清华大学 2025-2026 秋季学期，群与 Galois 理论，作业 5

请用 A4 大小的纸张**正反面**用钢笔，签字笔或者圆珠笔书写，并注明自己的姓名、年级（书院或系）和作业的**总页数**。除定理公式所涉及的人名之外，请使用**中文**。本次作业请扫描并上传至网络学堂，具体截止日期请查阅网络学堂，逾期视作零分。

A. 分式域的推广：局部化

在此问题中，字母 A 表示是某个给定的交换环，

A1) 给定子集 $S \subset A$，如果

- $1 \in S$;
- 对任意的 $s_1, s_2 \in S$，有 $s_1 \cdot s_2 \in S$。

我们就称 S 是**乘性子集**。证明，以下两个集合是乘性子集：$\{1, f, f^2, \cdots\}$，其中，$f \in A$；$A - \mathfrak{p}$，其中，$\mathfrak{p}$ 是素理想（特别的，如果 A 是整环，$A - \{0\}$ 是乘性子集）。

A2) 我们在 $A \times S$ 上定义等价关系：$(a, s) \sim (a', s')$ 指的是存在 $t \in S$，使得 $as' \cdot t = a's \cdot t$。证明，以上给出了 $A \times S$ 上的一个等价关系。

令 $A_S = {}^{A \times S}\!/\!_{\sim}$，我们用 $\frac{a}{s}$ 表示 (a, s) 所在的等价类。证明，对任意的 $s' \in S$，我们有 $\frac{s'a}{s's} = \frac{a}{s}$。

A3) 我们在 A_S 上定义如下的加法和乘法：

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

通过验证以上是良定义的来证明，A_S 在以上运算下成为一个环并指出它的乘法和加法单位元。进一步，我们还有自然的环同态：

$$\iota : A \to A_S, \ a \mapsto \frac{a}{1}.$$

我们把 A_S 称作是 A 对乘性子集 S 的**局部化**。

A4) 令 $S_0 = \{a \in A \mid ab = 0 \Leftrightarrow b = 0\}$。证明，$S_0$ 是乘性子集。我们称 A_{S_0} 为 A 的**全分式环**。进一步证明 $\iota : A \to A_{S_0}$ 是单射并且此时 $\frac{a}{s} = \frac{a'}{s'}$ 当且仅当 $as' = a's$。

A5) 给定乘性子集 $S \subset A$。证明，$\mathrm{Ker}(\iota) = \{a \in A | \text{存在 } s \in S, \text{ 使得} as = 0\}$。进一步证明，$\iota$ 为单射当且仅当 $S \subset S_0$。

A6)（局部化的泛性质）A, S, A_S 和 $\iota : A \to A_S$ 如上述。试验证，$\iota(S) \subset (A_S)^\times$。

$$\begin{tikzcd}
A \arrow[r, "\varphi"] \arrow[d, "\iota"] & B \\
A_S \arrow[ur, dashed, "\psi"'] &
\end{tikzcd}$$

证明，对任意的环 B 和环同态 $\varphi : A \to B$，如果 $\varphi(S) \subset B^\times$，则存在唯一的环同态 $\psi : A_S \to B$，使得 $\psi \circ \iota = \varphi$。

A7) A, S, A_S 和 $\iota: A \to A_S$ 如上述，$\widehat{S} = \{a \in A | \text{存在 } b \in A,\ \text{使得 } ab \in S\}$。证明，$\widehat{S} = \iota^{-1}\left((A_S)^\times\right)$。进一步证明环同构 $A_S \xrightarrow{\simeq} A_{\widehat{S}}$，其中，$\frac{a}{1}$ 的像是 $\frac{a}{1}$。

A8) A 和 B 是交换环，$\varphi: A \to B$ 是环同态，$S \subset A$ 和 $T \subset B$ 是乘性子集并且 $\varphi(S) \subset T$。证明，存在唯一的环同态 $\psi: A_S \to B_T$，使得如下图表交换[1]：

$$\begin{tikzcd} A \arrow[r, "\varphi"] \arrow[d, "\iota"] & B \arrow[d, "\iota"] \\ A_S \arrow[r, dashed, "\psi"] & B_T \end{tikzcd}$$

A9)（理想与局部化）$I \subset A$ 是理想，令 I_S 为 $\iota(I)$ 在 A_S 中生成的理想。

- 证明，$I_S = \{\frac{a}{s} | a \in I, s \in S\}$。进一步证明，$I_S = A_S$ 当且仅当 $S \cap I \neq \emptyset$。
- $J \subset A_S$ 是理想，证明，$\left(\iota^{-1}(J)\right)_S = J$。

A10)（素理想与局部化）我们证明 A_S 中的素理想与 A 中与 S 不交的素理想一一对应。

- $\mathfrak{p} \subset A$ 是素理想并且 $\mathfrak{p} \cap S = \emptyset$，证明，$\mathfrak{p}_S$ 为 A_S 中的素理想。
- $\mathfrak{q} \subset A_S$ 是素理想，证明，$\iota^{-1}\mathfrak{q}$ 是 A 中唯一满足 $\mathfrak{p}_S = \mathfrak{q}$ 的素理想。

A11) $\mathfrak{p} \subset A$ 是素理想，$S = A - \mathfrak{p}$，令 $A_{\mathfrak{p}} = A_S$。证明，$A_{\mathfrak{p}}$ 是局部环（即只有一个极大理想的环）并确定它的极大理想。

A12)（局部化与商可交换）$I \subset A$ 是理想，$S \subset A$ 是乘性子集，$\pi: A \to A/I$ 是商映射，$\pi(S) \subset A/I$ 也是乘性子集。证明，存在自然的环同构

$$\left(A/I\right)_{\pi(S)} \xrightarrow{\simeq} A_S/I_S.$$

A13) 给定 $f \in A$，$S = \{1, f, f^2, \cdots\}$，记 $A_f = A_S$。证明，我们有环同构

$$A[X]/(1 - fX) \xrightarrow{\simeq} A_f,\quad X \mapsto \frac{1}{f}.$$

B. $\mathbb{Z}\left[\sqrt{d}\right]^\times$ 与 Pell 方程，$d \neq \square, d > 0$

假设 $d \in \mathbb{Z}$ 不是完全平方数。令

$$\mathbb{Z}\left[\sqrt{d}\right] = \{x + y\sqrt{d} | x, y \in \mathbb{Z}\},\quad \mathbb{Q}\left[\sqrt{d}\right] = \{x + y\sqrt{d} | x, y \in \mathbb{Q}\}.$$

B1) 证明，$\mathbb{Z}\left[\sqrt{d}\right]$ 是环而 $\mathbb{Q}\left[\sqrt{d}\right]$ 为其分式域。

B2) 证明，如果 $d < 0$，$\mathbb{Z}\left[\sqrt{d}\right]$ 是 $\mathbb{C}$ 中的格点（从而是离散的）；如果 $d > 0$，$\mathbb{Z}\left[\sqrt{d}\right]$ 在 $\mathbb{R}$ 中稠密。

B3) 对任意的 $z = x + y\sqrt{d} \in \mathbb{Q}\left[\sqrt{d}\right]$，我们定义 $\overline{z} = x - y\sqrt{d}$（请注意，如果 $d > 0$，这不是复共轭）。证明，环 $\mathbb{Z}\left[\sqrt{d}\right]$ 的自同构群 $\mathbf{Aut}(\mathbb{Z}\left[\sqrt{d}\right])$ 恰有 2 个元素。

B4) 对任意的 $z \in \mathbb{Q}\left[\sqrt{d}\right]$，我们定义 $N(z) = z \cdot \overline{z}$。证明，对任意的 $a, b \in \mathbb{Q}\left[\sqrt{d}\right]$，$N(a \cdot b) = N(a) \cdot N(b)$ 并且 $N(\mathbb{Z}\left[\sqrt{d}\right]) \subset \mathbb{Z}$。据此证明：$\mathbb{Z}\left[\sqrt{d}\right]^\times = \left\{z \in \mathbb{Z}\left[\sqrt{d}\right] \middle| N(z) = \pm 1\right\}$。

[1] 请查阅图表交换的含义

B5) 对于 $d<0$，试计算 $\mathbb{Z}\left[\sqrt{d}\right]^{\times}$。

当 $d>0$ 时，$\mathbb{Z}\left[\sqrt{d}\right]^{\times}$ 的结构要复杂的多。实际上，

$$N(z=x+y\sqrt{d})=\pm 1 \quad \Leftrightarrow \quad x^2-dy^2=\pm 1.$$

上述方程通常被称作是 Pell 方程。研究 $\mathbb{Z}\left[\sqrt{d}\right]^{\times}$ 可以给出以上方程所有的整数解。

B6) 证明，$\mathbb{Z}\left[\sqrt{2}\right]^{\times}\cap(1,3)=\{1+\sqrt{2}\}$。

B7) 证明，$\mathbb{Z}\left[\sqrt{2}\right]^{\times}=\{\pm\left(1+\sqrt{2}\right)^k | k\in\mathbb{Z}\}$ 并给出群同构 $\mathbb{Z}\left[\sqrt{2}\right]^{\times}\simeq\mathbb{Z}\times{}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$。

B8) 如何刻画 Pell 方程 $x^2-2y^2=1$ 和 $x^2-2y^2=-1$ 的所有整数解?

以下假设 $d>0$。

B9) 证明，有序列 $\{z_n\}_{n\geqslant 1}\subset\mathbb{Z}\left[\sqrt{d}\right]-\{0\}$，使得 $\lim\limits_{n\to\infty}z_n=0$ 而 $\{N(z_n)\}_{n\geqslant 1}$ 是有界的。
（提示: 使用 Dirichlet 引理: 对任意 $\alpha\in\mathbb{R}$ 和正整数 M，存在整数 p 和正整数 $q\leqslant M$，使得 $|p-q\alpha|<\frac{1}{M}$。这个引理可以用抽屉原理直接证明或者请从文献中查阅证明）

B10) 证明，存在上述序列的子序列 $\{w_n\}_{n\geqslant 1}$ 以及整数 k，使得对任意的 $n,m\geqslant 1$，我们有 $N(w_n)=k$ 并且 $w_n\overline{w}_m\in k\mathbb{Z}\left[\sqrt{d}\right]$。（提示：考虑 w_n 在 ${}^{\mathbb{Z}\left[\sqrt{d}\right]}\!/_{k\mathbb{Z}\left[\sqrt{d}\right]}$ 中的像）

B11) 证明，$\mathbb{Z}\left[\sqrt{d}\right]^{\times}$ 是无限集。

B12) 证明，$\mathbb{Z}\left[\sqrt{d}\right]^{\times}\cap(0,\infty)$ 是乘法群 $(0,\infty)$ 的离散子群，即对任意的 $0<a<b<\infty$，$\mathbb{Z}\left[\sqrt{d}\right]^{\times}\cap(a,b)$ 是有限的。

B13) 证明，存在 $\eta_d\in(1,\infty)$（被称作是**基本单位**），使得 η_d 生成了 $\mathbb{Z}\left[\sqrt{d}\right]^{\times}\cap(0,\infty)$。特别地，$\mathbb{Z}\left[\sqrt{d}\right]^{\times}\simeq\mathbb{Z}\times{}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$。
（注意到：对任意的 $u\in\mathbb{Z}\left[\sqrt{d}\right]^{\times}-\{\pm 1\}$，四个点 $\pm u,\pm\overline{u}$ 在区间 $(-\infty,-1),(-1,0),(0,1),(1,\infty)$ 中各有一个）

If one proves the equality of two numbers a and b by showing first that *a is less than or equal to b*and then *a is greater than or equal to b*, it is unfair, one should instead show that they are really equal by disclosing the inner ground for their equality.

——— Emmy Noether

练习题（不提交）

1. A 是环（未必交换）。证明，如果 $a \in A$ 是幂零元[2]，$b \in A^{\times}$ 并且 $ab = ba$，那么 $a + b$ 可逆；如果 $a, b \in A$ 是幂零元并且 $ab = ba$，那么 $a + b$ 是幂零元；

2. 证明，如果 $ab \in A$ 是幂零元，那么，ba 也是幂零元。据此，给出 $(1 - ab)^{-1}$ 与 $(1 - ba)^{-1}$ 之间的联系。据此证明，如果 $1 - ab \in A^{\times}$，那么，$1 - ba \in A^{\times}$。

3. A 是交换环，$\mathfrak{Nil}(A) = \{a \in A | \text{存在 } n \geqslant 1\text{，使得 } x^n = 0\}$，$\mathrm{Spec}(A)$ 是 A 的所有素理想的集合。证明，$\mathfrak{Nil}(A) = \bigcap\limits_{\mathfrak{p} \in \mathrm{Spec}(A)} \mathfrak{p}$。

4. A 是交换环，$\mathrm{SpecMax}(A)$ 是其极大理想的集合，其 **Jacobson 根式理想**被定义为 $J(A) = \bigcap\limits_{\mathfrak{m} \in \mathrm{SpecMax}(A)} \mathfrak{m}$。证明，$a \in J(A)$ 当且仅当对任意的 $b \in A$，$1 - ab \in A^{\times}$。

5. A 是环，I 是双边理想。那么，我们有如下的一一对应

$$\{A \text{ 的左理想 } J \supset I\} \xrightarrow{1:1} \{{}^{A}\!/\!_{I} \text{ 的左理想}\}, \quad J \mapsto {}^{J}\!/\!_{I}.$$

6. A 和 B 是交换环，$\varphi : A \to B$ 是环同态。证明，对任意的理想 $J \subset B$，$\varphi^{-1}(J) \subset A$ 是理想。

7. A 和 B 是交换环，$\varphi : A \to B$ 是环同态。证明，如果 $\mathfrak{q} \subset B$ 是素理想，$\varphi^{-1}(\mathfrak{q}) \subset A$ 也是素理想。进一步利用 $\mathbb{Z} \to \mathbb{Q}$ 的自然映射说明极大理想的逆像未必是极大的。

8. A 是（交换）环，$\mathfrak{p}_1, \cdots, \mathfrak{p}_n$ 是素理想，I 是理想。如果 $I \subset \bigcup_{i=1}^n \mathfrak{p}_i$，证明，存在 i_0，使得 $I \subset \mathfrak{p}_{i_0}$。

9. A 是（交换）环，$I_1, \cdots, I_n$ 是素理想，$\mathfrak{p}$ 是素理想。如果 $\bigcap_{i=1}^n I_i \subset \mathfrak{p}$，证明，存在 i_0，使得 $I_{i_0} \subset \mathfrak{p}$。特别地，如果 $\bigcap_{i=1}^n I_i = \mathfrak{p}$，那么，存在 i_0，使得 $I_{i_0} = \mathfrak{p}$。

10. A 是环，I 和 J 是理想并且 I 与 J 互素（即 $I + J = A$）。证明，对任意的 $n \geqslant 1$，I^n 与 J^n 互素。

11. A 是环（未必交换），子集 $S \subset A$ 的中心化子 $\mathbf{Z}_S(A)$ 是 A 中在乘法意义下与 S 中所有元素均交换的元素的集合。证明，$\mathbf{Z}_S(A)$ 是 A 子环。

12. K 是域，$A = K[X]$ 是 K 上的多项式环，V 是 K-线性空间。给定线性映射 $T \in \mathrm{End}_K(V)$ 可以给出 V 上的一个 $K[X]$-模的结构：

$$K[X] \times V \to V, \quad (P(X), v) \mapsto P(T)v.$$

证明，V 上的每一个 $K[X]$-模的结构都恰好有某个 $T \in \mathrm{End}_K(V)$ 唯一决定。

---

[2] 即存在 $n \geqslant 1$，使得 $a^n = 0$