arXiv:2305.05041v3 [math.NT] 8 Aug 2023

Chevalley-Bass 定理

Yuri Bilu*

2023 年 8 月 9 日版本

摘要

本文阐述了 Chevalley（1951 年）和 Bass（1965 年）提出的一个定理。设 K 是一个特征 0 的有限生成域。那么存在一个正整数 Λ，仅依赖于 K，使得对于每个正整数 n，以下结论成立：如果 $\alpha \in K$ 是分圆扩张 $K(\zeta_{\Lambda n})$ 中的 Λn^{th} 次幂，那么 α 就是 K 中的 n^{th} 次幂。

我们还给出了两类适用的 Λ 的显式表达式：一种用 K_{ab} 的最大阿贝尔子域 K 的次数表示，另一种用 K_{ab} 的判别式表示。

目录

1 引言 2 不可约性定理 3 素数幂情形 4 关键引理 **1**
5 定理 1.1 的证明 6 域的 Chevalley-Bass 数 **3**
3
5
5
8

1 引言

设 K 是一个数域，n 是一个正整数。许多丢番图问题都取决于以下问题：假设 $\alpha \in K$ 在分圆扩张 $K(\zeta_n)$ 中是一个 n^{th} 次幂；它在 K 中是否也是一个 n^{th} 次幂？用符号表示：$K(\zeta_n)^n \cap K = K^n$ 是否成立？

一般来说，这并不成立：$-4 = (1+i)^4$ 在 $\mathbb{Q}(i)$ 中是一个 4th 次幂，但在 $\mathbb{Q}$ 中不是。不过，一个稍弱的说法是成立的。对于特征 0 的域 K，我们用 K_{ab} 表示 K 的最大阿贝尔子域；也就是说，它是 K 中最大的子域，且是 $\mathbb{Q}$ 的阿贝尔扩张。

定理 1.1. *[Chevalley, Bass]* 设 K 为一个特征 0 的域，且具有如下性质

$$K_{\text{ab}} \text{ is a finite extension of } \mathbb{Q}. \tag{1.1}$$

*波尔多数学研究所，波尔多大学与法国国家科学研究中心（CNRS）；yuri@math.u-bordeaux.fr

那么存在一个正整数 Λ，使得对于每个正整数 n，以下结论成立：如果 $\alpha \in K$ 是 $K(\zeta_{\Lambda n})$ 中的一个 Λn^{th} 次幂，那么 α 就是 K中的一个 n^{th} 次幂。用符号表示：$K(\zeta_{\Lambda n})^{\Lambda n} \cap K \subset K^n$。

注意，假设 $[K_{\mathrm{ab}}$：当 $\mathbb{Q}] < \infty$为数域时显然成立。更一般地，当 K 为有限生成域时也成立，参见第[6, VIII]章中的练习 4。

素数幂 n 的情形归功于 Chevalley [3], ，且不需要假设 (1.1)。此外，如果我们限制于奇素数幂 n，则可以取 $\Lambda = 1$，参见下文第 3 节。在附加假设 $i \in K$下，n 为 2 的幂时同样适用。

Bass [2] 将 Chevalley 的工作推广到了任意 n；他所陈述的结果在形式上弱于定理 1.1，但他证明的实际上正是定理 1.1。Smith [9] 给出了 Bass 定理的一个非常简洁的证明，并纠正了一些不准确之处。在第 4 节和第 5 节中，我们遵循 Smith 的论证，并补充了一些细节。

注意，Bass 和 Smith 都假设 K 为数域。我们借鉴 Georges Gras [4]的建议，将他们的论证推广到了满足 (1.1) 的域这一更一般的情形。

本文纯属综述，不涉及真正的新思想。第 6 节的结果从形式上说是新的，但它们是利用非常标准的论证从前面各节的结果推导出来的。

致谢：感谢 Keith Conrad 向我介绍这一课题，并让我读到 Chevalley、Bass 和 Smith 的文章。衷心感谢 Georges Gras 对本文早期版本提出的启发性意见，以及与我进行的许多富有启发性的讨论。感谢 Denis Benois 提供有益的建议，也感谢 Peter M¨uller 向我介绍文章 [1] 和 [5]。

第 6 节中的计算使用 PARI [10]完成。感谢 PARI 团队，尤其感谢 Bill Allombert，感谢他们随时提供帮助。

2023年6月，我在波恩马克斯·普朗克数学研究所访问期间撰写了本文；感谢该研究所提供经费支持和良好的学术环境。

本研究部分受 ANR 项目 JINVARIANT 资助。

¯记号与约定 在本文中，K 是一个域，K 是 K的一个固定代数闭包。给定 $\alpha \in K$ 和一个正整数 n，我们用 αK^n 表示 K 中 n^{th} 次幂与 α相乘所得的集合：

$$\alpha K^n := \{\alpha\beta^n : \beta \in K\}.$$

¯对于不被 K 的特征整除的正整数 n，令 $\zeta_n \in K$ 为阶数为 n 的本原单位根。我们用 μ_n 表示阶数为 n 的单位根群 ¯，并将其视为由 ζ_n 生成的 $K^\times$ 的子群。我们使用（略显滥用的）记号 $i = \sqrt{-1} = \zeta_4$。

全文中，p 表示素数，m、n、r、s表示严格正整数。

2 不可约性定理

回顾以下著名的二项式不可约性判别准则；例如，参见 [6, 第六章]中的定理 9.1。

定理 2.1。设 K 是一个域，$\alpha \in K^\times$ 和 n 是一个正整数。假设对所有 $p \mid n$，都有 $\alpha \notin K^p$。若 $4 \mid n$，则还假设 $\alpha \notin -4K^4$。那么多项式 $X^n - \alpha$ 在 $K[X]$中不可约。

我们将通过以下推论使用这个定理。

推论 2.2。设 K 是一个域，p 是一个素数。若 $p = 2$ 且 $\operatorname{char} K \neq 2$，则假设 $i \in K$。设 $\alpha \in K$，但 $\alpha \notin K^p$。那么对任意正整数 s，多项式 $X^{p^s} - \alpha$ 在 $K[X]$中不可约。

推论 2.3。设 K 是一个域，p 是一个不同于 K特征的素数。设 $r \geq 2$ 满足 $\zeta_{p^{r-1}} \in K$，但 $\zeta_{p^r} \notin K$。那么 $K(\zeta_{p^r})$ 是 K 的一个伽罗瓦扩张，其次数为 p。

不过，这两个推论都是定理 2.1 的直接推论，但推论 2.2 中 $p = 2$ and $\operatorname{char} K \neq 2$ 的情形或许需要作些说明。在这种情况下，$-4 = (1+i)^4 \in K^4$。因此，$\alpha \notin K^2$ 蕴含 $\alpha \notin -4K^4$，定理 2.1 便适用。

3 素数幂情形

本节证明切瓦莱定理。

定理 3.1（Chevalley）。设 K 是一个域，p 是一个与 K 的特征不同的素数。设 n 是 p 的幂。假设当 $p = 2$ 时，$i \in K$。设 $\alpha \in K^\times$ 满足 $\alpha \in K(\zeta_n)^n$。则 $\alpha \in K^n$。用符号表示：$K(\zeta_n)^n \cap K = K^n$。

写作 $n = p^r$，我们需要证明 $\alpha \in K(\zeta_{p^r})^{p^r}$ 蕴含 $\alpha \in K^{p^r}$。将域与指数分开来证明会更方便，下面证明一个更一般的命题。

定理 3.2。设 K 和 p 与定理 3.1 中相同；特别地，若 $p = 2$，则我们假设 $i \in K$。令 $s \geq r \geq 1$；则 $\alpha \in K(\zeta_{p^r})^{p^s}$ 意味着 $\alpha \in K^{p^s}$。用符号表示：$K(\zeta_{p^r})^{p^s} \cap K = K^{p^s}$。

证明。我们对 r 使用归纳法。在 $r = 1$ 的情况下，证明非常简单。写作 $\alpha = \beta^{p^s}$，其中 $\beta \in K(\zeta_p)$。取范数，得到 $\alpha^d = \gamma^{p^s}$，其中 $d = [K(\zeta_p) : K]$ 以及 $\gamma = \mathcal{N}_{K(\zeta_p)/K}\beta$。由于 $d \leq p-1$，我们有 最大公约数$(p^s, d) = 1$。令 $u, v \in \mathbb{Z}$ 使得 $ud + vp^s = 1$。那么 $\alpha = \alpha^{ud+vp^s} = \left(\gamma^u \alpha^v\right)^{p^s} \in K^{p^s}$，证毕。

现在假设 $r \geq 2$。如果 $p = 2$，那么根据假设有 $\zeta_4 \in K$。这意味着，在 $p^r = 4$ 的情况下，无须证明任何内容。因此，当 $p = 2$ 时，我们可以假设 $r \geq 3$。

我们假设 $\alpha \in K(\zeta_{p^r})^{p^s}$，并希望证明

$$\alpha \in K(\zeta_{p^{r-1}})^{p^s}. \tag{3.1}$$

由归纳法可知，$\alpha \in K^{p^s}$，这正是所要证明的。

如果 $\zeta_{p^r} \in K(\zeta_{p^{r-1}})$，那么无需证明。因此我们假设$\zeta_{p^r} \notin K(\zeta_{p^{r-1}})$。推论 2.3 现在说明，$K(\zeta_{p^r})$ 是 $K(\zeta_{p^{r-1}})$ 的一个次数为 p 的伽罗瓦扩张。

域 $K(\zeta_{p^s})$ 也是 $K(\zeta_{p^{r-1}})$ 的一个伽罗瓦扩张。令 σ为 $\mathrm{Gal}\big(K(\zeta_{p^s})/K(\zeta_{p^{r-1}})\big)$ 中的一个元素，使得其限制 $\sigma|_{K(\zeta_{p^r})}$生成 $K(\zeta_{p^r})$ 在 $K(\zeta_{p^{r-1}})$ 上的伽罗瓦群。对于某个不被 p 整除的 $g \in \mathbb{Z}$，有 $\sigma(\zeta_{p^s}) = \zeta_{p^s}^g$。由于 $\sigma(\zeta_{p^{r-1}}) = \zeta_{p^{r-1}}$，我们必须有 $g \equiv 1$(模 p^{r-1})。特别是，

$$g \equiv \begin{cases} 1 \pmod{p}, & \text{if } p \geq 3, \\ 1 \pmod{4}, & \text{if } p = 2. \end{cases} \tag{3.2}$$

写作 $\alpha = \beta^{p^s}$，其中 $\beta \in K(\zeta_{p^r})$。我们作出以下两个观察。

1. 由于 $\beta^{p^s} \in K \subset K(\zeta_{p^{r-1}})$，我们有

$$\sigma(\beta)/\beta \in \mu_{p^s}. \tag{3.3}$$

我们记 $\sigma(\beta) = \beta\zeta_{p^s}^m$，其中 $m \in \mathbb{Z}$。

素数 2. 由于 $\beta \in K(\zeta_{p^r})$，且限制 $\sigma|_{K(\zeta_{p^r})}$在群 $\mathrm{Gal}\big(K(\zeta_{p^r})/K(\zeta_{p^{r-1}})\big)$ 中的阶为 p，我们有 $\sigma^p(\beta) = \beta$。用上文引入的整数 m 和 g 表示，这意味着

$$m(1 + g + \cdots + g^{p-1}) \equiv 0 \pmod{p^s}.$$

现在我们已经准备好完成证明。利用 (3.2)，通过一个标准论证可知，

$$1 + g + \cdots + g^{p-1} = \frac{g^p - 1}{g - 1} \equiv p \pmod{p^2}.$$

因此 $m \equiv 0$ (模 p^{s-1})，这意味着 (3.3) 可以大幅精化：$\sigma(\beta)/\beta \in \mu_p$。

另一方面，由于 $\zeta_{p^r}^p \in K(\zeta_{p^{r-1}})$，我们也有 $\sigma(\zeta_{p^r})/\zeta_{p^r} \in \mu_p$。此外，由于 $\zeta_{p^r} \notin K(\zeta_{p^{r-1}})$，$p^{\text{th}}$根单位 $\sigma(\zeta_{p^r})/\zeta_{p^r}$ 必须是本原的。因此，存在 $b \in \mathbb{Z}$ 使得 $\sigma(\beta)/\beta = (\sigma(\zeta_{p^r})/\zeta_{p^r})^b$，这可以改写为 $\sigma(\beta') = \beta'$，其中 $\beta' := \beta\zeta_{p^r}^{-b}$。

因此，$\beta' \in K(\zeta_{p^{r-1}})$。由于 $(\beta')^{p^s} = \alpha$，这就推出了 (3.1)。定理得证。 □

“$i \in K$ 如果 $p = 2$ ”这一假设不可省略。例如，取 $K = \mathbb{R}$。那么 -1 在 K中不是平方，但对于每个 m，它都是 $K(\zeta_{4m}) = \mathbb{C}$中的 $4m^{\text{th}}$ 次幂。不过，Chevalley 作出了以下重要观察。

命题 3.3（Chevalley）。设 K 是一个特征为 $K \neq 2$ 的域，k 是一个满足 $\zeta_{2^{k+1}} \notin K$ (i) 的正整数。那么对于任意正整数 r，以下结论成立：如果 $\alpha \in K$ 是 $K(i)$ 中的 2^{r+k} 次幂，那么它就是 K 中的 2^r 次幂。用符号表示：$K(i)^{2^{r+k}} \cap K \subset K^{2^r}$。

证明。设 $\alpha \in K$ 是 $K(i)$ 中的 2^{r+k} 次幂。记 $\alpha = \beta^{2^{r+k}}$，其中 $\beta \in K(i)$。如果 $\beta \in K$，则无需证明，因此我们假设 $\beta \notin K$，并将 β 在 K 上的共轭记为 β。设 m 为满足性质 $\beta^{2^m} \in K$ 的最小整数。则 $\beta/\bar{\beta}$ 是一个本原的 2^m 次单位根。由于 $\beta/\bar{\beta} \in K(i)$，且 $\zeta_{2^{k+1}} \notin K(i)$，我们必须有 $m \leq k$；特别地，$\beta^{2^k} \in K$。因此 $\alpha = (\beta^{2^k})^{2^r} \in K^{2^r}$，这正是所要证明的。 □

4 关键引理

切瓦莱定理讨论了 $\alpha \in K(\zeta_{p^r})^{p^r}$ 的情形。要推广这一结论，我们需要讨论任意 n 下的 $\alpha \in K(\zeta_n)^{p^r}$。借助下面这个关键引理即可实现这一点；这个引理很可能受到了 Chevalley 的命题 3.3 的启发。

引理 4.1（Smith）。设 K 是一个域，p 是一个与 $\operatorname{char} K$ 不同的素数。如果 $p = 2$，那么我们假设 $i \in K$。设 L 是 K 的一个有限伽罗瓦扩张，并设 ℓ 是一个满足 $\zeta_{p^{\ell+1}} \notin L$ 的非负整数。那么对于任意正整数 r，以下结论成立：若 $\alpha \in K$ 是 L 中的 $p^{r+\ell}$ 次幂，则它也是 K 中的 p^r 次幂。用符号表示：$L^{p^{r+\ell}} \cap K \subset K^{p^r}$。

证明。设 $\alpha \in K$ 是 L 中的一个 $p^{r+\ell}$ 次幂。记 $\alpha = \beta^{p^{r+\ell}}$，其中 $\beta \in L$。如果 $\beta \in K$，则无需证明，因此我们假设 $\beta \notin K$。设 m 是满足性质 $\beta^{p^m} \in K$ 的最小整数。如果 $m \leq \ell$，则 $\beta^{2^\ell} \in K$，并且 $\alpha = (\beta^{2^\ell})^{2^r} \in K^{2^r}$，正如所需。

现在假设 $m > \ell$。那么 $\gamma := \beta^{p^m}$ 是 K 中的一个 p^{th} 次幂。事实上，若非如此，多项式 $X^{p^m} - \gamma$ 根据推论 2.2 将在 K 上不可约。由于它在 L 中有一个根 β，而 L 是 K 的伽罗瓦扩张，因此它的所有根都必须属于 L。特别地，$\beta\zeta_{p^m} \in L$，这意味着 $\zeta_{p^m} \in L$。由于 $m > \ell$，这与我们的假设 $\zeta_{p^{\ell+1}} \notin L$ 矛盾。

因此，对某个 $\eta \in K$，有 $\gamma = \eta^p$。注意，根据 m 的定义，$\eta \neq \beta^{p^{m-1}}$。因此，$\eta/\beta^{p^{m-1}}$ 是一个本原 p^{th} 次单位根；特别地，$\zeta_p \in L$。

如果 $\zeta_p \in K$，那么 $\beta^{p^{m-1}} \in K$，这与 m 的定义矛盾。因此，ζ_p 属于 L，但不属于 K；特别地，$[L : K(\zeta_p)] < [L : K]$。利用关于次数 $[L : K]$ 的归纳法，我们得出 $\alpha \in K(\zeta_p)^{p^r}$。现在由定理 3.2 可知 $\alpha \in K^{p^r}$。 □

5 定理 1.1 的证明

从本节开始，我们假设域 K 如定理 1.1 所述；也就是说，它的特征为 0，且其最大阿贝尔子域 K_{ab} 是有限的

在 $\mathbb{Q}$上。下面介绍一些记号。

设 $p \geq 3$ 为奇素数， $\mathfrak{p}$ 为 K_{ab} 上方的一个 p素数。由于 K_{ab}是 $\mathbb{Q}$的伽罗瓦扩张，分歧指数 $e_{\mathfrak{p}/p}$ 只取决于 p，而不取决于 $\mathfrak{p}$的具体选择。我们将其记为 ϵ_p:

$$\epsilon_p := e_{\mathfrak{p}/p}, \quad \text{where } \mathfrak{p} \text{ is a prime of } K_{\mathrm{ab}}, \quad \mathfrak{p} \mid p.$$

我们称 p 为特定素数，当且仅当 $p-1 \mid \epsilon_p$。

注意，特定素数必定在 K_{ab}中分歧。特别地，特定素数至多只有有限个。

“最奇特”的素数 2，和往常一样，需要特别考虑。回想一下，$1+i$ 是 2 上方的 $\mathbb{Q}(i)$ 素数。我们将 ϵ_2 定义为$1+i$ 上方的一个 $K_{\mathrm{ab}}(i)$ 素数相对于 $1+i$的分歧指数:

$$\epsilon_2 := e_{\mathfrak{p}/(1+i)}, \quad \text{where } \mathfrak{p} \text{ is a prime of } K_{\mathrm{ab}}(i), \quad \mathfrak{p} \mid 1+i.$$

同样， ϵ_2 是良定义的，因为 $e_{\mathfrak{p}/(1+i)}$ 与 $\mathfrak{p}$的具体选择无关。

命题 5.1。设 ℓ 为正整数。

1. 设 p 为奇素数。如果对于某个不能被 p整除的 m，有 $\zeta_p \in K(\zeta_m)$，则 p 是特征的。此外，若 $\zeta_{p^\ell} \in K(\zeta_m)$，则 $\ell \leq \nu_p(\epsilon_p) + 1$。
2. 假设对于某个奇整数 m，有 $\zeta_{2^\ell} \in K(i, \zeta_m)$。则 $\ell \leq \nu_2(\epsilon_2) + 3$。

证明。首先，我们断言 $K_{\mathrm{ab}}(\zeta_m)$ 是$K(\zeta_m)$ 的最大阿贝尔子域:

$$K(\zeta_m)_{\mathrm{ab}} = K_{\mathrm{ab}}(\zeta_m). \tag{5.1}$$

事实上，我们有

$$[K(\zeta_m) : K] = [K_{\mathrm{ab}}(\zeta_m) : K_{\mathrm{ab}}(\zeta_m) \cap K],$$

例如，参见 [6, 第六章]中的定理 1.12。根据 K_{ab}的定义，我们有 $K_{\mathrm{ab}}(\zeta_m) \cap K = K_{\mathrm{ab}}$，由此得到等式

$$[K_{\mathrm{ab}}(\zeta_m) : K_{\mathrm{ab}}] = [K(\zeta_m) : K].$$

类似地，令 $L := K(\zeta_m)$，我们有 $L_{\mathrm{ab}} \cap K = K_{\mathrm{ab}}$，这意味着$[L_{\mathrm{ab}} : K_{\mathrm{ab}}] = [KL_{\mathrm{ab}} : K]$。由于 $KL_{\mathrm{ab}} = K(\zeta_m)$，这证明了

$$[K_{\mathrm{ab}}(\zeta_m) : K_{\mathrm{ab}}] = [L_{\mathrm{ab}} : K_{\mathrm{ab}}],$$

由此得到（5.1），因为 $K_{\mathrm{ab}}(\zeta_m) \subseteq L_{\mathrm{ab}}$。

假设 p 是奇素数。设 $\mathfrak{p}$ 是 K_{ab} 中位于 p 上方的一个素理想， $\mathfrak{P}$ 是 $K_{\mathrm{ab}}(\zeta_m)$ 中位于 $\mathfrak{p}$ 上方的一个素理想。由于根据假设 $p \nmid m$， $\mathfrak{p}$ 在 $K_{\mathrm{ab}}(\zeta_m)$ 中不分歧；特别地，$e_{\mathfrak{p}/p} = e_{\mathfrak{P}/p}$。

另一方面， p 在 $\mathbb{Q}(\zeta_{p^\ell})$ 中完全分歧，分歧指数为 $p^{\ell-1}(p-1)$。如果 $\zeta_{p^\ell} \in K(\zeta_m)$，那么由 (5.1) 可得 $\zeta_{p^\ell} \in K_{\mathrm{ab}}(\zeta_m)$，这意味着

that $p^{\ell-1}(p-1) \mid e_{\mathfrak{P}/p}$。由于 $e_{\mathfrak{P}/p} = e_{\mathfrak{p}/p} = \epsilon_p$，这就证明了奇数 p的情形下的命题。

$p = 2$ 的情形类似。若 $\ell \leq 3$，则无需证明任何内容，因此不妨设 $\ell \geq 4$。设 $\mathfrak{p}$ 是 $K_{\mathrm{ab}}(i)$ 中位于 $1+i$ 之上的一个素理想， $\mathfrak{P}$ 是$K_{\mathrm{ab}}(i,\zeta_m)$中位于 $\mathfrak{p}$之上的一个素理想。由于 m 是奇数，我们有$e_{\mathfrak{p}/(1+i)} = e_{\mathfrak{P}/(1+i)}$。

素理想 $1+i$ 在 $\mathbb{Q}(\zeta_{2^\ell})$中完全分歧，分歧指数为$2^{\ell-3}$。若 $\zeta_{2^\ell} \in K(i,\zeta_m)$，则 $\zeta_{2^\ell} \in K_{\mathrm{ab}}(i,\zeta_m)$，因为 $K(i,\zeta_m)_{\mathrm{ab}} = K_{\mathrm{ab}}(i,\zeta_m)$，这与(5.1)的证明方法相同。于是得到

$$2^{\ell-3} \mid e_{\mathfrak{P}/(1+i)} = e_{\mathfrak{p}/(1+i)} = \epsilon_2,$$

这也证明了命题对 $p = 2$ 成立。 □

这一命题促成了下面的定义。对于一个素数 p，令

$$\lambda_p := \begin{cases} \nu_p(\epsilon_p) + 1, & \text{if } p \text{ is distinguished;} \\ \nu_2(\epsilon_2) + 3, & \text{if } p = 2; \\ 0, & \text{for the other } p. \end{cases}$$

下面的论述是定理 1.1证明的技术核心。

命题 5.2。设 n 为正整数， p 为 n的素因数，且 $\alpha \in K$。令 $r := \nu_p(n)$，于是 $p^r \| n$。为简化记号，记 $\lambda = \lambda_p$。

假设 $p \geq 3$，或者 $p = 2$ 且 $i \in K$。设 α 是$K(\zeta_{np^\lambda})$中的一个 $p^{\lambda+r}$次幂。那么，α 是 K中的一个 p^r次幂。用符号表示： $K(\zeta_{np^\lambda})^{p^{\lambda+r}} \cap K \subset K^{p^r}$。

当 $p = 2$ 且 $i \notin K$时，同样的结论仍成立，但要将 λ 替换为 2λ；也就是说，$K(\zeta_{n\cdot 4^\lambda})^{2^{2\lambda+r}} \cap K \subset K^{2^r}$。

证明。记 $n = p^r m$，于是 $p \nmid m$。首先假设 $p \geq 3$，或者 $p = 2$ 且$i \in K$。我们有 $K(\zeta_{np^\lambda}) = K(\zeta_m, \zeta_{p^{\lambda+r}})$。若 $\alpha \in K(\zeta_{np^\lambda})^{p^{\lambda+r}}$，则将 $\lambda + r$ 作为 r、将 $K(\zeta_m)$作为 K应用定理 3.1，可得 $\alpha \in K(\zeta_m)^{p^{\lambda+r}}$。

令 ℓ 为满足性质 $\zeta_{p^\ell} \in K(\zeta_m)$ 的最大整数。由命题 5.1 可知 $\ell \leq \lambda$；特别地， $\alpha \in K(\zeta_m)^{p^{\ell+r}}$。最后，将引理 4.1 应用于 $L = K(\zeta_m)$，得到 $\alpha \in K^{p^r}$。

借助命题 3.3， $p = 2$ 和 $i \notin K$ 的情形可归结为 $i \in K$ 的情形。令 k 和 ℓ 分别为满足性质 $\zeta_{2^k} \in K(i)$ 和 $\zeta_{2^\ell} \in K(i,\zeta_m)$ 的最大整数。于是 $k \leq \ell \leq \lambda$。仿照前面的论证，我们证明如下结论：若 $\alpha \in K(i,\zeta_{n\cdot 4^\lambda})^{2^{2\lambda+r}}$，则 $\alpha \in K(i)^{2^{k+r}}$。现在由命题 3.3 可知 $\alpha \in K^{2^r}$。 □

现在我们可以完成定理 1.1 的证明了。令

$$\Lambda := 4^{\lambda_2} \prod_{p \geq 3} p^{\lambda_p}. \tag{5.2}$$

该乘积定义良好，因为只有特征素数会对其产生贡献：对于其他奇数的 p，我们有 $\lambda_p = 0$。

设 n 为正整数，并设 $\alpha \in K$ 满足 $\alpha \in K(\zeta_{n\Lambda})^{n\Lambda}$。对于 $p \mid n$，我们定义

$$r_p := \nu_p(n), \qquad N_p := \begin{cases} n\Lambda/p^{\lambda_p}, & \text{if } p \geq 3, \\ n\Lambda/4^{\lambda_2}, & \text{if } p = 2. \end{cases}$$

那么 $p^{r_p} \| N_p$ 和

$$\alpha \in \begin{cases} K(\zeta_{N_p \cdot p^{\lambda_p}})^{p^{\lambda_p + r_p}}, & \text{if } p \geq 3, \\ K(\zeta_{N_2 \cdot 4^{\lambda_2}})^{2^{2\lambda_2 + r_2}}, & \text{if } p = 2. \end{cases}$$

将 N_p 作为 n 应用于命题 5.2，可得 $\alpha \in K^{p^{r_p}}$。由于 $K^n = \bigcap_{p|n} K^{p^{r_p}}$，定理 1.1 现即得证。

备注 5.3. 由命题 5.2 可知，当 $i \in K$ 时，可在 (5.2) 中用 2^{λ_2} 替换 4^{λ_2} 。

6 域的 Chevalley-Bass 数

设 K 是定理 1.1 中的域；也就是说，其特征为 0，且 $[K_{\mathrm{ab}} : \mathbb{Q}]$ 的次数有限。定理 1.1 意味着存在一个正整数 Λ，使得

$$K(\zeta_{\Lambda n})^{\Lambda n} \cap K \subset K^n \qquad (n = 1, 2, 3, \ldots). \tag{6.1}$$

称任意这样的 Λ 对 K 是适用的。最小的适用 Λ 称为 K 的切瓦利-巴斯数，记作 Λ_K。

命题 6.1. 设 K 如上。

1. 若 Λ_1 和 Λ_2 适用于 K，则 $\gcd(\Lambda_1, \Lambda_2)$ 也适用。
2. 若 Λ 适用于 K，则每个能被 Λ整除的正整数也适用。
3. 正整数 Λ适用于 K，当且仅当它能被 Chevalley-Bass 数 Λ_K整除。

证明. 证明非常简单。对于第 1 项，我们记 $\Lambda := \gcd(\Lambda_1, \Lambda_2)$，并证明 (6.1) 成立。由于 Λ_1 适用，我们有

$$K(\zeta_{\Lambda n})^{\Lambda_1 n} \cap K \subset K(\zeta_{\Lambda_1 n})^{\Lambda_1 n} \cap K \subset K^n.$$

类似地，$K(\zeta_{\Lambda n})^{\Lambda_2 n} \cap K \subset K^n$。由于 $K(\zeta_{\Lambda n})^{\Lambda_1 n} \cap K(\zeta_{\Lambda n})^{\Lambda_2 n} = K(\zeta_{\Lambda n})^{\Lambda n}$，这就证明了(6.1)。

为证明第 2 项，假设 Λ 适用。那么它的倍数 $k\Lambda$也适用，只需在 (6.1) 中用 kn替换 n 即可。

最后，第 3 项由前两项推出；事实上，第 1 项表明，任何适用数都能被 Λ_K 整除，而第 2 项表明，Λ_K 的每个倍数都是适用数。

□

6.1 Chevalley-Bass 数的估计

要确定给定域 K 的切瓦利-巴斯数的精确值似乎并不容易，但估算它却很容易。下面给出两种估算方法，一种以 K_{ab} 的次数为依据，另一种以判别式为依据。

命题 6.2. 设 K 如上所述。记 d 为 $[K_{\mathrm{ab}}:\mathbb{Q}]$ 的次数。

1. 令

$$\Delta := \prod_{p-1|d} p, \qquad \Delta_0 := 2^{\nu_2(d)+5}\Delta \prod_{p-1|d} p^{\nu_p(d)},$$
$$\Delta_1 := 2^{\nu_2(d)+5} d\Delta, \qquad \Delta_2 := 32d^2\Delta.$$

那么 Chevalley-Bass 数 Λ_K 整除数 Δ_0、Δ_1 和 Δ_2。

2. 若 $i \in K$，则 $\Lambda_K \mid 4d\Delta$。

3. 若 d 为奇数，则 Λ_K 是五个数 4、8、16、32、64 中的一个。

4. 如果 $d \geq 3$ 那么

$$\Lambda_K \leq \exp\exp\left(1.7\frac{\log d}{\log\log d}\right). \tag{6.2}$$

特别地，$\Lambda_K \leq \exp(d^{o(1)})$ 作为 $d \to \infty$。

证明需要一些初步事实，这些事实汇总在下面的引理中。

引理 6.3. 设 n 为正整数。则 n 的所有因数之积等于 $n^{\tau(n)/2}$，其中 $\tau(n)$ 是 n 的因数个数：

$$\prod_{m|n} m = n^{\tau(n)/2}. \tag{6.3}$$

我们还有以下估计

$$\log\tau(n) \leq 1.07\frac{\log n}{\log\log n} \qquad (n \geq 3), \tag{6.4}$$
$$\prod_{p\leq x}\frac{p}{p-1} \leq 2\log(x-1) \qquad (x \geq 25). \tag{6.5}$$

证明。我们有

$$\left(\prod_{m|n} m\right)^2 = \prod_{m|n} m \prod_{m|n}\frac{n}{m} = n^{\tau(n)},$$

这就证明了（6.3）。关于（6.4），请参见 [7, Th´eor`eme 1]。最后，（6.5）可由该估计轻易推出。

$$\prod_{p\leq x}\frac{p}{p-1} \leq 1.8\left(\log x + \frac{1}{\log x}\right),$$

这对所有素数 p 都成立，参见定理 8] 的推论 1 [8, 。 □

命题 6.2 的证明。由于对每个 p 都有 $\epsilon_p \mid d$，我们有 $p-1 \mid d$，其中 p 是一个特定的。因此，(5.2) 的右端整除

$$2^{2\nu_2(d)+6} \prod_{\substack{p-1 \mid d \\ p \geq 3}} p^{1+\nu_p(d)} = \Delta_0.$$

显然，$\Delta_0 \mid \Delta_1 \mid \Delta_2$。这就证明了第 1 项。

若 $i \in K$，则上文的 $2\nu_2(d)+6$ 可替换为 $\nu_2(d)+3$，见备注 5.3。因此，定义中的 $\nu_2(d)+5$ 可替换为 2。这就证明了第 2 项。

若 d 为奇数，则 $\Delta_0 = 64$。此外，当 d 为奇数时，$i \notin K$；而前面提到的例子 $-4 = (1+i)^4$ 表明 $\Lambda_K \neq 1$，2。这就证明了第 3 项。

现在只剩下估计式 (6.2) 需要证明。对于奇数 d，这显然成立，因为 (6.2) 右边大于 $\exp\exp(1.7e) > 64$。运行一个简单的 PARI 脚本后，我们验证了对于偶数 $d \leq 10^7$，Δ_1 不超过 (6.2) 的右边。（在一台普通笔记本电脑上，总计算时间不到 5 分钟。）因此，我们需要证明

$$\log \Delta_2 \leq \exp\left(1.7 \frac{\log d}{\log\log d}\right) \tag{6.6}$$

对于 $d \geq 10^7$。利用（6.3）和（6.4），我们得到

$$\Delta \leq \prod_{m \mid d} m \prod_{p \leq d+1} \frac{p}{p-1} \leq d^{\tau(d)/2} \cdot 2\log d.$$

由此可得，

$$\log \Delta_2 \leq \frac{1}{2}\tau(d)\log d + 2\log d + \log\log d + \log 64 \leq 2\tau(d)\log d,$$

其中，对于最后一个不等式，我们使用了 $\tau(d) \geq 2$ 和 $d \geq 10^7$。接下来，利用 (6.4)，我们得到

$$\log \Delta_2 \leq \exp\left(1.07 \frac{\log d}{\log\log d} + \log(2\log d)\right).$$

当 $d \geq 10^7$ 时，我们有 $\log(2\log d) \leq 0.6 \log d / \log\log d$。这就证明了 (6.6)。 □

由于特定素数在 K 中分歧，因此自然会预期存在一个适用的 Λ 关于绝对判别式 $\mathcal{D} := |\mathcal{D}_{K_{\mathrm{ab}}}|$ 的简单表达式。

命题 6.4。切瓦利-巴斯数 Λ_K 整除 $64\mathcal{D}$。如果 $i \in K$，那么 $\Lambda_K \mid 2\mathcal{D}$。

证明。根据备注 5.3，我们需要证明

$$\lambda_p \leq \begin{cases} \nu_p(\mathcal{D}), & \text{if } p \text{ is distinguished,} \\ \nu_2(\mathcal{D})+1, & \text{if } p = 2 \text{ and } i \in K, \\ \nu_2(\mathcal{D})/2+3, & \text{if } p = 2 \text{ and } i \notin K. \end{cases} \tag{6.7}$$

我们将使用以下众所周知的事实：如果 L 是数域且 p 是素数，那么

$$\nu_p(\mathcal{D}_L) \geq \sum_{\mathfrak{p}|p} (e_{\mathfrak{p}/p} - 1 + \delta_{\mathfrak{p}}) f_{\mathfrak{p}/p}, \qquad \text{where} \quad \delta_{\mathfrak{p}} := \begin{cases} 0, & \text{if } p \nmid e_{\mathfrak{p}/p}, \\ 1, & \text{if } p \mid e_{\mathfrak{p}/p}, \end{cases}$$

求和遍历 p 上方的 L 素理想。当 $L = K_{\mathrm{ab}}$ 时，显然有 $e_{\mathfrak{p}/p} = \epsilon_p$，对 $p \geq 3$ 成立。对于 $p = 2$，记 $\mathfrak{P}$ 为 $K(i)$ 中位于 K 素理想 $\mathfrak{p}$ 上方的素理想。注意，$\epsilon_2 = e_{\mathfrak{P}/(1+i)}$。于是

$$e_{\mathfrak{P}/2} = e_{(1+i)/2} e_{\mathfrak{P}/(1+i)} = e_{\mathfrak{p}/2} e_{\mathfrak{P}/\mathfrak{p}}.$$

由于

$$e_{(1+i)/2} = 2, \qquad e_{\mathfrak{P}/(1+i)} = \epsilon_2, \qquad e_{\mathfrak{P}/\mathfrak{p}} \in \{1, 2\},$$

这表明 $e_{\mathfrak{p}/2} \in \{\epsilon_2, 2\epsilon_2\}$，并且当 $i \in K$ 时有 $e_{\mathfrak{p}/2} = 2\epsilon_2$。

因此，无论哪种情况，我们都有

$$\nu_p(\mathcal{D}) \geq \epsilon_p - 1 + \delta_p, \qquad \text{where} \quad \delta_p := \begin{cases} 0, & \text{if } p \nmid \epsilon_p, \\ 1, & \text{if } p \mid \epsilon_p, \end{cases}$$

而在特殊情形 $p = 2$、$i \in K$ 下，我们有 $\nu_2(\mathcal{D}) \geq 2\epsilon_2$。因此，要证明 (6.7)，我们需要证明

$$\nu_p(\epsilon_p) \leq \begin{cases} \epsilon_p - 2 + \delta_p, & \text{if } p \text{ is distinguished}, \\ 2\epsilon_2 - 2, & \text{if } p = 2 \text{ and } i \in K, \\ (\epsilon_2 - 1 + \delta_2)/2, & \text{if } p = 2 \text{ and } i \notin K. \end{cases} \tag{6.8}$$

当 $p \nmid \epsilon_p$ 时，(6.8) 中的不等式成立（注意，当 p 是特定情形时，$\epsilon_p \geq p - 1 \geq 2$）。因此，我们可以假设 $p \mid \epsilon_p$；特别地，$\delta_p = 1$ 且 $\epsilon_p \geq p(p-1)$。由于 $\nu_p(\epsilon_p) \leq \log \epsilon_p / \log p$，且 $\epsilon_p - 1 \geq \epsilon_p/2$，条件 (6.8) 可由 $\log \epsilon_p / \log p \leq \epsilon_p/2$ 推出。当 $\epsilon_p = p = 2$ 时，这成立。在其余情形下，我们有 $\epsilon_p \geq 4$；要处理这些情形，只需注意函数 $x \mapsto \log x / \log 2 - x/2$ 在 $x \geq 4$ 上递减，并在 $x = 4$ 处取零。 □

6.2 分裂域的 Chevalley-Bass 数

在某些应用中，有必要估计有理多项式的分裂域的 Chevalley-Bass 数。

命题 6.5。设 $f(T) \in \mathbb{Q}[T]$ 是一个次数为 $m \geq 2$ 的多项式，且 K 是 f 的分裂域。那么 $\Lambda_K \leq \exp\exp(m/\log m)$。

证明。伽罗瓦群 $G := \mathrm{Gal}(K/\mathbb{Q})$ 是对称群 $\mathcal{S}_m$ 的一个子群，而 $d := [K_{\mathrm{ab}} : \mathbb{Q}]$ 是 G 的最大阿贝尔商群的阶；也就是说，$d = \#G/[G, G]$。众所周知，$d \leq 3^{m/3}$，参见 Kov´acs 和 Praeger 在第 284], 页的 [5, 推论，或 Aschbacher 和 Guralnick 的 [1, 定理 2]。

用 PARI 快速计算可知，对于 $m \leq 15$ 和 $d \leq 3^{m/3}$，我们有 $\log \Delta_0 \leq \exp(m/\log m)$，其中 Δ_0 来自命题 6.2。现在假设$m \geq 16$。估计式 (6.2) 表明，当 $d \leq 3^{m/3}$时，我们有

$$\begin{aligned}\log \Lambda_K &\leq \exp\left(1.7\frac{\log 3}{3}\frac{m}{\log m - \log(3/\log 3)}\right)\\ &\leq \exp\left(1.7\frac{\log 3}{3}\frac{\log 16}{\log 16 - \log(3/\log 3)}\frac{m}{\log m}\right)\\ &\leq \exp\left(0.98\frac{m}{\log m}\right),\end{aligned}$$

这甚至比预期的还要好。 □

6.3 开放问题

尽管第 6.1 小节中的结果提供了一些结论，但域的切瓦利-巴斯数仍然是一个神秘的量。特别是，对于任何一个域，我们都还不知道它的确切值。以下是一些我们希望能够得到解答的问题。

1. $\mathbb{Q}$ 的 Chevalley-Bass 数是多少？ $\mathbb{Q}(i)$ 的又是多少？2. 给定一个数域，是否可以判定其 Chevalley-Bass 数？根据第 6.1 小节的结果，这可归结为以下形式上更简单的问题：给定一个数域 K 和一个正整数 Λ，判定 Λ 是否适用于 K。3. 是否存在一个满足 $\Lambda_K = 1$ 的域 K？（或许，$\mathbb{Q}(i)$ 就是这样的域。）4. 是否存在一个域 K，使得 Λ_K 能被某个奇素数整除?

5. 命题 6.5 的估计能否改进？我们认为，形如 $\exp\exp(O((m/\log m)^{1/2}))$ 的估计必定成立。

我们希望这些问题中的一部分能在不久的将来得到解答。

参考文献

[1] Michael Aschbacher 和 Robert M. Guralnick, *On abelian quotients of primitive groups*, 《Proc. Amer. Math. Soc.》107（1989），第 1 期，89–95。MR 982398[2] H. Bass, *A remark on an arithmetic theorem of Chevalley*, 《Proc. Amer. Math. Soc.》16（1965），875–878。MR 184925[3] Claude Chevalley, *Deux théorèmes d'arithmétique*, 《J. Math. Soc. Japan》3（1951），36–44。MR 44570[4] Georges Gras，个人通信（2023 年）。[5] L. G. Kov´acs 和 Cheryl E. Praeger, *Finite permutation groups with large abelian quotients*, 《Pacific J. Math.》**136**（1989），第 2 期，283–292。MR 978615[6] Serge Lang, *Algebra*，第三版，《数学研究生教材》第 211 卷，Springer 出版社，纽约，2002 年。MR 1878556

[7] J.-L. Nicolas 和 G. Robin, *Majorations explicites pour le nombre de diviseurs de N*, 《Canad. Math. Bull.》26（1983），第 4 期，485–492。MR 716590[8] J. Barkley Rosser 和 Lowell Schoenfeld, *Approximate formulas for some functions of prime numbers* **6** 1962 64 94 137689 , 《Illinois J. Math.》（），–。MR[9] John H. Smith, *A result of Bass on cyclotomic extension fields*, 《Proc. Amer.Math. Soc.》24（1970），394–395。MR 257049[10] The PARI Group，波尔多大学, *PARI/GP version 2.15.4*，2023 年，可从 `http://pari.math.u-bordeaux.fr/` 获取。