目录

《代数数论》习题解答

高旭-GG 译

2015 年 6 月 22 日

1　结构说明

问题，解答形式。一个大问题的内部，若需证明一些中间结论，就引理，命题等做相对标号，在大问题内部形成一个完整的逻辑链。各个大问题解答独立。有名的引理，定理，注明定理名称，全局生效。

1.1　当前问题和进度条

0. 问题 2 引理 1 的验证
1. 5.4 和 5.7 连贯
2. 进度条第三章

2　第一章：高斯整数

2.1　练习题

1 **问题：** 证明 $\alpha \in \mathbb{Z}[i]$ 是单位当且仅当 $N(\alpha) = 1$。
解答： 设 $\alpha = x + iy$，其中 $x, y \in \mathbb{Z}$，则 $N(\alpha) = x^2 + y^2 \in \mathbb{Z}$。若 α 是单位，则存在 α^{-1}，使得 $N(\alpha)N(\alpha^{-1}) = N(1) = 1$，因此 $N(\alpha) = 1$。反之，若 $N(\alpha) = 1$，则其共轭 $\overline{\alpha} = x - iy$ 是其逆，因为 $\alpha\overline{\alpha} = (x + iy)(x - iy) = x^2 + y^2 = 1$。故 $\alpha \in \mathbb{Z}[i]$ 是单位当且仅当 $N(\alpha) = 1$。

2 **问题：** 在环 $\mathbb{Z}[i]$ 中，证明若 $\alpha\beta = \varepsilon\gamma^n$，其中 α, β 互素，ε 是单位，则存在单位 $\varepsilon', \varepsilon''$ 使得 $\alpha = \varepsilon'\xi^n$ 且 $\beta = \varepsilon''\eta^n$。
解答： 我们证明一个更一般的结果：不妨临时将其设为 **命题 A：在唯一分解整环 (UFD) 中，若 $\alpha\beta = \varepsilon\gamma^n$，$\alpha, \beta$ 互素，ε 是单位，则 $\alpha = \varepsilon'\xi^n$ 且 $\beta = \varepsilon''\eta^n$，其中 $\varepsilon', \varepsilon''$ 是单位。**

证明: 根据唯一分解性质, 设 $\alpha = \varepsilon_1\pi_1^{l_1}\pi_2^{l_2}\cdots\pi_s^{l_s}$, $\beta = \varepsilon_2\pi_1^{m_1}\pi_2^{m_2}\cdots\pi_s^{m_s}$, $\gamma = \varepsilon_3\pi_1^{n_1}\pi_2^{n_2}\cdots\pi_s^{n_s}$。由于 $(\alpha, \beta) = 1$，有 $l_jm_j = 0$（$j = 1, 2, \ldots, s$）。由 $\alpha\beta = \varepsilon\gamma^n$，得 $l_j + m_j = nn_j$。因此，对于每个 j，要么 $l_j = nn_j$，要么 $m_j = nn_j$。由此得出结论。

3 **问题：**证明方程 $x^2+y^2 = z^2$(其中 $x, y, z > 0$ 且 $(x, y, z) = 1$)的整数解(即“毕达哥拉斯三元组”)都可以通过公式 $x = u^2 - v^2, y = 2uv, z = u^2 + v^2$ 给出，其中 $u, v \in \mathbb{Z}, u > v > 0, (u, v) = 1$，且 u, v 不全为奇数（允许 x 和 y 互换)。
解答： 设 $\alpha = x + iy$，则 (x, y, z) 是毕达哥拉斯三元组意味着 $N(\alpha) = z^2$。可假设 $(\alpha, \overline{\alpha}) = 1$。由于唯一分解整环中存在如下命题:

在环 $\mathbb{Z}[i]$ 中，若 $\alpha\beta = \varepsilon\gamma^n$，其中 α, β 互素，ε 是单位，则存在单位 $\varepsilon', \varepsilon''$ 使得 $\alpha = \varepsilon'\xi^n$ 且 $\beta = \varepsilon''\eta^n$。

证明：根据唯一分解性质，设 $\alpha = \varepsilon_1\pi_1^{l_1}\pi_2^{l_2}\cdots\pi_s^{l_s}$，$\beta = \varepsilon_2\pi_1^{m_1}\pi_2^{m_2}\cdots\pi_s^{m_s}$，$\gamma = \varepsilon_3\pi_1^{n_1}\pi_2^{n_2}\cdots\pi_s^{n_s}$。由于 $(\alpha, \beta) = 1$，有 $l_j m_j = 0$（$j = 1, 2, \ldots, s$）。由 $\alpha\beta = \varepsilon\gamma^n$，得 $l_j + m_j = nn_j$。因此，对于每个 j，要么 $l_j = nn_j$，要么 $m_j = nn_j$。由此得出结论。

应用到此，设 $\alpha = x + iy$，$\beta = \overline{\alpha} = x - iy$，$\varepsilon = 1$，$\gamma = z$，$n = 2$，则 $\alpha\beta = z^2$。由于 $(\alpha, \overline{\alpha}) = 1$，由上述结论，得 $\alpha = \varepsilon\xi^2$，其中 ε 是单位。设 $\xi = u + iv$，则：

$$\xi^2 = (u + iv)^2 = u^2 - v^2 + 2uvi,$$

$$\alpha = \varepsilon\xi^2 = \varepsilon(u^2 - v^2 + 2uvi).$$

取 $\varepsilon = 1$，则：

$$x + iy = u^2 - v^2 + 2uvi \implies x = u^2 - v^2, \quad y = 2uv,$$

$$z^2 = x^2 + y^2 = (u^2 - v^2)^2 + (2uv)^2 = (u^2 + v^2)^2 \implies z = u^2 + v^2.$$

故结论成立。

4 **问题：** 证明环 $\mathbb{Z}[i]$ 不能被排序。
解答： 首先回顾有序环的定义：

定义： 一个有序环是带有全序 $\leqslant$ 的环 R，满足：若 $a \leqslant b$，则 $a + c \leqslant b + c$；若 $0 \leqslant a$ 且 $0 \leqslant b$，则 $0 \leqslant ab$。若 $a \neq 0$，$0 \leqslant a$ 则 a 为正，$a \leqslant 0$ 则 a 为负，0 既不正也不负。

命题： 在有序环中，对于每个元素 a，恰好满足以下之一：a 为正，$-a$ 为正，或 $a = 0$。特别地，a 为负当且仅当 $-a$ 为正。假设 $\mathbb{Z}[i]$ 可被全序 $\leqslant$ 排序。考虑 i：若 i 为正，则 $-1 = i^2$ 为正，从而 $1 = (-1)^2$ 也为正，与命题矛盾。故 $\mathbb{Z}[i]$ 不能被排序。

5 **问题：** 证明对于每个有理整数 $d > 1$，环 $\mathbb{Z}[\sqrt{-d}]$ 的单位仅为 ± 1。
解答： 元素 $\alpha = x + y\sqrt{-d}$ 的范数为 $N(\alpha) = x^2 + dy^2$。由于环 $\mathbb{Z}[i]$ 中，α 是单位当且仅当 $N(\alpha) = 1$。因此，α 是单位等价于 (x, y) 是方程 $x^2 + dy^2 = 1$ 的整数解。因 $d > 1$，该方程的唯一整数解为 $(\pm 1, 0)$。故单位仅为 ± 1。

6 **问题：** 证明对于每个无平方因子的整数 $d > 1$，环 $\mathbb{Z}[\sqrt{d}]$ 有无穷多个单位。
解答： 单位是指 $\mathbb{Z}[\sqrt{d}]$ 中范数为 ± 1 的元素。设 $\alpha = x + y\sqrt{d}$，其范数为 $N(\alpha) = (x + y\sqrt{d})(x - y\sqrt{d}) = x^2 - dy^2$。$\alpha$ 是单位当且仅当 $x^2 - dy^2 = \pm 1$。因此，问题等价于证明佩尔方程 $x^2 - dy^2 = \pm 1$ 有无穷多整数解。由于 $d > 1$ 且无平方因子，$\sqrt{d}$ 是无理数，我们通过证明 $x^2 - dy^2 = 1$ 有无穷多解来完成（因为存在一个非平凡解即可生成无穷多解）。

命题： 对于每个无平方因子的整数 $d > 1$，方程 $x^2 - dy^2 = 1$ 有无穷多整数解。此处使用狄利克雷逼近定理证明：

引理（狄利克雷逼近定理）： 对于无理数 θ，存在无穷多对整数 (x, y)（其中 $y > 0$）使得：

$$\left|\theta - \frac{x}{y}\right| < \frac{1}{y^2}.$$

证明：通过 Dirichlet 抽屉原理，对于每个正整数 N，存在整数 x 和 y 使得 $1 \leq y \leq N$ 且：

$$|x - y\theta| \leq \frac{1}{N + 1}.$$

具体而言，令 $\theta_y = y\theta - [y\theta]$ 对于 $1 \le y \le N$。若存在某个 y 使得 $\theta_y \in (0, \frac{1}{N+1})$ 或 $\theta_y \in [\frac{N}{N+1}, 1)$，则 $|[y\theta] - y\theta| < \frac{1}{N+1}$ 或 $|([y\theta]+1) - y\theta| < \frac{1}{N+1}$。否则，$N$ 个数 θ_y 分布在 $N-1$ 个区间 $[\frac{1}{N+1}, \frac{2}{N+1}), \ldots, [\frac{N-1}{N+1}, \frac{N}{N+1})$，故存在 $1 \le y_1 < y_2 \le N$ 和 $0 < k < N$ 使得 $\theta_{y_1}, \theta_{y_2} \in [\frac{k}{N+1}, \frac{k+1}{N+1})$。于是：

$$|([y_2\theta] - [y_1\theta]) - (y_2 - y_1)\theta| < \frac{1}{N+1}.$$

因此可以直接得出结论：给定一对 (x, y) 满足 $|x - y\theta| \le \frac{1}{N+1}$，可选择更大的 N' 使得 $|x - y\theta| > \frac{1}{N'+1}$，从而得到另一对 (x', y')，重复此过程可得无穷多对满足 $\left|\theta - \frac{x}{y}\right| < \frac{1}{y^2}$ 的整数对。

推论 1：对于每个无平方因子的整数 $d > 1$，存在无穷多对整数 (x, y)（其中 $y > 0$）使得：

$$\left|x^2 - dy^2\right| < 1 + 2\sqrt{d}.$$

证明：由引理（狄利克雷逼近定理），存在无穷多对 (x, y)（$y > 0$）满足 $|x - y\sqrt{d}| < \frac{1}{y}$。对于这些对，有：

$$\begin{aligned} |x + y\sqrt{d}| &= |x - y\sqrt{d} + 2y\sqrt{d}| \\ &\le |x - y\sqrt{d}| + 2y\sqrt{d} \\ &< \frac{1}{y} + 2y\sqrt{d}, \end{aligned}$$

因此：

$$\begin{aligned} \left|x^2 - dy^2\right| &= |x - y\sqrt{d}||x + y\sqrt{d}| \\ &< \frac{1}{y}\left(\frac{1}{y} + 2y\sqrt{d}\right) \\ &= \frac{1}{y^2} + 2\sqrt{d}. \end{aligned}$$

由于 $\frac{1}{y^2} \le 1$（因为 $y \ge 1$），则：

$$\left|x^2 - dy^2\right| \le 1 + 2\sqrt{d}.$$

推论 2：对于每个无平方因子的整数 $d > 1$，存在某个整数 k 满足 $1 \le |k| < 1 + 2\sqrt{d}$，且方程 $x^2 - dy^2 = k$ 有无穷多整数解。证明：显然，$x^2 - dy^2 = 0$ 的唯一整数解为 $(0, 0)$。由推论 1，存在无穷多对 (x, y)（$y > 0$）满足 $|x^2 - dy^2| < 1 + 2\sqrt{d}$。设 $m = x^2 - dy^2$，则 m 是整数，且 $|m| < 1 + 2\sqrt{d}$。可能的 m 值是有限的：$0, \pm1, \pm2, \ldots, \pm[1 + 2\sqrt{d}]$。由于 (x, y) 有无穷多对，由抽屉原理，存在某个 $k \ne 0$（因为 $(0, 0)$ 仅对应 $m = 0$）被无穷多次取到，即 $x^2 - dy^2 = k$ 有无穷多解，且 $1 \le |k| < 1 + 2\sqrt{d}$。

证明（命题）：由推论 2，存在某个 k（$1 \le |k| < 1 + 2\sqrt{d}$）使得 $x^2 - dy^2 = k$ 有无穷多整数解。取其中两个正整数解 (x_1, y_1) 和 (x_2, y_2) 满足 $x_1 \equiv x_2 \mod |k|$ 和 $y_1 \equiv y_2 \mod |k|$。则：

$$(x_1x_2 - dy_1y_2)^2 - d(x_1y_2 - x_2y_1)^2 = (x_1^2 - dy_1^2)(x_2^2 - dy_2^2) = k^2.$$

由于 $x_1 \equiv x_2 \mod |k|$ 且 $y_1 \equiv y_2 \mod |k|$，则 $x_1y_2 - x_2y_1 \equiv 0 \mod |k|$，故 k 整除 $x_1y_2 - x_2y_1$。由上式，k 也整除 $(x_1x_2 - dy_1y_2)k$，从而整除 $x_1x_2 - dy_1y_2$。因此：

$$\left(\frac{x_1x_2 - dy_1y_2}{k}, \frac{x_1y_2 - x_2y_1}{k}\right)$$

是方程 $x^2 - dy^2 = 1$ 的整数解。

令 (x_0,y_0) 表示 $x^2-dy^2=1$ 的最小正整数解，即 $x_0+y_0\sqrt{d}>1$ 最小（注意到平凡解 $(1,0)$ 对应 $1+0\cdot\sqrt{d}=1$，我们取非平凡解）。我们声称，方程 $x^2-dy^2=1$ 的整数解为：

$$\left\{(x,y)\mid |x+y\sqrt{d}|=|x_0+y_0\sqrt{d}|^n,\text{对于某个}n\in\mathbb{Z}\right\}.$$

设 (x,y) 是任意正整数解(由对称性,负解可类似处理)。若存在某个 $n\geq 0$ 使得 $(x_0+y_0\sqrt{d})^n<x+y\sqrt{d}<(x_0+y_0\sqrt{d})^{n+1}$，则：

$$1<(x+y\sqrt{d})(x_0-y_0\sqrt{d})^n<(x_0+y_0\sqrt{d}).$$

令 $x'+y'\sqrt{d}=(x+y\sqrt{d})(x_0-y_0\sqrt{d})^n$。由于 $(x_0-y_0\sqrt{d})^n=(x_0+y_0\sqrt{d})^{-n}$，且 $x^2-dy^2=1$，则：

$$(x'+y'\sqrt{d})(x'-y'\sqrt{d})=(x+y\sqrt{d})(x-y\sqrt{d})(x_0-y_0\sqrt{d})^n(x_0+y_0\sqrt{d})^{-n}=1,$$

故 $x'+y'\sqrt{d}$ 也满足 $x'^2-dy'^2=1$。此外：

$$1<x'+y'\sqrt{d}<(x_0+y_0\sqrt{d}),\quad x'-y'\sqrt{d}=(x'+y'\sqrt{d})^{-1},$$

则 $0<x'-y'\sqrt{d}<1$。于是：

$$x'=\frac{1}{2}\Big((x'+y'\sqrt{d})+(x'-y'\sqrt{d})\Big)>0,$$
$$y'=\frac{1}{2}\Big((x'+y'\sqrt{d})-(x'-y'\sqrt{d})\Big)>0,$$

因此 (x',y') 是一个正整数解，且 $x'+y'\sqrt{d}<x_0+y_0\sqrt{d}$，这与 (x_0,y_0) 的最小性矛盾。故 $x+y\sqrt{d}=(x_0+y_0\sqrt{d})^n$。

结论： 由命题，$x^2-dy^2=1$ 有非平凡解 (x_0,y_0)。令 $u_0=x_0+y_0\sqrt{d}$，则 $u_0^n=x_n+y_n\sqrt{d}$，且 $x_n^2-dy_n^2=1$。由于 $u_0>1$，$n\in\mathbb{Z}$ 产生无穷多不同解，从而 $\mathbb{Z}[\sqrt{d}]$ 的单位群由 $\pm u_0^n$ 生成，包含无穷多个单位。

7 **问题：** 证明对于每个无平方因子的整数 $d>1$，环 $\mathbb{Z}[\sqrt{2}]$ 是欧几里得环。此外，证明其单位由 $\pm(1+\sqrt{2})^n,n\in\mathbb{Z}$ 给出，并确定其素元。

解答： 该问题包含三部分：证明 $\mathbb{Z}[\sqrt{2}]$ 是欧几里得环，确定其单位群，并分类其素元。以下逐一解答。

回忆： 一个环 A 是欧几里得环，如果存在函数 $\delta:A\to\mathbb{N}$，满足：(1) $\delta(\alpha)=0\iff\alpha=0$；(2) 对任意 $\alpha,\beta\in A,\beta\neq 0$，存在 $\kappa,\gamma\in A$ 使 $\alpha=\kappa\beta+\gamma$ 且 $\delta(\gamma)<\delta(\beta)$。

证明： 为证明 $\mathbb{Z}[\sqrt{2}]$ 是欧几里得环，定义范数 $|N(a+b\sqrt{2})|=|a^2-2b^2|$ 为欧几里得函数。考虑 $\alpha=a+b\sqrt{2}\in\mathbb{Q}(\sqrt{2})$，选择 $\gamma=x+y\sqrt{2}\in\mathbb{Z}[\sqrt{2}]$，使 $|a-x|\leq\frac{1}{2}$，$|b-y|\leq\frac{1}{2}$。则：

$$|N(\alpha-\gamma)|=|(a-x)^2-2(b-y)^2|\leq|a-x|^2+2|b-y|^2\leq\frac{1}{4}+2\cdot\frac{1}{4}=\frac{3}{4}<1.$$

故 $|N|$ 满足欧几里得条件，$\mathbb{Z}[\sqrt{2}]$ 是欧几里得环。

验证 $\pm(1+\sqrt{2})^n$ 是单位：对于 $u=1+\sqrt{2}$，$N(u)=1-2=-1$。其逆为 $-1+\sqrt{2}$，因：

$$(1+\sqrt{2})(-1+\sqrt{2})=-1+2=1.$$

对 $n\in\mathbb{Z}$，$N((1+\sqrt{2})^n)=(-1)^n=\pm1$，故 $\pm(1+\sqrt{2})^n$ 均为单位。为证明其唯一性，设 $u=a+b\sqrt{2}$ 为单位，则 $N(u)=a^2-2b^2=\pm1$。取 $u_0=1+\sqrt{2}$ 为最小正单位（范数为 -1，系数正），所有单位形如 $\pm u_0^n$。

回忆：一个元素 p 称为素元，如果主理想 (p) 是一个非零素理想。在唯一因子分解域中，素元恰好是不可约元素。为了继续确定所有素元，我们需要一个引理。

引理 1：对于素数 $p>2$，二元一次方程：

$$a^2-2b^2=p,$$

有整数解当且仅当 $p\equiv 1$ 或 $7 \mod 8$。

证明：对于任意整数 a,b，a^2-2b^2 不能模 8 为 3 或 5。模 8 检查：$a^2\equiv 0,1,4; 2b^2\equiv 0,2$。则 $a^2-2b^2\equiv 0,1,2,4,6,7$。故不可能为 3 或 5。为了证明"当且"部分，我们只需证明这样的 p 在 $\mathbb{Z}[\sqrt{2}]$ 中不是素元。设 $p=\alpha\beta$，则 $N(\alpha)N(\beta)=N(p)=p^2$，因此 $N(\alpha)=\pm p$ 或 $\pm p^2$，其中 $\alpha=a+b\sqrt{2}$，于是 $p=N(\alpha)=a^2-2b^2$。

为此，我们验证当 $p\equiv 1$ 或 $7 \mod 8$ 时，同余式 $x^2\equiv 2 \mod p$ 有解。若如此，则 $p\mid x^2-2=(x+\sqrt{2})(x-\sqrt{2})$。但 $\frac{x+\sqrt{2}}{p}$ 和 $\frac{x-\sqrt{2}}{p}$ 都不在 $\mathbb{Z}[\sqrt{2}]$ 中，因此 p 不能是素元。

为了证明 2 是模 p 的二次剩余，即同余式 $x^2\equiv 2 \mod p$ 有解，当 $p\equiv 1$ 或 $7 \mod 8$ 时，我们引用 Legendre 符号和 Gauss 引理。

Legendre 符号：一个整数 a 称为模 n 的二次剩余，如果合同式 $x^2\equiv a \mod n$ 有解。我们定义模 n 的 Legendre 符号如下：

$$\left(\frac{a}{n}\right):=\begin{cases}1 & \text{若}a\text{ 是模}n\text{ 的二次剩余且}a\not\equiv 0 \mod p,\\ 0 & \text{若}a\equiv 0 \mod p,\\ -1 & \text{若}a\text{ 是模}n\text{ 的二次非剩余}.\end{cases}$$

引理 2：设 p 是一个奇素数，a 是一个整数，则：

$$\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}} \mod p.$$

证明：我们将正余数集 $1,2,\cdots,p-1$ 中的整数配对如下：如果 $xy\equiv a \mod p$，则将 x 与 y 配对。

若 a 是二次剩余，则存在某个 x_0 在正余数集中，使得 $x_0^2\equiv a \mod p$。在这种情况下，同余式 $x^2\equiv a \mod p$ 在正余数集中恰有两解：x_0 和 $p-x_0$。因此配对提供 $\frac{p-3}{2}$ 对和两个单元素，它们的乘积为：

$$(p-1)!\equiv a^{\frac{p-3}{2}}x_0(p-x_0)\equiv -a^{\frac{p-1}{2}} \mod p.$$

由于 $(p-1)!\equiv -1 \mod p$（Wilson 定理），得 $a^{\frac{p-1}{2}}\equiv 1 \mod p$。若 a 是二次非剩余，则配对提供 $\frac{p-1}{2}$ 对，它们的乘积为：

$$(p-1)!\equiv a^{\frac{p-1}{2}} \mod p.$$

于是 $a^{\frac{p-1}{2}}\equiv -1 \mod p$。结论为 $\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}} \mod p$。

引理 (Gauss 引理) 设 p 是一个奇素数，a 与 p 互质，则：

$$\left(\frac{a}{p}\right)\equiv (-1)^{\mu} \mod p,$$

其中 μ 是 $a,2a,\cdots,\frac{p-1}{2}a$ 模 p 的绝对余数中负整数的个数。

证明： 设 $r_1, r_2, \cdots, r_\tau$ 是 $a, 2a, \cdots, \frac{p-1}{2}a$ 模 p 的正绝对余数，而 $s_1, s_2, \cdots, s_\mu$ 是负的。则 $\tau+\mu=\frac{p-1}{2}$。注意 $r_1, r_2, \cdots, r_\tau, -s_1, -s_2, \cdots, -s_\mu$ 是互异的，因此它们是 $1, 2, \cdots, \frac{p-1}{2}$ 的一种排列。因此有：

$$r_1 r_2 \cdots r_\tau (-s_1)(-s_2)\cdots(-s_\mu) \equiv \left(\frac{p-1}{2}\right)! \mod p.$$

但：

$$r_1 r_2 \cdots r_\tau s_1 s_2 \cdots s_\mu \equiv \left(\frac{p-1}{2}\right)! a^{\frac{p-1}{2}} \mod p.$$

于是 $a^{\frac{p-1}{2}} \equiv (-1)^\mu \mod p$. 结果由引理 2 得出。

备注： 使用这个 Gauss 引理，可以确定 $\left(\frac{a}{p}\right)$。确实，$2, 4, \cdots, p-1$ 模 p 的绝对余数是 $2, 4, \cdots, 2\left[\frac{p-1}{4}\right]$ 和 $2\left[\frac{p-1}{4}\right]-p, \cdots, -1$。于是 $\mu=\frac{p-1}{2}-\left[\frac{p-1}{4}\right]$，我们得出 $\left(\frac{2}{p}\right)=(-1)^{\frac{p-1}{2}-\left[\frac{p-1}{4}\right]}=(-1)^{\frac{p^2-1}{8}}$。

命题 1： $\mathbb{Z}[\sqrt{2}]$ 的素元 π，在等价类元素 (associated elements) 下，可由如下给出：

(a) $\pi=\sqrt{2}$,

(b) $\pi=a+b\sqrt{2}$ 其中 $a^2-2b^2=p, p\equiv 1,7 \mod 8, a>b\sqrt{2}>0$,

(c) $\pi=p, p\equiv 3,5 \mod 8$.

证明： 设 π 是一个素元。我们将 $N(\pi)$ 分解为素数，则 π 必须除以其中之一，设为 p。则 $N(\pi)\mid N(p)=p^2$，因此 $N(\pi)=\pm p$ 或 $\pm p^2$。为了确定 π，需确定 $a^2-2b^2=p$：若无正整数解，则 $\pi=p$ 是素元，这是情况 3；若有正整数解 (a,b) 则 $\pi=a+b\sqrt{2}$ 是素元，这是情况 1 和 2。结果由**引理 1** 得出。

总结： 如上证明了 $\mathbb{Z}[\sqrt{2}]$ 是欧几里得环，单位为 $\pm(1+\sqrt{2})^n$，素元如**命题 1**。

3 第二章：整性

3.1 练习题

1 **问题：** 判断 $\frac{3+2\sqrt{6}}{1-\sqrt{6}}$ 是否为代数整数。
解答： 设 $\theta=\frac{3+2\sqrt{6}}{1-\sqrt{6}}$。计算得（分母有理化）：

$$\theta=\frac{3+2\sqrt{6}}{1-\sqrt{6}}\cdot\frac{1+\sqrt{6}}{1+\sqrt{6}}=\frac{(3+2\sqrt{6})(1+\sqrt{6})}{1-6}=\frac{3+3\sqrt{6}+2\sqrt{6}+12}{-5}=-\frac{15+5\sqrt{6}}{5}=-(3+\sqrt{6})$$

验证 θ 是否满足整系数单项式方程。计算：

$$\theta^2+6\theta+3=(3+\sqrt{6})^2-6(3+\sqrt{6})+3=9+6\sqrt{6}+6-18-6\sqrt{6}+3=0$$

因此，θ 满足整系数方程 $x^2+6x+3=0$，故 θ 是代数整数。

2 **问题：** 证明若整环 A 是整闭（integrally closed）的，则其多项式环 $A[t]$ 也是整闭的。此外，证明每个唯一因子分解整环（UFD）和每个 Dedekind 域是整闭的，并进一步说明 $A[t]$ 的整闭包与 A 的整闭包之间的关系。

解答： 该问题包含多个部分：证明 $A[t]$ 整闭，验证 UFD 和 Dedekind 域的整闭性，及 $A[t]$ 整闭包的性质。以下逐一解答。

回忆：一个整环 A 是整闭的，若其分式域 K 中对 A 整的元素均在 A 中。即，若 $x \in K$ 满足 $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$（$a_i \in A$），则 $x \in A$。

证明：设 K 为 A 的分式域，需证明 $A[t]$ 在其分式域 $K(t)$ 中整闭，即若 $f(t) \in K(t)$ 对 $A[t]$ 整，则 $f(t) \in A[t]$。已知 $K[t]$ 是主理想域（PID），由后述**命题 1 或 2**，$K[t]$ 整闭，且 $K(t)$ 是 $A[t]$ 和 $K[t]$ 的共同分式域。

设 $f(t) \in K(t)$ 对 $A[t]$ 整，则对 $K[t]$ 也整，故 $f(t) \in K[t]$。存在 $a_{n-1}(t), \ldots, a_0(t) \in A[t]$，使得：

$$f(t)^n + a_{n-1}(t)f(t)^{n-1} + \cdots + a_0(t) = 0.$$

取整数 m 大于 $a_{n-1}(t), \ldots, a_0(t)$ 和 $f(t)$ 的次数。令 $h(t) = t^m - f(t)$，则 $h(t)$ 对 $A[t]$ 整，且为首一多项式。代入得：

$$h(t)^n + a_{n-1}(t)h(t)^{n-1} + \cdots + a_0(t) = 0.$$

设 $g(t) = h(t)^{n-1} + a_{n-1}(t)h(t)^{n-2} + \cdots + a_1(t)$，则：

$$h(t)g(t) = -a_0(t).$$

因 $h(t)$ 和 $-a_0(t)$ 均为首一，且 $-a_0(t) \in A[t]$，由**引理 2**，$h(t)$ 的系数对 A 整。因 A 整闭，$h(t) \in A[t]$。故 $f(t) = t^m - h(t) \in A[t]$。$A[t]$ 整闭得证。

命题 1：每个唯一因子分解整环（UFD）是整闭的。

证明：设 A 为 UFD，K 为其分式域。任取 $a/b \in K$（$a, b \in A$，$b \neq 0$）对 A 整，存在 $a_{n-1}, \ldots, a_0 \in A$，使得：

$$(a/b)^n + a_{n-1}(a/b)^{n-1} + \cdots + a_0 = 0.$$

乘以 b^n：

$$a^n = -(a_{n-1}a^{n-1}b + \cdots + a_0 b^n).$$

右边被 b 整除，故 $b \mid a^n$。设 $b = p_1^{e_1} \cdots p_k^{e_k}$，若某质元 $p_i \mid b$，则 $p_i^{e_i n} \mid a^n$。若 $p_i \mid a$，则 a/b 非分式，矛盾。故 $p_i \nmid a$。由唯一因子分解，b 为单位，$a/b \in A$。A 整闭得证。

命题 2：每个 Dedekind 域是整闭的。

证明：设 $\mathcal{O}$ 为 Dedekind 域，K 为其分式域。任取 $r \in K$ 对 $\mathcal{O}$ 整，存在 n 使得 $r^n \in (r^{n-1}, r^{n-2}, \ldots, 1)$。记理想 $I = (r, 1)$，则：

$$I^n = (r^n, r^{n-1}, \ldots, 1) = (r^{n-1}, r^{n-2}, \ldots, 1) = I^{n-1}.$$

因 $\mathcal{O}$ 为 Dedekind 域，I 可逆，乘以 I^{-1} 得 $I = \mathcal{O}$。故 $r \in \mathcal{O}$。$\mathcal{O}$ 整闭得证。

引理 1（Gauss 引理）：设 A 为 UFD，K 为其分式域。若 $f, g \in K[t]$ 为首一多项式，$g \mid f$，且 $f \in A[t]$，则 $g \in A[t]$。

证明： **TODO 待确认**设 $f = gh$，$h \in K[t]$ 首一。存在 $a, b \in A$ 使 $ag, bh \in A[t]$，且 ag 和 bh 的系数无公共质因子）。则 $abf = (ag)(bh)$。因 $f \in A[t]$，由 Gauss 引理标准形式，$ag \in A[t]$ 的系数无非单位公共因子，因 g 首一，a 为单位，$g \in A[t]$。得证。

引理 2：设 A 为环，B 为 A-代数，$f, g \in B[t]$ 为首一多项式，$g \mid f$。若 f 的系数对 A 整，则 g 的系数也对 A 整。

证明： 设 $A' \subset B$ 为 f 系数生成的 A-子代数，则 A' 对 A 整。f 在分裂域中的根对 A' 整，因整性传递，对 A 整。g 的根为 f 的根子集，故对 A 整，其系数也对 A 整。得证。

命题 3： 设 A 为整域，A' 为其在 K 中的整闭包，则 $A[t]$ 在 $K(t)$ 中的整闭包为 $A'[t]$。

证明： (1) $A'[t]$ 对 $A[t]$ 整：任取 $f(t) = \sum a_i t^i \in A'[t]$，$a_i \in A'$ 对 A 整，满足 $a_i^n + b_{n-1}a_i^{n-1} + \cdots + b_0 = 0$（$b_j \in A$）。则：

$$f(t)^n + b_{n-1}f(t)^{n-1} + \cdots + b_0 = 0,$$

系数在 $A[t]$ 中，$f(t)$ 对 $A[t]$ 整。

(2) 若 $f(t) \in K(t)$ 对 $A[t]$ 整，则 $f(t) \in A'[t]$：由前述，$f(t) \in A[t]$。设 $f(t) = \sum c_i t^i$，$c_i \in K$ 对 A 整，因 A' 为整闭包，$c_i \in A'$。故 $f(t) \in A'[t]$。得证。

总结： 如上证明了若 A 整闭，则 $A[t]$ 整闭；UFD 和 Dedekind 域均整闭（**命题 1 和 2**）；$A[t]$ 的整闭包为 $A'[t]$（**命题 3**）。**引理 1 和 2** 提供了关键工具。

4 **问题：** 设 D 为不等于 0 或 1 的无平方因子有理整数，$K = \mathbb{Q}(\sqrt{D})$ 为二次数域，d 为其判别式。证明：

$$\begin{cases} d = D, & \text{若} D \equiv 1 \pmod 4, \\ d = 4D, & \text{若} D \equiv 2 \text{ 或} 3 \pmod 4, \end{cases}$$

且 K 的整基在第二种情况下为 $\{1, \sqrt{D}\}$，第一种情况下为 $\left\{1, \frac{1}{2}(1+\sqrt{D})\right\}$，且在两种情况下均为 $\left\{1, \frac{1}{2}(d+\sqrt{d})\right\}$。

解答： 设 $a + b\sqrt{D} \in \mathbb{Q}(\sqrt{D})$ 为代数整数，其最小多项式为 $x^2 - 2ax + (a^2 - Db^2)$。故 $2a \in \mathbb{Z}$，$a^2 - Db^2 \in \mathbb{Z}$。若 $a \in \mathbb{Z}$，则 $Db^2 \in \mathbb{Z}$，因 D 无平方因子，$b \in \mathbb{Z}$。若 $a \notin \mathbb{Z}$，则 $2a$ 为奇数，$D(2b)^2 \equiv 1 \pmod 4$，因 D 无平方因子，$2b \in \mathbb{Z}$，且 $D \equiv 1 \pmod 4$。因此，$\mathcal{O}_K = \mathbb{Z} + \frac{1}{2}(1+\sqrt{D})\mathbb{Z}$（若 $D \equiv 1 \pmod 4$），$\mathcal{O}_K = \mathbb{Z} + \sqrt{D}\mathbb{Z}$（若 $D \equiv 2$ 或$3 \pmod 4$）。

计算判别式 d。所有嵌入 $K \to \mathbb{C}$ 为恒等映射及 $\sigma : a + b\sqrt{D} \mapsto a - b\sqrt{D}$。若 $D \equiv 1 \pmod 4$，则：

$$d = d\left(1, \frac{1}{2}(1+\sqrt{D})\right) = \det \begin{pmatrix} 1 & \frac{1}{2}(1+\sqrt{D}) \\ 1 & \frac{1}{2}(1-\sqrt{D}) \end{pmatrix}^2 = D$$

若 $D \equiv 2$ 或$3 \pmod 4$，则：

$$d = d(1, \sqrt{D}) = \det \begin{pmatrix} 1 & \sqrt{D} \\ 1 & -\sqrt{D} \end{pmatrix}^2 = 4D$$

两情况下，$\mathcal{O}_K = \mathbb{Z} + \frac{1}{2}(d+\sqrt{d})\mathbb{Z}$。

4.1 **问题：** 设 $A \subset B$ 是环的扩展，且 B 作为 A-模是秩为 m 的自由模。给定 B 中的元素 $\beta_1, \cdots, \beta_m$，定义此基的判别式，并说明当基变换时判别式的变化规律。进一步说明判别式 $d(B/A)$ 如何作为 A/A^{*2} 中的元素，以及在更一般的情况下如何定义 $d(L/K)$。

解答： 设 $A \subset B$ 是环的扩展，且 B 作为 A-模是秩为 m 的自由模。对于 B 中的元素 $\beta_1, \cdots, \beta_m$，其判别式定义为：

$$d(\beta_1, \cdots, \beta_m) = \det\left(\mathrm{Tr}_{B|A}(\beta_i\beta_j)\right),$$

其中 $\mathrm{Tr}_{B|A}$ 是 B 相对于 A 的迹映射。可以验证，$(\alpha,\beta)\mapsto \mathrm{Tr}_{B|A}(\alpha\beta)$ 是一个对称双线性形式。因此，若 $\gamma_j=\sum_i a_{ji}\beta_i$（其中 $a_{ij}\in A$），则：

$$d(\gamma_1,\cdots,\gamma_m)=\det(a_{ij})^2 d(\beta_1,\cdots,\beta_m).$$

若 $\beta_1,\cdots,\beta_m$ 和 $\gamma_1,\cdots,\gamma_m$ 均为 B 的基，则 $\det(a_{ij})$ 是 A 中的单位，故判别式在单位平方乘积的意义下不变。因此，判别式可视为 A/A^{*2} 中的元素，记为 $d(B/A)$，称为 B 相对于 A 的判别式。

更一般地，设 K 是 A 的分式域，L 是 K 的度为 m 的扩展。若 A 在 L 中的整闭包 B 是 A 上秩为 m 的自由模，则 $d(B/A)$ 表示 $d(L/K)$。此外，若 $L\mid K$ 是可分的，则 $d(L/K)\neq 0$。

4.1.1 **问题：** 在问题 4.1 中，当 $A=\mathbb{Z}$ 时，说明判别式 $d(B/A)$ 是一个明确定义的整数，并解释为什么可以省略基环 $\mathbb{Z}$，直接记为 $d(B)$。对于数域 K 是 $\mathbb{Q}$ 上度为 m 的扩展的情况，说明环 $\mathcal{O}_K$ 在 $\mathbb{Z}$ 上是秩 m 的自由模，并定义 d_K 作为 K 的判别式。

解答： 当 $A=\mathbb{Z}$ 时，$\mathbb{Z}$ 中单位只有 ±1，其平方仅为 1。因此，判别式 $d(B/A)$ 作为一个在 $\mathbb{Z}/\mathbb{Z}^{*2}$ 中的元素，只可能是整数本身，不受单位平方的模除影响，故 $d(B/A)$ 是明确定义的整数。在这种情况下，我们可以省略基环 $\mathbb{Z}$，直接记为 $d(B)$。

对于数域 K 是 $\mathbb{Q}$ 上度为 m 的扩展，$\mathcal{O}_K$ 是 K 中整环，它在 $\mathbb{Z}$ 上是秩 m 的自由模。因此，$d(\mathcal{O}_K)$ 是一个明确定义的整数。我们定义 $d(K/\mathbb{Q})$ 作为 $\mathbb{Q}^*/\mathbb{Q}^{*2}$ 中的元素，由 $d(\mathcal{O}_K)$ 表示，并将此整数记为 d_K，称为数域 K 的判别式。

4.2 **问题：** 设 $\mathfrak{a}\subset\mathfrak{a}'$ 是数域 K 中两个非零的有限生成 $\mathcal{O}_K$-子模，证明指数（index）$(\mathfrak{a}':\mathfrak{a})$ 是有限的，并且满足关系：

$$d(\mathfrak{a})=(\mathfrak{a}':\mathfrak{a})^2 d(\mathfrak{a}').$$

解答： 设 $\beta_1,\cdots,\beta_m$ 是 $\mathfrak{a}'$ 的一个整基。因为 $\mathfrak{a}\subset\mathfrak{a}'$ 是 $\mathbb{Z}$-模，根据有限生成 $\mathbb{Z}$-模的基本定理，存在整数 $a_1,\cdots,a_m$ 满足 $a_i\mid a_{i+1}$（$i=1,\cdots,m-1$），使得 $a_1\beta_1,\cdots,a_m\beta_m$ 是 $\mathfrak{a}$ 的整基。此外，$\mathfrak{a}'/\mathfrak{a}\cong\mathbb{Z}/(a_1)\oplus\cdots\oplus\mathbb{Z}/(a_m)$，因此索引 $(\mathfrak{a}':\mathfrak{a})=a_1a_2\cdots a_m$ 是有限的。

现在计算判别式：

$$d(\mathfrak{a})=d(a_1\beta_1,\cdots,a_m\beta_m)=\det(T)^2 d(\beta_1,\cdots,\beta_m)=\det(T)^2 d(\mathfrak{a}'),$$

其中基变换矩阵 $T=\mathrm{diag}(a_1,a_2,\cdots,a_m)$，因此 $\det(T)=a_1a_2\cdots a_m=(\mathfrak{a}':\mathfrak{a})$。于是：

$$d(\mathfrak{a})=(\mathfrak{a}':\mathfrak{a})^2 d(\mathfrak{a}').$$

证毕。

5 **问题：** 证明 $\left\{1,\sqrt[3]{2},\sqrt[3]{2}^2\right\}$ 是 $\mathbb{Q}(\sqrt[3]{2})$ 的整基。

解答 1： 首先计算基 $\left\{1,\sqrt[3]{2},\sqrt[3]{2}^2\right\}$ 的判别式。$\mathbb{Q}(\sqrt[3]{2})$ 到 $\mathbb{C}$ 的嵌入为 $\sigma_1=\mathrm{id}$、$\sigma_2:\sqrt[3]{2}\mapsto\sqrt[3]{2}\omega$、$\sigma_3:\sqrt[3]{2}\mapsto\sqrt[3]{2}\omega^2$，其中 ω 为三次单位根。则：

$$\begin{aligned}
d\left(1,\sqrt[3]{2},\sqrt[3]{2}^2\right)&=\det\begin{pmatrix}1&\sqrt[3]{2}&\sqrt[3]{2}^2\\1&\sqrt[3]{2}\omega&\sqrt[3]{2}^2\omega^2\\1&\sqrt[3]{2}\omega^2&\sqrt[3]{2}\omega\end{pmatrix}^2\\
&=\left((\sqrt[3]{2}-\sqrt[3]{2}\omega)(\sqrt[3]{2}\omega-\sqrt[3]{2}\omega^2)(\sqrt[3]{2}-\sqrt[3]{2}\omega^2)\right)^2\\
&=4(1-\omega)^2(\omega-\omega^2)^2(1-\omega^2)^2\\
&=4(1-\omega)^6=4(-3\omega)^3=-108
\end{aligned}$$

命题 1：设 $\mathfrak{a}\subset\mathfrak{a}'$ 是数域 K 中两个非零的有限生成 $\mathcal{O}_K$-子模，则指数（index）$(\mathfrak{a}':\mathfrak{a})$ 是有限的，并且满足关系：

$$d(\mathfrak{a})=(\mathfrak{a}':\mathfrak{a})^2d(\mathfrak{a}').$$

由**命题 1** 可得：$\left(\mathcal{O}_K:\mathbb{Z}[\sqrt[3]{2}]\right)^2d_K=-108=-2^2\cdot3^3$。设指数为 m，则 $m=1,2,3$ 或 6。

Stickelberger 判别式关系：代数域 K 的判别式 d_K 总是 $\equiv 0$ 或1 (mod 4)。

由 **Stickelberger 判别式关系**可得：$m=1$ 或 3。若 $m=3$，则 $3\mathcal{O}_K\subset\mathbb{Z}[\sqrt[3]{2}]$，存在 $\alpha=\frac{1}{3}(a+b\sqrt[3]{2}+c\sqrt[3]{2}^2)\in\mathcal{O}_K$ 但 $\alpha\notin\mathbb{Z}[\sqrt[3]{2}]$，且可假设 $a,b,c\in\{0,-1,1\}$。α 的最小多项式为：

$$X^3-aX^2+\frac{1}{3}(a^2-2bc)X-\frac{1}{27}(a^3+2b^3+4c^3-6abc)$$

此多项式在此情况下非整，矛盾。故 $m=1$，$\mathcal{O}_K=\mathbb{Z}[\sqrt[3]{2}]$。

解答 2：利用艾森斯坦多项式和一引理给出另一证明。

艾森斯坦多项式：若多项式 $X^n+a_{n-1}X^{n-1}+\cdots+a_0\in\mathbb{Z}[X]$ 对素数 p 满足 $p\mid a_i(1\le i\le n-1)$ 且 $p\mid a_0$ 但 $p^2\nmid a_0$，则为艾森斯坦多项式。

引理 1：设 K 为 n 次数域，$\alpha\in K$ 为 n 次代数整数，其最小多项式对素数 p 为艾森斯坦多项式，则 $p\nmid(\mathcal{O}_K:\mathbb{Z}[\alpha])$。

证明：设 $f(X)=X^n+a_{n-1}X^{n-1}+\cdots+a_0$ 为 α 的最小多项式。若 $p\mid(\mathcal{O}_K:\mathbb{Z}[\alpha])$，则存在 $\beta\in\mathcal{O}_K$，使得 $p\beta\in\mathbb{Z}[\alpha]$ 但 $\beta\notin\mathbb{Z}[\alpha]$。写：

$$p\beta=b_{n-1}\alpha^{n-1}+\cdots+b_1\alpha+b_0,\quad b_i\in\mathbb{Z}$$

且不全被 p 整除。取最小 j（$0\le j\le n-1$）使得 $p\nmid b_j$。因 $p\mid b_i$（$i<j$），则 $\frac{b_i}{p}\alpha^i\in\mathcal{O}_K$。定义：

$$\gamma=\frac{b_{n-1}}{p}\alpha^{n-1}+\cdots+\frac{b_j}{p}\alpha^j=\beta-\frac{b_{j-1}}{p}\alpha^{j-1}-\cdots-\frac{b_0}{p}\in\mathcal{O}_K$$

因 $f(X)$ 为艾森斯坦多项式，$\frac{1}{p}\alpha^n=-\frac{a_{n-1}}{p}\alpha^{n-1}-\cdots-\frac{a_0}{p}\in\mathcal{O}_K$。于是：

$$\frac{b_j}{p}\alpha^{n-1}=\gamma\alpha^{n-j-1}-\left(b_{n-1}\alpha^{n-j-2}+\cdots+b_{j+1}\right)\frac{1}{p}\alpha^n\in\mathcal{O}_K$$

计算范数：

$$N_{K|\mathbb{Q}}\left(\frac{b_j}{p}\alpha^{n-1}\right)=\frac{b_j^n}{p^n}N_{K|\mathbb{Q}}(\alpha)^{n-1}=\frac{b_j^na_0^{n-1}}{p^n}\notin\mathbb{Z}$$

因 $p\nmid b_j$ 且 $p^2\nmid a_0$，矛盾。故 $p\nmid(\mathcal{O}_K:\mathbb{Z}[\alpha])$。

结合**艾森斯坦多项式**和**引理 1**，设 $m=\left(\mathcal{O}_K:\mathbb{Z}[\sqrt[3]{2}]\right)$，则 $m^2d_K=-108$。故 $m=1,2,3$ 或 6。需证 2 和 3 不整除 m。$\sqrt[3]{2}$ 的最小多项式 X^3-2 对 2 为艾森斯坦多项式，故 $2\nmid m$。设 $\alpha=1+\sqrt[3]{2}$，则 $K=\mathbb{Q}(\alpha)$。α 的最小多项式为 X^3-3X^2+3X-3，对 3 为艾森斯坦多项式，故 $3\nmid(\mathcal{O}_K:\mathbb{Z}[\alpha])$。因 $\mathbb{Z}[\alpha]=\mathbb{Z}[\sqrt[3]{2}]$，则 $3\nmid m$。故 $m=1$。

5.4 **问题：**设 $A\subset B$ 是环的扩展，x 是 B 中的元素。证明以下条件等价：

(1) x 在 A 上是整的；

(2) 对于 A 的每个乘闭子集 S，$x\in S^{-1}B$ 在 $S^{-1}A$ 上是整的；

(3) 对于 A 的每个素理想 $\mathfrak{p}$，$x\in B_\mathfrak{p}$ 在 $A_\mathfrak{p}$ 上是整的；

(4) 对于 A 的每个极大理想 $\mathfrak{m}$，$x\in B_\mathfrak{m}$ 在 $A_\mathfrak{m}$ 上是整的。

解答： 此问题刻画了整性的局部性质。假设条件 (4) 成立，即对于每个极大理想 $\mathfrak{m}$，$x \in B_{\mathfrak{m}}$ 在 $A_{\mathfrak{m}}$ 上是整的，则存在首一多项式 $f_{\mathfrak{m}}(t) \in A_{\mathfrak{m}}[t]$ 使得 $f_{\mathfrak{m}}(x) = 0$。通过通分，可将 $f_{\mathfrak{m}}(t)$ 提升为 $g_{\mathfrak{m}}(t) \in A[t]$，其首项系数 $a_{\mathfrak{m}} \notin \mathfrak{m}$。因为所有 $a_{\mathfrak{m}}$ 共同生成 A（由极大理想的性质），可通过这些 $g_{\mathfrak{m}}(t)$ 黏合得到全局首一多项式 $f(t) \in A[t]$，满足 $f(x) = 0$。故 x 在 A 上是整的，即条件 (1) 成立。

由局部化保持整性的性质，可得：条件 (1) $\Rightarrow$ 条件 (2) $\Rightarrow$ 条件 (3) $\Rightarrow$ 条件 (4)。因此，条件 (1) 至 (4) 等价。

5.7 **问题：** 设 $A \subset B$ 是环的扩展，A' 是 B 中 A 的子代数。证明以下条件等价：

(1) A' 是 A 在 B 中的整闭包；

(2) 对于 A 的每个乘闭子集 S，$S^{-1}A'$ 是 $S^{-1}A$ 在 $S^{-1}B$ 中的整闭包；

(3) 对于 A 的每个素理想 p，A'_p 是 A_p 在 B_p 中的整闭包；

(4) 对于 A 的每个极大理想 $\mathfrak{m}$，$A'_{\mathfrak{m}}$ 是 $A_{\mathfrak{m}}$ 在 $B_{\mathfrak{m}}$ 中的整闭包。

解答： 此问题刻画了整闭包的局部性质。若条件 (1) 成立，即 A' 是 A 在 B 中的整闭包，则由 5.4，$S^{-1}A' \subset S^{-1}A$ 在 $S^{-1}B$ 中的整闭包。反过来，若 $\frac{b}{s} \in S^{-1}B$ 在 $S^{-1}A$ 上整，设其最小多项式为 $X^n + \frac{a_{n-1}}{s_{n-1}}X^{n-1} + \cdots + \frac{a_0}{s_0} = 0$。则 $s_0 s_1 \cdots s_{n-1} b$ 在 A 上整，故属于 A'。因此，$\frac{b}{s} = \frac{s_0 s_1 \cdots s_{n-1} b}{s_0 s_1 \cdots s_{n-1}} \in S^{-1}A'$，$S^{-1}A'$ 是整闭包，即条件 (2) 成立。由局部化定义，条件 (2) $\Rightarrow$ 条件 (3) $\Rightarrow$ 条件 (4)。若条件 (4) 成立，即对于每个极大理想 $\mathfrak{m}$，$A'_{\mathfrak{m}}$ 是 $A_{\mathfrak{m}}$ 在 $B_{\mathfrak{m}}$ 中的整闭包，则 A' 中元素在 $B_{\mathfrak{m}}$ 中的像属于 $A'_{\mathfrak{m}}$，故在 $A_{\mathfrak{m}}$ 上整，由 5.4，属于 A 在 B 中的整闭包。反过来，若 $b \in B$ 在 A 上整，则其在 $B_{\mathfrak{m}}$ 中的像属于 $A'_{\mathfrak{m}}$。因 $\frac{b}{1} \in A'_{\mathfrak{m}}$ 对所有 $\mathfrak{m}$ 成立，故 $b \in A'$。因此，A' 是整闭包，即条件 (1) 成立。

综上，条件 (1) 至 (4) 等价。

6 **问题：** 证明 $\left\{1, \theta, \frac{1}{2}(\theta + \theta^2)\right\}$ 是 $\mathbb{Q}(\theta)$ 的整基，其中 $\theta^3 - \theta - 4 = 0$。

解答： 因为问题涉及到判别式的计算，并且问题的证明较为复杂，需要到一些中间结论，方可得证。所以首先给出基本定义和一些中间结论，再作完整证明。

定义（多项式判别式） 对于多项式 $f(X) \in K[X]$，其根为 $\theta_1, \theta_2, \ldots, \theta_n$，判别式为：

$$\Delta(f) = \prod_{1 \leq i < j \leq n} (\theta_i - \theta_j)^2$$

命题 1： 三次多项式 $X^3 + aX + b$ 的判别式满足：

$$\Delta(X^3 + aX + b) = -27b^2 - 4a^3.$$

证明： 设 $f(X) = X^3 + aX + b$ 的根为其分裂域中的 $\theta_1, \theta_2, \theta_3$。判别式定义为：

$$\Delta(f) = \prod_{1 \leqslant i < j \leqslant 3} (\theta_i - \theta_j)^2.$$

由对称多项式理论，$\Delta(f)$ 是 $\theta_1, \theta_2, \theta_3$ 的齐次对称多项式。根据 Vieta 公式，根的初等对称和为：

$$s_1 = \theta_1 + \theta_2 + \theta_3 = 0, \quad s_2 = \theta_1\theta_2 + \theta_1\theta_3 + \theta_2\theta_3 = a, \quad s_3 = \theta_1\theta_2\theta_3 = -b.$$

判别式是 6 次齐次多项式，故可设 $\Delta(f) = va^3 + wb^2$。为确定系数 v 和 w，考虑两个特例：取 $f(X) = X^3 - X$（$a = -1, b = 0$），根为 $-1, 0, 1$，则：

$$\Delta(f) = (-1-0)^2(0-1)^2(1-(-1))^2 = 1 \cdot 1 \cdot 4 = 4 = v(-1)^3 = -v,$$

故 $v=-4$。

取 $f(X)=X^3-1$（$a=0,b=-1$），根为 $1,\omega,\omega^2$（ω 为三次单位根），则：

$$\Delta(f)=(1-\omega)^2(\omega-\omega^2)^2(\omega^2-1)^2=(1-\omega)^6=(-3\omega)^3=-27=w(-1)^2=w,$$

故 $w=-27$。

因此，$\Delta(f)=-4a^3-27b^2=-27b^2-4a^3$。证毕。

引理 1： 设 $f(t)\in A[t_1,t_2,\ldots,t_n]$ 是对称多项式，次数为 d。存在权不超过 d 的多项式 $g(X_1,\ldots,X_n)$，使得：

$$f(t)=g(s_1,s_2,\ldots,s_n),$$

其中 s_i 是 $t_1,t_2,\ldots,t_n$ 的第 i 个初等对称多项式。

证明： 设 $f(t)\in A[t_1,t_2,\ldots,t_n]$ 是次数为 d 的对称多项式。由对称多项式基本定理，任何对称多项式可表示为初等对称多项式 $s_1,s_2,\ldots,s_n$ 的多项式，即存在 $g(X_1,\ldots,X_n)\in A[X_1,\ldots,X_n]$ 使得 $f(t)=g(s_1,s_2,\ldots,s_n)$。定义单项式 $X_1^{v_1}X_2^{v_2}\cdots X_n^{v_n}$ 的权为 $v_1+2v_2+\cdots+nv_n$，多项式的权为其单项式的最大权。因为 $f(t)$ 是齐次且次数为 d，其每一项的权（以 t_i 的次数加权）恰为 d。在 g 中，s_i 的权为 i，故 g 的每一项 $X_1^{v_1}\cdots X_n^{v_n}$ 的权 $v_1+2v_2+\cdots+nv_n\leq d$，否则 $f(t)$ 的次数将超过 d，矛盾。因此，存在权不超过 d 的 g 满足要求。

命题 2：：设 $f(X)=X^n+aX+b$（$a,b\in K$）是不可约且可分的，其判别式为：

$$\Delta(X^n+aX+b)=(-1)^{\frac{n(n-1)}{2}}\left(n^nb^{n-1}+(-1)^{n-1}(n-1)^{n-1}a^n\right).$$

证明： 设 $f(X)=X^n+aX+b$ 的根在其分裂域中为 $\theta_1,\theta_2,\ldots,\theta_n$。判别式定义为：

$$\Delta(f)=\prod_{1\leqslant i<j\leqslant n}(\theta_i-\theta_j)^2.$$

利用 $f'(X)=nX^{n-1}+a$，有：

$$\Delta(f)=(-1)^{\frac{n(n-1)}{2}}\prod_{i=1}^{n}\prod_{j\neq i}(\theta_i-\theta_j)=(-1)^{\frac{n(n-1)}{2}}\prod_{i=1}^{n}f'(\theta_i)=(-1)^{\frac{n(n-1)}{2}}N_{L|K}(f'(\theta)),$$

其中 θ 是任一根，$L=K(\theta)$。令 $\gamma=f'(\theta)=n\theta^{n-1}+a$，则：

$$f(X)=(X-\theta)h(X)+f(\theta)=(X-\theta)h(X),$$

且 $f\left(-\frac{nb}{\gamma+(n-1)a}\right)=0$，故 $\theta=-\frac{nb}{\gamma+(n-1)a}$，$K(\gamma)=K(\theta)$。计算 γ 的最小多项式，设：

$$f\left(\frac{-nb}{X+(n-1)a}\right)=\frac{P(X)}{Q(X)},$$

则 $P(\gamma)=0$，且：

$$P(X)=(X+(n-1)a)^n-na(X+(n-1)a)^{n-1}+(-n)^nb^{n-1}.$$

范数为：

$$N_{L|K}(\gamma)=(-1)^nP(0)=(-1)^{n-1}(n-1)^{n-1}a^n+n^nb^{n-1}.$$

代入得：

$$\Delta(f)=(-1)^{\frac{n(n-1)}{2}}\left(n^nb^{n-1}+(-1)^{n-1}(n-1)^{n-1}a^n\right).$$

证毕。

命题 3： 设 $\mathfrak{a} \subset \mathfrak{a}'$ 是数域 K 中两个非零的有限生成 $\mathcal{O}_K$-子模，指数（index）$(\mathfrak{a}' : \mathfrak{a})$ 是有限的，并且满足关系：

$$d(\mathfrak{a}) = (\mathfrak{a}' : \mathfrak{a})^2 d(\mathfrak{a}').$$

有了以上探索，现在进入正式证明环节。

回看问题，首先计算基 $\left\{1, \theta, \frac{1}{2}(\theta + \theta^2)\right\}$ 的判别式。设 $\sigma_1, \sigma_2, \sigma_3$ 为 $\mathbb{Q}(\theta) \to \mathbb{C}$ 的所有嵌入，$\theta_i = \sigma_i \theta$（$i = 1, 2, 3$）。则：

$$\begin{aligned} d\left(1, \theta, \frac{1}{2}(\theta + \theta^2)\right) &= \det \begin{pmatrix} 1 & \theta_1 & \frac{1}{2}(\theta_1 + \theta_1^2) \\ 1 & \theta_2 & \frac{1}{2}(\theta_2 + \theta_2^2) \\ 1 & \theta_3 & \frac{1}{2}(\theta_3 + \theta_3^2) \end{pmatrix}^2 \\ &= \frac{1}{4} \det \begin{pmatrix} 1 & \theta_1 & \theta_1^2 \\ 1 & \theta_2 & \theta_2^2 \\ 1 & \theta_3 & \theta_3^2 \end{pmatrix}^2 \\ &= \frac{1}{4} \prod_{1 \le i < j \le 3} (\theta_i - \theta_j)^2 \end{aligned}$$

根据**命题 1：** $\Delta(X^3 + aX + b) = -27b^2 - 4a^3$。此处 $f(X) = X^3 - \theta - 4$，$a = -1$，$b = -4$。则：

$$\Delta(f) = -27(-4)^2 - 4(-1)^3 = -27 \cdot 16 - 4 \cdot (-1) = -432 + 4 = -428$$

故：

$$d\left(1, \theta, \frac{1}{2}(\theta + \theta^2)\right) = \frac{1}{4} \cdot (-428) = -107$$

因 -107 为素数，由**命题 3**，$\left(\mathcal{O}_K : \mathbb{Z}[\theta, \frac{1}{2}(\theta + \theta^2)]\right)^2 d_K = -107$。指数只能为 1，故 $\left\{1, \theta, \frac{1}{2}(\theta + \theta^2)\right\}$ 为整基。由**命题 1** 的证明：设 $\theta_1, \theta_2, \theta_3$ 为 $f(X) = X^3 + aX + b$ 的根。$\Delta(f)$ 为 $\theta_1, \theta_2, \theta_3$ 的对称多项式。由维塔（Vieta）公式，初等对称多项式为 $s_1 = 0$、$s_2 = a$、$s_3 = -b$。由**引理 1**，$\Delta(f) = va^3 + wb^2$。- 取 $f(X) = X^3 - X$（$a = -1, b = 0$），根为 $-1, 0, 1$，$\Delta(f) = 4 = -v$，故 $v = -4$。- 取 $f(X) = X^3 - 1$（$a = 0, b = -1$），根为三次单位根，$\Delta(f) = -27 = w$，故 $w = -27$。因此，$\Delta(f) = -27b^2 - 4a^3$。

7 **问题：**（Stickelberger 判别式关系）证明代数域 K 的判别式 d_K 总是 $\equiv 0$ 或1 (mod 4)。
解答： 设 $\alpha_1, \ldots, \alpha_m$ 为 $\mathcal{O}_K$ 的整基，$\sigma_1, \ldots, \sigma_m$ 为 K 的所有嵌入。判别式为：

$$d_K = \det(\sigma_i \alpha_j)^2$$

行列式 $\det(\sigma_i \alpha_j)$ 为所有嵌入作用于 $\alpha_1, \ldots, \alpha_m$ 的排列乘积之和。设 P 为偶排列项之和，$-N$ 为奇排列项之和，则：

$$d_K = (P - N)^2 = (P + N)^2 - 4PN$$

设 G 为 K 在 $\mathbb{Q}$ 上伽罗瓦闭包的伽罗瓦群。每个嵌入可延拓为 G 中的元素，反之亦然。对任意 $\tau \in G$，$\tau\sigma_1, \ldots, \tau\sigma_m$ 为 $\sigma_1, \ldots, \sigma_m$ 的一个排列。根据排列的奇偶性：- 若为偶排列，则 $\tau P = P, \tau N = N$；- 若为奇排列，则 $\tau P = N, \tau N = P$。故 $P + N$ 和 PN 被 G 固定，在 $\mathbb{Q}$ 中。因其对 $\mathbb{Z}$ 整，必为整数。因此：

$$d_K \equiv (P + N)^2 \equiv 0 \text{ 或} 1 \pmod 4$$

4 第三章：理想

4.1 练习题

1 **问题：** 将 $33 + 11\sqrt{-7}$ 分解为 $\mathbb{Q}(\sqrt{-7})$ 中不可约的整元素。

解答： 根据练习 2.4，$\mathbb{Q}(\sqrt{-7})$ 的整数环为 $\mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$。在此环中，首先分解 $33+11\sqrt{-7}$ 为：

$$33 + 11\sqrt{-7} = 11 \cdot 2 \cdot \frac{3+\sqrt{-7}}{2}$$

在 $\mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$ 中，元素的范数为：

$$N\left(x + y\left(\frac{1+\sqrt{-7}}{2}\right)\right) = \left(x + \frac{y}{2}\right)^2 + 7\left(\frac{y}{2}\right)^2$$

分步骤证明如下：

步骤 1： 分解 11 为不可约元素。$N(11) = 121 = 11 \cdot 11$。11 可能本身不可约，或分解为两个范数为 11 的不可约元素 α 和 β。考虑方程：

$$\left(x + \frac{y}{2}\right)^2 + 7\left(\frac{y}{2}\right)^2 = 11$$

整数解为 $(1,2), (-3,2), (3,-2), (-1,-2)$，对应元素 $2+\sqrt{-7}, -2+\sqrt{-7}, 2-\sqrt{-7}, -2-\sqrt{-7}$。这些元素仅符号或共轭不同，故分解为：

$$11 = (2+\sqrt{-7}) \cdot (2-\sqrt{-7})$$

此分解在单位因子下唯一。

步骤 2： 分解 2 和 $\frac{3+\sqrt{-7}}{2}$ 为不可约元素。$N(2) = N\left(\frac{3+\sqrt{-7}}{2}\right) = 4 = 2 \cdot 2$。考虑方程：

$$\left(x + \frac{y}{2}\right)^2 + 7\left(\frac{y}{2}\right)^2 = 2$$

整数解为 $(0,1), (-1,1), (0,-1), (1,-1)$，对应元素 $\frac{1+\sqrt{-7}}{2}, \frac{-1+\sqrt{-7}}{2}, \frac{-1-\sqrt{-7}}{2}, \frac{1-\sqrt{-7}}{2}$。这些元素仅符号或共轭不同，故分解为：

$$2 = \frac{1+\sqrt{-7}}{2} \cdot \frac{1-\sqrt{-7}}{2}, \quad \frac{3+\sqrt{-7}}{2} = -\left(\frac{1-\sqrt{-7}}{2}\right)^2$$

此分解在单位因子下唯一。

步骤 3： 综合分解 $33 + 11\sqrt{-7}$：

$$33 + 11\sqrt{-7} = -(2+\sqrt{-7}) \cdot (2-\sqrt{-7}) \cdot \frac{1+\sqrt{-7}}{2} \cdot \left(\frac{1-\sqrt{-7}}{2}\right)^3$$

2 **问题：** 证明：

$$54 = 2 \cdot 3^3 = \frac{13+\sqrt{-47}}{2} \cdot \frac{13-\sqrt{-47}}{2}$$

是 $\mathbb{Q}(\sqrt{-47})$ 中本质不同的两种不可约整元素分解。

解答： 由于 $\frac{13\pm\sqrt{-47}}{2\cdot 2}$ 和 $\frac{13\pm\sqrt{-47}}{2\cdot 3}$ 不属于 $\mathbb{Q}(\sqrt{-47})$ 的整数环，2 和 3（以及 $2 \cdot 3^3$ 的其他非平凡因子）与 $\frac{13+\sqrt{-47}}{2}$ 或 $\frac{13-\sqrt{-47}}{2}$ 不关联。因此，这两种分解本质不同。

备注 2.1： 54 的分解不止这两种，例如 $54 = 3^2 \cdot \frac{5+\sqrt{-47}}{2} \cdot \frac{5-\sqrt{-47}}{2}$ 为另一种分解。

3 **问题：** 设 d 为无平方因子整数，p 为不整除 $2d$ 的素数，$\mathcal{O}$ 为 $\mathbb{Q}(\sqrt{d})$ 的整数环。证明 $(p)=p\mathcal{O}$ 是 $\mathcal{O}$ 的素理想当且仅当同余式 $x^2\equiv d \pmod p$ 无解。

解答： 引用 §1.1 的 1.7.2。由练习 2.4，$\mathcal{O}$ 为 $\mathbb{Z}[\sqrt{d}]$ 或 $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$。若 d 是模 p 的二次剩余，即存在整数 x 使得 $x^2\equiv d \pmod p$。则 $p\mid x^2-d=(x+\sqrt{d})(x-\sqrt{d})$。但因 $p\neq 2$，$\frac{x+\sqrt{d}}{p}$ 和 $\frac{x-\sqrt{d}}{p}$ 不在 $\mathcal{O}$ 中，故 p 不是素元素，(p) 不是素理想。反之，若 d 不是模 p 的二次剩余，证明 p 是素元素。设 $\mathcal{O}$ 中元素 $x_1+y_1\sqrt{d}$ 和 $x_2+y_2\sqrt{d}$ 的乘积在 (p) 中。因 $p\neq 2$，$\frac{x}{p}\in\mathbb{Z}$ 与 $\frac{x}{p}\in\frac{1}{2}\mathbb{Z}$ 等价，可归约至 $\mathcal{O}=\mathbb{Z}[\sqrt{d}]$。由：

$$(x_1+y_1\sqrt{d})(x_2+y_2\sqrt{d})\in(p)$$

得：

$$p^2=N(p)\mid N(x_1+y_1\sqrt{d})N(x_2+y_2\sqrt{d})$$

则 p 整除 $N(x_1+y_1\sqrt{d})$ 或 $N(x_2+y_2\sqrt{d})$，例如前者：

$$p\mid N(x_1+y_1\sqrt{d})=x_1^2-dy_1^2$$

即：

$$x_1^2\equiv dy_1^2 \pmod p$$

因 d 不是模 p 的二次剩余，y_1 在模 p 下不可逆，故 $p\mid y_1$ 且 $p\mid x_1$。因此 $x_1+y_1\sqrt{d}\in(p)$，(p) 是素理想。

4 **问题：** 具有有限个素理想的戴德金域是主理想域。

解答： 首先证明 $\mathcal{O}$ 仅有一个非零素理想 $\mathfrak{p}$ 的情况（例如局部环）。存在 $\pi\in\mathfrak{p}\setminus\mathfrak{p}^2$。考虑理想 (π)，由本节定理 (3.3)，其唯一分解为 $(\pi)=\mathfrak{p}^\nu$。但 $\pi\notin\mathfrak{p}^2$，故 $(\pi)=\mathfrak{p}$，表明 $\mathcal{O}$ 唯一素理想为主理想。由定理 (3.3)，所有理想为主理想。对于 $\mathcal{O}$ 有有限个素理想 $\mathfrak{p}_1,\dots,\mathfrak{p}_r$ 的情况，若 $\mathfrak{a}=\mathfrak{p}_1^{\nu_1}\cdots\mathfrak{p}_r^{\nu_r}\neq 0$，取 $\pi_i\in\mathfrak{p}_i\setminus\mathfrak{p}_i^2$。由中国剩余定理，存在 $a\in\mathcal{O}$ 对应余类 $\pi_i^{\nu_i} \pmod{\mathfrak{p}_i^{\nu_i+1}}$。设 $(a)=\mathfrak{p}_1^{\mu_1}\cdots\mathfrak{p}_r^{\mu_r}$。因 $a\equiv\pi_i^{\nu_i} \pmod{\mathfrak{p}_i^{\nu_i+1}}$，$a\notin\mathfrak{p}_i^{\nu_i+1}$，故 $\mu_i\leq\nu_i$；且 $a\in\mathfrak{p}_i^{\mu_i}$，故 $\mu_i\geq\nu_i$。因此 $(a)=\mathfrak{a}$。

5 **问题：** 戴德金域 $\mathcal{O}$ 被非零理想 $\mathfrak{a}$ 商得的商环 $\mathcal{O}/\mathfrak{a}$ 是主理想域。

解答：（备注 5.1：此命题错误，$\mathcal{O}/\mathfrak{a}$ 一般不是整环。正确结论为：$\mathcal{O}/\mathfrak{a}$ 是主环，即每个理想为主理想。）

首先证明 $\mathfrak{a}=\mathfrak{p}^n$ 的情况。$\mathcal{O}/\mathfrak{a}$ 的唯一真理想为 $\mathfrak{p}/\mathfrak{p}^n,\dots,\mathfrak{p}^{n-1}/\mathfrak{p}^n$。取 $\pi\in\mathfrak{p}\setminus\mathfrak{p}^2$，则 $\pi^i\mathcal{O}/\mathfrak{p}^n=\mathfrak{p}^i/\mathfrak{p}^n$（因 $\pi^i\in\mathfrak{p}^i\setminus\mathfrak{p}^{i+1}$），故所有真理想为主理想。一般情况，注意到 PID 的商环仍是主环，用归纳法即可。

命题 5.2（戴德金性是局部性质）： 设 D 为整环，则以下等价：

1. D 是戴德金域；
2. D 是诺特环，且对每个乘法闭子集 S，$S^{-1}D$ 是戴德金域；
3. D 是诺特环，且对每个素理想 $\mathfrak{p}$，$D_\mathfrak{p}$ 是戴德金域；
4. D 是诺特环，且对每个极大理想 $\mathfrak{m}$，$D_\mathfrak{m}$ 是戴德金域。

证明：戴德金域是诺特、整闭且非零素理想极大的环。$S^{-1}D$ 的素理想对应于 $D\setminus S$ 中的素理想，故“极大”条件是局部性质。由整闭性和诺特性的局部性得证。

备注 5.3：“戴德金性是局部性质”指命题 5.2，非严格局部性质。例如，$\mathbb{Z}$ 在 $\mathbb{Q}$ 加入所有素数 p 的 p 次单位根的域中整闭包非诺特，故非戴德金域。

6 **问题：** 戴德金域的每个理想可由两个元素生成。

解答： 对 $\mathcal{O}$ 的每个理想 $\mathfrak{a}$，取 $a\in\mathfrak{a}$，商环 $\mathcal{O}/(a)$ 为主环（练习 5）。$\mathfrak{a}$ 在 $\mathcal{O}/(a)$ 中的像

是主理想，由 $b \pmod{(a)}$（$b \in \mathfrak{a}$）生成，故 $\mathfrak{a} = (a) + (b)$。

定理 6.1： 戴德金域 $\mathcal{O}$ 是 PID 当且仅当其类群平凡。

证明：若类群平凡，每分式理想为主理想，故 $\mathcal{O}$ 是 PID。反之，若 $\mathcal{O}$ 是 PID，对每个分式理想 $\mathfrak{a}$，存在 $c \in \mathcal{O}$ 使 $c\mathfrak{a}$ 为主理想，故 $\mathfrak{a}$ 为主理想，类群平凡。

7 **问题：** 在诺特环 R 中，若每个素理想极大，则每个理想降链 $a_1 \supseteq a_2 \supseteq \cdots$ 最终稳定。

7.1 备注 "每个素理想极大"意味着 (0) 不能是素理想，除非 R 是域。

解答：

证明：首先，我们证明在诺特环中，(0) 具有素分解 $(0) = \mathfrak{p}_1 \cdots \mathfrak{p}_r$。实际上，由本节引理 (3.4)，在诺特环中，每个真理想（包括 (0)）具有素分解。因此，我们有 $(0) \supset \mathfrak{p}_1 \cdots \mathfrak{p}_r$。但 $(0) = \{0\}$，故 $(0) = \mathfrak{p}_1 \cdots \mathfrak{p}_r$。此外，$\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ 是所有素理想。若不是，则存在另一个素理想 $\mathfrak{q}$ 使得 $\mathfrak{p}_1 \cdots \mathfrak{p}_r = (0) \subset \mathfrak{q}$。因此，其中某个素理想，例如 $\mathfrak{p}_1$，必须被包含在 $\mathfrak{q}$ 中。但由于每个素理想是极大的，故 $\mathfrak{p}_1 = \mathfrak{q}$，这产生矛盾。因此，我们得到一个理想的降链：

$$R \supset \mathfrak{p}_1 \supset \mathfrak{p}_1\mathfrak{p}_2 \supset \cdots \supset \mathfrak{p}_1 \cdots \mathfrak{p}_r = (0)$$

每个因子 $\mathfrak{p}_1 \cdots \mathfrak{p}_{i-1}/\mathfrak{p}_1 \cdots \mathfrak{p}_i$ 是域 $R/\mathfrak{p}_i$ 上的向量空间。对于向量空间 V，链条件等价于 $\dim V$ 有限。因此，$\mathfrak{p}_1 \cdots \mathfrak{p}_{i-1}/\mathfrak{p}_1 \cdots \mathfrak{p}_i$ 是诺特模当且仅当它是阿廷模，作为 $R/\mathfrak{p}_i$-模（进而作为 R-模）。反复应用引理 7.2，我们看到 R 是诺特环当且仅当它是阿廷环。

引理 7.2： 设 $0 \to M' \to M \to M'' \to 0$ 为 R-模的短正合序列，则 M 是诺特（或阿廷）模当且仅当 M' 和 M'' 都是诺特（或阿廷）模。

证明：

对于"if"部分： 注意到 M 的子模链 (M_i) 由其在 M' 中的逆像 (M_i') 和在 M'' 中的像 (M_i'') 控制。依五引理（Five-Lemma）：考虑以下交换图：

$$\begin{array}{ccccccccc}
0 & \longrightarrow & M_i' & \longrightarrow & M_i & \longrightarrow & M_i'' & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle f_i'} & & \downarrow{\scriptstyle f_i} & & \downarrow{\scriptstyle f_i''} & & \\
0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0
\end{array}$$

事实上，对于足够大的 i，嵌入 $f_i' : M_i' \to M'$ 和 $f_i'' : M_i'' \to M''$ 成为恒等映射，因此依五引理，$f_i : M_i \to M$ 也为恒等映射。因此，M 的子模链最终稳定。

对于"only if"部分： 仅仅注意到 M' 或 M'' 的子模链会诱导 M 的子模链，故因 M 是诺特（或阿廷）模，M' 和 M'' 的链也稳定。

7.3（合成列）： R-模 M 的合成列是子模链：

$$M = M_0 \supset M_1 \supset \cdots \supset M_n = 0$$

其中无法插入额外子模。若 M 有合成列，则所有合成列长度相同（称为 M 的长度），任何子模链可扩展为合成列（参考 [AM94]）。

命题 7.4： M 有合成列当且仅当 M 既是诺特模又是阿廷模。

证明：若 M 有合成列，子模链长度有界，故 M 是诺特和阿廷模。若 M 是诺特和阿廷模，构造合成列：因 $M_0 = M$ 是诺特模，存在极大子模 M_1。类似地，M_1 有极大子模 M_2。继续得降链 $M = M_0 \supset M_1 \supset M_2 \supset \cdots$。因 M 是阿廷模，链有限，构成合成列。

推论 7.5： 对向量空间 V，以下等价：

1. V 有限维；
2. V 长度有限；

3. V 是诺特模；
4. V 是阿廷模。

应用此结果，$\mathfrak{p}_1\cdots\mathfrak{p}_{i-1}/\mathfrak{p}_1\cdots\mathfrak{p}_i$ 有限维，其子空间与 $\mathfrak{p}_1\cdots\mathfrak{p}_i$ 和 $\mathfrak{p}_1\cdots\mathfrak{p}_{i-1}$ 间的理想一一对应，故链 $R\supset\mathfrak{p}_1\supset\mathfrak{p}_1\mathfrak{p}_2\supset\cdots\supset\mathfrak{p}_1\cdots\mathfrak{p}_r=(0)$ 可扩展为合成列，R 是阿廷环，降链稳定。

8 **问题：** 设 $\mathfrak{m}$ 为戴德金域 $\mathcal{O}$ 的非零整理想。证明在 Cl_K 的每个理想类中，存在与 $\mathfrak{m}$ 互素的整理想。

解答： 对任意理想 $\mathfrak{a}$ 和 $\mathfrak{b}$，需存在 $c\in K$ 使 $c\mathfrak{a}$ 与 $\mathfrak{b}$ 互素。设 $\mathfrak{p}_1,\ldots,\mathfrak{p}_r$ 为包含 $\mathfrak{b}$ 的所有不同素理想。由命题 8.3，存在 $c_1\in\mathcal{O}$ 使 $\mathrm{ord}_{\mathfrak{p}_i}c_1=\mathrm{ord}_{\mathfrak{p}_i}\mathfrak{a}$，故 $\mathrm{ord}_{\mathfrak{p}_i}c_1^{-1}\mathfrak{a}=0$。若 $c_1^{-1}\mathfrak{a}$ 非整理想，设 $\mathfrak{q}_1,\ldots,\mathfrak{q}_s$ 为包含 c_1 且不同于 $\mathfrak{p}_i$ 的素理想，再取 $c_2\in\mathcal{O}$ 使 $\mathrm{ord}_{\mathfrak{p}_i}c_2=0$、$\mathrm{ord}_{\mathfrak{q}_j}c_2=\mathrm{ord}_{\mathfrak{q}_j}c_1$。则 $c_2c_1^{-1}\mathfrak{a}$ 为整理想且与 $\mathfrak{b}$ 互素。

命题 8.3： 对素理想 $\mathfrak{p}_1,\ldots,\mathfrak{p}_r$ 和整数 $\nu_1,\ldots,\nu_r$，存在 $x\in\mathcal{O}$ 使 $\mathrm{ord}_{\mathfrak{p}_i}x=\nu_i$（由中国剩余定理）。

9 **问题：** 设 $\mathcal{O}$ 为整环，其所有非零理想具有唯一素理想分解。证明 $\mathcal{O}$ 是戴德金域。

解答： **命题 9.3：** $\mathcal{O}$ 的每个非零素理想 $\mathfrak{p}$ 是极大的。

证明：

步骤 1： 对可逆素理想 $\mathfrak{p}$，对任意 $a\in\mathcal{O}\setminus\mathfrak{p}$，若 $(a)+\mathfrak{p}\neq\mathcal{O}$，设 $(a)+\mathfrak{p}=\mathfrak{p}_1\cdots\mathfrak{p}_m$、$(a^2)+\mathfrak{p}=\mathfrak{q}_1\cdots\mathfrak{q}_n$。在 $\mathcal{O}/\mathfrak{p}$ 中，$(b)=\mathfrak{p}_1/\mathfrak{p}\cdots\mathfrak{p}_m/\mathfrak{p}$、$(b^2)=\mathfrak{q}_1/\mathfrak{p}\cdots\mathfrak{q}_n/\mathfrak{p}$。由引理 9.2，$\mathfrak{p}_i/\mathfrak{p}$、$\mathfrak{q}_j/\mathfrak{p}$ 可逆。由引理 9.1，$(\mathfrak{p}_1/\mathfrak{p})^2\cdots(\mathfrak{p}_m/\mathfrak{p})^2=\mathfrak{q}_1/\mathfrak{p}\cdots\mathfrak{q}_n/\mathfrak{p}$，故 $n=2m$。因此 $(a^2)+\mathfrak{p}=((a)+\mathfrak{p})^2$。则 $\mathfrak{p}=a\mathfrak{p}+\mathfrak{p}^2$。因 $\mathfrak{p}$ 可逆，$(a)+\mathfrak{p}=\mathcal{O}$。

步骤 2： 证明每个非零素理想可逆。取 $a\in\mathfrak{p}\setminus\{0\}$，$(a)=\mathfrak{p}_1\cdots\mathfrak{p}_n$。由引理 9.2 和步骤 1，$\mathfrak{p}_i$ 可逆且极大，故 $\mathfrak{p}=\mathfrak{p}_i$。

命题 9.7： $\mathcal{O}$ 是诺特环。

证明：每个非零理想可逆（命题 9.4），故有限生成，$\mathcal{O}$ 是诺特环。

命题 9.8： 若 $\mathcal{O}$ 是局部环，则整闭。

证明：$\mathcal{O}$ 仅有素理想 $\mathfrak{m}$。取 $\pi\in\mathfrak{p}\setminus\mathfrak{p}^2$，$(\pi)=\mathfrak{p}^\nu$。因 $\pi\notin\mathfrak{p}^2$，$(\pi)=\mathfrak{p}$，$\mathcal{O}$ 是 PID，故整闭。

由命题 9.3、9.7、9.8，局部情况下 $\mathcal{O}$ 是戴德金域。一般情况，对素理想 $\mathfrak{p}$，$\mathcal{O}_\mathfrak{p}$ 满足条件，由定理 9.9 是戴德金域。结合命题 5.2，$\mathcal{O}$ 是戴德金域。

10 **问题：** 戴德金域 $\mathcal{O}$ 的分式理想 $\mathfrak{a}$ 是投影 $\mathcal{O}$-模。

解答： **命题 10.1：** 每个有限生成无挠 $\mathcal{O}$-模是投影的。

证明：对 PID，有限生成无挠模是自由的（[Lan02, III, 定理 7.3]），故投影。对有限生成无挠模 M，对素理想 $\mathfrak{p}$，$M_\mathfrak{p}$ 在 $\mathcal{O}_\mathfrak{p}$ 上自由，故投影。存在有限自由模 F 和满射 $f:F\to M$。局部分裂 $g_\mathfrak{p}:M_\mathfrak{p}\to F_\mathfrak{p}$。取 $c_\mathfrak{p}\notin\mathfrak{p}$ 使 $c_\mathfrak{p}g_\mathfrak{p}(M)\subset F$。$\{c_\mathfrak{p}\}$ 生成单位理想，否则矛盾。取 $\sum x_ic_{\mathfrak{p}_i}=1$。定义 $g=\sum x_ic_{\mathfrak{p}_i}g_{\mathfrak{p}_i}$，则 $f\circ g=\mathrm{id}$。故 M 是投影的。

随即得证，分式理想 $\mathfrak{a}$ 是投影 $\mathcal{O}$-模。

5 第四章：格

5.1 练习题

1 **问题：** 证明在 $\mathbb{R}^n$ 中的格 Γ 是完备的当且仅当商空间 $\mathbb{R}^n/\Gamma$ 是紧的。

解答： 若 Γ 是完备的，则基本网格 Φ 满足 $\Phi+\Gamma=\mathbb{R}^n$。投影 $\pi:\mathbb{R}^n\to\mathbb{R}^n/\Gamma$ 将紧集映射为紧集，且 Φ 和 $\Phi+\Gamma$ 在此投影下的像相同，因此 $\mathbb{R}^n/\Gamma$ 是紧的。反之，若 Γ 不完备，设 V_0 为 Γ 生成的子空间 $\mathbb{R}^n$ 中的子空间。则存在 $v\in\mathbb{R}^n\setminus V_0$，故 $\pi|_{V_0}$ 是单射。因 π 是拓扑群的商映射，故是开映射，$\pi|_{V_0}$ 是开嵌入。因此 $\mathbb{R}^n/\Gamma$ 不是紧的。

2 **问题：** 通过构造一个中心对称的凸集 $X\subset V$ 的例子，证明闵可夫斯基格点定理无法改进，其中 $\operatorname{vol}(X)=2^n\operatorname{vol}(\Gamma)$ 但 X 不含 Γ 的任何非零格点。然而，若 X 是紧的，则在等式情况下定理 (4.4) 仍然成立。

解答： 例如，考虑 $\mathbb{R}^2$ 中的格 $\mathbb{Z}^2$。集合 $X=(-1,1)\times(-1,1)$ 是中心对称的凸集，且体积为 4。但 X 不含任何非零格点。对于第二部分，使用定理 (4.4) 的方法。需证明存在两个不同格点 $\gamma_1,\gamma_2\in\Gamma$，使得：

$$\left(\frac{1}{2}X+\gamma_1\right)\cap\left(\frac{1}{2}X+\gamma_2\right)\neq\varnothing$$

若成立，则 $\gamma_1-\gamma_2\in X\cap\Gamma$。当 X 是紧的，若 $\frac{1}{2}X+\gamma$ 两两不相交，则：

$$\operatorname{vol}(\Phi)>\sum_{\gamma\in\Gamma}\operatorname{vol}\left(\Phi\cap\left(\frac{1}{2}X+\gamma\right)\right)$$

因 $(\Phi-\gamma)\cap\frac{1}{2}X$ 的体积与 $\Phi\cap\left(\frac{1}{2}X+\gamma\right)$ 相同，且 $\Phi-\gamma$（$\gamma\in\Gamma$）覆盖整个空间 V，有：

$$\operatorname{vol}(\Phi)>\sum_{\gamma\in\Gamma}\operatorname{vol}\left((\Phi-\gamma)\cap\frac{1}{2}X\right)=\operatorname{vol}\left(\frac{1}{2}X\right)=\frac{1}{2^n}\operatorname{vol}(X)$$

这与假设矛盾。

3 **问题：**（闵可夫斯基线性形式定理）设实线性形式为：

$$L_i(x_1,\dots,x_n)=\sum_{j=1}^{n}a_{ij}x_j,\quad i=1,\dots,n,$$

其中 $\det(a_{ij})\neq0$，且正实数 $c_1,\dots,c_n$ 满足 $c_1\cdots c_n>|\det(a_{ij})|$。证明存在整数 $m_1,\dots,m_n\in\mathbb{Z}$，使得：

$$|L_i(m_1,\dots,m_n)|<c_i,\quad i=1,\dots,n$$

解答： 考虑 $\mathbb{R}^n$ 中的格 $\Gamma=\mathbb{Z}^n$，$\operatorname{vol}(\Gamma)=1$。考虑子集：

$$X=\{(x_1,\dots,x_n)\in\mathbb{R}^n\mid|L_i(x_1,\dots,x_n)|<c_i,i=1,\dots,n\}$$

子集 $X_0=\prod_{i=1}^n(-c_i,c_i)$ 的体积为 $2^nc_1\cdots c_n$，通过变换 $(L_1,\dots,L_n)$ 得到 X，故：

$$\operatorname{vol}(X)=|\det(\frac{\partial L_i}{\partial x_j})|^{-1}\operatorname{vol}(X_0)=|\det(a_{ij})|^{-1}2^nc_1\cdots c_n>2^n=2^n\operatorname{vol}(\Gamma)$$

由闵可夫斯基格点定理，X 含有一个非零格点 $(m_1,\dots,m_n)$。

6 第五章：闵可夫斯基理论

6.1 练习题

1 **问题：**写出一个仅依赖于 K 的常数 A，使得 K 的每个非零整理想 $\mathfrak{a}$ 含有一个非零元素 a，满足：

$$|\tau a| < A(\mathcal{O}_K : \mathfrak{a})^{1/n},$$

其中 $n = [K : \mathbb{Q}]$，对所有 $\tau \in \mathrm{Hom}(K, \mathbb{C})$。

解答：设 $A = \sqrt[n]{(\frac{2}{\pi})^s\sqrt{|d_K|}}$，则 $c_\tau = A(\mathcal{O}_K : \mathfrak{a})^{1/n}$ 满足定理 (5.3) 的条件，故存在非零 a，对所有 $\tau \in \mathrm{Hom}(K, \mathbb{C})$ 满足：

$$|\tau a| < A(\mathcal{O}_K : \mathfrak{a})^{1/n}$$

2 **问题：**证明中心对称的凸集：

$$X = \left\{(z_\tau) \in K_\mathbb{R} \mid \sum_\tau |z_\tau| < t\right\}$$

的体积为 $\mathrm{vol}(X) = 2^r\pi^s\frac{t^n}{n!}$（见第三章 (2.15)）。

解答： X 在 $\mathbb{R}^{r+2s}$ 中的像为：

$$f(X) = \left\{(x_\tau) \in \prod_\tau \mathbb{R} \mid \sum_\rho |x_\rho| + 2\sum_\sigma \sqrt{x_\sigma^2 + x_{\bar\sigma}^2} < t\right\}$$

为简化记号，代 x_i（$i = 1, \dots, r$）代替 x_ρ，y_j, z_j（$j = 1, \dots, s$）代替 $x_\sigma, x_{\bar\sigma}$。$f(X)$ 的体积通过积分计算：

$$I(t) = \int_{f(X)} dx_1 \cdots dx_r dy_1 \cdots dy_s dz_1 \cdots dz_s$$

用极坐标 $y_j = u_j \cos\theta_j, z_j = u_j \sin\theta_j$，得：

$$I(t) = \int u_1 \cdots u_s dx_1 \cdots dx_r du_1 \cdots du_s d\theta_1 \cdots d\theta_s$$

积分域为：

$$\begin{cases} |x_1| + \cdots + |x_r| + 2u_1 + \cdots + 2u_s < t, \\ 0 \le u_j, \quad j = 1, \dots, s, \\ 0 \le \theta_j \le 2\pi, \quad j = 1, \dots, s \end{cases}$$

代 $2u_j = w_j$，得：

$$I(t) = 2^r 4^{-s}(2\pi)^s I_{r,s}(t)$$

其中：

$$I_{r,s}(t) = \int w_1 \cdots w_s dx_1 \cdots dx_r dw_1 \cdots dw_s$$

积分域为：

$$\begin{cases} x_1 + \cdots + x_r + w_1 + \cdots + w_s < t, \\ 0 \le x_i, \quad i = 1, \dots, r, \\ 0 \le w_j, \quad j = 1, \dots, s \end{cases}$$

显然 $I_{r,s}(t)=t^nI_{r,s}(1)$。由傅比尼定理：

$$\begin{aligned}I_{r,s}(1)&=\int_0^1 I_{r-1,s}(1-x_1)dx_1\\&=\int_0^1(1-x_1)^{n-1}I_{r-1,s}(1)dx_1\\&=\frac{1}{n}I_{r-1,s}(1)\end{aligned}$$

归纳得：

$$I_{r,s}(1)=\frac{1}{n(n-1)\cdots(n-r+1)}I_{0,s}(1)$$

类似地：

$$I_{0,s}(1)=\int_0^1 w_1(1-w_1)^{2s-2}I_{0,s-1}(1)dw_1=\frac{1}{2s(2s-1)}I_{0,s-1}(1)$$

故：

$$I_{0,s}(1)=\frac{1}{(2s)!}I_{0,0}(1)=\frac{1}{(2s)!}$$

因此 $I_{r,s}(1)=\frac{1}{n!}$，有：

$$\operatorname{vol}(X)=2^s\operatorname{vol}(f(X))=2^s\cdot 2^r\cdot 4^{-s}\cdot(2\pi)^s\cdot t^n\cdot I_{r,s}(1)=\frac{2^r\pi^st^n}{n!}$$

3 **问题：** 证明在 K 的整数环 $\mathcal{O}_K$ 的每个非零理想 $\mathfrak{a}$ 中，存在非零 a 满足：

$$|N_{K|\mathbb{Q}}(a)|\le M(\mathcal{O}_K:\mathfrak{a}),$$

其中 $M=\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s\sqrt{|d_K|}$（即所谓的闵可夫斯基界）。
解答： 考虑紧的、凸的、中心对称集合：

$$X=\left\{(z_\tau)\in K_{\mathbb{R}}\mid\sum_\tau|z_\tau|\le n\left(M(\mathcal{O}_K:\mathfrak{a})\right)^{1/n}\right\}$$

其体积为：

$$\operatorname{vol}(X)=\frac{2^r\pi^s}{n!}\cdot n^n\cdot\left(\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s\sqrt{|d_K|}\right)\cdot(\mathcal{O}_K:\mathfrak{a})=2^n\operatorname{vol}(\Gamma)$$

由练习 4.2，X 含 $\Gamma=j\mathfrak{a}$ 的非零元素，故存在 $\mathfrak{a}$ 中的非零 a 满足：

$$\begin{aligned}|N_{K|\mathbb{Q}}(a)|&=\prod_\tau|\tau(a)|\\&\le\left(\frac{1}{n}\sum_\tau|\tau(a)|\right)^n\\&\le M(\mathcal{O}_K:\mathfrak{a})\end{aligned}$$