arXiv:2303.14559v1 [math.AC] 25 Mar 2023

# 超域上的线性方程组、矩阵与向量空间

Kaique Matias de Andrade Roberto & Hugo Rafaelde Oliveira Ribeiro & Hugo Luiz Mariano & Kaique Ribeiro Prates Santos

2023年3月28日

**摘要**

受抽象二次型理论的一些最新进展启发，我们在本文中开始将线性代数扩展到多值结构（多代数结构本质上是一种赋有若干多值运算的代数结构）。我们引入并研究交换超环上的矩阵与行列式（粗略地说，交换超环是加法和乘法均为多值运算的环），并研究超域上的线性方程组与向量空间。作为应用，我们获得了一个对于发展超域代数扩张理论至关重要的结果。

## 引言

受抽象二次型理论近期发展的启发，我们从 [12] 开始研究超域的代数扩张；与此相关，我们也着手拓展线性代数，使之适用于多值结构：本研究的目标正是呈现这一部分内容。

多代数结构的概念——一种“类似代数”的结构，但具有某些多值运算——自 20 世纪 30 年代以来便受到研究；尤其是，Krasner 于 20 世纪 50 年代引入了超环的概念：它本质上是带有多值加法运算的环。同理，多环（[25] 本质上是具有多值加法但满足宽松分配律的环）和超环（[4]）大致上是加法与乘法均为多值运算的环。关于多重代数的一般代数研究已有一些成果：例如参见 [20] 和 [30]。

自2000年代中期以来，多环这一概念受到越来越多的关注：多环是一种满足弱分配律的宽松超环，而超域与多域则彼此相同。多环已在许多领域的应用中得到研究：包括抽象二次型理论（[25], [19], [13]）、热带几何（[31], [22]）、代数几何（（[24], [7]）、赋值理论（[23]）、Hopf代数（[18]）等（[6], [2], [3], [8]）。关于超环上的多项式这一概念的各种变体，更为详细的论述则是近来才出现的：参见 [22], [4], [7], 和 [15]。

我们简要介绍本文的结构：第 1 节介绍多环、超环和多项式超环的预备知识。第 2 节引入并研究交换超环上的矩阵和行列式。第 3 节研究超域上线性方程组。第 4 节展示前文所述内容的一项应用：通过添加不可约多项式的一个根，我们得到超域的一个简单代数扩张（定理 4.12）；这是发展超域代数扩张理论的一项基础性结果。第 5 节迈出了建立超域上向量空间理论的第一步。最后，我们在第 6 节提出一些展望。

# 1 预备知识

## 1.1 多结构

{defn:multimo

**定义 1.1** （改编自 [25]中的定义 1.1）。**多群**是一种一阶结构$(G,\cdot,r,1)$，其中 $G$ 是一个非空集合， $r\colon G\to G$ 是一个函数，1 是 $G$ 的一个元素， $\cdot\subseteq G\times G\times G$ 是一个三元关系（它将发挥二元多运算的作用，我们用 $d\in a\cdot b$ 表示$(a,b,d)\in\cdot$） ，使得对于所有 $a,b,c,d\in G$:

**M1 -** 若 $c\in a\cdot b$，则 $a\in c\cdot(r(b))\wedge b\in(r(a))\cdot c$。我们记 $a\cdot b^{-1}$，以简化 $a\cdot(r(b))$ 。**M2 -** $b\in a\cdot 1$ 当且仅当 $a=b$。

**M3 -** 若 $\exists x(x\in a\cdot b\wedge t\in x\cdot c)$，则 $\exists y(y\in b\cdot c\wedge t\in a\cdot y)$。

**M4 -** $c\in a\cdot b$ 当且仅当 $c\in b\cdot a$。

结构 $(G,\cdot,r,1)$ 若对所有 $a,b,c\in G$ 满足条件，则称为**交换的（或阿贝尔的）**

**M4 -** $c\in a\cdot b$ *iff* $c\in b\cdot a$.

结构 $(G,\cdot,1)$ 若满足 *M3*、*M4* 以及条件 $a\in 1\cdot a$ （对所有 $a\in G$），则称为**交换多幺半群（含幺元）**。

{defn:multiri

**定义 1.2** （改编自 [25]中的定义 2.1）。 多环是一个六元组 $(R,+,\cdot,-,0,1)$ 其中$R$ 是一个非空集合， $+\colon R\times R\to\mathcal{P}(R)\setminus\{\emptyset\}$、 $\cdot\colon R\times R\to R$ 和 $-\colon R\to R$ 是函数，0 和 1 是 $R$ 的元素，满足:

*i* - $(R,+,-,0)$ 是一个交换多群;

*ii* - $(R,\cdot,1)$ 是一个交换幺半群;

*iii* - $a.0=0$ 对所有 $a\in R$;

*iv* - 如果 $c\in a+b$，那么 $c.d\in a.d+b.d$。或者等价地，$(a+b).d\subseteq a.d+b.d$。

注意，如果 $a\in R$，那么 $0=0.a\in(1+(-1)).a\subseteq 1.a+(-1).a$，因此 $(-1).a=-a$。

如果 $R$满足 $a,b,c\in R$, $a(b+c)=ab+ac$，则称其为超环。

若一个多环（分别地，超环） $R$ 没有零因子，则称其为多整环（超整环）。若 $R$ 中的每个非零元素都有乘法逆元，则多环 $R$ 称为多域；注意，超域与多域是相同的。

{ex:1.3}

**例 1.3.**

*a* - 假设$(G,\cdot,1)$ 是一个群。定义 $a*b=\{a\cdot b\}$ 和 $r(g)=g^{-1}$，则$(G,*,r,1)$ 是一个多群。由此，每个环、整环和域分别都是多环、多整环和多域。

*b* - 设 $K=\{0,1\}$ 配备通常乘法，加法由关系 $x+0=0+x=x$、 $x\in K$和 $1+1=\{0,1\}$定义。这是一个称为 *Krasner* 多域 *[22]*的多域。

*c* - $Q_2=\{-1,0,1\}$ 是“信号”多域，采用通常乘法（在 $\mathbb{Z}$ 中），多值加法由以下关系定义

$$\begin{cases}0+x=x+0=x,\ for\ every\ x\in Q_2\\ 1+1=1,\ (-1)+(-1)=-1\\ 1+(-1)=(-1)+1=\{-1,0,1\}\end{cases}$$

{tropical-ex}

**例1.4 (**热带超域 [31])。 对于一个固定的全序阿贝尔群$(G,+,-,0,\leq)$，我们可以构造一个热带多域 $T_G=(G\cup\{\infty\},\otimes,\odot,\ominus,0,1)$，其中:

*i* - $\forall g \in G,\ g < \infty$;

*ii* - $g \otimes h := g + h$;

*iii* - $0 := \infty$;

*iv* - $1 := 0$;

*v* - $\forall g \in G,\ g^{-1} = -g$;

*vi* - *if* $g \neq h,\ g \oplus h = \{min\{g, h\}\}$;

*vii* - $g \oplus g = \{h \in G \cup \{\infty\} : g \leq h\}$;

*viii* - $\ominus g = g$.

在该序列中，我们给出一些对前面例子进行推广的例子。

{H-多元}

**例 1.5** (H-多域，[16]中的例 2.8)。令 $p \geq 1$ 为一个素数，且 $H_p := \{0, 1, ..., p-1\} \subseteq \mathbb{N}$。现在，定义 $H_p$ 中的二元多运算和运算如下：

$$a + b = \begin{cases} H_p \ \textit{if } a = b,\ a, b \neq 0 \\ \{a, b\} \ \textit{if } a \neq b,\ a, b \neq 0 \\ \{a\} \ \textit{if } b = 0 \\ \{b\} \ \textit{if } a = 0 \end{cases}$$

$$a \cdot b = k \ \textit{where } 0 \leq k < p \ \textit{and } k \equiv ab \ \textit{mod } p.$$

$(H_p,\ +,\ \cdot,\ -,\ 0,\ 1)$ 是一个超域，使得对所有的 $a \in H_p$，$-a = a$ 都成立。事实上，这些 $H_p$ 是 $K$ 的一种推广，其意义在于 $H_2 = K$。

{kaleid}

**例 1.6** （万花筒，[16] 中的例 2.7）。令 $n \in \mathbb{N}$ 并定义

$$X_n = \{-n, ..., 0, ..., n\} \subseteq \mathbb{Z}.$$

我们将 $n$-**kaleidoscope 多环**定义为 $(X_n,\ +,\ \cdot,\ -,\ 0,\ 1)$，其中 $-:\ X_n \to X_n$ 是 $\mathbb{Z}$ 中相反映射在 $+$ 上的限制，$+:\ X_n \times X_n \to \mathcal{P}(X_n) \setminus \{\emptyset\}$ 由以下规则给出：

$$a + b = \begin{cases} \{a\},\ \textit{if } b \neq -a \ \textit{and } |b| \leq |a| \\ \{b\},\ \textit{if } b \neq -a \ \textit{and } |a| \leq |b| \\ \{-a, ..., 0, ..., a\} \ \textit{if } b = -a \end{cases},$$

且 $\cdot:\ X_n \times X_n \to X_n$ 由以下规则给出：

$$a \cdot b = \begin{cases} sgn(ab) \max\{|a|, |b|\} \ \textit{if } a, b \neq 0 \\ 0 \ \textit{if } a = 0 \ \textit{or } b = 0 \end{cases}.$$

根据上述规则，$(X_n,\ +,\ \cdot,\ -,\ 0,\ 1)$ 是一个多环，但不是超环，因为 $n \geq 2$

$$n(1 - 1) = b \cdot \{-1, 0, 1\} = \{-n, 0, n\}$$

以及 $n - n = X_n$。注意，$X_0 = \{0\}$ 和 $X_1 = \{-1, 0, 1\} = Q_2$。

**例 1.7** (线性序的多群，[31]中的 3.4)。设$(\Gamma, \cdot, 1, \leq)$ 是一个有序阿贝尔群。我们有相应的超域结构$(\Gamma \cup \{0\}, +, -, \cdot, 0, 1)$，其运算规则为 $-a := a$, $a \cdot 0 = 0 \cdot a := 0$以及

$$a + b := \begin{cases} a \ \textit{if } a < b \\ b \ \textit{if } b < a \\ [0, a] \ \textit{if } a = b \end{cases}$$

这里我们约定，对于所有 $a \in \Gamma,\ 0 \leq a$。

现在我们来讨论态射：

{defn:morphis

**Defi定义 1.8.** 设 $A$和 $B$为多环。映射 $f:\ A \to B$是一个态射，当且仅当对所有 $a, b, c \in A$ :

*i* - $f(1) = 1$和 $f(0) = 0$;

*ii* - $f(-a) = -f(a)$;

*iii* - $f(ab) = f(a)f(b)$;

*iv* - $c \in a + b \Rightarrow f(c) \in f(a) + f(b)$.

态射 $f$ 称为**满态射**，如果对所有 $a$，$b \in A$,

$$f(a + b) = f(a) + f(b) \ and \ f(a \cdot b) = f(a) \cdot f(b).$$

**例1.9**。

*i* - 交换环的素理想（其扎里斯基谱）由到代数闭域的态射的等价类分类，但它们也可以通过到 *Krasner* 多域 $K = \{0, 1\}$ 的多环态射进行统一分类。

*ii*- 交换环的序（其实谱）由到实闭域的环同态的等价类分类，但它们也可以通过到信号多域 $Q_2 = \{-1, 0, 1\}$ 的多环态射进行统一分类。

*iii* - 具有值群$(G, +, -, 0, \leq)$的交换环上的 *Krull* 赋值，就是到多域 $T_G = G \cup \{\infty\}$ 的一个态射。

超环这一概念最早见于（[4]）。多环/超环理论已有许多重要进展和成果，例如，我们推荐阅读以下论文： [1], [3], [4], [2], [26], [29], [28], [27]。

**定义1.10** (定义 5，见 [4])。 超环是一个结构 $(S, +, \cdot, -, 0, 1)$，满足：

*i* - $(S, +, -, 0)$ 是一个交换多群。

*ii* - $(S, \cdot, 1)$ 是一个多幺半群。

*iii* - 0 是一个吸收元： $a \cdot 0 = \{0\} = 0 \cdot a$，对所有 $a \in S$ 均成立。

*iv* - 弱/半分配律成立：若 $d \in c.(a + b)$ 且 $e \in (a + b)c$，则 $d \in ca + cb$ 且 $e \in ac + bc$，对所有 $a, b, c, d, e \in S$ 均成立。

*v* - 符号规则成立： $-(ab) = (-a)b = a(-b)$，对所有 $a, b \in S$。

若$(S, \cdot, 1)$ 是交换的，则称超环为交换的。在此新背景下，超整环是一个非平凡且没有零因子的超环，也就是说，每当

$$0 \in a \cdot b \ iff \ a = 0 \ or \ b = 0$$

准超域是一个非平凡超环，其中每个非零元素在此新背景下都是可逆的[1],也就是说，每当

$$For \ all \ a \neq 0 \ exists \ b \ such \ that \ 1 \in a \cdot b.$$

超域是同时也是超整环的准超域。若对所有 $a, b, c, d \in S$,$d \in c \cdot (a + b)$，当且仅当 $d \in ca + cb$，则称超环为满的。

从现在起，所有超环都将是交换的（另有说明者除外）。

现在我们来讨论态射。

**定义 1.11.** 设 $A$ 和 $B$ 为超环。映射 $f \colon A \to B$ 是一个态射，当且仅当对所有 $a, b, c \in A$:

[1]对于准超域 $F$，我们**不要求**$(S \setminus \{0\}, \cdot, 1)$ 是一个交换多群，即如果 $d \in a \cdot b$，则 $b^{-1} \in a \cdot d^{-1}$。

*i* - $f(0)=0$;

*ii* - $f(1)=1$;

*iii* - $f(-a)=-f(a)$;

*iv* - $c\in a+b\Rightarrow f(c)\in f(a)+f(b)$;

*v* - $c\in a\cdot b\Rightarrow f(c)\in f(a)\cdot f(b)$.

态射 $f$ 是**满态射**，当且仅当对所有 $a,b\in A$,

$$f(a+b)=f(a)+f(b)\ and\ f(a\cdot b)=f(a)+f(b).$$

从现在起，我们采用以下约定：设 $(R,+,\cdot,-,0,1)$ 为一个超环， $p\in\mathbb{N}$ 并考虑一个 $p$ 元组 $\vec{a}=(a_0,a_1,...,a_{p-1})$。我们将有限和定义为：

$$x\in\sum_{i<0}a_i \text{ iff } x=0,$$
$$x\in\sum_{i<p}a_i \text{ iff } x\in y+a_{p-1} \text{ for some } y\in\sum_{i<p-1}a_i, \text{if } p\geq 1.$$

并将有限积定义为：

$$x\in\prod_{i<0}a_i \text{ iff } x=1,$$
$$x\in\prod_{i<p}a_i \text{ iff } x\in y\cdot a_{p-1} \text{ for some } y\in\prod_{i<p-1}a_i, \text{if } p\geq 1.$$

因此，若 $(\vec{a}_0,\vec{a}_1,...,\vec{a}_{p-1})$ 是由元组 $\vec{a}_i=(a_{i0},a_{i1},...,a_{im_i})$ 构成的一个 $p$ 元组，则有限积的有限和为：

$$x\in\sum_{i<0}\prod_{j<m_i}a_{ij} \text{ iff } x=0,$$
$$x\in\sum_{i<p}\prod_{j<m_i}a_{ij} \text{ iff } x\in y+z \text{ for some } y\in\sum_{i<p-1}\prod_{j<m_i}a_{ij} \text{ and } z\in\prod_{j<m_{p-1}}a_{p-1,j}, \text{if } p\geq 1.$$

{lembasic1}

**引理 1.12** (基本事实)。 设 $A$ 为一个超环。

***a*** - 对所有 $n\in\mathbb{N}$ 以及所有 $a_1,...,a_n\in A$，和 $a_1+...+a_n$ 与积 $a_1\cdot...\cdot a_n$ 不依赖于各项的顺序。

***b*** - 如果 $A$ 是满超整环，那么对于某个 $a\neq 0$， $ax=ay$ 蕴含 $x=y$。

***c*** - 如果 $A$ 是满的，那么对于所有 $d,a_1,...,a_n\in A$

$$d(a_1+...+a_n)=da_1+...+da_n.$$

***d*** - 设 $A$ 是满超整环，并令 $a\in A\setminus\{0\}$。如果 $1\in(a\cdot b)\cap(a\cdot c)$ 那么 $b=c$。

***e*** - （牛顿二项式公式）对于 $n\geq 1$ 和 $X\subseteq A$， 记作

$$nX:=\sum_{i=1}^{n}X.$$

那么对于 $A$， $B\subseteq A$,

$$(A+B)^n\subseteq\sum_{j=0}^{n}\binom{n}{j}A^jB^{n-j}.$$

{factstrong2}

**引理 1.13** （关于超环满态射的事实）。 设 $f:\ A\to B$ 是一个超环满态射。那么

*a* - 对所有 $a_1,...,a_n \in A$,

$$f(a_1 + ... + a_n) = f(a_1) + ... + f(a_n).$$

*b* - 对所有 $a_1,...,a_n, b_1,...,b_n \in A$,

$$f[(a_1 + b_1)(a_2 + b_2)...(a_n + b_n)] = (f(a_1) + f(b_1))(f(a_2) + f(b_2))...(f(a_n) + f(b_n)).$$

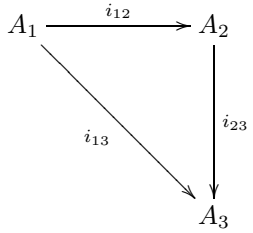
*c* - 对所有 $c_1,...,c_n, d_1,...,d_n \in A$,

$$f(c_1d_1 + c_2d_2 + ... + c_nd_n) = f(c_1)f(d_1) + f(c_2)f(d_2) + ... + f(c_n)f(d_n).$$

*d* - 对所有 $a_0,...,a_n, \alpha \in A$,

$$f(a_0 + a_1\alpha + ... + a_n\alpha^n) = f(a_0) + f(a_1)f(\alpha) + ... + f(a_n)f(\alpha)^n.$$

*e* - 设 $A_1, A_2, A_3$ 是超环，且有单态射（嵌入） $i_{12}$： $A_1 \to A_2$、 $i_{13}$： $A_1 \to A_3$ 和 $i_{23}$： $A_2 \to A_3$。




假设 $i_{13} = i_{23} \circ i_{12}$ 是满嵌入。若 $i_{23}$ 是满嵌入，则 $i_{12}$ 是满嵌入。

{char}

**定义 1.14**。

*i* - 超环的**特征** 是满足以下条件的最小整数 $n \geq 1$

$$0 \in \sum_{i<n} 1,$$

否则，特征为零。对于满超整环，这等价于说， $n$ 是满足以下条件的最小整数

$$For\ all\ a,\ 0 \in \sum_{i<n} a.$$

*ii* - 一个*i* **理想** 是超环 $A$ 的非空子集 $\mathfrak{a}$，满足 $A$、 $\mathfrak{a}+\mathfrak{a} \subseteq \mathfrak{a}$ 和 $A\mathfrak{a} \subseteq \mathfrak{a}$。我们记 *te*

$$\mathfrak{I}(A) = \{I \subseteq A : I\ is\ an\ ideal\}.$$

*iii* - 设 $S$ 是超环 $A$的一个子集。我们将由 $S$ **生成的理想**定义为

$$\langle S\rangle := \bigcap\{\mathfrak{a} \subseteq A\ ideal : S \subseteq \mathfrak{a}\}.$$

如果 $S = \{a_1, ..., a_n\}$，我们很容易验证

$$\langle a_1, ..., a_n\rangle = \sum Aa_1 + ... + \sum Aa_n,\ where\ \sum Aa = \bigcup_{n\geq 1}\{\underbrace{Aa + ... + Aa}_{n\ times}\}.$$

注意，如果 $A$ 是满超环，那么 $\sum Aa = Aa$。

*iv* - 若理想 $\mathfrak{p}$ 属于 $A$，且满足 $1 \notin \mathfrak{p}$ 和 $ab \subseteq \mathfrak{p} \Rightarrow a \in \mathfrak{p}$ 或 $b \in \mathfrak{p}$，则称其为**素**。我们记 *e*

$$Spec(A) = \{\mathfrak{p} \subseteq A : \mathfrak{p}\ is\ a\ prime\ ideal\}.$$

*v - An i* 理想 $\mathfrak{p}$ 属于 $A$，且满足 $1 \notin \mathfrak{p}$ 和 $ab \cap \mathfrak{p} \neq \emptyset \Rightarrow a \in \mathfrak{p}$ 或 $b \in \mathfrak{p}$，则称其为**强素**。我们记 $te$

$$Spec_s(A) = \{\mathfrak{p} \subseteq A : \mathfrak{p} \textit{ is a strongly prime ideal}\}.$$

注意，每个强素理想都是素理想。

*vi* - 若理想 $\mathfrak{m}$ 是极大的，则它是正理想，且对于所有满足 $\mathfrak{m} \subseteq \mathfrak{a} \subseteq A$ 的理想 $\mathfrak{a}$，都有 $\mathfrak{a} = \mathfrak{m}$ 或 $\mathfrak{a} = A$。

*vii* - 对于理想 $I \subseteq A$，我们在商 $A/I = \{x + I : x \in A\} = \{\overline{x} : x \in A\}$ 中定义运算，规则如下

$$\overline{x} + \overline{y} = \{\overline{z} : z \in x + y\}$$
$$\overline{x} \cdot \overline{y} = \{\overline{z} : z \in xy\}$$

对于所有 $\overline{x}$, $\overline{y} \in A/I$。

**注 1.15**。

*a* - 如果 $A$ 是一个多环，那么每个素理想都是强素理想。我们不知道一般超环是否也如此。

*b* - 如果 $A$ 是一个多环，那么每个极大理想都是素理想（*[?]* 的命题 *1.7*）。对于一般超环 $A$，我们不知道极大理想是否为素理想。

*c* - *H. Ribeiro* 在其博士论文 *[?]*, 中讨论了多环 $A$ 上的弱可逆元素 weaklyinvertible 。这或许可以作为处理上述问题的一种替代方法。

根据上述所有约定和记号，我们得到下面的引理，它将环（以及多环）中成立的一些性质推广到了超环。

{lem1}

**引理 1.16**。设 $A$ 是一个超环， $I$ 是一个理想。

*i* - $I = A$ 当且仅当 $1 \in I$。

*ii* - $A/I$ 是一个超环。此外，如果 $A$ 是满的，那么 $A/I$ 也满。

*iii* - $I$ 是强素的，当且仅当 $A/I$ 是超整环。

如果 $A$ 是满的，那么

*iv* - $I = A$ 当且仅当 $1 \in I$，这又当且仅当 $A^* \cap I \neq \emptyset$ （换句话说，当且仅当 $I$包含一个可逆元）。

*v* - $A$ 是超域，当且仅当 $\mathfrak{I}(A) = \{0, A\}$。

*vi* - $I$ 是极大的，当且仅当 $A/I$ 是超域。

**命题 1.17.** 设 $A$ 是一个超环， $I$ 是一个理想。

*i* - 如果 $I$ 是一个极大理想，那么它就是素理想。*ii* - 理想 $I$ 是素理想，当且仅当 $A/I$ 是拟超整环[2]。

*iii* - （素理想定理）设 $S \subseteq A$ 是一个乘法集（$1 \in S$ 和 $S \cdot S \subseteq S$）。假设$S \cap I = \emptyset$。那么存在一个素理想 $p$，使得 $I \subseteq p$ 且 $S \cap p = \emptyset$。

[2]如果对于给定的 $a$、$b \in B$，只要满足 $ab = \{0\}$，就有 $a = 0$ 或 $b = 0$，则称超环 $B$ 为拟超整环。

## 1.2 非交换多项式超环

尽管类环多代数结构已有 70 多年的研究历史，但关于类环多代数结构中多项式概念的研究似乎直到近十年才取得较显著的进展：例如， [22] 引入了某种多重多项式的概念，以便将其应用于代数和热带几何； [4] 则对超环上多元多项式概念的各种变体进行了更详细的论述，并以此获得了希尔伯特基底定理的一种形式。

这里我们将遵循 [4] 中的观点：设 $(R, +, -, \cdot, 0, 1)$ 为一个超环，并且设 t

$$R[X] := \{(a_n)_{n\in\omega} \in R^\omega : \exists t \forall n(n \geq t \to a_n = 0)\}.$$

当然 ，我们将 $(a_n)_{n\in\omega} \neq 0$ 的**次数** 定义为满足以下条件的最小 $t$： 对所有 $n > t$，都有 $a_n = 0$。

现在定义二元多重运算 $+, \cdot$： $R[X]\times R[X] \to \mathcal{P}^*(R[X])$、一元运算 $-$： $R[X] \to R[X]$， 以及元素 0, $1 \in R[X]$，如下所示:

$$\begin{aligned}
(c_n)_{n\in\omega} &\in (a_n)_{n\in\omega} + (b_n)_{n\in\omega} \text{ iff } \forall n(c_n \in a_n + b_n)\\
(c_n)_{n\in\omega} &\in ((a_n)_{n\in\omega} \cdot (b_n)_{n\in\omega} \text{ iff } \forall n(c_n \in a_0 \cdot b_n + a_1 \cdot b_{n-1} + ... + a_n \cdot b_0)\\
-(a_n)_{n\in\omega} &= (-a_n)_{n\in\omega}\\
0 &:= (0)_{n\in\omega}\\
1 &:= (1, 0, ..., 0, ...)
\end{aligned}$$

为方便起见，我们将 $R[X]$ 的元素记作 $\alpha = (a_n)_{n\in\omega}$。除此之外，我们记

$$\begin{aligned}
1 &:= (1, 0, 0, ...),\\
X &:= (0, 1, 0, ...),\\
X^2 &:= (0, 0, 1, 0, ...)
\end{aligned}$$

等等。从这个意义上说，我们的“单项式” $a_iX^i$ 记作 (0, ...0, $a_i$, 0, ...)，其中 $a_i$ 位于第 $i$ 个位置；特别地，我们将 $\underline{b} = (b, 0, 0, ...)$ 记作.....，并且经常将 $b \in R \rightsquigarrow \underline{b} \in R[X]$视为.....。

下面引理中所述的性质可由涉及 $R[X]$的定义立即推出:

{lemperm}

**引理 1.18**。 设 $R$ 是一个超环， $R[X]$ 如上所述，且 $n$， $m \in \mathbb{N}$。

*a* - $\{X^{n+m}\} = X^n \cdot X^m$.

*b* - 对所有 $a \in R$, $\{aX^n\} = \underline{a} \cdot X^n$。

*c* - 给定 $\alpha = (a_0, a_1, ....., a_n, 0, 0, .....) \in R[X]$, 其中其中 次数 $\alpha \leq n$ 且 $m \geq 1$，则有

$$\alpha X^m = (0, 0, ..., 0, a_0, a_1, ..., a_n, 0, 0, ...) = a_0X^m + a_1X^{m+1} + ... + a_nX^{m+n}.$$

*d* - 对于 $\alpha = (a_n)_{n\in\omega} \in R[X]$, 其中 次数 $\alpha = t$,

$$\{\alpha\} = a_0 \cdot 1 + a_1 \cdot X + ... + a_t \cdot X^t = a_0 + X(a_1 + a_2X + ... + a_nX^{t-1}).$$

*e* - $R[X]$是超整环，当且仅当 $R$ 是超整环。

*f* - $R[X]$是超环。

*g* - 映射 $a \in R \mapsto \underline{a} = (a, 0, \cdots, 0, \cdots)$ 定义了一个满嵌入 $R \rightarrowtail R[X]$。

*h* - 对于普通环 $R$ （将其视为严格超环），超环 $R[X]$自然同构于 $R$上的一元多项式普通环（所关联的超环）。

引理 1.18 让我们能够像往常一样处理超环 $R[X]$。换言之，我们可以假设对于 $\alpha \in R[x]$，存在 $a_0, a_1, ..., a_n \in R$，使得 $\alpha = a_0 + a_1X + ... + a_nX^n$，然后我们可以像往常一样简单地记作 $\alpha = f(X)$。例如，结合上述定义和所有事实，我们得到

$$(x - a)(x - b) = x^2 + (a - b)x + ab = \{x^2 + dx + e : d \in a - b \text{ and } e \in ab\}.$$

**注 1.19.** 如果 $R$ 是一个满超整环，一般来说并不能推出 $R[X]$ 也是一个满超整环。事实上，即使 $R$ 是一个超域，也存在一些例子，例如 $R = K$，$Q_2$，使得 $R[X]$ 不是一个满超整环（见 [4]）。

**定义 1.20.** 超环 $R[X]$称为以 $R$ 为系数、含一个变量的**多项式超环**。$R[X]$ 的元素称为多项式。记作 $R[X_1, ..., X_n] := (R[X_1, ..., X_{n-1}])[X_n]$

.

{degreelemma}

**L引理 1.21**（改编自 [4] 的定理 5）。设 $R$ 为超环，且 $f, g \in R[X] \setminus \{0\}$ .

*i - If* $t(X) \in f(X) + g(X)$ *and* $f \neq -g$ *then*

$$\min\{\deg(f), \deg(g)\} \leq \deg(t) \leq \max\{\deg(f), \deg(g)\}.$$

*ii -* 若 $R$ 是超整环，且 $t(X) \in f(X)g(X)$，则 $\deg(t) = \deg(f) + \deg(g)$。特别地，若 $f_1(X)\ f_2(X)\ ...,\ f_n(X) \neq 0$ 且 $t(X) \in f_1(X)f_2(X)...f_n(X)$，则

$$\deg(t) = \deg(f_1) + \deg(f_2) + ... + \deg(f_n).$$

*iii -*（部分因式分解）设 $R$ 为超整环，$\deg(f) = n$ 且 $f \in (X - a_1)(X - a_n)...(X - a_p)$。则 $p = n$。

设 $f(X) = a_0 + ... + a_n X^n$ 和 $g(X) = b_0 + ... + b_m X^m$ 满足 $a_n, b_m \neq 0$。我们建立如下记号：对于满足 $k \leq \deg(f)$ 的 $k \in \mathbb{N}$，定义 $(f)_k := a_k$（$f$ 的第 $k$ 个系数）。

尽管 $R[X]$ 通常不是满的，但我们有一个强有力的引理来解决这一问题。

{lemfator}

**引理 1.22.** 设 $R$ 是一个超环，且 $f \in R[X]$ 满足 $f(X) = a_n X^n + ... + a_1 X + a_0$。那么：

*i - For all* $b, c \in R$, $(b + cX)f(X) = bf(X) + cXf(X)$.

*ii -* 对所有 $b, c \in R$ 以及所有满足 $p < q$ 的 $p, q \in \omega$，

$$(bX^p + cX^q)f(X) = bX^p f(X) + cX^p f(X).$$

*iii -* 对所有 $b, c, d \in R$ 以及所有满足 $p < q < r$ 的 $p, q, r \in \omega$，

$$(bX^p + cX^q + dX^r)f(X) = bX^p f(X) + cX^p f(X) + dX^r f(X).$$

*iv -* 对所有 $b_0, ...., b_m \in R$,

$$(b_0 + b_1 X + b_2 X^2 + ... + b_m X^m)f(X) =$$
$$b_0 f(X) + (b_1 X + b_2 X^2 + ... + b_m X^m)f(X).$$

*v -* 对所有 $b_0, ...., b_m \in R$,

$$(b_0 + b_1 X + b_2 X^2 + ... + b_{m-1} X^{m-1} + b_m X^m)f(X) =$$
$$(b_0 + b_1 X + b_2 X^2 + ... + b_{m-1} X^{m-1})f(X) + b_m X^m f(X).$$

*vi -* 对所有 $b_0, ...., b_m \in R$,

$$(b_0 + b_1 X + ... + b_j X^j + b_{j+1} X^{j+1} + ... + b_m X^m)f(X) =$$
$$(b_0 + b_1 X + ... + b_j X^j)f(X) + (b_{j+1} X^{j+1} + ... + b_m X^m)f(X).$$

特别地，如果 $d \in R$, $g(X) \in R[X]$ 且 $r > \deg(g(X))$，那么

$$(g(X) + dX^r)f(X) = g(X)f(X) + dX^r f(X).$$

{euclid}

定理 *1.23*（欧几里得除法算法（ [9] 中的 *3.4*））。设 $K$ 是一个超域。给定多项式$f(X)$ $g(X) \in K[X]$，满足 $g(X) \neq 0$，则存在 $q(X)$ $r(X) \in K[X]$，使得 $f(X) \in q(X)g(X) + r(X)$，其中 $\deg r(X) < \deg g(X)$ 或 $r(X) = 0$。

**注 1.24.**

*i* - 注意到，定理 *1.23* 中的多项式 $q$ 和 $r$ 通常并不唯一：若 $f \in gq + r$，则$f \in g(q + 1 - 1) + r$ 且 $f \in gq + (r + 1 - 1)$，那么，若 $\{0\} \neq 1 - 1$，我们就有许多种 $q$和 $r$。

*ii* - 然而，若 $R$ 是一个环，则定理 *1.23* 给出了通常的欧几里得算法，其中商和余数是唯一的。

{teoPID}

**定理 1.25 (**改编自 [4]中的定理 6)。设 $F$ 是一个全超域。则 $F[X]$ 是一个主理想超整环。

## 1.3 关于求值与根

设 $R$、$S$ 为超环，且 $h: R \to S$ 为一个态射。则 $h$ 自然延拓为超环多元多项式之间的态射 $h^X: R[X] \to S[X]$:

$$(a_n)_{n\in\mathbb{N}} \in R[X] \mapsto (h(a_n))_{n\in\mathbb{N}} \in S[X]$$

现在设 $s \in S$。我们将 $s$ 在 $f(X) \in R[X]$ 处的 $h$-**求值** 定义为 $f(X) = a_0 + a_1X + ... + a_nX^n$:

$$f^h(s) = ev^h(s, f) := \{s' \in S : s' \in h(a_0) + h(a_1).s + h(a_2).s^2 + ... + h(a_n).s^n\}.$$

对于子集 $I \subseteq S$，我们将 $h$-**求值** 定义为

$$f^h(I) = \bigcup_{s\in I} f^h(s).$$

特别 是，如果 $S \supseteq R$ 是超环且 $\alpha \in S$，则 $\alpha$ 在 $f(X) \in R[X]$ 处的**求值** 为

$$f(\alpha, S) = ev(\alpha, f, S) = \{b \in S : b \in a_0 + a_1\alpha + a_2\alpha^2 + ... + a_n\alpha^n\} \subseteq S.$$

注意，求值**取决于** $S$的选择。当 $S = R$时，我们将 $f(\alpha, R)$记作 $f(\alpha)$。

$f$在 $S$中的**根**是满足 $0 \in ev(\alpha, f, S)$的元素 $\alpha \in S$。在这种情况下，我们称 $\alpha$在 $R$上是$S$-**代数的**。$f$ 在 $S$中的**有效根**是满足 $f \in (X - \alpha) \cdot g(X)$的元素 $\alpha \in S$，其中 $g(X) \in R[X]$。如果超环 $R$ 中的每个非恒定多项式都有一个根属于 $R$，则称该超环**代数闭**。

注意，如果 $F$ 是域，那么将 $F[X]$ 视为环时的求值与通常的求值相同；当然，根和有效根也是一回事。因此，如果 $F$ 作为超域和超域都是代数闭的，那么它在通常意义下也是代数闭的。

{unexpected-r

**注 1.26**。将上述域论概念推广到超域（尤其是超域）的多代数理论中，会带来新的现象:

*i*-（多项式可以有无限多个根）：设 $F$ 是一个无限预特殊超域（*[16]*）。那么 $F$ 的特征为$0$，$a^2 = 1$ 对所有 $a \neq 0$ 成立，因此多项式 $f(X) = X^2 - 1$ 有无限多个根（即，对所有 $\alpha \in F$，$.0 \in ev(f, \alpha)$）。

*ii*-（有限超域可以是代数闭的）。超域 $K = \{0, 1\}$ 是代数闭的。事实上，若 $p(X) = a_0 + a_1X + a_2X^2 + ... + a_nX^n \in K[X]$，且 $a_n \neq 0$，那么 $0 \in p(0)$（若 $a_0 = 0$）或$p(1) = K$，因为 $1 + 1 = \{0, 1\}$。

关于不可约性，我们已经获得了很好的结果（例如，见下文定理 1.29）。这些结果是发展超域扩张的关键，并将引领我们走向某种代数闭包。

**定义 1.27** (不可约性)。 设 $R$ 是一个超域，且 $f$， $d \in R[X]$。我们称 $d$ 整除 $f$，当且仅当 $f \in \langle d \rangle$，记作 $d|f$。若 $f$ 满足**不可约**，则称其为不可约的；若次数 $f \geq 1$ 且 $u|f$ 对于某个 $u \in R[X]$ 成立（即 $f \in \langle u \rangle$），则 $\langle f \rangle = \langle u \rangle$。

{lemquadext2}

**定理 1.28.** 设 $F$ 是一个全超域，且 $p(X) \in F[X]$ 是一个不可约多项式。那么 $\langle p(X) \rangle$是一个极大理想。

如果 $F$ 不是满的，我们无法证明 $\langle p(X) \rangle$ 是一个极大理想。但我们仍然知道 $F[X]/\langle p \rangle$ 是一个超域。

{lemquadext}

**定理 1.29.** 设 $F$ 是一个超域，且 $p \in F[X]$ 是一个不可约多项式。那么 $F[X]/\langle p \rangle$ 是一个超域。特别地，$\langle p \rangle$ 是强素的。

**定义 1.30.** 设 $F$ 是一个超域，且 $p(X) \in F[X]$ 是一个不可约多项式。我们将$F(p) := F(p(X)) = F[X]/\langle p(X) \rangle$记为。

{lemfator2}

**引理 1.31.** 设 $F$ 是一个超域， $p(X) \in F[X]$ 是一个不可约多项式。记作 $\overline{X} = \lambda$，并设 $f \in F(p)$ 满足 $f = \overline{a_n}\lambda^n + ... + \overline{a_1}\lambda + \overline{a}_0$。那么：

$i$ - *For all* $b, c \in F$, $(\overline{b} + \overline{c}\lambda)f = \overline{b}f + \overline{c}\lambda f$.

$ii$ - 对所有 $b_0, ...., b_m \in F$,

$$(\overline{b_0} + \overline{b_1}\lambda + ... + \overline{b_j}\lambda^j + \overline{b_{j+1}}\lambda^{j+1} + ... + \overline{b_m}\lambda^m)f =$$
$$(\overline{b_0} + \overline{b_1}\lambda + ... + \overline{b_j}\lambda^j)f + (\overline{b_{j+1}}\lambda^{j+1} + ... + \overline{b_m}\lambda^m)f.$$

特别地，若 $d \in F$, $g \in F(p)$ 满足 $g = \overline{b_0} + \overline{b_1}\lambda + \overline{b_2}\lambda^2 + ... + \overline{b_m}\lambda^m$ 和 $r > m$，则

$$(g + \overline{d}\lambda^r)f = gf + \overline{d}\lambda^r f.$$

# 2 交换超环上的矩阵与行列式

**定义 2.1.** 设 $m, n$ 为正整数。交换超环 $R$ 上的 $m \times n$ **矩阵** 是一个由 $F$ 中元素构成的双重序列 $A$，分布在 $m$ 行和 $n$ 列中。 $m \times n$ 矩阵的集合记为 $M_{m \times n}(R)$。当 $m = n$时，我们将 $n \times n$ 矩阵记为 $M_n(R)$。

矩阵 $A \in M_{m \times n}(R)$ 通常简记为 $A = (a_{ij})$（必要时带有 $m$ 和 $n$ 下标），或用如下表格表示：

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

对于 $A, B \in M_{n \times m}(R)$ 以及满足 $A = (a_{ij})$ 和 $B = (b_{ij})$ 的 $\lambda \in R$，我们定义 $-A = (-a_{ij})$ 及（多重）运算

$$A + B := \{(d_{ij}) : d_{ij} \in a_{ij} + b_{ij} \text{ for all } i, j\} \neq \emptyset$$

and

$$\lambda A = \{(d_{ij}) : d_{ij} \in \lambda a_{ij} \text{ for all } i, j\}.$$

若 $A \in M_{n \times m}(R)$ 满足 $A = (a_{ij})$，且 $B \in M_{m \times p}(R)$ 满足 $B = (a_{ij})$，则我们定义 $A \times B = AB \subseteq M_{n \times p}(R)$ 为

$$AB = \{(d_{ij}) : d_{ij} \in \sum_{k=1}^{n} a_{ik}b_{kj} = a_{i1}b_{1j} + a_{i2}b_{2j} + ... + a_{in}b_{nk} \text{ for all } i, j\} \neq \emptyset.$$

我们分别用 $0 = (0_{ij}) \in M_{m \times n}(R)$ 和 $1 = (\delta_{ij})_{ij} \in M_n(R)$ 表示通常的零矩阵和单位矩阵。

我们称 $A \in M_n(R)$ 是**可逆** 的，当且仅当存在 $B \in M_n(R)$，使得 $1 \in AB$ 且 $1 \in BA$ .

当然，我们可以自由采用交换代数中常用的简化记法。例如，对于$A = (a_{ij})$和 $B = (b_{ij})$，我们简单地写作

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \dots & b_{mn} \end{pmatrix} = \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} & \dots & a_{1n}+b_{1n} \\ a_{21}+b_{21} & a_{22}+b_{22} & \dots & a_{2n}+b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}+b_{m1} & a_{m2}+b_{m2} & \dots & a_{mn}+b_{mn} \end{pmatrix}$$

对 $\lambda A$ 和 $AB$也作类似的简化。

**例 2.2.** 考虑例 *1.6* 中的 $X_2 = \{-2, -1, 0, 1, 2\}$ 以及由下式给出的矩阵 $A$， $B$， $C \in M_2(X_2)$

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} \text{ and } C = \begin{pmatrix} 2 & 0 \\ -1 & 2 \end{pmatrix}.$$

采用我们的记法，有

$$A + B = \begin{pmatrix} 1-1 & 1+1 \\ 0+0 & 1-1 \end{pmatrix} =$$
$$\left\{ \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}$$

$$A \cdot B = \begin{pmatrix} 1\cdot(-1)+1\cdot 0 & 1\cdot 1+1\cdot(-1) \\ 0\cdot(-1)+1\cdot(0) & 0\cdot 1+1\cdot(-1) \end{pmatrix} = \begin{pmatrix} -1 & 1-1 \\ 0 & -1 \end{pmatrix} =$$
$$\left\{ \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} \right\}$$

$$A \cdot C = \begin{pmatrix} 1\cdot 2+1\cdot(-1) & 1\cdot 0+1\cdot 2 \\ 0\cdot 2+1\cdot(-1) & 0\cdot 0+1\cdot 2 \end{pmatrix} = \begin{pmatrix} 2-1 & 2 \\ -1 & 2 \end{pmatrix} = \left\{ \begin{pmatrix} 2 & 2 \\ -1 & 2 \end{pmatrix} \right\}.$$

在这里，我们将通常用于域的对角、三角、分块和初等矩阵等术语“推广”到超域。

利用这些记法，并根据$(R, +, -, 0)$是一个交换多群这一事实，我们立即得到以下定理。

{matrix1}

**定理 2.3.** 设 $R$ 是一个超环。那么 $(M_{m\times n}(R)\ +,\ -,\ 0)$ 是一个交换多群 .

对于一般的超环 $R$， $M_n(R)$ 中的矩阵乘积通常不满足结合律（当然，$M_n(R)$ 通常也不是超环）。

**例 2.4.** 设 $R = X_2$ 如例 *1.6* 所示。当然， $R$ 并不是满的，因为，例如 ，

$$2(1-1) = \{-2, 0, 2\} \text{ and } 2-2 = R.$$

现在，考虑这些矩阵

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} \text{ and } C = \begin{pmatrix} 2 & 0 \\ -1 & 2 \end{pmatrix}.$$

事实上，我们有

$$\begin{aligned} (AB)C &= \left[ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} \right] \begin{pmatrix} 2 & 0 \\ -1 & 2 \end{pmatrix} \\ &= \begin{pmatrix} -1 & 1-1 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ -1 & 2 \end{pmatrix} = \begin{pmatrix} -2-(1-1) & 2(1-1) \\ 1 & -2 \end{pmatrix} \end{aligned}$$

*and*

$$A(BC) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \left[ \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ -1 & 2 \end{pmatrix} \right] \\ = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -2-1 & 2 \\ 1 & -2 \end{pmatrix} = \begin{pmatrix} (-2-1)+1 & 2-2 \\ 1 & -2 \end{pmatrix}.$$

那么我们有 $(AB)C \neq A(BC)$。

尽管一般而言， $M_n(R)$ 并不是超环，但它是一种值得关注的结构（例如，我们将在定理 4.12 中看到这一点）。在下面的引理中，我们汇总了一般情形下乘积所满足的性质。我们假设，若 $A$ 和 $B$ 是 $R$ 上的矩阵，且记作 $AB$，那么 $A$ 的列数与 $B$ 的行数相同（对 $A+B$ 也采用类似约定）。

{matrix2}

**引理 2.5**。设 $R$ 是超环，且 $A$， $B$， $C$ 是矩阵。则：

***a*** - $A \cdot 0 = 0 \cdot A = \{0\}$。

***b*** - 若 $m = n$，则 $A \cdot 1 = 1 \cdot A = \{A\}$。

***c*** - 若 $A(B+C) \subseteq AB + AC$，且当 $R$ 是满的时取等号。

***d*** - $(B+C)A \subseteq BA + CA$，当 $R$ 为满的时取等号。

***e*** - 若 $R$ 为满的，则 $(AB)C = A(BC)$。

首先，我们明确一下 $AB$ 的记号：记作

$$AB = \begin{pmatrix} D_{11} & D_{12} & \dots & D_{1n} \\ D_{21} & D_{22} & \dots & D_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ D_{m1} & D_{m2} & \dots & D_{mn} \end{pmatrix}$$

或者 $AB = (D_{ij})$，其中对于所有的 $i$， $j$， $D_{ij}$ 是集合

$$D_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj} = a_{i1}b_{1j} + a_{i2}b_{2j} + ... + a_{in}b_{nk} \text{ (of course, this is an equality of sets).}$$

或者，我们可以更直接地处理，直接写作

$$AB = \begin{pmatrix} \sum_{k=1}^{n} a_{1k}b_{k1} & \sum_{k=1}^{n} a_{1k}b_{k2} & \dots & \sum_{k=1}^{n} a_{1k}b_{kn} \\ \sum_{k=1}^{n} a_{2k}b_{k1} & \sum_{k=1}^{n} a_{2k}b_{k2} & \dots & \sum_{k=1}^{n} a_{2k}b_{kn} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{k=1}^{n} a_{mk}b_{k1} & \sum_{k=1}^{n} a_{mk}b_{k2} & \dots & \sum_{k=1}^{n} a_{mk}b_{kn} \end{pmatrix}$$

现在我们来证明该引理。

引理 *2.5* 的证明。这里的论证实际上与域上线性代数中使用的论证非常相似。

a - 令 $A \cdot 0 = (D_{ij})$（如上所述）。对于所有 $i, j$，我们有

$$D_{ij} = \sum_{k} a_{ik} 0_{kj} = \sum_{k} a_{ik} \cdot 0 = \sum_{k} 0 = 0.$$

那么 $A \cdot 0 = \{0\}$。同样的推理可得 $0 \cdot A = \{0\}$。

b - 令 $A\cdot 1=(D_{i,\ j})$。由于 $1=(\delta_{i,\ j})$，且 $\delta_{i,\ j}\in\{0,1\}$ 和 $\delta_{i,\ j}=1$ 当且仅当 $i=j$，我们有

$$D_{i,j}=\sum_k a_{i,k}\delta_{k,j}=a_{i,j}\cdot 1=\{a_{i,j}\}.$$

因此，$A\cdot 1=\{A\}$。类似地，$1\cdot A=\{A\}$。

c -

$$\begin{aligned}A(B+C)&=(a_{i,j})_{i,j}\cdot(b_{i,j}+c_{i,j})_{i,j}\\&=\left(\sum_k a_{i,k}(b_{k,j}+c_{k,j})\right)_{i,j}\\&\subseteq\left(\sum_k a_{i,k}b_{k,j}+a_{i,k}c_{k,j}\right)_{i,j}\\&=\left(\sum_k a_{i,k}b_{k,j}\right)_{i,j}+\left(\sum_k a_{i,k}c_{k,j}\right)_{i,j}=AB+BC.\end{aligned}$$

当 $R$ 是满的时，由上文可立即得出 $A(B+C)=AB+AC$。

d - 论证与上文类似。

e - 假设 $R$ 是满的。那么

$$\begin{aligned}(AB)C&=\left[(a_{i,j})_{i,j}\cdot(b_{i,j})_{i,j}\right]\cdot(c_{i,j})_{i,j}\\&=\left(\sum_k a_{i,k}b_{k,j}\right)_{i,j}\cdot(c_{i,j})_{i,j}\\&=\left(\sum_l\left(\sum_k a_{i,k}b_{k,l}\right)\cdot c_{l,j}\right)_{i,j}\\&=\left(\sum_l\sum_k a_{i,k}b_{k,l}c_{l,j}\right)_{i,j}\\&=\left(\sum_k a_{i,k}\cdot\left(\sum_l b_{k,l}c_{l,j}\right)\right)_{i,j}\\&=(a_{i,j})\cdot\left(\sum_l b_{i,l}c_{l,j}\right)_{i,j}=A(BC).\end{aligned}$$

□

事实上，由定理 2.3 和引理 2.5，我们得出如下结论。

{matrix3}

**定理 2.6.** 对于超环 $R$，如果 $R$ 是满的，那么 $M_n(R)$ 是一个满超环；若 $n\geq 2$，则它是非交换的。

We 也有引理 2.5 的推广版本（证明与其中给出的证明类似）

.

{matrix4}

**引理 2.7.** 设 $R$ 是一个超环，且 $A,B,C,D,E,F$ 是矩阵，其中 $A\in M_{m\times n}(R)$、$B,C\in M_{n\times p}(R)$、$D,E\in M_{p\times m}(R)$ 以及 $F\in M_{p\times q}(R)$。则：

*a* - $A\cdot 0_{n\times p}=\{0_{m\times p}\}$ 和 $0_{p\times n}\cdot A=\{0_{p\times n}\}$。

*b* - $A\cdot 1_{n\times n}=1_{m\times m}\cdot A=\{A\}$。

**c** - $A(B+C) \subseteq AB+AC$，当且仅当 $R$ 是满的。
**d** - $(D+E)A \subseteq DA+EA$，当且仅当 $R$ 是满的。
**e** - 如果 $R$ 是满的，那么 $(AB)F = A(BF)$。

尽管对于一般的超环 $R$， $M_n(R)$中不满足完全结合律，但我们有以下有用的结果。先给出一个技术性定义:

**定义2.8**。 设 $R$ 是一个超环。若对所有 $a$， $b$， $c$， $d \in R$，称 $R$ 为**原完全**的。

$$[(ab+ac)d] \cap [a(bd+cd)] \neq \emptyset.$$

**引理2.9**。 设 $R$ 是一个原完全超环。那么对所有 $a$， $b_1$，...$b_n$， $d \in R$，我们有

$$[(ab_1+...+ab_n)d] \cap [a(b_1d+...+b_nd)] \neq \emptyset.$$

然后，改写引理2.7(e)的证明，可得如下结论。

{matrix5}

**引理2.10**。 设 $R$ 是一个原完全超环， $A$， $B$， $C$ 是矩阵，且 $A \in M_{m\times n}(R)$、 $B \in M_{n\times p}(R)$和 $C \in M_{p\times q}(R)$。那么

$$[(AB)C] \cap [A(BC)] \neq \emptyset.$$

{determinant}

**定义2.11.** 令 $\mathcal{A} \subseteq M_n(R)$。我们将 $\mathcal{A}$ 的**行列式** 定义为子集 $\det(\mathcal{A}) \subseteq R$，其定义规则如下:

$$\det(\mathcal{A}) = \bigcup_{A\in\mathcal{A}} \left\{ \sum_{\sigma\in S_n} sgn(\sigma) \prod_{j=1}^{n} a_{j\sigma(j)} \right\}.$$

若 $\mathcal{A} = \{A\}$，我们就将上述公式简写为$\det(A)$ 。

**引理2.12** （行列式的性质）。 $A, B \in M_n(R)$， $A = (a_{ij})$， $B = (b_{ij})$ 以及 $\lambda \in R$。那么:

**a** - $\det(\lambda A) \subseteq \lambda^n \det(A)$，当 $R$ 为满的时取等号;

**b** - 若 $A$ 中有一整行或一整列为零，则$\det(A) = \{0\}$。

**c** - 若 $A = (a_{ij})$ 是三角矩阵（尤其是对角矩阵），则 $\det(A) = a_{11}a_{22}...a_{nn}$ .

证明。

a - 根据定义可得

$$\begin{aligned}\det(\lambda A) &= \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) \prod_{j=1}^{n} (\lambda a_{j\sigma(j)}) = \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma)\lambda^n \prod_{j=1}^{n} a_{j\sigma(j)} \\ &\subseteq \lambda^n \left( \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) \prod_{j=1}^{n} a_{j\sigma(j)} \right) = \lambda^n \det(A)\end{aligned}$$

b - 在此情况下，对于所有 $n \in S_n$，都有 $0 \in \{a_{1\sigma(1)}, a_{2\sigma(2)}, ..., a_{n\sigma(n)}\}$。于是

$$\prod_{j=1}^{n} a_{j\sigma(j)} = \{0\} \text{ for all } \sigma \in S_n,$$

这意味着 $\det(A) = \{0\}$。

c - 直接由定义2.11得出。

□

# 3 超域上的线性系统

在本节中，固定一个超域 $F$。

{lin-equation

**定义 3.1. 线性方程**是一个形如以下形式的方程（超域语言中的项）：

$$Ax \subseteq B$$

其中 $A \in M_{1\times n}(F)(n \in \mathbb{N})$， $x$ 是一个由变量组成的 $n \times 1$ 向量，且 $B \subseteq F$。

**注 3.2.** 我们用矩阵来定义"线性方程"（以及更一般的"线性方程组"）。这样做是因为对于超域，我们无法像在一般线性代数中那样将标量与变量合并。例如，没有理由认为"$a_1x_1 + b_1x_1$"等于"$(a_1 + b_1)x_1$"[3]。

尽管有此注释，给定一个线性方程 $Ax \subseteq B$，我们仍可以"通俗地"写成

$$a_1x_1 + a_2x_2 + ... + a_nx_n \subseteq B,$$

其中有 $a_1, ..., a_n \in F$。当然，我们可以将该方程

$$a_1x_1 + a_2x_2 + ... + a_nx_n \supseteq B$$

视为线性方程，并采用两种类型的线性方程。不过，3.1 中讨论的类型（乍看之下）似乎更"自然"。

我们可以用这种"口语化"的方式来写方程（进而写方程组）；在处理单个方程（方程组）时，我们将采用这种"口语化"的说法。但为了得到更一般的证明和定义，我们始终使用矩阵。

**定义 3.3.** 线性方程 $Ax \subseteq B$ 的**解（弱解）**是一个矩阵 $d \in M_{n\times 1}(F)$，使得 $Ad \subseteq B(Ad \cap B \neq \emptyset)$。

**定义 3.4. 线性方程组**是以下类型方程（超域语言中的项）的合取

$$Ax \subseteq B$$

其中 $A \in M_{m\times n}(F)(n \in \mathbb{N})$， $x$ 是一个由变量构成的 $n \times 1$ 向量，而 $B \subseteq M_{m\times 1}(F)$。

从这个意义上说，线性方程组通常可以用惯常的方式表示

$$S: \begin{cases} a_{11}x_1 + a_{12}x_2 + ... + a_{1n}x_n \subseteq B_1 \\ a_{21}x_1 + a_{22}x_2 + ... + a_{2n}x_n \subseteq B_2 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + ... + a_{mn}x_n \subseteq B_m \end{cases}$$

线性方程组的**（弱）解**是一个元组 $(d_1, ..., d_n)$，满足 $Ad \subseteq B(Ad \cap B \neq \emptyset$ ).

**定义 3.5**。 线性方程组 $Ax \subseteq B$ 称为**缩放后的**，如果 $A$ 是一个上三角矩阵。

在通常的表示法中，缩放线性系统的形式如下：

$$\begin{cases} a_{1r_1}x_1 + \quad ... \quad + a_{1n}x_n \subseteq B_1 \\ \quad a_{2r_2}x_2 + \quad ... \quad + a_{1n}x_n \subseteq B_2 \\ \vdots \\ \quad a_{nr_k}x_k + \quad ... \quad + a_{nn}x_n \subseteq B_k \end{cases}$$

其中 $r_j \geq 1$，且 $a_{jr_j} \neq 0, j = 1, ..., k$ e $r_1 < r_2 < ... < r_k$。对于缩放后的方程组，我们有三种情况 s:

[3]换句话说，为了得到 $a_1x_1 + b_1x_1 = (a_1 + b_1)x_1$，我们应该定义什么是"满的"变量，但这并不是逻辑中的标准做法。

I - 最后一个方程的类型是

$$0x_1 + ... + 0x_n \subseteq B_p \text{ with } 0 \notin B_p.$$

在这种情况下 $S$ 是不可能的。

II - 不存在类型为 (I) 且 $p = n$ 的方程。

III - 不存在类型为 (I) 且 $p < n$ 的方程。

假设 $S$ 属于类型 (II)。那么我们有如下情形

$$\begin{cases} a_{11}x_1 + & ... & + a_{1n}x_n \subseteq B_1 \\ \quad a_{23}x_3 + & ... & + a_{2n}x_n \subseteq B_2 \\ \vdots & & \\ & & ... + a_{nn}x_n \subseteq B_n \end{cases}$$

其中对所有 $i = 1, ..., n$ 都有 $a_{ii} \neq 0$。通过适当选择，递归地得到 $x_1, ..., x_n$

$$\begin{cases} x_n & \in a_{nn}^{-1}B_n \\ x_k & \in a_{kk}^{-1}B_k - a_{kk}^{-1}a_{k(k+1)}x_{k+1} - ... - a_{kk}^{-1}a_{kn}x_n \text{ for } k = n-1, ..., 1 \end{cases} \tag{1}$$

{rec-sol}{rec-sol}

我们有该方程组的一个弱解 $S$（这个解之所以是弱解，基本上是因为 $a_{kk}^{-1}a_{kn}$ 通常不是单元素集）。同样的推理表明，对于 (III) 型缩放后的方程组，我们可以找到该方程组的一个参数化弱解。

{sistem-solve

**例 3.6.** 考虑 $n = 2$ 以及定义在 $F$ 上的方程组，

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \subseteq \begin{pmatrix} D_1 \\ D_2 \end{pmatrix}$$

或者用我们“口语化”的表示法，该方程组为

$$\begin{cases} ax + by \subseteq D_1 \\ \quad cy \subseteq D_2 \end{cases} \quad with\ a, c \neq 0.$$

由于 $D_2 \subseteq c(c^{-1}D_2)$，对于所有 $d_2 \in D_2$，都存在 $z \in c^{-1}D_2$ 使得 $d_2 \in cz$。取 $y_0 = z$。于是我们有

$$cy_0 \subseteq c(c^{-1}D_2) \ with\ cy_0 \cap D_2 \neq \emptyset.$$

因此我们得到 $y_0 \in c^{-1}D_2$，并且可以选择 $x_0 \in a^{-1}D_1 - by_0$，从而得到

$$ax_0 + by_0 \subseteq a(a^{-1}D_1 - by_0) + by_0 \subseteq aa^{-1}D_1 - aa^{-1}by_0 + by_0 \ and\ ax_0 + by_0 \cap D_1 \neq \emptyset.$$

当然，超域上线性方程组比域上线性方程组具有更大的灵活性。正如下面的例子所示，超域上线性方程组比域上线性方程组更容易得到弱解。

**例3.7**。设 $F = \mathbb{Q}/_m\mathbb{Q}^{*2}$。我们有 $2,\ 5 \notin D(\langle 1,\ 1\rangle)$，因为 $2 = 1 \cdot 1^2 + 1 \cdot 1^2$ 且 $5 = 1 \cdot 2^2 + 1 \cdot 1^2$。于是 $2, \overline{5} \in \overline{1} + \overline{1}$，并且方程组

$$\begin{cases} x + y \subseteq \{\overline{1}\} \\ \quad y \subseteq \{\overline{5}\} \end{cases}$$

在 $F$ 上至少有一个弱解 $x = y = 1$。

**定义 3.8** (初等变换)。设 $A \in M_{m\times n}(F)$。这些**初等变换**:

*I* - **交换**行 $i$ *e* $j$; 这将用 $L_i \leftrightarrow L_j$ 表示;

*II - Mu* **将**某一行 $i$ 的每个系数乘以 $F$ 中的一个元素 $\lambda \neq 0$；这将用 $L_i \leftarrow \lambda L$ 表示 $_i$;

*III - 超um* 行 $i$ 与行 $j$ 并将结果保留在行 $i$中；这将用 $L_i \leftarrow L_i + L_j$表示 .

当然，给定一个线性方程组 $Ax \subseteq B$，对矩阵 $A$ 和 $B$进行一系列初等变换后，我们会得到不止一个方程组。经过初等变换序列$O = \{o_1, ..., o_n\}$后得到的方程组记为一个方程组集合 $Ax \subseteq B$（其中 $A \subseteq M_{m\times n}(F)$、 $B \subseteq M_{m\times 1}(F)$），并记作 $(Ax \subseteq B)^O$。

上述定义的初等变换可以用矩阵乘法来描述（就像我们通常对域所做的那样）。例如，考虑由下式给出的矩阵 $A \in M_{2\times 2}(F)$

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

应用 $L_1 \leftrightarrow L_2$ 就是

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} c & d \\ a & b \end{pmatrix}$$

若 $R$ 是原满超域，则在方程组 $Ax \subseteq B$ 上执行初等变换，等价于用初等矩阵 [4] $E \in M_{m\times m}(F)$ 乘以 $A$ 和 $B$，从而得到方程组 $(EA)x \subseteq (EB)$。

{element-sol}

**引理 3.9**。设 $Ax \subseteq B$ 是线性方程组的集合，且 $O = \{o_1, ..., o_n\}$。那么， $Ax \subseteq B$ 中某个方程组的每个解，都是 $(Ax \subseteq B)^O$ 中某个方程组的解。若 $F$ 是满的，则 $Ax \subseteq B$ 中某个方程组的每个弱解，都是 $(Ax \subseteq B)^O$ 中某个方程组的弱解。

证明。 我们只需处理初等变换。考虑方程组

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & d_{m2} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \subseteq \begin{pmatrix} B_1 \\ B_2 \\ \vdots \\ B_n \end{pmatrix}$$

我们已经知道，运算 (I) 和 (II) 保持解不变。现在不失一般性地考虑初等变换 $L_1 \leftarrow L_1 + L_2$。于是我们得到方程组的集合

$$\begin{pmatrix} a_{11}+a_{21} & a_{12}+a_{22} & \dots & a_{1n}+a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & d_{m2} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \subseteq \begin{pmatrix} B_1+B_2 \\ B_2 \\ \vdots \\ B_n \end{pmatrix}$$

如果我们得到 $d_1$, ....., $d_n$，其中

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & d_{m2} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_n \end{pmatrix} \subseteq \begin{pmatrix} B_1 \\ B_2 \\ \vdots \\ B_n \end{pmatrix}$$

特别是

$$(a_{11}d_1 + ... + d_{1n}d_n) + (a_{21}d_1 + ... + d_{2n}d_n) \subseteq B_1 + B_2,$$

and

$$\begin{pmatrix} a_{11}+a_{21} & a_{12}+a_{22} & \dots & a_{1n}+a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & d_{m2} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_n \end{pmatrix} \subseteq \begin{pmatrix} B_1+B_2 \\ B_2 \\ \vdots \\ B_n \end{pmatrix}$$

[4]初等矩阵是许多《线性代数》教材中的标准主题。如需快速查阅，请参见 https://en.wikipedia.org/wiki/Elementary_matrix。

证明（经过归纳法） $Ax \subseteq B$ 的每个解都是一个解（$Ax \subseteq B$）$^{O}$。对于弱解部分，假设 $F$是满的，并且 $d_1$、.....、 $d_n$ 满足

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & d_{m2} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_n \end{pmatrix} \cap \begin{pmatrix} B_1 \\ B_2 \\ \vdots \\ B_n \end{pmatrix} \neq \emptyset$$

特别是

$$[(a_{11}+a^{21})d_1+...+(a_{1n}+a_{2n})d_n] = (a_{11}d_1+...+d_{1n}d_n)+(a_{21}d_1+...+d_{2n}d_n) \cap (B_1+B_2) \neq \emptyset,$$

and

$$\begin{pmatrix} a_{11}+a_{21} & a_{12}+a_{22} & \dots & a_{1n}+a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & d_{m2} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_n \end{pmatrix} \cap \begin{pmatrix} B_1+B_2 \\ B_2 \\ \vdots \\ B_n \end{pmatrix} \neq \emptyset.$$

证明（经归纳法） $Ax \subseteq B$ 的每个弱解都是弱解（$Ax \subseteq B$）$^{O}$。 □

给定一个方程组 $Ax \subseteq B$，我们可以像通常那样经过有限次初等变换，得到一组缩放后的方程组（$Ax \subseteq B$）$^{scaled}$。遗憾的是，尽管引理 3.9 得出了相应结果，我们仍不知道（$Ax \subseteq B$）$^{scaled}$ 的解是否为 $Ax \subseteq B$的解。

从现在起，给定一个方程组 $Ax \subseteq B$，**求解** $Ax \subseteq B$ 意为**求出** $Ax \subseteq B$的一个弱解，而 $n \times n$ **方程组**意为一个满足 $A \in M_{n\times n}(F)$（以及$B \in M_{n\times 1}(F)$）的方程组 $Ax \subseteq B$。

**定义 3.10**。令 $A=(a_{ij}) \in M_n(F)$，并将 $A_i=(a_{i1},...,a_{in})$ 记为第 $i$ 行，将 $A^j=(a_{1j},...,a_{nj})$ 记为第 $j$ 列。若存在 $a_1,...,a_{i-1},a_{i+1},...,a_n \in F$，使得 $A_i$ 是 $\{A_1,...,A_{i-1},A_{i+1},...,A_n\}$ 的线性组合，则称 $A_i$ 是 $\{A_1,...,A_{i-1},A_{i+1},...,A_n\}$ 的线性组合。

$$A_i \cap \left[ \left( \sum_{j=1}^{r_1} \lambda_{j1} \right) A_1 + ... + \left( \sum_{j=1}^{r_{i-1}} \lambda_{j(i-1)} \right) A_{i-1} + \left( \sum_{j=1}^{r_{i+1}} \lambda_{j(i+1)} \right) A_{i+1} + ... + \left( \sum_{j=1}^{r_n} \lambda_{jn} \right) A_n \right] \neq \emptyset.$$

{scal4}

**引理 3.11.** 设 $F$ 是一个超域，$A \in M_n(F)$ 是一个上三角矩阵。那么，$A$ 可逆当且仅当$0 \notin \det(A)$。

证明。设

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_{nn} \end{pmatrix}$$

我们已经知道 $\det(A) = a_{11}a_{22}...a_{nn}$。因此，我们需要证明，对于所有 $i=1, 2, ..., n$，$A$ 可逆当且仅当 $a_{ii} \neq 0$。

现在，设 $B \in M_n(F)$ 是另一个上三角矩阵，即

$$B = \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ 0 & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & b_{nn} \end{pmatrix}$$

我们还知道

$$AB = \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12}+a_{12}b_{22} & a_{11}b_{13}+a_{12}b_{23}+a_{13}b_{33} & \dots & \sum_{k=1}^{n} a_{1k}b_{kn} \\ 0 & a_{22}b_{22} & a_{22}b_{23}+a_{23}b_{33} & \dots & \sum_{k=2}^{n} a_{2k}b_{kn} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & a_{nn}b_{nn} \end{pmatrix}$$

and

$$BA = \begin{pmatrix} b_{11}a_{11} & b_{11}a_{12}+b_{12}a_{22} & b_{11}a_{13}+b_{12}a_{23}+b_{13}a_{33} & \dots & \sum_{k=1}^{n} b_{1k}a_{kn} \\ 0 & b_{22}a_{22} & b_{22}a_{23}+b_{23}a_{33} & \dots & \sum_{k=2}^{n} b_{2k}a_{kn} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & b_{nn}a_{nn} \end{pmatrix}$$

那么，如果 $a_{ii} = 0$ 对某个 $i \in \{1, 2, ..., n\}$成立，则对所有 $B \in M_n(F)$ 都有 $I_n \notin AB \cap BA$。这足以证明 $A$ 不可逆。

现在，假设对所有的 $i = 1$、2、...、$n$，$a_{ii} \neq 0$。我们将选择元素 $b_{ij}$，以便得到

$$I_n \in AB \cap BA.$$

首先，选择 $b_{ii} = a_{ii}^{-1}$。然后，考虑 $AB = (P_{ij})$ 和 $BA = (Q_{ij})$，我们希望对所有的 $i \neq j$ 都得到 $0 \in P_{ij}$ 和 $0 \in Q_{ij}$。我们需要选择 $b_{(n-1)n}$，以便得到

$$0 \in a_{(n-1)(n-1)}b_{(n-1)n} + a_{(n-1)n}b_{nn} \text{ and}$$
$$0 \in b_{(n-1)(n-1)}a_{(n-1)n} + b_{(n-1)n}a_{nn}.$$

然后（记住 $b_{ii} = a_{ii}^{-1}$），我们需要

$$b_{(n-1)n} \in -a_{(n-1)n}a_{(n-1)(n-1)}^{-1}a_{nn}^{-1}.$$

然后我们选择 $b_{nn}$、$b_{(n-1)(n-1)}$ 和 $b_{(n-1)n}$（即，我们完成 $B$ 的第 $n$ 行和第（$n-1$）行的过程）。

现在，我们需要选择 $b_{(n-2)(n-1)}$ 和 $b_{(n-2)n}$，以便得到

$$0 \in a_{(n-2)(n-2)}b_{(n-2)(n-1)} + a_{(n-2)(n-1)}b_{(n-1)(n-1)} + a_{(n-2)n}b_{n(n-1)} \text{ and}$$
$$0 \in a_{(n-2)(n-2)}b_{(n-2)n} + a_{(n-2)(n-1)}b_{(n-1)n} + a_{(n-2)n}b_{nn}$$

and

$$0 \in b_{(n-2)(n-2)}a_{(n-2)(n-1)} + b_{(n-2)(n-1)}a_{(n-1)(n-1)} + b_{(n-2)n}a_{n(n-1)} \text{ and}$$
$$0 \in b_{(n-2)(n-2)}a_{(n-2)n} + b_{(n-2)(n-1)}a_{(n-1)n} + b_{(n-2)n}a_{nn}$$

选取 $b_{(n-2)(n-1)}$ 和 $b_{(n-2)n}$，使得

$$b_{(n-2)n} \in -a_{(n-2)(n-2)}^{-1}a_{(n-2)(n-1)}b_{(n-1)n} - a_{(n-2)(n-2)}^{-1}a_{(n-2)n}b_{nn} \text{ and}$$
$$b_{(n-2)(n-1)} \in -a_{(n-2)(n-2)}^{-1}a_{(n-2)(n-1)}b_{(n-1)(n-1)} - a_{(n-2)(n-2)}^{-1}a_{(n-2)n}b_{n(n-1)}$$

我们完成了对 $B$ 的第 $n$、$(n-1)$ 和 $(n-2)$ 行的处理。再重复此过程 $n-3$ 次，我们便得到矩阵 $B$，使得 $I_n \in AB \cap BA$，如所需。 □

# 4 超域代数扩张理论的应用

为了定义超域扩张的概念，我们有几种可能性需要考虑:

{extension}

**定义 4.1** (扩张)。设 $F$ 和 $K$ 为超域。

*i* - 我们称 $K$ 是 $F$ 的原型超域扩张（或简称原扩张）$K|_pF$，记作，若 $F \subseteq K$。

*ii* - 我们称 $K$ 是 $F$ 的**超域扩张（或简称扩张）**，记作 $K|F$，如果 $F \subseteq K$ 且包含映射 $F \hookrightarrow K$ 是一个超域态射。

*iii* - 我们称 $K$ 是 $F$ 的**完全超域扩张（或简称满扩张）**，记作 $K|_fF$，如果 $F \subseteq K$，且包含映射 $F \hookrightarrow K$ 是一个完全超域态射。

**例 4.2**。

*i* - 显然，每个满扩张都是扩张，而每个扩张都是原扩张。

*ii* - 我们有 $K \subseteq Q_2$，但包含映射 $K \hookrightarrow Q_2$ 不是一个态射。因此，我们有一个原扩张 $Q_2|_p K$，但它不是扩张。

*iii* - 对于 $p$，$q$ 个满足 $q \geq p$ 的素整数，我们有一个包含态射 $H_p \hookrightarrow H_q$，但这个态射不是满的。因此，我们有一个扩张 $H_q|H_p$，但它不是满扩张。

*iv* - 设 $F$是一个超域，$p \in F[X]$ 是一个不可约多项式，且 $F(p) = F[X]/\langle p \rangle$。那么，我们有一个满态射 $F \hookrightarrow F(p)$，因此我们有一个满扩张 $F(p)|_f F$。

*v* - 设 $F$，$K$ 是满足 $F \subseteq K$的域。那么，域扩张 $K|F$ 满足定义 *4.1* 中的所有条件。

下面的结果说明了深入研究完全超域扩张的必要性。

{unicityext}

**定理** **4.3.** 设 $K_1|_f F$和 $K_2|_f F$是完全超域扩张，并假设 $\gamma \in K_1 \cap K_2$。*Then*

$$F[\gamma, K_1] = F[\gamma, K_2].$$

**定义** **4.4**（代数扩张）。若原扩张 $K|_p F$ 中的所有元素都在 $F$ 上代数的。对于扩张和满扩张，我们也采用相同的记号。

**定义 4.5 (**线性无关性、基、次数**)**。设 $K|_p F$ 是一个原扩张，且 $I \subseteq K$。若对所有互不相同的 $\lambda_1, ..., \lambda_n \in I$, $n \in \mathbb{N}$，下列条件成立，则称 $I$ 是 $F$**-线性无关** 的：

$$If\ 0 \in \left(\sum_{j=1}^{r_1} a_{j1}\right)\lambda_1 + ... + \left(\sum_{j=1}^{r_1} a_{n1}\right)\lambda_n\ then\ 0 \in \left(\sum_{j=1}^{r_1} a_{ij}\right)\ for\ all\ j.$$

并且，若 $I$ 不是 $F$-线性无关的，则称其为 $F$**-线性相关** 。若 $I$ 线性无关，且 $K$ 是由 $I$**生成的**，即，则称 $I$ 是 $K$ 的 $F$**-基**，

$$K = \bigcup_{n \geq 0} \left\{ \sum_{i=0}^{n} a_i \lambda_i : a_i \in F,\ \lambda_i \in I \right\}.$$

在这种情况下，记作 $K = F[I]$。我们将 $K|_p F$ 的**次数** 定义为，记作 $[K\colon F]$，如下：

$[K\colon F] := \infty$ 或 $[K\colon F] :=$最大值$\{n :$对于所有 $\lambda \in K\}$., 集合 $\{1, \lambda, \lambda^2, ..., \lambda^n\}$ 都是线性无关的

{rem1}

**注 4.6**。由上述定义可立即得到以下结论：

*a* - 这里，线性无关、生成元和维数的定义都是临时规定的（因为到目前为止，我们还不知道是否存在适用于超域的"线性代数理论"）。

*b* - 如果 $I \subseteq K$ 线性无关且 $J \subseteq I$，那么 $J$ 也线性无关。

*c* - 元素 $\alpha \in K$是 $F$-代数的，当且仅当 $\{\alpha^k\colon \ k \in \mathbb{N}\}$ 线性相关。

*d* - 如果 $[K\colon \ F] < \infty$，那么所有 $\alpha \in K$都是 $F$-代数的。

*e* - 设 $F$ 是一个超域，$p \in F[X]$ 是一个不可约多项式，例如 $p(X) = a_0 + a_1 X + ... + a_n X^{n-1} + X^n$。那么 $\{\overline{1}, \overline{X}, ..., \overline{X}^{n-1}\}$ 是 $F$（$p$）的一个基。

现在，设 $K|_p F$是一个原扩张，且 $\gamma \in K$ 是代数的。那么存在一个不可约多项式$f(X)$，使得 $0 \in f(\gamma, K)$。令 $\mathrm{Irr}_F(\gamma, K)$ 为满足 $0 \in f(\gamma, K)$ 的 $f(X)$ 的最低次数不可约多项式。令 $F[\gamma, K] \subseteq K$为集合

$$F[\gamma, K] := \bigcup_{f \in F[X]} ev(f, \gamma, K) \subseteq K,$$

且 $I_{\gamma,\ K} \subseteq F[\gamma, K]$ 为集合

$$I_{\gamma,K} := \bigcup_{f \in \langle \mathrm{Irr}_F(\gamma,K) \rangle} ev(f, \gamma, K) \subseteq K.$$

注意，对于所有 $g \in F[X]$ 和所有 $a_0, ..., a_n \in F$，应用“牛顿二项式公式”可得

$$ev(g, (a_0 + a_1\gamma + a_2\gamma^2 + ... + a_{n-1}\gamma^{n-1} + a_n\gamma^n), K) \subseteq F[\gamma, K].$$

**注 4.7.**

*i* - 如果 $K|F$ 是域扩张，那么我们的 $F[\gamma, K]$ 与通常的单扩张 $F(\gamma)$ 相同 .

*ii* - 如果 $K|F$ 是超域扩张且 $\gamma \in K$，那么 $F[\gamma, K]$ **取决于** $K$ 的选择。例如，考虑 $H_3|H_1$ 和 $H_5|H_1$ 以及元素 $2 \in H_3$（当然，也在 $H_5$ 中）。那么

$$H_2[2, H_3] = \bigcup_{f \in H_2[X]} ev(f, \gamma, H_3) = H_3,$$
$$H_2[2, H_5] = \bigcup_{f \in H_2[X]} ev(f, \gamma, H_5) = H_5,$$

于是， $H_2[2, H_3] \neq H_2[2, H_5]$。

*iii* - 对于原扩张 $K|_pF$，集合 $F[\gamma, K]$ 可能不是超域！设 $F = H_2$, $K = \mathbb{R}$ 和 $\gamma = 2$。那么

$$H_2[2, \mathbb{R}] = 2\mathbb{Z}$$

它不是超域。

此时，我们的目标是为超域的单扩张取得一个恰当的概念。换言之，给定一个满扩张 $K|_fF$ 和 $\alpha \in K$ 代数的情形，我们非常希望得到一个超域$F(\alpha)$，使其满足：

1. $F \cup \{\alpha\} \subseteq F(\alpha)$;
2. $F(\alpha)$是满足条件（1）的最小超域（相对于包含关系而言）；
3. $F(\alpha)$在某种意义上是“可计算的”（或者更现实地说，我们希望 $F(\alpha) \cong F(p)$，其中 $p(X) = \mathrm{Irr}_F(\alpha)$)[5]。

对于一般的超域，实现这一目标存在一些障碍。首先， $R[X]$ 通常不是满的。不过，对于所有的 $a$、$b \in R[X]$，我们有一个有趣的性质：

$$a(1 + X) = a + aX \text{ and } (a + b)X = aX + bX.$$

这一性质启发了下面的定义。

{almostfull}

**定义 4.8.** 设 $K|_pF$ 是一个原型超域扩张，且 $\gamma \in K$。假设 $K$ 由 $\{1, \gamma^2, ..., \gamma^n\}$作 $F$-生成。若对所有 $a$， $b$， $c \in F$以及所有互不相同的 $p$， $q$， $r \in \mathbb{N}$，我们称 $K$相对于 $\gamma$是 $F$-**几乎满** $\gamma$ **（或简称几乎满）**

$$(a\gamma^p + b\gamma^q + c\gamma^r)\gamma = a\gamma^{p+1} + b\gamma^{q+1} + c\gamma^{r+1}.$$

以下是定义 4.8 的一些直接推论：

{lemfator3}

**引理 4.9.** 设 $K|_fF$是一个相对于 $\gamma$而言 $F$-几乎满的满扩张，并且

$$A = a_0 + a_1\gamma + a_2^2 + ... + a_n\gamma^n.$$

于是：

[5]正如我们稍后将看到的，对超域进行简单计算也极具挑战性.....

*i* - 对所有的 $b$， $c \in F$ $(b+c\gamma)\ A = bA + c\gamma A$。

*ii* - 对所有 $b_0, ...., b_m \in F$,

$$(b_0 + b_1\gamma + ... + b_j\gamma^j + b_{j+1}\gamma^{j+1} + ... + b_m\gamma^m)A =$$
$$(b_0 + b_1\gamma + ... + b_j\gamma^j)A + (b_{j+1}\gamma^{j+1} + ... + b_m\gamma^m)A.$$

特别地，若 $d \in F$, $B \subseteq K$ 满足 $B = b_0 + b_1\gamma + b_2\gamma^2 + ... + b_m\gamma^m$ 和 $r > m$，则

$$(B + d\gamma^r)A = AB + d\gamma^r A.$$

{almostfact}

**引理 4.10.** 设 $K|_f F$是一个相对于 $\gamma$ 为 $F$-几乎满的满扩张。则：

*i* - $K = F[\gamma, K]$;

*ii* - 若 $K|_f F$和 $L|_f K$几乎满，则 $L|F$几乎满；

*iii* - 若 $L|_f F$是另一个满扩张，且 $\pi\colon K \to L$是满的满射态射，则 $L|_f F$相对于 $\pi(\gamma)$ 是 $F$-几乎满的；

*iv* - 对所有 $a_0, ..., a_n, b_0, ..., b_n \in F$,

$$(a_0 + a_1\gamma + a_2\gamma^2 + ... + a_{n-1}\gamma^{n-1} + a_n\gamma^n)(b_0 + b_1\gamma + b_2\gamma^2 + ... + b_{n-1}\gamma^{n-1} + b_n\gamma^n) \subseteq$$
$$a_0b_0 + \left(\sum_{j=0}^{1} a_j b_{1-j}\right)\gamma + ... + \left(\sum_{j=0}^{2n-1} a_j b_{(2n-1)-j}\right)\gamma^{2n-1} + \left(\sum_{j=0}^{2n} a_j b_{1-j}\right)\gamma^{2n}$$

按约定， $a_j = b_j = 0$ 若 $j > n$。

设 $K|_f F$是一个满扩张，且 $\alpha \in K$在 $F$上代数。我们的目标是构造一个包含 $F$和 $\alpha$的几乎满代数扩张 $F(\alpha)|_f F$。关键在于找到描述 $K$的代数元的方法。这里给出朝这个方向迈出的第一个结果。

**定理 4.11 (**几乎满牛顿二项式**)**。 设 $K|F$ 是由 $\{1, \gamma, ..., \gamma^n\}$, $\gamma \in K$ 生成的几乎满超域扩张 $F$。那么对所有 $a, b \in F$,

$$(a + b\gamma)^n = \sum_{j=0}^{n} \binom{n}{j} a^j (b\gamma)^{n-j}.$$

证明。 用归纳法，只需证明 $n = 2$ 的情形。我们有

$$(a + b\gamma)^2 := (a + b\gamma)(a + b\gamma) \overset{4.9}{=} a(a + b\gamma) + b\gamma(a + b\gamma) = a^2 + ab\gamma + b\gamma a + (b\gamma)^2$$
$$= a^2 + ab\gamma + ab\gamma + (b\gamma)^2 = a^2 + 2ab\gamma + (b\gamma)^2 := \sum_{j=0}^{2} \binom{n}{j} a^j (b\gamma)^{n-j}.$$

□

作为超域上线性方程组理论的应用，接下来我们将给出超域代数扩张理论中的一个关键结果，它表明我们的“单扩张最佳候选” $F(p)$是 $F$ 的一个满代数扩张和几乎满扩张。我们先证明 $F(p)$ 是原完全的。

{teohell2}

**定理 4.12**。 设 $F$是一个超域， $p \in F[X]$ 是一个不可约多项式。那么 $F(p)|_f F$是一个代数扩张。此外，如果 $\deg p = n + 1$，那么 $[F(p)\colon F] \leq n + 1$。

证明。 请记住， $F(p)$ 是由 $\{1, \gamma, ..., \gamma^n\}$ 生成的，其中 $\gamma = \overline{X}$、 $n \in \mathbb{N}$。此外，我们可以将 $n$视为满足以下条件的最小整数：存在 $a_0$、...、 $a_{n+1}$，使得

$$0 \in a_0 + a_1\gamma + ... + a_{n+1}\gamma^{n+1}.$$

现在令 $b_0 + b_1\gamma + ... + b_n\gamma^n \in F(p)^*$。由于对所有 $x$， $x \cdot y \neq \emptyset$， $y \in F(P)$，因此对所有 $k = 0, ..., n$，存在

$$d_{k0} + d_{k1}\gamma + ... + d_{kn}\gamma^n \in (b_0 + b_1\gamma + ... + b_n\gamma^n)^k$$

适当的 $d_{ij} \in F$。用矩阵记法表示，可得

$$D \begin{pmatrix} 1 \\ \gamma \\ \vdots \\ \gamma^n \end{pmatrix} \subseteq \begin{pmatrix} (b_0 + b_1\gamma + ... + b_n\gamma^n)^0 \\ (b_0 + b_1\gamma + ... + b_n\gamma^n)^1 \\ \vdots \\ (b_0 + b_1\gamma + ... + b_n\gamma^n)^n \end{pmatrix}$$

with

$$D = \begin{pmatrix} d_{00} & d_{01} & \dots & d_{1n} \\ d_{10} & d_{11} & \dots & d_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ d_{n0} & d_{n1} & \dots & d_{nn} \end{pmatrix}$$

由于 $F(p)$ 几乎满，我们可以对矩阵 $D$ 进行缩放，令

$$D_{scaled} = \begin{pmatrix} e_{00} & e_{01} & \dots & e_{1n} \\ 0 & e_{11} & \dots & e_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & e_{nn} \end{pmatrix}$$

并得到

$$\begin{pmatrix} e_{00} & e_{01} & \dots & e_{1n} \\ 0 & e_{11} & \dots & e_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & e_{nn} \end{pmatrix} \begin{pmatrix} 1 \\ \gamma \\ \vdots \\ \gamma^n \end{pmatrix} \in \begin{pmatrix} \sum_{j=0}^n g_{0j}(b_0 + b_1\gamma + ... + b_n\gamma^n)^j \\ \sum_{j=0}^n g_{1j}(b_0 + b_1\gamma + ... + b_n\gamma^n)^j \\ \vdots \\ \sum_{j=0}^n g_{nj}(b_0 + b_1\gamma + ... + b_n\gamma^n)^j \end{pmatrix} \tag{$*$}$$

适当的 $g_{ij} \in F$。

如果 $D_{scaled}$ 不可逆，那么 $0 \in \det(D_{scaled}) = e_{11}e_{22}...e_{nn}$，于是，存在某个 $i \in \{1, ..., n\}$，使得 $e_{ii} = 0$（见引理 3.11）；这意味着（通过同样的缩放过程）存在一行 $i$，其中 $L_i$ 是其他各项的线性组合。不失一般性，设

$$L_{n+1} \cap \left[ \left( \sum_{j=1}^{r_1} \lambda_{j1} \right) L_1 + ... + \left( \sum_{j=1}^{r_n} \lambda_{jn} \right) L_n \right] \neq \emptyset.$$

这意味着

$$0 \in z_0 + z_1(b_0 + b_1\gamma + ... + b_n\gamma^n)^1 + ... + z_n(b_0 + b_1\gamma + ... + b_n\gamma^n)^{n-1} - (b_0 + b_1\gamma + ... + b_n\gamma^n)^{n+1},$$

对于合适的 $z_0, ..., z_n \in F$，接着，对于 $f(X) = z_0 + z_1X + ... + z_nX^n - X^{n+1}$，我们有

$$0 \in f(b_0 + b_1\gamma + ... + b_n\gamma^n),$$

这意味着 $b_0 + b_1\gamma + ... + b_n\gamma^n$ 是代数的。若 $D_{scaled}$ 可逆，由于 $F(p)|_f F$ 几乎满，我们得到

$$\begin{pmatrix} 1 \\ \gamma \\ \vdots \\ \gamma^n \end{pmatrix} \in D_{scaled}^{-1} \left[ D_{scaled} \begin{pmatrix} 1 \\ \gamma \\ \vdots \\ \gamma^n \end{pmatrix} \right].$$

将方程（$*$）乘以 $D_{scaled}^{-1}$ 后，我们得到一个方程组

$$\begin{pmatrix}1\\ \gamma\\ \vdots\\ \gamma^n\end{pmatrix} \in D_{scaled}^{-1}\left[D_{scaled}\begin{pmatrix}1\\ \gamma\\ \vdots\\ \gamma^n\end{pmatrix}\right] \subseteq D_{scaled}^{-1}\begin{pmatrix}\sum_{j=0}^{n} g_{0j}(b_0+b_1\gamma+...+b_n\gamma^n)^j\\ \sum_{j=0}^{n} g_{1j}(b_0+b_1\gamma+...+b_n\gamma^n)^j\\ \vdots\\ \sum_{j=0}^{n} g_{nj}(b_0+b_1\gamma+...+b_n\gamma^n)^j\end{pmatrix}$$

那么我们的情况是

$$\begin{pmatrix}1\\ \gamma\\ \vdots\\ \gamma^n\end{pmatrix} \in D_{Scaled}^{-1}\begin{pmatrix}\sum_{j=0}^{n} g_{0j}(b_0+b_1\gamma+...+b_n\gamma^n)^j\\ \sum_{j=0}^{n} g_{1j}(b_0+b_1\gamma+...+b_n\gamma^n)^j\\ \vdots\\ \sum_{j=0}^{n} g_{nj}(b_0+b_1\gamma+...+b_n\gamma^n)^j\end{pmatrix} \qquad (**)$$

令 $D_{Scaled}^{-1} = (h_{ij})$。由（$**$）可得，计算矩阵乘积后得到

$$\begin{cases}\gamma^0 \in \sum_{j=0}^{n} g_{0j}h_{0j}(b_0+b_1\gamma+...+b_n\gamma^n)^j\\ \gamma_1 \in \sum_{j=0}^{n} g_{1j}h_{1j}(b_0+b_1\gamma+...+b_n\gamma^n)^j\\ \vdots\\ \gamma^n \in \sum_{j=0}^{n} g_{nj}h_{nj}(b_0+b_1\gamma+...+b_n\gamma^n)^j\end{cases}$$

这意味着

$$\begin{cases}a_0\gamma^0 \in \sum_{j=0}^{n} a_0g_{0j}h_{0j}(b_0+b_1\gamma+...+b_n\gamma^n)^j\\ a_1\gamma_1 \in \sum_{j=0}^{n} a_1g_{1j}h_{1j}(b_0+b_1\gamma+...+b_n\gamma^n)^j\\ \vdots\\ a_n\gamma^n \in \sum_{j=0}^{n} a_ng_{nj}h_{nj}(b_0+b_1\gamma+...+b_n\gamma^n)^j\end{cases}$$

Then

$$a_1a_n\gamma^{n+1} \subseteq \left(\sum_{j=0}^{n} a_1g_{1j}h_{1j}(b_0+b_1\gamma+...+b_n\gamma^n)^j\right)\left(\sum_{j=0}^{n} a_ng_{nj}h_{nj}(b_0+b_1\gamma+...+b_n\gamma^n)^j\right)$$

and

$$\begin{aligned}&0 \in a_0+a_1\gamma+...+a_{n+1}\gamma^{n+1} \subseteq\\ &\sum_{p=0}^{n}\left[\sum_{j=0}^{n} a_pg_{pj}h_{pj}(b_0+b_1\gamma+...+b_n\gamma^n)^j\right]+\\ &\left(\sum_{j=0}^{n} a_1g_{1j}h_{1j}(b_0+b_1\gamma+...+b_n\gamma^n)^j\right)\left(\sum_{j=0}^{n} a_ng_{nj}h_{nj}(b_0+b_1\gamma+...+b_n\gamma^n)^j\right).\end{aligned}$$

现在，从多项式的角度来看，我们有

$$\begin{aligned}A(X) &:= \sum_{p=0}^{n}\left[\sum_{j=0}^{n} a_pg_{pj}h_{pj}X^j\right]+\left(\sum_{j=0}^{n} a_1g_{1j}h_{1j}X^j\right)\left(\sum_{j=0}^{n} a_ng_{nj}h_{nj}X^j\right)=\\ &\left[\sum_{p=0}^{n}\sum_{j=0}^{n} a_pg_{pj}h_{pj}\right]X^j+\left(\sum_{j=0}^{n} a_1g_{1j}h_{1j}X^j\right)\left(\sum_{j=0}^{n} a_ng_{nj}h_{nj}X^j\right)=\\ &= P(X)+S(X)T(X),\end{aligned}$$

with

$$P(X) = \left[\sum_{p=0}^{n}\sum_{j=0}^{n} a_p g_{pj} h_{pj}\right] X^j$$
$$S(X) = \sum_{j=0}^{n} a_1 g_{1j} h_{1j} X^j$$
$$T(X) = \sum_{j=0}^{n} a_n g_{nj} h_{nj} X^j$$

Then

$$0 \in ev\left(A(X), b_0 + b_1\gamma + ... + b_n\gamma^n\right);$$

这意味着至少存在一个多项式 $f(X) \in A(X) = P(X) + S(X)T(X)$，满足

$$0 \in f(b_0 + b_1\gamma + ... + b_n\gamma^n).$$

那么， $b_0 + b_1\gamma + ... + b_n\gamma^n$ 是代数的。当然，这也意味着 $[F(p): F] \leq n + 1$ . □

# 5 向量空间

既然我们已经有了适用于超环的矩阵和多项式，那么理论的一个自然扩展就是引入某种“向量空间”以及一些线性代数方法。我们在此开始这一探索，采用与 Hofmann 和 Kunze 的《线性代数》([21])非常相似的方式。

{mvec}

**定义 5.1.** 超域 $F$上的一个（多）向量空间 是一个元组 $(V, +, \cdot, 0)$，使得 $(V, +, 0)$是一个阿贝尔多群，并且 $\cdot: F \times V \to \mathcal{P}^*(V)$ 是一个函数（其像记为 $\cdot(\lambda, v) := \lambda v$），满足以下性质，其中 $\lambda, \mu \in F$ 和 $v, w \in V$ 任意：

**MV0 -** $1v = \{v\}$ *and* $0 \cdot v = \{0\}$*;*

**MV1 -** $(\lambda\mu)v = \lambda(\mu v)$.

这里采用以下约定：如果 $A \subseteq F$ 和 $v \in V$，我们设

$$Av := \bigcup\{\lambda v : \lambda \in A\}.$$

**MV2 -** $\lambda(v + w) \subseteq \lambda v + \lambda w$*;*

**MV3 -** $(\lambda + \mu)v \subseteq \lambda v + \mu v$.

如果 *MV2* 和 *MV3* 中的等式成立，则向量空间 $(V, +, 0)$ 是**满的**。

我们继续采用处理多项式和矩阵时使用的做法：省略“乘 i”而只说 “超域上的向量空间”。

当然，我们这里仍然只讨论向量空间，不过也有“模”的定义，只需将定义 5.1 中的超域替换为超环即可。

下面给出一些向量空间的自然例子。

{extvec}

**命题 5.2**。 设 $K|F$ 是一个超域扩张。那么 $K$ 是一个 $F$-向量空间，当且仅当该扩张是满的。

证明。 这里的 $\cdot: F \to K \to \mathcal{P}^*(K)$ 只是将乘法限制到 $F$ 的第一个坐标上。M0 显然成立，而 M1-M3 是超环公理的推论。显然， $K$ 是满向量空间当且仅当 $K|_f F$。

□

{fnvec}

**定理 5.3**。 设 $F^n$ 是通常的 $n$ 重笛卡尔积 $F \times ... \times F$。我们已经知道， $F^n$在诱导的加法下是一个多群。现在，对于 $\lambda \in F$和 $v = (x_1, ..., x_n) \in F^n$ 定义

$$\lambda v := (\lambda x_1, ..., \lambda x_n).$$

那么（$F^n$， $+$， $\cdot$， $0$）是一个向量空间。此外， $F^n$是满的，当且仅当 $F$是满的。

证明。我们已经知道， $F^n$ 是一个交换的超环。根据数乘的定义，我们得到 $1v = v$。现在令 $v$、$w \in F^n$（$x_1$，...，$x_n$）、 $w =$（$y_1$，...，$y_n$）以及 $\lambda$和 $\mu \in F$。我们有

$$\begin{aligned}(\lambda + \mu)v &:= ((\lambda + \mu)x_1, ..., (\lambda + \mu)x_n) \\ &\subseteq (\lambda x_1 + \mu x_1, ..., \lambda x_n + \mu x_n) \\ &= (\lambda x_1, ..., \lambda x_n) + (\mu x_1, ..., \mu x_n) = \lambda v + \mu w.\end{aligned}$$

同理，我们得出（$\lambda + \mu$）$v \subseteq \lambda v + \mu v$。

那么 $F^n$ 是一个向量空间；若 $F$ 是满的，则它也是满的。

现在假设 $F^n$ 是满的。那么对于 $\alpha$、 $\lambda$、 $\mu \in F$和 $v =$（$\alpha$，$0$，...，$0$），我们有

$$(\lambda\alpha + \mu\alpha, 0, ..., 0) = \lambda v + \lambda v = (\lambda + \mu)v = ((\lambda + \mu)\alpha, 0, ..., 0);$$

这意味着 $(\lambda + \mu)\alpha = \lambda\alpha + \mu\alpha$。类似地，我们得出 $\alpha(\lambda + \mu) = \alpha\lambda + \alpha\mu$。 □

**定理 5.4.** 设 $F$ 是一个超域，且 $n \geq 1$。那么 $M_n(F)$ 是一个向量空间，当且仅当 $F$ 是满的 *ll.*

证明。 这是引理 2.7 的推论，将 $F$ 与 $M_{1\times 1}(F)$ 等同即可。 □

**定理 5.5**。 设 $F$是一个超域，且 $n \geq 1$。那么 $F[X_1, ..., X_n]$ 是一个向量空间，当且仅当 $F$是满的。

证明。 这里的论证与定理 5.3 中的论证类似。 □

**定义 5.6**（子空间）。 设 $V$ 是一个 $F$-向量空间，且 $W \subseteq V$。我们称 $W$ 为**子空间**，如果$0 \in W$，并且对所有 $w_1$， $w_2 \in W$ 以及所有 $\lambda \in F$，都有 $w_1 + w_2 \subseteq W$ 和 $\lambda w_1 \subseteq W$。

**The定理 5.7**。 设 $F$ 是一个全超域，并考虑方程组 $Ax = 0$、 $A \in M_{n\times m}$（$F$）。那么

$$Sol[Ax = 0] := \{v \in M_{n\times 1}(F) : 0 \in Av\}$$

是 $M_{n\times 1}$（$F$） 的子空间。

证明。 这是引理 2.7 的另一条推论。要得出如下结论，我们需要 $F$ 是满的：若 $0 \in Av$ 且 $0 \in Aw$，则 $0 \in A(v + w) = Av + Aw$。 □

**定义 5.8**（张成子空间）。 设 $V$ 是一个 $F$-向量空间，且 $A \subseteq V$。由**生成的子空间** ***d***
**由** $A$定义 于

$$\langle A\rangle := \bigcap\{W \subseteq V : W \textit{ is a subspace and } A \subseteq W\}.$$

**定义 5.9 (**线性组合**)**。 设 $V$是一个 $F$-向量空间， $A \subseteq V$和 $w \in V$。我们称 $w$ 为 $A$ 中元素的**线性组合**，如果存在 $\{v_1, ..., v_n\} \subseteq A$ 使得

$$w \in \sum_{j=1}^{r_1} \lambda_{j1}v_1 + ... + \sum_{j=1}^{r_n} \lambda_{jn}v_n$$

对于某个 $\lambda_{ij} \in F$。我们将 $V$ 的线性组合集合记为

$$\mathcal{CL}(A) = \bigcup \left\{ \sum_{j=1}^{r_1} \lambda_{j1}v_1 + ... + \sum_{j=1}^{r_n} \lambda_{jn}v_n : \{v_1, ..., v_n\} \subseteq A,\ \lambda_{ij} \in F,\ r_1, ..., r_n \in \mathbb{N} \right\}.$$

如果 $V$ 是满的，那么

$$\mathcal{CL}(A) := \bigcup\{\lambda_1 v_1 + ... + \lambda_n v_n : v_i \in A,\, \lambda_i \in F,\, i = 1, ..., n,\, n \geq 1\}.$$

{gen1}

**定理 5.10.** 设 $V$是一个 $F$-向量空间，且 $A \subseteq V$。那么 $\langle A\rangle = \mathcal{CL}(A)$。

证明。 我们知道 $\mathcal{CL}(A)$ 是一个子空间，由此可得 $\langle A\rangle \subseteq \mathcal{CL}(A)$。如果 $W \subseteq V$ 且 $A \subseteq W$，根据子空间的定义（以及归纳法），我们有 $\mathcal{CL}(A) \subseteq W$，由此可得 $\mathcal{CL}(A) \subseteq \langle A\rangle$。 □

{gen2}

**引理 5.11.** 设 $V$是一个 $F$-向量空间，且 $A$， $B \subseteq V$。那么

*i* - $\langle\langle A\rangle\rangle = \langle A\rangle$;

*ii* - 如果 $A \subseteq B$，那么 $\langle A\rangle$ 是 $\langle B\rangle$的一个子空间;

*iii* - 如果 $A \subseteq B$，且对所有 $v \in B$， $v \in \langle A\rangle$，那么 $\langle A\rangle = \langle B\rangle$。

证明。 □

**定义 5.12**（线性无关）。 设 $V$是一个 $F$-向量空间，且 $A \subseteq V$。如果对所有互不相同的 $v_1, ..., v_n \in A$, $n \in \mathbb{N}$，下列条件均成立，我们就称 $A$ 是**-线性无关的**：

$$\textit{If } 0 \in \sum_{j=1}^{r_1} \lambda_{j1} v_1 + ... + \sum_{j=1}^{r_n} \lambda_{jn} v_n \textit{ then } 0 \in \sum_{j=1}^{r_1} \lambda_{ji} \textit{ for all } i = 1, ..., n.$$

如果 $I$ 不是 $F$-线性无关的，我们就称其**-线性相关**。

**定义 5.13**（基）。 设 $V$是一个 $F$-向量空间，且 $B \subseteq V$。如果 $B$线性无关且 $V = \langle B\rangle$，我们就称 $B$是一个**-基**。

**定义 5.14**。 如果一个 $F$-向量空间满足 $V = \langle S\rangle$ 对某个有限的 $S \subseteq V$，则称其为**有限生成的**。

{basis1}

**定理 5.15**。 每个有限生成的 $F$-向量空间 $V$ 都有一个基。

证明。 设 $V$ 是一个有限生成的 $F$-向量空间，其生成元为 $V = \langle v_1, ..., v_n\rangle$ ($v_1, ..., v_n \in V$)。如果 $\{v_1, ..., v_n\}$ 线性无关，则结论成立。否则，必要时重新排列指标后，不失一般性地设 $v_1 \in \mathcal{CL}(\{v_2, ..., v_n\})$。于是（利用定理 5.10 和引理 5.11）有

$$V = \mathcal{CL}(\{v_1, ..., v_n\}) = \mathcal{CL}(\{v_2, ..., v_n\}).$$

如果 $\{v_2, ..., v_n\}$ 线性无关，则结论成立。否则，不失一般性地设 $v_2 \in \mathcal{CL}(\{v_3, ..., v_n\})$。于是有

$$V = \mathcal{CL}(\{v_1, ..., v_n\}) = \mathcal{CL}(\{v_2, ..., v_n\}) = \mathcal{CL}(\{v_3, ..., v_n\}).$$

重复这一过程，经过有限步后，我们得到 $V$ 的一个基 $\{v_k, v_{k+1}, ..., v_n\}$，其中某个 $k$ 满足 $1 \leq k \leq n$。 □

遗憾的是，对于一般的超域 $F$，我们不知道有限生成的 $F$-向量空间中的所有基是否具有相同的维数。为了解决这个问题，我们提出以下概念。

{linearly-clo

**定义 5.16**。 设 $F$ 为超域。我们称 $F$ 是**线性闭的**，如果方程组 $Ax = 0$ 对于所有满足 $m > n$ 的 $A \in M_{n\times m}(F)$，至少有一个非平凡弱解。

当然，每个域都是线性闭超域。正如我们稍后将看到的（定理 5.20），超域也具有这一性质。线性闭这一概念有助于为有限生成 $F$-向量空间的一个子类定义维数。

{basis2}

**定理 5.17.** 设 $F$ 为线性闭超域， $V$ 为有限生成的 $F$-向量空间，且$V = \langle v_1,..., v_n\rangle$ ($v_1,..., v_n \in V$)。那么， $V$ 的每个线性无关子集至多含有 $n$ 个元素。

证明. 我们只需证明，若 $S \subseteq V$ 且 $|S| > n$，则 $S$ 线性相关。

令 $S$ 为这样一个集合，其中包含 $S = \{w_1, ..., w_m\}$、 $m > n$。由于 $V = \langle v_1、...、 v_n \rangle$，因此存在标量 $a_{ij} \in F$，使得

$$w_j \in a_{1j}v_1 + ... + a_{nj}v_n,\ j = 1, ..., m.$$

于是，对于所有 $\lambda_1、...、\lambda_m \in F$，我们得到

$$\lambda_1 w_1 + ... + \lambda_m w_m = \sum_{j=1}^{m} \lambda_j w_j \subseteq \sum_{j=1}^{m} \lambda_j \sum_{i=1}^{n} a_{ij} v_i \subseteq \sum_{j=1}^{m} \sum_{i=1}^{n} (\lambda_j a_{ij}) v_i = \sum_{i=1}^{n} \left[ \sum_{j=1}^{m} \lambda_j a_{ij} \right] v_i$$

如果 $0 \in \lambda_1 w_1 + ... + \lambda_m w_m$，那么我们得到

$$0 \in \sum_{i=1}^{n} \left[ \sum_{j=1}^{m} \lambda_j a_{ij} \right] v_i,$$

从而

$$0 \in \begin{pmatrix} a_{11} & a_{21} & \dots & a_{m1} \\ a_{21} & a_{22} & \dots & a_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n} & a_{2n} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_m \end{pmatrix}$$

Let

$$A = \begin{pmatrix} a_{11} & a_{21} & \dots & a_{m1} \\ a_{21} & a_{22} & \dots & a_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n} & a_{2n} & \dots & a_{mn} \end{pmatrix}$$

由于 $F$ 是线性闭的，方程组 $Ax = 0$ 在 $m > n$ 时有弱解，并且当 $m > n$ 时， $S$ 线性相关。

□

{basis4}

**定理 5.18**。设 $F$ 是线性闭超域， $V$ 是有限生成的 $F$-向量空间。若 $B_1$ 和 $B_2$ 是 $V$ 的基，则 $|B_1| = |B_2|$。

证明。设 $B_1 = \{v_1, ..., v_n\}$ 和 $B_2 = \{w_1, ..., w_m\}$。由于 $V = \langle B_1 \rangle$ 和 $B_2$ 线性无关，由定理 5.17 可得 $m \leq n$。由于 $V = \langle B_2 \rangle$ 和 $B_1$ 线性无关，由定理 5.17 可得 $n \leq m$。于是 $m = n$。

□

**定义 5.19**。设 $F$ 是线性闭超域， $V$ 是有限生成的 $F$-向量空间。我们将 $V$ 的**维数** 定义为$\dim(V) := |B|$，其中 $B \subseteq V$ 是 $V$ 的任意一组基。

{basis5}

**定理 5.20**。每个超域作为超域都是线性闭的。

证明。首先，记住每个超域都是满的。现在，令 $A \in M_{n \times m}(F)$，其中 $m > n$。其次，由于$F$是一个超域，考虑向量空间 $F^n$，我们有一个满的 $F$-向量空间，使得对于所有 $\lambda \in F$和所有 $v \in F^n$， $\lambda v$ 都是单元素集合。

牢记这一点，我们将构造一个弱解 $b \in M_{m \times 1}(F)$，并将证明分为若干 e 情形。

**情形 I -** $n = 1$ **（这意味着** $m \geq 2$）。在这种情形下，令 $A \in M_{m \times 1}(F)$，其中

$$A = \begin{pmatrix} a_1 & a_2 & ... & a_m \end{pmatrix}$$

我们需要找到 $x_1, ..., x_m \in F$（不全为零），使得

$$0 \in a_1 x_1 + a_2 x_2 + ... + a_m x_m.$$

若 $a_1 = a_2 = 0$，只需对所有 $i \geq 3$ 选取 $x_1 = x_2 = 1$ 和 $x_i = 0$。若 $0 \notin \{a_1, a_2\}$，则对所有 $i \geq 3$、$x_2 = 1$ 和 $x_1 = -a_1^{-1} a_2$ 选取 $x_i = 0$。于是

$$a_1 x_1 + a_2 x_2 + a_3 x_3 + ... + a_m x_m = a_1 x_1 + a_2 x_2 = a_1[-a_1^{-1} a_2] + a_2 = a_2 - a_2 \text{ with } 0 \in a_2 - a_2.$$

我们进一步将这种用于求出 $x_1$、$x_2$、.....、$x_m$ 的策略称为“情形 I 方法”。 {case-I-metho

* * *

**情形 II -** $n=2$ **（这意味着** $m\geq 3$**）**。在这种情况下，令 $A\in M_{m\times 2}(F)$ 其中

$$A=\begin{pmatrix} a_1 & a_2 & ... & a_m \\ b_1 & b_2 & ... & b_m \end{pmatrix}$$

我们需要找出 $x_1,...,x_m\in F$（不全为零），使得

$$\begin{aligned} 0&\in a_1x_1+a_2x_2+...+a_mx_m \\ 0&\in b_1x_1+b_2x_2+...+b_mx_m \end{aligned} \tag{2}$$ {eq-01-sys-ca

这里有几种情况。如果对某个 $j$ 有 $a_j=b_j=0$，只需令 $x_j=1$，并对所有 $i\neq j$ 令 $x_i=0$。如果 $0\in\{a_1,...,a_m,b_1,...,b_m\}$，也就是说 $b_1=0$ 和 $a_1\neq 0$。于是问题归结为

$$\begin{aligned} 0&\in a_1x_1+a_2x_2+...+a_mx_m \\ 0&\in b_2x_2+...+b_mx_m \end{aligned} \tag{3}$$ {eq-02-sys-ca

现在，找出一些 $d_2,...,d_m\in F$（不全为零），使得 $0\in b_2d_2+...+b_md_m$（如情形 I 方法中所述），并选择 $d_1$，以得到 $d_1\in -a_1^{-1}[a_2d_2+...+a_md_m]$。因此，$(d_1,...,d_m)$ 是约化方程组 3 的一个非平凡弱解。现在，设 $0\notin\{a_1,...,a_m,b_1,...,b_m\}$。如果 $\{$（$a_1,...,a_m$），那么 $(b_1,...,b_m)\}$ 线性相关，即 $(b_1,...,b_m)=\lambda(a_1,...,a_m)$，我们只需选择 $d_1,d_2,...,d_m\in F$，使其不全为零（如情形 I 中所述），并满足 $0\in a_1d_1+a_2d_2+...+a_md_m$，从而得到此情形下方程组 2 的一个解。

现在，假设 $0\notin\{a_1,...,a_m,b_1,...,b_m\}$，且 $\{$（$a_1,...,a_m$），$(b_1,...,b_m)\}$ 线性无关。由于 $F$ 是一个超域，求方程组 2 的一个非平凡弱解，等价于求下列方程组的一个非平凡弱解

$$\begin{aligned} 0&\in x_1+a_1^{-1}a_2x_2+...+a_1^{-1}a_mx_m \\ 0&\in x_1+b_1^{-1}b_2x_2+...+b_1^{-1}b_mx_m \end{aligned}$$

那么，不失一般性，我们可以假设 $a_1=b_1=1$，并且需要求出下列方程组的一个弱解

$$\begin{aligned} 0&\in x_1+a_2x_2+...+a_mx_m \\ 0&\in x_1+b_2x_2+...+b_mx_m \end{aligned} \tag{4}$$ {eq-03-sys-ca

现在，考虑经过初等变换 $L_2\leftarrow L_2-L_1$ 后得到的方程组集合：

$$\begin{aligned} 0&\in x_1+a_2x_2+...+a_mx_m \\ 0&\in (1-1)x_1+(b_2-a_2)x_2+...+(b_m-a_m)x_m \end{aligned} \tag{5}$$ {eq-04-sys-ca

与情形 I 一样，设 $d_2,...,d_m\in F$（不全为零），且满足

$$0\in(b_2-a_2)d_2+...+(b_m-a_m)d_m.$$

特别地，存在 $z\in F$，满足

$$z\in(a_2x_2+...+a_mx_m)\cap(a_2x_2+...+a_mx_m).$$

令 $x_1=-z$。那么 $(-z,d_2,d_3,...,d_m)$ 是 4 和 5 的弱解，从而完成了情形 II 的证明。我们还将这种求得 $z$ 的技巧称为“情形 II 方法”。 {case-II-meth

* * *

**情形 III -** $n=3$ **（这意味着** $m\geq 4$**）**。在这种情况下，令 $A\in M_{m\times 2}$（$F$）其中

$$A=\begin{pmatrix} a_1 & a_2 & ... & a_m \\ b_1 & b_2 & ... & b_m \\ c_1 & c_2 & ... & c_m \end{pmatrix}$$

我们需要找出 $x_1, ..., x_m \in F$（不全为零），使得

$$\begin{aligned} 0 &\in a_1x_1 + a_2x_2 + ... + a_mx_m \\ 0 &\in b_1x_1 + b_2x_2 + ... + b_mx_m \\ 0 &\in c_1x_1 + c_2x_2 + ... + c_mx_m \end{aligned} \tag{6}$$ {eq-01-sys-ca

我们需要处理以下几种情况。如果对于某个 $j$， $a_j = b_j = c_j = 0$，只需选择 $x_j = 1$，并对所有 $i \neq j$ 取 $x_i = 0$。那么不失一般性，我们可以假设 $0 \notin \{a_1, b_1, c_1\}$。对于 $j \geq 5$ 选取 $x_j = 0$ 后，我们只需处理化简后的方程组

$$\begin{aligned} 0 &\in a_1x_1 + a_2x_2 + a_3x_3 + a_4x_4 \\ 0 &\in b_1x_1 + b_2x_2 + b_3x_3 + b_4x_4 \\ 0 &\in c_1x_1 + c_2x_2 + c_3x_3 + c_4x_4 \end{aligned} \tag{7}$$ {eq-0202-sys-case-III} sys-case-III}

此外，由于 $F$ 是超域，要找到 7 的非平凡弱解，等价于找到

$$\begin{aligned} 0 &\in x_1 + a_1^{-1}a_2x_2 + a_1^{-1}a_3x_3 + a_1^{-1}a_4x_4 \\ 0 &\in x_1 + b_1^{-1}b_2x_2 + b_1^{-1}b_3x_3 + b_1^{-1}b_4x_4 \\ 0 &\in x_1 + c_1^{-1}c_2x_2 + c_1^{-1}c_3x_3 + c_1^{-1}c_4x_4 \end{aligned}$$

那么不失一般性，我们可以假设 $a_1 = b_1 = c_1 = 1$，只需处理新的简化方程组

$$\begin{aligned} 0 &\in x_1 + a_2x_2 + a_3x_3 + a_4x_4 \\ 0 &\in x_1 + b_2x_2 + b_3x_3 + b_4x_4 \\ 0 &\in x_1 + c_2x_2 + c_3x_3 + c_4x_4 \end{aligned} \tag{8}$$ {eq-0303-sys-case-III} sys-case-III}

如果集合 $\{(1, a_2, a_3, a_4); (1, b_2, b_3, b_4)\}$、 $\{(1, a_2, a_3, a_4); (1, c_2, c_3, c_4)\}$ 和 $\{(1, b_2, b_3, b_4); (1, c_2, c_3, c_4)\}$ 中有一个线性相关，则问题可归结为情形 II。因此，我们可以假设这三个集合都线性无关（特别是这意味着 $0 \notin b_i - a_i$ 和 $0 \notin b_i - a_i$ 对于 $i = 2$、 3、 4）。进行初等变换 $\{L_2 \leftarrow L_2 - L_1; L_3 \leftarrow L_3 - L_1\}$ 后，我们得到方程组

$$\begin{aligned} 0 &\in x_1 + a_2x_2 + a_3x_3 + a_4x_4 \\ 0 &\in (1-1)x_1 + (b_2 - a_2)x_2 + (b_3 - a_3)x_3 + (b_4 - a_4)x_4 \\ 0 &\in (1-1)x_1 + (c_2 - a_2)x_2 + (c_3 - a_3)x_3 + (c_4 - a_4)x_4 \end{aligned}$$

考虑缩放后的方程组

$$\begin{aligned} 0 &\in x_1 + a_2x_2 + a_3x_3 + a_4x_4 \\ 0 &\in (b_2 - a_2)x_2 + (b_3 - a_3)x_3 + (b_4 - a_4)x_4 \\ 0 &\in (c_2 - a_2)x_2 + (c_3 - a_3)x_3 + (c_4 - a_4)x_4 \end{aligned} \tag{9}$$ {eq-04-sys-ca

若对所有 $i = 2, 3, 4$，均有 $b_i - a_i = \lambda(c_i - a_i)$，或者对所有 $i = 2, 3, 4$，均有 $b_i - a_i = \lambda(c_i - a_i)$，则可归结为情形 II 方法（5）。否则，由于 $0 \notin b_2 - a_2$ 和 $0 \notin c_2 - a_2$，进行初等变换$\{L_3 \leftarrow (b_2 - a_2)L_3 - (c_2 - a_2)L_2\}$ 后，我们得到方程组

$$\begin{aligned} 0 &\in x_1 + a_2x_2 + a_3x_3 + a_4x_4 \\ 0 &\in (b_2 - a_2)x_2 + (b_3 - a_3)x_3 + (b_4 - a_4)x_4 \\ 0 &\in [(b_2 - a_2)(c_2 - a_2) - (c_2 - a_2)(b_2 - a_2)]x_2 + \\ &\quad + [(b_2 - a_2)(c_3 - a_3) - (c_2 - a_2)(b_3 - a_3)]x_3 + [(b_2 - a_2)(c_4 - a_4) - (c_2 - a_2)(b_4 - a_4)]x_4 \end{aligned}$$

考虑（第二个）缩放后的方程组

$$\begin{aligned} 0 &\in x_1 + a_2x_2 + a_3x_3 + a_4x_4 \\ 0 &\in (b_2 - a_2)x_2 + (b_3 - a_3)x_3 + (b_4 - a_4)x_4 \\ 0 &\in [(b_2 - a_2)(c_2 - a_2) - (c_2 - a_2)(b_3 - a_3)]x_3 + [(b_2 - a_2)(c_4 - a_4) - (c_2 - a_2)(b_4 - a_4)]x_4 \end{aligned} \tag{10}$$ {eq-0505-sys-case-III} sys-case-III}

利用情形 I 方法 (5)，我们可以找到 $d_3, d_4 \in F$（不全为零），使得

$$0 \in [(b_2 - a_2)(c_3 - a_3) - (c_2 - a_2)(b_3 - a_3)]d_3 + [(b_2 - a_2)(c_4 - a_4) - (c_2 - a_2)(b_4 - a_4)]d_4,$$

这尤其意味着存在某个 $z \in F$，满足

$$z \in [(b_2 - a_2)(c_2 - a_2)d_3 + (b_2 - a_2)(c_4 - a_4)d_4] \cap [(c_2 - a_2)(b_3 - a_3)d_3 + (c_2 - a_2)(b_4 - a_4)d_4].$$

设 $d_2 \in -[(b_3 - a_3)d_3 + (b_4 - a_4)d_4]$ 使得 $-z \in (c_2 - a_2)d_2$。那么

$$0 \in (c_2 - a_2)[(b_2 - a_2)d_2 + (b_3 - a_3)d_3 + (b_4 - a_4)d_4],$$

这意味着

$$0 \in (b_2 - a_2)d_2 + (b_3 - a_3)d_3 + (b_4 - a_4)d_4,$$

并且特别地，存在

$$w \in [a_2d_2 + a_3d_3 + a_4d_4] \cap [b_2d_2 + b_3d_3 + b_4d_4].$$

取 $d_1 = -w$，则 $(d_1, d_2, d_3, d_4)$ 是方程组 8、9 和 10（集合）的一个弱解，由此完成情形 III 的证明。我们还将这种寻找 $z$ 和 $w$ 的策略称为“情形 III 方法”。 {case-III-met

* * *

**情形 IV——一般情形** $m > n$ **（以及** $n \geq 3$**）**。只需对 $m$ 使用归纳法。基例为情形 I 和情形 II，归纳步骤则采用与情形 III 方法 (5) 类似的论证。 □

由此可见，为了证明定理 5.20，我们付出了很大努力。因此，我们提出以下问题。

**问题 5.21**。

1. 每个全超域 $F$ 都是线性闭超域吗？
2. 超域 $F$ 成为线性闭超域的必要条件是什么？

作为这些超域线性代数片段的应用，我们得到以下定理，它是定理 4.12、命题 5.2、定理 5.17 和定理 5.20 的综合结果。

**定理 5.22**。设 $F$ 是一个线性闭超域，$p \in F[X]$ 是一个满足次数 $p = n + 1$的不可约多项式。那么 $F(p)$ 是一个满的 $F$-向量空间，并且维数$(F(p)) = n + 1$。

**定理 5.23**。设 $F$ 是一个线性闭超域，$p \in F[X]$ 是一个满足次数 $p = n + 1$的不可约多项式。那么 $F(p)$ 也是线性闭的。

证明。记住，$F(p)$ 由 $\{1, \gamma, ..., \gamma^n\}$ 生成，满足 $\gamma = \overline{X}$、$n \in \mathbb{N}$。此外，我们可以将 $n$ 视为满足以下条件的最小整数：存在 $a_0$，.....，$a_{n+1}$，使得

$$0 \in d_0 + d_1\gamma + ... + d_{n+1}\gamma^{n+1}.$$

设 $A \in M_{m \times q}(F(p))$，也就是说，$A = (\alpha_{ij})$。我们可以将每个 $\alpha_{ij}$ 写成

$$\alpha_{ij} = a_{0ij} + a_{1ij}\gamma + ... + a_{nij}\gamma^n$$

对于适当的 $a_{kij} \in F$。于是，$F(p)$ 上的方程组 $Ax = 0$ 可以拆分为 $F$ 上的 $n + 1$ 个方程组 $A_kx = 0$，其中每个 $k = 0$ 都满足 $A_k = (a_{kij})$，1，...，$n$（事实上，$Ax = 0$ 表示 $A_0x + \gamma A_1x + \gamma^2 A_2x + ... + \gamma^n A_nx = 0$）。由于 $F$ 是线性闭的，每个 $A_kx = 0$ 都至少有一个非平凡解，从而为 $Ax = 0$ 提供一个非平凡解。 □

# 6 结语与未来工作

我们才刚刚开始发展一种（或一种可能的途径来研究）“多值线性代数”。毫无疑问，要更全面地分析向量空间这一概念，并定义和分析不变子空间，还需要付出大量努力。

本文对多值线性代数的初步探讨表明，这可能是一套颇有前景的理论：“克罗内克构造”（定理 4.12）在超域框架中给出简单的代数扩张，是一项关键成果，有助于推动一项研究计划：在自然的代数扩张和多项式的根概念下研究超域与超域。这项计划与近期的 [7] 研究有一些共同特点。事实上，在 [12]，中，我们基于定理 4.12 证明，每个“性质良好”的超域都有一个满的代数扩张（在同构意义下唯一），且该扩张是一个代数闭超域。

超域代数扩张研究计划的下一步，是发展伽罗瓦理论和伽罗瓦上同调理论，并设想将其应用于其他数学理论，例如二次型的抽象结构和实代数几何（（[16],[13],[14]）。该计划的部分内容正在 [11] 和 [10] 中推进；具体而言，我们在 [11] 中发展了超域和超域二次扩张理论的初步内容，并将其应用于特殊群理论（[17]），从而将阿拉松–普菲斯特性质（[5],[17]）推广至每个 特殊群。

# 参考文献

[1] Madeline Al Tahan、Sarka Hoskova-Mayerova 和 Bijan Davvaz。关于 hv-环的（广义）模糊多重 hv-理想的一些结果。*Symmetry*，11(11):1376，2019年。[2] R Ameri、M Eyvazi 和 S Hoskova-Mayerova。超域枚举方面的进阶结果。*AimsMathematics*，5(6):6552–6579，2020年。[3] R Ameri、A Kordi 和 S Hoskova-Mayerova。分式乘法超环与互素超理想。*Analele Universitatii" Ovidius" Constanta-Seria Matematica*，25(1):5–23，2017年。[4] Reza Ameri、Mansour Eyvazi 和 Sarka Hoskova-Mayerova。超环上的多项式超环。*Mathematics*，7(10):902，2019年。[5] J. Arason 和 A. Pfister。Krull 交定理的证明。*InventionesMathematicae*，(12):173—-176，1971年。[6] Matthew Baker 和 Tong Jin。关于由域的商得到的超域的结构。*Proceedings of the American Mathematical Society*，149(1):63–70，2021年。[7] Matthew Baker 和 Oliver Lorscheid。笛卡尔符号法则、牛顿多边形与超域上的多项式。*Journal of Algebra*，569:416–441，2021年。[8] Nathan Bowler 和 Ting Su。双重分配斜超域与严格超群的分类。*Journal of Algebra*，574:669–698，2021年。[9] B Davvaz 和 T Musavi。超环上的码。*Matematicki Vesnik*，68(1):26–38，2016年。[10]Kaique Matias de Andrade Roberto、Ana Luiza da Conceição Tenório、Hugo Rafael de Oliveira Ribeiro 和 Hugo Luiz Mariano。超域伽罗瓦理论 I。准备中，2022。[11]Kaique Matias de Andrade Roberto、Hugo Rafael de Oliveira Ribeiro 和 Hugo Luiz Mariano。特殊超域的 Aranson-Pfister 主定理。预印本：*https://arxiv.org/abs/2210.03784*，2022。[12]Kaique Matias de Andrade Roberto、Hugo Rafael de Oliveira Ribeiro 和 Hugo Luiz Mariano。关于超域的代数扩张与代数闭包。预印本：*https://arxiv.org/pdf/2208.08537*，2022。

[13] Kaique Matias de Andrade Roberto、Hugo Rafael de Oliveira Ribeiro 和 Hugo Luiz Mariano。（多重）环相关的二次结构。范畴与一般代数结构，16(1):105–141，2022。[14] Kaique Matias de Andrade Roberto 和 Hugo Luiz Mariano。抽象二次型理论中的 K-理论与自由归纳分次环。范畴与一般代数结构，17(1):1–46，2022。[15] Kaique Matias de Andrade Roberto 和 Hugo Luiz Mariano。关于多项式超环与代数闭多域。应用逻辑学杂志，9(1):419–444，2022。[16] Hugo Rafael de Oliveira Ribeiro、Kaique Matias de Andrade Roberto 和 Hugo Luiz Mariano。多环与各种抽象二次型理论之间的函子关系。圣保罗数学科学杂志，16:5–42，2022。[17] Maximo Dickmann 和 Francisco Miraglia。特殊群：二次型理论中的布尔理论方法。第689号。美国数学学会，2000年。[18] Chris Eppolito、Jaiung Jun 和 Matt Szczesny。超域上拟阵的 Hopf代数。*Journalof Algebra*，556:806–835，2020年。[19] Pawel Gladki 和 Krzysztof Worytkiewicz。二次可表示域的维特环。范畴与一般代数结构，12(1):1–23，2020年。[20] Ana Claudia Golzio。代数与逻辑中超结构的简要历史回顾。南美逻辑学杂志，2018年。[21] Kenneth Hoffman 和 Ray Kunze。线性代数。恩格尔伍德克利夫斯，新泽西州，1971年。[22] Jaiung Jun。超环上的代数几何。数学进展，323:142–192，2018年。[23] Jaiung Jun。半环的赋值。纯粹与应用代数杂志，222(8):2063–2088，2018年。[24] Jaiung Jun。超域的几何。*Journal of Algebra*，569:220–257，2021年。[25] Murray Marshall。实约化多重环与多域。纯粹与应用代数杂志，205(2):452–468，2006年。[26] Ch G Massouros。超环与超域理论。代数与逻辑，24(6):477–485，1985年。[27] Christos G Massouros 和 Gerasimos G Massouros。关于并超环。载于第十届代数超结构及其应用国际大会，捷克共和国布尔诺，第203–215页，2009年。[28] Geronimos G Massouros 和 Christos G Massouros。超幺半群与并超环上的同态关系。*Ratio Mathematica*，13(1):61–70，1999年。[29] Anastase Nakassis。超环与超域理论的最新成果。国际数学与数学科学杂志，11，1988年。[30] Cosmin Pelea 和 Ioan Purdea。多重代数、泛代数与恒等式。澳大利亚数学学会杂志，81(1):121–140，2006年。[31] Oleg Viro。用于热带几何的超域 I：超域与去量子化。*arXiv* 预印本 *arXiv:1006.3034*，2010年。