

三次型

Cubic forms

我们现在着手证明：一个具有整系数的齐次三次方程

$$C(x_1, \dots, x_n) = 0, \quad (13.1)$$

当 $n \geq 17$ 时，总能在整数 $x_1, \dots, x_n$ （不全为 0）中求解。第一个这样的结果，附带条件 $n \geq 32$ ，于 1957 年被证明 [21]；改进后的结果在 1962 年初被发现 [20]。1963 年我证明了条件 $n \geq 16$ 已经足够 [22]，但这需要一个性质上颇为特殊、超出 $n \geq 17$ 所需的更细致的论证。

Mordell 于 1937 年 [61] 指出，存在九个变量的三次型不表示零，因而条件 $n \geq 10$ 对于 (13.1) 总可解而言是必不可少的。Mordell 的例子基于一个三次域的范数型的性质。如果 p 是一个在该域中不分解的素数，那么范数型 $N(x, y, z)$ 永远不能被 p 整除，除非 x, y, z 都能被 p 整除。由此容易推出，方程

$$N(x_1, x_2, x_3) + pN(x_4, x_5, x_6) + p^2N(x_7, x_8, x_9) = 0$$

除平凡解外，没有整数解 $x_1, \dots, x_9$ 。事实上，我们还可以进一步断言：相应的模 p^3 的同余式除了所有变量都 $\equiv 0 \pmod{p}$ 之外没有解。一个简单的例子可由取 $p = 7$ 并令

$$N(x, y, z) = x^3 + 2y^3 + 4z^3 - 6xyz$$

给出，这正是由 $\sqrt[3]{2}$ 生成的域的范数型。一个与上述类似的构造，给出了 k^2 个变量中 k 次齐次不可解方程的例子。

关于三次方程的定理的证明分为若干章，每一章在很大程度上是自成一体的。我们从考虑与一个三次型相关联的指数和开始。写

$$C(\mathbf{x}) = C(x_1, \dots, x_n) = \sum_i \sum_j \sum_k c_{ijk} x_i x_j x_k,$$

其中各求和指标从 1 跑到 n ，系数 c_{ijk} 是整数，并且我们可以假设 c_{ijk} 是关于 i, j, k 的对称函数。设 P 是一个大的正整数。设 $\mathfrak{B}$ 是 n 维空间中一个固定的盒子，即由 n 个区间构成的笛卡尔积

$$x'_j < x_j \leq x''_j, \quad (1 \leq j \leq n).$$

仅为方便起见，我们假设 $x''_j - x'_j < 1$ 。令

$$S(\alpha) = \sum_{P\mathfrak{B}} e(\alpha C(x_1, \dots, x_n)),$$

其中求和遍历盒子 $P\mathfrak{B}$ 中的所有整点，盒子 $P\mathfrak{B}$ 由下式给出

$$Px'_j < x_j \leq Px''_j, \quad (1 \leq j \leq n).$$

设 $\mathcal{N}(P)$ 表示 $P\mathfrak{B}$ 中满足 (13.1) 的整点 $\mathbf{x}$ 的个数。则

$$\mathcal{N}(P) = \int_0^1 S(\alpha) d\alpha. \quad (13.2)$$

我们的目标（原则上）是证明：通过适当选取盒子 $\mathfrak{B}$ ，当 $P \rightarrow \infty$ 时 $\mathcal{N}(P)$ 有一个渐近公式，其中主项的阶为 P^{n-3} 。实际上这并不总是成立。我们将要得到的，是一个看似自相矛盾的结果：该渐近公式在 (13.1) 不可解（从而 $\mathcal{N}(P) = 0$ ）的假设下成立！这对我们的目的而言已经足够，因为它将证明 (13.1) 是可解的。

$|S(\alpha)|$ 的平凡估计是 P^n 。我们首先研究：若对于某个特定的 α ，有

$$|S(\alpha)| \geq P^{n-K}, \quad (13.3)$$

会发生什么，其中 K 是某个正数。最终，正如前几章那样，我们的目标是能够从 α 的集合中去掉任何对积分贡献的量低于 P^{n-3} 阶的子集。

第一步是证明 Weyl 不等式的一个推广。对于任意两点 $\mathbf{x}, \mathbf{y}$, 我们定义一组 n 个双线性型:

$$B_j(\mathbf{x} | \mathbf{y}) = \sum_i \sum_k c_{ijk} x_i y_k, \quad (1 \leq j \leq n).$$

引理 13.1. 假设 (13.3) 蕴含

$$\sum_{|\mathbf{x}| < P} \sum_{|\mathbf{y}| < P} \prod_{j=1}^n \min(P, \|6\alpha B_j(\mathbf{x} | \mathbf{y})\|^{-1}) \gg P^{3n-4K}.$$

证. 我们有

$$\begin{aligned} |S(\alpha)|^2 &= \sum_{\mathbf{z} \in P\mathfrak{B}} \sum_{\mathbf{z}' \in P\mathfrak{B}} e(\alpha C(\mathbf{z}') - \alpha C(\mathbf{z})) \\ &= \sum_{\mathbf{z} \in P\mathfrak{B}} \sum_{\mathbf{y} + \mathbf{z} \in P\mathfrak{B}} e(\alpha C(\mathbf{y} + \mathbf{z}) - \alpha C(\mathbf{z})). \end{aligned}$$

对任意的 $\mathbf{z}$, 盒子 $P\mathfrak{B} - \mathbf{z}$ 包含于 $|\mathbf{y}| < P$ 之内。因此

$$|S(\alpha)|^2 \leq \sum_{|\mathbf{y}| < P} \left| \sum_{\mathbf{z} \in \mathcal{R}(\mathbf{y})} e(\alpha C(\mathbf{y} + \mathbf{z}) - \alpha C(\mathbf{z})) \right|,$$

其中 $\mathcal{R}(\mathbf{y})$ 表示盒子 $P\mathfrak{B}$ 与 $P\mathfrak{B} - \mathbf{y}$ 的公共部分。由 Cauchy 不等式,

$$|S(\alpha)|^4 \ll P^n \sum_{|\mathbf{y}| < P} \left| \sum_{\mathbf{z} \in \mathcal{R}(\mathbf{y})} e(\alpha C(\mathbf{y} + \mathbf{z}) - \alpha C(\mathbf{z})) \right|^2.$$

我们现在对内层求和重复上述论证。其平方不超过

$$\sum_{|\mathbf{x}| < P} \left| \sum_{\mathbf{z} \in \mathcal{S}(\mathbf{x}, \mathbf{y})} e(\alpha (C(\mathbf{z} + \mathbf{x} + \mathbf{y}) - C(\mathbf{z} + \mathbf{x}) - C(\mathbf{z} + \mathbf{y}) + C(\mathbf{z}))) \right|,$$

其中 $\mathcal{S}(\mathbf{x}, \mathbf{y})$ 是依赖于 $\mathbf{x}$ 和 $\mathbf{y}$ 的关于 $\mathbf{z}$ 的盒子, 其各棱边长度小于 P 。我们有

$$\alpha(C(\mathbf{z} + \mathbf{x} + \mathbf{y}) - C(\mathbf{z} + \mathbf{x}) - C(\mathbf{z} + \mathbf{y}) + C(\mathbf{z})) = 6\alpha \sum_{i,j,k} c_{ijk} x_i y_k z_j + \phi$$

其中 ϕ 不涉及 $\mathbf{z}$ 。由一个现已熟悉的估计,

$$\left| \sum_{\mathbf{z} \in \mathcal{S}(\mathbf{x}, \mathbf{y})} e \left(6\alpha \sum_j B_j(\mathbf{x} | \mathbf{y}) z_j \right) \right| \ll \prod_{j=1}^n \min(P, \|6\alpha B_j(\mathbf{x} | \mathbf{y})\|^{-1}).$$

代入前面的不等式中, 并结合 (13.3), 即得结论。 ■

注. 在估计一个指数和时, 看一看平凡估计给出什么, 以判断 (如果有的话) 损失了多少 (永远地损失了), 是一种有用的预防措施。在当前情形中, 对乘积中始终取 P 作为最小值, 则 $|S(\alpha)|^4$ 的平凡估计将是 P^{4n} , 这是令人满意的。

引理 13.2. 假设 (13.3) 蕴含: 满足¹

$$|\mathbf{x}| < P, \quad |\mathbf{y}| < P, \quad \|6\alpha B_j(\mathbf{x} | \mathbf{y})\| < P^{-1}, \quad (1 \leq j \leq n), \quad (13.4)$$

的整点对 $\mathbf{x}, \mathbf{y}$ 的个数

$$\gg P^{2n-4K} (\log P)^{-n}.$$

证. 设 $Y(\mathbf{x})$ 表示对给定的 $\mathbf{x}$ 满足 (13.4) 的点 $\mathbf{y}$ 的个数。于是, 对任意满足 $0 \leq r_j < P$ 的整数 $r_1, \dots, r_n$, 使每个坐标都落在某个长度为 P 的指定区间内、并满足

$$\frac{r_j}{P} \leq \{6\alpha B_j(\mathbf{x} | \mathbf{y})\} < \frac{r_j + 1}{P}, \quad (1 \leq j \leq n)$$

的整点 $\mathbf{y}$ 的个数不能超过 $Y(\mathbf{x})$, 其中 $\{\theta\}$ 表示任意实数 θ 的小数部分。因为若 $\mathbf{y}'$ 是这样一个点, 而 $\mathbf{y}$ 是任意这样的点, 我们应有 $|\mathbf{y} - \mathbf{y}'| < P$ 以及

$$\|6\alpha B_j(\mathbf{x} | \mathbf{y} - \mathbf{y}')\| < P^{-1}, \quad (1 \leq j \leq n).$$

因此 $\mathbf{y}$ 的可能性不能超过 $Y(\mathbf{x})$ 个。(注意在 (13.4) 中允许 $\mathbf{y} = \mathbf{0}$ 。)

将立方体 $|\mathbf{y}| < P$ 划分为 2^n 个边长为 P 的立方体, 我们得到

$$\sum_{|\mathbf{y}| < P} \prod_{j=1}^n \min(P, \|6\alpha B_j(\mathbf{x} | \mathbf{y})\|^{-1}) \ll Y(\mathbf{x}) \sum_{r_1=0}^{P-1} \cdots \sum_{r_n=0}^{P-1} \min\left(P, \frac{P}{r_j}, \frac{P}{r_j -}\right)$$

将其代入引理 13.1 的结论中, 给出

$$(P \log P)^n \sum_{|\mathbf{x}| < P} Y(\mathbf{x}) \gg P^{3n-4K}.$$

由于 $\sum Y(\mathbf{x})$ 即为满足 (13.4) 的点对 $\mathbf{x}, \mathbf{y}$ 的个数, 结论随之成立。 ■

注. 由于满足 (13.4) 的点对 $\mathbf{x}, \mathbf{y}$ 个数的平凡估计是 P^{2n} , 我们放弃了一个因子 $(\log P)^n$ 。但这并不重要。

引理 13.3. 设 θ 与 P 无关且满足 $0 < \theta < 1$ 。假设 (13.3) 蕴含: 满足

$$|\mathbf{x}| < P^\theta, \quad |\mathbf{y}| < P^\theta, \quad \|6\alpha B_j(\mathbf{x} | \mathbf{y})\| < P^{-3+2\theta}, \quad (13.5)$$

的整点对 $\mathbf{x}, \mathbf{y}$ 的个数

$$\gg P^{2n\theta-4K} (\log P)^{-n}.$$

证. 我们将通过两次应用引理 12.6 得到结论。首先把 $\mathbf{x}$ 看作 (13.4) 中固定的, 并考虑整点 $\mathbf{y}$ 的个数。关于 $\mathbf{y}$ 的不等式是

$$\begin{cases} |y_1| < P, \dots, |y_n| < P, \\ |L_1(\mathbf{y}) - u_{n+1}| < P^{-1}, \dots, |L_n(\mathbf{y}) - u_{2n}| < P^{-1}, \end{cases} \quad (13.6)$$

其中 $L_j(\mathbf{y}) = 6\alpha B_j(\mathbf{x} | \mathbf{y})$, 而 u_{n+j} 是最接近 $L_j(\mathbf{y})$ 的整数。形式 $L_j(\mathbf{y})$ 满足前一章的对称性条件, 因为 L_j 中 y_k 的系数是 $6\alpha \sum_i c_{ijk} x_i$, 它在交换 j 与 k 时保持不变。我们将引理 12.6 应用于此, 以 $y_1, \dots, y_n$ 代 $u_1, \dots, u_n$, 并取

$$a = P, \quad Z_2 = 1, \quad Z_1 = P^{-1+\theta}.$$

当 $Z_2 = 1$ 时, 引理 12.6 的不等式即上面的不等式 (13.6)。设这些不等式有 $N(\mathbf{x})$ 个关于 $\mathbf{y}$ 的解。当取 $Z = Z_1$ 时, 引理 12.6 的不等式变为

$$|y_1| < P^\theta, \dots, |y_n| < P^\theta, \quad |L_1(\mathbf{y}) - u_{n+1}| < P^{-2+\theta}, \dots, |L_n(\mathbf{y}) - u_{2n}| <$$

因此这些不等式关于 $\mathbf{y}$ 的解的个数

$$\gg N(\mathbf{x}) P^{-n(1-\theta)}.$$

于是满足

$$|\mathbf{x}| < P, \quad |\mathbf{y}| < P^\theta, \quad \|6\alpha B_j(\mathbf{x} | \mathbf{y})\| < P^{-2+\theta} \quad (13.7)$$

的点对 $\mathbf{x}, \mathbf{y}$ 的个数

$$\gg P^{-n(1-\theta)} \sum_{|\mathbf{x}| < P} N(\mathbf{x}) \gg P^{n+n\theta-4K} (\log P)^{-n},$$

此处用到了引理 13.2。

现在我们进行一个类似的论证, 但固定 $\mathbf{y}$ 而让 $\mathbf{x}$ 变化。对每个 $\mathbf{y}$, 条件 (13.7) 即为

$$|x_1| < P, \dots, |x_n| < P, \\ |M_1(\mathbf{x}) - u_{n+1}| < P^{-2+\theta}, \dots, |M_n(\mathbf{x}) - u_{2n}| < P^{-2+\theta},$$

其中 $M_j(\mathbf{x}) = B_j(\mathbf{y} | \mathbf{x})$, 而 u_{n+j} 现在是最接近 $M_j(\mathbf{x})$ 的整数。这些是引理 12.6 中取

$$a = P^{\frac{3}{2}-\frac{1}{2}\theta}, \quad Z = Z_2 = P^{-\frac{1}{2}+\frac{1}{2}\theta}$$

的不等式。我们取 $Z_1 = P^{-\frac{3}{2}+\frac{3}{2}\theta}$ 。于是引理告诉我们,

$$|x_1| < P^\theta, \dots, |x_n| < P^\theta, \quad |M_1(\mathbf{x}) - u_{n+1}| < P^{-3+2\theta}, \dots, |M_n(\mathbf{x}) - u_{2n}$$

的解的个数 $\gg P^{-n(1-\theta)} N_1(\mathbf{y})$, 其中 $N_1(\mathbf{y})$ 表示对给定的 $\mathbf{y}$, (13.7) 的解的个数。因此满足 (13.5) 的整点对 $\mathbf{x}, \mathbf{y}$ 的个数

$$\gg P^{-n+n\theta} \sum_{|\mathbf{y}| < P^\theta} N_1(\mathbf{y}) \gg P^{-n+n\theta} P^{n+n\theta-4K} (\log P)^{-n},$$

由此即得结论。 ■

引理 13.4. 设 θ 与 P 无关且满足 $0 < \theta < 1$ 。设 ε 是任意小的固定正数。那么, 或者

(A) 存在多于 $P^{n\theta+\varepsilon}$ 个满足

$$|\mathbf{x}| < P^\theta, \quad |\mathbf{y}| < P^\theta, \quad B_j(\mathbf{x} | \mathbf{y}) = 0, \quad (1 \leq j \leq n) \quad (13.8)$$

的整点对 $\mathbf{x}, \mathbf{y}$;

或者

(B) 对每个 α , 假设

$$|S(\alpha)| \geq P^{n-\frac{1}{4}n\theta+\varepsilon} \quad (13.9)$$

蕴含 α 有一个有理逼近 a/q 使得

$$(a, q) = 1, \quad 1 \leq q \ll P^{2\theta}, \quad |q\alpha - a| < P^{-3+2\theta}. \quad (13.10)$$

证. 我们在 (13.3) 中取 $K = \frac{1}{4}n\theta - \varepsilon$, 使得它与 (13.9) 相同。由引理 13.3, 存在

$$\gg P^{2n\theta-4K} (\log P)^{-n} \gg P^{n\theta+\varepsilon}$$

个满足 (13.5) 的整点对 $\mathbf{x}, \mathbf{y}$ 。如果对所有这些点都有 $B_j(\mathbf{x} | \mathbf{y}) = 0$ 对一切 j 成立, 那么选项 (A) 成立。如果不然, 那么对某个点对 $\mathbf{x}, \mathbf{y}$ (在 (13.5) 中) 及某个

j , 我们有 $B_j(\mathbf{x} | \mathbf{y}) \neq 0$ 以及

$$\|6\alpha B_j(\mathbf{x} | \mathbf{y})\| < P^{-3+2\theta}.$$

取 $q = 6|B_j(\mathbf{x} | \mathbf{y})|$, 并取 a 为最接近 αq 的整数。则

$$|q\alpha - a| < P^{-3+2\theta}.$$

此外,

$$q \ll |B_j(\mathbf{x} | \mathbf{y})| \ll \sum_{i,k} |c_{ijk}| |x_i| |y_k| \ll |\mathbf{x}| |\mathbf{y}| \ll P^{2\theta}.$$

我们未必有 $(a, q) = 1$, 但通过从 q 和 a 中去掉任何公因子即可保证这一点。于是我们得到选项 (B)。 ■

注. 可以看出选项 A 并不涉及 α 。它本质上也不涉及 θ , 因为若我们令 $R = P^\theta$, 则其断言为: 满足

$$|\mathbf{x}| < R, \quad |\mathbf{y}| < R, \quad B_j(\mathbf{x} | \mathbf{y}) = 0, \quad (1 \leq j \leq n) \quad (13.11)$$

的点对 $\mathbf{x}, \mathbf{y}$ 的个数大于 $R^{n+\varepsilon'}$ (对某个固定的 $\varepsilon' > 0$)。于是选项 A 关系到三次型的一个内禀性质。注意, 如果我们愿意, 可以从 (13.11) 中排除 $\mathbf{x} = \mathbf{0}$ 和 $\mathbf{y} = \mathbf{0}$, 因为这类点对的个数 $\ll R^n$ 。

选项 B 给出了一个原则上与我们在前几章中已经熟悉的情形类似的局面。它将使我们能够在第 15 章中令人满意地估计由一大类 α 对 $\int_0^1 S(\alpha) d\alpha$ 所作的贡献, 并留给我们相对较少的若干短区间, 在其上我们可以逼近 $S(\alpha)$ 。

1. 此处我们对任意点 $\mathbf{x}$ 记 $|\mathbf{x}| = \max(|x_1|, \dots, |x_n|)$ 。这与第 12 章的记号不同，在那里 $|\mathbf{x}|$ 表示点 $\mathbf{x}$ 到原点的距离。然而，对我们的目的而言，这种差别无关紧要。↵