arXiv:2611.29386v1 [math.NT] 22 Nov 2026

关于希腊人的数论

FRANZ LEMMERMEYER

Zusammenfassung. 在我们关于欧几里得四数定理的文章 ¨第二部分（参见 [25]）中，我们从不可公度的概念出发，阐明代数数无理性的证明。在此过程中，我们会遇到高斯引理、整闭性和 Dedekind–Prager 定理，最终又回到四数定理。

第二部分：高斯引理与 Riesz 环

8. Noch einmal die Alten Griechen: Inkommensurabilität

众所周知，毕达哥拉斯学派也被认为发现了不可公度性，即观察到例如正方形的对角线 d与边长 s之间不存在有理数比¨，也就是说，不能将其写成$d:\ s=p:q$，其中¨是自然数¨，q。对此有无数种证明，其中有两种可追溯至古希腊人¨：

- 一种证明由 $\sqrt{2}=\frac{p}{q}$ 推出，p 和 q 都必须是偶数，这与分数（或比例）的可约性相矛盾。该证明可追溯至亚里士多德，在某些《几何原本》的（较早）版本中作为命题 X.117收录；但如今一般认为这是后来加入的补充内容。

- 另一种证明（参见 Hasse [17] 和 Apostol [2]）具有几何性质，其基础是“交替相减法”，即欧几里得算法的前身。

毕达哥拉斯学派早已发现不可公度线段的存在，这一点被认为是确定无疑的；然而，希帕索斯是否作出了（或公开了）这一发现，则并不确定。同样无法确定的是，他是否通过研究五角星而受到启发（见 Fritz [14]）。时常可以见到一种说法，认为这最终引发了希腊数学的“基础危机”；但这一说法没有任何历史事实可以加以证实（不过这并不意味着它一定是错误的）。

随着数概念从几何概念扩展为算术概念，线段不可通约性的问题也从几何问题转变为算术问题：对我们而言，两条线段之比简单来说就是一个数，而正方形的边与对角线不可通约，则意味着 2 的平方根是无理数。

如果知道环 $\mathbb{Z}$ 是唯一分解的，那么证明 $\sqrt{2}$ 的无理性就变得¨显而易见：从 $2q^2=p^2$ 可以看出，2 在左边以奇数次幂出现，而
整除其正整数次幂：矛盾。

2020 *Mathematics Subject Classification.* 01A20,01A60,11T55。

同一证明更一般地表明[1]:

定理 1. *F¨ur* $m \in \mathbb{Z}$ 是有理数，当且仅当 m 是一个整数的平方。

这也是一个定理，其实质内容古希腊人早已知晓；不过，在欧几里得《几何原本》中并没有如此明确的表述。

我们不必借助唯一素因子分解来证明 $\sqrt{2}$ 的无理性，也可以利用带余数的欧几里得除法来证明（鉴于欧几里得环都是唯一分解环，这当然不足为奇）：设 $m \in \mathbb{N}$ 不是正方形；那么存在一个 $n \in \mathbb{N}_0$，使得 $n^2 < m < (n+1)^2$,，也就是说 $0 < \sqrt{m} - n < 1$。若 $\sqrt{m}$ 是有理数，那么我们可以写成 $\sqrt{m} = \frac{p}{q}$，其中 $q \in \mathbb{N}$ 取最小值。于是，$r := q(\sqrt{m} - n) = p - nq$ 也是整数；又由于 $0 < \sqrt{m} - n < 1$，可得$0 < r < q$。现在，$r\sqrt{m} = q(\sqrt{m} - n)$ $\sqrt{m} = mq - nq\sqrt{m} = mq - np$ 是整数；但由$\sqrt{m} = \frac{r\sqrt{m}}{r}$，这与 q的最小性矛盾。关于这种推理方式的推广[2] 以及其他无理数证明，参见例如第 1]章中的 ¨练习。

这里给出一个证明，它基于 $\mathbb{Z}$ 是贝祖环这一事实；更一般地，它表明，一个整数m 的有理数 n次根已经是整数：设 $\sqrt[n]{m} = \frac{p}{q}$，其中 p 和 q是互素整数，即 $(p, q) = (1)$。那么由 $p^n = mq^n$

$$(1) = (p,q)^n \subseteq (p^n, q) = (mq^n, q) \subseteq (q),$$

因此 $(q) = (1)$，于是 $q = \pm 1$ 和 $\sqrt[n]{m} = \pm p$ 是整数。

尽管这类证明十分巧妙，但在某种程度上，它们仍掩盖了问题的核心；我们将在下一节揭示这一核心。

9. 整闭性

学生通常会在入门代数课程中接触到整闭性的概念：若 R 是一个整环，其商域为K，那么如果 $t \in K$ 是首一多项式$f \in R[X]$ 的零点，就称 $t \in K$ 在 R上整。如果每个在 R 上整的 $t \in K$都已包含于 R 中，就称 R 是整闭的（在其商域¨中）。

若 t_1, t_2（在 K 的扩域中）都在 R 上整，则 $t_1 + t_2$ 和 $t_1 t_2$ 也在 R 上整。随着时间推移，基于结式的经典证明已被有限生成模证明所取代；不过，借助张量语言来表述时，经典证明在优雅程度上几乎可与模证明媲美：t_j 是一个首一次数为 m_j、系数取自 R 的多项式的零点，因此也是一个 $m_j \times m_j$ 矩阵 T_j（伴随矩阵）的特征值，该矩阵的元素取自 R。现在很容易证明，$t_1 t_2$ 是克罗内克积的特征值

[1]没有唯一分解就会出问题：在模 4 的所有自然数 M 0，1，2 幺半群中，9 是商幺半群里的分数 $\frac{6}{2}$ 的正方形，但不是 M 中某个数的正方形。-同样，$2i$ 不是 $\mathbb{Z}[2i] = \mathbb{Z} \oplus 2i\mathbb{Z}$ 中的正方形，但由于 $2i = (1+i)^2 = (\frac{2+2i}{2})^2$，它却是商域 $\mathbb{Q}(i)$ 中的正方形。[2]这个证明基本上可追溯到 Dedekind [11]；关于 Haj´os 对该证明的几何化表述，参见 [37]。这一证明的变体还见于 [3, 13, 34, 38, 40] 等文献。

$T_1 \otimes T_2$，因此（作为其特征多项式的零点）在 R 上整。相应地可得，$t_1 + t_2$ 是 $T_1 \otimes I_{m_2} + I_{m_1} \otimes T_2$ 的特征值，其中 I_k 是维数为 k 的单位矩阵（参见 [22]）。

唯一分解整环是整闭的这一命题，属于代数专业学生的基础知识；通常的证明甚至给出了更强的结论：最大公因子环是整闭的。然而，即使在代数数论课程中，人们也很少清楚地阐明整闭这一概念对于该学科发展有多么根本，以及自从 Dedekind 和 Emmy Noether 从 Dedekind 的理想理论体系中提炼出这一概念以来，它对现代代数具有何等重要的意义。事实上，只要看一眼下图就会发现，在代数入门课程中出现的大多数环的类都是整闭的：

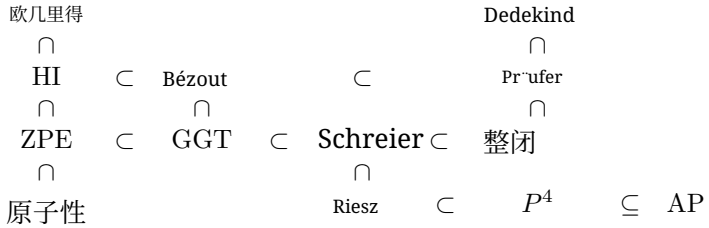


Abbildung 1. 环的类

$\mathbb{Z}$ 整闭性也是定理 1 成立的根本原因。事实上，若 $n \in \mathbb{Z}$ 是一个有理数的平方，例如 $\sqrt{n} = \frac{p}{q}$，那么 $\frac{p}{q}$ 就是二次多项式 $X^2 - n \in \mathbb{Z}[X]$的零点。由于 $\mathbb{Z}$ 是整闭的，因此必有 $\frac{p}{q} \in \mathbb{Z}$。

因此，利用¨的阶乘性来证明 $\sqrt{2}$ 的无理¨性，完全不足为奇。进一步地，可以尝试使用所有同样能够推出 $\mathbb{Z}$ 整闭性的定理来进行此类无理¨性证明。下面是一个例子：

[3]Kummer 并不了解代数整数的概念，也没有认识到整闭性的重要意义。他在圆分域中构造理想数之所以行得通，是因为 Kummer 所考察的环都是整闭的；然而，他关于理想数的理论体系存在一个缺口，后来 Dedekind 才利用整闭性将其弥补（参见 [26]）。Dirichlet 和 Eisenstein 也没有发现整闭性：Dirichlet 在形如 $\mathbb{Z}[\alpha]$的环中证明了单位定理，其中 α 是一个代数整数；而从 Eisenstein 的一条注记可以推出，代数整数构成一个环。Heine 将代数整数定义为能够通过环运算以及反复开取 n次根，从整数中得到的数。Dedekind 证明，在数域 $K \subseteq \mathbb{C}$ 的整数环中，每个非零理想都能唯一地分解为素理想的乘积；最终，Emmy Noether 于 1926年证明，这一定理适用于所有满足某些公理的整环——其中一条公理就是整闭性。[4]第 12 节和第 13 节将解释 Schreier 等尚未定义的概念。

$$\begin{aligned}\sqrt{m} \text{ ist rational} &\iff X^2-m \text{ ist reduzibel in } \mathbb{Q}[X]\\ &\iff X^2-m \text{ ist reduzibel in } \mathbb{Z}[X]\\ &\iff X^2-m=(X-n)(X+n) \text{ für ein } n\in\mathbb{Z}\\ &\iff m=n^2 \text{ für ein } n\in\mathbb{Z}.\end{aligned}$$

¨从 $\mathbb{Q}[X]$ 到 $\mathbb{Z}[X]$ 的过渡使用了高斯提升引理[5]，该引理适用于首一多项式¨:

引理2。若 $g,h\in\mathbb{Q}[X]$ 是首一多项式，且 $gh=f\in\mathbb{Z}[X]$，则$g,h\in\mathbb{Z}[X]$。

高斯提升引理以这种形式出现在《算术研究》中（即在 [15, 第 42]条），并在那里用于证明当 p为素数时，分圆多项式 $F_p(X)$的不可约性。为将它与其他同样以“高斯引理”之名著称的结果区分开来[6]，我们将引理2称为高斯提升引理（适用于首一多项式）。

利用引理2可以证明远不止某些平方根是无理数这一点：若¨ α 是一个具有整数系数的首一多项式的零点（也就是代数整数），那么 α 要么是整数，要么是无理数。事实上，若 α 是首一多项式 $f\in\mathbb{Z}[X]$的有理数零点，那么$f(X)=(X-\alpha)g(X)$，且 $g\in\mathbb{Q}[X]$ 为首一多项式。于是，适用于首一多项式的高斯提升引理表明 $X-\alpha\in\mathbb{Z}[X]$, 因此 $\alpha\in\mathbb{Z}$。

首一多项式的高斯提升引理是以下定理的一个特例

定理3（高斯提升引理）。设 $F\in\mathbb{Z}[X]$ 是一个多项式，且存在多项式 g、$h\in\mathbb{Q}[X]$，使得 $F=gh$，那么存在一个 $c\in\mathbb{Q}^\times$，满足$G=cg$、$H=\frac{1}{c}h\in\mathbb{Z}[X]$。因此，任意在 $\mathbb{Q}[X]$ 中的分解 $F=gh$ 都可以“提升”为在 $\mathbb{Z}[X]$ 中的分解 $F=GH$。

即使在今天的代数课程中，这个定理仍是证明多项式不可约性时的重要辅助工具，例如在证明 Eisenstein 判别法时就会用到：借助它可以证明，$\mathbb{Z}[X]$ 中次数为 ≥ 1 的本原多项式在 $\mathbb{Q}[X]$中不可约，当且仅当它在 $\mathbb{Z}[X]$ 中不可约。

设 R 是一个带有分式域 K 的整环，若每个从 $F\in R[X]$ 到 $R[X]$ 的因式分解都可以提升，我们就说高斯提升引理在 $R[X]$ 中成立；也就是说，对于任意满足 $g,h\in K[X]$ 的 $F=gh$，总存在一个 $c\in K^\times$，使得 $cg,\frac{1}{c}h\in R[X]$。现在我们来探讨上述版本的高斯提升引理在哪些环中成立。对于首一多项式，这个问题相对容易回答:

[5]这个名称旨在暗示，$\mathbb{Q}$ 上的多项式因式分解可以提升为 $\mathbb{Z}$ 上的因式分解。[6]至少有三个这样的结果：上文提到的提升引理，以及分别来自二次剩余理论和二次型理论的两个结果。这三者都见于《算术研究》。此外，高斯提升引理在 $\mathbb{Z}$ 中常以不同形式表述。这些版本虽然在 $\mathbb{Z}$上与上文所述的提升引理等价，但在一般整环上则不等价。

定理 4。设 R 是一个带有分式域 K 的整环。以下命题等价：

(1) R 是整闭的。(2) 在 $R[X]$ 中，对于首一多项式，高斯提升引理成立：若 g、$h \in K[X]$ 是首一多项式，且 $gh = f \in R[X]$，那么 g、$h \in R[X]$。
(3) 在 $R[X]$ 中，*Dedekind–Prager* 定理成立：

$$b(X) = \sum_{i=0}^{m} b_i X^i \quad und \quad c(X) = \sum_{j=0}^{n} c_j X^j \tag{1}$$

是 $R[X]$中的多项式，且 $a \mid b(X)c(X)$ 对于一个 $a \in R$，有 $a \mid b_i c_j$ 对于所有 $0 \le i \le m$、$0 \le j \le n$均成立。

在给出定理 4 的证明并考察一般提升引理的有效性之前，我们还要对 Dedekind–Prager 定理的意义作一些说明。

10. Dedekinds Prager Satz

从历史上看，Dedekind–Prager 定理在构建 Dedekind 的理想理论时发挥了重要作用。Dedekind 认为，在构建其理想理论时使用多项式进行论证并不恰当，并寻求其他途径。随后，赫尔维茨发表了一种理想理论的处理方法，该方法以 Dedekind–Prager 定理为基础（当时赫尔维茨并不知道这一点）；于是 Dedekind 解释说，他知道这条途径，但出于方法论上的原因，仍更倾向于自己的构建方式。希尔伯特的数论报告和 Landau 关于代数数的教材都采用了赫尔维茨的处理方法，而如今人们更倾向于使用局部化（这无疑会得到 Dedekind 的赞同）。

Dedekind [9] 给出了他的布拉格定理的两个证明；第一个见于 Landau [24]（希尔伯特在《数论报告》[20] 中没有给出证明，而是引用了 Dedekind [9], 、赫尔维茨 [21], 、Kronecker [23] 和默滕斯 [31]的著作），第二个证明则依赖于 Dedekind–Mertens 引理 f¨，该引理的历史与后续发展，尤其是 Artin 和 Rees 的贡献，值得专门撰写一篇文章加以探讨 h¨（参见 [7, 8]）。

---

[7]Dedekind 在《布拉格数学学会会刊》上发表了这一证明，如今“布拉格定理”这一名称已经约定俗成。[8]参见 Dedekind 对赫维茨的理想理论构建的评论，分别见第 53 页（“因为使用变量函数在我看来总像是一种与主题无关的辅助工具”）和第 55 页（“出于同样的原因，上文提到的证明……仍然不能完全使我满意，因为在我看来，变量函数的介入损害了理论的纯粹性”）。[9]Landau 在第 [24, 页将 Dedekind–Prager 定理称为“Kronecker 的定理”；在 Cohn 的著作中，它被称为“Hurwitz引理”。Walter Strobl 在其毕业论文第 [36, 页指出，Bachmann 在其五卷本数论教程的第三卷和第五卷中详细讨论了布拉格定理。另见 Edwards 的导论。[10]Dedekind 的定理用于证明：对于数域的极大阶中的每个理想 $\mathfrak{a} \neq (0)$，都存在一个理想 $\mathfrak{b} \neq (0)$，使得 $\mathfrak{ab}$ 为主理想。

这里我们将给出第三种证明，其依据是这样一个观察：Dedekind 的布拉格定理恰好在整闭环中成立[11]；由此，关于整闭性的布拉格定理 ¨等价于高斯关于首一多项式的提升引理 f¨。关键步骤(1) $\Longrightarrow$(3)依赖于一个经典引理，其本质上可追溯至 Kronecker¨：

引理 5 (Kronecker)。 设 R 是一个商域为 K的整环，并设$f(X) = \lambda\prod_{k=1}^{N}(X-\theta_k) \in R[X]$，其中 $\lambda \neq 0$ 和 θ_k 属于 K 的一个扩域 L。那么，对任意子集 $I \subseteq \{1,\dots,N\}$，元素 $\lambda\theta_I$都是 R上的整元，其中 $\theta_I = \prod_{k\in I}\theta_k$。

证明。 设 $e_1,\dots,e_N$是 θ_k的初等对称函数；因为 n $f = \lambda X^N - \lambda e_1 X^{N-1} \pm \dots$对所有 k都成立，而且显然 $\lambda \in R$。为 r 固定的 $r = |I|$，我们考虑多项式

$$P(Y) = \prod_{|J|=r}(Y - \lambda\theta_J),$$

其中 J遍历 $\{1,\dots,N\}$的所有含 r个元素的子集。 Y^{M-s}的系数（其中 $M = \binom{N}{r}$）为（-1）$^s\lambda^s E_s$，其中 E_s是 θ_J的第 s个初等对称函数。 E_s是关于 θ_1、.....、θ_N的对称多项式，系数为整数，且每个变量的次数至多为 s（每个θ_J 至多简单¨包含每个 θ_k 一次）。根据对称函数基本定理（以通常证明所给出的精确形式）， E_s因此是关于 e_1、.....、 e_N的一个总次数为 $\le s$、系数为整数的多项式。然而，对于每个满足 $v \le s$的单项式 $e_{k_1}\cdots e_{k_v}$，都有 $\lambda^s e_{k_1}\cdots e_{k_v} = \lambda^{s-v}(\lambda e_{k_1})\cdots(\lambda e_{k_v}) \in R$。因此， P是一个系数属于 R的首一多项式，而 $\lambda\theta_I$ 作为 P 的零点，在 R 上是整的。□

定理 *4* 的(1) $\Longrightarrow$ (2)：设 L 是 f ¨在 K上的一个分裂域；在其中， g和 h 也分解为一次因子，例如 $g(X) = \prod_i(X-\alpha_i)$ 和 $h(X) = \prod_j(X-\beta_j)$。由于 $f(\alpha_i) = f(\beta_j) = 0$， α_i 和 β_j 都是整 ¨于 R的。因此，关于 α_i 和 β_j的初等对称函数，也就是g 和 h的系数，都是整 ¨于 R的。由于它们属于 K，且 R 是整闭的，它们实际上属于 R，于是得到 g， $h \in R[X]$ （此证明出自 [4]）。

(2) $\Longrightarrow$ (1)：设 $t \in K$ 整 ¨于 R，即为一个首一多项式$f \in R[X]$的零点。那么 $f(X) = (X-t)g(X)$，其中 $g \in K[X]$是首一的；由 (2) 可知 $X - t \in R[X]$，因此 $t \in R$。

(1) $\Longrightarrow$ (3)：设 $a \mid b(X)c(X)$。若 $a = 0$ 或 $b = 0$ 或 $c = 0$，则无需证明（在 $a = 0$ 的情况下， $bc = 0$）。因此设 a、b、$c \neq 0$、 $b_m \neq 0 \neq c_n$，并且$f = \frac{bc}{a} \in R[X]$ 的首项系数为 $\lambda = \frac{b_m c_n}{a}$。在 bc¨关于 K的一个分裂域 L中，有 $b = b_m\prod_{k=1}^{m}(X-\beta_k)$、 $c = c_n\prod_{l=1}^{n}(X-\gamma_l)$，因此 $f = \lambda\prod_{k=1}^{m+n}(X-\theta_k)$，其中 $(\theta_1,\dots,\theta_{m+n}) = (\beta_1,\dots,\beta_m,\gamma_1,\dots,\gamma_n)$。现在

$$\frac{b_i c_j}{a} = \lambda\cdot\frac{b_i}{b_m}\cdot\frac{c_j}{c_n} = \pm\lambda\, e_{m-i}(\beta_1,\dots,\beta_m)\, e_{n-j}(\gamma_1,\dots,\gamma_n),$$

将右边展开后，得到一组形如 $\lambda\theta_I$mit $I \subseteq \{1,\dots,m+n\}$ 的项之和。由引理 5 可知，因此 $\frac{b_i c_j}{a} \in K$ 在 ¨上是整的，也就是说属于 R，即 $a \mid b_i c_j$。

[11]Emmy Noether 了解定理 4，这一点从她对 Dedekind 的文章 [10]in seinenWerken 的评论中可以清楚看出。

(3) $\Longrightarrow$ (1)：设 $t \in K$ 在 R 上是整的，也就是说，它是一个首一多项式 $f \in R[X]$的零点。那么， $f(X) = (X - t)g(X)$，其中 $g \in K[X]$ 是首一的；设 $a, b \in R \setminus \{0\}$，满足 $at \in R$ 和 $bg \in R[X]$。因此， $[a(X - t)][bg(X)] = abf(X)$ 可被 ab 整除，而 Dedekind–Prager 定理表明， $ab \mid atb$ 在 R 中成立（右边除符号外，是 $a(X - t)$ 的常数项与 $bg(X)$ 的最高系数 b 的乘积）；由此可得 $t = \frac{atb}{ab} \in R$。□

备注。按照“$f = \frac{b}{a} \cdot c$是 $K[X]$中的一个因式分解，因此可以将其提升”的思路，从 (2) 直接推出 (3) 是不可能的，因为一般而言， b 和 c 并非首一：为此需要一般的提升引理，而正如我们将会看到的，该引理只适用于施赖尔环。

Dedekind–Prager 定理在当今的代数和数论中实际上已不再发挥作用；正如 Dedekind 本人所指出的，这也合乎情理：该定理等价于基环的整闭性。依 Dedekind 之见，与其借助 Prager 定理给出计算性的证明，不如优先采用以整闭性等抽象原理为基础的概念性证明。历史证明他是正确的，正如 Emmy Noether 在评论 Dedekind 的著作时所写的那样；尽管希尔伯特在其《数论报告》中，尤其推崇赫维茨的理想理论构建。这一“失误”（从抽象代数的立场看；当然，希尔伯特的选择自有充分理由）大概也是 Emmy Noether 多次批评希尔伯特《数论报告》的缘由之一（参见 [27]）。

因此，布拉格定理无论如何都具有历史意义：随着人们背离布拉格定理，数学研究开始从计算型证明转向概念型证明，并开始运用抽象方法深入探究研究对象。这一转变由 Dedekind 开创，Emmy Noether 将其提升为一项纲领，而格罗滕迪克的工作[12] 则使之达到一个暂时的“高”潮。

11. Plus ça change ...

正如我们所见，对于整环上的首一多项式，“高斯提升引理”成立，当且仅当该环“是整闭的。一般的高斯提升引理则并非如此：多项式

$$2X^2 - 5 = 2(X - \tfrac{\sqrt{10}}{2})(X + \tfrac{\sqrt{10}}{2}) = (\sqrt{2}\,X - \sqrt{5}\,)(\sqrt{2}\,X + \sqrt{5}\,)$$

在“上可分解，在 $\mathbb{Q}(\sqrt{10})$（以及“在 $\mathbb{Z}[\sqrt{2}, \sqrt{5}]$上”），但不能在整闭环 $R = \mathbb{Z}[\sqrt{10}]$上分解。事实上，若提升引理“对 R 成立，那么我们就必须能够在 R 中将 2 分解为“（即能够“（也就是 $2 = \alpha\beta$ 借助 $\alpha, \beta \in R$）），使得因子 $\alpha(X - \frac{\sqrt{10}}{2})$和 $\beta(X + \frac{\sqrt{10}}{2})$的系数属于 R。然而，既然 2 在 $\mathbb{Z}[\sqrt{10}]$中不可约，那么 α 或 β 就是一个单位，这样就会得到“：矛盾。

现在或许会猜想，高斯提升引理失效的原因在于环 $\mathbb{Z}[\sqrt{10}]$ 不是唯一分解的。事实上，这离真相并不远：提升引理在 $R[X]$ 中成立与否，与 R 中欧几里得四数定理是否成立有关。借助

[12] W. Scharlau 最近“出版了一部值得一读的格罗滕迪克传记（[35]）”。

方程 $2\cdot 5=\sqrt{10}\sqrt{10}$ 很容易看出，元素 2 在 $\mathbb{Z}[\sqrt{10}]$中虽然不可约，却不是素元（因此也不是素元）。特别是，$\mathbb{Z}[\sqrt{10}]$ 不是 Riesz。现在我们来证明

命题 6。 若 $R[X]$ 是 *Riesz*，则在 $R[X]$ 中提升引理成立。

证明。设 $F\in R[X]$ 和 $F=gh$ 满足 g、$h\in K[X]$; 不妨设 $F\neq 0$。选择 ¨、b、$c\in R\backslash\{0\}$，使得 bg、$ch\in R[X]$ 成立，并令 $a=bc$。则 $aF=(bg)(ch)$ 属于 $R[X]$，由于 $R[X]$ 是 Riesz，存在 m、n、r、$s\in R[X]$，使得 $a=mr$、$bg=nr$、$ch=ms$ 以及 $F=ns$。由于 grad $a=0$ m¨，必有 m、$r\in R$。此外，$G=\frac{bg}{r}=n$ 和 $H=\frac{ch}{m}=s$ 都属于 $R[X]$，且存在 $F=\bar{G}\bar{H}$，满足 $G=\frac{b}{r}g$、$\bar{H}=\frac{c}{m}h$ 和 $\frac{b}{r}\cdot\frac{c}{m}=1$。因此提升引理成立。□

接下来我们想证明逆命题：若在 $R[X]$中高斯提升引理成立，则 $R[X]$ 是 Riesz。为此，我们必须证明所有元素都是 $R[X]$ 素元。朝这个方向迈出的第一步，是证明 R 中的所有素元都属于 $R[X]$。最后，一个更小的步骤是下面这个

引理 7. 若在 $R[X]$ 中高斯提升引理成立，则 R 是 *Riesz*。

证明。设 $ad=bc$ f¨对于 $a,b,c,d\in R$. 当 $abcd=0$ 时，结论很容易证明；因此我们可以假设 $abcd\neq 0$。现在考察多项式

$$F(X)=a\Big(X-\frac{b}{a}\Big)\Big(X-\frac{c}{a}\Big)=aX^2-(b+c)X+d\in R[X].$$

由于我们可以将这个因式分解提升到 $R[X]$，因此对于 $G,H\in R[X]$，有 $F(X)=G(X)H(X)$ f¨，其中 G 是 $X-\frac{b}{a}$ 的一个常数倍，而 H 是$X-\frac{c}{a}$的一个常数倍。因此，设 $G(X)=\alpha X-\beta$，且 $H(X)=\delta X-\gamma$，其中 $\alpha,\beta,\gamma,\delta\in R$。由于 G和 $g(X)=X-\frac{b}{a}$ 有相同的根，因此 $\frac{b}{a}=\frac{\beta}{\alpha}$，即 $\alpha b=\beta a$; 同理可得 $\gamma a=\delta c$。此外，通过比较系数可得 $a=\alpha\delta$ 和 $d=\beta\gamma$。由此推出.$bc=ad=a\beta\gamma=\beta\delta c$，即 $b=\beta\delta$。类似地可得 $bc=a\beta\gamma=b\alpha\gamma$，从而得到$c=\alpha\gamma$。综上，我们现在有 $a=\alpha\delta$, $b=\beta\delta$, $c=\alpha\gamma$ 和 $d=\beta\gamma$，这正是要证明的。□

注记。 注意，证明引理 7 时，只需假设二次多项式的高斯提升引理。

我们现在知道，在 Riesz 环中 $R[X]$ 高斯引理成立，而且由 $R[X]$ 中高斯引理成立¨可推出 R 是 Riesz 的。现在我们想证明，若 R 成立，$R[X]$ 也¨是 Riesz 的；然而这行不通：

命题 8。 如果所有 $a\in R$ 在 $R[X]$ 中也都是素元，那么 R 就是整闭的。特别地，如果 $R[X]$ 是 *Riesz* 的，那么 R 就是整闭的。

证明。设 $t\in K$ 在 ¨上整，R，即为某个首一多项式 $f\in R[X]$的零点。于是 $f(X)=(X-t)g(X)$ f¨对于某个首一 $g\in K[X]$。现在存在r、$s\in R\setminus\{0\}$，使得 $r(X-t)\ sg(X)\in R[X]$。根据假设，元素 $q=rs\in R$在 $R[X]$中是素元，并且有 $q\mid[r\cdot(X-t)][s\cdot g(X)]=rsf(X)$。因此，$q=ab$满足 $a\mid r\cdot(X-t)$ 和 $b\mid s\cdot g(X)$，其中 a、$b\in R$是单位，因为它们整除常数 q。由于 $X-t$和 $g(X)$都是首一的，必有 $a\mid r$和 $b\mid s$成立。由于 $ab=rs$

由此可知，$\frac{r}{a}$，$\frac{s}{b} \in R^\times$ 是单位。然而由 $\frac{r}{a}(X-t) \in R[X]$ 可得$t \in R$，因此 R 是整闭的。□

因此，为了将 R 在 $R[X]$ ¨ 上的 Riesz 性质推广到 ¨，我们需要 ¨ 的整闭性。事实证明，从提升引理推出 R 的 Riesz 性质时，其实并不需要预先假设这一点，因为它可以由提升引理推出：

命题 9。设 R 是一个整环。若 $R[X]$ 中成立高斯提升引理，则 R 是整闭的。

证明。设 K 是 R 的商域，且 $t \in K$ 在 R 上整，即它是多项式 $f(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in R[X]$ 的零点。那么在 $K[X]$ 中存在一个因式分解 $f(X) = (X-t)g(X)$，其中 $X-t, g(X) \in K[X]$。根据高斯提升引理，存在一个 $q \in K^\times$，使得 $q(X-t)$ 和 $\frac{1}{q}g(X)$ 都属于 $R[X]$。由于 $X-t$ 和 $g(X)$ 都是首一的，也就是说首项系数为 1，因此必有 $q \in R$ 和 $\frac{1}{q} \in R$。所以 $q \in R^\times$ 是单位，这意味着 $X-t, g(X) \in R[X]$。因此 $t \in R$，且 R 是整闭的。□

特别是，高斯提升引理对 $R = \mathbb{Z}[\sqrt{-3}]$ 不成立：显然，分解 $X^2 + X + \overline{1} = (X-\rho)(X-\rho^2)$（其中 $\rho = \frac{-1+\sqrt{-3}}{2} \in K = \mathbb{Q}(\sqrt{-3})$）无法~~提升为~~ $\overline{R[X]}$ 中的分解。

12. Cohns Permanenzsatz

现在回到我们的问题：我们要证明，高斯提升引理在 $R[X]$ 中成立，可以推出 $R[X]$ 是 Riesz 整环：我们已经看到，此时 R 是 Riesz 整环且为整闭；由此我们希望得出 $R[X]$ 也是 Riesz 整环。朝这个方向迈出的第一步是以下命题。

命题 10. 设 R 是 *Riesz* 整环且为整闭。那么所有 $a \in R$ 在 $R[X]$ 中也都是素元。

证明。设 $a \in R \setminus \{0\}$ 且 $a \mid b(X)c(X)$ f¨对于多项式 $b,\ c \in R[X] \setminus \{0\}$。由 Dedekind–Prager 定理可知[13] $a \mid b_i c_j$ f¨对于所有 $i,\ j$。由于 R 是 Riesz 群，整除群 $G(R)$ 是一个 Riesz 群；根据第一部分中的欧几里得细化性质（应用于非零系数；系数 0 可被任意元素整除），存在一个因式分解 $a = rs$，满足 $r \mid b_i$ 及 $s \mid c_j$ f¨ 对于所有 $0 \le i \le m$ 和 $0 \le j \le n$。因此，$r \mid b(X)$ 且 $s \mid c(X)$；换言之：a 在 $R[X]$中也是素元。□

备注。这里仅假设单个元素 a在 R 中的素元性是不够的：欧几里得细化性质 $E_{m,\ n}$ 利用了整个群 $G(R)$ 的插值性质，而不仅仅是 a的素元性。

由上述论述可得出以下定理：

定理 11. 设 R 是一个整环。那么以下性质等价：(1) $R[X]$是 *Riesz*。

[13]对于《几何原本》 $a, b, c \in R$ 在 R 中的关系与在 $R[X]$中的关系等价，因此我们无须区分 $a \mid_R bc$ 和 $a \mid_{R[X]} bc$。

(2) 在 $R[X]$ 中，高斯提升引理成立。(3) R 是 *Riesz* 且整闭。(4) $R[X]$ 是 *Riesz* 且整闭。

整闭的 Riesz 环也称为 Schreier 环（依 Cohn 命名）。

迄今我们已证明 (1) $\Longrightarrow$ (2) $\Longrightarrow$ (3)成立，而显然 (4) $\Longrightarrow$ (1) 是平凡的。因此，还需证明 Schreier 性质的“保持定理” (3) $\Longrightarrow$(4)。提升引理恰好在 Schreier 环中成立（这由 McAdam 与 Rush [30]证明），因此，鉴于其他蕴含关系相当显然，这在本质上等价于 Cohn 保持定理 (3) $\Longrightarrow$ (4)（参见 [29, 定理 9.12]）。

有些性质可以从一个环 R 遗传到多项式环$R[X]$ 。例如，众所周知，若 R ，则 $R[X]$ 也总是唯一分解的[14]。此外，成为最大公因子环（或整闭）的性质，也会从 R传递到 $R[X]$。由命题 8（以及一个 Riesz 环但非整闭的环的例子）可知，Riesz 性质并不总是 ¨传递的。

虽然“高斯定理”有几种简单的证明，但（3） $\Longrightarrow$ （4）的证明似乎更深奥；由于我只知道 Cohn 的证明[15][6] 以及 Anderson 与 Zafrullah[16] [1] 给出的版本，谨在此恳请读者思考这个定理的其他证明，或许还能找到更直接的证明。

为了证明在适当条件下 $R[X]$ 是 Riesz 环，我们必须从 $a \mid bc$ 关于多项式 $a, b, c \in R[X]$ 推出存在一种因式分解 $a = rs$，其中 $r, s \in R[X]$ ，且 $r \mid b$ 与 $s \mid c$ 满足相应条件。在最大公因子环中，我们可以直接令 $r = \mathrm{ggT}(a, b)$；在这里，如果转到欧几里得环 $K[X]$ ¨，也可以这样做，此时 K 是 R 的商域。由此得到一种因式分解 $a = \rho\sigma$ ，其中 $\rho, \sigma \in K[X]$ ，且 $\rho \mid b$、 $\sigma \mid c$ 也属于 $K[X]$。为了由此得到 $R[X]$ 中的因式分解，自然会想到应用高斯提升引理。因此，我们先证明定理 11 中的方向（3）$\Longrightarrow$ （2）：

命题 12. 若 R *Riesz* 环是整闭的，则在 $R[X]$ 中高斯提升引理成立。

证明。 设 $f \in R[X]$ 且 $f = gh$ 满足 g， $h \in K[X] \setminus \{0\}$。那么存在 b， $c \in R \setminus \{0\}$ 满足 bg， $ch \in R[X]$, 并且由 $a = bc$ 可得 $af = (bg)(ch)$, 因此 $a \mid (bg)(ch)$ 属于 $R[X]$。根据布拉格定理，对于所有 i， j，都有 $a \mid (bg)_i(ch)_j$ f¨ur，其中 $(bg)_i = bg_i$ 且

[14]这个定理常被称为高斯定理，尽管高斯既没有表述也没有证明它。大概直到 Hensel 才首次明确地表述并证明了这个定理， [19], 当然，Kronecker 早已知道一些特殊情形，¨例如多项式环的唯一分解性质。 $\mathbb{Z}[X_1, \ldots, X_n]$（该定理也可能早已出现在代数课程中，例如 Emil Artin 和 Emmy Noether 的课程；无论如何，它不久之后便见于 van der Waerden 的著作，¨该书是以这些课程为基础的。）“高斯定理”这一名称大概源于 van der Waerden 在¨这里的如下评论：“这里要给出的证明源自高斯。” [39], 事实上，他借助高斯引理证明了该定理。¨这里给出的证明结构不同于 Cohn 的证明（后者采用了一条途径， [39] 借助一个类似于 Nagata 定理（参见例如 ¨）的结果，建立环的 Schreier 性质与其局部化之间的联系，¨），但实质上使用了相同的工具：Riesz 环中的插值性质或细化性质，以及 Dedekind–Prager 定理。[15]他们的证明和我们的证明一样，使用了欧几里得细化性质。

$(ch)_j = ch_j$ 表示 bg 和 ch 的系数。Riesz 群 $G(R)$中的欧几里得细化性质给出了一个因式分解$a = rs$，满足 $r \mid bg_i$，且对所有 i，j，都有 $s \mid ch_j$f¨ur。因此， $G = \frac{b}{r}g$和 $H = \frac{c}{s}h$是 $R[X]$中的多项式，并且有 $GH = \frac{bc}{rs}gh = f$。这正是要证明的。□

现在我们加强引理 7 的结论，并证明定理 11 中的 (2) $\Longrightarrow$(1)；由于我们已经知道，在 $R[X]$ 中高斯提升引理成立，可推出 R 的整闭性，进而也可推出 $R[X]$ 的整闭性，因此我们也证明了 (2) $\Longrightarrow$(4)，从而证明了整个定理 11。

命题 13. 若高斯提升引理在 $R[X]$ 中成立，则 $R[X]$ 是 *Riesz* 群。

证明. 根据引理 7 和命题 9， R 是 Riesz 群且整闭；特别地，Dedekind–Prager 定理（定理 4）在 $R[X]$中成立，并且整除群$G(R) = K^\times/R^\times$ 是一个 Riesz 群，因此具有插值性质 $R_{m,\,n}$对所有 m， n均成立（第一部分）。我们仍将 x，$y \in K^\times$写作 $x \le y$，当$\frac{y}{x} \in R$ 成立时；特别地， $1 \le x$ 就表示 $x \in R$。

设 $a \mid bc$，也就是说，对于多项式 a、b、c、$d \in R[X]$，有 $ad = bc$f¨。若其中一个多项式等于 0，则命题很容易验证；因此设 a、b、c、$d \neq 0$。由于 $K[X]$ 是最大公因子环，存在多项式 r、s、t、$u \in K[X]$，使得 $a = rs$、 $d = tu$，以及 $b = rt$ 和 $c = su$。由于 $R[X]$ 中高斯提升引理成立，我们可以对 r、s、t、u 作常数因子的调整，使得 r、s、t、$u \in R[X]$ 成立，并保持方程 $a = rs$ 和 $d = tu$ 不变。此时另外两个方程只在相差常数因子的意义下成立：存在一个 $q \in K^\times$，使得 $b = q\,rt$；又由于 $rt \cdot su = ad = bc = q\,rt \cdot c$，因此 $c = q^{-1}su$。

设$q = \frac{\beta}{\alpha}$取为 $\alpha, \beta \in R$，则 $\alpha b = (\beta r)t$，因此 $\alpha \mid (\beta r)t$ 属于 $R[X]$，而 Dedekind–Prager 定理给出 $\alpha \mid \beta r_i t_j$，也就是说，对于 r 中任意非零系数 r_i 以及 t中任意非零系数 t_j，都有 $1 \le qr_it_j$ f¨。同理，由 $\beta c = (\alpha s)u$可得，对于 s 中任意非零系数 s_k 以及 u 中任意非零系数 u_l，都有 $1 \le q^{-1}s_ku_l$ f¨。

现在我们要寻找一个 $\kappa \in K^\times$，使得

$$r' = \kappa r, \quad s' = \kappa^{-1}s, \quad t' = q\kappa^{-1}t, \quad u' = q^{-1}\kappa u$$

属于 $R[X]$。那么显然 n¨amlich $a = rs = r's'$, $d = tu = t'u'$, $b = q\,rt = r't'$ 和 $c = q^{-1}su = s'u'$，而 $a \mid bc$ 已按所需形式分解。条件$r', s', t', u' \in R[X]$ 为

$$r_i^{-1} \le \kappa, \quad qu_l^{-1} \le \kappa, \quad \kappa \le s_k, \quad \kappa \le qt_j$$

对于所有 i, j, k, l（系数均不为 0）。根据 Riesz 插值性质，只要每个左端界都小于每个右端界，就存在这样的 κ。而事实确实如此：

- $r_i^{-1} \le s_k$ 表示 $1 \le r_is_k$，这由 $r_is_k \in R$ 可知成立；
- $r_i^{-1} \le qt_j$ 表示 $1 \le qr_it_j$，见上文；
- $qu_l^{-1} \le s_k$ 表示 $1 \le q^{-1}s_ku_l$，见上文；
- $qu_l^{-1} \le qt_j$ 表示 $1 \le t_ju_l$，这由 $t_ju_l \in R$ 可知成立。

至此，证明完成。 □

还要再次指出，Cohn 保持定理的概念性证明将会非常受欢迎。

13. Andere Formen des Gaussschen Lemmas

许多资料对高斯引理的表述有所不同。若 R 是一个整环，则当多项式 $f \in R[X]$ 本原 的系数的每个公因子都是 f 中的单位时，称该多项式为 $f \in R[X]$ 本原。若 R 是一个最大公因子环，且 $f(X) = f_0 + f_1X + \ldots + f_nX^n$，则称 ct($f$) =ggT($f_0$, f_1, ……, f_n) 为 f 的内容。正如 Dedekind（在 $R = \mathbb{Z}$ 的情形下；参见 [9]）所指出的，高斯提升引理可以表述如下。

引理 14. 若 R 是唯一分解环（或者甚至只是最大公因子环），则本原多项式的乘积在 $R[X]$ 中仍是本原的。更确切地说，对于 f、$g \in R[X]$，有 $\mathrm{ct}(fg) = \mathrm{ct}(f)\,\mathrm{ct}(g)$（相差一个单位）。

多项式的内容 ct(f) 具有如下性质：对于 $a \in R$ 和 $g \in R[X]$，ct(ag) $= a$ ct(g)；特别地，由 $a \mid f$ 可知，对于 $f \in R[X]$，总有 $a \mid$ ct(f)。

由此可得最大公因子整环的提升引理：若 $F = gh$ 是多项式，且 $F \in R[X]$ 和 g、$h \in K[X]$，则存在 a、$b \in R \setminus \{0\}$，使得 ag、$bh \in R[X]$。因此，$abF = (ag)(bh)$ 是一个在 $R[X]$中的分解，并且有 ab ct(F) = ct(ag) ct(bh)。由$r =$ ggT(ab, ct(ag)) 和 $s = \frac{ab}{r}$，可得 $ab = rs$，其中 $r \mid ag$；由于$\overline{s} = \frac{ab}{r}$ 和 ct($_{ag}$) 互素，且 $s \mid$ ct($_{ag}$) $_r$ ct(bh)，故也有$\overline{s} \mid$ ct(bh)，即 $s \mid bh$。因此，$G = \frac{a}{r}g$和 $H = \frac{b}{s}h = \frac{r}{a}h$是 $R[X]$中的多项式，且满足 $F = GH$。

定义。如果两个本原多项式的乘积在 $R[X]$中仍为本原多项式，我们就称 R为一个 P^4-环（¨表示：本原多项式的乘积是本原的）。

我们已经看到，对于 $R[X]$中的首一多项式，高斯提升引理成立，当且仅当 R（因而 $R[X]$）是整闭的，或者说，当 Dedekind–Prager 定理成立时。相应地，对于任意多项式，高斯提升引理恰好在 Schreier 环中成立。也不难证明，P^4-环介于 Riesz 环与 AP 环之间（见图 1；事实上，只要线性多项式满足 P^4-性质，就已经可以推出 AP）。最后，引理 14 形式的高斯引理成立，当且仅当 R是最大公因子环。

现在可以在任意整环中考察由 f 的系数生成的理想 c(f)，并探究在什么条件下方程 c(fg) = c(f)c(g) 成立。对此，以下定理给出了答案：

定理 15. 对于整环 R，以下命题等价：

(1) 每个有限生成理想都是投射的。(2) 每个非零有限生成理想 $\neq(0)$ 都是可逆的。(3) 对于每个非零素理想 $P \neq(0)$，局部化 R_P 是赋值环。(4) 每个满足 $R \subseteq S \subseteq K$ 的环 S 都是整闭，其中 K 是 R 的商域。(5) 对于所有多项式 f、$g \in R[X]$，有 $\mathfrak{c}(fg) = \mathfrak{c}(f)\mathfrak{c}(g)$。

证明。 Sh. [16, 第 IV 章]。 □

因此，这一版本的高斯引理当且仅当系数环是施赖尔环时成立。Prüfer本人（见 [33, 第 23]页）将该定理 c（fg） = c（f） c（g）称为“高斯–克罗内克–戴德金定理”。

Zu guter Letzt ...

撰写本文的动机主要源于我对 [29] （其中讨论了施赖尔环中的高斯提升引理）和 [32] （其中探讨了欧几里得证明其第七卷命题19时存在的缺漏）的阅读，以及希望以略有不同的方式整理其中内容的愿望。此外，我还要感谢Bill Dubuque在sci.math中发表的各种文章，尤其是在开始阶段，它们对我帮助很大。最后，我还要感谢Heinz Lüneburg和Klaus Volkert，以及两位匿名审稿人提出的大量有益且富有帮助的意见。

第二部分：高斯引理与里斯域

Abstract. 在我们关于欧几里得四数定理的文章的第二部分（参见{v2）中，我们从不可公度性的概念出发，进一步考察代数数的无理性证明。在此过程中，我们会遇到高斯引理、整闭包和戴德金布拉格定理，最后又回到四数定理。

8. The Ancient Greeks once more: incommensurability

众所周知，毕达哥拉斯学派也因发现不可公度性而受到赞誉，也就是说，他们观察到，例如，正方形的对角线 d与边s 之间不存在有理比，因此无法用自然数 p,q写成 $d:s=p:q$。关于这一论断，有许多种证明，其中两种可追溯至古希腊人：

- 一种证明从 $\sqrt{2}=\frac{p}{q}$ 推出 p和 q 都必须是偶数，这与分数（或比例）的可约性相矛盾。这一证明可追溯至亚里士多德，并见于某些（较早的）《几何原本》版本中，作为命题 X.117；然而如今人们认为它是后来的插入内容。
- 另一种证明（参见 Hasse [17] 和 Apostol [2]）本质上是几何学的，基于“连续相减法”（倒数相减），而连续相减法是欧几里得算法的前身。

毕达哥拉斯学派已经发现了不可公度线段的存在，这一点被认为是确定无疑的；至于是否是希帕索斯作出了（或公开了）这一发现，则尚不确定；同样不确定的还有一种说法，即他是在研究五角星（参见 von Fritz [14]）时得出这一发现的。最后，偶尔还能见到一种说法，认为这在希腊数学中造成了“基础危机”；但这一说法如今已无法得到任何历史事实的支持（这并不意味着它必然是错误的）。

随着数概念的扩展，线段的不可公度性已经从几何问题转变为算术问题：对我们而言，两条线段的比简单地就是一个数，而正方形的边与对角线的不可公度性，就是平方根 2 的无理性。

如果知道环 $\mathbb{Z}$ 是唯一分解的，那么 $\sqrt{2}$的无理性证明就变得微不足道：由 $2q^2=p^2$ 可以看出，2 在左边以奇数次幂整除，而在右边以偶数次幂整除：矛盾。

同样的证明更一般地表明[17]：

定理 16。对于 $m\in\mathbb{Z}$，$\sqrt{m}$ 是有理数，当且仅当 m 是某个整数的平方。

这同样是一个希腊人基本上已经知晓的定理；然而，在欧几里得的《几何原本》中找不到以这种明确形式表述的内容。

我们不必借助唯一分解来证明 $\sqrt{2}$ 的无理性，也可以使用带余欧几里得除法得到这一结论（鉴于欧几里得环是唯一分解环，这当然不足为奇）：设 $m\in\mathbb{N}$ 为非平方数；那么存在一个 $n\in\mathbb{N}_0$，使得 $n^2<m<(n+1)^2$,，即 $0<\sqrt{m}-n<1$。如果 $\sqrt{m}$ 是有理数，我们可以将其写成 $\sqrt{m}=\frac{p}{q}$，其中 $q\in\mathbb{N}$取最小值。

[17]没有唯一分解，这一结论就不成立：在由所有自然数组成的幺半群 $M\equiv 0,\ 1,\ 2$ 模 4 中，数 9 是商幺半群中分数 $\frac{6}{2}$的平方，但不是 M中某个元素的平方。同样，$2i$在 $\mathbb{Z}[2i]=\mathbb{Z}\oplus 2i\mathbb{Z}$中不是平方，但它是商域 $\mathbb{Q}(i)$中的平方，因为 $2i=(1+i)^2=(\frac{2+2i}{2})^2$。

于是 $r := q(\sqrt{m} - n) = p - nq$ 也是一个整数，而 $0 < \sqrt{m} - n < 1$ 蕴含 $0 < r < q$。现在 $r\sqrt{m} = q(\sqrt{m} - n)\sqrt{m} = mq - nq\sqrt{m} = mq - np$ 是一个整数；由于 $\sqrt{m} = \frac{r\sqrt{m}}{r}$，这与 q 的最小性相矛盾。关于这类论证的推广[18] 以及其他无理性证明，参见例如[28,第 1] 章中的练习。

这里给出一个基于 $\mathbb{Z}$ 是贝祖整环这一事实的证明；它更一般地表明，整数 m 的有理 n 次根本身就是整数：设 $\sqrt[n]{m} = \frac{p}{q}$，其中 p 和 q 是互素整数，即 $(p,\ q) = (1)$。那么 $p^n = mq^n$ 给出

$$(1) = (p, q)^n \subseteq (p^n, q) = (mq^n, q) \subseteq (q),$$

因此 $(q) = (1)$，所以 $q = \pm 1$ 和 $\sqrt[n]{m} = \pm p$ 是整数。

这类证明或许十分优美，但在某种意义上，它们掩盖了问题的真正核心；下一节我们将揭示这一核心。

9. Integral closure

学生通常会在代数入门课程中接触到整闭包这一概念：如果 R 是一个商域为 K 的整环，那么若元素 $t \in K$ 是首一多项式 $f \in R[X]$ 的根，就称 $t \in K$ 在 R 上整；如果每个在 R 上整的 $t \in K$ 都属于 R，那么就称 R 是整闭的（在其商域中）。

如果 t_1，t_2（在 K 的某个扩域中）在 R 上都是整的，那么 $t_1 + t_2$ 和 $t_1 t_2$ 也都是整的。随着时间推移，使用结式的经典证明已被基于有限生成模的证明所取代；不过，若用张量的语言来表述，经典证明的优雅程度几乎不逊于模证明：作为一个次数为 m_j、系数属于 R 的首一多项式的根，t_j 也是一个 $m_j \times m_j$ 矩阵 T_j（伴随矩阵）的特征值，该矩阵的元素属于 R。现在很容易证明，$t_1 t_2$ 是克罗内克积 $T_1 \otimes T_2$ 的特征值，因此（作为其特征多项式的一个根）在 R 上是整的。同理，$t_1 + t_2$ 是 $T_1 \otimes I_{m_2} + I_{m_1} \otimes T_2$ 的特征值，其中 I_k 表示维数为 k 的单位矩阵（见 [22]）。

唯一分解整环是整闭的这一[19] 定理，属于代数学生应掌握的基础知识；通常的证明甚至给出了更强的结论，即最大公因子整环是整闭的。然而，即使在代数数论课程中，人们也很少明确说明，整闭包这一概念对于该学科的发展是多么根本，以及自 Dedekind 和 Emmy Noether 从 Dedekind理想理论的构建中提炼出这一概念以来，它对现代代数获得了何等重要的意义。事实上，只需看一下下面的图表就会发现，

---

[18]这一证明本质上可追溯至 Dedekind [11]；关于 Haj´os 所提出的这一证明的几何版本，参见 [37]。这一证明的变体还可见于其他文献，例如 [3, 13, 34, 38, 40]。[19]Kummer 并不了解代数整数这一概念，也未能认识到整闭包的重要性。他在分圆域中构造理想数之所以可行，是因为 Kummer 所研究的环都是整闭的；然而，他发展理想数理论时留下了一个漏洞，后来 Dedekind 运用整闭包填补了这一漏洞（参见 [26]）。Dirichlet 和 Eisenstein 也没有认识到整闭包：Dirichlet 在形如 $\mathbb{Z}[\alpha]$ 的环中证明了他的单位定理，其中 α 是一个代数整数；而从 Eisenstein 的一条注记可以推出，代数整数构成一个环。Heine [18] 将代数整数定义为那些可以通过环运算以及反复开 n 次方从整数得到的数。Dedekind 证明，在数域 $K \subseteq \mathbb{C}$ 的整数环中，每个非零理想 $\neq$ 都能唯一分解为素理想的乘积；最终，1926年 Emmy Noether 成功证明，这一定理适用于满足某些公理的所有整环，其中一条公理就是整闭性。

代数入门课程中出现的大多数环的类别[20]都是整闭的：

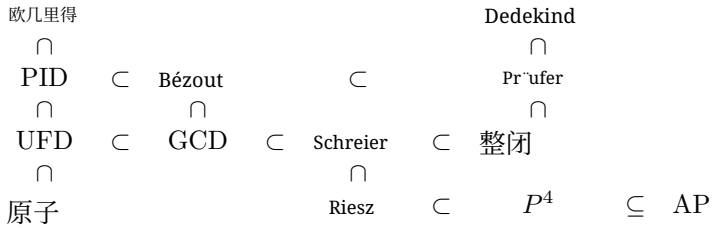


ABBILDUNG 2. 环的类别

$\mathbb{Z}$ 的整闭包也是定理 16成立的真正原因。事实上，如果 $n \in \mathbb{Z}$ 是一个有理数的平方，比如说 $\sqrt{n} = \frac{p}{q}$，那么 $\frac{p}{q}$ 就是二次多项式 $X^2 - n \in \mathbb{Z}[X]$的一个根。由于 $\mathbb{Z}$ 是整闭的，我们必有$\frac{p}{q} \in \mathbb{Z}$。

因此，利用 $\mathbb{Z}$的唯一分解性来证明 $\sqrt{2}$ 的无理性，完全不足为奇。此外，也可以尝试利用任何能够推出 $\mathbb{Z}$ 的整闭包的定理来给出这样的无理性证明。下面就是一个例子：

$$\begin{aligned}
\sqrt{m} \text{ is rational} &\iff X^2 - m \text{ is reducible in } \mathbb{Q}[X] \\
&\iff X^2 - m \text{ is reducible in } \mathbb{Z}[X] \\
&\iff X^2 - m = (X-n)(X+n) \text{ for some } n \in \mathbb{Z} \\
&\iff m = n^2 \text{ for some } n \in \mathbb{Z}.
\end{aligned}$$

从 $\mathbb{Q}[X]$ 到 $\mathbb{Z}[X]$ 的过渡通过首一多项式的高斯提升引理[21] 实现：

引理 17. 若 $g, h \in \mathbb{Q}[X]$ 是满足 $gh = f \in \mathbb{Z}[X]$的首一多项式，则$g, h \in \mathbb{Z}[X]$。

高斯提升引理以这种形式出现在《算术研究》中（即第 [15, Art. 42] 条），其中它被用于证明素数 p 的分圆多项式 $F_p(X) = \frac{X^p-1}{X-1}$ 的不可约性。为了将它与其他也称为“高斯引理”[22], 的结果区分开来，我们将引理 17 称为高斯提升引理（针对首一多项式）。

[20]Schreier 或 P^4 等尚未定义的概念，将在第 12 节和第 13 节中解释。[21]这个名称意在表明，多项式在 $\mathbb{Q}$ 上的因式分解可以提升为在 $\mathbb{Z}$上的因式分解。[22]至少有三个这样的结果：上面的提升引理，以及分别来自二次剩余理论和二次型理论的结果。这三者都见于《算术研究》。此外，$\mathbb{Z}$ 中的高斯提升引理通常有不同的表述；虽然这些表述与上文所述的提升引理在 $\mathbb{Z}$上等价，但在一般整环上并不等价。

引理 17 让我们能够证明的不仅仅是某些平方根的无理性：如果 α 是一个整数系数首一多项式的根（即一个代数整数），那么 α 要么是整数，要么是无理数。事实上，如果 α 是首一多项式 $f \in \mathbb{Z}[X]$ 的有理根，那么 $f(X) = (X-\alpha)g(X)$，其中 $g \in \mathbb{Q}[X]$ 是首一的。随后，首一多项式的高斯提升引理表明 $X - \alpha \in \mathbb{Z}[X]$，因此 $\alpha \in \mathbb{Z}$。

首一多项式的高斯提升引理是以下定理的特例

定理 18 (高斯提升引理)。若 $F \in \mathbb{Z}[X]$ 是一个多项式，且存在多项式 g、$h \in \mathbb{Q}[X]$，使得 $F = gh$，那么就存在一个 $c \in \mathbb{Q}^\times$，使得 $G = cg$、$H = \frac{1}{c}h \in \mathbb{Z}[X]$。因此，$\mathbb{Q}[X]$ 中的每个因式分解 $F = gh$ 都可以“提升”为 $\mathbb{Z}[X]$ 中的一个因式分解 $F = GH$。

这一定理仍是当今代数课程中证明多项式不可约性的重要工具，例如，它被用于艾森斯坦判别法的证明：借助它可以证明，$\mathbb{Z}[X]$ 中一个次数为 ≥ 1 的本原多项式在 $\mathbb{Q}[X]$ 中不可约，当且仅当它在 $\mathbb{Z}[X]$ 中不可约。

若 R 是一个商域为 K 的整环，我们称高斯提升引理在 $R[X]$ 中成立，是指每个 $F \in R[X]$ 的因式分解都可以从 $K[X]$ 提升到 $R[X]$；也就是说，对于满足 g 的每个因式分解 $F = gh$，$h \in K[X]$，都存在一个 $c \in K^\times$，使得 cg，$\frac{1}{c}h \in R[X]$。现在我们来考察上述版本的高斯提升引理在哪些环中成立。对于首一多项式，这个问题相对容易回答：

定理 19。设 R 是一个商域为 K 的整环。那么以下命题等价：

(1) R 是整闭的。(2) 首一多项式的高斯提升引理在 $R[X]$ 中成立：若 g、$h \in K[X]$ 是首一多项式，且 $gh = f \in R[X]$，那么 g、$h \in R[X]$。(3) 戴德金布拉格定理在 $R[X]$ 中成立：若

$$b(X) = \sum_{i=0}^{m} b_i X^i \quad and \quad c(X) = \sum_{j=0}^{n} c_j X^j \tag{2}$$

是 $R[X]$ 和 $a \mid b$ 中的多项式 $(X)c(X)$ 对于某个 $a \in R$ 成立，那么对于所有 $0 \leq i \leq m$、$0 \leq j \leq n$，$a \mid b_i c_j$。

在给出定理 19 的证明并考察一般提升引理是否成立之前，我们先对戴德金布拉格定理的重要性作几点评论。

10. Dedekind's Prague theorem

从历史上看，戴德金布拉格定理[23] 在构建戴德金理想理论的过程中发挥了重要作用。戴德金认为，在构建理想理论时用多项式进行论证并不恰当[24]，于是寻找其他

[23]戴德金在布拉格数学学会的期刊上发表了这一定理，如今“布拉格定理”这一名称已广为确立。[24]参见戴德金对赫尔维茨理想理论方法的评论，[10], 例如第 53 页，他在那里说，变量函数的使用在他看来始终是与该主题格格不入的辅助工具；又如第 55 页，他在那里说，上文提到的证明仍不能令他满意

方法。赫尔维茨 [21] 随后发表了一种以戴德金布拉格定理为基础的理想理论方法（当时赫尔维茨并不知道这一点），戴德金于是声明，自己也知道这条路，但出于方法论上的考虑，他更倾向于自己的方法。希尔伯特《数论报告》 [20] 和 Landau[25] 关于代数数的教科书 [24] 都采用了赫尔维茨的方法[26], ，而如今人们更倾向于使用局部化（这显然会得到戴德金的赞同）。

Dedekind [9]给出了布拉格定理的两种证明；第一种见于 Landau [24] （希尔伯特在他的《数论报告》 [20], 中没有给出证明，而是提到了 Dedekind [9], 、赫尔维茨 [21], 、 Kronecker [23] 和默滕斯 [31] 的论文），第二种证明导出了戴德金 – 默滕斯引理。该引理的历史及其进一步发展——其中包括 Artin 和 Rees 的工作——值得专门撰写一篇文章（参见 [7, 8]）。

这里我们想给出第三种证明，其依据是这样一个观察：Dedekind布拉格定理恰好在整闭整环[27]中成立；因此，通过整闭包，布拉格定理等价于首一多项式的高斯提升引理。关键步骤 (1) $\Longrightarrow$ (3) 建立在一个基本引理之上，该引理实质上可追溯至 Kronecker：

引理20 (Kronecker)。 设 R 是一个整环，其商域为 K，并设 $f(X)=\lambda\prod_{k=1}^{N}(X-\theta_k)\in R[X]$，其中 $\lambda\neq 0$ 和 θ_k 属于某个K的 L。那么对于每个子集 $I\subseteq\{1,\dots,N\}$，元素 $\lambda\theta_I$（其中 $\theta_I=\prod_{k\in I}\theta_k$）都是整的，即整 *over* R。

证明。 设 e_1，……， e_N 是 θ_k 的初等对称函数；由于 $f=\lambda X^N-\lambda e_1X^{N-1}\pm\dots$, 对于所有 k，都有 $\lambda e_k\in R$，当然还有 $\lambda\in R$。固定$r=|I|$，考虑多项式

$$P(Y)=\prod_{|J|=r}(Y-\lambda\theta_J),$$

其中 J遍历 $\{1,\dots,N\}$ 的所有 r-元素子集。 Y^{M-s} 的系数（其中 $M=\binom{N}{r}$）为 $(-1)^s\lambda^sE_s$，其中 E_s 是 θ_J 的第 s 个初等对称函数。现在， E_s 是 θ_1，……， θ_N 中的对称多项式，具有整数系数，且每个变量的次数至多为 s（每个 θ_J 至多包含每个θ_k 一次）。根据对称函数基本定理（以其通常证明所提供的更精确形式）， E_s 因而是 e_1, ……， e_N 中总次数为 $\le s$ 的多项式，且具有整数系数。然而，对于每个满足 $v\le s$ 的单项式 $e_{k_1}\cdots e_{k_v}$，都有 $\lambda^se_{k_1}\cdots e_{k_v}=\lambda^{s-v}(\lambda e_{k_1})\cdots(\lambda e_{k_v})\in R$。因此， P 是一个首一多项式，其系数属于 R，而 $\lambda\theta_I$ 是 P 的一个根，所以它在 R 上是整的。□

定理*19*的(1) $\Longrightarrow$ (2)：设 L 是 K上 f 的分裂域；在该域中， g 和h 也分解为一次因子，即 $g(X)=\prod_i(X-\alpha_i)$ 和 $h(X)=\prod_j(X-\beta_j)$。

完全如此，因为在他看来，变量函数的介入损害了理论的纯粹性。[25]Landau [24, 第 145] 页将戴德金布拉格定理称为“Kronecker定理”；在 Cohn [5] 中，它被称为“Hurwitz引理”。Walter Strobl 在其论文 [36, 第157–161] 页指出，Bachmann 在其五卷本数论专著的第三卷和第五卷中详细讨论了布拉格定理。另请参阅 Edwards [12]中的引言。[26]戴德金定理用于证明：对于数域的极大序中的每个理想 $\mathfrak{a}\neq(0)$，都存在一个理想 $\mathfrak{b}\neq(0)$，使得 $\mathfrak{ab}$ 是一个主理想。[27]从 Emmy Noether 对其文集所收录的 Dedekind的文章 [10]所作的评论中，可以清楚看出她知道定理19。

由于 $f(\alpha_i) = f(\beta_j) = 0$， α_i和 β_j是 R上的整元。因此，关于 α_i 和 β_j的初等对称函数，即 g 和 h的系数，也都是 R 上的整元。由于它们属于 K，且 R 是整闭的，所以它们本来就属于 R，于是得到 $g,\ h \in R[X]$ （此证明取自 [4]）。

(2) $\Longrightarrow$ (1)：设 $t \in K$ 在 R上整，即它是一个首一多项式$f \in R[X]$的根。于是 $f(X) = (X - t)g(X)$，其中 $g \in K[X]$是首一的；由 (2) 可得$X - t \in R[X]$，即 $t \in R$。

(1) $\Longrightarrow$ (3)：设 $a \mid b(X)c(X)$。若 $a = 0$ 或 $b = 0$ 或 $c = 0$，则无需证明（若 $a = 0$，则 $bc = 0$）。因此设 $a, b, c \neq 0$, $b_m \neq 0 \neq c_n$，且 $f = \frac{bc}{a} \in R[X]$的首项系数为$\lambda = \frac{b_m c_n}{a}$。在 bc关于 K 的分裂域 L 中，有$b = b_m \prod_{k=1}^{m}(X - \beta_k)$、 $c = c_n \prod_{l=1}^{n}(X - \gamma_l)$，因此 $f = \lambda \prod_{k=1}^{m+n}(X - \theta_k)$，其中 $(\theta_1, \dots, \theta_{m+n}) = (\beta_1, \dots, \beta_m, \gamma_1, \dots, \gamma_n)$。现在

$$\frac{b_i c_j}{a} = \lambda \cdot \frac{b_i}{b_m} \cdot \frac{c_j}{c_n} = \pm\lambda\, e_{m-i}(\beta_1, \dots, \beta_m)\, e_{n-j}(\gamma_1, \dots, \gamma_n),$$

展开右侧可得一系列形如 $\lambda\theta_I$ with$I \subseteq \{1, \dots, m+n\}$ 的项。由引理20，$\frac{b_i c_j}{a} \in K$ 因而在 R 上整，因此属于R，即 $a \mid b_i c_j$。

(3) $\Longrightarrow$ (1)：设 $t \in K$ 在 R 上整，即是首一多项式$f \in R[X]$的一个根。于是 $f(X) = (X - t)g(X)$，其中 $g \in K[X]$ 为首一多项式；设 $a,\ b \in R \setminus \{0\}$ with$at \in R$ and $bg \in R[X]$。那么 $[a(X - t)][bg(X)] = abf(X)$ 可被 ab 整除，而戴德金布拉格定理表明 $ab \mid atb$ 属于 R （差一个符号，右侧是 $a(X - t)$ 的常数项与 $bg(X)$ 的首项系数 b的乘积）；这意味着 $t = \frac{atb}{ab} \in R$。□

注。不能用“$f = \frac{b}{a} \cdot c$ 是 $K[X]$中的一个因式分解，因此可以将其提升”这类论证直接从（2）推出（3），因为 b和 c 通常并非首一多项式：要做到这一点，就需要一般的提升引理；而我们将看到，这一引理只在施赖尔整环中成立。[28]

戴德金布拉格定理在当今代数和数论中几乎不起作用；正如戴德金本人所说，这也在情理之中：该定理等价于基环的整闭性。戴德金认为，与其借助布拉格定理给出计算性证明，不如采用整闭性等抽象原理进行概念性证明。历史证明了他的看法是正确的，正如 Emmy Noether 早已在她对戴德金著作的评论中指出的那样，尽管希尔伯特尤其是在《数论报告》中仍然更偏爱赫尔维茨的理想理论方法。这种“错误的选择”（从抽象代数的角度而言；希尔伯特的选择当然有充分理由）大概也属于 Emmy Noether 一再借以批评希尔伯特《数论报告》的那些问题之一（参见 [27]）。

无论如何，布拉格定理因此可以宣称自己具有历史意义：背离布拉格定理标志着一种运动的开始，即从计算性证明转向概念性证明，并以抽象手段深入研究对象；这一运动由 Dedekind 发起，由 Emmy

[28]保罗·波拉克于2016年指出了原证明中的错误。本译文中的修正归功于 Claude（Anthropic）。

Noether 使之成为自己的纲领，并在格罗滕迪克的工作中达到暂时的顶峰[29]。

11. Plus ça change ...

如我们所见，首一多项式的高斯提升引理在整环 R 上成立，当且仅当 R 是整闭的。一般的提升引理则并非如此：多项式

$$2X^2-5=2(X-\tfrac{\sqrt{10}}{2})(X+\tfrac{\sqrt{10}}{2})=(\sqrt{2}\,X-\sqrt{5}\,)(\sqrt{2}\,X+\sqrt{5}\,)$$

在 $\mathbb{Q}(\sqrt{10})$ 上（以及在 $\mathbb{Z}[\sqrt{2},\sqrt{5}\,]$ 上）可分解，但在整闭环 $R=\mathbb{Z}[\sqrt{10}\,]$ 上不可分解。事实上，若提升引理在 R 上成立，那么我们就必须能够在 R 中分解 2（即，$2=\alpha\beta$，其中 α，$\beta\in R$），使得因子 $\alpha(X-\frac{\sqrt{10}}{2})$ 和 $\beta(X+\frac{\sqrt{10}}{2})$ 的系数都属于 R。但由于 2 在 $\mathbb{Z}[\sqrt{10}\,]$ 中不可约，α 或 β 必为单位，于是 $\frac{\sqrt{10}}{2}\in R$：矛盾。

现在或许有人会猜测，高斯提升引理失效的原因在于环 $\mathbb{Z}[\sqrt{10}\,]$ 不是唯一分解的。事实上，这与真相相去不远：提升引理在 $R[X]$ 中是否成立，与欧几里得四数定理在 R 中是否成立有关。利用等式 $2\cdot5=\sqrt{10}\sqrt{10}$，很容易看出，$\mathbb{Z}[\sqrt{10}\,]$ 中的元素 2 是不可约的，但不是素元（因而也不是素元）。特别地，$\mathbb{Z}[\sqrt{10}\,]$ 不是里斯域。下面我们将证明

命题21。 如果 $R[X]$是里斯域，则提升引理在 $R[X]$中成立。

证明。设 $F\in R[X]$ 和 $F=gh$ 满足 g、$h\in K[X]$；不妨设$F\neq0$。取 b、$c\in R\setminus\{0\}$使得 bg、$ch\in R[X]$，并令 $a=bc$。则在 $R[X]$中，$aF=(bg)(ch)$，由于 $R[X]$是里斯域，存在 m、n、r、$s\in R[X]$，满足 $a=mr$、$bg=nr$、$ch=ms$ 和 $F=ns$。由于$\deg a=0$，必有m、$r\in R$。此外，$G=\frac{bg}{r}=n$ 和 $H=\frac{ch}{m}=s$ 都属于 $R[X]$，且 $F=GH$满足 $G=\frac{b}{r}g$、$H=\frac{c}{m}h$和 $\frac{b}{r}\cdot\frac{c}{m}=1$。因此提升引理成立。□

接下来，我们想证明其逆命题：如果高斯提升引理在 $R[X]$ 中成立，那么 $R[X]$ 是里斯域。为此，我们必须证明 $R[X]$ 的所有元素都是素元。朝这个方向迈出的第一步，是证明 R 的所有元素在 $R[X]$ 中都是素元。再往前迈一小步，便是下面这个命题

引理 22. 如果高斯提升引理在 $R[X]$ 中成立，那么 R 是里斯域。

证明。设 $ad=bc$ 为 a，b，c，$d\in R$。若 $abcd=0$，结论很容易验证；因此我们可以假设 $abcd\neq0$。现在考虑多项式

$$F(X)=a\Big(X-\frac{b}{a}\Big)\Big(X-\frac{c}{a}\Big)=aX^2-(b+c)X+d\in R[X].$$

由于我们可以将这个因式分解提升到 $R[X]$，因此有 $F(X)=G(X)H(X)$，其中G，$H\in R[X]$，其中 G是 $X-\frac{b}{a}$的常数倍，而 H是 $X-\frac{c}{a}$之一。因此，设 $G(X)=\alpha X-\beta$，且 $H(X)=\delta X-\gamma$，其中 α，β，γ，$\delta\in R$。由于 G与$g(X)=X-\frac{b}{a}$有相同的根，因此有 $\frac{b}{a}=\frac{\beta}{\alpha}$，即 $\alpha b=\beta a$；类似地，我们得到$\gamma a=\delta c$。此外，比较系数可得 $a=\alpha\delta$ 和 $d=\beta\gamma$。这意味着 $bc=ad=a\beta\gamma=\beta\delta c$，因此 $b=\beta\delta$。类似地，我们得到 $bc=a\beta\gamma=b\alpha\gamma$，从而

[29] W. Scharlau 最近出版了一部格罗滕迪克的传记 [35]，很值得一读。

$c = \alpha\gamma$。综上，我们现在有 $a = \alpha\delta$、 $b = \beta\delta$、 $c = \alpha\gamma$ 和 $d = \beta\gamma$，这正是我们要证明的。□

注。 请注意，引理 22 的证明只需要关于二次多项式的高斯提升引理。

现在我们知道，如果 $R[X]$ 是里斯域，则高斯引理在 $R[X]$ 中成立；并且，高斯引理在 $R[X]$ 中成立意味着 R 是里斯域。现在我们希望证明，只要 R 是里斯域， $R[X]$ 就是里斯域；然而，这是不可能的：

命题 23。 如果所有 $a \in R$ 在 $R[X]$ 中也是素元，那么 R 是整闭的。特别地，如果 $R[X]$ 是里斯域，则 R 是整闭的。

证明。设 $t \in K$ 在 R 上整，即为首一多项式 $f \in R[X]$ 的一个根。于是，对于某个首一 $g \in K[X]$，有 $f(X) = (X - t)g(X)$。现在存在 r、 $s \in R \setminus \{0\}$，使得 $r(X - t)$ $sg(X) \in R[X]$。根据假设，元素 $q = rs \in R$ 在 $R[X]$ 中是素元，并且 $q \mid [r \cdot (X - t)][s \cdot g(X)] = rsf(X)$。因此 $q = ab$，其中 $a \mid r \cdot (X - t)$ 且 $b \mid s \cdot g(X)$；由于它们整除常数 q，故有 a、 $b \in R$。由于 $X - t$ 和 $g(X)$ 是首一的，我们必有 $a \mid r$ 和 $b \mid s$。由于 $ab = rs$，这意味着 $\frac{r}{a}$、 $\frac{s}{b} \in R^\times$ 是单位。但此时 $\frac{r}{a}(X - t) \in R[X]$ 意味着 $t \in R$，因此 R 是整闭的。□

因此，为了将 R 的 Riesz 性质传递给 $R[X]$，我们需要 R 是整闭的。不过，事实证明，从提升引理推出 $R[X]$的 Riesz 性质时，我们不必作此假设，因为整闭性可由提升引理推出：

命题 24. 设 R 是一个整环。如果高斯提升引理在$R[X]$中成立，那么 R 是整闭的。

证明. 设 K 是 R 的商域，且设 $t \in K$ 在 R上整，即它是多项式 $f(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in R[X]$的一个根。于是，在 $K[X]$ 中存在一个因式分解 $f(X) = (X - t)g(X)$，其中 $X - t, g(X) \in K[X]$。根据高斯提升引理，存在一个 $q \in K^\times$，使得 $q(X - t)$ 和 $\frac{1}{q}g(X)$ 都属于 $R[X]$。由于 $X - t$ 和 $g(X)$ 都是首一的，即首项系数为 1，因此必有$q \in R$ 和 $\frac{1}{q} \in R$。于是 $q \in R^\times$ 是一个单位，这意味着 $X - t, g(X) \in R[X]$。因此， $t \in R$， 且 R 是整闭的。□

特别地，高斯提升引理在 $R = \mathbb{Z}[\sqrt{-3}]$ 上不成立：因式分解 $X^2 + X + 1 = (X - \rho)(X - \rho^2)$（其中 $\rho = \frac{-1+\sqrt{-3}}{2} \in K = \mathbb{Q}(\sqrt{-3})$）显然无法提升为 $R[X]$ 中的因式分解。

12. Cohn's permanence theorem

现在回到我们的问题：我们要证明，高斯提升引理在 $R[X]$ 中成立意味着 $R[X]$ 是一个里斯域：我们已经看到，此时 R 是一个里斯域且是整闭的；由此我们希望得出 $R[X]$ 也是一个里斯域。朝这个方向迈出的第一步是以下定理

命题25。 设 R 是一个整闭的 *Riesz* 域。那么所有 $a \in R$ 在 $R[X]$中也都是素元。

证明。设 $a \in R \setminus \{0\}$ 和 $a \mid b(X)c(X)$ 是多项式 $b, c \in R[X] \setminus \{0\}$。由戴德金布拉格定理可知，对于所有 i, j，都有[30] $a \mid b_i c_j$。由于 R 是一个 Riesz 域，其整除群 $G(R)$ 是一个 Riesz 群；根据第一部分中的欧几里得细化性质（应用于非零系数；系数 0 可被任意元素整除），存在因式分解 $a = rs$，其中 $r \mid b_i$，且对于所有 $0 \le i \le m$ 和 $0 \le j \le n$，都有 $s \mid c_j$。因此 $r \mid b(X)$ 且 $s \mid c(X)$；换言之：a 在 $R[X]$中也为素元。□

备注。在这里，仅假设单个元素 a 在 R 中是素元还不够：欧几里得细化性质$E_{m,n}$ 利用的是整个群 $G(R)$的插值性质，而不仅仅是 a 的素性。

根据我们上述的讨论，可以得到以下定理：

定理 26。设 R 是一个整环。则以下性质等价：

(1) $R[X]$ 是里斯域。(2) 高斯提升引理在 $R[X]$ 中成立。(3) R 是整闭里斯域。(4) $R[X]$ 是整闭里斯域。

整闭里斯域也被称为 Schreier 域（沿用 Cohn 的称呼）。

迄今我们已证明 (1) $\Longrightarrow$ (2) $\Longrightarrow$ (3)，当然 (4) $\Longrightarrow$ (1) 显然成立。尚待证明的是关于施赖尔性质的“保持定理” (3) $\Longrightarrow$ (4)。由于其他蕴含关系都相当直接，因此，提升引理恰好在施赖尔整环中成立这一事实（由 McAdam 与 Rush [30]证明）实质上等价于 Cohn 的保持定理 (3) $\Longrightarrow$ (4)（参见 [29, 定理 9.12]）。

有些性质会从环 R传递到多项式环 $R[X]$。例如，众所周知，若 R 是[31]，则 $R[X]$ 是唯一分解的。最大公因子整环的性质（或整闭性质）也会从 R 传递到 $R[X]$。命题 23（以及一个作为里斯域但非整闭的环的例子）表明，里斯性质并非总能传递。

虽然“高斯定理”有几种简单的证明，但（3）$\Longrightarrow$（4）的证明似乎更为深奥；我只知道 Cohn 的证明[32] [6] 及其由

---

[30]对于元素 a，b，$c \in R$，$a \mid bc$在 R中的关系等价于在 $R[X]$中的关系，因此我们无需区分 $a \mid_R bc$和 $a \mid_{R[X]} bc$。[31]这个定理通常被称为高斯定理，尽管高斯既没有表述也没有证明它。可能最早明确表述并证明该定理的是 Hensel [19],，不过像 $\mathbb{Z}[X_1, \ldots, X_n]$ 的多项式环具有唯一分解整环性质这样的特殊情形，Kronecker 当然早已知晓（该定理也可能曾出现在代数课程中，例如 Emil Artin 和 Emmy Noether 的课程；无论如何，不久之后便可以在 van der Waerden 的著作 [39], 中找到它，该书正是以这些课程为基础编写的）。“高斯定理”这一名称大概源于 van der Waerden 在 [39] 中的评论，即将要给出的证明可以追溯到高斯。事实上，他借助高斯引理证明了该定理。[32]这里给出的证明与 Cohn 的证明结构不同（Cohn 通过一个类似于 Nagata 定理的结果来进行证明（见例如 [28]），该结果建立了环 R 的施赖尔性质与其局部化 R_S的施赖尔性质之间的联系），但实质上使用了相同的工具：里斯域中的插值性质和细化性质，以及戴德金布拉格定理。

Anderson 和 Zafrullah[33] [1], 我热切鼓励读者进一步思考这个定理的证明，或许能找到更直接的证明。

为了证明在适当的假设下 $R[X]$ 是一个里斯域，我们必须从 $a \mid bc$ 推导出，对于多项式 a，b，$c \in R[X]$ 存在一个因式分解$a = rs$，其中 r，$s \in R[X]$ 满足 $r \mid b$ 和 $s \mid c$。在最大公因子整环中，我们可以直接令 $r = \gcd(a,\ b)$；在这里，如果从 $R[X]$ 转到欧几里得环 $K[X]$，其中 K 是 R的商域，这种做法也行得通。由此得到因式分解 $a = \rho\sigma$，其中 ρ，$\sigma \in K[X]$ 且 $\rho \mid b$、$\sigma \mid c$ 属于 $K[X]$。为了据此在 $R[X]$中得到因式分解，自然要应用高斯提升引理。因此，我们先证明定理26的方向 (3) $\Longrightarrow$(2):

命题27。若 R 是整闭的里斯域，则高斯提升引理在 $R[X]$ 中成立。

证明。设 $f \in R[X]$ 和 $f = gh$ 满足 g、$h \in K[X] \setminus \{0\}$。那么存在 b、$c \in R \setminus \{0\}$，满足 bg、$ch \in R[X]$，并且对于 $a = bc$，有 $af =$(bg)(ch)，即 $a \mid$(bg)(ch) 在 $R[X]$ 中。根据布拉格定理，对于所有 i、j，都有 $a \mid (bg)_i(ch)_j$，其中 $(bg)_i = bg_i$ 和 $(ch)_j = ch_j$ 分别表示 bg 和 ch的系数。里斯群 $G(R)$ 中的欧几里得细化性质给出一个因式分解 $a = rs$，满足 $r \mid bg_i$，且对于所有 i、j，都有 $s \mid ch_j$。因此 $G = \frac{b}{r}g$ 和 $H = \frac{c}{s}h$ 是 $R[X]$ 中的多项式，并且 $GH = \frac{bc}{rs}gh = f$。这正是我们要证明的。□

现在我们进一步精确表述引理 22，并证明定理 26 的 (2) $\Longrightarrow$ (1)；由于我们已经知道，高斯提升引理在 $R[X]$ 中成立意味着 R，因而也意味着 $R[X]$，是整闭的，因此我们也证明了 (2) $\Longrightarrow$(4)，从而证明了定理 26 的全部内容。

命题28. 如果高斯提升引理在 $R[X]$ 中成立，那么 $R[X]$ 是一个里斯域。

证明. 由引理 22 和命题24，R 是一个整闭的里斯域；特别地，戴德金布拉格定理在 $R[X]$ 中成立（定理19），且整除群 $G(R) = K^\times/R^\times$ 是一个 Riesz 群，因而具有插值性质 $R_{m,\ n}$对所有 m，n 均成立（第一部分）。和之前一样，如果 $\frac{y}{x} \in R$，我们记 $x \leq y$ 为 x，$y \in K^\times$；特别地，$1 \leq x$ 就是指 $x \in R$。

设 $a \mid bc$，即 $ad = bc$对于多项式 a、b、c、$d \in R[X]$。若这些多项式中有一个为 0，则结论容易验证；因此设 a、b、c、$d \neq 0$。由于 $K[X]$ 是最大公因子整环，存在多项式 r、s、t、$u \in K[X]$，使得 $a = rs$、$d = tu$，以及$b = rt$和 $c = su$。由于高斯提升引理在 $R[X]$中成立，我们可以通过常数因子调整 r、s、t、u，使得 r、s、t、$u \in R[X]$，且方程 $a = rs$ 和 $d = tu$ 仍然成立。于是另外两个方程只在相差常数因子的意义下成立：存在一个 $q \in K^\times$，使得 $b = q\,rt$；又由于 $rt \cdot su = ad = bc = q\,rt \cdot c$，因此有 $c = q^{-1}su$。

设 $q = \frac{\beta}{\alpha}$ with $\alpha, \beta \in R$，则有 $\alpha b =$ (βr)t，即 $\alpha \mid$ (βr)t 属于 $R[X]$，而戴德金布拉格定理给出 $\alpha \mid \beta r_i t_j$，即对于 r 的所有非零系数 r_i 以及 t的所有非零系数 t_j，都有 $1 \leq qr_it_j$。类似地，$\beta c =$ (αs)u 意味着对于 s 的所有非零系数 s_k 以及 u的所有非零系数 u_l，都有 $1 \leq q^{-1}s_ku_l$。

现在我们要寻找一个 $\kappa \in K^\times$，使得

$$r' = \kappa r, \quad s' = \kappa^{-1}s, \quad t' = q\kappa^{-1}t, \quad u' = q^{-1}\kappa u$$

[33]和我们一样，他们的证明也使用了欧几里得细化性质。

属于 $R[X]$。于是 $a = rs = r's'$、$d = tu = t'u'$、$b = qrt = r't'$ 和 $c = q^{-1}su = s'u'$，而 $a \mid bc$ 已被分解为所需的形式。条件 r'，s'，t'，$u' \in R[X]$ 读作

$$r_i^{-1} \le \kappa, \quad qu_l^{-1} \le \kappa, \quad \kappa \le s_k, \quad \kappa \le qt_j$$

对所有 i，j，k，l（系数非零）。根据黎斯插值性质，只要每个下界都小于每个上界，这样的 κ 就存在。而事实确实如此：

- $r_i^{-1} \le s_k$ 表示 $1 \le r_i s_k$，这成立是因为 $r_i s_k \in R$；
- $r_i^{-1} \le qt_j$ 表示 $1 \le qr_i t_j$，见上文；
- $qu_l^{-1} \le s_k$ 表示 $1 \le q^{-1}s_k u_l$，见上文；
- $qu_l^{-1} \le qt_j$ 表示 $1 \le t_j u_l$，这成立是因为 $t_j u_l \in R$。

证明至此完成。 □

我们再指出一次，若能给出 Cohn 永久性定理的概念性证明，将会非常受欢迎。

13. Other forms of Gauss's Lemma

在许多资料中，高斯引理的表述有所不同。若 R 是一个整环，则当 f 的系数的每个公因子都是 R 中的单位时，称多项式 $f \in R[X]$ 为本原的。若 R 是一个最大公因子整环，且 $f(X) = f_0 + f_1 X + \ldots + f_n X^n$，则 $\mathrm{ct}(f) = \gcd(f_0, f_1, \ldots, f_n)$ 称为 f 的内容。正如 Dedekind 所观察到的（在 $R = \mathbb{Z}$ 的情形下；见 [9]），高斯提升引理可以表述如下。

引理29。若 R 是一个唯一分解整环（或仅为最大公因子整环），则 $R[X]$ 中本原多项式的乘积仍是本原的。更确切地说：对于 f、$g \in R[X]$，有 $\mathrm{ct}(fg) = \mathrm{ct}(f)\,\mathrm{ct}(g)$（相差一个单位）。

多项式的内容 $\mathrm{ct}(f)$ 具有如下性质：对于 $a \in R$ 和 $g \in R[X]$，$\mathrm{ct}(ag) = a\,\mathrm{ct}(g)$；特别地，对于 $f \in R[X]$，$a \mid f$ 总是意味着 $a \mid \mathrm{ct}(f)$。

最大公因子整环的提升引理现在可如下得出：如果对于多项式 $F \in R[X]$ 和 g，$F = gh$ $h \in K[X]$，则存在 a、$b \in R \setminus \{0\}$，使得 ag、$bh \in R[X]$。因此，$abF = (ag)(bh)$ 是 $R[X]$ 中的一个因式分解，并且 $ab\,\mathrm{ct}(F) = \mathrm{ct}(ag)\,\mathrm{ct}(bh)$。由 $r = \gcd(ab, \mathrm{ct}(ag))$ 和 $s = \frac{ab}{r}$，我们于是得到 $ab = rs$，其中 $r \mid ag$；由于 $s = \frac{ab}{r}$ 与 $\mathrm{ct}(ag)_r$ 互素，且 $s \mid \mathrm{ct}(ag)_r\,\mathrm{ct}(bh)$，我们还得到 $s \mid \mathrm{ct}(bh)$，即 $s \mid bh$。因此，$G = \frac{a}{r}g$ 和 $H = \frac{b}{s}h = \frac{r}{a}h$ 是 $R[X]$ 中的多项式，且 $F = GH$。

定义。如果在 $R[X]$ 中，两个本原多项式的乘积仍是本原多项式，我们就称 R 为 P^4-整环（$P^4 = PPPP$：本原多项式的乘积仍是本原多项式）。

我们已经看到，首一多项式的高斯提升引理在 $R[X]$ 当且仅当 R（从而 $R[X]$）整闭时成立，或者等价地说，当戴德金布拉格定理成立时成立。同样，任意多项式的高斯提升引理恰好在施赖尔整环中成立。不难证明，P^4-整环介于里斯域和 AP 整环之间（见图2；事实上，只要线性多项式满足 P^4 性质，就已经可以推出 AP）。最后，引理29形式的高斯引理当且仅当 R 是最大公因子整环时成立。

现在，在任意整环中，可以考虑由 f的系数生成的理想 $\mathfrak{c}(f)$，并考察方程 $\mathfrak{c}(fg) = \mathfrak{c}(f)\mathfrak{c}(g)$ 成立的条件。答案由下面的定理给出

定理30。 对于整环 R，以下命题等价：

(1) 每个有限生成理想都是投射的。(2) 每个有限生成理想 $\neq(0)$ 都是可逆的。(3) 对于每个素理想 $P \neq(0)$，局部化 R_P 是赋值环。(4) 每个满足 $R \subseteq S \subseteq K$ 的环 S 都是整闭的，其中 K 是 R 的商域。(5) $\mathfrak{c}(fg) = \mathfrak{c}(f)\mathfrak{c}(g)$ 对于所有多项式 f、$g \in R[X]$ 均成立。

证明。 参见 [16, 第 IV 章]。 □

因此，当且仅当系数环是 Prüfer 整环时，这一版本的高斯引理成立。Prüfer 本人（参见 [33, 第 23] 页）将定理 $\mathfrak{c}(fg) = \mathfrak{c}(f)\mathfrak{c}(g)$ 称为“高斯–克罗内克–戴德金定理”。

Last but not least ...

撰写本文的动机，主要源于我阅读了 [29]（该文讨论施赖尔整环中的高斯提升引理）和 [32]（该文讨论欧几里得证明其第七卷命题19时存在的漏洞），以及希望以稍有不同的方式呈现其中所述内容。我还要感谢 Bill Dubuque 在 sci.math 上发布的各种帖子，这些帖子对我帮助很大，尤其是在初期。最后，我还要感谢 Heinz L¨ uneburg 和 Klaus Volkert 提出了许多有用的意见，也感谢两位匿名审稿人。

本文发表于《数学学期报告》第56卷（2009年），第39–51页。英文译文是在 Claude（Anthropic）的协助下完成的，Claude 也补全了定理19证明中的漏洞。

Literatur

[1] D.D. Anderson, M. Zafrullah, *The Schreier property and Gauss' Lemma*, 《意大利数学联合会公报》(8 **10** 2007 43 62 10, 23) **-B** ( ), – T. Apostol, [2] *Irrationality of the square root of two – a geometric proof*, 《美国数学月刊》 **107** 2000 841 842 1, 14 ( ), – D.M. Bloom, *A one-sentence proof that* $\sqrt{2}$ *is irrational* **68** 1995 286 2, 15 , [3] *Prime ideals and integral dependence* 《数学杂志》( ), I.S. Cohen, A. Seidenberg, , 《美国数学会通报》**52** (1946 252 261 6, 19), – H. Cohn, [4] *A second course in number theory*, 纽约, J. Wiley & Sons, 1962; 1980年由Dover出版社在纽约重印, 书名为 *Advanced Number Theory* 5, 18[5] P.M. Cohn, *Bezout rings and their subrings*, 《剑桥哲学学会会刊》**64** (1968), 251–264 10, 22[6] *A direct proof of the Dedekind-Mertens Lemma* 2007 5, 18 Th. Coquand, , 预印本 Th. Coquand, L. Ducos, H. Lombardi, C. Quitte, *L'idéal des coefficients du produit de deux polynômes*, 预印本, 2002 5, 18[7] R. Dedekind, *Über einen arithmetischen Satz von Gauß*, 《布拉格德国数学会通讯》(1892), 1–11; 《著作集》II, 28–38 5, 12, 18, 24[8] R. Dedekind, *Über die Begründung der Idealtheorie*, 《哥廷根新闻》(1895), 106–113; 《著作集》II, XXV., 50–58 5, 6, 17, 18[9] R. Dedekind, *Stetigkeit und irrationale Zahlen*, 布伦瑞克, 1872; 第2版, 1892; 第3版, 1905 4 1912 5 1927 2, 15 ; 第.版; 第.版 H. Edwards, , Birkhauser出版社, 波士顿, 1990 5, [10] *Divisor Theory* ¨ 18

[13] *Look Ma no primes* **49** 1976 249 2, 15 N.J. Fine, , , , 《数学杂志》( ), K.
[14] *The discovery of incommensurability by Hippasus of Metapontum*
von Fritz, , 《数学年刊》(2) 46 (1945), 242–264 1, 14[15]C.F. Gauß, *Disquisitiones Arithmeticae*, 莱比锡, 1801; 由
H. Maser翻译成德文, 施普林格出版社, 柏林, [16] *Multiplicative Ideal Theory*R. Gilmer, , Marcel Dekker出
版社, 纽约[17] *Proben mathematischer Forschung in allgemeinverständlicher Behandlung*H. Hasse, , Otto
Salle出版社, 法兰克福, 1955 1, 14[18] E. Heine,
Der Eisensteinsche Satz über die Reihen-Entwickelung algebraischer Functionen, 《纯粹与应用数学杂志》
45 1853 285 302 3, 15 ( ), – K. Hensel, 《纯粹与应用数学杂志》158 (1927), 195–
[19] *Über eindeutige Zerlegung in Primelemente*
198 10, 22[20] D. 希尔伯特, *Die Theorie der algebraischen Zahlkörper (Zahlbericht)*, 《德国数学家协会年报》4
(1897), 175–546; I. Adamson的英文译本《代数数域理论》, 施普林格出版社, 柏林, [21] A.
Über einen Fundamentalsatz der arithmetischen Theorie der algebraischen
赫尔维茨, *Größen* ¨ 1895 230 , 《哥廷根新闻》
240 5, 18
( ), –[22] D. Kalman, R. Mena, S. Shahriari,
Variations on an irrational theme – geometry, dynamics,
algebra **70** 1997 93 104 3, 15 , 《数学杂志》( ), –
[23] L. Kronecker,
Grundzüge einer arithmetischen Theorie der algebraischen Größen, 《纯粹与应用数学杂志》
92 1882 1 122 5, 18 ( ), – E. Landau,
[24]
Einführung in die elementare und analytische Theorie der algebraischen Zahlen
und der Ideale 1918 1949 5, 18 , 莱比锡和柏林（Teubner）;
[25] *Zur Zahlentheorie der Griechen; Teil I*
Chelsea重印版 F. Lemmermeyer, *Euklids Fundamentalsatz der*
Arithmetik **54** 2008 1 , 《数学学期刊》( ), –
15 1, 14
[26] *Jacobi and Kummer's ideal numbers*F. Lemmermeyer, 准备中
3, 15
[27] F. Lemmermeyer, N. Schappacher,
Introduction to the English edition of Hilbert's Zahlbericht, 载于 *The theory of algebraic number fields*; [20] 的英文译本由
I. Adamson翻译, 施普林格出版社, 1998 7, 19[28] F. Lorenz, F. Lemmermeyer, *Algebra I. Körper und Galoistheorie*,
2007 2, 10, 15, 22
第4版, Elsevier, 海德堡, [29] A. Magidin, D. McKinnon, *Gauss's Lemma for number fields*,
《美国数学月刊》112 (2005 385 416 10, 13, 22, 25), – S. McAdam, D.E. Rush,
[30]
Schreier rings **10** 1978 77 80 10, 22 , 《伦敦数学会会刊》( ), –
[31] *Über einen algebraischen Satz* **101** 1892 1560
F. 默滕斯, , 维也纳科学院会议录 ( ), 1566 5, 18[32] D. Pengelley, F. Richman,
Did Euclid need the Euclidean algorithm to prove unique factor-
ization? **113** 2006 196 , 《美国数学月刊》( ), –
205 13, 25
[33] ¨ *Untersuchungen über Teilbarkeitseigenschaften in Körpern*H. Prufer, 《纯粹与应用数学杂志》
168 1932 1 36 12, 25 ( ), – Y. Sagher,
[34]
What Pythagoras could have done **95** 1988 117 2, 15 , 《美国数学月刊》( ),
[35] *Wer ist Alexander Grothendieck? Anarchie Mathematik Spiritualität*
W. Scharlau, , 哈维克斯贝克, 2007 7, 20[36] W. Strobl,
Historische und systematische Entwicklung der arithmetischen Theorie der algeb-
raischen Funktionen von Dedekind und Weber (西班牙语), 马德里大学学士
学位论文, 1980 5, 18[37]J. Sur´anyi, *Schon die alten Griechen haben das gewusst*, 载于 *Große Augenblicke aus der Geschichte der Mathematik*, BI Mannheim, 1991 2, 15
[38] *On the irrationality of roots* **67** 1960 576 578 2, 15 H.E. Vaughan, 《美国
[39] *Moderne Algebra*
数学月刊》( ), – B.L. van der Waerden, , 施普林格出版社, 柏林, 1930 10, 22
[40] *Why square roots are irrational* **93** W.C. Waterhouse, 《美国数学月刊》
(1986), 213–214 2, 15