $S = R$ 且 $|SS| = 1$，矛盾。因此 $|RR| \geq 2$。于是，由定理 2.5，环 $\mathrm{M}_n(R) = \mathrm{M}_n(S) - \mathrm{M}_n(S)$ 是单的。这意味着半环 $\mathrm{M}_n(S)$ 是锥形的。□

现在我们可以证明关于同余单加法可消去矩阵半环的主要结果了。

定理 4.6. 设 S 是一个加法可消去半环。假设以下两个条件中至少有一个成立：

(a) 对所有 $a, b \in S$，存在 $c \in S$，使得 $c \leq_S a$ 且 $c \leq_S b$（即，序 $\leq_S$ 是向下有向的，参见注 4.3）。(b) 对某个 $m \geq 2$，S 是加法 m-可除的。

那么以下条件等价：
(i) 对每个 $n \geq 1$，$\mathrm{M}_n(S)$ 都是同余单的。(ii) 对至少一个 $n \geq 2$，$\mathrm{M}_n(S)$ 是同余单的。(iii) S 是同余单的，且 $|SS| \geq 2$。

证明。(i)⇒(ii)：显然。
(ii)⇒(iii)：由命题 2.2 得出。
(iii)⇒(i)：假设条件 (iii) 成立。对于 $k \geq 2$，定义 $S \times S$ 上的关系 ϱ_k：$(x, y) \in \varrho_k$ 当且仅当 $kx = ky$，则它是 S 上的半环同余。
若 $\varrho_k = S \times S$，则元素 $w = kx$ 是乘法吸收元（事实上，$yw = y(kx) = k(yx) = w$，类似地，$wy = w$ 对所有 $x, y \in S$ 均成立）。由于 S 可嵌入一个环且 $|S| \geq 2$，半环S 没有双吸收元。因此，由定理 2.5 可知，对于每个 $n \geq 1$，半环 $\mathrm{M}_n(S)$ 都是同余单的。
因此，假设对每个 $k \geq 2$，都有 $\varrho_k \neq S \times S$。由于 S 是同余单的，故对每个 $k \geq 2$，都有 $\varrho_k = id_S$。因此，如果对于某个 $m \geq 2$，S 在加法下是 m-可除的，那么 S 在加法下是唯一 m-可除的。

因此，根据命题 3.11 以及假设 (a) 或 (b)，可得对每个 a、$b \in S$，都存在 $c \in S$，使得 $c \leq_S a$ 且 $c \leq_S b$。

现在要证明，对于给定的 $n \geq 1$，半环 $\mathrm{M}_n(S)$ 是同余单的，我们需要验证定理 4.1 中的条件 (1)、(2) 和 (3)。
首先，由于 S 是同余单的，根据定理 4.1(1)，S 是锥形的。因此，由命题 4.5 可知，$\mathrm{M}_n(S)$ 也是锥形的。

此外，由于 S 可嵌入某个环，S 不含双吸收元，因此 S 的每个双理想至少含有两个元素。因此，鉴于半环 S 是双理想单的，根据定理 4.1(2)，可知 S 是双理想自由的。因此，由命题 3.10 可知，$\mathrm{M}_n(S)$ 是双理想自由的。

最后，由定理 4.1(3)，S 是加法阿基米德的。因此，根据命题 4.4，$\mathrm{M}_n(S)$也是加法阿基米德的。

由定理 4.1 可得，$\mathrm{M}_n(S)$是同余单的。□

当半环 S 是交换的时，我们可以将定理 4.6 中的刻画进一步精确化。

定理 4.7. 设 S 是加法可消去半环。假设以下两个条件中至少有一个成立：

(a) S 是交换的。
(b) S 有单位元或加法中性元。
那么，以下条件等价：

(i) 对每个 $n \geq 1$，$\mathrm{M}_n(S)$ 都是同余单的。(ii) 至少存在一个 $n \geq 2$，使得 $\mathrm{M}_n(S)$ 是同余单的。(iii) S 是同余单的，$|SS| \geq 2$ 并且对于所有 $a, b \in S$，都存在 $c \in S$，使得 $c \leq_S a$ 和 $c \leq_S b$。

证明。(i)⇒(ii)：显然。

(ii)⇒(iii)：由命题 2.2，S 是同余单的，且 $|SS| \geq 2$。假设条件 (a) 或 (b) 成立。设 $a, b \in S$。我们证明存在 $c \in S$，使得 $c \leq_S a$ 且 $c \leq_S b$。

如果 S 有加法中性元 $\omega \in S$，那么 $\omega \leq_S a$ 且 $\omega \leq_S b$。如果 S 没有加法中性元，那么 S 不是环；根据定理 2.3，半环 S 是交换的。现在，半环 $\mathrm{M}_n(S)$ 是双理想单的，并且根据命题 3.7，它也是双理想自由的。因此，根据命题 3.9，存在 $c \in S$，使得 $c \leq_S a$ 且 $c \leq_S b$。

(iii)⇒(i)：由定理 4.6 得出。 □

鉴于定理 4.6 和 4.7，我们提出以下猜想。

猜想：设 S 是加法可消去半环。那么，定理 4.7 中的条件 (i)、(ii) 和 (iii) 等价。

请注意，根据 [1, 定理 10.1], ，任何加法可消的同余单半环，只要它是交换的但不是环，都是正实数 $\mathbb{R}^+$ 的子半环。正如 [12], 所示，正有理数的半环 $\mathbb{Q}^+$ 含有不可数多个这样的子半环。对于 [12] 中找到的列表，目前仍不清楚它是否完整；而且，看来 $\mathbb{R}^+$ 的同余单子半环仍远未得到充分理解。

以下例子表明，$\mathbb{Q}^+$ 的许多同余单子半环都满足定理 4.7 中的条件 (iii)，因此，它们对应的矩阵半环提供了一大类非交换同余单半环的例子。

例 4.8 中的半环满足定理 4.6 和 4.7 中的假设 (a)，但不满足其中任何条件 (b)。此外，定理 2.5 不适用于这些半环。

例 4.8. 考虑有理数域的以下子半环 [12]

$$S = \{x \in \mathbb{Q}^+ \mid a^{v_p(x)} < x\}$$

其中 $0 < a < 1$ 是实数，p 是素数，且 $v_p : \mathbb{Q}^+ \to \mathbb{Z}$ p-进赋值。

这个半环 S 具有以下性质：

(i) S 是同余单的（见 [12,定理 2.16]）。(ii) S 既没有零元，也没有单位元。(iii) 对所有 $x, y \in S$，存在 $z_0 \in S$ 使得 $z_0 \leq_S x$ 和 $z_0 \leq_S y$。(iv) $\mathrm{M}_n(S)$是同余单的，且既没有零元，也没有单位元（使用定理 4.7 和命题1.1和1.2）。(v) 对任何 $m \geq 2$，S 都不是加法 m-可除的。

我们证明性质 (iii)。对于 $x, y \in S$，存在 $0 < \varepsilon \in \mathbb{R}$ 使得 $a^{v_p(x)} < x - \varepsilon$，且$a^{v_p(y)} < y - \varepsilon$。现在，存在 $k \in \mathbb{N}$ 使得 $k > v_p(x)$、$k > v_p(y)$ 且 $a^k < \varepsilon$。根据 [12, 引理 1.9]，集合 $\{z \in \mathbb{Q}^+ \mid v_p(z) = k\}$ 在 $\mathbb{Q}^+$ 中（在通常拓扑下）稠密。因此存在 $z_0 \in \mathbb{Q}^+$ 使得$a^k < z_0 < \varepsilon$，且 $v_p(z_0) = k$，由此我们得到 $z_0 \in S$。

此外，显然 $x - z_0 \in \mathbb{Q}^+$。由于 $v_p(z_0) > v_p(x)$，根据 p-进赋值的基本性质，我们得到 $v_p(x - z_0) = \min\{v_p(x) v_p(z_0)\} = v_p(x)$。因此 $a^{v_p(x-z_0)} = a^{v_p(x)} < x - \varepsilon < x - z_0$，从而可得 $x - z_0 \in S$，即 $z_0 \leq_S x$。用类似的论证可得 $z_0 \leq_S y$。

最后，我们证明性质 (v)。设 $m \geq 2$。只需找到 $x \in S$，使得 $\frac{x}{m} \notin S$。

我们有 $v_p(m) \geq 0$，因此$1 < \frac{m}{a^{v_p(m)}}$。现在，任取一个 $k \in \mathbb{Z}$。由此可得$a^k < a^k \frac{m}{a^{v_p(m)}} = m a^{k - v_p(m)}$，并根据稠密性论证（见上文），存在 $x \in \mathbb{Q}^+$，使得$a^k < x < m a^{k - v_p(m)}$，且 $v_p(x) = k$。因此 $x \in S$，又由于 $\frac{x}{m} < a^{v_p(x) - v_p(m)} = a^{v_p(x/m)}$，我们得到 $\frac{x}{m} \notin S$。

例4.9. 设 $S' = \mathrm{M}_k(S)$，其中 $k \geq 2$ 和 S 是例 4.8 中的半环。那么容易根据例 4.8 的性质验证，S' 是一个非交换的同余单半环，满足定理 4.6 中的假设(a)，但既不满足同一定理中的条件(b)，

也不满足定理 4.7 中的任何条件(a)或(b)。此外，定理 2.5 不适用于 S'。

注 4.10. 设 S 是有限加法可消去半环，且 $n \geq 2$。那么，$\mathrm{M}_n(S)$ 是同余单的，当且仅当对于某个有限域 $\mathbb{F}_q$ 和 $k \geq 1$，有 $S \cong \mathrm{M}_k(\mathbb{F}_q)$。

事实上，有限加法可消去半环 S 必定是一个环（因为有限可消半群必定是群）。若 $\mathrm{M}_n(S)$ 是同余单的，则根据定理 2.2，S 是同余单的，且 $|SS| \geq 2$。根据有限同余单半环的基本分类 [20, 定理 12]，以及文献 [2] 中所有二元素半环的列表，可知对于某个有限域 $\mathbb{F}_q$ 和 $k \geq 1$，有 $S \cong \mathrm{M}_k(\mathbb{F}_q)$。反向蕴含显然成立。

References

[1] R. El Bashir, J. Hurt, A. Jančařík, T. Kepka, *Simple commutative semirings*, 《代数杂志》236 (2001), 277–306. [2] R. El Bashir, T. Kepka, *Congruence-simple semirings*, 《半群论坛》75 (2007), 588–608. [3] I. I. Bogdanov, *Hidden matrix semirings*, 《数学科学杂志》135(5) (2006), 3276–3280. [4] P. M. Cohn, *On a class of simple rings*, *Mathematika* **5** (1958) 103–117. [5] P. M. Cohn, *Simple rings without zero-divisors, and Lie division rings*, *Mathematika* **6** (1959) 14–18. [6] M. Durcheva, *Semirings as Building Blocks in Cryptography*, 剑桥学者出版社, 2020. [7] J. S. Golan, *The Theory of Semirings with Applications in Mathematics and Theoretical Computer Science*, Pitman, 1991. [8] J. S. Golan, *Semirings and their Applications*, Kluwer Academic, 多德雷赫特, 1999. [9] I. Itenberg, G. Mikhalkin, E. Shustin, *Tropical Algebraic Geometry* (第 2 版), Birkh¨auser, 巴塞尔, 2009. [10] U. Hebisch, H. J. Weinert, *Semirings: Algebraic Theory and Applications in Computer Science*, World Sci. Publishing, 新加坡, 1998. [11] J. Jeˇzek, V. Kala, T. Kepka, *Finitely generated algebraic structures with various divisibility conditions*, 《数学论坛》24 (2012), 379–397. [12] V. Kala, M. Korbel´aˇr, *Congruence-simple subsemirings of* $\mathbb{Q}^+$, 《半群论坛》81 (2010), 286–296. [13] V. Kala, M. Korbel´aˇr, *Idempotence of finitely generated commutative semifields*, 《数学论坛》30 (2018), 1461–1474。[14] Y. Katsov, T. G. Nam, J. Zumbr¨agel, *On simpleness of semirings and complete semirings*, 《代数及其应用杂志》13(6) (2014), 29 页。[15] Y. Katsov, T. G. Nam, J. Zumbr¨agel, *On congruence-semisimple semirings and the K_0-group characterization of ultramatricial algebras over semifields*, 《代数杂志》**508** (2018) 157–195。[16] T. Kepka, J. Kortelainen, P. Nˇemec, *Simple semirings with zero*, 《代数及其应用杂志》15(3) (2016), 9 页。[17] A. Kendziorra, S. E. Schmidt, J. Zumbr¨agel, *Invertible matrices over finite additively idempotent semirings*, 《半群论坛》86 (2013), 525–536. [18] G. L. Litvinov, *The Maslov dequantization, idempotent and tropical mathematics: a brief introduction*, 载于：G. L. Litvinov, V. P. Maslov（编），《幂等数学与数学物理》，《当代数学》第 377 卷，美国数学会，2005 年，第 1–17 页。*Extended version at* arXiv:math/0507014. [19] G. Maze, C. Monico, J. Rosenthal, *Public key cryptography based on semigroup actions*, 《数学通信进展》1(4) (2007), 489–507. [20] C. Monico, *On finite congruence-simple semirings*, 《代数杂志》271 (2004), 846–854. [21] J. C. Robson, *Recognition of matrix rings*, 《代数通讯》19(7) (1991), 2113–2124. [22] Ya. Shitov, *A separation between tropical matrix ranks*, 《美国数学会会刊》151 (2023), 489–499.

Department of Algebra, Faculty of Mathematics and Physics, Charles University, Sokolovská 83, 186 75 Prague 8, Czech Republic*Email address*: vitezslav.kala@matfyz.cuni.cz

Department of Algebra, Faculty of Mathematics and Physics, Charles University, Sokolovská 83, 186 75 Prague 8, Czech Republic*Email address*: kepka@karlin.mff.cuni.cz

Department of Mathematics, Faculty of Electrical Engineering, Czech Technical University in Prague, Technická 2, 166 27 Prague 6, Czech Republic*Email address*: korbemir@fel.cvut.cz