切瓦莱群中的丢番图问题 s

Elena Bunina，巴伊兰大学 Alexey Myasnikov，
史蒂文斯理工学院 Eugene Plotkin，巴伊兰大学[1]

arXiv:2304.06259v1 [math.NT] 13 Apr 2023

摘要

本文研究切瓦莱群 $G_\pi(\Phi, R)$中的丢番图问题，其中 Φ 是秩为 > 1的不可分解根系， R 是任意含幺交换环。

我们为初等幺幂元 $x_\alpha(1)$建立了一个双中心化子定理的变体。该定理对任意含幺交换环均成立。这一结果是证明任意单参数子群 $X_\alpha, \alpha \in \Phi$在 G中是丢番图的关键。随后我们证明，$G_\pi(\Phi, R)$中的丢番图问题与 R中的丢番图问题在多项式时间内等价（更准确地说，是卡普等价）。这一事实为特定类型的环带来了一系列模型论推论。

关键词：丢番图问题、丢番图集、切瓦莱群、双中心化子定理。

1. Introduction and State of Art

回顾一下，可数代数结构 $\mathcal{A}$ 中的丢番图问题（也称为希尔伯特第十问题或广义希尔伯特第十问题），记作 $\mathcal{D}(\mathcal{A})$，所询问的是：是否存在一种算法，对于给定的含有限个变量且系数属于 $\mathcal{A}$的有限 S 方程组，判定 S 在 $\mathcal{A}$ 中是否有解。特别地，如果 R 是一个可数环，那么 $\mathcal{D}(R)$所询问的是：含有 R 中系数的有限多项式方程组在 R 中是否有解，这个问题是否可判定。通常假定环 R带有一个固定的枚举，即一个函数 $\nu\colon \mathbb{N} \to R$，这使得人们能够枚举环中所有非交换多项式的环 $R\langle x_1;\ x_2;\ \dots\rangle$（含有可数多个变量 $x_1;\ x_2;$ .....），以及所有有限多项式方程组 $p(x_1;$ .....; $x_n) = 0$，其中 $p(x_1;$ .....; $x_n) \in R\langle x_1;\ x_2;\ \dots\rangle$，因此可以将它们作为判定算法的输入。如果环 R 是交换的（我们的情形正是如此），那么按照惯例，只考虑来自 $R[x_1;\ x_2;\ \dots]$ 的交换多项式。这个问题的原始版本由希尔伯特针对整数环 $\mathbb{Z}$ 提出。1970年，Matiyasevich [75] 在 Davis、Putnam和 Robinson [30]的工作基础上证明了否定的结论。随后，人们在各种各样的交换环 R 中研究了丢番图问题，并通过将 $\mathcal{D}(\mathbb{Z})$归约到 $\mathcal{D}(R)$，证明了它是不可判定的。根据定义，结构 $\mathcal{A}$ 中的丢番图问题归约到结构 $\mathcal{B}$ 中的丢番图问题，符号表示为 $\mathcal{D}(\mathcal{A}) \leqslant \mathcal{D}(\mathcal{B})$，是指：对于给定的系数属于 $\mathcal{A}$ 的有限方程组 S，存在一种算法能够构造出系数属于 $\mathcal{B}$ 的方程组S^*，使得 S 在 $\mathcal{A}$ 中有解，当且仅当 S^* 在 $\mathcal{B}$中有解。因此，如果 $\mathcal{D}(\mathbb{Z}) \leqslant \mathcal{D}(R)$，那么 $\mathcal{D}(R)$ 是不可判定的。如果归约算法是多项式时间的，则这种归约称为多项式时间归约（或卡普归约）。在本文中，我们证明

[1]Eugene Plotkin 的研究得到了以色列科学基金会资助项目 1994/20 的支持1

$G_\pi(\Phi, R)$ 和 R 中的丢番图问题在多项式时间内等价，确切地说， $\mathcal{D}(G_\pi(\Phi, R))$ 和 $\mathcal{D}(R)$ 可以在多项式时间内相互归约。特别是，它们要么都可判定，要么都不可判定。如果 R 因而 $G_\pi(\Phi, R)$ 不可数，则需要将 R 和 $G_\pi(\Phi, R)$ 中的丢番图问题限制为系数取自 R 或 $G_\pi(\Phi, R)$ 的某个固定可数子集的方程。对定义作适当调整后， R 和 $G_\pi(\Phi, R)$ 中的丢番图问题仍然在多项式时间内等价（稍后我们会进一步讨论这一点）。

关于交换环中方程的研究已经很多。然而，对于 $\mathbb{Q}$ 以及作为 $\mathbb{Q}$ 的有限代数扩张的域 F，丢番图问题仍未解决。关于域 F 的代数整数环 $\mathcal{O}$ 中的丢番图问题，已知的结果要多得多。具体而言，已有证明表明，对于某些代数数域 $\mathcal{O}$， $\mathcal{D}(\mathbb{Z})$ 可归约为 $\mathcal{D}(\mathcal{O})$；因此，在这类 $\mathcal{O}$ 中，丢番图问题 $\mathcal{D}(\mathcal{O})$ 是不可判定的。有关数论性质各异的环和域中的丢番图问题的更多信息，请参阅 [86], [83], [95] 。一些由来已久的猜想（例如，见 [32], [83]）指出，如上所述， $\mathbb{Q}$、 F 和 $\mathcal{O}$ 中的丢番图问题都是不可判定的。以下结果对本文很重要。如果交换幺环 R 是无限且有限生成的，那么在正特征的情形下， $\mathcal{D}(R)$ 是不可判定的；在特征为零的情形下，对于某个代数整数环 $\mathcal{O}$， $\mathcal{D}(\mathcal{O})$ 可在多项式时间内归约为 $\mathcal{D}(R)$（参见 Kirsten Eisentraeger 的博士论文（定理 7.1），该论文可在其个人网站上获取；另见 [47]）。

最近，Kharlam- povich 和 Myasnikov 在 [60] 中证明，在非交换结合含幺环类中，域上的自由结合代数以及各种无挠群的群代数中的丢番图问题是不可判定的，这些群包括环面型相对双曲群、直角 Artin 群、交换传递群以及各种群图的基本群。对于非结合环，已有证明表明，在系数取自任意整环、秩至少为三的自由李代数中，丢番图问题是不可判定的 [59]。针对非交换环中的丢番图问题（通过归约到交换环）， [46] 提出了一种通用方法。

另一方面，模型论方面的研究表明，某些经典域的一阶理论是可判定的：塔斯基证明了复数 $\mathbb{C}$ 和实数 $\mathbb{R}$ [104]的情形，而 Ershov、Ax 和 Kochen 证明了 p 进数 $\mathbb{Q}_p$ 和 $\mathbb{Z}_p$ ([40], [5], [6])的情形。给定有限方程组在 R 中有解这一陈述，可以用一个非常特殊的存在公式（正原子公式）来表示，其中系数取自 R，因此丢番图问题似乎是一阶理论 R的一部分，但系数的介入使整个问题变得复杂。事实上，常数（系数）的介入使丢番图问题与标准群语言或环语言中关于一等等价和一阶理论可判定性的经典模型论问题大不相同。稍后我们将对此作进一步说明，具体讨论线性群和切瓦莱群。

与环中的丢番图问题类似，如果一个结构 $\mathcal{A}$ 是可数的或有限的，那么我们假设它配备了一个枚举 $\nu\colon \mathbb{N} \to \mathcal{A}$，这使得人们能够枚举语言 $\mathcal{A}$中带有来自 $\mathcal{A}$的常数的所有项，进而枚举所有方程（在这种情况下，它们表示为两个项之间的等式），以及 $\mathcal{A}$上的所有有限方程组。另一方面，如果 $\mathcal{A}$ 是不可数的，那么根据定义，人们只能考虑带有来自 A的一个固定任意可数（或有限）子集 C 中的常数的方程。我们将这种形式的丢番图问题记作 $\mathcal{D}_C(\mathcal{A})$。这一修改使得人们能够以更加精确且也更加统一的方式考虑任意结构上的丢番图问题。正如我们

如下文所示，即使在可数结构 $\mathcal{A}$ 中，丢番图问题 $\mathcal{D}_C(\mathcal{A})$ 对一个子集 $C \subseteq \mathcal{A}$ 可能是可判定的，而对另一个子集则可能是不可判定的。此外，这还可能取决于对可数集合 C 所选取的枚举。容易看出，对于 $\mathcal{A}$ 的可数（或有限）子集 C，丢番图问题 $\mathcal{D}_C(\mathcal{A})$ 和 $\mathcal{D}_{\langle C\rangle}(\mathcal{A})$ 可以相互归约，其中 $\langle C\rangle$ 是 $\mathcal{A}$ 中由 C 生成的子结构。此外，若 $\mathcal{D}_C(\mathcal{A})$ 可判定，则按照 Maltsev [72] 和 Rabin [87], 的意义，$\langle C\rangle$ 是可计算的（递归的、可构造的）；因此，若 $\langle C\rangle$ 不可计算（这可能取决于 C 的枚举），则丢番图问题 $\mathcal{D}_C(\mathcal{A})$ 不可判定。因此，从一开始就可以只考虑具有可计算子结构 $\langle C\rangle$ 的 C 的枚举。

关于群中的方程组及其可判定性的研究历史悠久，可追溯至 1912 年 Dehn 对有限表示群中的字问题和共轭问题所做的开创性工作。回顾一下，群 G 中的一个方程是如下形式的表达式：$w(x_1, \ldots, x_n, g_1, \ldots, g_m) = 1$，其中 w 是变量 $x_1, \ldots, x_n$ 和常数 $g_1, \ldots, g_m \in G$ 上的群字。目前，研究群中丢番图问题有两种主要方法。第一种方法是，对于给定的固定群 G，尝试寻找一个交换含幺环 $\mathcal{A}$，使得 $\mathcal{A}$ 中的丢番图问题可算法地归约到 G 中的丢番图问题。在这种情况下，如果 $\mathcal{D}(\mathcal{A})$ 不可判定，那么 $\mathcal{D}(G)$ 也不可判定。此方向上的首个重要结果由 Romankov 得出：他证明，任何幂零类至少为 9 的非阿贝尔自由幂零群 N 中的丢番图问题都是不可判定的（他证明，即使只考虑群 N 中的单个方程，$\mathcal{D}(\mathbb{Z}) \leqslant \mathcal{D}(N)$ 仍成立） [91]。最近，Duchin 、 Liang 和 Shapiro 在 [39] 中证明，对于任意非阿贝尔自由幂零群 N，$\mathcal{D}(\mathbb{Z}) \leqslant \mathcal{D}(N)$，因此 $\mathcal{D}(N)$ 不可判定。Garreta、Myasnikov 和 Ovchinnikov 在 [45] 中得到了这些结果的重大推广，他们证明，对于任意有限生成的非虚阿贝尔幂零群 G，都存在一个代数整数环 $\mathcal{O}$（取决于 G），它由方程可解释于 G 中，因此 $\mathcal{D}(\mathcal{O})$ 是 Karp 可归约到 $\mathcal{D}(\{v44)\}$ 的。此外，他们在 [44] 中给出了环 $\mathcal{O}$ 同构于 $\mathbb{Z}$ 的一个一般充分条件，因此在这种情况下，G 中的丢番图问题不可判定。基于此，他们证明，随机幂零群 G（由幂零类至多为 c 的幂零群簇 $\mathcal{N}_c$ 中的随机表示给出，其中任意 $c \geqslant 2$）具有 $\mathcal{O} \cong \mathbb{Z}$，因此其丢番图问题不可判定。关于幂零群的这些结果可通过 H 的适当丢番图幂零子群，或通过 H [45] 的适当丢番图幂零商群，广泛应用于非幂零群 H 中的丢番图问题。例如，这项技术可以证明，任何有限生成的自由可解非阿贝尔群中的丢番图问题都是不可判定的。

这一系列结果在第二种方法中发生了巨大变化：该方法试图证明，通过将给定群 G 中的丢番图问题归约到非阿贝尔自由群 F 或自由幺半群 M 中的丢番图问题，可以判定前者（例如参见 Rips 和 Sela [90], 、 Damani 和 Guirardel [29], 、 Diekert 和 Muschol [38], 、 Casals-Ruiz 和 Kazachkov [23], [22], , 以及 Diekert 和 Lohrey [37]）。关于这一领域的更多结果，参见 [58] 。此处的主要结果由 Makanin [68], [69] 和 Razborov [88], [89] 给出，他们证明了丢番图问题 $\mathcal{D}(M)$ 和 $\mathcal{D}(F)$ 是可判定的；并且，对于自由群 F，他们还进一步用 Makanin–Razborov 图描述了任意有限方程组的解集。F 中解集的另一种描述则是用 NTQ 系统（也称为 ω-剩余自由塔）给出的，见 [57]。NTQ 系统为自由群的代数几何和模型论提供了一种有效方法。最近，一种截然不同的方法

求解自由群、自由幺半群和双曲群中的方程问题的方法在一系列论文 [36], [54], [55], [24], [25] 中得到发展。

在其经典论文中，[70] A.I. Maltsev 研究了矩阵群 $\mathcal{G}_n(F)$ 的初等等价，其中 $\mathcal{G}_n$ 是 GL$_n$、SL $_n$、PGL $_n$、PSL $_n$ $n \geqslant 3$ 之一，而 F是一个域。具体而言，他证明了 $\mathcal{G}_n(F) \equiv \mathcal{G}_m(L)$ 当且仅当 $n = m$ 且 $F \equiv L$。他的证明基于两个主要结果。第一个结果指出，对于任意整数 $k \geqslant 3$ 以及上述的 $\mathcal{G}_n$，存在一个群语句 $\Phi_{k,\mathcal{G}}$，使得对于任意 n和域 F，$\Phi_{k,\mathcal{G}}$ 在 $\mathcal{G}_n(F)$ 中成立，当且仅当 $k = n$。第二个结果是，F 与 $\mathcal{G}_n(F)$ 可以相互解释。更准确地说，$\mathcal{G}_n(F)$ 可在 F 中绝对解释（即不使用参数），而 F 可在 $\mathcal{G}_n(F)$ 中相对于某个可定义的参数元组子集一致地解释（所谓的正则可解释性）。这意味着，理论 $Th(F)$ 与 $Th(\mathcal{G}_n(F))$ 在多项式时间内可相互归约，因此 $Th(\mathcal{G}_n(F))$ 可判定，当且仅当 $Th(F)$ 可判定。后来，Beidar 和 Mikhalev 提出了研究经典矩阵群初等等价的另一种通用方法 [9]。他们的证明基于 Keisler–Shelah 定理（两个结构初等等价，当且仅当它们在某些非主超滤子上的超幂同构（见 [56], [94]））），以及对 $\mathcal{G}_n(F)$ 这类群的抽象同构的描述。E. Bunina 将他们的结果推广到酉线性群和切瓦莱群（见 [14], [16], [17], [15]）。需要注意的是，上述所有结果中的一阶理论仅包含群和环的语言中的标准常数。O. Belegradek 详细研究了群 $UT_n(R)$ 的模型论，其中 $n \geqslant 3$，且 R 是任意的酉结合环 [10]。他大量利用了环 R 可在$UT_n(R)$ 中（带参数）解释这一事实。A. Myasnikov 和 M. Sohrabi 研究了域及代数整数环上群 SL $_n(\mathcal{O})$、GL $_n(\mathcal{O})$ 和 $T_n(\mathcal{O})$ 在 [79] 和 [78]中的模型论。他们的方法利用了群与环之间的相互可解释性（以及双可解释性）。类似地，N. Avni、A. Lubotsky 和 C. Meiri 在 [7] 中研究了非一致高秩算术群的一阶刚性（另见 [8]）。最近，D. Segal 和 K. Tent（见 [92]）证明，对于整环 R 上的秩为 > 1 的切瓦莱群 $G_\pi(\Phi, R)$，如果 $G_\pi(\Phi, R)$ 具有有限初等宽度或为伴随群，那么 $G_\pi(\Phi, R)$ 与 R 是双可解释的。在 [20] 中，E. Bunina 证明，在局部环上，秩为 > 1 的切瓦莱群 $G_\pi(\Phi, R)$ 与相应的环正则双可解释。

尽管相关，上述模型论结果都未能为相应群中的丢番图问题提供多少启示。因为要关联 $\mathcal{G}_n(R)$ 或 $G_\pi(\Phi, R)$ 与 R 中的丢番图问题，就必须证明它们通过方程而非任意一阶公式相互可解释。Myasnikov 和 Sohrabi 在其论文 [77] 中正是针对经典线性群一般线性群 $_n(R)$、特殊线性群 $_n(R)$、$T_n(R)$、$UT_n(R)$ 做到了这一点；而本文则针对切瓦莱群 $G_\pi(\Phi, R)$ 进行研究。

回顾一下，群 G 的一个子集（尤其是子群）H 若能在 G 中由如下形式的公式定义，则称其在 G 中是丢番图的：

$$\Phi(x) = \exists y_1 \ldots \exists y_n \left(\bigwedge_{i=1}^{k} w_i(x, y_1, \ldots, y_n) = 1 \right),$$

其中 $w_i(x, y_1, \ldots, y_n)$ 是关于 $x, y_1, \ldots, y_n$ 的群字。这类公式称为丢番图公式（在数论中）或正原子公式（在模型论中）。遵循 [47],，我们称结构 $\mathcal{A}$ 在结构 $\mathcal{B}$ 中是 e-可解释的（或由方程可解释，或丢番图可解释），如果 $\mathcal{A}$ 可通过丢番图公式在 $\mathcal{B}$ 中可解释（见下文）。重点在于♀♀♀♀♀♀

这个定义是指，如果 $\mathcal{A}$ 是 $\mathcal{B}$ 的e-可解释结构，那么 $\mathcal{A}$ 中的丢番图问题可以在多项式时间内归约（卡普归约）到 $\mathcal{B}$中的丢番图问题。一方面，获得 e-可解释性比获得可解释性本身更困难，因为在后者中可以使用任意公式（而不仅仅是丢番图公式）；但另一方面，要研究结构的一阶等价，通常不会使用语言中的常数，而在丢番图问题中则要求使用常数。

如果一个子群 $G \subseteq$ 一般线性群$_n(R)$包含子群 $E_n(R)$，则称其为大子群；该子群是在一般线性群$_n(R)$中由所有换位 $t_{ij}(\alpha)$、 $i \neq j$和 $\alpha \in R$ 生成的。特别地，子群特殊线性群 $_n(R)$（当 R 为交换的时）以及 $E_n(R)$ 本身都是大子群。类似地，切瓦莱群的一个子群 $G \subseteq G_\pi(\Phi, R)$ 称为大子群，如果它包含由所有初等幺幂元 $x_\alpha(t)$、 $\alpha \in \Phi$、 $t \in R$生成的初等切瓦莱群（子群）$E_\pi(\Phi, R)$。引入一般线性群$_n(R)$（$G_\pi(\Phi, R)$）的大子群，使我们能够统一处理类似的论证；否则，这些论证需要分别针对一般线性群 $_n(R)$、特殊线性群$_n(R)$ 和 $E_n(R)$ 使用。这也强调了这样一个事实：本文 [77] 以及本论文所采用的方法，不同于Maltsev的论文 [70],中使用的方法，完全建立在换位和幂零子群（初等幺幂元）之上。下文中，通过X_α、 $\alpha \in \Phi$，我们表示一参数子群 $\{x_\alpha(t) \mid t \in R\}$。在第5节中，我们研究大子群 $G_\pi(R)$ 的丢番图子群。特别地，我们证明以下关键的技术性结果（与 [77] 比较）：

结果 1（命题3和命题5）。设 G 是 $G_\pi(\Phi, R)$ 的一个大子群， $rank\,\Phi > 1$。那么对于任意 $\alpha \in \Phi$ ，单参数子群 X_α 在 G 中是丢番图的（由集合 $\{x_\alpha(1) \mid \alpha \in \Phi\}$ 中的常数定义）。

这一结果与 [77], 中相应的结果类似，但它主要基于对任意交换环上的切瓦莱群 $G_\pi(\Phi, R)$ 中某些集合的中心化子的描述。该描述在第2节至第4节中得到证明：第2节针对所有域上的切瓦莱群，利用布鲁哈分解和直接计算完成证明；第3节针对所有局部环上的切瓦莱群，利用高斯分解、上一节的结果以及直接计算完成证明；第4节则借助局部化方法和上一节的结果，将其推广到所有交换环。最后，我们证明以下结果（该结果本身也有独立价值）：

结果 2（定理 3）。对于任意切瓦莱群（或其大子群） $G = G_\pi(\Phi, R)$，其中Φ 是秩为 > 1的不可约根系， R 是任意含幺交换环，若对于某个 $\alpha \in \Phi$ ，元素 $g \in C_G(\Gamma_\alpha)$，则 $g = cx_\alpha(t)$，但 $t \in R$, $c \in Z(G)$的情形除外，且 α 是短的。

在 $\Phi = \mathsf{C}_l = \{\pm e_i \pm e_j \mid 1 \leqslant i, j \leqslant l, i \neq j\} \cup \{\pm 2e_i \mid 1 \leqslant i \leqslant l\}$ 且 $\alpha = e_1 + e_2$的情形下，若$g \in C_G(\Gamma_\alpha)$，则

$$g = cx_{e_1+e_2}(t_1)x_{2e_1}(t_2)x_{2e_2}(t_3), \quad c \in Z(G).$$

结果 1 有助于证明

结果 3（定理 4）。设 G 是切瓦莱群 $G_\pi(\Phi, R)$的一个大子群，其中 Φ是秩为 $\ell > 1$的不可分解根系，R 是任意含幺交换环。那么，环 R 可在 G 中解释（使用集合 $C_\Phi = \{x_\alpha(1) \mid \alpha \in \Phi\}$中的常数）。

最后这个定理给出了关于（初等）切瓦莱群与相应环之间 Karpe 等价的结果：

结果 4（定理 6 和 7）。若 Φ 是秩为 >1的不可分解根系， R 是任意含幺交换环，则任意切瓦莱群$G_\pi(\Phi, R)$中的丢番图问题与 R中的丢番图问题卡普等价。更准确地说：

1) 如果 C 是 $G_\pi(\Phi, R)$ 的可数子集，那么 $\mathcal{D}_C(G_\pi(\Phi, R))$ 卡普归约到 $\mathcal{D}_{R_C}(R)$。2) 如果 T 是 R 的可数子集，那么存在 $G_\pi(\Phi, R)$ 的一个可数子集 C_T ，使得 $\mathcal{D}_T(R)$ 卡普归约到 $\mathcal{D}_{C_T}(G_\pi(\Phi, R))$。

如果初等切瓦莱群 $E_\pi(\Phi, R)$ 具有有界初等生成，那么 $E_\pi(\Phi, R)$ 中的丢番图问题与 R 中的丢番图问题卡普等价。

第 6 节致力于介绍主要定理的应用。在 [77] 中，针对经典线性群证明了类似的推论，这里我们对切瓦莱群重复这些推论。

结果5（定理 8）。如果 Φ 是秩为 >1 的不可分解根系，那么所有切瓦莱群 $G_\pi(\Phi, \mathbb{Z})$ 中的丢番图问题与 $\mathbb{Z}$ 中的丢番图问题卡普等价，特别是它是不可判定的。

以下是数论中的一个重要猜想：

丢番图问题在 $\mathbb{Q}$ 中，以及在任意数域 F 或任意代数整数环 $\mathcal{O}$ 中，都是不可判定的。

以下结果将数域或代数整数环上的切瓦莱群的丢番图问题从群论转向数论。

结果 6（定理 9）。设 Φ 是秩为 >1 的不可分解根系，且 R 是数域或代数整数环。那么，当且仅当切瓦莱群 $G_\pi(\Phi, R)$ 中的丢番图问题不可判定时，上述猜想对 R 成立。

以下来自 [47] 的结果描述了有限生成交换环中丢番图问题的当前状况：

设 R 为无限有限生成结合交换含幺环。则以下情形之一成立：

(1) 如果 R 具有正特征 $n>0$，那么对于某个超越元 t 和某个素数 p，多项式环 $\mathbb{F}_p[t]$ 在 R 中是 e-可解释的；并且 $\mathcal{D}(R)$是不可判定的。(2) 如果 R 具有零特征且秩为无限，那么上述相同结论仍成立：对于某个 t 和 p，多项式环 $\mathbb{F}_p[t]$ 在 R 中是 e-可解释的；并且 $\mathcal{D}(R)$是不可判定的。(3) 如果 R 具有零特征且秩为有限，那么代数整数环 $\mathcal{O}$ 在 R中是 e-可解释的。

这一事实与结果4 一起推出了以下定理，该定理彻底阐明了关于无限有限生成交换含幺环上的切瓦莱群中的丢番图问题的情形：

结果7（定理10）。设 Φ 是秩为 >1 的不可分解根系， R 是任意无限有限生成的含幺交换环，且 $G_\pi(\Phi, R)$ 是相应的 Chevalley 群。那么：

1）如果 R 具有正特征，那么 $G_\pi(\Phi, R)$中的丢番图问题是不可判定的。2）如果 R 具有零特征且秩无限，那么$G_\pi(\Phi, R)$中的丢番图问题是不可判定的。

3）如果 R 具有零特征且秩有限，那么某个代数整数环 $\mathcal{O}$ 中的丢番图问题可 Karp 归约到 $G_\pi(\Phi, R)$中的丢番图问题。因此，如果猜想 1 成立，那么 $G_\pi(\Phi, R)$中的丢番图问题是不可判定的。

如果 R 是一个代数闭域，那么

1) 如果 A 是 R 的可计算子域，那么带有来自 A 的常数的语言中的 R 的一阶理论 $Th_A(R)$ 是可判定的。特别地，丢番图问题 $\mathcal{D}_A(R)$ 是可判定的。¯2) 如果 A 是 R 的可计算子域，那么 R 中 A 的代数闭包 A 是可计算的。结合上述事实与定理 6 和 7，我们得到

结果 8（定理 12）。设 Φ 是秩为 >1 的不可分解根系， R 是代数闭域，而 $G_\pi(\Phi, R)$ 是相应的切瓦莱群。如果 A 是 R 的可计算子域，那么 $G_\pi(\Phi, R)$ 中带有来自 $G_\pi(\Phi, A)$ 的常数的丢番图问题是可判定的（在对 $G_\pi(\Phi, A)$ 进行适当枚举的条件下）。

令 $R = \mathbb{R}$ 为实数域， A 为 $\mathbb{R}$的一个可数（或有限）子集。我们对 $\mathbb{R}$ 上切瓦莱群的丢番图问题的处理，基于以下两个关于 $\mathbb{R}$ 上丢番图问题的结果；这些结果广为人知:

令 A 为 $\mathbb{R}$的一个有限或可数子集。那么，当且仅当有序子域 $F(A)$ 是可计算的， A 上系数取自 A 的丢番图问题才是可判定的。此外，在这种情况下，整个一阶理论 $Th_A(\mathbb{R})$ 都是可判定的。

如果能以任意精度有效地用有理数逼近一个实数 $a \in \mathbb{R}$ ，那么该实数就是可计算的。所有可计算实数 $\mathbb{R}^c$ 构成 $\mathbb{R}$的一个实闭子域；特别地， $\mathbb{R}^c$与 $\mathbb{R}$一阶等价。若矩阵 $A \in \mathbf{GL}_n(\mathbb{R})$ 的所有元素 A都是可计算实数，则称该矩阵为可计算的。切瓦莱群 $G_\pi(\Phi, \mathbb{R})$ 是 $\mathbb{R}$ 上的矩阵代数群，因此可以将其元素视为矩阵。

结果 9（定理 13）。设 Φ 是秩为 >1 的不可分解根系， $G_\pi(\Phi, \mathbb{R})$ 是定义在实数域 $\mathbb{R}$ 上的切瓦莱群。若 A 是 $\mathbb{R}$ 的可计算有序子域，则带有来自 $G_\pi(\Phi, A)$ 的常数的一阶理论 $Th(G_\pi(\Phi, \mathbb{R}))$ 是可判定的。特别地， $G_\pi(\Phi, \mathbb{R})$ 中带有来自 $G_\pi(\Phi, A)$ 的常数的丢番图问题是可判定的（在对 $G_\pi(\Phi, A)$ 进行适当枚举的条件下）。

结果10（定理 14）。设 Φ 是秩为 >1 的不可分解根系， $G_\pi(\Phi, \mathbb{R}^c)$ 是定义在可计算实数域 $\mathbb{R}^c$ 上的切瓦莱群。则以下结论成立:

1）可计算群 $G_\pi(\Phi, \mathbb{R}^c)$ 中的丢番图问题是不可判定的。2）对于 $G_\pi(\Phi, \mathbb{R}^c)$ 的任意有限生成子群 C， $G_\pi(\Phi, \mathbb{R}^c)$ 中系数取自 C 的丢番图问题是可判定的。

结果 11（定理 15）。设 Φ 是秩为 >1 的不可分解根系， $G_\pi(\Phi, \mathbb{R})$ 是定义在可计算实数域 $\mathbb{R}^c$ 上相应的切瓦莱群。如果元素 $g \in E_\pi(\Phi, \mathbb{R})$ 不可计算，那么对于系数属于 $\{x_\alpha(1) \mid \alpha \in \Phi\} \cup \{g\}$ 的方程，丢番图问题在 $G_\pi(\Phi, \mathbb{R})$ 的任意大子群中都是不可判定的。

与实数的情形类似，对于每个固定的素数 p，都可以定义可计算的 p-进数。

结果 12（定理 16）。设 Φ 是秩为 >1 的不可分解根系。则以下结论成立:

1) 设 $a_1, \ldots, a_m \in \mathbb{Q}_p^c$，且 $A = \mathbb{Q}(a_1, \ldots, a_m)$ 是由 $a_1, \ldots, a_m$ 生成的 $\mathbb{Q}_p$ 的子域。则带有来自 $G_\pi(\Phi, A)$ 的常数的一阶理论 $Th(G_\pi(\Phi, \mathbb{Q}_p))$ 是可判定的。特别地，带有来自 $G_\pi(\Phi, A)$ 的常数的 $G_\pi(\Phi, \mathbb{Q}_p)$ 中的丢番图问题是可判定的（在对 $G_\pi(\Phi, A)$ 进行适当枚举的条件下）。
2) 设 $a_1, \ldots, a_m \in \mathbb{Z}_p^c$，且 $A = \mathbb{Z}(a_1, \ldots, a_m)$ 是由 $a_1, \ldots, a_m$ 生成的 $\mathbb{Z}_p$ 的子环。则带有来自 $G_\pi(\Phi, A)$ 的常数的一阶理论 $Th(G_\pi(\Phi, \mathbb{Q}_p))$ 是可判定的。特别地，带有来自 $G_\pi(\Phi, A)$ 的常数的 $G_\pi(\Phi, \mathbb{Q}_p)$ 中的丢番图问题是可判定的（在对 $G_\pi(\Phi, A)$ 进行适当枚举的条件下）。

结果13（定理 17）。设 Φ 是一个秩为 > 1 的不可分解根系，且 $G_\pi(\Phi, \mathbb{Q}_p)$ ($G_\pi(\Phi, \mathbb{Z}_p)$ $p \neq 2$) 是其对应的切瓦莱群，它定义在 $\mathbb{Q}_p$ ($\mathbb{Z}_p$) 上。如果一个元素 $g \in E_\pi(\Phi, \mathbb{Q}_p)$ ($g \in E_\pi(\Phi, \mathbb{Z}_p)$ $p \neq 2$)不可计算，那么对于 $\{x_\alpha(1) \mid \alpha \in \Phi\} \cup \{g\}$ 中系数的方程，丢番图问题在 $G_\pi(\Phi, \mathbb{Q}_p)$($G_\pi(\Phi, \mathbb{Z}_p)$ $p \neq 2$) 的任意大子群中都是不可判定的。

2. Chevalley groups

本节将介绍一些记号，并回顾本文中会用到的技术性结果。

对于群 G 和 x、$y \in G$，我们用 x^y 表示 x 被 y 共轭得到的 yxy^{-1}，用 $[x, y]$ 表示交换子 $xyx^{-1}y^{-1}$。对于子集 $A \subseteq G$，我们用 $C_G(A)$ 表示中心化子 $\{x \in G \mid [x, a] = 1 \forall a \in A\}$；特别地，$Z(G) = \{x \in G \mid [x, y] = 1 \forall y \in G\}$ 是 G 的中心。对于子集 X、$Y \subseteq G$，我们用 $[X, Y]$ 表示由所有交换子 $[x, y]$ 生成的 G 的子群，其中 $x \in X$、$y \in Y$。于是 $[G; G]$ 是 G 的导出子群 G'（G 的换位子群）。

在本文其余部分中，R 表示任意带单位元 1 的交换结合环。用 R^* 表示 R 的可逆（单位）元素构成的乘法群，用R^+ 表示 R的加法群。

2.1. 根系与半单李代数。

我们固定一个秩为 $\ell > 1$、单根组为 Δ的不可分解根系 Φ，其正根（负根）集为 Φ^+ (Φ^-)，魏尔群为 W。回顾一下，任何两个等长根在魏尔群的作用下都是共轭的。令 $|\Phi^+| = m$。关于根系及其性质的更详细论述，可参见书籍 [51], [13]。

还要记住，对于 α、$\beta \in \Phi$

$$\langle \alpha, \beta \rangle = 2\frac{(\alpha, \beta)}{(\beta, \beta)},$$

其中 (α, β) 表示根空间上的标准内积。

现在假设我们有一个半单复李代数 $\mathcal{L}$，其嘉当子代数为 $\mathcal{H}$（有关半单李代数的更多详细信息，例如可参见书籍 [51]）。

李代数 $\mathcal{L}$ 有分解 $\mathcal{L} = \mathcal{H} \oplus \sum_{\alpha \neq 0} \mathcal{L}_\alpha$,

$$\mathcal{L}_\alpha := \{x \in \mathcal{L} \mid [h, x] = \alpha(h)x \text{ for every } h \in \mathcal{H}\},$$

并且如果 $\mathcal{L}_\alpha \neq 0$，那么 $\dim \mathcal{L}_\alpha = 1$，所有非零的 $\alpha \in \mathcal{H}$ 使得 $\mathcal{L}_\alpha \neq 0$，构成某个根系 Φ。根系 Φ 与有理数域 $\mathbb{C}$上的半单李代数 $\mathcal{L}$ 唯一地（在自同构意义下）相互确定。

在李代数 $\mathcal{L}$ 上可以引入双线性 Killing 形式 $\varkappa(x,y) = \mathrm{tr}(\mathrm{ad}\, x\, \mathrm{ad}\, y)$，它在 $\mathcal{H}$上非退化。因此，我们可以将空间 $\mathcal{H}$ 与 $\mathcal{H}^*$等同起来。

我们可以选取一组基 $\{h_1,\dots,h_l\}$ in $\mathcal{H}$，并且对每个 $\alpha\in\Phi$ 元素 $x_\alpha\in\mathcal{L}_\alpha$，使得$\{h_i;\ x_\alpha\}$ 是 $\mathcal{L}$ 中的一组基，且这组基中任意两个元素的交换子都是同一组基中元素的整数线性组合。这组基称为切瓦利基。

2.2. 初等切瓦莱群。

现在介绍初等切瓦利群（见 [99]）。

设 $\mathcal{L}$ 为一个（在 $\mathbb{C}$ 上的）半单李代数，具有根系 Φ，$\pi:\ \mathcal{L}\to\mathfrak{gl}(V)$ 为其有限维忠实表示（维数为 n）。若 $\mathcal{H}$ 是 $\mathcal{L}$ 的一个嘉当子代数，则称线性泛函 $\lambda\in\mathcal{H}^*$ 为给定表示的一个权，若存在一个非零向量 $v\in V$（称为权向量），使得对任意 $h\in\mathcal{H}$ $\pi(h)v=\lambda(h)v$.

在切瓦莱基 V中，所有 $k\in\mathbb{N}$ 的算子 $\pi(x_\alpha)^k/k!$ 都写成整数（幂零）矩阵。整数矩阵也可以视为任意含幺交换环上的矩阵。设 R 是这样的环。考虑环 R 上的矩阵 $n\times n$，矩阵 $\pi(x_\alpha)^k/k!$（$\alpha\in\Phi$、$k\in\mathbb{N}$）包含在 $M_n(R)$ 中。

现在考虑自由模 R^n 的如下形式的自同构

$$\exp(tx_\alpha)=x_\alpha(t)=1+t\pi(x_\alpha)+t^2\pi(x_\alpha)^2/2+\dots+t^k\pi(x_\alpha)^k/k!+\dots$$

由于所有矩阵 $\pi(x_\alpha)$ 都是幂零的，因此这个级数是有限的。自同构 $x_\alpha(t)$ 称为初等根元素。由所有 $x_\alpha(t)$（$\alpha\in\Phi$、$t\in R$）生成的 Aut (R^n) 中的子群称为初等切瓦莱群（记作：$E_\pi(\Phi,R)$）。

在初等切瓦莱群中，我们可以引入以下重要元素和子群:

- $w_\alpha(t)=x_\alpha(t)x_{-\alpha}(-t^{-1})x_\alpha(t)$，$\alpha\in\Phi$, $t\in R^*$;
- $h_\alpha(t)=w_\alpha(t)w_\alpha(1)^{-1}$;
- N 由所有的 $w_\alpha(t)$，$\alpha\in\Phi$, $t\in R^*$ 生成;
- H 由所有的 $h_\alpha(t)$，$\alpha\in\Phi$, $t\in R^*$ 生成;
- 切瓦莱群 $G(E)$ 的子群 $U=U(R)$ 由元素 $x_\alpha(t)$,$\alpha\in\Phi^+$, $t\in R$ 生成，子群 $V=V(R)$ 由元素 $x_{-\alpha}(t)$，$\alpha\in\Phi^+$ $t\in R$ 生成。

x_α切瓦莱基上的 $x_\alpha(t)$ 作用见 [21], [106] 的描述。

众所周知，群 N 是初等切瓦莱群中 H 的正规化子，商群 N/H 同构于魏尔群 $W(\Phi)$。

给定表示的所有权通过加法生成一个格（自由阿贝尔群，其中每个 $\mathbb{Z}$-基也是 $\mathcal{H}^*$中的 $\mathbb{C}$-基），称为权格 Λ_π。

初等切瓦莱群的定义甚至不需要切瓦莱群的表示，只需其权格即可。也就是说，除去抽象同构的差异，初等切瓦莱群完全由根系 Φ、含幺元的交换环 R 和权格 Λ_π确定。

在所有格中，我们可以特别指出两个：一个是对应于伴随表示的格，由所有根生成（根格 Λ_{ad}）；另一个是由所有表示的所有权生成的格（权格 Λ_{sc}）。对于每个忠实表示 π，都有包含关系 $\Lambda_{ad}\subseteq\Lambda_\pi\subseteq\Lambda_{sc}$.。相应地，我们有伴随型和万能型（单连通）初等切瓦莱群。

每个初等切瓦莱群都满足以下关系:

(R1) $\forall\alpha\in\Phi\ \forall t,u\in R\quad x_\alpha(t)x_\alpha(u)=x_\alpha(t+u)$;

(R2) $\forall \alpha, \beta \in \Phi\ \forall t, u \in R \quad \alpha + \beta \neq 0 \Rightarrow$

$$[x_\alpha(t), x_\beta(u)] = x_\alpha(t)x_\beta(u)x_\alpha(-t)x_\beta(-u) = \prod x_{i\alpha+j\beta}(c_{ij}t^i u^j),$$

其中 i、j 为整数，乘积遍历所有根 $i\alpha + j\beta$，并按某个固定顺序取； c_{ij} 是不依赖于 t 和 u、但依赖于 α 、 β 以及乘积中根的顺序的整数。

(R3) $\forall \alpha \in \Phi\ w_\alpha = w_\alpha(1)$; **(R4)** $\forall \alpha, \beta \in \Phi\ \forall t \in R^*\ w_\alpha h_\beta(t) w_\alpha^{-1} = h_{w_\alpha(\beta)}(t)$;
(R5) $\forall \alpha, \beta \in \Phi\ \forall t \in R^*\ w_\alpha x_\beta(t) w_\alpha^{-1} = x_{w_\alpha(\beta)}(ct)$，其中 $c = c(\alpha, \beta) = \pm 1$;
(R6) $\forall \alpha, \beta \in \Phi\ \forall t \in R^*\ \forall u \in R\ h_\alpha(t) x_\beta(u) h_\alpha(t)^{-1} = x_\beta(t^{\langle \beta, \alpha \rangle} u)$。对于给定的 $\alpha \in \Phi$ 乘 X_α，我们将子群 $\{x_\alpha(t) \mid t \in R\}$ 记为。

2.3. 环上的切瓦莱群。

我们简要回顾与切瓦莱群定义相关的一些基础知识。关于环上的切瓦莱群的更多详情，参见 [99], [27], [11], [21], [31], [105], [106], 及其中的参考文献。

设 Φ 是秩为 $\geqslant 2$ 的约化不可约根系， $W = W(\Phi)$ 是其 Weyl 群。考虑一个格 Λ_π，它介于根格 Λ_{ad} 与权格 Λ_{sc} 之间。设R 是一个含幺交换环，其乘法群为 R^*。

这些数据确定了类型为 (Φ, Λ_π)、定义在 R 上的切瓦莱群 $G = G_{\Lambda_\pi}(\Phi, R)$。它通常构造为类型为 (Φ, Λ_π) 的 Chevalley–Demazure 群概形 $G_{\Lambda_\pi}(\Phi, -)$ 的 R-点群。在 $\Lambda_\pi = \Lambda_{sc}$ 的情形下，群 G 称为单连通群，记作 $G_{sc}(\Phi, R)$。在另一极端情形 $\Lambda_\pi = \Lambda_{\mathrm{ad}}$ 下，群 G 称为伴随群，记作 $G_{\mathrm{ad}}(\Phi, R)$。许多结果与格 Λ_π 无关，对给定类型 Φ 的所有群都成立。在所有此类情形下，或当 Λ_π 可由上下文确定时，我们在记号中省略对π 的任何提及，并用 $G(\Phi, R)$ 表示定义在 R 上的任意类型为 Φ 的切瓦莱群。

在下文中，我们还固定 $G = G(\Phi, R)$ 中的一个分裂极大环面 $T = T(\Phi, R)$。这一选择唯一确定 G 中关于 T 初等的幺幂根子群 X_α, $\alpha \in \Phi$。照例，我们固定映射 $x_\alpha\colon R \mapsto X_\alpha$, 使得 $X_\alpha = \{x_\alpha(t) \mid t \in R\}$，并要求这些参数化由带整数系数的 Chevalley 交换子公式相互关联，见 R1–R2。上述幺幂元 $x_\alpha(t)$，其中 $\alpha \in \Phi$, $t \in R$ 关于 $T(\Phi, R)$ 初等，也称为初等幺幂根元，或简称根幺幂元。

进一步，

$$E(\Phi, R) = \langle x_\alpha(t),\ \alpha \in \Phi,\ t \in R \rangle$$

表示由所有初等根幺幂元，或等价地由所有根子群 X_α, $\alpha \in \Phi$ 张成的 $G(\Phi, R)$ 的初等子群。

这正是上一节中定义的初等切瓦莱群。我们也可以从代数群的角度来考察切瓦莱群。这种观点对于许多应用尤为重要。

所有这些群都定义在 $\mathrm{SL}_n(R)$ 中，是矩阵条目 a_{ij} 的整数系数多项式的公共零点集（例如，对于根系 C_ℓ 和泛表示，我们有 $n = 2l$，以及条件 $(a_{ij})Q(a_{ji}) - Q = 0$中的多项式）。现在显然，乘法和取逆元素也由整数系数多项式定义。因此，这些多项式可以视为任意含幺交换环上的多项式。设某个定义在 $\mathbb{C}$ 上的初等切瓦莱群 E 为

由多项式 $p_1(a_{ij}), \dots, p_m(a_{ij})$ 定义在 $\mathrm{SL}_n(\mathbb{C})$ 中。对于含幺交换环 R，考虑群

$$G(R) = \{(a_{ij}) \in \mathrm{SL}_n(R) \mid \widetilde{p}_1(a_{ij}) = 0, \dots, \widetilde{p}_m(a_{ij}) = 0\},$$

其中 $\widetilde{p}_1(\dots) \dots \widetilde{p}_m(\dots)$ 是与 $p_1(\dots) \dots, p_m(\dots)$ 具有相同系数的多项式，但它们是在 R 上考虑的。

代数闭域 K 上的半单线性代数群 G 恰好是切瓦莱群 $G(K) = E(\Phi, K)$（参见 [99], §5）。

切瓦莱群 $G_\pi(\Phi, R)$ 的标准极大环面通常记作 $T_\pi(\Phi, R)$，并且同构于 $\mathrm{Hom}(\Lambda_\pi, R^*)$。

我们用 $h(\chi)$ 表示环面 $T_\pi(\Phi, R)$ 中对应于同态 $\chi \in Hom(\Lambda(\pi), R^*)$ 的元素。

特别地，$h_\alpha(u) = h(\{v4, u)$ $(u \in R^*, \alpha \in \Phi)$，其中

$$\chi_{\alpha,u} : \lambda \mapsto u^{\langle \lambda, \alpha \rangle} \quad (\lambda \in \Lambda_\pi).$$

2.4. 切瓦莱群与其初等子群之间的联系。

切瓦莱群与相应初等子群之间的联系，是环上切瓦莱群理论中的一个重要问题。对于初等切瓦莱群，存在一套方便的生成元 $x_\alpha(\xi)$、$\alpha \in \Phi$、$\xi \in R$，这些生成元之间的所有关系都已为人熟知。对于一般的切瓦莱群，情况则并非总是如此。

若 R 是代数闭域，则

$$G_\pi(\Phi, R) = E_\pi(\Phi, R)$$

对任意表示 π，都有此结论。即使对于非代数闭域，这个等号也不成立。

然而，如果 G 是单连通群，且环 R 是半局部的（即只含有限个极大理想），那么我们有如下性质

$$G_{sc}(\Phi, R) = E_{sc}(\Phi, R).$$

[74], [1], [98], [3]。

下面以环 R 为半局部环、相应切瓦莱群非单连通的情形为例，说明切瓦莱群与其初等子群之间的差别。在这种情况下，$G_\pi(\Phi, R) = E_\pi(\Phi, R)T_\pi(\Phi, R)]$（见 [1], [3], [74]），而元素 $h(\chi)$ 与初等生成元之间的联系可由公式表示为

$$h(\chi)x_\beta(\xi)h(\chi)^{-1} = x_\beta(\chi(\beta)\xi). \tag{1}$$

注 1. 由于 $\chi \in \mathrm{Hom}(\Lambda(\pi), R^*)$，如果我们知道 χ 在一组能够生成所有根的根上的取值（例如，在 Φ 的某个基上），那么对于所有 $\beta \in \Phi$，我们就知道所有 β 的 χ；相应地，对于所有 $\beta \in \Phi$ 和 $\xi \in R^*$，我们也知道所有 ξ 的 $x_\beta(h(\chi))$。

因此，特别地，如果对于 Φ 的某个生成集中的所有根 β，都有 $[x_\beta(1), h(\chi)] = 1$，那么 $h(\chi) \in Z(E_\pi(\Phi, R))$，从而 $h(\chi) \in Z(G_\pi(\Phi, R))$。

我们将在下一节中多次使用这一观察结果。

如果 Φ 是秩为 $\ell \geqslant 2$ 的不可约根系，那么 $E(\Phi, R)$ 在 $G(\Phi, R)$ 中总是正规，甚至是特征性的（见 [103], [49]）。对于半局部环，容易证明

$$[G(\Phi, R), G(\Phi, R)] = E(\Phi, R).$$

除了 $\Phi = \mathsf{B}_2, \mathsf{G}_2$, $R = \mathbb{F}_2$ 的情形。

然而，在 $\ell = 1$ 的情形下，初等矩阵子群 $E_2(R) = E_{sc}(\mathsf{A}_1, R)$ 不一定是特殊线性群 $\mathsf{SL}_2(R) = G_{sc}(\mathsf{A}_1, R)$ 的正规子群（见 [28], [101], [100]）。

一般情况下， $G_\pi(\Phi, R)$ 与 $E_\pi(\Phi, R)$ 之间的差异由 K_1-函子衡量。

3. The Diophantine problem

3.1. 方程、常数和可计算结构。

回顾一下，代数结构 $\mathcal{A}$ 中的丢番图问题（记作 $\mathcal{D}(\mathcal{A})$）是确定给定的带有 $\mathcal{A}$ 中常数的有限方程组在 $\mathcal{A}$中是否有解的任务。若存在一种算法，对于给定的带有 $\mathcal{A}$ 中常数的有限 S 方程组，该算法能够判定 S 在 $\mathcal{A}$中是否有解，则$\mathcal{D}(\mathcal{A})$是可判定的。这里，假定结构 $\mathcal{A}$ 是可数的，并且进一步假定它配备了一个固定的枚举 $\mathcal{A} = \{a_1, a_2, \dots\}$，该枚举由一个满射 $\nu\colon \mathbb{N} \to \mathcal{A}$ 给出（该函数不必是单射）。可以利用该函数枚举在 $\mathcal{A}$ 中、含有可数多个变量 $x_1, x_2, \dots$ 的所有有限方程组，然后将它们作为丢番图问题 $\mathcal{D}(\mathcal{A})$的判定算法的输入。这里首先需要解决的问题是， $\mathcal{D}(\mathcal{A})$的可判定性在多大程度上取决于枚举$\nu : \mathbb{N} \to \mathcal{A}$的选择。事实证明， $\mathcal{D}(\mathcal{A})$的可判定性确实取决于枚举 ν，因此对于某些 ν， $\mathcal{D}(\mathcal{A})$可能是可判定的，而对于另一些则可能不是。例如，每个非平凡的有限群或可数群都有一个具有不可判定字问题的无限可数表示，因此，关于与这类无限表示相关的枚举的该群中的丢番图问题是不可判定的。然而，研究者通常只对“自然的”枚举 ν感兴趣，这些枚举来自 $\mathcal{A}$ 的元素的有限描述，并且反映了结构 $\mathcal{A}$的本质。例如，如果 $\mathcal{A}$ 是有限生成群，那么可以用固定有限生成元集合中的有限字来描述 $\mathcal{A}$ 的元素，并使用字的已知有效枚举；而如果 $\mathcal{A}$ 是例如环 R上的一般线性群 $\mathsf{GL}_n(R)$，那么$\mathsf{GL}_n(R)$的元素可以由来自 R的元素的 n^2-元组描述，因此可以使用 R的枚举来枚举 $\mathsf{GL}_n(R)$的元素。在这里以及其他所有地方，我们将字（或多项式，或有限签名中的任何其他公式）的有效枚举理解为给定有限或可数字母表中单词的一种枚举 $\mu : n \mapsto w_n$，使得对于任意数$n \in \mathbb{N}$，都可以计算出字 w_n，并且对于给定字母表中的任意字 w，都可以计算出一个数 n，使得 $w = w_n$。如果 $\mathcal{A}$ 是一个有限生成的结合含幺环 R，那么 $\mathcal{A}$ 的元素可以表示为有限多个变量中的带整数系数的非交换多项式（也可以将其视为有限秩的自由结合含幺环的元素），然后进行有效枚举。类似地，对于交换环 R，可以使用通常的交换多项式。有两种方式可以使丢番图问题的表述更加精确：一种是明确固定丢番图问题中 $\mathcal{A}$ 的枚举 ν（将其记作 $\mathcal{D}_\nu(\mathcal{A})$）；另一种是规定，当存在 $\mathcal{A}$ 的某个枚举ν 使得 $\mathcal{D}(\mathcal{A})$可判定时，称 $\mathcal{D}(\mathcal{A})$是可判定的。为了研究在丢番图问题的讨论中哪些枚举是“合理的”，我们需要转而考察可计算代数理论，或可计算模型论；该理论源于 Rabin [87] 和Maltsev [72] 的开创性工作（详情参见书籍 [41] 及较新的综述 [43]）。

回忆一下，有限签名的结构 $\mathcal{A}$ 关于枚举 $\nu\colon \mathbb{N} \to \mathcal{A}$ 是可计算的，是指其上的所有基本运算和谓词（包括等号） $\mathcal{A}$ 都是可计算的

关于枚举 ν。特别地，群 G 关于 ν 是可计算的，是指存在两个可计算函数 $f(x,y)$ 和 $h(x,y)$，使得对任意 $i,j\in\mathbb{N}$，以下关系成立： $\nu(i)\cdot\nu(h) = \nu(f(i,j))$，且 $\nu(i) = \nu(j) \iff h(i,j) = 1$。类似地，可数环 R 关于枚举 $\nu:\mathbb{N}\to R$ 是可计算的，是指除满足上述条件外，还存在一个可计算函数 $g(x,y)$，使得 $\nu(i)+\nu(j) = \nu(g(i,j))$。

以下观察揭示了丢番图问题的可判定性与可计算结构之间的联系。

引理 1. 设 $\mathcal{A}$ 是一个可数结构，并给定其枚举 $\nu:\mathbb{N}\to\mathcal{A}$。如果丢番图问题 $\mathcal{D}_\nu(\mathcal{A})$ 是可判定的，那么结构 $\mathcal{A}$ 关于 ν 是可计算的。

引理 1 表明，关于丢番图问题，$\mathcal{A}$ 的枚举中唯一值得关注的是那些使 $\mathcal{A}$ 可计算的枚举；它们称为 $\mathcal{A}$ 的构造化。给定的可数结构 $\mathcal{A}$ 是否具有构造化，是可计算模型论中的一个基本问题，因此在这方面已有许多结果（见 [41], [43], [42]），可供本文使用。

设 μ 和 ν 是 $\mathcal{A}$ 的两个枚举。根据定义，如果存在一个可计算函数 $f(x)$ 使得 $\mu = \nu\circ f$，则 μ 可归约到 ν（记作 $\preceq$）。此外，如果 $\mu\preceq\nu$ 且 $\nu\preceq\mu$，则称 μ 和 ν 等价（记作 $\sim$）。

引理 2（[41]）。设 $\mathcal{A}$ 是一个有限生成结构，且至少有一个构造化表示。那么 $\mathcal{A}$ 的所有构造化表示都彼此等价。

由此可知，有限生成结构 $\mathcal{A}$ 有构造化表示，当且仅当相对于某个（任意一个）有限生成集，$\mathcal{A}$ 中的字问题是可判定的。在这种情况下，任何其他构造化表示都等价于上述由任意给定的有限生成元集构造出的表示。因此，对于有限生成结构，通常不会明确提及枚举。

如果 $\mathcal{A}$ 是不可数的，那么正如我们在引言中提到的，只需考虑常数取自 $\mathcal{A}$ 的某个固定可数（或有限）子集 C 的方程，并且该子集配有一个枚举 $\nu:\mathbb{N}\to C$。这种形式的丢番图问题记作 $\mathcal{D}_C(\mathcal{A})$。我们不妨用 $\mathcal{A}$中由 C 生成的子结构 $\langle C\rangle$ 代替集合 C 来考察。在这种情况下，需要考虑与给定的 C枚举“相容”的 $\langle C\rangle$ 的枚举。为此，我们引入可计算模型论中的以下概念（见 [41]）。设 S 是一个带有枚举 $\nu:\mathbb{N}\to S$ 的集合，且 $\varphi:S\to S^*$ 是集合的一个嵌入。若存在可计算函数 $f:\mathbb{N}\to\mathbb{N}$使得 $\varphi\circ\nu = \nu^*\circ f$，则称枚举 $\nu^*:\mathbb{N}\to S^*$ 扩展了枚举 ν。容易构造出一个扩展给定生成集 C枚举的 $\langle C\rangle$的枚举（见 [41], 第 6 章第 1 节定理 1）。对于 $\mathcal{A}$ 的子集 C，除非另有说明，我们始终考虑扩展给定枚举 $\nu:\mathbb{N}\to C$的枚举 $\nu^*:\mathbb{N}\to\langle C\rangle$。此外，我们始终假设，对于给定的 $n\in\mathbb{N}$，可以计算出结构 $\mathcal{A}$ 的语言中一个带有来自 C 的常数的项 t，该项在结构 $\langle C\rangle$中表示元素 $\nu^*(n)$。反过来，对于 $\mathcal{A}$ 的语言中任意一个带有来自 C 的常数的项 t，都可以计算出一个数 $n\in\mathbb{N}$，使得 $\nu^*(n) = t$。我们称这类枚举 ν^* 为有效枚举。当 $\mathcal{A}$ 是群时，要构造 $\langle C\rangle$ 的有效枚举，只需有效枚举字母表 $C^{\pm1}$上的所有字；而当 $\mathcal{A}$ 是交换含幺环时，则需要枚举 $\mathbb{Z}[C]$中的所有多项式。

以下来自 [77] 的引理很有用。

引理 3. 设 $\mathcal{A}$ 是一个结构， C 是 $\mathcal{A}$ 的一个有限或可数子集，并配备一个枚举 ν，且 $\langle C\rangle$ 是 $\mathcal{A}$ 中由 C 生成的子结构，具有一个扩展 ν 的有效枚举。则以下结论成立：

1) 丢番图问题 $\mathcal{D}_C(\mathcal{A})$ 与 $\mathcal{D}_{\langle C\rangle}(\mathcal{A})$ 等价（可以相互归约）。

2) 如果 $\mathcal{D}_C(\mathcal{A})$ 是可判定的，那么对于 $\langle C\rangle$ 的任意一个扩展了生成集 C 的枚举 ν 的枚举， $\langle C\rangle$ 都是可计算的。

从现在起，我们始终不失一般性地假设，丢番图问题中的系数取自可数子结构 C ，而非集合 C。

3.2. 丢番图集与 e-可解释性。

要证明对于某些结构 $\mathcal{A}$ 和 $\mathcal{M}$ ， $\mathcal{D}(\mathcal{A})$ 可归约到 $\mathcal{D}(\mathcal{M})$，只需证明 $\mathcal{A}$ 在 $\mathcal{M}$ 中由方程可解释（或 e-可解释）。

e-可解释性的概念由 [45], [44], [46] 引入。这里我们重述这一概念，并陈述后文将用到的一些基本事实。

在下文中，我们经常使用非斜体粗体字母来表示元素元组：例如 $\mathbf{a} = (a_1, \ldots, a_n)$。此外，我们总是假设方程可以包含所考虑的代数结构中的常数。

定义 1. 如果存在一个有限方程组，即 $\Sigma_D(x_1, \ldots, x_m, y_1, \ldots, y_k)$，其语言为 $\mathcal{M}$ ，使得对于任意元组 $\mathbf{a} \in M^m$， $\mathbf{a} \in D$ 当且仅当方程组 $\Sigma_D(\mathbf{a}, \mathbf{y})$ 关于变量 $\mathbf{y}$ 在 $\mathcal{M}$ 中有解，那么称子集 $D \subset M^m$ 是丢番图的，或称其可由 $\mathcal{M}$ 中的方程组定义，或称其在 $\mathcal{M}$ 中是 e-可定义的。在这种情况下，称 Σ_D 在 $\mathcal{M}$ 中 e-定义了 D。

注释2。在上述记号中，若 $D \subset M^m$ 是 e-可定义的，则它可由 $\exists \mathbf{y} \Sigma_D(\mathbf{x}, \mathbf{y})$ 公式在 $\mathcal{M}$ 中定义。此类公式称为正原子公式，或 pp-公式。因此，e-可定义子集有时也称为 pp-可定义子集。另一方面，在数论中，这类集合通常被称为丢番图集合。然而，在代数几何中，它们可以描述为代数集的投影。

定义 2. 如果存在 $n \in \mathbb{N}$、一个子集 $D \subseteq M^n$ 以及一个满射（称为解释映射） $\varphi : D \to \mathcal{A}$，使得：则称代数结构 $\mathcal{A} = (A; f, \ldots, r, \ldots, c, \ldots)$ 在另一个代数结构 $\mathcal{M}$ 中 e-可解释：

1. D 在 $\mathcal{M}$ 中是 e-可定义的。

2. 对于 $\mathcal{A}$ 的语言中的每个函数 $f = f(x_1, \ldots, x_n)$，其图在 φ 下的原像，即集合

$$\{(x_1, \ldots, x_k, x_{k+1}) \mid \varphi(x_{k+1}) = f(x_1, \ldots, x_k)\},$$

在 $\mathcal{M}$ 中是 e-可定义的。

3. 对于 $\mathcal{A}$ 的语言中的每个关系 r ，以及 $\mathcal{A}$ 中的等号关系 $=$ ，其图在 φ 下的原像在 $\mathcal{M}$ 中是 e-可定义的。

设 $\mathcal{A}$ 按照上述定义在 $\mathcal{M}$ 中 e-可解释。这种解释完全由映射 φ 以及一个元组 Γ 决定；该元组由丢番图公式组成，这些公式分别定义了 1) 中的集合 D 、2) 中的函数 f 和 3) 中的关系 r 。我们用 $P_\Gamma \subseteq \mathcal{M}$ 表示公式 Γ 中出现的有限常数集（参数）。e- 可解释性是经典一阶可解释性概念的一种变体：作为解释公式的不是任意一阶公式，而是有限方程组。

以下是 e-可解释性的一个基本性质。直观地说，它表明，如果 $\mathcal{A}$可通过公式 Γ 和解释映射 φ: $D \to \mathcal{A}$在 $\mathcal{M}$ 中 e-可解释，那么任意一个方程组

在 $\mathcal{A}$中的方程都可以通过算法“编码”为 $\mathcal{M}$中的一个等价方程组。为作说明，我们需要引入以下记号。设 C 是 $\mathcal{A}$ 的一个有限或可数子集，并配有一个枚举 $\nu\colon \mathbb{N}\to C$。对于每个 $c_i=\nu(i)\in C$，固定一个任意的元组 $d_i\in\varphi^{-1}(c_i)$。用 D_R 表示 $\mathcal{M}$ 中所有作为元组 d_i 的分量出现的元素所组成的集合，其中这些元组取自 R。用 C_Γ 表示集合 $D_R\cup P_\Gamma$。如果存在一种算法，能够对每个 $i\in\mathbb{N}$ 计算元组 d_i各分量的 ν*编号，那么我们就称枚举 $\nu^*\colon \mathbb{N}\to C$ 与枚举 ν 相容（相对于代表元集合 R）。例如，可以先枚举 P_Γ 中的所有元素，然后对于 $i=1$、2、.....，按自然顺序枚举 d_1、d_2、.....中的所有分量。

引理 4（[45]）。设 $\mathcal{A}$ 可通过一组公式 Γ 和一个解释映射 $\varphi\colon D\to\mathcal{A}$在 $\mathcal{M}$ 中 e-可解释。设 C 是 $\mathcal{A}$ 的一个带有枚举 ν的有限或可数子集。那么存在一个多项式时间算法，对于 $\mathcal{A}$中每个系数取自 C 的有限方程组 S(x)，构造一个系数取自 C_Γ （通过相容枚举 $\nu^*\colon \mathbb{N}\to C_\Gamma$给出）的 $\mathcal{M}$ 中的有限方程组 S^*(y, z)，使得如果 (b, c) 是 $\mathcal{M}$中 S^*(y; z) 的一个解，那么 b $\in D$，且 φ(b) 是 $\mathcal{A}$中 S(x) 的一个解。此外， $\mathcal{A}$ 中 S(x) 的任意解 a 都能以这种方式得到，即对于某个 $\mathcal{M}$中 S^*(y, z) 的解 (b; c)，有 a $=\varphi$(b)。

现在我们展示引理 4 的两个关键推论。

推论 1. 设 $\mathcal{A}$ 可通过一组公式 Γ 和解释映射$\varphi : D\to\mathcal{A}$在 $\mathcal{M}$ 中 e-可解释。设 C 是 $\mathcal{A}$ 的一个有限或可数子集，并配备枚举 ν。那么，关于任意与 ν相容的枚举 ν^*，带有 C 中系数的 $\mathcal{A}$ 上的丢番图问题，可在多项式时间内（Karp 可归约）归约为带有 C_Γ 中系数的 $\mathcal{M}$ 上的丢番图问题。因此，如果 $\mathcal{D}_C(\mathcal{A})$ 是不可判定的，那么 $\mathcal{D}_{C_\Gamma}(\mathcal{M})$（相对于 ν^*）也不可判定。

推论 2. e-可解释性是一种传递关系，即如果 $\mathcal{A}_1$ 在 $\mathcal{A}_2$中 e-可解释，且$\mathcal{A}_2$ 在 $\mathcal{A}_3$中 e-可解释，那么 $\mathcal{A}_1$ 在 $\mathcal{A}_3$中 e-可解释。

4. Double centralizers of uniponent elements in Chevalley groups

在本文中，我们要证明，对于任意含幺交换环 R 上的切瓦莱群或其大子群 G，其中 $C=Z(G)$ 的子群 $C\cdot X_\alpha$ 是切瓦莱群中某个有限个初等幺幂元组成的集合的中心化子。此结果适用于所有根系，但 C_l 的短根除外；对于这种情况，结论会略有不同。

许多论文中都研究过非常相似的问题（见 [92], [20], [66]）。我们不能想当然地采用这些结果，因为就我们的目标而言，需要一个适用于任意交换环的双中心化子定理版本。为此，我们采用局部化方法，而该方法只需要与形如 $x_\alpha(1)$的元素进行共轭。

4.1. 环与模的局部化；环嵌入其局部化的乘积。

定义 3. 设 R 为交换环。如果子集 $S\subset R$ 满足 $1\in S$，且 S 在乘法下封闭，则称其在 R 中是乘法封闭的。

在有序对集合 $R \times S$ 上引入如下等价关系 $\sim$:

$$\frac{a}{s} \sim \frac{b}{t} \Longleftrightarrow \exists u \in S: \ (at - bs)u = 0.$$

我们用 $\frac{a}{s}$ 表示对 (a, s) 这一对的整个等价类，用 $S^{-1}R$ 表示所有等价类的集合。在集合 $S^{-1}R$ 上，我们可以引入环结构，即

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}, \quad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}.$$

定义 4. 环 $S^{-1}R$ 称为 R 关于 R 的分式环。

设 $\mathfrak{p}$ 是 R 的素理想。那么集合 $S = R \setminus \mathfrak{p}$ 是乘法封闭的（这与素理想的定义等价）。在这种情况下，我们将分式环 $S^{-1}R$ 记作 $R_{\mathfrak{p}}$。元素 $\frac{a}{s}$ 、 $a \in \mathfrak{p}$ 在 $R_{\mathfrak{p}}$ 中构成一个理想 $\mathfrak{M}$ 。若 $\frac{b}{t} \notin \mathfrak{M}$，则 $b \in S$，因此 $\frac{b}{t}$ 在 $R_{\mathfrak{p}}$ 中可逆。因此，理想 $\mathfrak{M}$ 由环 $R_{\mathfrak{p}}$ 的所有非可逆元组成，即 $\mathfrak{M}$ 是这个环的最大理想，所以 $R_{\mathfrak{p}}$ 是一个局部环。

从 R 到 $R_{\mathfrak{p}}$ 的过程称为在 $\mathfrak{p}$ 处的局部化。

命题 1. 每个含幺交换环 R 都可以自然地嵌入到其所有关于极大理想的局部化所成的笛卡尔积中

$$S = \prod_{\mathfrak{m} \text{ is a maximal ideal of } R} R_{\mathfrak{m}}$$

通过对角映射，将每个 $a \in R$ 映射到元素

$$\prod_{\mathfrak{m}} \left(\frac{a}{1}\right)_{\mathfrak{m}}$$

S的。

4.2. 域上切瓦莱群中幺幂元的双中心化子。

在下一节中，我们将不再特别说明地使用来自 [99]的切瓦莱群元素之间的关系。

定义 5. 对任意切瓦莱群 $G_\pi(\Phi, R)$ 以及任意 $\alpha \in \Phi$ le t

$$\Gamma_\alpha = \{x_\beta(1) \mid \beta \in \Phi \text{ and } [x_\beta(1), x_\alpha(1)] = e\}.$$

另请回忆，我们用 $C_G(M)$ 表示群 G 中集合 M 的中心化子。

本节的目标是证明以下定理，它可以看作双中心化子定理的一个变体：

定理 1（与 [92] 比较）。对于任意切瓦莱群（或其大子群） $G = G_\pi(\Phi, \mathbb{F})$，其中 $\mathbb{F}$ 是任意域， Φ 是秩为 > 1 的不可约根系，若某个元素$g \in C_G(\Gamma_\alpha)$，则 $g = cx_\alpha(t)$，其中 $t \in \mathbb{F}$， $c \in Z(G)$，但 $\Phi = \mathsf{C}_l$, $l \geqslant 2$ 且 α 为短的情形除外。

在 $\Phi = \mathsf{C}_l = \{\pm e_i \pm e_j \mid 1 \leqslant i, j \leqslant l, i \neq j\} \cup \{\pm 2e_i \mid 1 \leqslant i \leqslant l\}$ 且 $\alpha = e_1 + e_2$ 的情形下，若$g \in C_G(\Gamma_\alpha)$，则

$$g = cx_{e_1+e_2}(t_1)x_{2e_1}(t_2)x_{2e_2}(t_3), \quad c \in Z(G).$$

注3。注意，如果 $\Phi = \mathsf{C}_l$ 且 α 是任意一个短根，那么它总是可以通过 W中的某个元素共轭到 $e_1 + e_2$。因此，考虑根 $\alpha = e_1 + e_2$ 并不会失去任何一般性。

在本节中，我们将使用布鲁哈分解

$$G = BWB = \bigcup_{w \in W} BwB$$

以下列形式

命题 2（见 [99]）。任意元素 $g \in G$ 都可以唯一地表示为以下形式

$$g = tx_{\alpha_1}(a_1) \dots x_{\alpha_m}(a_m)\mathbf{w}x_{\alpha_1}(b_1) \dots x_{\alpha_m}(b_m), \ where\ t \in T, \mathbf{w} \in W,$$

$\alpha_1, \dots, \alpha_m$ 都是 Φ 的正根，按任意固定顺序排列；若 $\mathbf{w}(\alpha_i) \in \Phi^+$，则 $b_i = 0$。

由于在 W 的作用下，所有等长根都互为共轭，因此我们可以对根系 Φ 的单根进行编号，使得 $\alpha = \alpha_1$（第一个单根）以及所有单根 $\alpha_3, \dots, \alpha_l$ 都与 α_1 正交。

此外，我们假设 $\alpha_1, \dots, \alpha_m$ 的高度非递减，即从单根 $\alpha_1, \alpha_2, \dots, \alpha_l$ 开始，然后是它们的和，依此类推。

在这种情况下，根 α_3、.....、 α_l 与 α_1 正交，因此

$$\forall i = 3, \dots, l \ [x_{\pm\alpha_i}(1), x_{\alpha_1}(1)] = 1 \Longrightarrow x_{\pm\alpha_i}(1) \in \Gamma_\alpha.$$

我们还知道，对于 Φ 的最高根 γ

$$\gamma + \alpha_1 \notin \Phi \Longrightarrow x_\gamma(1) \in \Gamma_\alpha.$$

此外，

$$x_{\alpha_1}(1), x_{-\alpha_2}(1) \in \Gamma_\alpha.$$

假设我们有布鲁哈分解中的某个 g

$$g = tx_{\alpha_1}(a_1) \dots x_{\alpha_m}(a_m)\mathbf{w}x_{\alpha_1}(b_1) \dots x_{\alpha_m}(b_m) \in C_G(\Gamma_\alpha).$$

我们的首要且最重要的目标是证明 $\mathbf{w} = \mathbf{e}_W$。

引理 5。给定最高根 $\gamma \in \Phi$，$\mathbf{w}(\gamma) = \gamma$.

证明。首先，列出元素 $x_\beta(1)$ 对不同元素作用的共轭公式是有用的。

对于 $t \in T$，有

$$t^{x_\beta(1)} = tt^{-1}x_\beta(1)tx_\beta(-1) = tx_\beta(c_t^\beta)x_\beta(-1) = tx_\beta(c_t^\beta - 1), \quad c_t^\beta \in \mathbb{F}^*.$$

对于 $\mathbf{w} \in W$，有

$$\mathbf{w}^{x_\beta(1)} = x_\beta(1)\mathbf{w}x_\beta(-1)\mathbf{w}^{-1}\mathbf{w} = x_\beta(1)x_{\mathbf{w}(\beta)}(-1)\mathbf{w}.$$

对于最高根 γ 的情形，我们知道，对于所有 $i = 1, \dots, m$， $[x_{\alpha_i}(1)\ x_\gamma(1)] = 1$，因此

$$\begin{aligned} g^{x_\gamma(1)} = tx_\gamma(c_t^\gamma - 1)x_{\alpha_1}(a_1) \dots x_{\alpha_m}(a_m)x_\gamma(1)x_{\mathbf{w}(\gamma)}(-1)\mathbf{w}x_{\alpha_1}(b_1) \dots x_{\alpha_m}(b_m) = \\ = tx_{\alpha_1}(a_1) \dots x_{\alpha_m}(a_m)x_\gamma(c_t^\gamma)x_{\mathbf{w}(\gamma)}(-1)\mathbf{w}x_{\alpha_1}(b_1) \dots x_{\alpha_m}(b_m) = \\ = g = tx_{\alpha_1}(a_1) \dots x_{\alpha_m}(a_m)\mathbf{w}x_{\alpha_1}(b_1) \dots x_{\alpha_m}(b_m). \end{aligned}$$

利用布鲁哈分解的唯一性并比较等号两边的部分，我们得到：(1) $\mathbf{w}(\gamma) = \gamma$，这正是所需的；

(2) $c_t^\gamma = 1$，即 t 与 $x_\gamma(1)$ 可交换。 ■

回顾一下，单根集合 Δ 由 α_1、.....、 α_l 组成。我们假设根 α_3、.....、 α_l 与 α_1 正交。

引理 6. 对于任意根 $\beta \in \{\alpha_1, \alpha_3, \dots, \alpha_l\}$，我们有 $\mathrm{w}(\beta) \in \Phi^+$。

证明。假设 $\beta \in \{\alpha_1, \alpha_3, \dots, \alpha_l\}$, $\beta = \alpha_i$，显然在这种情况下 $x_\beta(1) \in \Gamma_\alpha$。假设 $\mathrm{w}(\beta) = \delta \in \Phi^-$。那么，利用 (R3) 关系，

$$\begin{aligned} tx_{\alpha_1}(a_1)\dots x_{\alpha_m}(a_m)\mathbf{w}x_{\alpha_1}(b_1)\dots x_{\alpha_m}(b_m) = g = \\ = g^{x_\beta(1)} = tx_\beta(c_t^\beta - 1)x_{\alpha_1}(a_1)\dots x_{\alpha_l}(a_l)x_{\alpha_{l+1}}(\widetilde{a}_{l+1})\dots x_{\alpha_m}(\widetilde{a}_m)x_\beta(1)\mathbf{w}\cdot \\ \cdot x_\beta(-1)x_{\alpha_1}(b_1)\dots x_{\alpha_l}(b_l)x_{\alpha_{l+1}}(\widetilde{b}_{l+1})\dots x_{\alpha_m}(\widetilde{b}_m) = \\ = t\widetilde{u}\mathbf{w}x_{\alpha_1}(b_1)\dots x_{\alpha_i}(b_i - 1)\dots x_{\alpha_l}(b_l)x_{\alpha_{l+1}}(\widetilde{b}'_{l+1})\dots x_{\alpha_m}(\widetilde{b}'_m). \end{aligned}$$

要将这个表达式化为标准布鲁哈分解的通常形式，我们还需要把所有对应于符号不变的根的幺正元移到 w 的左侧。但这样做时，$x_\beta(\cdot)$ 中的参数在 w 的作用下并不改变。因此，同一个元素有两种不同的布鲁哈分解。区别在于 w 右侧的幺正元 $x_\beta(\cdot)$ 的参数。矛盾，因此 $\mathrm{w}(\beta) \in \Phi^+$。 ■

引理 7. 对任意根 $\beta \in \{\alpha_3, \dots, \alpha_l\}$，有 $\mathrm{w}(\beta) = \beta$。

证明。若 $\beta \in \{\alpha_3, \dots, \alpha_l\}$，则 $x_\beta(1)\, x_{-\beta}(1) \in \Gamma_\alpha$，因此 $w_\beta(1)$ 与 g 可交换。此外还要指出，在 g 的布鲁哈分解中，w 右边省略了元素 $x_\beta(\cdot)$，因为 $\mathrm{w}(\beta) \in \Phi^+$（根据前一个引理）。

由于 β 是单根，w^β 将所有正根（β 除外）也映射为正根。因此，

$$\begin{aligned} tx_{\alpha_1}(a_1)\dots x_\beta(a_\beta)\dots x_{\alpha_m}(a_m)\mathbf{w}x_{\alpha_1}(b_1)\dots x_{\alpha_m}(b_m) = g = g^{w_\beta(1)} = \\ = \widetilde{t}x_{\mathbf{w}_\beta(\alpha_1)}(a_1)\dots x_{\mathbf{w}_\beta(\beta)}(a_\beta)\dots x_{\mathbf{w}_\beta(\alpha_m)}(a_m)\mathbf{w}^{w_\beta(1)}x_{\mathbf{w}_\beta(\alpha_1)}(b_1)\dots x_{\mathbf{w}_\beta(\alpha_m)}(b_m) = \\ = \widetilde{t}x_{\alpha_1}(\widetilde{a}_1)\dots x_{-\beta}(a_\beta)\dots x_{\alpha_m}(\widetilde{a}_m)\mathbf{w}^{w_\beta(1)}x_{\mathbf{w}_\beta(\alpha_1)}(b_1)\dots x_{\mathbf{w}_\beta(\alpha_m)}(b_m) = \end{aligned}$$

（因为对任意 $\delta \in \Phi^+$ $[x_\delta(a)\ x_{-\beta}(a_\beta)]$，其中都不含负根对应的任何幺正元）

$$\begin{aligned} = \widetilde{t}x_{\alpha_1}(\widetilde{a}_1)\dots x_{\alpha_m}(\widetilde{a}_m)x_{-\beta}(a_\beta)\mathbf{w}^{w_\beta(1)}x_{\mathbf{w}_\beta(\alpha_1)}(b_1)\dots x_{\mathbf{w}_\beta(\alpha_m)}(b_m) = \\ = \widetilde{t}x_{\alpha_1}(\widetilde{a}_1)\dots x_{\alpha_m}(\widetilde{a}_m)w_\beta(1)x_\beta(a_\beta)\mathbf{w}w_\beta(1)^{-1}x_{\mathbf{w}_\beta(\alpha_1)}(b_1)\dots x_{\mathbf{w}_\beta(\alpha_m)}(b_m) = \\ = \widetilde{t}x_{\alpha_1}(\widetilde{a}_1)\dots x_{\alpha_m}(\widetilde{a}_m)w_\beta(1)\mathbf{w}x_{\mathbf{w}(\beta)}(a_\beta)w_\beta(1)^{-1}x_{\mathbf{w}_\beta(\alpha_1)}(b_1)\dots x_{\mathbf{w}_\beta(\alpha_m)}(b_m) = \\ = \widetilde{t}x_{\alpha_1}(\widetilde{a}_1)\dots x_{\alpha_m}(\widetilde{a}_m)\mathbf{w}^{w_\beta(1)}x_{\mathbf{w}_\beta\mathbf{w}(\beta)}(a_\beta)x_{\mathbf{w}_\beta(\alpha_1)}(b_1)\dots x_{\mathbf{w}_\beta(\alpha_m)}(b_m). \end{aligned}$$

由于 $\mathrm{w}(\beta) \in \Phi^+$，且 β 是单根，因此要么 $\mathrm{w}^\beta(\mathrm{w}(\beta)) \in \Phi^+$，要么 $\mathrm{w}(\beta) = \beta$（在后一种情况下，我们的引理已经得证）。在第一种情况下，w 右边的所有幺正元都对应正根。因此，根据布鲁哈分解的唯一性可得

$$\mathbf{w} = \mathbf{w}^{w_\beta(1)} \Longrightarrow \mathbf{w}(\beta) = \pm\beta.$$

由于 $\mathrm{w}(\beta) \in \Phi^+$ $\mathrm{w}(\beta) = \beta$，这正是所需的。 ■

引理 8. 假设 g 在布鲁哈分解中

$$g = tx_{\alpha_1}(a_1)\dots x_{\alpha_m}(a_m)\mathbf{w}x_{\alpha_1}(b_1)\dots x_{\alpha_1}(b_m) \in C(\Gamma_\alpha),$$

其中， α 对所有方程组而言都是单根，除了C_l, $l \geqslant 2$ ； 而对于方程组C_l, $l \geqslant 2$, 它是长单根。如果 $\Phi = \mathsf{C}_l$, α 是短的，那么我们假设

$$\alpha_1 = e_1 - e_2, \alpha_2 = e_2 - e_3, \ldots, \alpha_{l-1} = e_{l-1} - e_l, e_l = 2e_l \ and \ \alpha = e_1 + e_2.$$

在所有这些情形中，$\mathsf{w} = \mathsf{e}_W$。

证明。注意，根 α_3、.....、α_l、 γ 线性无关，并在根系 Φ 的空间 V 中生成一个超平面 V'。根 α_1 与向量 $\{\alpha_3, \ldots, \alpha_l\}$ 正交。

由于根据引理 5 和 7，我们的 w 在超平面 V' 的基上作用为恒等映射，因此它要么是恒等映射，要么是反射 w_δ，其中 δ 是与所有 α_3、.....、 α_l 正交的根 γ。

让我们在不同的根系中寻找这样的 δ 。

1. 根系 A_l。在 $\mathbb{R}^{l+1}$、 $\alpha_i = e_i - e_{i+1}$、 $3 \leqslant i \leqslant l$、 $\gamma = e_1 - e_{l+1}$ 中。由于 A_l 的所有根都具有 $e_j - e_k$ 的形式，所需的 δ 不存在，因此 $\mathsf{w} = \mathsf{e}_W$。

2. 根系 B_l, $l \geqslant 3$。根系为 $\{\pm e_i, \pm e_i \pm e_j \mid 1 \leqslant i < j \leqslant l\}$,$\{\alpha_3, \ldots, \alpha_l\} = \{e_3 - e_4, \ldots, e_{l-1} - e_l, e_l\}$ 或 $\{e_1 - e_2, \ldots e_{l-2} - e_{l-1}\}$，具体取决于 α 的长度。最高根 γ 为 $e_1 + e_2$。第一种情况下 $\delta = e_1 - e_2 = \alpha$，第二种情况下$\delta = e_l = \alpha$。这两种情况都不可能，因为我们知道 $\mathsf{w}(\alpha) \in \Phi^+$。

3. 根系 C_l, $l \geqslant 2$。根系为 $\{\pm 2e_i, \pm e_i \pm e_j \mid 1 \leqslant i < j \leqslant l\}$, $\{\alpha_3, \ldots, \alpha_l\} = \{e_3 - e_4, \ldots, e_{l-1} - e_l, 2e_l\}$ 或 $\{e_1 - e_2, \ldots e_{l-2} - e_{l-1}\}$，同样取决于 α 的长度。最高根 γ 为 $2e_1$。第一种情况下 $\delta = 2e_2$，第二种情况下 $\delta = 2e_l = \alpha_1$，这是不可能的，因为 $\mathsf{w}(\alpha_1) \in \Phi^+$。

现在假设我们有相同的简单根／正根集，但 $\alpha = e_1 + e_2$。在这种情况下也有 $\delta = 2e_2$,

$$g = tx_{\alpha_1}(a_1) \ldots x_{\alpha_m}(a_m)\mathbf{w}_\delta x_{e_2-e_3}(b_{e_2-e_3}) \ldots x_{e_2-e_l}(b_{e_2-e_l})x_{e_2+e_3}(b_{e_2+e_3}) \ldots x_{e_2+e_l}(b_{e_2+e_l})x_{2e_2}(b_{2e_2}),$$

因为在 w_δ 的作用下，只有正根 $e_2 - e_i$、 $e_2 + e_i$ 和 $2e_2$ 会映射为负根。但对所有这些根而言，它们与 $\alpha = e_1 + e_2$ 的和都不是根，因此 $x_\alpha(1)$ 与这一右侧部分可交换。因此,

$$\begin{aligned} g = g^{x_\alpha(1)} &= (tx_\alpha(c_t^\alpha - 1))x_{\alpha_1}(a_1) \ldots x_{\alpha_i}(a_i') \ldots x_{\alpha_m}(a_m')x_{e_1+e_2}(1)\mathbf{w}_{2e_2}x_{e_1+e_2}(1)^{-1} \cdot \\ &\cdot x_{e_2-e_3}(b_{e_2-e_3}) \ldots x_{e_2-e_l}(b_{e_2-e_l})x_{e_2+e_3}(b_{e_2+e_3}) \ldots x_{e_2+e_l}(b_{e_2+e_l})x_{2e_2}(b_{2e_2}) = \\ &= (tx_\alpha(c_t^\alpha - 1))x_{\alpha_1}(a_1) \ldots x_{\alpha_i}(a_i') \ldots x_{\alpha_m}(a_m')x_{e_1+e_2}(1)x_{e_1-e_2}(\pm 1)\mathbf{w}_{2e_2} \cdot \\ &\cdot x_{e_2-e_3}(b_{e_2-e_3}) \ldots x_{e_2-e_l}(b_{e_2-e_l})x_{e_2+e_3}(b_{e_2+e_3}) \ldots x_{e_2+e_l}(b_{e_2+e_l})x_{2e_2}(b_{2e_2}) = \\ &= tx_{\alpha_1}(a_1) \ldots x_{e_1-e_2}(a_{e_1-e_2} \pm 1) \ldots x_{e_1+e_2}(c_t + a_{e_1+e_2}) \ldots x_{\alpha_i}(a_i'') \ldots x_{\alpha_m}(a_m'')\mathbf{w}_{2e_2} \cdot \\ &\cdot x_{e_2-e_3}(b_{e_2-e_3}) \ldots x_{e_2-e_l}(b_{e_2-e_l})x_{e_2+e_3}(b_{e_2+e_3}) \ldots x_{e_2+e_l}(b_{e_2+e_l})x_{2e_2}(b_{2e_2}), \end{aligned}$$

因为 $\mathsf{w}_{2e_2}(e_1 + e_2) = e_1 - e_2$，且新的 $x_{e_1-e_2}(\ldots)$ 或 $x_{e_1+e_2}(\ldots)$ 不可能由其他任何共轭产生。因此这种情况不可能发生，且 $\mathsf{w} = \mathsf{e}_W$。

4. 根系 D_l, $l \geqslant 4$。根系为 $\{\pm e_i \pm e_j \mid 1 \leqslant i < j \leqslant l\}$,$\{\alpha_3, \ldots, \alpha_l\} = \{e_3 - e_4, \ldots, e_{l-1} - e_l, e_{l-1} + e_l\}$, $\gamma = e_1 + e_{l+1}$。由于 D_l 的所有根都具有 $\pm e_j \pm e_k$ 的形式，所需的 δ 不存在，因此 $\mathsf{w} = \mathsf{e}_W$。

5. 根系 E_l, $l = 6$、7、8。这里不列出所有根的清单，而是引自 [13]。经明确检验可知，在所有三种情形下 $\delta = \alpha_1$，这是不可能的，因为 $\mathsf{w}(\alpha_1) \in \Phi^+$。

6. 根系 F_4。系统 F_4 的根为

$$\pm e_i, i=1,2,3,4, \quad \pm e_i \pm e_j, i,j=1,2,3,4, i\neq j, \quad \frac{1}{2}(\pm e_1 \pm e_2 \pm e_3 \pm e_4);$$

我们假设 $\Delta = \{\frac{1}{2}(e_1-e_2-e_3-e_4)\ e_4, e_3-e_4, e_2-e_3.\}$ 因此 $\{\alpha_3,\alpha_4\} = \{e_3-e_4, e_2-e_3\}$ 或 $\{\frac{1}{2}(e_1-e_2-e_3-e_4)\ e_4\}$, $\gamma = e_1+e_2$。在第一种情况下，$\delta = \frac{1}{2}(e_1-e_2-e_3-e_4) = \alpha_1$；在第二种情况下，这样的 δ 不存在。第一种情况也不可能，因为我们知道 $\mathsf{w}(\alpha)\in\Phi^+$。

7. 根系 G_2。如果 α 是 G_2 的长单根，β 是短单根，那么无论如何，δ 都与最高根 $2\alpha+3\beta$ 正交，即 $\delta=\beta$。显然，如果我们最初的 α_1 是 β，这是不可能的，因此我们假设 $\alpha_1=\alpha$。

假设 $\mathsf{w} = \mathsf{w}\beta$,

$$g = tx_\alpha(a_1)x_\beta(a_2)x_{\alpha+\beta}(a_3)x_{\alpha+2\beta}(a_4)x_{\alpha+3\beta}(a_5)x_{2\alpha+3\beta}(a_6)\mathbf{w}_\beta x_\beta(b_2).$$

由于 $x_{\alpha+2\beta}(1)\in\Gamma_\alpha$，我们可以用 $x_{\alpha+2\beta}(1)$ 共轭 g：

$$\begin{aligned}
g^{x_{\alpha+2\beta}(1)} &= (tx_{\alpha+2\beta}(c_t^{\alpha+2\beta}-1))x_\alpha(a_1)(x_\beta(a_2)x_{\alpha+3\beta}(\pm 2a_2))(x_{\alpha+\beta}(a_3)x_{2\alpha+3\beta}(\pm 2a_3))\cdot\\
&\quad\cdot x_{\alpha+2\beta}(a_4)x_{\alpha+3\beta}(a_5)\cdot x_{2\alpha+3\beta}(a_6)x_{\alpha+2\beta}(1)\mathbf{w}_\beta x_{\alpha+2\beta}(1)^{-1}x_\beta(b_2) =\\
&= (tx_{\alpha+2\beta}(c_t^{\alpha+2\beta}-1))x_\alpha(a_1)(x_\beta(a_2)x_{\alpha+3\beta}(\pm 2a_2))(x_{\alpha+\beta}(a_3)x_{2\alpha+3\beta}(\pm 2a_3))\cdot\\
&\quad\cdot x_{\alpha+2\beta}(a_4)x_{\alpha+3\beta}(a_5)\cdot x_{2\alpha+3\beta}(a_6)x_{\alpha+2\beta}(1)x_{\alpha+\beta}(\pm 1)\mathbf{w}_\beta x_\beta(b_2) =\\
&\quad = tx_\alpha(a_1)x_\beta(a_2)x_{\alpha+\beta}(a_3\pm 1)x_{\alpha+2\beta}(\dots)x_{\alpha+3\beta}(\dots)x_{2\alpha+3\beta}(\dots)\mathbf{w}_\beta x_\beta(b_2),
\end{aligned}$$

这不可能，因为 $a_3\neq a_3\pm 1$。因此 $\mathsf{w} = \mathsf{e}_W$。 ■

因此，可以假设，如果 $g\in C_G(\Gamma_\alpha)$，那么 g具有形式 $tx_{\alpha_1}(a_1)\dots x_{\alpha_m}(a_m)$，即 $g\in B$。

剩下要证明的是，任意 $g\in B\cap C_G(\Gamma_\alpha)$ 都具有定理 2 中指定的形式。
我们将依次检查所有根系来证明这一事实。

注 4. 以下所有计算对于任意含幺交换环仍然成立。

引理 9. 若 $\Phi=\mathsf{G}_2$ 且

$$g = tx_{\alpha_1}(a_1)\dots x_{\alpha_m}(a_m)\in C(\Gamma_\alpha),$$

则 $a_2=\dots=a_m=0$ 和 $t\in Z(G)$。

证明. 若 α 和 β 是系统 G_2的单根，α 为长根，β 为短根，则（见 [99],引理 57）：

$$\begin{aligned}
[x_\alpha(t),x_\beta(u)] &= x_{\alpha+\beta}(tu)x_{\alpha+3\beta}(-tu^3)x_{\alpha+2\beta}(-tu^2)x_{2\alpha+3\beta}(t^2u^3),\\
[x_{\alpha+\beta}(t),x_\beta(u)] &= x_{\alpha+2\beta}(2tu)x_{\alpha+3\beta}(-3tu^2)x_{2\alpha+3\beta}(3t^2u^3),\\
[x_\alpha(t),x_{\alpha+3\beta}(u)] &= x_{2\alpha+3\beta}(tu),\\
[x_{\alpha+2\beta}(t),x_\beta(u)] &= x_{\alpha+3\beta}(-3tu),\\
[x_{\alpha+\beta}(t),x_{\alpha+2\beta}(u)] &= x_{2\alpha+3\beta}(3tu).
\end{aligned}$$

情形 1，$\alpha_1=\alpha$ 是长根。于是

$$x_\alpha(1),x_{\alpha+\beta}(1),x_{\alpha+2\beta}(1),x_{2\alpha+3\beta}(1),x_{-\beta}(1),x_{-\alpha-2\beta}(1),x_{-\alpha-3\beta}(1)\in\Gamma_\alpha.$$

If

$$g = tx_\alpha(t_1)x_\beta(t_2)x_{\alpha+\beta}(t_3)x_{\alpha+2\beta}(t_4)x_{\alpha+3\beta}(t_5)x_{2\alpha+3\beta}(t_6) \in C(\Gamma_\alpha),$$

then

$$g^{x_\alpha(1)} = (tx_\alpha(c_t^\alpha - 1))x_\alpha(t_1)(x_\beta(t_2)x_{\alpha+\beta}(t_2)x_{\alpha+3\beta}(-t_2^3)x_{\alpha+2\beta}(-t_2^2)x_{2\alpha+3\beta}(t_2^3))\cdot$$
$$\cdot\, x_{\alpha+\beta}(t_3)x_{\alpha+2\beta}(t_4)(x_{\alpha+3\beta}(t_5)x_{2\alpha+3\beta}(t_5))x_{2\alpha+3\beta}(t_6) =$$
$$= tx_\alpha(c_t^\alpha - 1 + t_1)x_\beta(t_2)x_{\alpha+\beta}(t_2+t_3)x_{\alpha+2\beta}(t_4 - t_2^2)x_{\alpha+3\beta}(t_5 - t_2^3)x_{2\alpha+3\beta}(t_6 + t_5 + t_2^3 - 3t_2^2t_3).$$

根据布鲁哈分解的唯一性，我们有

$$c_t^\alpha = 1, \quad t_2 = 0, \quad t_5 = 0,$$

因此

$$[t, x_\alpha(1)] = 1 \text{ and } g = tx_\alpha(t_1)x_{\alpha+\beta}(t_3)x_{\alpha+2\beta}(t_4)x_{2\alpha+3\beta}(t_6).$$

由于 $x_{\alpha+\beta}(1) \in \Gamma_\alpha$，我们有（类似地） $[t, x_{\alpha+\beta}(1)] = 1$和 $3t_4 = 0$，因此根据注 1， $t \in Z(G)$。

现在让我们使用 $x_{-\beta}(1)$，注意到 $[t, x_\beta(1)] = 1$和 $3t_4 = 0$:

$$g^{x_{-\beta}(1)} = tx_\alpha(t_1)(x_\alpha(3t_3)x_{\alpha+\beta}(t_3))(x_{\alpha+\beta}(2t_4)x_\alpha(-3t_4)x_{-\beta}(3t_4^2)x_{\alpha+2\beta}(t_4))x_{2\alpha+3\beta}(t_6) =$$
$$= tx_\alpha(t+3t_3)x_{\alpha+\beta}(t_3+2t_4)x_{\alpha+2\beta}(t_4)x_{2\alpha+3\beta}(t_6),$$

所以 $2t_4 = 0$ 与 $3t_4 = 0$ 一起给出 $t_4 = 0$，因此

$$g = tx_\alpha(t_1)x_{\alpha+\beta}(t_3)x_{2\alpha+3\beta}(t_6), \quad 3t_3 = 0, t \in Z(G).$$

现在让我们应用 $x_{-\alpha-2\beta}(1)$:

$$g^{x_{-\alpha-2\beta}(1)} =$$
$$= tx_\alpha(t_1)(x_{-\beta}(\pm 2t_3)x_\alpha(\pm 3t_3^2)x_{-\alpha-3\beta}(\pm 3t_3)x_{\alpha+\beta}(t_3))(x_{-\alpha-2\beta}(1)x_{2\alpha+3\beta}(t_6)x_{-\alpha-2\beta}(1)^{-1}) =$$
$$= tx_\alpha(t_1)x_{-\beta}(\pm 2t_3)x_{\alpha+\beta}(t_3)x_{\alpha+\beta}(t_6)x_{-\beta}(-t_6)x_{-\alpha-3\beta}(t_6)x_\alpha(t_6^2)x_{2\alpha+3\beta}(t_6),$$

因此 $t_6 = 0$，然后 $2t_3 = 0$ ，并且与 $3t_3 = 0$ 一起可推出 $t_3 = \qquad 0.$

因此我们证明了 $g = tx_\alpha(t_1)$，其中 $t \in Z(G)$。

情形 2， $\alpha_1 = \beta$ 是一个短根。于是

$$x_\beta(1), x_{\alpha+3\beta}(1), x_{2\alpha+3\beta}(1), x_{-\alpha}(1), x_{-2\alpha-3\beta}(1) \in \Gamma_\beta.$$

If

$$g = tx_\beta(t_2)x_\alpha(t_1)x_{\alpha+\beta}(t_3)x_{\alpha+2\beta}(t_4)x_{\alpha+3\beta}(t_5)x_{2\alpha+3\beta}(t_6) \in C(\Gamma_\beta),$$

then

$$g^{x_{\alpha+3\beta}(1)} = (tx_{\alpha+3\beta}(c_t^{\alpha+3\beta} - 1))x_\beta(t_2)x_\alpha(t_1)x_{2\alpha+3\beta}(t_1)x_{\alpha+\beta}(t_3)x_{\alpha+2\beta}(t_4)x_{\alpha+3\beta}(t_5)x_{2\alpha+3\beta}(t_6),$$

因此 $[t, x_{\alpha+3\beta}(1)] = 1$并且 $t_1 = 0$。

Now

$$g^{x_\beta(1)} = (tx_\beta(c_t^\beta - 1))\cdot$$
$$\cdot x_\beta(t_2)(x_{\alpha+\beta}(t_3)x_{\alpha+2\beta}(2t_3)x_{\alpha+3\beta}(-3t_3)x_{2\alpha+3\beta}(3t_3^2))(x_{\alpha+2\beta}(t_4)x_{\alpha+3\beta}(-3t_4))x_{\alpha+3\beta}(t_5)x_{2\alpha+3\beta}(t_6) =$$
$$= tx_\beta(c_t^\beta - 1 + t_2)x_{\alpha+\beta}(t_3)x_{\alpha+2\beta}(2t_3+t_4)x_{\alpha+3\beta}(-2t_3-3t_4+t_5)x_{2\alpha+3\beta}(3t_3^2+t_6),$$

所以 $[t, x_\beta(1)] = 1$ (并由注记 1 $t \in Z(G)$ 得出), $2t_3 = 3t_3^2 = 0$ (因此 $t_3^2 = 0$) 并且 $3t_4 = 0$。

考虑到 $t_3^2 = 0$, 应用 $x_{-\alpha}(1)$:

$$g^{x_{-\alpha}(1)} = tx_\beta(t_2)(x_{\alpha+\beta}(t_3)x_\beta(\pm t_3))x_{\alpha+2\beta}(t_4)x_{\alpha+3\beta}(t_5)x_{2\alpha+3\beta}(t_6)x_{\alpha+3\beta}(\pm t_6),$$

因此 $t_3 = t_6 = 0$。

由于 $x_{2\alpha+3\beta}(1)$和 $x_{-2\alpha-3\beta}(1)$都属于 Γ_β, 所以 $[w_{2\alpha+3\beta}(1)\ g] = 1$; 又由于$w_{2\alpha+3\beta}(\alpha+2\beta) = -\alpha-\beta$, $w_{2\alpha+3\beta}(\alpha+3\beta) = -\alpha$, 因此 $t_4 = t_5 = 0$, 这正是所需的。 ■

引理10. 若 $\Phi = A_l$, D_l 或初等子群, $l \geqslant 2$,

$$g = tx_{\alpha_1}(a_1)\dots x_{\alpha_m}(a_m) \in C(\Gamma_\alpha),$$

则 $a_2 = \dots = a_m = 0$ 且 $t \in Z(G)$。

证明. 在这个单键情形中, 所有根的长度都相同, 并且在魏尔群的作用下彼此共轭, 因此我们总可以假设 $\alpha = \alpha_1$。

如果 $\beta \neq \alpha$ 是某个正根, 那么它要么与 α 正交, 要么 α 和 β 是 A_2 的单根（如果它们之间的夹角为 $120°$）, 要么 α 和 $\gamma = \beta - \alpha$ 是 A_2 的单根（如果它们之间的夹角为 $60°$）。

在第二种和第三种情况下, 我们有根 α、β、$\alpha+\beta$, 它们构成系统 A_2, , 其中$x_\alpha(1)$ $x_{\alpha+\beta}(1)$ 和 $x_{-\beta}(1)$ 属于 Γ_α。

If

$$g = tx_\alpha(t_1)\dots x_\beta(t_\beta)\dots x_{\alpha+\beta}(t_{\alpha+\beta})\dots,$$

then

$$g^{x_\alpha(1)} = tx_\alpha(c_t^\alpha - 1 + t_1)\dots x_\beta(t_\beta)x_{\alpha+\beta}(t_\beta)\dots x_{\alpha+\beta}(t_{\alpha+\beta})\dots,$$

其中 $x_\alpha(\dots)$ $x_\beta(\dots)$ $x_{\alpha+\beta}(\dots)$ 不会出现在其他任何地方。因此 $[t, x_\alpha(1)] = 1$ 和 $t_\beta = 0$。

Now

$$g = tx_\alpha(t_1)\dots x_{\alpha+\beta}(t_{\alpha+\beta})\dots$$

and

$$g^{x_{-\beta}(1)} = (tx_{-\beta}(c_t^{-\beta} - 1))x_\alpha(t_1)\dots x_\alpha(t_{\alpha+\beta})x_{\alpha+\beta}(t_{\alpha+\beta})\dots,$$

其中, 对于所有其他 $x_\gamma(\dots)$（$x_{-\beta}(c_t^{-\beta} - 1)$ 除外）, $x_\alpha(\dots)$ $x_{-\beta}(\dots)$ $x_{\alpha+\beta}(\dots)$ 不会出现在其他任何地方, γ 均为正。因此 $[t, x_{-\beta}(1)] = 1$ 和 $t_{\alpha+\beta} = 0$。

现在我们看到, 如果 $\gamma \neq \alpha$ 中出现了形如 $x_\gamma(\dots)$ 的 g元素, 那么 γ 与 α 正交。但在这种情况下, $x_\gamma(1)$ $x_{-\gamma}(1) \in \Gamma_\alpha$, 因此 $[w_\gamma(1)\ g] = e$。从单根 γ 出发, 我们看到

$$g^{w_\gamma(1)} = \widetilde{t}x_\alpha(t_1)x_{-\gamma}(t_\gamma)\dots x_{\mathbf{w}_\gamma(\delta)}(t_\delta)\dots,$$

其中所有 $w_\gamma(\delta) \in \Phi^+$。因此 $[t, x_\gamma(1)] = 1$, $t_\gamma = 0$。 t 元素与所有简单根 γ 对应的 $x_\gamma(1)$ 都可交换, 因此由注 1 可得 $t \in Z(G)$。

我们还证明了, 在 g 中, 除了 $x_\alpha(t_1)$ 之外, 不存在单根为 γ 且形如 $x_\gamma(t_\gamma)$ 的元素。接下来处理高度为 2 的根, 采用相同的方法, 并注意到它们也都满足 $t_\gamma = 0$。继续对高度为 3、4、..... 的根应用这一过程, 最终得到对所有 $\gamma \in \Phi^+\backslash\alpha$, 都有 $t_\gamma = 0$, 这正是所需的结论。 ■

引理 11. 对于根系 $B_2 = \{\alpha, \beta, \alpha+\beta, \alpha+2\beta\}$和 $g = tx_\alpha(t_1)x_\beta(t_2)x_{\alpha+\beta}(t_3)x_{\alpha+2\beta}(t_4)$: （1）若 $g \in C(\Gamma_\alpha)$, 则 $g = tx_\alpha(t_1)$, 其中 $t \in Z(G)$; （2）若 $g \in C(\Gamma_{\alpha+\beta})$, 则 $g = tx_\alpha(t_1)x_{\alpha+\beta}(t_3)x_{\alpha+2\beta}(t_4)$, 其中 $t \in Z(G)$。

证明. 让我们回顾一下根系 B_2 中单根对应的初等幺幂元的交换子公式（参见 [99], 引理 33）。若 α 是长单根，β 是短单根，则

$$[x_\alpha(t), x_\beta(u)] = x_{\alpha+\beta}(\pm tu)x_{\alpha+2\beta}(\pm tu^2),$$
$$[x_{\alpha+\beta}(t), x_\beta(u)] = x_{\alpha+2\beta}(\pm 2tu).$$

情形 1，$g \in C(\Gamma_\alpha)$。在这种情形下

$$x_\alpha(1), x_{\alpha+\beta}(1), x_{\alpha+2\beta}(1), x_{-\beta}(1), x_{-\alpha-2\beta}(1) \in \Gamma_\alpha.$$

从 $x_\alpha(1)$ 开始，我们得到

$$g = tx_\alpha(t_1)x_\beta(t_2)x_{\alpha+\beta}(t_3)x_{\alpha+2\beta}(t_4) =$$
$$= g^{x_\alpha(1)} = (tx_\alpha(c_t^\alpha - 1))x_\alpha(t_1)(x_\beta(t_2)x_{\alpha+\beta}(\pm t_2)x_{\alpha+2\beta}(\pm t_2^2))x_{\alpha+\beta}(t_3)x_{\alpha+2\beta}(t_4),$$

因此 $[t, x_\alpha(1)] = 1$, $t_2 = 0$。

Then

$$g^{x_{-\beta}(1)} = (tx_{-\beta}(c_t^{-\beta} - 1))x_\alpha(t_1)(x_\alpha(\pm 2t_3)x_{\alpha+\beta}(t_3))(x_{\alpha+\beta}(\pm t_4)x_\alpha(\pm t_4)x_{\alpha+2\beta}(t_4))$$

因此 $[t, x_{-\beta}(1)] = 1$（所以根据注 1，$t \in Z(G)$），$t_4 = 0$ 和 $2t_3 = 0$。

因此,

$$g = tx_\alpha(t_1)x_{\alpha+\beta}(t_3), \quad t \in Z(G), 2t_3 = 0.$$

由于 $[w_{\alpha+2\beta}(1)\ g] = 1$，因此

$$g = g^{w_{\alpha+2\beta}(1)} = tx_\alpha(t_1)x_{\mathbf{w}_{\alpha+2\beta}(\alpha+\beta)}(t_3) = tx_\alpha(t_1)x_{-\beta}(\pm t_3),$$

因此 $t_3 = 0$。

第一种情况已完成。

情形 2, $g \in C(\Gamma_{\alpha+\beta})$。在这种情况下仅

$$x_\alpha(1), x_{\alpha+\beta}(1), x_{\alpha+2\beta}(1) \in \Gamma_\beta.$$

从 $x_\alpha(1)$ 开始，我们得到

$$g^{x_\alpha(1)} = (tx_\alpha(c_t^\alpha - 1))x_\alpha(t_1)(x_\beta(t_2)x_{\alpha+\beta}(\pm t_2)x_{\alpha+2\beta}(\pm t_2^2))x_{\alpha+\beta}(t_3)x_{\alpha+2\beta}(t_4),$$

因此 $t_2 = 0$, $[t, x_\alpha(1)] = 1$ 和 $g = tx_\alpha(t_1)x_{\alpha+\beta}(t_3)x_{\alpha+2\beta}(t_4)$。

我们使用 $x_{\alpha+\beta}(1)$:

$$g^{x_{\alpha+\beta}(1)} = (tx_{\alpha+\beta}(c_t^{\alpha+\beta} - 1))x_\alpha(t_1)x_{\alpha+\beta}(t_3))x_{\alpha+2\beta}(t_4),$$

因此 $[t, x_{\alpha+\beta}(1)] = 1$，从而

$$g = tx_\alpha(t_1)x_{\alpha+\beta}(t_3)x_{\alpha+2\beta}(t_4), \quad t \in Z(G),$$

这就是所要求的。 ■

引理 12. 若 $\Phi = \mathsf{B}_l$、C_l、F_4, $l \geqslant 3$, $g = tx_{\alpha_1}(t_1) \ldots x_{\alpha_m}(t_m)$，$\alpha_1, \ldots, \alpha_m \in \Phi^+$，根$\alpha_1, \ldots, \alpha_m$按其高度排列，$g \in C(\Gamma_\alpha)$，则:

(1) 若 α 是长根，或 α 是短根，且 $\Phi = \mathsf{F}_4$ 或 B_l 对于 $l \geqslant 3$成立，则 $g = tx_{\alpha_1}(t_1)$，其中$t \in Z(G)$;

(2) 若 $\alpha = e_1 + e_2$属于标准系 C_l, $l \geqslant 3$，则 $g = tx_{e_1+e_2}(t_1)x_{2e_1}(t_2)x_{2e_2}(t_3)$，其中$t \in Z(G)$。

证明。

步骤 1. 假设 $\alpha = \alpha_1$ 是 Φ 的长单根。在这种情况下， Φ 的任何其他正根 γ 都与 α 构成以下构型:

(1) α 和 γ 正交（且它们的和不是根）；(2) α 和 γ 或 α 和 $\gamma - \alpha$ 是系统 A_2 的单根；(3) α 和 γ 或 α 和 $\gamma - \alpha$ 是系统 B_2, 的单根，其中 α 是长根。

在第二种情形下，根据 $x_\gamma(t_\gamma)$和 $x_{\alpha+\gamma}(t_{\alpha+\gamma})$（或 $x_{\gamma-\alpha}(t_{\gamma-\alpha})$）中的引理10，我们有$t_\gamma = t_{\gamma\pm\alpha} = 0$，并且 $[x_\alpha(1)\ t] = 1$, $[x_\gamma(1)\ t] = 1$。

在第三种情形下，根据 $x_\gamma(t_\gamma)$、 $x_{\alpha+\gamma}(t_{\alpha+\gamma})$和 $x_{\alpha+2\gamma}(t_{\alpha+2\gamma})$中的引理 11，我们有$t_\gamma = t_{\alpha+\gamma} = t_{\alpha+2\gamma} = 0$, 并且 $[x_\gamma(1)\ t] = 1$。

应用这些论证，我们得到 $g = tx_\alpha(t_1)\ \ldots x_\gamma(t_\gamma)\ldots$，其中所有出现在 g 中的 γ 都与 α 正交。

之后，我们从单根 γ 开始，并以最高根结束，采用与引理10中相同的论证，通过 $w_\gamma(1)$ 共轭 g。

因此，对于所有长根 α，引理得证。

现在我们可以假设 α 是短根。

步骤2。我们来考察系统 B_l, $l \geqslant 3$。

该系统的根为 $\{\pm e_i, \pm e_i \pm e_j \mid 1 \leqslant i < j \leqslant l\}$，其中 $e_1, \ldots, e_l$ 是欧几里得空间的一组标准基。在我们的情形下，可以假设 $\alpha = \alpha_1 = e_l$, $\alpha_2 = e_{l-1} - e_l, \ldots, \alpha_l = e_1 - e_2$。

我们先来看由 $x_\alpha(1) \in \Gamma_\alpha$ 进行的共轭:

$$g^{x_\alpha(1)} = (tx_\alpha(c_t^\alpha - 1))x_\alpha(t_1)\ldots(x_{e_i}(t_{e_i})x_{e_i+e_l}(\pm 2t_{e_i}))\ldots \\ \ldots(x_{e_i-e_l}(t_{e_i-e_l})x_{e_i}(\pm t_{e_i-e_l})x_{e_i+e_l}(\pm t_{e_i-e_l}))\ldots,$$

因此，对所有 $i = 1$，都有 $[x_\alpha(1)\ t] = 1$ 和 $t_{e_i-e_l} = 0$，....., $l - 1$。

同样地，让我们对 g 用 $x_{e_l-e_i}(1) \in \Gamma_\alpha$ 做共轭:

$$g^{x_{e_l-e_i}(1)} = (tx_{e_l-e_i}(c_t^{e_l-e_i} - 1))x_\alpha(t_1)\ldots(x_{e_i+e_j}(t_{e_i+e_j})x_{e_j+e_l}(t_{e_i+e_j}))\ldots \\ \ldots(x_{e_i}(t_{e_i})x_{e_l}(\pm t_{e_i})x_{e_l+e_i}(\pm t_{e_i}^2))\ldots,$$

因此，对所有 $i \neq j$、 i、 $j \neq l$，有 $[x_{e_l-e_i}(1)\ t] = 1$（因此 $t \in Z(G)$），且 $t_{e_i+e_j} = 0$；并且对所有 $i \neq l$，有 $t_{e_i} = 0$。

Now

$$g = tx_\alpha(t_1)\ldots x_{e_i-e_j}(t_{e_i-e_j})\ldots x_{e_i+e_l}(t_{e_i+e_l})\ldots, \text{ where } i, j \neq l, i < j.$$

让我们用 $x_{e_j+e_l}(1) \in \Gamma_\alpha$ 共轭 g：

$$g^{x_{e_j+e_l}(1)} = tx_\alpha(t_1)\ldots(x_{e_i-e_j}(t_{e_i-e_j})x_{e_i+e_l}(t_{e_i-e_j}))\ldots x_{e_i+e_l}(t_{e_i+e_l})\ldots,$$

因此 $t_{e_i-e_j} = 0$ 和

$$g = tx_\alpha(t_1)x_{e_{l-1}+e_l}(t_{e_{l-1}+e_l})\ldots x_{e_1+e_l}(t_{e_1+e_l}).$$

由于 $l \geqslant 3$，对于每个 $i \neq l$ 我们有 $k \neq i$， l。对这样的 k 取元素 $x_{e_k-e_i}(1) \in \Gamma_\alpha$，我们有

$$g^{x_{e_k-e_i}(1)} = tx_\alpha(t_1)\ldots\ldots(x_{e_i+e_l}(t_{e_i+e_l})x_{e_k+e_l}(t_{e_i+e_l}))\ldots,$$

因此， $t_{e_i+e_l} = 0$ 和 $g = tx_\alpha(t_1)$，这正是所要求的。

步骤 3. 考察系统 F_4, ，采用与步骤 2 相同的论证，并依次通过 $x_\alpha(1)$、 $x_{-\alpha_2}(1)$、 $x_{-\alpha_3}(1)$、 $x_{-\alpha_4}(1)$ 等进行共轭，可得相同的结果： $g = tx_\alpha(t_1)$，其中$t \in Z(G)$。

第 4 步。最后一种情况最有意思：根系 C_l, $l \geqslant 3$。根为

$$\pm 2e_i \text{ and } \pm e_i \pm e_j, \text{ where } 1 \leqslant i < j \leqslant l,$$

正根的集合为

$$e_i - e_j,\ i > j, \quad e_i + e_j,\ i \neq j, \quad 2e_i.$$

与上文一样，这里我们假设 $\alpha = e_1 + e_2$。
集合 Γ_α 由以下元素组成

$$\{e_1 + e_2; 2e_1; 2e_2; \pm 2e_i, e_1 \pm e_i, e_2 \pm e_i, i \geqslant 3; \pm e_i \pm e_j, i \neq j, i, j \geqslant 3\}.$$

将 g 与 $x_{e_1+e_i}(1)$、 $i \geqslant 3$共轭，得到

$$g^{x_{e_1+e_i}(1)} = (tx_{e_1+e_i}(c_t^{e_1+e_i} - 1))x_{e_1+e_2}(t_{e_1+e_2}) \dots (x_{e_2-e_i}(t_{e_2-e_i})x_{e_1+e_2}(t_{e_2-e_i})) \dots \\ \dots (x_{e_k-e_i}(t_{e_k-e_i})x_{e_1+e_k}(t_{e_k-e_i}) \dots, \quad 3 \leqslant k < i,$$

而这些额外的 $x_{e_1+e_2}(\dots)$ 和 $x_{e_1+e_k}(\dots)$ 不可能通过这种共轭从任何其他元素中产生。因此，对所有 $2 \leqslant k < i \leqslant l$， $t_{e_k-e_i} = 0$。此外， $[t, x_{e_1+e_i}(1)] = 1$。
用 $i \geqslant 3$ 通过 $x_{e_2+e_i}(1)$ 共轭 g，我们得到

$$g^{x_{e_2+e_i}(1)} = (tx_{e_2+e_i}(c_t^{e_2+e_i} - 1))(x_{e_1-e_2}(t_{e_1-e_2})x_{e_1+e_i}(t_{e_1-e_2})) \dots \\ \dots (x_{e_1-e_i}(t_{e_1-e_i})x_{e_1+e_2}(t_{e_1-e_i})) \dots,$$

而这些额外的 $x_{e_1+e_2}(\dots)$ 和 $x_{e_1+e_i}(\dots)$ 不可能由共轭作用下的任何其他元素产生。因此，对所有 $3 \leqslant i \leqslant l$， $t_{e_1-e_2} = 0$ 和 $t_{e_1-e_i} = 0$。此外， $[t, x_{e_2+e_i}(1)] = 1$。
将 g 共轭于 $x_{e_1+e_2}(1)$，我们有

$$g^{x_{e_1+e_2}(1)} = (tx_{e_1+e_2}(c_t^{e_1+e_2} - 1))x_{\alpha_1}(a_1) \dots x_{\alpha_m}(a_m).$$

因此 $[t, x_{e_1+e_2}(1)] = 1$。
用 $x_{e_2-e_i}(1)$ 共轭 g、 $i \geqslant 3$，我们得到

$$g^{x_{e_2-e_i}(1)} = (tx_{e_2-e_i}(c_t^{e_2-e_i} - 1)) \dots (x_{e_1+e_i}(t_{e_1+e_i})x_{e_1+e_2}(t_{e_1+e_i})) \dots (x_{2e_i}(t_{2e_i})x_{e_2+e_i}(\pm t_{2e_i})x_{2e_2}(\pm t_{2e_2})) \\ \dots (x_{e_i+e_j}(t_{e_i+e_j})x_{e_2+e_j}(t_{e_i+e_j})) \dots (x_{e_2+e_i}(t_{e_2+e_i})x_{2e_2}(\pm 2t_{e_2+e_i})), \quad j \geqslant 3, j \neq i.$$

因此 $t_{e_1+e_i} = 0$ 和 $t_{2e_i} = 0$ 对于 $i \geqslant 3$， $t_{e_i+e_j} = 0$ 对所有 $3 \leqslant i, j \leqslant l$， $i \neq j$。此外$[t, x_{e_2-e_i}(1)] = 1$。
通过 $x_{e_1-e_i}(1)$、 $i \geqslant 3$ 共轭也是同样的情况，这给出了 $t_{e_2+e_i} = 0$ for $i \geqslant 3$and $[t, x_{e_1-e_i}(1)] = 1$。

因此 $t \in Z(G)$ 和

$$g = tx_{e_1+e_2}(t_{e_1+e_2})x_{2e_1}(t_{2e_1})x_{2e_2}(t_{2e_2}).$$

这正是所需的内容。直接（且简单的）计算表明，对于这个根系，这样的 g 总是属于 $C(\Gamma_\alpha)$。 ■

由此，定理 2 得证。

4.3. 局部环上切瓦莱群中幺幂元的双中心化子。

本节将证明，对于局部环上的切瓦莱群的大子群，同样的定理也成立。在论文 [20] 中，我们已经得到了局部环的一个类似结果，但我们假设在某些根系中，这些环包含 $1/2$ 或 $1/3$。现在，重要的是证明该结果对所有局部环都成立，不附带任何限制。

定理 2（参见 [20]）。对于任意切瓦莱群（或其大子群） $G = G_\pi(\Phi, R)$，其中Φ 是秩为 > 1 的不可约根系， R 是局部环；若对于某个 $\alpha \in \Phi$ ，元素$g \in C_G(\Gamma_\alpha)$，则 $g = cx_\alpha(t)$，其中 $t \in R$, $c \in Z(G)$，但以下情形除外： $\Phi = \mathbf{C}_l$, $l \geqslant 2$，且 α 是短根。

在 $\Phi = \mathbf{C}_l = \{\pm e_i \pm e_j \mid 1 \leqslant i, j \leqslant l, i \neq j\} \cup \{\pm 2e_i \mid 1 \leqslant i \leqslant l\}$ 且 $\alpha = e_1 + e_2$ 的情形下，若$g \in C_G(\Gamma_\alpha)$，则

$$g = cx_{e_1+e_2}(t_1)x_{2e_1}(t_2)x_{2e_2}(t_3), \quad c \in Z(G).$$

证明。令 $\Gamma_\alpha = \{x_\beta(1) \mid [x_\beta(1)\ x_\alpha(1)] = e\}$, $g \in C_G(\Gamma_\alpha)$。

我们将剩余域 $R/\operatorname{Rad} R$ 记作 k，并将商群 $\overline{G} = \underline{G}_\pi(\Phi, k)$ 中元素 g、$x_\beta(1)$ t、u 等的像分别记作 $\overline{g}$、 $x_\beta(1)$ $\overline{t}$、 $\overline{u}$。

由于 $g \in C_G(\Gamma_\alpha)$，我们有$\overline{g} \in C_{\overline{G}}(\overline{\Gamma}_\alpha)$，其中 $\overline{\Gamma}_\alpha = \{x_\beta(1) \mid [x_\beta(1)\ x_\alpha(1)^{-}] = \overline{e}\}$。由于 $\overline{G}$ 是域上的切瓦莱群，根据定理 2

$$\overline{g} = \overline{c}x_\alpha(\overline{t}),\ \overline{c} \in Z(\overline{G}) \quad (\text{or } \overline{c}x_{e_1+e_2}(\overline{t}_1)x_{2e_1}(\overline{t}_2)x_{2e_2}(\overline{t}_3),\ \text{if } \Phi = \mathbf{C}_l,\ l \geqslant 2,\ \alpha = e_1 + e_2).$$

如在上一节中一样，我们假设 $\alpha = \alpha_1$ 是第一个单根。

在局部环上的切瓦莱群 G 中，存在如下形式的高斯分解$G = UTVU$（见 [97], [1], [3], [52]）。因此我们固定 g 的一个表示为

$$g = x_{\alpha_1}(r_1) \dots x_{\alpha_m}(r_m)tx_{-\alpha_1}(s_1) \dots x_{-\alpha_m}(s_m)x_{\alpha_1}(t_1) \dots x_{\alpha_m}(t_m),$$

其中 α_i是正根， r_i、 s_i、 $t_i \in R$、 $t \in T(R)$。由于 g在典范同态下的像是

$$x_\alpha(\overline{r}_1)\overline{t} \quad (\text{or } x_{e_1+e_2}(\overline{r}_1)x_{2e_1}(\overline{r}_2)x_{2e_2}(\overline{r}_3)\overline{t} \text{ in the case } \Phi = \mathbf{C}_l, l \geqslant 2, \alpha = e_1 + e_2).$$

因此，在所有情况下，元素 $s_1, \dots, s_m, t_1, \dots, t_m \in \operatorname{Rad} R$。

根据公式

$$x_{-\gamma}(s)x_\gamma(t) = h_\gamma\left(\frac{1}{1+st}\right)x_\gamma(t(1+st))x_{-\gamma}\left(\frac{s}{1+st}\right) \text{ for all } \gamma \in \Phi \qquad (*)$$

（通过用 SL_2 中的矩阵表示 $x_\gamma(\cdot)$、 $x_{-\gamma}(\cdot)$、 $h_\gamma(\cdot)$，可直接验证这一点）。由于 $1 + st \in R^*$ if $s \in \operatorname{Rad} R$ or $t \in \operatorname{Rad} R$，我们可以将所有 $x_\beta(t_i)$ 从分解的右边移到左边。于是得到一个形式如下的 g 表示

$$g = x_{\alpha_1}(r_1) \dots x_{\alpha_m}(r_m)tx_{-\alpha_1}(s_1) \dots x_{-\alpha_m}(s_m), \quad s_1, \dots, s_m \in \operatorname{Rad} R.$$

请注意，与原始高斯分解不同，这种分解是唯一确定的。事实上，假设

$$u_1t_1v_1 = u_2t_2v_2.$$

如果我们把所有正根移到一边： $t_1v_1v_2^{-1}t_2^{-1} = u_1^{-1}u_2$，那么由于 $TV \cap U = 1$，因此 $u_1 = u_2$ 和 $v_1v_2^{-1} = t_2t_1^{-1}$。由于 $T \cap V = 1$，我们有 $v_1 = v_2$， $t_1 = t_2$，所以这种分解形式是唯一的。

我们还使用公式

$$x_\gamma(1)x_{-\gamma}(s)x_\gamma(1)^{-1} = h_\gamma\left(\frac{1}{1-s}\right)x_\gamma(s^2-s)x_{-\gamma}\left(\frac{s}{1-s}\right) \text{ for all } \gamma\in\Phi \qquad (**)$$

这直接由（$*$）得到。

与上一节一样，我们假设根 α_1、...、α_m 按其高度排序。

在我们的高斯分解 UTV 情形下，方便起见，假设对于 $g = utv \in UTV$ 总是

$$u = x_{\alpha_1}(r_1)\dots x_{\alpha_m}(r_m)tx_{-\alpha_m}(s_m)\dots x_{-\alpha_1}(s_1).$$

Ca第 1 节。等长根的根系：$\mathbf{A}_l$、$\mathbf{D}_l$、$\mathbf{E}_l$.

考虑一个根 $\beta\in\Phi$，使得 $\alpha+\beta\notin\Phi$，因此元素 $x_\beta(1)\in\Gamma_\alpha$。由于 $g\in C(\Gamma_\alpha)$，所以 $g^{x_\beta(1)} = g$。我们来考察该元素的共轭对 g 及其因子的作用（假设 β 为正）：

$$\begin{aligned} g = g^{x_\beta(1)} &= x_{\alpha_1}(r_1)^{x_\beta(1)}\dots x_{\alpha_m}(r_m)^{x_\beta(1)}t^{x_\beta(1)}x_{-\alpha_m}(s_m)^{x_\beta(1)}\dots x_{-\alpha_1}(s_1)^{x_\beta(1)} = \\ &= x_{\alpha_1}(r_1)\dots(x_{\alpha_i}(r_i)x_{\alpha_i+\beta}(\pm r_i))\dots x_{\alpha_m}(r_m)\cdot(x_\beta(c_t^\beta-1)t)\cdot \\ &\cdot(x_{-\alpha_m}(s_m)x_{-\alpha_m+\beta}(\pm s_m))\dots\left(h_\beta\left(\frac{1}{1-s_{-\beta}}\right)x_\beta(s_{-\beta}^2-s_{-\beta})x_{-\beta}\left(\frac{s_{-\beta}}{1-s_{-\beta}}\right)\right)\dots x_{-\alpha_1}(s_1). \end{aligned}$$

让我们分析所得的等号。

注意，从 t 的左边只有带正根的幺正元，也就是说，是 U 的一个元素。从 t 的右边有一个环面 T 的元素 $h_\beta\left(\frac{1}{1-s_{-\beta}}\right)$。由于环面显然会规范化任意 X_α，我们可以将这个元素移到左边，并得到 $t\cdot h_\beta\left(\frac{1}{1-s_{-\beta}}\right)$，而不是 t。由于所有通过任意带负根的幺正元与 $x_\beta(1)$ 共轭而出现的带正根的幺正元 $-\gamma$，其高度都严格小于 γ，因此可以将它们向左移到 T 和 U 的方向，并且在这一移动过程中不可能遇到具有相反根的幺正元。这意味着，可以将位于 t 右边的所有带正根的幺正元移到 t 的左边。因此，t 和 $h_\beta\left(\frac{1}{1-s_{-\beta}}\right)$ 不会发生改变。之后，$g^{x_\beta(1)}$ 将被写成 UTV 的形式，即

$$t = t\cdot h_\beta\left(\frac{1}{1-s_{-\beta}}\right),$$

因此 $s_{-\beta} = 0$。

因此，t 的左侧部分或右侧部分中都不会出现新的 $x_\beta(\cdot)$，见 $g^{x_\beta(1)}$。由此，在表达式 $t^{x_\beta(1)} = x_\beta(c_t^\beta - 1)$ 中，我们必然有 $c_t^\beta = 1$，也就是说

$$[t, x_\beta(1)] = 1.$$

如果 $\beta\in\Gamma_\alpha\cap\Phi^+$ 和 $\gamma = \beta-\alpha\in\Phi$，那么

$$\begin{aligned} g = g^{x_\beta(1)} &= u'tx_{-\alpha_m}(s_m)^{x_\beta(1)}\dots x_{-\alpha_i}(s_i)^{x_\beta(1)}\dots x_{-\gamma}(s_\gamma)^{x_\beta(1)}\dots x_{-\alpha_1}(s_1) = \\ &= u'tx_{-\alpha_m}(s_m)x_{-\alpha_m+\beta}(\pm s_m)\dots x_{-\alpha_i}(s_i)x_{-\alpha_i+\beta}(\pm s_i)\dots x_{-\gamma}(s_{-\gamma})x_\alpha(\pm s_{-\gamma})\dots x_{-\alpha_1}(s_1). \end{aligned}$$

在 V 部分出现了一个新的元素 $x_\alpha(\pm s_{-\gamma})$，而不可能从任何其他共轭 $x_\delta(\cdot)^{x_\beta(1)}$ 中得到 $x_\alpha(\cdot)$。当我们将 $x_\alpha(\pm s_{-\gamma})$ 及其他 $x_{-\delta+\beta}(\cdot)$、$-\delta+\beta\in\Phi^+$移到等式左侧时，同样无法得到任何新的 $x_\alpha(\cdot)$。因此 $s_{-\gamma} = 0$。

因此我们看到，对于所有满足 $\alpha+\gamma\notin\Phi$ 的根 $\gamma\in\Phi^+$，以及所有满足 $\alpha+\gamma\in\Phi$ 的根 $\gamma\in\Phi^+$，都有 $s_{-\gamma}=0$，但 $\alpha+2\gamma\notin\Phi$。然而，对于单根长根系，所有正根都具有这些性质之一。

因此 $g\in UT$ 并且我们来到了引理10的情形，该引理是针对任意交换环证明的。根据此引理 $g=cx_{\alpha_1}(r_1)$，其中 $c\in Z(G)$。因此，定理 3对根系 A_l、D_l、初等子群$_l$、 $l\geqslant 2$ 得证。

情形 2. 根系 G_2.

我们再次指出，该根系的单根为 α,β，正根为 $\alpha,\beta,\alpha+\beta,\alpha+2\beta,\alpha+3\beta,2\alpha+3\beta$,

$$\Gamma_\alpha=\{x_\alpha(1),x_{\alpha+\beta}(1),x_{\alpha+2\beta}(1),x_{2\alpha+3\beta}(1),x_{-\beta}(1),x_{-\alpha-2\beta}(1),x_{-\alpha-3\beta}(1)\}$$

and

$$\Gamma_\beta=\{x_\beta(1),x_{\alpha+3\beta}(1),x_{2\alpha+3\beta}(1),x_{-\alpha}(1),x_{-2\alpha-3\beta}(1)\}.$$

在第一种情况下， $g\in C(\Gamma_\alpha)$，依据与前一种情况相同的论证

$$s_{-\alpha}=s_{-\alpha-\beta}=s_{-\alpha-2\beta}=s_{-2\alpha-3\beta}=r_\beta=r_{\alpha+2\beta}=r_{\alpha+3\beta}=0\text{ and }t\in Z(G),$$

因此

$$g=x_\alpha(r_\alpha)x_{\alpha+\beta}(r_{\alpha+\beta})x_{2\alpha+3\beta}(r_{2\alpha+3\beta})tx_{-\beta}(s_{-\beta})x_{-\alpha-3\beta}(s_{-\alpha-3\beta}),\quad t\in Z(G).$$

用 $x_{2\alpha+3\beta}(1)$ 共轭 g 后，我们有

$$g^{x_{2\alpha+3\beta}(1)}=x_\alpha(r_\alpha)x_{\alpha+\beta}(r_{\alpha+\beta})x_{2\alpha+3\beta}(r_{2\alpha+3\beta})tx_{-\beta}(s_{-\beta})x_{-\alpha-3\beta}(s_{-\alpha-3\beta})x_\alpha(\pm s_{-\alpha-3\beta}),$$

因此 $s_{-\alpha-3\beta}=0$ 并且

$$g=x_\alpha(r_\alpha)x_{\alpha+\beta}(r_{\alpha+\beta})x_{2\alpha+3\beta}(r_{2\alpha+3\beta})tx_{-\beta}(s_{-\beta}),\quad t\in Z(G).$$

将 g 按 $x_{-\beta}(1)$ 共轭，得到

$$g^{x_{-\beta}(1)}=x_\alpha(r_\alpha)x_\alpha(\pm 3r_{\alpha+\beta})x_{\alpha+\beta}(r_{\alpha+\beta})x_{2\alpha+3\beta}(r_{2\alpha+3\beta})tx_{-\beta}(s_{-\beta}),$$

因此 $3r_{\alpha+\beta}=0$。

将 g 按 $x_{\alpha+2\beta}(1)$ 共轭，得到

$$\begin{aligned}g^{x_{\alpha+2\beta}(1)}&=\\&=x_\alpha(r_\alpha)x_{\alpha+\beta}(r_{\alpha+\beta})x_{2\alpha+3\beta}(r_{2\alpha+3\beta}\pm 3r_{\alpha+\beta})tx_{2\alpha+3\beta}(\pm 3s_{-\beta})x_\alpha(\pm 3s_{-\beta}^2)x_{\alpha+\beta}(\pm 2s_{-\beta})x_{-\beta}(s_{-\beta})=\\&=x_\alpha(r_\alpha\pm 3s_{-\beta}^2)x_{\alpha+\beta}(r_{\alpha+\beta}\pm 2s_{-\beta})x_{2\alpha+3\beta}(r_{2\alpha+3\beta}\pm 3r_{\alpha+\beta}\pm 3s_{-\beta})tx_\beta(s_{-\beta}),\end{aligned}$$

由于 $3r_{\alpha+\beta}=0$，我们有 $2s_{-\beta}=3s_{-\beta}=0$，因此 $s_{-\beta}=0$。

现在 $g\in UT$，我们的结论由引理 9 得出。

在第二种情况下 $g\in C(\Gamma_\beta)$，我们有

$$s_{-\beta}=s_{-\alpha-3\beta}=s_{-2\alpha-3\beta}=r_\alpha=r_{2\alpha+3\beta}=0\text{ and }t\in Z(G),$$

因此

$$g=x_\beta(r_\beta)x_{\alpha+\beta}(r_{\alpha+\beta})x_{\alpha+2\beta}(r_{\alpha+2\beta})x_{\alpha+3\beta}(r_{\alpha+3\beta})tx_{-\alpha}(s_{-\alpha})x_{-\alpha-\beta}(s_{-\alpha-\beta})x_{-\alpha-2\beta}(s_{-\alpha-2\beta}).$$

用 $x_{-\alpha}(1)$ 共轭 g，可得

$$\begin{aligned}g^{x_{-\alpha}(1)}=x_\beta(r_\beta)(&x_{\alpha+\beta}(r_{\alpha+\beta})x_\beta(\pm r_{\alpha+\beta})x_{\alpha+2\beta}(\pm r_{\alpha+\beta}^2)x_{2\alpha+3\beta}(\pm r_{\alpha+\beta}^3)x_{\alpha+3\beta}(r_{\alpha+3\beta}^3))\cdot\\&\cdot x_{\alpha+2\beta}(r_{\alpha+2\beta})x_{\alpha+3\beta}(r_{\alpha+3\beta})tx_{-\alpha}(s_{-\alpha})x_{-\alpha-\beta}(s_{-\alpha-\beta})x_{-\alpha-2\beta}(s_{-\alpha-2\beta}),\end{aligned}$$

因此 $r_{\alpha+\beta}=0$。

类似地，如果我们用 $x_{\alpha+3\beta}(1)$ 共轭 g，就得到 $s_{-\alpha-2\beta}=0$。

因此在这一阶段

$$g=x_\beta(r_\beta)x_{\alpha+2\beta}(r_{\alpha+2\beta})x_{\alpha+3\beta}(r_{\alpha+3\beta})tx_{-\alpha}(s_{-\alpha})x_{-\alpha-\beta}(s_{-\alpha-\beta}).$$

现在用 $x_{2\alpha+3\beta}(1)$ 对 g 作共轭，我们有

$$\begin{aligned}g^{x_{2\alpha+3\beta}(1)}=x_\beta(r_\beta)x_{\alpha+2\beta}(r_{\alpha+2\beta})x_{\alpha+3\beta}(r_{\alpha+3\beta})t(x_{\alpha+3\beta}(\pm s_{-\alpha})x_{-\alpha}(s_{-\alpha}))\cdot\\ \cdot(x_{-\alpha-\beta}(s_{-\alpha-\beta})x_{\alpha+2\beta}(\pm s_{-\alpha-\beta})x_\beta(\pm s^2_{-\alpha-\beta})x_{-\alpha}(\pm s^3_{-\alpha-\beta})x_{\alpha+3\beta}(\pm s^3_{-\alpha-\beta})),\end{aligned}$$

因此 $s_{-\alpha}=s_{-\alpha-\beta}=0$和 $g=x_\beta(r_\beta)x_{\alpha+2\beta}(r_{\alpha+2\beta})x_{\alpha+3\beta}(r_{\alpha+3\beta})t$。

现在再次得到 $g\in UT$，因此定理 3 的结果可由引理 9 推出。

情形 3。根系 B_l, $l\geqslant 3$，以及 F_4。

我们记得，B_l 由根 $\{\pm e_i,\pm e_i\pm e_j\mid 1\leqslant i,j\leqslant l,i\neq j\}$组成。如果 α 是一个长根 e_1-e_2，那么

$$\Gamma_\alpha=\{x_{e_1\pm e_2}(1),x_{-e_1-e_2}(1),x_{e_1\pm e_i}(1),x_{-e_2\pm e_i}(1),x_{\pm e_i\pm e_j}(1),x_{e_1}(1),x_{-e_2}(1),x_{\pm e_i}(1)\},$$

其中 $3\leqslant i$、$j\leqslant l$、$i\neq j$。

因此，理由与上文相同，

$$s_{-e_1\pm e_2}=r_{e_1+e_2}=s_{-e_1\pm e_i}=r_{e_2\pm e_i}=r_{\pm e_i\pm e_j}=s_{-e_1}=r_{e_2}=r_{\pm e_i}=0,\qquad t\in Z(G),$$

其中 $3\leqslant i$、$j\leqslant l$、$i\neq j$。

因此

$$\begin{aligned}g=x_{e_1-e_2}(r_{e_1-e_2})\dots x_{e_1-e_l}(r_{e_1-e_l})x_{e_1+e_3}(r_{e_1+e_3})\dots x_{e_1+e_l}(r_{e_1+e_l})x_{e_1}(r_{e_1})t\cdot\\ \cdot x_{-e_2-e_3}(s_{-e_2-e_3})\dots x_{-e_2-e_l}(s_{-e_2-e_l})x_{-e_2+e_3}(s_{-e_2+e_3})\dots x_{-e_2+e_l}(s_{-e_2+e_l})x_{-e_2}(s_{-e_2}).\end{aligned}$$

用 $x_{-e_2+e_i}(1)$ 共轭 g，我们得到

$$\begin{aligned}g^{x_{-e_2+e_i}(1)}=x_{e_1-e_2}(r_{e_1-e_2})\dots(x_{e_1-e_i}(r_{e_1-e_i})x_{e_1-e_2}(\pm r_{e_1-e_i}))\dots\\ \dots x_{e_1-e_l}(r_{e_1-e_l})x_{e_1+e_3}(r_{e_1+e_3})\dots x_{e_1+e_l}(r_{e_1+e_l})x_{e_1}(r_{e_1})t\cdot\\ \cdot x_{-e_2-e_3}(s_{-e_2-e_3})\dots x_{-e_2-e_l}(s_{-e_2-e_l})x_{-e_2+e_3}(s_{-e_2+e_3})\dots x_{-e_2+e_l}(s_{-e_2+e_l})x_{-e_2}(s_{-e_2}),\end{aligned}$$

因此对于所有 $3\leqslant i\leqslant l$，我们有 $r_{e_1-e_i}=0$。

将 g 通过 $x_{-e_2-e_i}(1)$ 共轭，我们同样得到 $r_{e_1+e_i}=0$ 对所有 $3\leqslant i\leqslant l$。所以我们看到

$$\begin{aligned}g=x_{e_1-e_2}(r_{e_1-e_2})x_{e_1}(r_{e_1})t\cdot\\ \cdot x_{-e_2-e_3}(s_{-e_2-e_3})\dots x_{-e_2-e_l}(s_{-e_2-e_l})x_{-e_2+e_3}(s_{-e_2+e_3})\dots x_{-e_2+e_l}(s_{-e_2+e_l})x_{-e_2}(s_{-e_2}).\end{aligned}$$

对于 $3\leqslant i\leqslant l$ 的情形，我们先用 $x_{e_1+e_i}(1)$ 再用 $x_{e_1-e_i}(1)$ 对 g 进行共轭，处理方式非常相似。省略相应的计算。我们得到

$$g=x_{e_1-e_2}(r_{e_1-e_2})x_{e_1}(r_{e_1})tx_{-e_2}(s_{-e_2}).$$

将 g 通过 $x_{-e_1-e_2}(1)$ 共轭，得到 $r_{e_1}=0$；将 g 通过 $x_{e_1+e_2}(1)$ 共轭，得到$s_{-e_2}=0$，这正是所需的。

这是 B_l, $l\geqslant$的情形，其中 α 是长根。现在我们假设 α 是短根，例如 $\alpha=e_1$。

在这种情况下

$$\Gamma_\alpha = \{x_{e_1}(1), x_{e_1\pm e_i}(1), x_{\pm e_i\pm e_j}(1)\}, \text{ where } 2 \leqslant i, j \leqslant l, i \neq j.$$

因此

$$s_{-e_1} = s_{-e_1\pm e_i} = r_{\pm e_i\pm e_j} = 0 \text{ for } 2 \leqslant i, j \leqslant l, i \neq j$$

and

$$g = x_{e_1}(r_{e_1}) \dots x_{e_l}(r_{e_l}) x_{e_1-e_2}(r_{e_1-e_2}) \dots x_{e_1-e_l}(r_{e_1-e_l}) x_{e_1+e_2}(r_{e_1+e_2}) \dots x_{e_1+e_l}(r_{e_1+e_l}) t \cdot \\ \cdot x_{-e_2}(s_{-e_2}) \dots x_{-e_l}(s_{-e_l}).$$

将 g 用 $x_{e_2-e_i}(1)$ 共轭，得到

$$g^{x_{e_2-e_i}(1)} = x_{e_1}(r_{e_1}) \dots (x_{e_i}(r_{e_i}) x_{e_2}(\pm r_{e_i}) x_{e_2+e_i}(\pm r_{e_i})^2) \dots x_{e_l}(r_{e_l}) \cdot \\ \cdot (x_{e_1-e_2}(r_{e_1-e_2}) x_{e_1-e_i}(\pm r_{e_1-e_2})) \dots x_{e_1-e_l}(r_{e_1-e_l}) x_{e_1+e_2}(r_{e_1+e_2}) \dots \\ \dots (x_{e_1+e_i}(r_{e_1+e_i}) x_{e_1+e_2}(\pm r_{e_1+e_i})) \dots x_{e_1+e_l}(r_{e_1+e_l}) t \cdot \\ \cdot (x_{-e_2}(s_{-e_2}) x_{-e_i}(\pm s_{-e_2}) x_{-e_2-e_i}(\pm s_{-e_2}^2)) \dots x_{-e_l}(s_{-e_l}),$$

这直接推出

$$r_{e_i} = r_{e_1-e_2} = r_{e_1+e_i} = s_{-e_2} = 0 \text{ for all } 3 \leqslant i \leqslant l.$$

将 g 用 $x_{e_2+e_i}(1)$ 共轭，我们同样得到

$$r_{e_1-e_i} = s_{-e_i} = 0 \text{ for all } 3 \leqslant i \leqslant l.$$

因此

$$g = x_{e_1}(r_{e_1}) x_{e_2}(r_{e_2}) x_{e_1+e_2}(r_{e_1+e_2}) t.$$

现在将 g 用 $x_{e_3-e_2}$ 1 共轭，(得到

$$g^{x_{e_3-e_2}(1)} = x_{e_1}(r_{e_1})(x_{e_2}(r_{e_2}) x_{e_3}(\pm r_{e_2}) x_{e_2+e_3}(\pm r_{e_2}^2)) \cdot (x_{e_1+e_2}(r_{e_1+e_2}) x_{e_1+e_3}(\pm r_{e_1+e_2})) \cdot t,$$

因此$g = x_{e_1}(r_{e_1})t$、 $t \in Z(G)$，这正是所需的。

$\Phi = \mathrm{F}_4$ 的情形也可以用非常类似的方法处理。我们省略相应的计算。

4. $\Phi = \mathrm{C}_l$, $l \geqslant 2$, α 的情形很长。设（如上）

$$\Phi = \{\pm e_i \pm e_j, \pm 2e_i \mid 1 \leqslant i, j \leqslant l, i \neq j\}, \quad \alpha = 2e_1.$$

Then

$$\Gamma_\alpha = \{x_{2e_1}(1), x_{\pm 2e_i}(1), x_{e_1\pm e_i}(1), x_{\pm e_i\pm e_j}(1)\}, \text{ where } 2 \leqslant i, j \leqslant l, i \neq j.$$

因此，在 g

$$s_{-2e_1} = r_{2e_i} = s_{-2e_i} = s_{-e_1\pm e_i} = r_{\pm e_i\pm e_j} = 0, \quad t \in Z(G)$$

and

$$g = x_{2e_1}(r_{2e_1}) x_{e_1-e_2}(r_{e_1-e_2}) \dots x_{e_1-e_l}(r_{e_1-e_l}) x_{e_1+e_2}(r_{e_1+e_2}) \dots x_{e_1+e_l}(r_{e_1+e_l}) t,$$

即 g 与引理 12 中相同，且由同样的论证可得 $g = x_{2e_1}(r_{2e_1})t$, $t \in Z(G)$】【。

5. $\Phi = \mathrm{C}_l$, $l \geqslant 2$, α 的情形是短的。

我们假设 $\alpha = e_1 + e_2$。那么

$$\Gamma_\alpha = \{x_{2e_1}(1), x_{2e_2}(1), x_{\pm 2e_i}(1), x_{e_1\pm e_i}(1), x_{e_2\pm e_i}(1), x_{\pm e_i\pm e_j}(1)\}, \text{ where } 3 \leqslant i, j \leqslant l, i \neq j,$$

因此在 g 中

$$s_{-2e_1} = s_{-2e_2} = r_{2e_i} = s_{-2e_i} = s_{-e_1\pm e_i} = s_{-e_2\pm e_i} = r_{\pm e_i\pm e_j} = 0, \quad t \in Z(G),$$

因此 $g \in UT$，同一个引理 12 完成了证明。 ■

4.4. 任意交换环上切瓦莱群中幺幂元的双中心化子。

最后，我们能够 证明对于任意含幺交换环，同一定理也成立。

定理 3. 对于任意切瓦莱群（或其大子群） $G = G_\pi(\Phi, R)$，其中 Φ 是秩为 > 1 的不可约根系， R 是任意含幺交换环，若对某个 $\alpha \in \Phi$ ，存在元素 $g \in C_G(\Gamma_\alpha)$，则 $g = cx_\alpha(t)$，其中 $t \in R$， $c \in Z(G)$，但 $\Phi = \mathsf{C}_l$、 $l \geqslant 2$ 的情形除外，且 α 是短的。

在 $\Phi = \mathsf{C}_l = \{\pm e_i \pm e_j \mid 1 \leqslant i, j \leqslant l, i \neq j\} \cup \{\pm 2e_i \mid 1 \leqslant i \leqslant l\}$ 且 $\alpha = e_1 + e_2$ 的情形下，若 $g \in C_G(\Gamma_\alpha)$，则

$$g = cx_{e_1+e_2}(t_1)x_{2e_1}(t_2)x_{2e_2}(t_3), \quad c \in Z(G).$$

证明。我们将环 R 嵌入其关于极大理想的所有局部化所成的笛卡尔积中:

$$R \subset \widetilde{R} = \prod_{\mathfrak{m} \text{ is a maximal ideal of } R} R_{\mathfrak{m}}.$$

相应地，切瓦莱群 $G = G_\pi(\Phi, R)$自然嵌入切瓦莱群

$$\widetilde{G} = G_\pi(\Phi, \widetilde{R}) = \prod_{\mathfrak{m} \text{ is a maximal ideal of } R} G_\pi(\Phi, R_{\mathfrak{m}}).$$

~假设某个 $g \in G$ 与集合 Γ_α中的所有元素都交换。由于 $G \subset G$，我们有$g \in \prod_{\mathfrak{m}} G_\pi(\Phi, R_{\mathfrak{m}})$，并且可以将 g表示为 $g = (g_{\mathfrak{m}})_{\mathfrak{m} \in \mathfrak{M}}$, $g_{\mathfrak{m}} \in G_\pi(\Phi, R_{\mathfrak{m}})$，其中 $\mathfrak{M}$是 R的所有极大理想的集合。

由于对于任意不同的极大理想 $\mathfrak{m}_1$ 和 $\mathfrak{m}_2$ ，若 $x = (x_{\mathfrak{m}})_{\mathfrak{m} \in \mathfrak{M}}$，其中 $x_{\mathfrak{m}} = e_{R_{\mathfrak{m}}}$ 对所有$\mathfrak{m} \neq \mathfrak{m}_1$ 成立，且 $y = (y_{\mathfrak{m}})_{\mathfrak{m} \in \mathfrak{M}}$，其中 $y_{\mathfrak{m}} = e_{R_{\mathfrak{m}}}$ 对所有 $\mathfrak{m} \neq \mathfrak{m}_2$成立，则这些 x 和 y 交换，于是$[g, \Gamma_\alpha] = 1$ 推出

$$\forall \mathfrak{m} \in \mathfrak{M} \, \forall \beta \in \Gamma_\alpha \; [g_{\mathfrak{m}}, x_\beta(1_{R_{\mathfrak{m}}})] = e_{G_{\mathfrak{m}}}.$$

~因此，如果 g 属于整个切瓦莱群 G中集合 Γ_α 的中心化子，那么它的每个分量 $g_{\mathfrak{m}}$ 都属于相应集合的中心化子

$$\Gamma_{\alpha,\mathfrak{m}} = \{x_\beta(1_{R_{\mathfrak{m}}}) \mid [x_\beta(1_{R_{\mathfrak{m}}}), x_\alpha(1_{R_{\mathfrak{m}}})] = e\}.$$

由于所有 $R_{\mathfrak{m}}$ 都是局部环，由上一节可知，

$$\forall \mathfrak{m} \in \mathfrak{M} \; g_{\mathfrak{m}} = x_\alpha(t_{\mathfrak{m}}) \cdot C_{\mathfrak{m}}, \text{ where } t_{\mathfrak{m}} \in R_{\mathfrak{m}} \text{ and } C_{\mathfrak{m}} \in Z(G_\pi(\Phi, R_{\mathfrak{m}}))$$

（或者在 C_l, $l \geqslant 2$ 的情况下，

$$\forall \mathfrak{m} \in \mathfrak{M} \; g_{\mathfrak{m}} = x_{e_1+e_2}(t_{\mathfrak{m}})x_{2e_1}(r_{\mathfrak{m}})x_{e_2}(s_{\mathfrak{m}}) \cdot C_{\mathfrak{m}}, \text{ where } t_{\mathfrak{m}}, r_{\mathfrak{m}}, s_{\mathfrak{m}} \in R_{\mathfrak{m}} \text{ and } C_{\mathfrak{m}} \in Z(G_\pi(\Phi, R_{\mathfrak{m}})).$$

这意味着

$$g = (x_\alpha(t_{\mathfrak{m}}) \cdot C_{\mathfrak{m}})_{\mathfrak{m} \in \mathfrak{M}} = x_\alpha(t) \cdot C, \text{ where } t \in \widetilde{R} \text{ and } C \in Z(\widetilde{G})$$

（或在 C_l, $l \geqslant 2$ 的情况下，

~ ~$g = (x_{e_1+e_2}(t_{\mathfrak{m}})x_{2e_1}(r_{\mathfrak{m}})x_{e_2}(s_{\mathfrak{m}}) \cdot C_{\mathfrak{m}})_{\mathfrak{m} \in \mathfrak{M}} = x_{e_1+e_2}(t)x_{e_1}(r)x_{2e_2}(s) \cdot C$，其中 t、 r、 $s \in R$和 $C \in Z(G)$ 定理已完全证明。 ■

5. Diophantine structure in large subgroups of Chevalley groups $G_\pi(\Phi, R)$

本节证明，切瓦莱群的许多重要子群都是丢番图的。我们会直接使用预备知识中的记号。

5.1. 单参数子群 X_α 在 $G_\pi(\Phi, R)$ 的大子群中是丢番图的。我们先给出以下关键结果。

命题 3. 设 G 是 $G_\pi(\Phi, R)$ 的大子群，其中 Φ 是秩为 $\ell > 1$ 的不可分解根系，$\Phi \neq \mathsf{C}_2$，R 是任意带单位元的交换环。则对任意根 $\alpha \in \Phi$，子群 X_α 在 G 中是丢番图的（由常数 $\mathbf{x} = \{x_\beta(1) \mid \beta \in \Phi\}$ 定义）。

证明. 根据定理 3，对于除 C_ℓ 以外的所有根系 $\ell \geqslant 2$，任意 $\alpha \in \Phi$ 均有

$$C_G(\Gamma_\alpha) = X_\alpha \cdot Z(G),$$

其中 $Z(G)$ 是群 G 的中心。

在所有秩为 > 1 的根系 $\Phi \neq \mathsf{C}_\ell$ 中，都存在两个根 α 和 β，它们共同构成根系 A_2 的基。

因此，

$$X_{\alpha+\beta} = [C_G(\Gamma_\alpha), x_\beta(1)],$$

所以子群 $X_{\alpha+\beta}$ 在 G 中是丢番图的。

1. 根系 A_ℓ、D_ℓ、E_ℓ、F_4。由于所有等长根在群 W 的作用下均共轭，我们现在证明，对于根系 A_ℓ、D_ℓ、E_ℓ、F_4，所有子群 X_α、$\alpha \in \Phi$ 都是 G 中的丢番图子群；对于根系 G_2 以及 B_ℓ、$\ell \geqslant 3$，子群 X_α、α 是长根，且在 G 中是丢番图的。

2. 根系 G_2。在 $\Phi = \mathsf{G}_2$ 的情形下，所有切瓦莱群都是伴随的，因此它们的中心总是平凡的（见 [4]）。所以对于 G_2，对所有 $\alpha \in \Phi$，都有 $C_G(\Gamma_\alpha) = X_\alpha$。

3. 根方程组 $\mathsf{B}_\ell, \ell \geqslant 3$。对于 B_ℓ, $\ell \geqslant 3$ 的情形，我们已经证明，所有长根 α 的 X_α 以及所有短根 β 的 $X_\beta Z(G)$ 在 G 中都是丢番图的。取两个根 $\alpha, \beta \in \Phi$，其中 α 是长根，β 是短根，且它们构成方程组 B_2。

因为

$$[x_\alpha(t), x_\beta(1)] = x_{\alpha+\beta}(\pm t) x_{\alpha+2\beta}(\pm t), \quad \alpha+\beta \text{ is short}, \alpha+2\beta \text{ is long},$$

令 $w \in W$ 使得 $w(\alpha) = \alpha + 2\beta$，为确保起见，设两个符号均为 $+$，那么

$$X_{\alpha+\beta} Z(G) \cap [X_\alpha, x_\beta(1)] \cdot X_{\alpha+2\beta}$$

恰好是 $X_{\alpha+\beta}$。因此 $X_{\alpha+\beta}$，然后 X_β 是 G 中两个丢番图集的交集。

4. 根系 $\mathsf{C}_\ell, \ell \geqslant 3$。现在我们只需要证明关于根系 $\Phi = \mathsf{C}_\ell$, $\ell \geqslant 3$ 的结论。在这个方程组中

$$C_G(\Gamma_{e_1-e_2}) = X_{e_1-e_2} X_{2e_1} X_{-2e_2} C,$$

and

$$[x_{e_1-e_2}(t) x_{2e_1}(r) x_{-2e_2}(s) c, x_{e_2-e_3}(1)] = x_{e_1-e_3}(t) x_{-e_2-e_3}(s) x_{-2e_3}(s),$$

之后

$$[x_{e_1-e_3}(t) x_{-e_2-e_3}(s) x_{-2e_3}(s), x_{e_1+e_2}(1)] = x_{e_1-e_3}(s),$$

因此

$$[[C_G(\Gamma_{e_1-e_2}), x_{e_2-e_3}(1)], x_{e_1+e_2}(1)] = X_{e_1-e_3},$$

因此， X_α 对任意短 $\alpha \in \Phi$ 都是 G中的丢番图集。

现在我们知道， $X_\alpha \cdot Z(G)$ 对任意长 $\alpha \in \Phi$，以及 X_β 对任意短 $\beta \in \Phi$，都是 G中的丢番图集。我们再次取两个根 α、$\beta \in \Phi$，其中 α 是长根， β 是短根，且它们构成系统 $\mathsf{C}_2 = \mathsf{B}_2$。那么集合

$$X_{\alpha+2\beta} = X_{\alpha+2\beta} Z(G) \cap [X_\alpha Z(G), x_\beta(1)] \cdot X_{\alpha+\beta}$$

是 G中的丢番图集，因为它是两个丢番图集的交集。 ■

命题 4. 设 G 是 $G_\pi(\mathsf{C}_2, R)$, $\mathsf{C}_2 = \{\pm e_1 \pm e_2, \pm 2e_1, \pm 2e_2\}$ 的一个大子群，其中R 是任意含幺交换环，且 $\pi = \mathsf{ad}$ 或 $1/2 \in R$。那么对每个$\gamma \in \Phi$ ，子群 X_γ 都是 G中的丢番图集。

证明。情形 1. 如果我们的切瓦莱群是伴随的（$\pi = \mathsf{ad}$），那么它的中心是平凡的。对于任意长根 $\gamma \in \Phi$，我们知道 $X_\gamma = X_\gamma Z(G) = C_G(\Gamma_\gamma)$ 是 G中的丢番图集。

Let

$$[x_{2e_1}(t), x_{e_2-e_1}(u)] = x_{e_1+e_2}(\pm tu) x_{2e_2}(\pm tu^2),$$

例如

$$[x_{2e_1}(t), x_{e_2-e_1}(u)] = x_{e_1+e_2}(tu) x_{2e_2}(tu^2).$$

此外，假设对于 $w \in W$，有 $w(2e_1) = 2e_2$。那么

$$X_{e_1+e_2} = \{[y, x_{e_2-e_1}(1)] \cdot w y^{-1} w^{-1} \mid y \in X_{2e_1}\}.$$

因此，对于所有短根 $\gamma \in \Phi$， X_γ 在 G 中都是丢番图的。

情形 2. 假设 $1/2 \in R$。如上所述，我们将利用这一点：对于任意长根 $\gamma \in \Phi$，集合 $X_\gamma Z(G)$ 在 G 中是丢番图的。根据前一种情形，显然对于任意短根，集合 $X_\gamma Z(G)$ 在 G 中也是丢番图的。接着利用关系

$$[x_{e_1+e_2}(t), x_{e_2-e_1}(u)] = x_{2e_2}(\pm 2tu).$$

我们有

$$[X_{e_1+e_2} Z(G), x_{e_2-e_1}(1/2)] = X_{2e_2},$$

t因此 X_γ 是丢番图的 hantine in G f或任意 long γ，一d as in the 情形 1 f或任意 s hort root γ. ■

在情形 C_2 中， $\pi = sc$, $1/2 \notin R$ 我们需要特殊辅助集 Y 是丢番图的。

命题 5. 设 G 是 $G_{sc}(\mathsf{C}_2, R)$ 的一个大子群，其中 R 是一个不含 $1/2$ 的任意交换环。则子群 $Y_{e_1+e_2} = \{x_{e_1+e_2}(t) x_{2e_2}(t) \mid t \in R\}$ 在 G 中是丢番图的。

证明。在 C_2 的情况下，我们知道

$$C_G(\Gamma_{\pm 2e_i}) = X_{\pm 2e_i} C, \quad i = 1, 2, \ C = Z(G)$$

and

$$C_G(\Gamma_{\pm e_1 \pm e_2}) = X_{\pm e_1 \pm e_2} X_{\pm 2e_1} X_{\pm 2e_2} C, \quad C = Z(G).$$

此外，我们还记得

$$[x_{2e_1}(t), x_{e_2-e_1}(u)] = x_{e_1+e_2}(\pm tu) x_{2e_2}(\pm tu^2),$$
$$[x_{e_1+e_2}(t), x_{e_2-e_1}(u)] = x_{2e_2}(\pm 2tu).$$

因此

$$[C_G(\Gamma_{2e_1}), x_{e_2-e_1}(1)] = Y_{e_1+e_2}.$$

■

5.2. 切瓦莱群的初等子群可解释性。

定理 4. 设 G 是切瓦莱群 $G_\pi(\Phi, R)$ 的一个大子群，其中 Φ 是秩为 $\ell > 1$ 的不可分解根系，R 是任意含幺交换环。那么，环 R 在 G 中是 e-可解释的（使用来自集合 $C_\Phi = \{x_\alpha(1) \mid \alpha \in \Phi\}$ 的常数），对每个 X_α、$\alpha \in \Phi$ 均成立，但以下情形除外：$G = G_{sc}(\mathsf{C}_2, R)$，$1/2 \notin R$；在此情形下，$R$ 在 G 中关于命题 5 中的集合 Y_α 是 e-可解释的。

证明。需要考虑四种情形：
— A_2, 系统中的根；— G_2, 系统的短根；— $\mathsf{B}_2/\mathsf{C}_2$, 系统中的根，其中所有 X_α 都是丢番图的；— 以及具有集合 Y_α 的 C_2。

情形 1。假设我们有一个根系 $\mathsf{A}_2 = \langle \alpha, \beta \rangle$，并且想在 $X_{\alpha+\beta}$ 上解释环 R。我们将按如下方式把集合 $X_{\alpha+\beta}$ 变成一个环 $\langle X_{\alpha+\beta}, \oplus, \otimes \rangle$。

对于 $x, y \in X_{\alpha+\beta}$，我们定义

$$x \oplus y = x \cdot y.$$

注意，如果 $x = x_{\alpha+\beta}(a)$、$y = x_{\alpha+\beta}(b)$，那么 $xy = x_{\alpha+\beta}(a+b)$，这对应于 R 中的加法。

为给定的 x定义 $x \otimes y$，我们需要引入一些记号。设 x_1、$y_1 \in G$ 满足

$$x_1 \in X_\alpha \text{ and } [x_1, x_\beta(1)] = x; \quad y_1 \in X_\beta \text{ and } [x_\alpha(1), y_1] = y.$$

注意，这样的 x_1、y_1总是存在且唯一。若 $x = x_{\alpha+\beta}(a)$、$y = x_{\alpha+\beta}(b)$，则 $x_1 = x_\alpha(a)$、$y_1 = x_\beta(b)$。现在定义

$$x \otimes y := [x_1, y_1].$$

注意，在这种情况下

$$[x_1, y_1] = [x_\alpha(a), x_\beta(b)] = x_{\alpha+\beta}(ab).$$

因此，它对应于 R中的乘法。为完成证明，我们需要两个断言。

断言 1. 映射 $a \mapsto x_{\alpha+\beta}(a)$导出环同构 $R \to \langle X_{\alpha+\beta}, \oplus, \otimes \rangle$。由上面的论证可知，这一点显然成立。

断言 2. 环 $\langle X_{\alpha+\beta}, \oplus, \otimes \rangle$ 在 G中是 e-可解释的。

为了解这一点，首先观察到，正如上文所述，$X_{\alpha+\beta}$ 在 G 中是丢番图的。定义的加法显然在 G 中是丢番图的。由于子群 X_α 和 X_β 在 G 中是丢番图的，乘法 $\otimes$ 在 G 中也同样是丢番图的。这证明了情形 1。

情形 2. 假设我们想在系统 G_2 的某个短根上解释一个环 R。由于 G_2 的长根构成子系 A_2,，因此环 R 已经在所有 X_α 上解释出来了（这些都是长根 α），所以只需找到一个丢番图同构 $\mu\colon X_\alpha \to X_{\alpha+\beta}$，其中 α 是长根，而 β 是短根。

我们将使用该关系

$$[x_\alpha(t), x_\beta(u)] = x_{\alpha+\beta}(tu)x_{\alpha+3\beta}(-tu^3)x_{\alpha+2\beta}(-tu^2)x_{2\alpha+3\beta}(t^2u^3),$$

这表明

$$x_{\alpha+\beta}(t) = \mu(x_\alpha(t)) = X_{\alpha+\beta} \cap [x_\alpha(t), x_\beta(1)]X_{2\alpha+3\beta}X_{\alpha+3\beta}X_{\alpha+2\beta}.$$

由于 μ 是丢番图的，且 R 在 G 中关于 X_α是 e-可解释的，因此 R 在 G 中关于 $X_{\alpha+\beta}$ 也是 e-可解释的，进而对所有根而言，在所有 X_γ 中都是如此。

情形 3。现在我们来考虑根系 C_2, ，其中所有 X_γ、 $\gamma \in \Phi$ 都是丢番图的。当然，对于 x、$y \in X_\gamma$，我们定义

$$x \oplus y = x \cdot y$$

对于任意根 $\gamma \in \Phi$，它等价于 R 中的加法。

为了对给定的 x、$y \in X_\gamma$ 定义 $x \otimes y$，我们将从定义同构 μ 开始，它介于 X_α 与 $X_{\alpha+\beta}$ 之间，其中 α 是长根， β 和 $\alpha+\beta$ 是短根，并且 $\mu(x_\alpha(t)) = x_{\alpha+\beta}(t)$。

例如，可以通过以下方式确定这个同构 μ

$$x_{\alpha+\beta}(t) = \mu(x_\alpha(t)) = X_{\alpha+\beta} \cap [x_\alpha(t), x_\beta(1)] \cdot X_{\alpha+2\beta}.$$

现在，既然 μ 已定义，显然只需对一个 X_γ 定义运算 $\otimes$ 。我们将对 $\gamma = \alpha+\beta = e_1+e_2$ 进行定义。

设 x、$y \in X_{\alpha+\beta}$ 和 $x_1 \in X_\alpha$ 定义为 $\mu^{-1}(x)$， $y_2 \in X_\beta$ 为 $y^{w_{e_1}^{-1}}$。那么我们将 $x \otimes y$ 定义为

$$x \otimes y = X_{\alpha+\beta} \cap [x_1, y_2] \cdot X_{\alpha+2\beta}.$$

若 $x = x_{\alpha+\beta}(a)$，则 $x_1 = x_\alpha(a)$；若 $y = x_{\alpha+\beta}(b)$，则 $y_2 = x_\beta(b)$。在此情形下， $[x_1, y_2] = x_{\alpha+\beta}(ab) \cdot x_{\alpha+2\beta}(\pm ab^2)$，并且

$$X_{\alpha+\beta} \cap x_{\alpha+\beta}(ab) \cdot x_{\alpha+2\beta}(\pm ab^2) \cdot X_{\alpha+2\beta} = x_{\alpha+\beta}(ab).$$

因此，环 $\langle X_{\alpha+\beta}, \oplus, \otimes \rangle \cong R$ 可在 G 中 e-可解释。

情形 4. 若 $\Phi = \mathsf{C}_2$，且集合 X_α 不是 G 中的丢番图集合，则根据命题 5，子群 $Y_{e_1+e_2} = \{x_{e_1+e_2}(t)x_{2e_2}(t) \mid t \in R\}$ 是 G 中的丢番图集合。

我们在 $Y_{e_1+e_2}$ 上对 R 进行 e-解释，将其转化为环 $\langle Y_{e_1+e_2}, \oplus, \otimes \rangle$ ，如下所示。

对于 $x, y \in Y_{e_1+e_2}$ ，我们定义

$$x \oplus y = x \cdot y.$$

注意，如果 $x = x_{e_1+e_2}(a)x_{2e_2}(a)$， $y = x_{e_1+e_2}(b)x_{2e_2}(b)$，那么

$$xy = x_{e_1+e_2}(a)x_{2e_2}(a)x_{e_1+e_2}(b)x_{2e_2}(b) = (x_{e_1+e_2}(a)x_{e_1+e_2}(b))(x_{2e_2}(a)x_{2e_2}(b)) = x_{e_1+e_2}(a+b)x_{2e_2}(a+b),$$

这对应于 R中的加法。

要为给定的 $x, y \in Y_{e_1+e_2}$ 定义 $x \otimes y$，我们需要使用一些技巧。

首先，令 $x_1 \in G$ 满足

$$x_1 \in X_{2e_1}C = C(\Gamma_{2e_1}) \text{ and } [x_1, x_{e_2-e_1}(1)] = x.$$

注意，如果 $x = x_{e_1+e_2}(a)x_{2e_2}(a)$，那么必有 $x_1 = x_{2e_1}(a)c$, $c \in Z(G)$。

其次，令 y_2 为

$$y^{w_{2e_1}(1)} = x_{\mathbf{w}_{2e_1}(e_1+e_2)}(b)x_{\mathbf{w}_{2e_1}(2e_2)}(b) = x_{e_2-e_1}(b)x_{2e_2}(b).$$

我们看到

$$[x_1, y_2] = [x_{2e_1}(a), x_{e_2-e_1}(b)x_{2e_2}(b)] = [x_{2e_1}(a), x_{e_2-e_1}(b)] = x_{e_2+e_1}(ab)x_{2e_2}(ab^2).$$

如果我们设

$$x \otimes y := ([x_1, y_1]C(\Gamma_{2e_2}) \cap Y_{e_1+e_2}) = x_{e_1+e_2}(ab)x_{2e_2}(ab),$$

因为 $[x_1, y_1]C(\Gamma_{2e_2}) = x_{e_2+e_1}(ab)x_{2e_2}(t)c$, $t \in R$, $c \in Z(G)$。

因此，情形 4 也得以完成。 ■

现在我们证明定理 4 的逆命题。我们相信，这一结果在民间已广为人知。

命题 6. 所有切瓦莱群 $G_\pi(\Phi, R)$，其中 R 是任意交换环，都可以在 R 中进行 e-可解释（不使用来自 R 的常数，整数除外）。

证明. 我们用 n^2-元组 $\overline{x}$ 来表示一个元素属于 R 的 $n \times n$矩阵 $x = (x_{ij})$，其中

$$\overline{x} = (x_{11}, \dots, x_{1n}, x_{21}, \dots, x_{n1}, \dots, x_{nn}).$$

元组 R^n 上的矩阵乘法 $\otimes$ 定义如下：

$$\overline{x} \otimes \overline{y} = \overline{z} \iff \bigwedge_{i,j=1}^{n} z_{ij} = P_{ij}(\overline{x}, \overline{y}),$$

其中 $P_{ij}(\overline{x}, \overline{y})$ 是整数多项式 $\sum_{k=1} x_{ik} y_{kj}$。乘法 $\otimes$ 显然是丢番图的。要完成在 R 中对群 $G_\pi(\Phi, R)$ 的解释，只需用丢番图公式定义 R^{n^2} 的相应子集。

但根据切瓦莱群的定义，这一点显然成立：它们都是由有限个带整数系数的多项式方程组定义的。 ■

我们无法证明，对于任意交换环 R，初等切瓦莱群 $E_\pi(\Phi, R)$ 在 R 中是 e-可解释的。

然而，以下结论成立。

定理 5. 如果初等切瓦莱群 $E_\pi(\Phi, R)$ 具有有界初等生成，那么 $E_\pi(\Phi, R)$ 可以在 R 中进行 e-解释。

6. Diophantine problem in Chevalley groups

本节研究环上的切瓦莱群中的丢番图问题。我们的论证通常与经典线性群中的相应论证相似，因此我们要么不加证明地陈述结果并请读者参阅 [77]，要么给出证明的简短概述。

6.1.一般约化。我们在此考虑形如 $\mathcal{D}_C(G_\pi(\Phi, R))$ 的丢番图问题，其中 C 是 $G_\pi(\Phi, R)$ 的一个可数子集，并配备了一个枚举 $\nu\colon \mathbb{N} \to C$。记 R_C 为 R 中所有出现在 C的矩阵里的元素所组成的集合。枚举 ν 产生一个枚举 $\mu : \mathbb{N} \to R_C$；要构造 μ，只需按照 ν 枚举 C中的矩阵，对每个矩阵 $\nu(n)$ 按某个固定顺序枚举其条目，并将所有这些枚举合并为一个枚举 μ。

现在我们可以证明本文的主要结果。

定理 6. 若 Φ 是秩为 > 1 的不可分解根系， R 是任意含幺交换环，则任意切瓦莱群 $G_\pi(\Phi, R)$ 中的丢番图问题与 R 中的丢番图问题卡普等价。更确切地说：

1) 若 C 是 $G_\pi(\Phi, R)$ 的可数子集，则 $\mathcal{D}_C(G_\pi(\Phi, R))$ 卡普归约到 $\mathcal{D}_{R_C}(R)$。2) 若 T 是 R 的可数子集，则存在 $G_\pi(\Phi, R)$ 的可数子集 C_T，使得 $\mathcal{D}_T(R)$ 卡普归约到 $\mathcal{D}_{C_T}(G_\pi(\Phi, R))$.

证明。1）直接由命题 6 得出（参见 [77]中的引理 7.1）。2）由定理 4 得出。 ■

定理 7。设 Φ 是一个秩为 >1 的不可分解根系，且 R 是任意含幺交换环。如果初等切瓦莱群 $E_\pi(\Phi, R)$ 具有有界初等生成，那么 $E_\pi(\Phi, R)$ 中的丢番图问题与 R中的丢番图问题卡普等价。

证明。结论由定理 5 得出。 ■

6.2. 代数整数环和数域上的切瓦莱群中的丢番图问题。数域 F 指的是 $\mathbb{Q}$的有限代数扩张。数域 F 的代数整数环 $\mathcal{O}_F$ 是 F 的子环，由所有具有整数系数的首一多项式的根组成。

这是一个经典结果： $\mathbb{Z}$ 中的丢番图问题是不可判定的 [75]。

定理 8（与 [77]中的定理 7.2 比较）。若 Φ 是秩为 >1 的不可分解根系，则所有切瓦莱群 $G_\pi(\Phi, \mathbb{Z})$中的丢番图问题与 $\mathbb{Z}$中的丢番图问题卡普等价；特别地，它是不可判定的。

以下是数论中的一个重要猜想。

猜想 1. $\mathbb{Q}$中的丢番图问题，以及任意数域 F或任意代数整数环 $\mathcal{O}$中的丢番图问题，都是不可判定的。

对于 $\mathbb{Q}$ 及其任意有限扩张 F，上述猜想仍悬而未决。然而，对于域 F 的代数整数环 $\mathcal{O}_F$，已有结果证实丢番图问题具有不可判定性。具体而言，已知当[F 满足以下条件时， $\mathbb{Z}$ 在 $\mathcal{O}_F$ 中是丢番图的： $\mathbb{Q}] = 2$，或者 F 是全实的 [33, 35], ；或者 $[F:\ \mathbb{Q}] > 3$，且 F 在复数域 [84], 中恰有两个非实嵌入；或者 F 是阿贝尔数域 [96]。关于这一问题的详情，请参阅两篇综述和一本著作 [83, 85, 95] 。

以下结果将数域或代数整数环上切瓦莱群中的丢番图问题，从群论转移到了数论。

定理 9. 设 Φ 是秩为 >1 的不可分解根系，且 R 是数域或代数整数环。则猜想 1 对 R 成立，当且仅当切瓦莱群 $G_\pi(\Phi, R)$中的丢番图问题不可判定。

6.3. 有限生成交换环上的切瓦莱群中的丢番图问题。为了继续讨论，我们需要回顾一些定义。

带乘法单位元的环（即含幺环）的特征，是满足 $1 + \overset{n}{\ldots} + 1 = 0$ 的最小正整数 n。环 R 的秩，是指将 R 视为阿贝尔群（即忽略其乘法运算）时的秩：也就是说，非零元素 $r_1, \ldots, r_m \in R$ 的最大个数为 m，并且只要对于某些整数 $r_1, \ldots, r_m$ 有 $a_1 r_1 + \cdots + a_m r_m = 0$，就有 $r_i a_i = 0$ 对所有 $i = 1, \ldots, m$ 成立。如果 R 是整环，那么当 R 的特征 p 为正时，其秩与其作为 $\mathbb{F}_p$-向量空间的维数一致；否则，秩与将 R 视为 $\mathbb{Z}$-模时的维数一致。

以下结果引自 [47] ，描述了有限生成交换环中丢番图问题的现状。请注意，在 [33, 34] 中，Denef 证明了系数取自整环的多项式环中的丢番图问题是不可判定的。

定理 10（[47]）。设 R 是一个无限的有限生成结合交换含幺环。那么下列情况之一成立：

（1）如果 R 的特征为正特征 $n>0$，那么对于某个超越元 t 和某个素数 p，多项式环 $\mathbb{F}_p[t]$ 在 R 中 e-可解释；并且 $\mathcal{D}$（R）不可判定。（2）如果 R 的特征为零且秩无限，那么上述相同结论成立：对于某个 t 和 p，多项式环 $\mathbb{F}_p[t]$ 在 R 中 e-可解释；并且 $\mathcal{D}$（R）不可判定。（3）如果 R 的特征为零且秩有限，那么代数整数环 $\mathcal{O}$ 在 R 中 e- 可解释。

这与定理 6 一起推出以下结果，彻底阐明了无限有限生成交换含幺环上的切瓦莱群丢番图问题的情况。

定理 11. 设 Φ 是秩为 >1 的不可分解根系， R 是任意无限有限生成含幺交换环，且 $G_\pi(\Phi, R)$ 是相应的切瓦莱群。则：

1) 如果 R 具有正特征，那么 $G_\pi(\Phi, R)$中的丢番图问题是不可判定的。2) 如果 R 具有零特征且其秩为无限秩，那么$G_\pi(\Phi, R)$中的丢番图问题是不可判定的。3) 如果 R 具有零特征且其秩为有限秩，那么某个代数整数环 $\mathcal{O}$ 中的丢番图问题可 Karp 归约到 $G_\pi(\Phi, R)$中的丢番图问题。因此，如果猜想 1 成立，那么 $G_\pi(\Phi, R)$中的丢番图问题是不可判定的。

6.4. 代数闭域上的切瓦莱群中的丢番图问题。设R 是一个代数闭域。我们需要以下已知结果（详见 [77] 及其中的参考文献），其中 R 。

1) 若 A 是 R 的可计算子域，则语言中带有来自 A 的常数的 R 的一阶理论 $Th_A(R)$是可判定的。特别地，丢番图问题 $\mathcal{D}_A(R)$是可判定的。¯2) 若 A是 R 的可计算子域，则 A在 R 中的代数闭包 A 是可计算的。

定理 12. 设 Φ 是秩为 >1的不可分解根系， R 是一个代数闭域， $G_\pi(\Phi, R)$是相应的切瓦莱群。若 A 是 R的可计算子域，则 $G_\pi(\Phi, R)$中的丢番图问题（常数来自 $G_\pi(\Phi, A)$）是可判定的（在对 $G_\pi(\Phi, A)$作适当枚举的条件下）。

6.5. 实数域上的切瓦莱群中的丢番图问题。设 $R=\mathbb{R}$为实数域， A为 $\mathbb{R}$的一个可数（或有限）子集。

我们对 $\mathbb{R}$ 上的切瓦莱群中的丢番图问题的处理，基于以下两个关于 $\mathbb{R}$ 中的丢番图问题的结果，这些结果广为人知。详情请参阅 [77]。

命题 7（[77], 命题 7.4）。设 A 为 $\mathbb{R}$的一个有限或可数子集。那么，当且仅当有序子域$F(A)$是可计算的时，A 上系数的 $\mathbb{R}$ 中的丢番图问题才是可判定的。此外，在这种情况下，整个一阶理论 $Th_A(\mathbb{R})$是可判定的。

回顾一下，如果实数 $a\in\mathbb{R}$ 的标准十进制展开 $a=a_0.a_1a_2\ldots$是可计算的，即整数函数 $n\mapsto a_n$ 是可计算的，那么该实数就是可计算的。换言之， a 是可计算的，当且仅当可以用任意精度的有理数对其进行有效逼近。所有

可计算实数 $\mathbb{R}^c$ 构成 $\mathbb{R}$的一个实闭子域，特别是 $\mathbb{R}^c$ 与 $\mathbb{R}$一阶等价。

在下面的 命题中，我们收集了关于 $\mathbb{R}$ 的可计算有序子域的一些事实 .

命题 8（[77], 命题 7.5）。以下结论成立：

1) 每个有序可计算子域都包含于 $\mathbb{R}$。 2) 带有从 $\mathbb{R}$ 诱导序的有序子域 $\mathbb{R}^c \leq \mathbb{R}$ 不可计算。 3) 若 F 是可计算有序域，则其实闭包也可计算。特别地，若 F 是 $\mathbb{R}$ 的可计算子域，则 F 在 $\mathbb{R}$ 中的代数闭包 F 是可计算有序域。 4) 若 a_1、.....、 a_m 是可计算实数，则带有从 $\mathbb{R}$ 诱导序的有序子域 $\mathbb{Q}(a_1, ..., a_m) \leq \mathbb{R}$ 是可计算的。

推论 3。以下结论成立：

- $\mathbb{R}$ 中系数取自 $\mathbb{R}^c$ 的丢番图问题不可判定；
- 在 $\mathbb{R}^c$ 的任意有限子集上取系数时， $\mathbb{R}$ 中的丢番图问题是可判定的；
- 当 a 不可计算时，在 $\{a\}$ 上取系数的 $\mathbb{R}$ 中的丢番图问题是不可判定的。

回顾一下，若矩阵 $A \in \mathrm{GL}_n(\mathbb{R})$ 的所有元素都是可计算实数，则称其为可计算矩阵。

切瓦莱群 $G_\pi(\Phi, \mathbb{R})$ 是 $\mathbb{R}$ 上的矩阵代数群，因此可以将其元素视为矩阵

定理 13. 设 Φ 是秩为 > 1 的不可分解根系， $G_\pi(\Phi, \mathbb{R})$ 是实数域 $\mathbb{R}$ 上的切瓦莱群。若 A 是 $\mathbb{R}$ 的可计算有序子域，则带有来自 $G_\pi(\Phi, A)$ 的常数的一阶理论 $Th(G_\pi(\Phi, \mathbb{R}))$ 是可判定的。特别地，在对 $G_\pi(\Phi, A)$ 进行适当枚举的条件下，带有来自 $G_\pi(\Phi, A)$ 的常数的 $G_\pi(\Phi, \mathbb{R})$ 中的丢番图问题是可判定的。

定理14。设 Φ 是秩为 > 1 的不可分解根系，且 $G_\pi(\Phi, \mathbb{R}^c)$是可计算实数域 $\mathbb{R}^c$ 上的 Chevalley 群。则以下结论成立：

1) 可计算群 $G_\pi(\Phi, \mathbb{R}^c)$ 中的丢番图问题是不可判定的。2) 对于 $G_\pi(\Phi, \mathbb{R}^c)$ 的任意有限生成子群 C，在 C 中取系数的 $G_\pi(\Phi, \mathbb{R}^c)$ 中的丢番图问题是可判定的。

我们称矩阵 $A \in \mathrm{GL}_n(\mathbb{R})$ 是可计算的，如果 A 中的所有条目都是可计算实数，即 $A \in \mathrm{GL}_n(\mathbb{R}^c)$。因此， $\mathrm{SL}_n(\mathbb{R})$ 中的可计算矩阵恰好是来自 $\mathrm{SL}_n(\mathbb{R}^c)$ 的矩阵。由于切瓦莱群 $G_\pi(\Phi, \mathbb{R})$ 的元素由来自 $\mathrm{SL}_n(\mathbb{R})$ 的矩阵表示，我们称元素 $g \in G_\pi(\Phi, \mathbb{R})$ 是可计算的，如果它由来自 $\mathrm{SL}_n(\mathbb{R}^c)$ 的可计算矩阵表示。

定理 15。设 Φ 是一个秩为 > 1 的不可分解根系，且 $G_\pi(\Phi, \mathbb{R})$ 是定义在实数域 $\mathbb{R}$ 上的相应切瓦莱群。如果元素 $g \in E_\pi(\Phi, \mathbb{R})$ 不可计算，则关于系数属于 $\{x_\alpha(1) \mid \alpha \in \Phi\} \cup \{g\}$ 的方程的丢番图问题，在 $G_\pi(\Phi, \mathbb{R})$ 的任意大子群中都是不可判定的。

6.6. p 进数上的切瓦莱群中的丢番图问题。与实数的情形类似，对于每个固定的素数 p，都可以定义可计算的 p 进数。回顾一下， that

每个 p-进数 $a \in \mathbb{Q}_p$ 都有唯一的表示形式 $a = p^m\xi$，其中 $m \in \mathbb{Z}$，而 ξ是环 $\mathbb{Z}_p$中的单位。反过来，单位 ξ 由自然数序列 $\{\xi(i)\}_{i\in\mathbb{N}}$唯一确定，其中

$$0 \le \xi(i) < p^{i+1},\ \xi(i+1) = \xi(i)(\bmod p^{i+1}),\ (i \in \mathbb{N}).$$

如果序列 $i \to \xi(i)$ 可计算，则 p进数 $a = p^m\xi$ 是可计算的。在这种情况下，序列 $\{\xi(i)\}_{i\in\mathbb{N}}$ 给出了 ξ 的有效 p进近似。众所周知（例如参见 [76]），所有可计算的 p进数构成 $\mathbb{Q}_p$ 的一个子域 $\mathbb{Q}_p^c$，使得 $\mathbb{Q}_p \equiv \mathbb{Q}_p^c$。还要注意，环 $\mathbb{Z}_p$ 在 $\mathbb{Q}_p$ 中是丢番图的。更确切地说，如果 $p \neq 2$, 则 $\mathbb{Z}_p$ 在 $\mathbb{Q}_p$ 中由公式 $\exists y(1 + px^2 = y^2)$ 定义；而如果 $p = 2$，则 $\mathbb{Z}_p$ 由公式 $\exists y(1 + 2x^3 = y^3)$ 定义（见 [41]）。

以下结果在 [76] 中得到了证明:

a) $Th(\mathbb{Z}_p, a_1, \ldots, a_n)$ 可判定，当且仅当 $a_1, \ldots, a_n$ 中的每一个都是可计算的 p进数。

b) $Th(\mathbb{Q}_p, a_1, \ldots, a_n)$ 可判定，当且仅当 $a_1, \ldots, a_n$ 中的每一个都是可计算的 p进数。

c) 如果一个 p进整数 a 不可计算，那么带有来自 $\mathbb{Q} \cup \{a\}$ 的常数的方程在 $\mathbb{Z}_p$ 中不可判定。 d) 如果一个 p进数 $a \in \mathbb{Q}_p$ 不可计算，那么带有来自 $\mathbb{Q}\cup\{a\}$ 的常数的方程在 $\mathbb{Q}_p$ 中不可判定。

定理 16。设 Φ 是一个秩为 > 1 的不可分解根系。则以下结论成立 :

1) 设 $a_1,\ldots, a_m \in \mathbb{Q}_p^c$ 且 $A = \mathbb{Q}(a_1,\ldots, a_m)$是由 $a_1, \ldots, a_m$ 生成的 $\mathbb{Q}_p$的子域。则带有来自 $G_\pi(\Phi, A)$ 的常数的一阶理论 $Th(G_\pi(\Phi, \mathbb{Q}_p))$ 是可判定的。特别地，带有来自 $G_\pi(\Phi, A)$ 的常数的 $G_\pi(\Phi, \mathbb{Q}_p)$ 中的丢番图问题是可判定的（在对 $G_\pi(\Phi, A)$进行适当枚举的条件下）。

2) 设 $a_1, \ldots, a_m \in \mathbb{Z}_p^c$ 且 $A = \mathbb{Z}(a_1,\ldots, a_m)$是由 $a_1, \ldots, a_m$ 生成的 $\mathbb{Z}_p$的子环。则带有来自 $G_\pi(\Phi, A)$ 的常数的一阶理论 $Th(G_\pi(\Phi, \mathbb{Q}_p))$ 是可判定的。特别地，带有来自 $G_\pi(\Phi, A)$ 的常数的 $G_\pi(\Phi, \mathbb{Q}_p)$ 中的丢番图问题是可判定的（在对 $G_\pi(\Phi, A)$ 进行适当枚举的条件下）。

证明。由定理 6 以及上面的结果 a) 和 b) 可得。 ■

如果矩阵 $A \in \mathrm{GL}_n(\mathbb{Q}_p)$ 的所有项 A 都是可计算的 p 进数，即 $A \in \mathrm{GL}_n(\mathbb{Q}_p^c)$，我们就称该矩阵为可计算矩阵。因此，$\mathrm{SL}_n(\mathbb{Q}_p)$ 中的可计算矩阵恰好是来自 $\mathrm{SL}_n(\mathbb{Q}_p^c)$ 的矩阵。由于切瓦莱群 $G_\pi(\Phi, \mathbb{Q}_p)$ 的元素由来自 $\mathrm{SL}_n(\mathbb{Q}_p)$ 的矩阵表示，我们称元素 $g \in G_\pi(\Phi, \mathbb{Q}_p)$ 为可计算的，如果它由来自 $\mathrm{SL}_n(\mathbb{Q}_p^c)$ 的可计算矩阵表示。类似地，我们定义切瓦莱群 $G_\pi(\Phi, \mathbb{Z}_p)$ 中的可计算元素。

定理 17. 设 Φ 是秩为 > 1 的不可分解根系，且 $G_\pi(\Phi, \mathbb{Q}_p)$（$G_\pi(\Phi, \mathbb{Z}_p)$ $p \neq 2$）是其在 $\mathbb{Q}_p$ （$\mathbb{Z}_p$）上的相应切瓦莱群。若元素 $g \in E_\pi(\Phi, \mathbb{Q}_p)$（$g \in E_\pi(\Phi, \mathbb{Z}_p)$ $p \neq 2$）不可计算，则对于系数属于 $\{x_\alpha(1) \mid \alpha \in \Phi\} \cup \{g\}$ 的方程，丢番图问题在 $G_\pi(\Phi, \mathbb{Q}_p)$（$G_\pi(\Phi, \mathbb{Z}_p)$ $p \neq 2$）的任意大子群中都是不可判定的。

References

[1] Abe E. 局部环上的切瓦莱群。《东北数学杂志》，21(3)，1969，474–494。[2] Abe E. 交换环上切瓦莱群的正规子群。《当代数学》，83，1989，1–17。[3] Abe E., Suzuki K. 关于交换环上切瓦莱群的正规子群。《东北数学杂志》，28(1)，1976，185–198。[4] Abe E., Hurley J. 交换环上切瓦莱群的中心。《通信代数》，1988，16(1)，57–74。[5] Ax J., Kochen S. 局部域上的丢番图问题。I、II。《美国数学杂志》，1965，87，605–648。[6] Ax J., Kochen S. 局部域上的丢番图问题。III。《美国数学杂志》，1966，83，437–456。[7] Avni N., Lubotzky A., Meiri C. 非一致高秩算术群的一阶刚性。《数学发明》，217(1)，2019，219–240。[8] Avni N., Meiri C. 关于高秩算术群的模型论。arXiv:2008.01793，2022。[9] Beidar C.I., Mikhalev A.V. 关于线性群初等等价性的马尔采夫定理。《当代数学》，131(1)，1992，29–35。[10] Belegradek O. V. 单位上三角群的模型论。《纯粹与应用逻辑年刊》，1994，68，225–261。[11] Borel A. 切瓦莱群的性质与线性表示。《代数群研讨班》，M.，1973，9–59。[12] Bragin V., Bunina E. 有限多个中心幂等元的环上及布尔环上线性群的初等等价性。《数学科学杂志》，201，2014，438–445。[13] Bourbaki N. 群与李代数。Hermann，1968。 Ź Bunina E. 环与斜域上的酉线性群的初等等价性。《俄罗斯数学调查》，53(2)，1998，137–138。[14] Bunina E., Mikhalev A.V. 线性群与切瓦莱群的组合与逻辑方面。《应用数学学报》，85(1–3)，2005，57–74。[15] Bunina E. 域上切瓦莱群的初等等价性。《数学科学杂志》，152，2008，155–190。[16] Bunina E. 局部环上切瓦莱群的初等等价性。《数学文集》，201(3)，2010，321–337。[17] Bunina E. 交换环上不同类型切瓦莱群的自同构。《代数杂志》，355(1)，2012，154–170。[18] Bunina E. 交换环上切瓦莱群的同构与初等等价性。《数学文集》，210(8)，2019，1067–1091。[19] Bunina E. 局部环上切瓦莱群的正则双重可解释性。Arxiv.org/abs/2208.13623，2022。[20] Carter R.W. 李型单群，第 2 版。Wiley，伦敦等地，1989。[21] Casals-Ruiz M., Kazachkov I. 关于群的自由积上的方程组。《代数杂志》，2011，333(1)，368–426。[22] Casals-Ruiz M., Kazachkov I. 关于自由部分交换群上的方程组。《美国数学会回忆录》，2011，美国数学会。[23] Ciobanu L., Diekert V., Elder M. 自由群上方程的解集是 EDT0L 语言。《国际代数与计算杂志》，2016，26(5)，843–886。[24] Ciobanu L., Elder M. 双曲群中方程解集的复杂度，arXiv:2001.09591[25] math.GR[。]Chang C., Keisler H. 模型论。North Holland，1990。[26] Chevalley C. 半单群的某些概形。布尔巴基研讨班，219，1960–1961，1–16。[27] Cohn P. 关于环的[28] 的结构。《高等科学研究所数学出版物》，30，1966，365–413。 GL_2 Dahmani F., Guirardel V. 用叶状结构求解群中的方程：自由群、几乎自由群与双曲群。《拓扑学杂志》，2016，3(2)，343–404。[29] Davis M., Putnam H., Robinson J. 指数丢番图方程的判定问题。《数学年刊》，74(3)，1961，425–436。[30] Demazure M., Gabriel P. 代数群。I. North Holland，阿姆斯特丹等地，1970，1–770。[31] Denef J., Lipshitz L. 某些代数整数环上的丢番图集。《伦敦数学会杂志》，1978，18(3)，385-391。 Ź J. Denef，二次环上的希尔伯特第十问题。《美国数学会会刊》48（1975），214-220。

[34] J. Denef，正特征多项式环上的丢番图问题，载于：Logic Colloquium ’78，North-Holland，1979，131–145。[35] J. Denef，代数整数的丢番图集，II，《美国数学会汇刊》257，1980，227–236。[36] Diekert V., Jez A., Plandowski W. 求解自由群和带对合幺半群中方程的所有解。《信息与计算》，2016，251，263–286。[37] Diekert V., Lohrey M. 图积上的字方程。《代数与计算国际杂志》，2008，18(3)，493–533。[38] Diekert V., Muscholl A, 图群中的方程可解性是可判定的。《代数与计算国际杂志》，2006，16(6)，1047–1069。[39] Duchin M., Liang H., Shapiro M. 幂零群中的方程。《美国数学会会刊》，2015，143(11)，4723–4731。[40] Ershov Yu. 关于局部域的初等理论。Algebra i Logika，Sem 4，1965，2，5–30。[41] Ershov Yu. 可判定性问题与可构造模型。莫斯科，Nauka，1980。[42] Ershov Yu. 域论的算法问题（积极方面）。《数理逻辑手册》，1982，3，268–353，Nauka。[43] Ershov Yu., Goncharov S. 构造模型。西伯利亚代数与逻辑学派。Consultants Bureau，纽约，2000。[44] Garreta A., Miasnikov A., Ovchinnikov D. 满秩表示与幂零群：结构、丢番图问题与泛性质。《代数杂志》，2020，556，1–34。[45] Garreta A., Miasnikov A., Ovchinnikov D. 可解群中的丢番图问题。《数学科学通报》，2020，10(1)，DOI：10.1142/S1664360720500058[46] Garreta A., Miasnikov A., Ovchinnikov D. 环与代数中的丢番图问题：不可判定性及归约到代数整数环，arXiv：1805.02573[47] Garreta A., Miasnikov A., Ovchinnikov D. 交换环中的丢番图问题，预印本。[48] Goncharov S. 可数布尔代数与可判定性。新西伯利亚：Science books，1996（俄文）。[49] Hazrat R., Vavilov N. K_1 切瓦莱群是幂零的。《纯粹与应用代数杂志》，179(1-2)，2003，99–116。[50] Hodges W. 模型论。剑桥大学出版社，剑桥，1993。[51] Humphreys J. 李代数与表示论导论。Springer–Verlag，纽约，1978。[52] Iwahori N., Matsumoto H. 关于某些布鲁哈分解以及 p进切瓦莱群的赫克环结构，高等科学研究所数学出版物，1965，25，5–48。[53] Jarden M., Lubotzky A. 有限群的初等等价。《伦敦数学会通报》，40(5)，887–896。[54] Jez A. 重新压缩：一种简单而强大的字方程技术。《美国计算机协会杂志》，63(1):4:1–4:51，2016，ISSN 0004-5411/2015。doi：10.1145/2743014。URL http://dx.doi.org/10.1145/2743014。[55] Jez A. 线性空间中的字方程。arXiv:1702.00736 [cs.FL][56] Keisler H.J. 超积与初等模型。Indagationes Mathematicae，23，1961，477–495。[57] Kharlampovich O., Myasnikov A. 自由群上的不可约仿射簇。II：三角准二次形式中的方程组与剩余自由群的描述。《代数杂志》，1998，200(2)，517–570。[58] Kharlampovich O., Myasnikov A. 群中的模型论与代数几何、非标准作用及算法问题。2014年国际数学家大会论文集，首尔，第2卷，特邀报告，223–244。[59] Kharlampovich O., Myasnikov A. 自由李代数中方程的不可判定性。《美国数学会汇刊》，2017，08 ??[60] Kharlampovich O., Myasnikov A. 代数中的方程。《代数与计算国际杂志》，2018，28(8)，1517–1533。[61] Kharlampovich O., Myasnikov A. 非阿贝尔自由群的初等理论。《代数杂志》，302，2006，451–552。[62] Kharlampovich O., Myasnikov A., Sohrabi M. 丰富群、弱二阶逻辑及其应用。arXiv:2109.13133v1，2021。[63] Khelif A. 双重可解释性与 QFA 结构： 可解群与交换环的研究。巴黎科学院报告，I辑，345，2007，59–61。

[64] Kopeiko V.I.，多项式环上的辛群的稳定化，《苏联数学文集》，1978，34，655-669。[65] Kunyavskii B.、Plotkin E.、Vavilov N.，切瓦莱群的有界生成与交换子宽度：函数情形。arXiv:2204.10951，2022。[66] Kunyavskii B.、Plotkin E.、Vavilov N. ???[67] Lasserre C. 多循环有限群与一阶语句。《代数杂志》，396，2013，18–38。[68] Makanin G. S. 自由群中的方程（俄文）。《苏联科学院学报，数学辑》，1982，46(1)，199–1273（译载于《苏联数学消息》，21，1983；MR 84m:20040）。[69] Makanin G. S. 自由群的全称理论与正理论的可判定性。《苏联科学院学报，数学辑》，1985，48(1)，735–749（译载于《苏联数学消息》，1985，25；MR 86c:03009）。[70] Maltsev A.I. 线性群的初等性质。《数学与力学问题》，莫斯科，1961（俄文）。[71] Maltsev A.I. 无限群的同构矩阵表示。《数学文集》 [Mat. Sbornik] 8(50)，1940，405–422（俄文，附英文摘要）。[72] Maltsev A.I. 构造性代数 I，《数学科学进展》，1961，3，3–60。[73] Marker D. 模型论：导论。Springer，2002。[74] Matsumoto H.，关于半单分裂 ′群的算术子群。 ′《高等师范学校科学年刊》，第四辑，2，1969，1–62。[75] Matijasevich Yu. 可枚举集合的丢番图性。《苏联科学院学报》，1970，191，279–282。[76] A. Myasnikov 和 V. Remeslennikov，递归 p 进数与有限生成 pro-p 群的初等理论，1988 美国数学会，《苏联数学消息》，第30卷，第3期。[77] Myasnikov A.、Sohrabi M. 经典矩阵群中的丢番图问题。《俄罗斯科学院学报，数学辑》，85(6)，2021，205–244。[78] Myasnikov A.、Sohrabi M. 与 $\mathbb{Z}$ 的双可解释性以及 SL$_n(\mathcal{O})$、GL $_n(\mathcal{O})$、 $T_n(\mathcal{O})$、 $n \geqslant 3$的完备初等理论的模型。arXiv:2004.03585，2020。[79] Myasnikov A. G.、Sohrabi M. 关于与三角矩阵群 $T_n(R)$ 初等等价的群，arXiv:1609.09802。[80] Nies A. 用一阶公式区分群类。《国际代数与计算杂志》，13，2003，287–302。[81] Nies A. 描述群。《符号逻辑通报》，13(3)，2007，305–339。[82] Oger F.、Sabbagh G. 拟有限公理化的幂零群。《群论杂志》，9(1)，2006，95–106。[83] Pheidas T.、Zahidi K. 环与域的存在理论的不可判定性：综述。《当代数学》，2000，270，49–106。[84] T. Pheidas，关于一类代数整数环的希尔伯特第十问题，《美国数学会会刊》104，1988，611–620。[85] B. Poonen，数论相关环上的希尔伯特第十问题，《亚利桑那冬季学校“数论与逻辑”讲义》，2003。[86] Poonen B. 数论相关环上的希尔伯特第十问题。《亚利桑那冬季学校“数论与逻辑”讲义》，2003。[87] Rabin M. 可计算代数、一般理论与可计算域理论，《美国数学会汇刊》，1960，95(2)，341–360。[88] Razborov A. 自由群中的方程组。《苏联数学消息》，1985，25(1)，115–162。[89] Razborov A. 自由群中的方程组。博士论文，斯捷克洛夫数学研究所，莫斯科，1987。[90] Rips E.、Sela Z. 双曲群中的典范代表与方程。《数学发明》，1995，120(1)，489–510。[91] Romankov V. 自由幂零群与自由环中的端同态可约性问题的不可解性。《代数与逻辑》，1977，16(4)，310–320。[92] Segal D.、Tent K. 定义 R 与 $G(R)$。arXiv:2004.13407，2020。[93] Sela Z. 群上的丢番图几何 VI. 自由群的初等理论。《几何与泛函分析》，16(3)，2016，707–730。

[94] Shelah S.，每两个初等等价的模型都有同构的超幂。《以色列数学杂志》，10，1971，224–233。[95] ShlapentokhA.《希尔伯特第十问题：丢番图类及其向整体域的扩展》。《新数学专著》，2007，剑桥大学出版社。[96] H. N.Shapiro，A. Shlapentokh，代数数域之间的丢番图关系，《纯粹与应用数学通讯》，42，8，1989，1113–1122。[97] SmolenskyA.，SuryB.，Vavilov N.重新审视切瓦莱群的高斯分解。《国际群论杂志》，2012，01(1)，3–16。[98] SteinM.R. 关于 K_2 及相关函子的零维满射稳定性。《美国数学会汇刊》，178(1)，1973，165–191。[99] Steinberg R.《切瓦莱群讲义》。耶鲁大学，1967。[100] Suslin A.A. 关于Cohn定理。《苏联数学杂志》，17(2)，1981，1801–1803。[101] SwanR. 某些特殊线性群的生成元与关系。《数学进展》，6，1971，1–77。[102] SzmielewW. 阿贝尔群的初等性质。《数学基础》，41，1955，203–271。[103] Taddei G. 环上的切瓦莱群中初等群的正规性。《当代数学》，55(II)，1986，693–710。[104] Tarski A.初等代数与几何的判定方法。第2版修订版，伯克利、洛杉矶，1951。[105] Vavilov N.A.交换环上的切瓦莱群的结构。非结合代数及相关主题会议论文集（广岛，1990），世界科学出版社，新加坡，1991，219–335。[106] Vavilov N.A.，Plotkin E.B. 交换环上的切瓦莱群：I. 初等计算。《应用数学学报》，45，1996，73–115。[107] ZilberB.I.代数闭域上单代数群的某些模型论。《数学学术讨论会》，2，1984，173–180。