arXiv:2603.19205v1 [math.RA] 19 Mar 2026

O有限超域的渐近行为

TUONG LE、CHAYIM LOWEN

Abstract. Hobby 最近证明，几乎所有偶数阶有限超域都不是某个域的商。我们利用概率论论证将这一结果推广到所有阶：有限超域几乎总是非商的。这证实了 Baker–Jin 的一个猜想。我们证明，在几乎所有有限超域中，任意四个或更多非零元素的和都包含零元。我们还给出了给定有限阿贝尔群上有限超域数量的精确渐近式。

1. 引言与结果概述

超域是域的一种推广，它放宽了加法必须为单值的要求。Krasner 引入了超域 [Kra57]，将其作为研究赋值域的一种手段。近年来，随着 Baker–Bowler 关于超域上的拟阵的理论（见 [BB17]）受到关注，超域再度引起人们的兴趣。这一框架同时推广了拟阵、定向拟阵和赋值拟阵，并已应用于 Lorentzian 多项式理论（[BHKL25], [HHSW25]）。

在 [Kra83], Krasner 提出了一种方法——推广了 [Kra57] 中的方法——通过将域除以乘法子群来构造超域。随后，他提出了一个问题：每个超域是否都能以这种方式得到？ [Mas85] 给出了否定的答案，并提供了一种构造反例的通用方案。 [BJ21], Baker 和 Jin 给出了一种算法，用于判定哪些有限超域是有限域的商；此外，他们还给出了超域成为无限域的商的一个必要判据。基于这些结果，他们猜想，几乎所有有限超域都是非商：

猜想 1.1 ([BJ21, 问题 (4)])。 设 $\mathcal{H}_n$ 为阶为 n的超域的同构类集合， $\mathcal{Q}_n \subseteq \mathcal{H}_n$ 为其中同构于某个域的商的那些超域所构成的子集。那么

$$\lim_{n\to\infty} \frac{\#\mathcal{Q}_n}{\#\mathcal{H}_n} = 0.$$

[Hob25], Hobby 证明了，如果我们只考虑偶数阶 n的超域，猜想 1.1 就成立。我们的主要结果是对这一猜想的完整证明。事实上，我们证明了下面这个更强的结果。

定理 1.2。 对于阶至多为 2 的有限阿贝尔群 G 和 $\epsilon \in G$ ，令 $\mathcal{H}(G,\epsilon)$ 为底层群为 G 且其中 -1 由 ϵ给出的超域集合——按保持 ϵ 的同构计。再令 $\mathcal{I}(G,\epsilon)$ 为其中属于斜域同态像的子集。那么[1]

$$\frac{\#\mathcal{I}(G,\epsilon)}{\#\mathcal{H}(G,\epsilon)} = e^{-\Omega(\#G)}.$$

[1]我们的渐近记号遵循 Knuth 在 [Knu76] 中提出的广为采用的惯例。值得注意的是，对我们而言，表达式 $f = \Omega(g)$ 的含义是存在一个 *positive* 常数 $C > 0$ ，使得对于所有充分大的 n， $f(n) \geq Cg(n)$。这与 Hardy 和 Littlewood [HL14, §2.21] 中的定义有显著差异。

推论 1.3。 渐近而言，几乎没有有限超域同构于斜域的商。[2]

我们进一步确定了一类相对简单的超域；从渐近意义上看，几乎所有有限超域都属于这一类。

定义 1.4。 若超域 $\mathrm{H} \neq \mathrm{F}_2$ 满足以下条件，则称其为*4*-满 超域：

$$0 \in a \boxplus b \boxplus c \boxplus d$$

对所有 a、 b、 c、 $d \in \mathrm{H}^\times$均成立。

注记 1.5。 4-满超域 H 具有如下性质：对所有 a_1，.....， $a_m \in \mathrm{H}^\times$ ，只要 $m \geq 4$，就有 $0 \in a_1 \boxplus \cdots \boxplus a_m$。这也是排除域 F_2的原因之一。

定义 1.6。 若对所有 $x \in \mathrm{H}$，都能找到 r、 $s \in 1 \boxplus -1$，使得 $s \neq 0$ 满足 $x = rs^{-1}$，则称超域 H 具有 0/0 性质。非正式地说，我们有“$\frac{1-1}{1-1} = \mathrm{H}$”——这就是该名称的由来。

注记 1.7. $0/0$ 超域恰好是能够自然构造（范畴论）积的那些超域。精确表述及证明见附录 A。

定理 1.8. 设阿贝尔群 G 和 $\epsilon \in G$ 的阶至多为 2，令 $\mathcal{H}(G, \epsilon)$ 表示底层群为 G 且 -1 由 ϵ 给定的超域集合（模保留 ϵ 的同构）。再令 $\mathcal{F}(G, \epsilon)$ 表示其中既是 *4*-满又是 $0/0$ 的子集。那么

$$\frac{\#\mathcal{F}(G, \epsilon)}{\#\mathcal{H}(G, \epsilon)} = 1 - e^{-\Omega(\#G)}.$$

推论 1.9. 渐近地，几乎所有有限超域都是 *4*-满且为 *0/0*。

由 [BZ23，定理 4.1] 可知，每个 4-满超域都是完美的，[3] 其意义见 [BB19]。因此，推论 1.9 表明：

推论 1.10. 几乎所有有限超域都是完美的。

在 [BSZ25 的问题 5.13], 中，Baker、Solomon 和 Zhang 询问每个超域是否都具有所谓的 FETVINS 性质。这意味着，关于 m 未知数的每个 $m+1$齐次线性方程组都有非零解。 [Hob25 的定理 5.2] 的证明表明，每个具有 0/0 性质的 4-满超域也具有 FETVINS 性质。[4] 因此，推论 1.9 表明：

推论 1.11。 几乎所有有限超域都具有 *FETVINS* 性质。

众所周知，一个原理是：足够丰富的组合结构通常不应具有任何自同构。对于有限超域而言，情况确实如此。

定理 1.12。 设 G 为有限阿贝尔群，且 $\epsilon \in G$ 的阶至多为 *2*。令 $\mathcal{H}$（G、 ϵ）为一组超域，其中底层群为 G ，且 -1 由 ϵ给出——按保持 ϵ 的同构计。令 $\mathcal{A}$（G、 ϵ）为其中具有某个非平凡自同构的超域所组成的子集。那么

$$\frac{\#\mathcal{A}(G, \epsilon)}{\#\mathcal{H}(G, \epsilon)} = e^{-\Omega(\#G^2)}.$$

[2]超域按定义是交换的，但它们可能是非交换斜域的商。有关示例，请参见注 2.19。[3]这种完美性的概念与域论中名称相同的概念无关。相反，它与给定超域上的拟阵理论是否表现良好有关。[4]更确切地说，在其引理 5.4 中，Hobby 表明，他所称的 $ample$ 超域具有我们在命题 2.25 中标记为（$\star$）的性质，而其定理 5.4 的证明表明，（$\star$）蕴含 FETVINS。在命题 2.25 中，我们证明了（$\star$）等价于 4-满性与 0/0 性质的合取。

推论 1.13。 几乎所有有限超域都没有非恒等自同构。

最后，借助定理 1.12，我们给出了一个渐近公式，用于计算乘法群为给定阿贝尔群 G 的超域的同构类数量。

定理 1.14。 设 G 是一个充分大的[5] 有限阿贝尔群。设 $\mathcal{H}(G)$ 为底层群为 G 的超域同构类的集合。则

$$\#\mathcal{H}(G) = \left(1 - e^{-\Theta(\#G)}\right) \frac{\#G[2]}{\#\operatorname{Aut} G} \cdot 2^{\frac{1}{6}(\#G^2+3\#G+2\#G[3])}$$

其中， $G[2]$ 和 $G[3]$ 分别是 G 的 *2*-挠子群和 *3*-挠子群。[6]

推论 1.15。 设 $\mathcal{H}_n$ 为阶为 n 的超域同构类的集合。则

$$\log_2 \#\mathcal{H}_n = n^2/6 + O(n)\,.$$

这些结果证明中最重要的要素，是超域中基本对的六边形这一简单但实用的概念。这些概念最早出现在 Semple 的学位论文[Sem98]中。后来，Pendavingh 和 Van Zwam[PZ10] 在偏域的框架下开展的工作，使这些概念得到了更明确的阐述。Baker 和 Lorscheid [BL25b]将这些思想应用到了更一般的牧场框架中——超域可以看作牧场的一种特殊情形——并且还创造了“六边形”这一富有表现力的术语。他们的框架与 Hobby 所采用的块这一概念基本等价。我们沿用较早的 Baker–Lorscheid 命名法，但对其含义作了细微调整（见备注 2.22）。

论文概述。 在第 2 节中，我们定义超域、六边形和基本对，并阐释它们之间的关系。在第 3 节中，我们搭建用于证明主要结果的概率框架。随后，我们利用该框架证明随机有限超域的基本性质。在第 4 节中，我们利用前面的工作推导出上述宣布的结果。最后，我们在第 5 节中讨论将我们的结果推广到有限斜超域这一情形的可能性。在附录 A 中，我们展示 $0/0$ 性质与超域的乘积构造之间的密切联系。在附录 B 中，我们证明有限超域在有限斜超域中占据主导地位。

2. Hyperfields、 pastures and hexagons

本节将讨论我们研究结果所需的背景知识。首先，在略微更一般的斜超域框架下展开讨论将更为方便。出于这一点及其他原因，我们始终采用乘法记号表示群——无论群是否为阿贝尔的——并用 1 表示它们的单位元。

关于多值二元算子的一点说明。给定一个集合 S，一个多值二元算子是一个函数 $\star\colon S \times S \to \mathcal{P}(S)$，其中 $\mathcal{P}(S)$ 是 S 的幂集。按照通常的约定，给定 $s,\ t \in S$ 我们将 $s \star t$ 记作 $\star(s,\ t)$。给定这样的二元算子，我们可以自然地将其扩展为 $\mathcal{P}(S)$ 上的二元算子，定义如下

$$A \star B = \bigcup_{\substack{a\in A\\ b\in B}} a \star b$$

[5]要求 G 足够大，是为了确保表达式 $\#G[2]\,\#\operatorname{Aut} G \cdot 2^{\frac{1}{6}(\#G^2+3\#G+2\#G[3])}$ 是底层群为 G 的超域数量的一个 *overestimate*。[6]这里我们采用 Knuth 的 Θ 记号： $f = \Theta(g)$ 是 $f = \Omega(g)$ 与 $g = \Omega(f)$ 的合取。

对于 $s \in S$ 和 $A \subseteq S$，我们也将 $s \star A$ 记作 $\{s\} \star A$，将 $A \star s$ 记作 $A \star \{s\}$。如果对于所有 s、$t \in S$，都有 $s \star t = t \star s$，则称$\star$是交换的。当且仅当单值算子 $\star\colon \mathcal{P}(S) \times \mathcal{P}(S) \to \mathcal{P}(S)$ 是交换的，这一性质才成立。类似地，如果对于所有 s、t、$u \in S$，都有 $(s\star t)\star u = s\star(t\star u)$，则称 $\star$是结合的。同样，当且仅当 $\star\colon \mathcal{P}(S)\times\mathcal{P}(S) \to \mathcal{P}(S)$ 是结合的，这一性质才成立。与单值结合运算的情形一样，如果 $\star$ 是结合的，我们就可以无歧义地写出诸如 $x_1 \star x_2 \star \cdots \star x_n$ 这样的表达式——此时每个 x_i 都可以是 S 的一个元素或子集。[7]

定义 2.1。斜超域是一个六元组 $\mathrm{H} = (G,\ \cdot,\ \boxplus,\ 0,\ 1,\ -1)$，其中

- $(G,\ \cdot,\ 1)$ 是一个群，称为 H 的底层群。我们将 $\mathrm{H}^\times$ 记作 G。
- $-1 \in G$ 是 G 的中心中的一个元素，满足 $(-1)^2 = 1$，称为 H 的单位元。
- 0 是一个形式上添加的符号，原本不包含于 G中。我们称 0 为 H 的零元。我们将 H 与集合 $G \sqcup \{0\}$ 等同。通过对所有 $g \in G$设置 $0 \cdot 0 = 0 \cdot g = g \cdot 0 = 0$，我们形式上扩展 $\mathrm{H}^\times$ 上的乘法规则。[8]

- $\boxplus\colon \mathrm{H} \times \mathrm{H} \to \mathcal{P}(\mathrm{H})$ 是一个多值二元算子，称为加法。

使得这些元素共同满足

（I）运算符 $\boxplus$是结合且交换的。（II）对于任意 $g,\ h \in \mathrm{H}$，成立 $0 \in g \boxplus h$ 当且仅当 $g = -1 \cdot h$。（III）对于所有 $g,\ h,\ k \in \mathrm{H}$，成立 $g(h \boxplus k) = gh \boxplus gk$和 $(h \boxplus k)g = hg \boxplus kg$。

若 G是阿贝尔的，我们称 H 为超域。

注 2.2. 我们用 $-g$ 表示 $g \in \mathrm{H}$，意为 $-1 \cdot g$。注意，正如预期的那样，$-(-g) = g$。

注 2.3. 通常会将 $g \boxplus 0 = 0 \boxplus g = \{g\}$ 对所有 $g \in \mathrm{H}$ 都成立列为一条公理。在我们的设定中，这可由 $\boxplus$ 的交换律以及以下等价关系推出

$$x \in g \boxplus 0 \overset{\text{(II)}}{\Leftrightarrow} 0 \in -x \boxplus (g \boxplus 0) \overset{\text{(I)}}{\Leftrightarrow} 0 \in (-x \boxplus g) \boxplus 0 \overset{\text{(II)}}{\Leftrightarrow} -x \boxplus g \ni -1 \cdot 0 = 0 \overset{\text{(II)}}{\Leftrightarrow} -g = -x \Leftrightarrow g = x$$

类似地，规则 $g \in h \boxplus k$ 当且仅当 $h \in g \boxplus -k$ 对于 $g,\ h,\ k \in \mathrm{H}$ 成立，这可由

$$g \in h \boxplus k \overset{\text{(II)}}{\Leftrightarrow} 0 \in -g \boxplus (h \boxplus k) \overset{\text{(I)}}{\Leftrightarrow} 0 \in h \boxplus (-g \boxplus k) \overset{\text{(III)}}{\Leftrightarrow} 0 \in -h \boxplus (g \boxplus -k) \overset{\text{(II)}}{\Leftrightarrow} h \in g \boxplus -k$$

注 2.4. 尽管我们允许 $\boxplus$输出 H 的任意子集，但实际上不可能出现$g \boxplus h = \varnothing$。因为若如此，先应用 (II)，再应用 (I)，就会得到

$$\{h\} = 0 \boxplus h \subseteq (-g \boxplus g) \boxplus h = -g \boxplus (g \boxplus h) = -g \boxplus \varnothing = \varnothing$$

注 2.5. 根据注 2.3，指定斜超域时，无须指定与 0 的加法。同样，根据规则 (III)，只需为所有 $g \in \mathrm{H}^\times$ 指定 $1 \boxplus g$。$g, h \in \mathrm{H}^\times$ 时 $g \boxplus h$ 的值可由 $g \boxplus h = g(1 \boxplus g^{-1}h)$ 推出。最后，-1 的值可根据以下事实推出：$0 \in 1 \boxplus g$ 当且仅当 $g = -1$。

例 2.6. 任意斜域 F 都能导出一个典范斜超域，其底层群为 $\mathrm{F}^\times$，加法定义为 $a \boxplus b := \{a + b\}$。当且仅当 F 是域时，它才是超域。以这种方式得到的斜超域 F，恰好是其中 $\boxplus$ 为单值的那些斜超域。也就是说，对于所有 $a,\ b \in \mathrm{F}$，都有 $\#(a \boxplus b) = 1$。

---

[7]按照数学各领域的惯例（集合论除外），我们默认所讨论的集合 S 与其幂集不相交，因此不会产生歧义。

[8]读者会注意到，此时乘法是 H 上的一个结合二元运算，单位元为 1，且可逆元恰好是 $\mathrm{H}^\times$ 中的元素。若 G 是阿贝尔的，则乘法是交换的。

注记 2.7. 要验证（斜）超域中的 $\boxplus$ 是单值的，实际上只需验证 $1\boxplus -1=\{0\}$。确实，若此条件成立，那么对于任意 $a,\ b\in \mathrm{F}$ 以及任意 $x,\ y\in a\boxplus b$
$x\boxplus -y\subseteq (a\boxplus b)\boxplus -(a\boxplus b)=(a\boxplus -a)\boxplus (b\boxplus -b)=a(1\boxplus -1)\boxplus b(1\boxplus -1)$
$=\{0\}\boxplus\{0\}=\{0\}$根据注 2.4 和公理（II），这意味着 $x=y$。

例 2.8。 若取 G 为平凡群，并令 $1\boxplus 1=\{0,1\}$，所得超域称为 ***Krasner*** 超域，记作 K。

例 2.9。 若取 $G=\{1,-1\}$——即二阶循环群——并定义 $1\boxplus 1=\{1\}$,$1\boxplus -1=\{1,0,-1\}$，所得超域称为 符号超域，记作 S。

例 2.10。 取 $G=\mathrm{R}_{>0}$，将 $G\sqcup\{0\}$ 与 $\mathrm{R}_{\geq 0}$ 视为相同，并定义加法 b y

$$x\boxplus y\coloneqq\begin{cases}\{\max(x,y)\} & \text{if } x\neq y\\ [0,x] & \text{if } x=y\end{cases}$$

那么所得的超域称为热带超域，记作 T_0。

例 2.11。 取 $G=\mathrm{R}_{>0}$，将 $G\sqcup\{0\}$ 与 $\mathrm{R}_{\geq 0}$ 视为相同，并定义

$$x\boxplus y=\{z\in \mathrm{R}_{\geq 0}\mid x,\ y,\ z\text{构成一个可能退化的三角形的边长}\}$$

那么所得的超域称为三角超域，记作 T_1。

定义 2.12。 斜超域 H 与 G 之间的同态是一个群同态 $f\colon \mathrm{H}^\times\to \mathrm{G}^\times$，它通过形式化地令 $f(0)=0$扩展后满足

$$f(g\boxplus h)\subseteq f(g)\boxplus f(h)$$

对于所有 $g,\ h\in \mathrm{H}^\times$。由此得到一个斜超域范畴。例 2.6 中将斜域重新解释为斜超域的过程，诱导出一个从斜域范畴到斜超域范畴的完全忠实嵌入。显然，域的子范畴落在超域的子范畴之内。

注 2.13。 如果 $f\colon \mathrm{H}\to \mathrm{G}$ 是一个斜超域同态，那么按照约定$f(0)=0$，对于所有 $g,\ h\in \mathrm{H}$，有 $f(gh)=f(g)f(h)$。此外，$f(-1)=-1$。

斜超域之所以受到关注，主要是因为它们与斜域之间的相互作用。例如，从斜域 F 出发的同态 $\mathrm{F}\to \mathrm{S}$ 与 F 的一个全序所包含的数据相同；同态 $\mathrm{F}\to \mathrm{T}_0$ 与 F 上一个（取实值的）赋值所包含的数据相同；而同态 $\mathrm{F}\to \mathrm{T}_1$ 与 F 上一个绝对值所包含的数据相同。斜域与斜超域之间更直接的相互作用由以下构造给出。

定义 2.14. 设 F 是一个斜域，且 $\Gamma\subseteq \mathrm{F}^\times$ 是其乘法群的一个正规子群。群 $\mathrm{F}^\times/\Gamma$ 配备了典范斜超域结构（见 [Kra83]）。具体而言，对于 $a,b\in \mathrm{F}^\times/\Gamma\cup\{0\}$，我们定义

$$\bar{a}\boxplus\bar{b}=\left\{\overline{\alpha+\beta}\mid \alpha,\beta\in\mathbb{F},\bar{\alpha}=\bar{a},\bar{\beta}=\bar{b}\right\}$$

其中，$\bar{x}$ 表示陪集 $x\Gamma$，若 $x\in \mathrm{F}^\times$ 且 $\bar{0}=0$。所得超域记作 F/Γ，并配备典范的商同态 $\mathrm{F}\to \mathrm{F}/\Gamma$。若一个斜超域与这种形式的斜超域同构，则称其为商 斜超域。

注 2.15. 商构造可以更一般地定义，只要 F 是一个斜超域即可。不过，我们并不需要如此一般的情形。

E例 2.16. 例 2.9 中的符号超域 S 是商 $\mathrm{R}/\mathrm{R}_{>0}$。

例 2.17. 例 2.8 中的 Krasner 超域 K 是商 F/F$^\times$ ，其中 F 是任意基数至少为 3 的斜域。

例 2.18。 例 2.11 中的三角超域 T_1 是商 C/S^1 ，其中S^1 是模为 1 的复数群。

注 2.19。 域的每个商都是超域。然而，非交换斜域可能具有一个超域商。例如，若 H 是实四元数代数，则 H/[H$^\times$，H$^\times$] 是一个与 T_1同构的超域。根据例 2.18，T_1 也是 C 的一个商。本文作者未能构造出这样一个超域的例子：它是某个非交换斜域的商，但不是任何域的商（参见问题 5.1）。

现在我们开始具体分析超域。我们将用满足 $a \boxplus b \boxplus c \ni 0$ 的三元组（a、 b、 c）来描述它们。我们先给出以下定义。

定义 2.20。 设 G是一个阿贝尔群。 G^3集合上有 G 和 S_3 的自然作用，前者通过乘法作用，后者通过置换坐标作用。 G 的一个基本对 是 G^3的一个 G-轨道。我们将元素 $(x, y, z) \in G^3$ 的轨道与对 (xz^{-1}, yz^{-1}) 等同——因此得名。由此可将基本对集合与 G^2等同。

G 的一个六边形 是 G^3的一个 $(S_3 \times G)$-轨道。对于 $(x, y, z) \in G^3$的 $(S_3 \times G)$-轨道，我们记作 (x, y, z)。我们将 $(x, y, z) \in G^3$ 的六边形与对应的六个基本对所构成的多重集等同。这些是

$$(xz^{-1}, yz^{-1}),\ (yz^{-1}, xz^{-1}),\ (xy^{-1}, zy^{-1}),\ (zy^{-1}, xy^{-1}),\ (yx^{-1}, zx^{-1}),\ (zx^{-1}, yx^{-1})$$

用基本对 (u, v) 表示：$= (xz^{-1}, yz^{-1})$，这六个分别是

$$(u, v),\ (v, u),\ (uv^{-1}, v^{-1}),\ (v^{-1}, uv^{-1}),\ (vu^{-1}, u^{-1}),\ (u^{-1}, vu^{-1})$$

群 S_3 作用于 G 的所有基本对构成的集合，每个轨道都是一个六边形。我们用 $\hexagon(G)$ 表示 G 的六边形集合，用 (u, v) 表示包含基本对 (u, v) 的六边形。我们可以通过图 1 所示的六边形图来直观呈现这些数据。

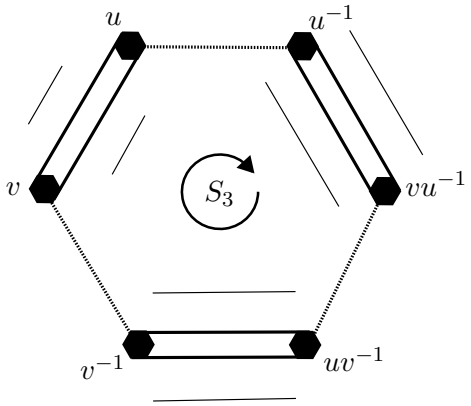


FIGURE 1. 基本对的一个六边形

由定义 2.1 中的公理 (I) 和 (III) 可知，对于超域 H，集合

$$\{(a, b, c) \in \mathbb{H}^\times \mid 0 \in a \boxplus b \boxplus c\}$$

在 S_3的置换作用和(H$^\times$)^3 的乘法作用下保持不变。因此，自然会考虑 $\hexagon$(H$^\times$)中相应的六边形集合。

不难根据公理 (I)–(III) 看出，超域由以下数据确定：(i) 其底层群，(ii) 其单位元，以及 (iii) 其六边形集合——也就是说，所有满足 $x \boxplus y \boxplus z \ni 0$ 的 $(x,\ y,\ z) \in G^3$ 的集合（参见命题 2.23）。不过，并非每一组这样的数据都能构成超域。因此，有必要为由这类数据组成的较简单结构命名。Baker 和 Lorscheid 在 [BL21], 中将其称为“牧场”。在 [BL25a] 中，牧场被有效地用于系统化并推广拟阵表示理论中的若干结果。现在，我们基于上述框架定义牧场。作为比较，请参见 [BL25a，定义 2.1]。

D定义 2.21。 一个牧场 P 由三元组 $\mathrm{P} = (G,\ -1,\ \mathrm{Hex(P)})$ 构成，其中

- G是一个阿贝尔群，称为 P 的底层群 ，记作 $\mathrm{P}^\times$。
- $-1 \in G$ 是满足 $(-1)^2 = 1$ 的元素，称为 P 的单位元 。
- $\mathrm{Hex(P)} \subseteq \bigcirc(G)$ 是 G 的六边形子集，称为 P 的（非平凡）零集 。

备注 2.22。 我们在两方面偏离了 [BL21] 中的术语。首先，在 Baker–Lorscheid 的约定中，$(x,\ y,\ z)$ 的基本对表示为 $(-xz^{-1},\ -yz^{-1})$，而不是 $(xz^{-1},\ yz^{-1})$。我们的约定具有一个优点，即群 G 中可用的六边形集合与单位元 -1 无关。其次，按照 Baker 和 Lorscheid 的含义，零集 ——用我们的术语来说——是集合

$$\{0+0+0\} \cup \{x+\epsilon x+0 \mid x \in G\} \cup \left\{ x+y+z \;\middle|\; \overline{(x,y,z)} \text{ lies in } \mathrm{Hex}(\mathbb{P}) \right\}$$

其中， $a+b+c$ 是一个形式符号，表示 $(\mathrm{P}^\times \sqcup \{0\})^3$ 中 $(a,\ b,\ c)$ 的 S_3-轨道。我们当前的约定将使后续论证更加清晰。

正如我们已经观察到的，对于一个超域 H，我们可以将其与如下牧场相联系：底层群 $G = \mathrm{H}^\times$、H 的单位元 -1 以及 H 的六边形。下面我们刻画那些能够产生超域的牧场。

命题 2.23。 与一个超域相关联的牧场能够唯一确定该超域。在一个群 G 上的牧场 $\mathbb{P}$ 源自一个超域，当且仅当满足以下两个条件：
(A) 对于所有 $x \in G$ 满足 $x \neq -1$的情形，存在 $y \in G$，使得 $\overline{(x,y)} \in$ *Hex(P)*。*(B)* 对于所有 x、y、z、$w \in G$，如果 $\overline{(x,y)} \in$ *Hex(P)*、$\overline{(z,w)} \in$ *Hex(P)*，且 $\overline{(x,y)} \neq \overline{(z,w)}$，那么存在 $t \in G$，使得 $\overline{(tx,-tz)} \in$ *Hex(P)* 且 $\overline{(-ty,tw)} \in$ *Hex(P)*。

证明。 设 $G := G \sqcup \{0\}$。若 P 是某个超域的牧场，则可以通过以下规则恢复加法算子 $\boxplus$

$$x \boxplus y := \begin{cases} \{y\} & \text{if } x = 0 \\ \{x\} & \text{if } y = 0 \\ \left\{ z \in G \;\middle|\; \overline{(x,y,-z)} \in \mathrm{Hex}(\mathbb{P}) \right\} & \text{if } x,y \in G,\ x \neq -y \\ \left\{ z \in G \;\middle|\; \overline{(x,y,-z)} \in \mathrm{Hex}(\mathbb{P}) \right\} \cup \{0\} & \text{if } x,y \in G,\ x = -y \end{cases}$$

另一方面——对于任意牧场 P（G）——如果我们按此规则定义 二元算子 $\boxplus$：$G \times G \to \mathcal{P}(G)$，那么 $\boxplus$ 是一个定义良好、交换的多值二元算子。根据构造，它满足定义 2.1 的公理（II）。我们验证它满足公理（III）。注意，$g(h \boxplus k) = gh \boxplus gk$ 在 $g = 0$ 时显然成立；若 $h = 0$，则由 $x \boxplus 0 = 0 \boxplus x = \{x\}$ 可得，或者

$k=0$。因此，我们可以假设 $g,\ h,\ k\in G$。那么，根据构造，对于 $z\in G$

$$\begin{aligned} z\in gh\boxplus gk &\Leftrightarrow \overline{(gh,gk,-z)}\in \mathrm{Hex}(\mathbb{P})\\ &\Leftrightarrow \overline{(h,k,-g^{-1}z)}\in \mathrm{Hex}(\mathbb{P})\\ &\Leftrightarrow g^{-1}z\in h\boxplus k \Leftrightarrow z\in g(h\boxplus k)\end{aligned}$$

由于 G 是阿贝尔的，这足以证明 (III)。现在还需确定 $\boxplus$的结合律。注意，根据 $\boxplus$的交换律，结合律可归结为以下断言

$$\text{for all } g,h,k\in G,\quad (g\boxplus h)\boxplus k\subseteq g\boxplus(h\boxplus k)$$

我们证明，当且仅当 P 满足条件 (A) 和 (B) 时，该结论成立。若 g,h,k 中任意一个为 0，则恒等式 $(g\boxplus h)\boxplus k=g\boxplus(h\boxplus k)$ 显然成立。设 $g,h,k\neq 0$。由 (II) 成立可得

$$0\in(g\boxplus h)\boxplus k \Leftrightarrow -k\in g\boxplus h \Leftrightarrow \overline{(g,h,k)}\in \mathrm{Hex(P)} \Leftrightarrow -g\in h\boxplus k \Leftrightarrow 0\in g\boxplus(h\boxplus k)$$

由此情形可得，对于 $z\in G$ ，有

$$z\in(g\boxplus h)\boxplus k \Leftrightarrow 0\in((g\boxplus h)\boxplus k)\boxplus -z \Leftrightarrow 0\in(g\boxplus h)\boxplus(k\boxplus -z)$$

同样地，$z\in g\boxplus(h\boxplus k)$ 当且仅当 $0\in(-z\boxplus g)\boxplus(h\boxplus k)$。令 $\ell=-z$，结合律条件可写为

(1) 对于所有 g、h、k、$\ell\in G$，如果 $0\in(g\boxplus h)\boxplus(k\boxplus\ell)$，那么 $0\in(g\boxplus\ell)\boxplus(h\boxplus k)$

假设 $0\in(g\boxplus h)\boxplus(k\boxplus\ell)$ 成立。这恰好意味着以下情况之一成立。

- $0\in g\boxplus h$ 且 $0\in k\boxplus\ell$。
- $s\in g\boxplus h$ 且对于某个 $s\in G$，$-s\in k\boxplus\ell$。

我们证明，(1) 在第一种情况下成立恰好是条件 (A)，而在第二种情况下成立恰好是条件 (B)。

在第一种情况下，$h=-g$ 和 $k=-\ell$。所需的结论是

$$0\in(g\boxplus\ell)\boxplus(-g\boxplus-\ell)=(g\boxplus\ell)\boxplus-(g\boxplus\ell)$$

当且仅当 $g\boxplus\ell\neq\varnothing$时，这一结论成立。若 $g=-\ell$，显然成立。否则，它等价于存在 $q\in G$，使得 $(g,\ell,q)\in$Hex(P)，即 $(g\ell^{-1},q\ell^{-1})\in$Hex(P)。由于 g 和 ℓ 是任意的，这恰好归结为条件 (A)。

在第二种情况下，关于 g、h、k、ℓ 的假设是存在 $s\in G$，使得 $(g,h,s)\in$Hex(P)，且 $(k,\ell,-s)\in$Hex(P)。根据公理（III），所讨论的条件在 G 的乘法作用下保持不变。因此，将 g、h、k、ℓ 乘以s^{-1}后，假设变为 $(g,h,1),(k,\ell,-1)\in$Hex(P)。也就是说，$(g,h),(-k,-\ell)\in$Hex(P)。

若 $g=-\ell$ 和 $h=-k$，则 (1) 的结论显然成立。若 $g\neq-\ell$ 或 $h\neq-k$，则 (1) 的结论等价于存在 $r\in G$，使得 $(g,\ \ell,\ r)\in$Hex(P)，且 $(h,\ k,\ -r)\in$Hex(P)。我们将其改写为

$$\overline{(r^{-1}g,r^{-1}\ell)}\in\mathrm{Hex}(\mathbb{P})\quad\text{and}\quad\overline{(-r^{-1}h,-r^{-1}k)}\in\mathrm{Hex}(\mathbb{P})$$

利用对应关系 $x\leftrightsquigarrow g$, $y\leftrightsquigarrow h$, $z\leftrightsquigarrow-\ell$, $w\leftrightsquigarrow-k$, $t\leftrightsquigarrow r^{-1}$，我们恰好得到条件 (B)。□

注 2.24。当且仅当超域不是域时，条件 (A) 中的限制 $x\neq-1$ 可以去掉。这是对注记 2.7 的重述。

以下结果使用第 1 节（定义 1.4 和 1.6）中定义的*4*-满 和 *0/0* 超域的概念。

命题 2.25. 牧场$\mathbb{P}$ 当且仅当满足以下条件时，能够导出一个 *4*-满、*0/0* 超域：

$(\star)$ *For all* $x, y, z, w \in G$*, there exists* $t \in G$ *such that both* $\overline{(tx, ty)}, \overline{(tz, tw)} \in \mathrm{Hex}(\mathbb{P})$.

证明。 假设 P 满足 $(\star)$。对于任意 $x \in G$，将 $(\star)$ 应用于 $(1, x, 1, x)$，可知存在 t，使得 $(t, tx) \in$ Hex(P)，这意味着 $(t^{-1}, x) \in$ Hex(P)。因此，P 满足命题 2.23 中的条件 (A)。条件 (B) 也显然成立。于是 P 由此导出一个超域。

令 $s = t^{-1}$，性质 $(\star)$ 可以用超域的语言表述如下：

$(\star\star)$ 对所有 $x, y, z, w \in G$，都存在 $s \in G$，使得 $s \boxplus x \boxplus y \ni 0$ 且 $s \boxplus z \boxplus w \ni 0$。

因此，只需证明一个超域满足 $(\star\star)$ 当且仅当它是 4-满的，并且 $0/0$.我们将证明，一个超域是 4-满的当且仅当对 $y \neq -x, z \neq -w$，$(\star\star)$ 成立；而它是 $0/0$ 当且仅当在特殊情形 $y = -x, z = -w$ 下 $(\star\star)$ 成立。

对于前半部分，注意到 $0 \in x \boxplus y \boxplus z \boxplus w$ 当且仅当存在 $s \in$ H，使得$s \in x \boxplus y$ 并且 $-s \in z \boxplus w$.。若 $y = -x$ 且 $z = -w$，则取 $s = 0$ 即可使该条件显然成立。否则， s 不能取 0，而该条件等价于：$-x \boxplus -y \boxplus s \ni 0$ 并且 $s \boxplus w \boxplus z \ni 0$.。也就是说，对于 $(-x,\ -y,\ z,\ w)$，这等价于 $(\star\star)$。由于$x \mapsto -x$ 是 G 上的一个对合，我们已经证明，除非 $y = -x,\ z = -w$.，否则 4-满性等价于 $(\star\star)$ 成立。

现在我们证明剩余的断言： $0/0$ 性质等价于对所有满足 $x, z \in G$ 的四元组 $(x, -x, z, -z)$，$(\star\star)$ 均成立。事实上，注意到 $x \boxplus -x \boxplus t \ni 0$与 $-1 \boxplus 1 \boxplus -x^{-1}t \ni 0$相同，而后者又与 $x^{-1}t \in 1 \boxplus -1$. 相同。因此，令 $S = 1 \boxplus -1$，则 $(x, -x, z, -z)$ 中 $(\star\star)$ 的内容为：存在 t 使得 $x^{-1}t \in S$ 且 $z^{-1}t \in S$.。这成立当且仅当 zx^{-1} 可以表示为 rs^{-1}，其中 $r, s \in S$.。因此，该断言由映射 $(x, z) \mapsto zx^{-1}$ 从 G^2 到 G 是满射这一事实得出。□

定义牧场之间的态射将很有用。例如， [BL25b]中已经给出了这一定义。我们按照自己的约定表述该定义。

定义 2.26. 从牧场 P_1 到牧场 P_2 的态射 是一个群同态 $f : \mathrm{P}_1^\times \to \mathrm{P}_2^\times$，它将 P_1 的单位元映射到 P_2 的单位元，并且满足

$$\text{if} \quad \overline{(x, y)} \in \mathrm{Hex}(\mathbb{P}_1) \quad \text{then} \quad \overline{(f(x), f(y))} \in \mathrm{Hex}(\mathbb{P}_2)$$

以下命题的证明很容易，我们略去。

命题 2.27. 超域同态会导出相应牧场之间的态射。牧场之间的每个态射都可由此方式得到。这定义了从超域范畴到牧场范畴的完全忠实嵌入。

3. A hyperfield lottery

在本节中，我们固定一个基数为 n 的有限阿贝尔群 $G = \#G$，以及一个满足 $\epsilon^2 = 1$ 的“单位元”$\epsilon \in G$。我们将考虑如下过程：在 G 上构造一个单位元为 ϵ 的随机牧场，即从 $\mathcal{N} \subseteq \mathcal{O}(G)$ 中均匀随机地选取一个子集，从而得到牧场 $\mathrm{P} = (G,\ \epsilon,\ \mathcal{N})$。由此得到一个取值于牧场的随机变量 $\mathbb{\Pi}$。我们称之为超域抽签，原因很快就会明了。注意，选择 $\mathcal{N}$ 也可以用以下等价方式描述： $\mathcal{O}(G)$ 中的每个元素都以 $1\ 2$ 的概率独立于其他所有六边形被纳入 $\mathcal{N}$。将概率语言转化为计数陈述很简单： $\mathbb{\Pi}$ 以概率 p 满足条件 X，当且仅当具有性质 X 的 $(G,\ \epsilon)$ 上的牧场数量为 $p \cdot 2^{\#\mathcal{O}(G)}$。不过，原因或许已经显而易见，以概率的方式来表述问题将非常有用。

下文将证明超域抽签的若干性质。首先要证明的是，它几乎总会得到一个超域。具体而言，我们给出一个下界，说明 $\mathbb{\Pi}$ 满足命题 2.25 的条件 $(\star)$ 的概率至少为多少。

命题 3.1。当 n 足够大时，对于某个绝对常数 $c>0$，$\mathbb{\Pi}$ 满足 $(\star)$ 的概率至少为 $1-e^{-cn}$。

Proof. 只需证明：对于某个绝对常数 $c>0$ 以及任意 x、y、z、$w\in$, G $\to$ 以至少 $1-e^{-cn}$ 的概率，$(tx$、$ty)\in\overline{\mathcal{N}}$ 和 $\overline{(tz}$、$tw)\in\overline{\mathcal{N}}$ 同时对至少一个 $t\in G$ 成立。

事实上，如果对于所有 $(x$、y、z、$w)\in G^4$ 都是这种情况，那么 $(\star)$ 将以至少 $1-n^4e^{-cn}$ 的概率成立。对于任意 $0<c'<c$ 以及足够大的 n，该概率下界为 $1-e^{-c'n}$。

现在固定 x、y、z、w，并考虑由六边形的（无序）对组成的序列 s

$$h_t\coloneqq\left\{\overline{(tx,ty)},\overline{(tz,tw)}\right\},\qquad(t\in G)$$

（注意，h_t 可能退化为只包含一个元素。）

$t\in G$ 对应的元组（tx，ty）彼此各不相同。对于（tz，tw）也是如此。由于一个六边形至多包含 6 个元素，因此（G，ϵ）中的每个六边形至多可以出现在 h_t 个不同的六边形对中。我们构造一个图 Γ，其顶点集为 G：当六边形对 h_s 和 h_t 交于同一个六边形时，就在 s 与 $t\in G$ 之间连一条边。于是，Γ 有 n 个顶点，并且 Γ 中每个顶点的度至多为 $2\times(12-1)=22$。根据标准的图论论证，这保证了 Γ 包含一个大小为 $\geq n/23$ 的独立集。也就是说，我们可以找到 t_1、.....、$t_m\in G$，使得 $m=\lceil n/23\rceil$，并且 h_{t_1}、.....、h_{t_m} 两两不相交。对于任意 i，h_{t_i} 中的一个或两个六边形属于 $\mathcal{N}$ 的概率至少为 $\left(\frac{1}{2}\right)^2=1/4$。回想一下，在选择 $\mathcal{N}$ 时，某个六边形是否被包含的这些事件彼此完全独立。由于六边形对 h_{t_1}、.....、h_{t_m} 两两不相交，

$$\mathbb{P}\left[h_{t_1}\nsubseteq\mathcal{N}\wedge\cdots\wedge h_{t_m}\nsubseteq\mathcal{N}\right]=\prod_{i=1}^{m}\mathbb{P}\left[h_{t_i}\nsubseteq\mathcal{N}\right]\leq\left(1-\frac{1}{4}\right)^m\leq\left(\frac{3}{4}\right)^{n/23}$$

如果对于某个 i，$h_{t_i}\subseteq\mathcal{N}$，那么上述陈述对 (x,y,z,w) 成立。因此，我们可以取 $c=\frac{1}{23}\log(4/3)$。□

上述命题给出了 $\mathcal{N}$ 不是超域的概率上界。以下结果给出了这一概率的下界。

命题 3.2. 在超域抽签中，若 $n\geq2$，则 $\mathbb{\Pi}$ 不是超域的概率至少为 2^{-n}。

证明。设 $g\in G\setminus\{\epsilon\}$。$\mathbb{\Pi}$ 的零集不包含任何形如 (g,x) 的六边形的概率至少为 2^{-n}，因为这类六边形至多有 n 个。此时，$\mathbb{\Pi}$不可能是超域，因为它不满足命题 2.23 的条件 (A)。□

命题 3.3. 对所有 $x\in G$，$(\epsilon,x)\in\mathcal{N}$ 的概率至多为某个绝对常数 $c>0$ 的 e^{-cn}。

证明。当 x 遍历 G时，表达式 (ϵ,x) 至少取到 $\overline{n/6}$ 个不同的值。令 $x_1,\ldots,x_m\in G$ 满足 (ϵ,x_1) $\ldots,(\epsilon,x_m)$ 互不相同，且 $m=\overline{\lceil n/6\rceil}$。事件 “$\overline{(\epsilon,x_i)}$ 中某一个包含在 $\mathcal{N}$ 中 ” 彼此独立，每个事件发生的

概率为 1 2。因此

$$\mathbb{P}\left[\overline{(\epsilon, x_1)} \in \mathcal{N} \wedge \cdots \wedge \overline{(\epsilon, x_m)} \in \mathcal{N}\right] = \prod_{i=1}^{m} \mathbb{P}\left[\overline{(\epsilon, x_i)} \in \mathcal{N}\right] = \left(\frac{1}{2}\right)^m \leq \left(\frac{1}{2}\right)^{n/6}$$

因此我们可以取 $c = \frac{1}{6}\log 2$。 □

之　在讨论下一个性质之前，我们需要以下几个基本观察。

引理 3.4. 设$\mathbb{H}$ 是 G 上的任意超域。那么$\mathbb{H}$ 至少有$(n-1)/6$ 个六边形。

证明。 任取元素 $x \neq 0, -1 \in$H。由注 2.4，集合 $x \boxplus 1$ 中含有某个非零元素 y。于是 $x \boxplus -y \ni -1$。因此，$(x, -y)$ 是一个基本对。由此可知，H 的 $n-1$ 个元素都属于 H 中某个六边形的基本对。由于每个六边形至多包含 6 个元素，便得到所需的下界。□

引理 *3.5. </style}*自同态 $G \to G$至多有 $n^{\log_2 n}$ 个。

证明. 根据有限阿贝尔群结构定理，我们可以写成 $G = \prod_{i=1}^{m} G_i$，其中每个 G_i 都是非平凡循环群。由于从循环群出发的同态由生成元的像决定，因此我们有

$$\#\operatorname{Hom}(G, G) = \#\prod_{i=1}^{m} \operatorname{Hom}(G_i, G) = \prod_{i=1}^{m} \#\operatorname{Hom}(G_i, G) \leq \prod_{i=1}^{m} \#G = n^m$$

另一方面，

$$n = \#G = \#\prod_{i=1}^{m} G_i = \prod_{i=1}^{m} \#G_i \geq \prod_{i=1}^{m} 2 = 2^m$$

因此 $m \leq \log_2 n$，且 #Hom(G, G) $\leq n^{\log_2 n}$。 □

注 3.6. 在所有有限群这一一般情形下，可以得到更精确的上界。例如参见 [Neu95]。上述粗略上界足以满足我们的需要。

命题 3.7. 设 $\mathbb{H}$ 是定义在 G 上的超域。对于充分大的 n，存在双射态射 $\mathbb{H} \to \mathbb{\Pi}$ 的概率至多为 e^{-cn}，其中 $c > 0$ 是某个绝对常数。

证明。 底层群同态$G \to G$至多有 # Aut G 种可能。根据引理 3.5，

$$\#\operatorname{Aut} G \leq \#\operatorname{Hom}(G, G) \leq n^{\log_2 n} \leq e^{(\log_2 n)^2} = e^{o(n)}$$

只需证明，恒等元 映射 $G \to G$ 诱导出一个态射 H $\to \mathbb{\Pi}$ 的概率至多为某个绝对常数 $c > 0$。如果 ϵ 不是 H 的单位元，这种情况便不可能发生。否则，当且仅当 Hex(H) $\subseteq \mathcal{N}$时，这种情况才会发生。根据引理 3.4，Hex(H) 至少包含 $(n-1)/6$ 个六边形。由于 $\mathbb{\Pi}$ 中的六边形是彼此独立地选入的，每个以1 2的概率选入，因此 $\mathcal{N}$ 包含所有这些六边形的概率至多为 $2^{-(n-1)/6}$。因此，我们可以取 $c = \frac{1}{7}\log 2$。□

虽然此前我们并未用到这一点，但此时若能对 ○(*G*)的大小作出良好估计，将会极有帮助。

命题 3.8. 记 $G[3]$ 为 G的 *3*-挠子群。那么

$$\#\bigcirc(G) = \frac{n^2 + 3n + 2\#G[3]}{6}$$

证明。 我们对群 S_3 作用于$G^2 = G^3/G$中的基本对使用伯恩赛德引理。在恒等元作用下不变的基本对数目显然为 #G^2。在对换 (x, y) $\mapsto$ (y, x) 下不变的元素恰好是满足$x \in G$的那些对 (x, x)。这样的对恰有 n 个。由对称性，其他对换的不动点数目相同。3-循环 (x, y) $\mapsto$ (yx^{-1}, x^{-1}) 的不动点恰好是满足 $x^3 = 1$ 的那些对 (x, x^2)，其中 $x \in G$ 。这样的元素共有 #G[3] 个。其逆 3-循环 x, $y \mapsto$ (y^{-1}, xy^{-1}) 的不动点数目相同。因此，不动点的平均数恰好是上述所给的数目。□

由命题 3.8 可知，#○(G) $\sim$ $\#_6^{G^2}$ 。现在我们利用这一点证明，大多数有限牧场都没有自同构。

命题 3.9。 当 n充分大时， ℙ具有非平凡自同构的概率至多为 2^{-cn^2} ，其中 $c > 0$是某个绝对常数。

证明。 由引理 3.5， G 至多有 $e^{o(n)}$ 个自同构。因此，只需证明：对任意固定的非平凡自同构 $f\colon G \to G$， $\mathcal{N}$ 在f 作用下保持不变的概率至多为 $2^{-c'n^2}$ ，其中 c'是某个绝对常数。我们首先证明， ○(G)中的六边形有正比例不会被 f固定。我们用 $[x\colon y\colon z]$ 表示（x, y, z）在 G 作用下的轨道 $\in G^3$，它是一个基本对。若 $[x\colon y : z]$ 所在的六边形被 f固定，那么

$$[f(x) : f(y) : f(z)] = [x : y : z]^\sigma \quad \text{for some } \sigma \in S_3$$

如果 σ 是恒等元，那么

$$[f(x) : f(y) : f(z)] = [x : y : z]$$

表明 xz^{-1}, $yz^{-1} \in G^f$。这样的六边形恰有 #○(G^f) 个。

如果 σ 是对 换，那么——不失一般性——我们可以假设 σ =(12)。那么

$$[f(x) : f(y) : f(z)] = [y : x : z]$$

表明 $yz^{-1} = f(xz^{-1})$。因此，六边形 (x, y, z) 的形式为 (g, $f(g)$)。给定一个对换 σ，这样的六边形至多有 #G 个，因此总数至多为 3#G 。

如果 σ 是一个 3-循环，那么——不失一般性——我们可以假设

$$[f(x) : f(y) : f(z)] = [z : x : y]$$

特别地，这给出 $yz^{-1} = f(zx^{-1})$。也就是说， $yz^{-1} = f(xz^{-1})^{-1}$。因此，六边形 ($x$, y, z) 的形式为 (g, $f(g)^{-1}$)。同样，对于给定的 3-循环σ，这样的六边形至多有 #G 个，因此总共至多有 2#G 个。

由于 f 是非平凡自同构，我们有 #G^f $\leq$#$G/2$。根据命题 3.8，可知被 f 固定的六边形数量至多为

$$\#\bigcirc(G^f) + 5\#G \leq \frac{n^2}{24} + O(n) = \left(\frac{1}{4} + o(1)\right)\#\bigcirc(G)$$

因此，当 n 足够大时， G 的六边形中至多三分之一被 f 固定。因此， ○(G) 的 f-轨道数量至多为 $_{23}$#○(G)。这意味着，与总共的 $2^{\#\bigcirc(G)}$ 个牧场相比， G 上至多有 $2^{\ _{23}\#\bigcirc(G)}$ 个牧场在 f 下保持不变。由渐近 #○(G) $\sim$ $\frac{n^2}{6}$ ，结论得证。□

我们以一个一般引理结束本节，该引理将关于超域抽签的陈述转化为关于按同构考虑的超域的陈述。

引理 3.10. 存在一个绝对常数 $c > 0$，使得下述结论成立。设 S 是 G 上单位元为 ϵ 的超域的任意一组同构类。设 p 是 $\mathbb{P}$ 属于 S 的概率。采用定理 *1.2* 中的记号，我们有

$$\frac{\#S}{\#\mathcal{H}(G,\epsilon)} \leq cpe^{(\log_2 n)^2}$$

只要 $\#G$ 足够大。

证明。由引理 3.5，固定 ϵ 的 G 的自同构群 $\mathscr{A} := \mathrm{Aut}(G,\epsilon)$ 的阶至多为 $e^{(\log_2 n)^2}$。由于 $\mathcal{H}(G,\epsilon)$ 的每个元素都对应于 $2^{\square(G)}$ 的一个 $\mathscr{A}$-轨道——且每个此类轨道的大小至多为 $e^{(\log_2 n)^2}$——因此，能够导出一个超域的 $2^{\square(G)}$ 中的元素数量至多为 $e^{(\log_2 n)^2}\#\mathcal{H}(G,\epsilon)$。另一方面，由命题 3.1 可知，对于某个绝对常数 $c' > 0$，该数量至少为 $(1-e^{-c'n})\cdot 2^{\#\square(G)}$。因此

$$e^{(\log_2 n)^2}\cdot\#\mathcal{H}(G,\epsilon) \geq (1-e^{-c'n})\cdot 2^{\#\square(G)}$$

现在，由于 S 中的任意等价类都可以由 $2^{\square(G)}$ 中的某个零集实现，我们有

$$p \geq \frac{\#S}{2^{\#\square(G)}}$$

将上述两个不等式相乘并整理，得到

$$\frac{e^{(\log_2 n)^2}}{1-e^{-c'n}}\cdot p \geq \frac{\#S}{\#\mathcal{H}(G,\epsilon)}$$

因此，我们可以取 $c = (1-e^{-c'})^{-1}$。 □

4. Proofs of results

定理 *1.8* 的证明。使用第 3 节的超域彩票术语，$\mathbb{P}$ 是一个既不是 0/0 也不是 4-满的超域的概率为 $e^{-\Omega(\#G)}$，由命题 3.1 可知。因此，作为引理 3.10 的直接推论，我们有

$$1-\frac{\#\mathcal{F}(G,\epsilon)}{\#\mathcal{H}(G,\epsilon)} = O\left(e^{-\Omega(\#G)}\cdot e^{(\log_2\#G)^2}\right) = e^{-\Omega(\#G)}$$ □

注 4.1。定理 1.8 的证明还表明，渐近地，几乎所有有限牧场都是超域。这一结论乍看令人意外，因为牧场的“结构不如”超域丰富。

正如在 [BJ21]，中所观察到的，Turnwald [Tur94] 的以下结果对大域的小商施加了强约束。（另见 Bergelson–Shapiro[BS92]，的较早结果，该结果证明了无限域的情形。）

定理 4.2 ([Tur94，定理 1])。设 $\mathbb{F}$ 为斜域，且 $\Gamma \subseteq \mathbb{F}^\times$ 是 $\mathbb{F}^\times$中一个有限指数的真子群。若 $\#\mathbb{F}^\times > (\mathbb{F}^\times : \Gamma)^4$ 则 $\Gamma - \Gamma = \mathbb{F}$。

注 4.3。Turnwald 实际上给出了界 $\#\mathbb{F} \geq (k-1)^4 + 4k$，其中 $k = (\mathbb{F}^\times : \Gamma)$。这对 $k \geq 2$ 给出了更强的结论。对于 $k = 1$，修改后的陈述很容易验证。较简洁的表达式会更便于使用。

推论 4.4. 设 G 是一个阶为 n的有限群。同构意义下，底层群为 G 且满足 $1 \boxplus -1 \neq \mathbb{H}$的商斜超域$\mathbb{H}$ 至多有 n^4个。

证明。 设 H 是某个斜域 F 关于正规子群 $\Gamma \subseteq \mathrm{F}^\times$的商，且该正规子群的指数必为有限。于是 $1 \boxplus -1$ 是 $\Gamma - \Gamma$ 在商同态下的像。此外， $n = (\mathrm{F}^\times : \Gamma)$。设 $1 \boxplus -1 \neq \mathrm{H}$。根据定理 4.2，$\mathrm{F}^\times$ 的基数至多为n^4。因此 F 是有限域。对于任意给定的有限域 F，循环群 $\mathrm{F}^\times$ 至多有一个阶为 n的商。因此，同构意义下，底层群为 G 且为 F 的商的超域至多有一个。由于任意给定阶数的有限域至多有一个，H 至多有n^4 种可能。□

定理 *1.2* 的证明。 我们再次考虑第 3 节的随机牧场 $\mathbb{F}$。任何来自斜域 F 的态射$\phi : \mathrm{F} \to \mathbb{F}$ 都可分解为 $\mathrm{F} \to \mathrm{F}/\ker \phi \to \mathbb{F}$。因此， $\mathbb{F}$ 存在来自某个斜域的满射态射，当且仅当存在来自某个关于 G的商超域 $\mathbb{O}$ 的双射同态。如果在 $\mathbb{O}$ 中有 $1 \boxplus -1 = \mathbb{O}$，那么在 $\mathbb{F}$ 中必有 $1 \boxplus -1 = \mathbb{F}$。后者恰好表示，对于所有$x \in G$，$(-1,\ x) \in \mathrm{Hex}(\mathbb{F})$。根据命题 3.3，这种情况发生的概率为 $e^{-\Omega(\#G)}$。另一方面，如果在 $\mathbb{O}$ 中有 $1 \boxplus -1 \neq \mathbb{O}$，那么根据推论 4.4，$\mathbb{O}$ 是关于 G 且具有该性质的至多 $\#G^4$ 个商超域之一。对于这些超域中的每一个 $\mathbb{O}$，根据命题 3.7，存在双射态射 $\mathbb{O} \to \mathbb{F}$ 的概率为$e^{-\Omega(\#G)}$。这种情况对某个这样的 $\mathbb{O}$ 成立的概率至多为 $\#G^4 \cdot e^{-\Omega(\#G)} = e^{-\Omega(\#G)}$。因此， $\mathbb{F}$ 是一个存在来自某个域的满射同态的超域的概率至多为 $e^{-\Omega(\#G)}$。根据引理 3.10，这意味着

$$\frac{\#\mathcal{I}(G,\epsilon)}{\#\mathcal{H}(G,\epsilon)} = O\left(e^{-\Omega(\#G)} \cdot e^{(\log_2 n)^2}\right) = e^{-\Omega(\#G)}.$$ □

定理 *1.12* 的证明。 在超域抽签中， $\mathbb{F}$ 是具有非平凡自同构的超域的概率至多为 $e^{-\Omega(\#G^2)}$，由命题 3.9 得出。由引理 3.10 可知，

$$\frac{\#\mathcal{A}(G,\epsilon)}{\#\mathcal{H}(G,\epsilon)} = O\left(e^{-\Omega(\#G^2)} \cdot e^{(\log_2 n)^2}\right) = e^{-\Omega(\#G^2)}.$$ □

定理 *1.14* 的证明。 由于 G 上的牧场由一个单位元 $\epsilon \in G[2]$ 和 $\circlearrowleft(G)$ 中的六边形子集给出，因此恰有

$$N \coloneqq \#G[2] \cdot 2^{\frac{1}{6}(\#G^2 + 3\#G + 2\#G[3])}$$

根据命题 3.8， G 上有这些牧场。

- 根据命题 3.1，其中属于超域的比例为 $1 - e^{-\Omega(\#G)}$。因此， G 在同构意义下 的超域数量至少为

$$\frac{1}{\#\operatorname{Aut} G}\left(1 - e^{-\Omega(\#G)}\right) \cdot N$$

- 根据命题 3.2，其中属于非超域的比例至少为$e^{-O(\#G)}$，具有非平凡自同构的比例至多为 $e^{-\Omega(\#G^2)}$。因此， G 在同构意义下 的超域数量至多为

$$\left(\frac{1}{\#\operatorname{Aut} G}\left(1 - e^{-O(\#G)}\right) + e^{-\Omega(\#G^2)}\right) \cdot N = \frac{1}{\#\operatorname{Aut} G}\left(1 - e^{-O(\#G)}\right) \cdot N$$

对于足够大的 $\#G$. □

为了证明推论 1.15，我们需要给出任意给定阶的阿贝尔群数量的上界。虽然这一上界很容易得到，但为准备第 5 节中的讨论，我们现在来讨论给定阶的群的数量上界。

定理 4.5 （[Neu69], 定理 A。 阶为n 的群的同构类数量为 $e^{O((\log n)^4)}$ 。

Neumann 的这一结果依赖于这样一个假设：阶为 n 的有限单群的数量也存在类似的上界。有限单群分类表明，事实上，这个后一个函数是 $O(1)$。

证明 *o f* 推论 *1.15*。 设 G 是阶为 $n-1$ 的任意阿贝尔群。[9] 根据定理 1.14 ，

$$\log_2 \#\mathcal{H}(G) = \log_2 \#G[2] - \log_2 \#\operatorname{Aut} G + \frac{1}{6}((n-1)^2 + 3(n-1) + 2\#G[3]) - e^{-\Theta(\#G)}$$

由于 $\#G[2] = O(n)$、$\#G[3] = O(n)$ 和 $\#\operatorname{Aut} G = O(n \log_2 n)$（根据引理 3.5），我们得到

$$\log_2 \#\mathcal{H}(G) = \frac{n^2}{6} + O(n)$$

利用定理 4.5，将所有阶为 $n-1$ 的有限阿贝尔群的这些值相加，得到

$$\log_2 \#\mathcal{H}_n = \frac{n^2}{6} + O((\log n)^4) + O(n) = \frac{n^2}{6} + O(n) \qquad \square$$

5. Beyond the commutative case

试图将我们的结果推广到斜超域时，会遇到许多困难。在讨论这些困难之前，我们先谈谈猜想 1.1 与推论 1.3 之间一个有趣的差异。Baker 和 Jin 的猜想针对的是域的商，而我们证明了一个先验上更强的结果：斜域的商几乎从来都不是超域。我们不知道这是否确实是一个更强的结论。也就是说：

问题 5.1. 每个作为某个斜域之商的超域，是否实际上都是某个域的商？如果要求该超域是有限的，这一结论是否仍然成立？

将猜想 1.1 直接推广到斜超域的情形，出于一个相当平凡的原因而成立，具体如下。

定理 5.2. 设 $\mathcal{S}_n$ 为阶为 n 的斜超域的同构类集合， $\mathcal{H}_n \subseteq \mathcal{S}_n$ 为其中属于超域的那些同构类组成的子集。则

$$\frac{\#\mathcal{H}_n}{\#\mathcal{S}_n} = 1 - e^{-\Omega(n^2)}.$$

我们在附录 B 中给出定理 5.2 的证明。证明所需的要素有两个。第一当然是定理 4.5，它使我们能够对阶为 n 的非交换群的数量进行一定控制。第二是六边形框架。它可以推广到非交换情形——G 的一个六边形是在 G^3 中由 $G \times S_3 \times G$ 的作用产生的一个轨道，其中第一个 G 通过左乘作用，第二个通过右乘作用——但需要注意的是，六边形的大小可能千差万别，而且六边形的总数与阿贝尔情形相比可能少得多。这使得任何试图复现命题 3.1 证明中论证的做法都变得复杂。

定理 5.2 表明，渐近地，除了一个趋于零的极小比例外，所有有限斜超域实际上都是超域。因此，根据推论 1.3，几乎所有斜超域都是非商的。有人可能会正确地反驳说，这回答的是错误的问题。例如，我们可能希望将范围限制在某些群类中（例如非交换有限

[9]按照约定，阶为 n 的超域具有阶为 $n-1$ 的底层群。这与有限域的约定一致。

群、对称群、有限单群等）。在交换情形下，定理 1.2 对于施加此类限制的有限超域的普遍行为给出了完整的理解。对于非交换群，拥有类似的论述是值得期待的。我们还可以询问非交换群的定理 1.8 的类似结果。定理 1.12 的类似结果将表明，对于有限群 G 上的一个一般斜超域，所有自同构都由 G 的内自同构诱导。最后，如果能得到给定非交换群上斜超域的同构类数量的渐近结果，也将十分有趣。

Acknowledgements

作者谨此感谢 Noah Solomon 让我们注意到论文 [Hob25]，并感谢亚利桑那—新墨西哥交换代数及其交叉领域研讨会提供了一个有利于合作讨论的平台。我们正是在那里认识了 Noah。我们也感谢 Alexander Divoux 指出了本手稿早期版本中的一处错误。

References

[BB17] M. Baker 和 N. Bowler. 超域上的拟阵. 2017. arXiv: 1601.01204[math.CO].[BB19] M. Baker 和 N. Bowler. “部分超结构上的拟阵”。载于：数学进展 343 (2019)，第 821–863 页。[BHKL25] M. Baker、J. Huh、M. Kummer 和 O. Lorscheid. 三角超域上的 Lorentzian 多项式与拟阵 1：拓扑方面. 2025. arXiv: 2508.02907 [math.CO].[BJ21] M. Baker 和 T. Jin. “作为域的商得到的超域的结构”。载于：美国数学会会刊 149.1 (2021)，第 63–70 页。[BL21] M. Baker 和 O. Lorscheid. “ 拟阵模空间 ”。载于：数学进展 390 (2021)。[BL25a] M. Baker 和 O. Lorscheid. 拟阵基础，第一部分：不含大型均匀拟阵子式的拟阵. 美国数学会回忆录. 美国数学会，2025。[BL25b] M. Baker 和 O. Lorscheid. “牧场上拟阵表示的提升定理”。载于：组合论杂志 B 辑 170 (2025)，第 1–55 页。[BS92] V. Bergelson 和 D. B. Shapiro. “环中有限指数的乘法子群”。载于：美国数学会会刊 116.4 (1992)，第 885–896 页。[BSZ25] M. Baker、N. Solomon 和 T. Zhang. 关于拟环上矩阵的若干秩概念. 2025. arXiv: 2202.02356 [math.CO].[BZ23] M. Baker 和 T. Zhang. “牧场与拟环的融合规则”。载于：欧洲组合学杂志 108 (2023)。[Cre21] S. Creech. 牧场范畴中的极限与余极限. 2021. arXiv: 2103.08655 [math.CT].[HHSW25] D. Huang、J. Huh、D. Soskin 和 B. Wang. Lorentzian 矩阵的有界比率. 2025. arXiv: 2510.25030 [math.CO].[HL14] G. H. Hardy 和 J. E. Littlewood. “丢番图逼近的一些问题”。载于：数学学报 37.1 (1914)，第 193–239 页。

[Hob25] D. Hobby. 有限超域中的块. 2025. arXiv: 2507.18908 [math.RA].[Knu76] D. E. Knuth. “大 omicron、大 omega 和大 theta”。载于：SIGACT News 8.2 (1976 年 4 月), 第 18–24 页。[Kra57] M. Krasner. “用特征为 0 的完备赋值域逼近特征为 ´ 的完备赋值域”。载于：高等代数研讨会。比利时数学研究中心。鲁汶：Etablissements Ceuterick，1957。[Kra83] M. Krasner. “一类超环与超域”。载于：国际数学与数学科学杂志 6 (1983)，第 307–311 页。[Mas85] Ch. G. Massouros. “构造超域的方法”。载于：国际数学与数学科学杂志 8.4 (1985)，第 725–728 页。[Neu69] P. M. Neumann. “有限群的计数定理”。载于：数学季刊 20.1 (1969 年 1 月)，第 395–401 页。 ISSN: 0033-5606。[Neu95] P. M. Neumann. “证明 Garrett Birkhoff 与 Philip Hall 关于有限群自同构的猜想”。载于：伦敦数学学会会刊 27.3 (1995 年 5 月)，第 222–224 页。[PZ10] R. A. Pendavingh 和 S. H. M. van Zwam. “偏域上拟阵表示的提升”。载于：组合理论杂志 B 辑 100.1 (2010 年 1 月)，第 36–67 页。ISSN: 0095-8956。[Sem98] C. A. Semple. “k-正则拟阵”。博士论文。维多利亚惠灵顿大学，1998。[Tur94] G. Turnwald. “除环中有限指数的乘法子群”。载于：美国数学会会刊 120.2 (1994)，第 377–381 页。

Appendix A. Products of hyperfields

这里我们讨论牧场与超域范畴中的积与$0/0$ 性质的关系。由 [Cre21]可知，牧场范畴是完备且余完备的。由其中的结果可知，牧场 P_1 与 P_2 的积的底层群为 $\mathrm{P}_1^\times \times \mathrm{P}_2^\times$，单位元为 $\begin{bmatrix}-1\\-1\end{bmatrix}$，其六边形为

$$\mathrm{Hex}(\mathbb{P}_1 \times \mathbb{P}_2) = \left\{ \overline{\left(\begin{bmatrix} u_1 \\ u_2 \end{bmatrix}, \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} \right)} \;\middle|\; (u_1, v_1) \in \mathrm{Hex}(\mathbb{P}_1), (u_2, v_2) \in \mathrm{Hex}(\mathbb{P}_2) \right\}$$

（此处及下文，我们用 $\begin{bmatrix}a\\b\end{bmatrix}$ 表示两个群的积中的元素（a, b）。这样写的好处是，它在视觉上有别于我们对基本对的记法。）

若 H 和 G 是超域，自然会问：牧场范畴中的积 $\mathrm{H} \times \mathrm{G}$ 何时仍是超域？若是如此，那么根据命题 2.27，这个积也就是它们在超域范畴中的积。我们将证明以下结论。

定理 A.1. 设$\mathbb{H}$ 和$\mathbb{G}$ 为超域。那么，$\mathbb{H}$ 与$\mathbb{G}$ 的牧场积$\mathbb{H} \times \mathbb{G}$ 是超域，当且仅当

- $\mathbb{H}$ 和$\mathbb{G}$ 都为 $0/0$，或者
- $\mathbb{H} \cong \mathbb{K}$，或者$\mathbb{G} \cong \mathbb{K}$，或者
- $\mathbb{H} \cong \mathbb{G} \cong \mathbb{F}_2$.

在第一种情况下，积仍为 $0/0$。

要证明定理 A.1，我们需要两个引理。

引理 A.2。 设$\mathbb{H}$ 是一个超域，且$\mathbb{H} \ncong \mathbb{F}_2$,$\mathbb{F}_3$,$\mathbb{K}$。则存在 $x, y \in \mathbb{H}^\times$ ，满足$x \neq y$ 使得 $(x, y) \in \mathrm{Hex}(\mathbb{H})$。

证明。 由于 H 不是 F_2, ，它必定有某个基本对。若 H 有一个基本对 $(x,\ y) \neq (1,\ 1)$，那么要么是 $x \neq y$——此时结论成立——要么是 $x = y$，此时 $(1,\ x^{-1})$ 和 $(1,\ y^{-1})$ 都是 H 中的基本对，且至少其中一个具有所需形式。假设 (1，1) 是 Hex(H) 中唯一的基本对。根据命题 2.23 中的判据 (A)，$H \setminus \{0, -1\}$ 中的任意元素都属于某个基本对。因此 $H = \{0, 1, -1\}$，且其唯一的基本对是 (1，1)。根据 $1 = -1$ 是否成立，这意味着 $H \cong K$ 或 F_3。□

下面给出命题 2.23 的一个变体。

引理 A.3。 群 G 上的牧场$\mathbb{P}$ 来自一个 *0/0* 超域，当且仅当满足以下两个条件：

(A) 对所有 $x \in G$，存在 $y \in G$，使得 $(x,\ y) \in \mathrm{Hex}(\mathbb{P})$。*(B)* 对所有 $(x,\ y)$、$(z,\ w) \in \mathrm{Hex}(\mathbb{P})$，存在 $t \in G$，使得 $(tx,\ -tz)$、$(-ty,\ tw) \in \mathrm{Hex}(\mathbb{P})$.

证明。我们将每个条件与命题 2.23 中的对应条件进行比较。对于条件 (A)，加强之处在于我们允许 $x = -1$。但根据注 2.24，这对任何非域超域都成立。显然，域不可能是 0/0。对于条件 (B)，加强之处恰恰在于允许 $(x, y) = (z, w)$。也就是说，我们要求：如果 $(x, y) \in$ Hex(P)，那么存在 $t \in G$，使得 $(tx, -tx)$、$(-ty, ty) \in$ Hex(P)。用超域的术语来说，这表示 $1 \boxplus -1 \ni t^{-1}x^{-1}, t^{-1}y^{-1}$。这恰好表明存在 $r, s \in 1 \boxplus -1 \setminus \{0\}$，使得 $rs^{-1} = xy^{-1}$。这对所有基本对 (x, y) 都必须成立。利用基本对上的对合 $(x, y) \mapsto (xy^{-1}, y^{-1})$，我们看到，该条件变为：每当 $(x, y) \in$ Hex(P) 时，就存在 $r, s \in 1 \boxplus -1 \setminus \{0\}$，使得

$$rs^{-1} = (xy^{-1})(y^{-1})^{-1} = x$$

假设 (A) 成立，$P^\times$ 中的每个元素都属于某个基本对。因此，我们恰好恢复了 $0/0$ 条件（除去平凡情形 $x = 0$）。□

定理 *A.1* 的证明。 如果 $H \cong F_2$，那么 $H \times G$ 的基数等于 #G，但没有六边形（因为 F_2 没有六边形）。根据引理 3.4，这迫使 $\#G \leq 2$。这意味着 G 同构于 F_2 或 K。现在假设 H、G 中没有一个同构于 K、F_2, ，但 H 同构于 F_3。令 $x \in G$ 满足 $x \neq 0,\ -1$。由于在 F_3 中，元素-1 不属于任何六边形，因此元素 $\begin{bmatrix} -1 \\ x \end{bmatrix}$ 不属于 $H \times G$ 中的任何六边形，但它不是这个牧场的单位元。由命题 2.23 的判据 (A) 可知，这表明 $H \times G$ 不是超域。

现在假设 H、G 均不同构于任意 K、F_2, F_3, ，但它们的积是一个超域。我们将证明它们必定是 $0/0$。只需对 G 证明这一点。由引理 A.2，可找到 $(a,\ b) \in H$ 的六边形集合，使得 $a \neq b$。令 $(c,\ d) \in G$ 的六边形集合为任意一个基本对。那么

$$\left(\begin{bmatrix} a \\ c \end{bmatrix}, \begin{bmatrix} b \\ d \end{bmatrix}\right) \quad \text{and} \quad \left(\begin{bmatrix} b \\ c \end{bmatrix}, \begin{bmatrix} a \\ d \end{bmatrix}\right)$$

是 $H \times G$ 的不同基本对。根据命题 2.23 中的判据 (B)，我们可以找到$t \in H^\times,\ u \in G^\times$，使得

$$\left(\begin{bmatrix} ta \\ uc \end{bmatrix}, \begin{bmatrix} -tb \\ -uc \end{bmatrix}\right) \quad \text{and} \quad \left(\begin{bmatrix} -tb \\ -ud \end{bmatrix}, \begin{bmatrix} ta \\ ud \end{bmatrix}\right)$$

都是 H ×G 的基本对。只看底行，条件是$u^{-1}c^{-1}$和 $u^{-1}d^{-1}$ 都属于 G 中的和 $1\boxplus -1$。特别地，在 G 中我们可以找到 $r,\ s\in 1\boxplus -1$，满足 $s\neq 0$，使得 $rs^{-1}=cd^{-1}$。注意，$0\neq s\in 1\boxplus -1$ 意味着 G 不是域。现在令 $x\in$G$^\times$ 任意。根据命题 2.23 的判据 (A) 和注 2.24，存在某个基本对 $(x,\ y)\in$ Hex(G)。那么 $(xy^{-1},\ y^{-1})$ 也是 G 的基本对。通过恒等对应 $c\rightsquigarrow xy^{-1}, d\rightsquigarrow y^{-1}$，我们看到，对于某个 $r,\ s\in 1\boxplus -1$，有$rs^{-1}=x$。这表明 0/0 条件成立（除平凡情形 $x=0$ 外）。

还需证明所述情形中的积确实是超域。牧场乘积同构 $\mathrm{F}_2\times\mathrm{F}_2\cong\mathrm{F}_2$ 和 P ×K ≅ P（对所有牧场 P）很容易验证。这表明，在第二种和第三种情形下，我们得到的是超域。

现在假设 H,G 是 0/0 超域。我们证明 H × G 也是如此。首先检查它是否满足引理 A.3 中的判据 (A)。设 $\begin{bmatrix}h\\g\end{bmatrix}\in$ H$^\times$ ×G$^\times$。根据 H 和 G 满足的相同性质，我们可以找到 $u\in$H$^\times$, $v\in$G$^\times$，使得 $(h,y)\in$H 的六边形集合，且 $(g,z)\in$G 的六边形集合。于是

$$\left(\begin{bmatrix}h\\g\end{bmatrix},\begin{bmatrix}y\\z\end{bmatrix}\right)\in\mathrm{Hex}(\mathbb{H}\times\mathbb{C})$$

对于性质 (B)，假设

$$\left(\begin{bmatrix}x_1\\x_2\end{bmatrix},\begin{bmatrix}y_1\\y_2\end{bmatrix}\right)\quad\text{and}\quad\left(\begin{bmatrix}z_1\\z_2\end{bmatrix},\begin{bmatrix}w_1\\w_2\end{bmatrix}\right)$$

是 G × H 的基本对。那么 (x_i,y_i),(z_i,w_i) 分别是 H 和 G 关于 $i=1$,2 的基本对。根据这些超域的性质 (B)，我们可以找到 $t_1\in$ H$^\times$ 和 $t_2\in$G$^\times$，使得 $(t_ix_i,-t_iz_i),(-t_iy_i,t_iw_i)$ 是相应超域中的基本对。因此，

$$\left(\begin{bmatrix}t_1\\t_2\end{bmatrix}\cdot\begin{bmatrix}x_1\\x_2\end{bmatrix},-\begin{bmatrix}t_1\\t_2\end{bmatrix}\cdot\begin{bmatrix}z_1\\z_2\end{bmatrix}\right)\quad\text{and}\quad\left(-\begin{bmatrix}t_1\\t_2\end{bmatrix}\cdot\begin{bmatrix}y_1\\y_2\end{bmatrix},\begin{bmatrix}t_1\\t_2\end{bmatrix}\cdot\begin{bmatrix}w_1\\w_2\end{bmatrix}\right)$$

是 H ×G 中的基本对。这为该积给出了性质 (B)。 □

注记 A.4. 定理 A.1 将“牧场”替换为“拟环”后仍然成立，其含义是[BB19], 不过我们在此不再赘述。

与上述结果相反，我们注意到，两个超域的积可能存在于超域范畴中，却不与牧场的积相一致。为此，我们需要以下命题。

命题 A.5. 设 $\mathbb{H}$是一个（斜）超域，$\mathbb{F}$ 是一个（斜）域。若存在同态$\mathbb{H}\to\mathbb{F}$，则$\mathbb{H}$ 是一个（斜）域。

证明。 假设 H 不是一个（斜）域。根据注记 2.7，H 中的和 $1\boxplus -1$ 包含某个非零元。若存在态射 H $\to$F，则 F 中的和 $1\boxplus -1$ 必定包含一个非零元。□

由此观察，我们推得：

命题 A.6. 设 p 是一个素数，$\mathbb{F}_p$ 是相应的素域。那么在超域范畴中，$\mathbb{F}_p$ 与自身的积仍是$\mathbb{F}_p$。

证明。 由命题 A.5 可知，任何映入 F$_p$ 的同态，其定义域都是一个域。由于任何域同态都是一个嵌入，且 F$_p$ 是素的，因此映入 F$_p$ 的唯一超域同态就是恒等元 $\mathrm{F}_p\to$F$_p$。由此可得结论。□

注意，域永远不会是 0/0。

另一方面，范畴积可能不会在超域范畴中存在。

命题 A.7。 设 p、q 互素，且均为素数幂。则$\mathbb{F}_p$ 与$\mathbb{F}_q$的积在超域范畴中不存在。

证明。 如上所述，根据命题 A.5，任何到 F_p 或 F_q 的超域同态，其定义域都是一个域。由于域同态只能存在于固定的特征中，因此不存在能够同时映射到 F_p 和 F_q 的超域。由此可知，这两个超域在超域范畴中不可能有积。□

Appendix B. The sparsity of finite skew hyperfields

这里概述定理 5.2 的证明。证明通过仿照第 2 节的六边形框架展开，但其中存在细微而重要的差异。

下面是定义 2.20 的类比。

定义 B.1。 设 G 是一个群。G 对 G^3 的左乘与右乘所产生的综合作用，以及 S_3 对 G^3 的置换作用，可以概括为群 $G \times S_3 \times G$ 对 G^3的作用。该作用的一个轨道称为 G的六边形 。我们用 $\hexagon(G)$表示 G的六边形集合。利用归一化映射 $(x, y, z) \mapsto (xz^{-1}, yz^{-1})$，我们可以将 $\hexagon(G)$与 G^2 在 $S_3 \times G$作用下的轨道集合等同，其中 G 通过共轭作用。我们用 (x, y)表示与对 $(x, y) \in G^2$相关联的六边形。

与交换情形一样，由定义 2.1 中的公理 (I) 和 (III) 可知，对于斜超域 H，集合

$$\{(a, b, c) \in \mathbb{H}^\times \mid 0 \in a \boxplus b \boxplus c\}$$

在 $(\mathrm{H}^\times)^3$ 的左乘和右乘作用以及 S_3 的置换作用下保持不变。因此，我们应考虑 $\mathrm{H}^\times$ 中相应的六边形集合。它们称为 H 的六边形。这些数据可概括如下（参见定义 2.21）。

定义 B.2. 一个斜牧场 P 由三元组 $\mathrm{P} = (G, \epsilon, \mathrm{Hex(P)})$ 构成，其中

- G是一个群，称为 P 的底层群 ，记作 $\mathrm{P}^\times$。
- $\epsilon \in G$ 是 G 中的一个元素，且位于中心并满足 $\epsilon^2 = 1$，称为 P 的单位元 。
- $\mathrm{Hex(P)} \subseteq \hexagon(G)$ 是 G 的六边形的一个子集，称为 P 的零集 。

斜牧场之间的态射定义同定义 2.26。

如上所述，每个斜超域都确定一个牧场，它由以下部分组成：(i) 其乘法群，(ii) 其单位元，以及 (iii) 其六边形的集合。以下命题的证明显然，故略去。

命题 B.3. 斜超域由其斜牧场唯一确定。超域同态会诱导相应斜牧场之间的态射，而且这些斜牧场之间的每个态射都以此方式产生。这便诱导出从斜超域范畴到斜牧场范畴的完全忠实嵌入。

定理 5.2 证明中的关键观察如下。

命题 B.4. 设 G是一个阶为 n的非交换群。那么， G至多有$\frac{1}{6}(5n^2/8 + 5n)$ 个六边形。

证明。我们使用伯恩赛德引理，按照定义 B.1 中的方法，计算 G^2 在$S_3 \times G$ 作用下的轨道数。对于 g、$h \in G$，我们用 ${}^g h$ 表示 ghg^{-1}的共轭元。$\in S_3 \times G$ 中 $(1, g)$ 的不动点恰好是满足 $x, y \in C(g)$ 的元素 $(x, y) \in G^2$（其中 $C(g)$ 是 g 的中心化子）。若 τ 是 S_3 中将 $(x, y) \mapsto (y, x)$ 的对换，那么任何被 (τ, g) 固定的有序对 $(x, y) \in G^2$ 都必须满足 $y = {}^g x$。因此，此类有序对至多有 n 个。其他任何对换也同样如此。最后，若 ρ 是将 $(x, y) \mapsto (yx^{-1}, x^{-1})$ 的 3-循环，那么任何被 (ρ, g) 固定的有序对 $(x, y) \in G^2$ 都必须满足 $y = {}^g x^{-1}$。同样，这样的有序对至多有 n 个。逆 3-循环也同样如此。

由上述讨论和伯恩赛德引理可知，轨道数量的上界为

$$\#\bigcirc(G) \leq \frac{1}{6n} \sum_{g \in G} ((\#C(g))^2 + 5n) = \frac{1}{6} \left(\frac{1}{n} \sum_{g \in G} \#C(g)^2 + 5n \right) \tag{2}$$

记 $Z(G)$ 为 G 的中心。对于 $g \in Z(G)$，有 $C(g) = G$ 。对于 $g \notin Z(G)$， $C(g)$ 是 G 的真子群，因此指数至少为 2。注意， $Z(G)$ 本身也是 G 的真子群，因此指数也至少为 2。由此我们得出

$$\begin{aligned} \sum_{g \in G} \#C(g)^2 = \sum_{g \in Z(G)} \#C(g)^2 + \sum_{g \notin Z(g)} \#C(g)^2 &\leq n^2 \cdot \#Z(G) + \frac{n^2}{4}(n - \#Z(G)) \\ &= \frac{3n^2}{4} \cdot \#Z(G) + \frac{n^3}{4} \leq \frac{3n^2}{4} \cdot \frac{n}{2} + \frac{n^3}{4} = \frac{5n^3}{8} \end{aligned}$$

将其代入式 (2) 得

$$\#\bigcirc(G) \leq \frac{1}{6} \left(\frac{5n^2}{8} + 5n \right) \qquad \square$$

定理 *5.2* 的证明。设 G 是一个阶为 $n-1$ 的有限非阿贝尔群。根据命题 B.3， G 上的斜超域由以下数据确定：(i) G 的一个阶至多为 2 的中心元素；(ii) G 的六边形的一个子集。因此， G 上的斜超域数量至多为

$$(n-1) \cdot 2^{\#\bigcirc(G)} \leq n \cdot 2^{\frac{1}{6}(5(n-1)^2/8 + 5(n-1))} = 2^{n^2/6} \cdot 2^{-n^2/16 + O(n)}$$

根据命题 B.4。由于根据定理 4.5，阶为 $n-1$ 的群至多有 $e^{O((\log n)^4)}$ 个；根据推论 1.15，阶为 n 的超域有 $2^{n^2/6 + O_{(n)}}$ 个，因此我们有

$$\frac{\#S_n - \#H_n}{\#H_n} \leq \frac{e^{O((\log n)^4)} \cdot 2^{n^2/6} \cdot 2^{-n^2/16 + O(n)}}{2^{n^2/6}} = 2^{-n^2/16 + O(n)}$$

由此即可得出该结论。 $\square$

Department of Mathematics, Princeton University, Princeton, NJ 08540, USA
Email address: tl0101@princeton.edu

Department of Mathematics, Princeton University, Princeton, NJ 08540, USA
Email address: chayiml@princeton.edu