群与 Galois 理论
作业 5

陈宏泰

2024011131

清华大学数学科学系

cht24@mails.tsinghua.edu.cn

2025 年 11 月 29 日

目录

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) .

证明：设 $S_1=\{1,f,f^2,\cdots\}$, 则 $1\in S_1$ 显然成立. 对于任意的 $s_1,s_2\in S_1$, 存在非负整数 m,n, 使得 $s_1=f^m,s_2=f^n$. 因此, $s_1\cdot s_2=f^{m+n}\in S_1$. 所以, S_1 是乘性子集.

设 $S_2=A-\mathfrak{p}$, 则 $1\in S_2$ 显然成立, 否则 $\mathfrak{p}=A$, 这与 $\mathfrak{p}$ 为素理想矛盾. 对于任意的 $s_1,s_2\in S_2$, 如果 $s_1\cdot s_2\notin S_2$, 则 $s_1\cdot s_2\in\mathfrak{p}$. 由于 $\mathfrak{p}$ 是素理想, 所以 $s_1\in\mathfrak{p}$ 或 $s_2\in\mathfrak{p}$, 这与 $s_1,s_2\in S_2$ 矛盾. 因此, $s_1\cdot s_2\in S_2$. 所以, S_2 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 $\frac{s'a}{s's}=\frac{a}{s}$.

证明：设 $(a,s),(a',s'),(a'',s'')\in A\times S$.

(自反性) 取 $t=1\in S$, 则 $as\cdot t=as\cdot t$, 所以 $(a,s)\sim(a,s)$.

(对称性) 如果 $(a,s)\sim(a',s')$, 则存在 $t\in S$, 使得 $as'\cdot t=a's\cdot t$. 自然有 $a's\cdot t=as'\cdot t$, 因此, $(a',s')\sim(a,s)$.

(传递性) 如果 $(a,s)\sim(a',s')$ 且 $(a',s')\sim(a'',s'')$, 则存在 $t_1,t_2\in S$, 使得 $as'\cdot t_1=a's\cdot t_1$ 且 $a's''\cdot t_2=a''s'\cdot t_2$. 对前式两边同乘 $s''\cdot t_2$, 对后式两边同乘 $s\cdot t_1$, 由 A 为交换环有

$$as's''\cdot(t_1t_2)=a'ss''\cdot(t_1t_2),\quad a's''s\cdot(t_1t_2)=a''s's\cdot(t_1t_2).$$

从而有

$$as''\cdot(s't_1t_2)=a'ss''\cdot(t_1t_2)=a's''s\cdot(t_1t_2)=a''s\cdot(s't_1t_2)$$

由 S 为乘性子群, 知 $s't_1t_2\in S$, 从而有 $(a,s)\sim(a'',s'')$.

综上, $\sim$ 是 $A\times S$ 上的等价关系.

下面证明对于任意的 $s'\in S$, 有 $\frac{s'a}{s's}=\frac{a}{s}$. 只需证明 $(s'a,s's)\sim(a,s)$ 即可. 对于任意的 $s'\in S$,

$$(s'a)s\cdot 1=s'as=as's\cdot 1,$$

$1\in S$, 所以 $(s'a,s's)\sim(a,s)$. □

注: 要求 $s'\in S$ 是保证 $s's\in S$. 因此就算 $s'\notin S$, 但只要 $s's\in S$ 也能保证有 $(s'a,s's)\sim(a,s)$.
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**.

证明: 设 $\frac{a}{s}=\frac{a'}{s'}$ 且 $\frac{b}{t}=\frac{b'}{t'}$.

(加法良定义) 则存在 $t_1,t_2\in S$, 使得 $as'\cdot t_1=a's\cdot t_1$ 且 $bt'\cdot t_2=b't\cdot t_2$. 对前式两边同乘 $tt't_2$, 后式两边同乘 $ss't_1$, 得

$$ats't'\cdot(t_1t_2)=a't'st\cdot(t_1t_2),\quad bts't'\cdot(t_1t_2)=b's'st\cdot(t_1t_2).$$

将这两式相加, 即有

$$(at+bs)s't'\cdot(t_1t_2)=(a't'+b's')st\cdot(t_1t_2).$$

又由 S 为乘性子集, 知 $t_1t_2\in S$. 因此, $(at+bs,st)\sim(a't'+b's',s't')$ 说明 $\frac{at+bs}{st}=\frac{a't'+b's'}{s't'}$, 从而加法良定义.

(乘法良定义) 则存在 $t_1,t_2\in S$, 使得 $as'\cdot t_1=a's\cdot t_1$ 且 $bt'\cdot t_2=b't\cdot t_2$. 将上面两式相乘, 有

$$abs't'\cdot(t_1t_2)=a'b'st\cdot(t_1t_2).$$

又由 S 为乘性子集, 知 $t_1t_2\in S$. 因此, $(ab,st)\sim(a'b',s't')$ 说明 $\frac{ab}{st}=\frac{a'b'}{s't'}$, 从而乘法良定义.

综上, A_S 在以上运算下良定义. 下面验证环的公理.

(加法交换律) 对于任意的 $\frac{a}{s},\frac{b}{t}\in A_S$, 有

$$\frac{a}{s}+\frac{b}{t}=\frac{at+bs}{st}=\frac{bs+at}{ts}=\frac{b}{t}+\frac{a}{s}.$$

(加法结合律) 对于任意的 $\frac{a}{s},\frac{b}{t},\frac{c}{u}\in A_S$, 有

$$(\frac{a}{s}+\frac{b}{t})+\frac{c}{u}=\frac{(at+bs)u+cst}{stu}=\frac{aut+bus+cst}{stu}=\frac{a}{s}+(\frac{b}{t}+\frac{c}{u}).$$

(加法单位元) 对于任意的 $\frac{a}{s}\in A_S$, 有

$$\frac{a}{s}+\frac{0}{1}=\frac{a\cdot 1+0\cdot s}{s\cdot 1}=\frac{a}{s}.$$

(加法逆元) 对于任意的 $\frac{a}{s}\in A_S$, 有

$$\frac{a}{s}+\frac{-a}{s}=\frac{as-as}{ss}=\frac{0}{1}.$$

(乘法交换律) 对于任意的 $\frac{a}{s}, \frac{b}{t} \in A_S$, 有

$$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st} = \frac{ba}{ts} = \frac{b}{t} \cdot \frac{a}{s}.$$

(乘法结合律) 对于任意的 $\frac{a}{s}, \frac{b}{t}, \frac{c}{u} \in A_S$, 有

$$(\frac{a}{s} \cdot \frac{b}{t}) \cdot \frac{c}{u} = \frac{ab}{st} \cdot \frac{c}{u} = \frac{abc}{stu} = \frac{a}{s} \cdot (\frac{b}{t} \cdot \frac{c}{u}).$$

(乘法单位元) 对于任意的 $\frac{a}{s} \in A_S$, 有

$$\frac{a}{s} \cdot \frac{1}{1} = \frac{a \cdot 1}{s \cdot 1} = \frac{a}{s}.$$

(分配律) 对于任意的 $\frac{a}{s}, \frac{b}{t}, \frac{c}{u} \in A_S$, 有

$$\frac{a}{s} \cdot (\frac{b}{t} + \frac{c}{u}) = \frac{a}{s} \cdot \frac{bu + ct}{tu} = \frac{a(bu + ct)}{stu} = \frac{abu}{stu} + \frac{act}{stu} = \frac{a}{s} \cdot \frac{b}{t} + \frac{a}{s} \cdot \frac{c}{u}.$$

综上, A_S 在以上运算下成为一个环. 加法单位元为 $\frac{0}{1}$, 乘法单位元为 $\frac{1}{1}$.

下面验证 $\iota : A \to A_S, a \mapsto \frac{a}{1}$ 为环同态. 对于任意的 $a, b \in A$, 有

$$\iota(a + b) = \frac{a + b}{1} = \frac{a \cdot 1 + b \cdot 1}{1 \cdot 1} = \frac{a}{1} + \frac{b}{1} = \iota(a) + \iota(b),$$

$$\iota(ab) = \frac{ab}{1} = \frac{a \cdot b}{1 \cdot 1} = \frac{a}{1} \cdot \frac{b}{1} = \iota(a) \cdot \iota(b).$$

因此, ι 为环同态. □

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 $as' = a's$.

证明: 设 $S_0 = \{a \in A \mid ab = 0 \Leftrightarrow b = 0\}$.

(乘性子集) 显然 $1 \in S_0$. 对于任意的 $s_1, s_2 \in S_0$, 如果 $s_1 s_2 b = 0$, 则 $s_1(s_2 b) = 0$. 由于 $s_1 \in S_0$, 所以 $s_2 b = 0$. 又由于 $s_2 \in S_0$, 所以 $b = 0$. 因此, $s_1 s_2 \in S_0$. 所以, S_0 是乘性子集.

(单射) 设 $\iota(a) = \iota(a')$, 则 $\frac{a}{1} = \frac{a'}{1}$. 根据等价关系的定义, 存在 $t \in S_0$, 使得 $a \cdot 1 \cdot t = a' \cdot 1 \cdot t$, 即 $at = a't$. 因为 $t \in S_0$, 所以 $a = a'$. 因此, ι 为单射.

(充要条件) 如果 $\frac{a}{s} = \frac{a'}{s'}$, 则存在 $t \in S_0$, 使得 $as' \cdot t = a's \cdot t$. 因为 $t \in S_0$, 所以 $as' = a's$. 反之, 如果 $as' = a's$, 则对于任意的 $t \in S_0$, 有 $as' \cdot t = a's \cdot t$. 因此, $\frac{a}{s} = \frac{a'}{s'}$.

综上, $\iota : A \to A_{S_0}$ 是单射并且 $\frac{a}{s} = \frac{a'}{s'}$ 当且仅当 $as' = a's$. □

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

证明: 设 $K = \{a \in A \mid$ 存在 $s \in S$, 使得 $as = 0\}$.

($\mathrm{Ker}(\iota)$ 的刻画) 如果 $a \in \mathrm{Ker}(\iota)$, 则 $\iota(a) = \frac{a}{1} = \frac{0}{1}$. 根据等价关系的定义, 存在 $t \in S$, 使得 $a \cdot 1 \cdot t = 0 \cdot 1 \cdot t$, 即 $at = 0$. 因此, $a \in K$. 反之, 如果 $a \in K$, 则存在 $s \in S$, 使得 $as = 0$.

对于任意的 $t \in S$, 有 $as \cdot t = 0 \cdot t$, 即 $a \cdot 1 \cdot (st) = 0 \cdot 1 \cdot (st)$. 因为 $st \in S$, 所以 $\frac{a}{1} = \frac{0}{1}$, 即 $a \in \mathrm{Ker}(\iota)$. 因此, $\mathrm{Ker}(\iota) = K$.

(单射条件) 如果 ι 为单射, 则 $\mathrm{Ker}(\iota) = \{0\}$. 根据上面的等式, 对于任意的 $s \in S$, 如果 $as = 0$, 则 $a = 0$. 因此, $s \in S_0$. 所以, $S \subset S_0$. 反之, 如果 $S \subset S_0$, 则对于任意的 $a \in \mathrm{Ker}(\iota)$, 存在 $s \in S$, 使得 $as = 0$. 因为 $s \in S_0$, 所以 $a = 0$. 因此, $\mathrm{Ker}(\iota) = \{0\}$, 即 ι 为单射.

综上, $\mathrm{Ker}(\iota) = \{a \in A \mid 存在\ s \in S\ , 使得\ as = 0\}$ 并且 ι 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 $\psi \circ \iota = \varphi$.

证明: (包含关系) 对于任意的 $s \in S$, 有

$$\iota(s) = \frac{s}{1}.$$

设 $\frac{1}{s}$ 为 $\frac{s}{1}$ 的乘法逆元, 则有

$$\frac{s}{1} \cdot \frac{1}{s} = \frac{s \cdot 1}{1 \cdot s} = \frac{1}{1}.$$

因此, $\iota(s) \in (A_S)^\times$. 所以, $\iota(S) \subset (A_S)^\times$.

(存在性) 定义映射 $\psi : A_S \to B$, 对于任意的 $\frac{a}{s} \in A_S$, 令

$$\psi(\frac{a}{s}) = \varphi(a) \cdot \varphi(s)^{-1}.$$

下面验证 ψ 为环同态且 $\psi \circ \iota = \varphi$.

(良定义) 如果 $\frac{a}{s} = \frac{a'}{s'}$, 则存在 $t \in S$, 使得 $as' \cdot t = a's \cdot t$. 应用 φ, 有

$$\varphi(a)\varphi(s')\varphi(t) = \varphi(a')\varphi(s)\varphi(t).$$

由于 $\varphi(t), \varphi(s), \varphi(s') \in B^\times$, 所以

$$\psi(\frac{a}{s}) = \varphi(a)\varphi(s)^{-1} = \varphi(a')\varphi(s)^{-1} = \psi(\frac{a'}{s'}).$$

因此, ψ 良定义.

(环同态) 对于任意的 $\frac{a}{s}, \frac{b}{t} \in A_S$, 有

$$\begin{aligned} \psi(\frac{a}{s} + \frac{b}{t}) &= \psi(\frac{at + bs}{st}) = \varphi(at + bs) \cdot \varphi(st)^{-1} \\ &= (\varphi(a)\varphi(t) + \varphi(b)\varphi(s)) \cdot (\varphi(s)\varphi(t))^{-1} \\ &= \varphi(a)\varphi(s)^{-1} + \varphi(b)\varphi(t)^{-1} = \psi(\frac{a}{s}) + \psi(\frac{b}{t}), \end{aligned}$$

$$\begin{aligned}\psi(\frac{a}{s}\cdot\frac{b}{t}) &= \psi(\frac{ab}{st}) = \varphi(ab)\cdot\varphi(st)^{-1}\\ &= (\varphi(a)\varphi(b))\cdot(\varphi(s)\varphi(t))^{-1}\\ &= \varphi(a)\varphi(s)^{-1}\cdot\varphi(b)\varphi(t)^{-1} = \psi(\frac{a}{s})\cdot\psi(\frac{b}{t}).\end{aligned}$$

因此, ψ 为环同态.

对于任意的 $a\in A$, 有

$$\psi(\iota(a)) = \psi(\frac{a}{1}) = \varphi(a)\cdot\varphi(1)^{-1} = \varphi(a)\cdot 1 = \varphi(a).$$

因此, $\psi\circ\iota = \varphi$.

(唯一性) 如果存在环同态 $\psi' : A_S \to B$, 使得 $\psi'\circ\iota = \varphi$, 则对于任意的 $\frac{a}{s}\in A_S$, 有

$$\psi'(\frac{a}{s}) = \psi'(\iota(a)\cdot\iota(s)^{-1}) = \psi'(\iota(a))\cdot\psi'(\iota(s))^{-1} = \varphi(a)\cdot\varphi(s)^{-1} = \psi(\frac{a}{s}).$$

因此, $\psi' = \psi$. □

A7) A, S, A_S 和 $\iota : A \to A_S$ 如上述, $\widehat{S} = \{a \in A \mid$ 存在 $b\in A$, 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 $\frac{a}{1}$.

证明： 设 $\widehat{S} = \{a\in A \mid$ 存在 $b\in A$, 使得 $ab\in S\}$.

($\widehat{S}$ 的刻画) 如果 $a\in\widehat{S}$, 则存在 $b\in A$, 使得 $ab\in S$. 设 $\iota(a) = \frac{a}{1}$, 则

$$\iota(a)\cdot\iota(b) = \frac{a}{1}\cdot\frac{b}{1} = \frac{ab}{1}.$$

因为 $ab\in S$, 所以 $\frac{ab}{1}\in(A_S)^\times$. 因此,

$$\frac{1}{a}\cdot(\frac{1}{b}(\frac{1}{ab})^{-1}) = \frac{1}{1},$$

所以 $\iota(a)\in(A_S)^\times$, 即 $a\in\iota^{-1}((A_S)^\times)$. 反之, 如果 $a\in\iota^{-1}((A_S)^\times)$, 则 $\iota(a) = \frac{a}{1}\in(A_S)^\times$. 设 $\frac{c}{d}$ 为 $\frac{a}{1}$ 的乘法逆元, 则有

$$\frac{a}{1}\cdot\frac{c}{d} = \frac{ac}{d} = \frac{1}{1}.$$

根据等价关系的定义, 存在 $t\in S$, 使得 $ac\cdot t = d\cdot t$. 因为 S 为乘性子集, 所以 $dt\in S$. 因此, $a(ct) = dt\in S$, 即 $a\in\widehat{S}$. 综上, $\widehat{S} = \iota^{-1}((A_S)^\times)$.

再证明环同构 $A_S \xrightarrow{\simeq} A_{\widehat{S}}$. 定义映射 $\phi : A_S \to A_{\widehat{S}}$, 对于任意的 $\frac{a}{s}\in A_S$, 令

$$\phi(\frac{a}{s}) = \frac{a}{s},$$

其中右边的分式表示在 $A_{\widehat{S}}$ 中. 下面验证 ϕ 为环同构.

(良定义) 如果 $\frac{a}{s} = \frac{a'}{s'}$, 则存在 $t\in S$, 使得 $as'\cdot t = a's\cdot t$. 因为 $S\subset\widehat{S}$, 所以 $t\in\widehat{S}$. 因此, $(a,s)\sim(a',s')$ 在 $A_{\widehat{S}}$ 中亦成立, 即 $\frac{a}{s} = \frac{a'}{s'}$ 在 $A_{\widehat{S}}$ 中成立. 所以, ϕ 良定义.

(环同态) 对于任意的 $\frac{a}{s}, \frac{b}{t} \in A_S$, 有

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

因此, ϕ 为环同态.

(双射性) 如果 $\phi(\frac{a}{s})=\phi(\frac{a'}{s'})$, 则 $\frac{a}{s}=\frac{a'}{s'}$ 在 $A_{\widehat{S}}$ 中成立. 根据等价关系的定义, 存在 $t\in\widehat{S}$, 使得 $as'\cdot t=a's\cdot t$. 由 $t\in\widehat{S}$, 存在 $c\in A$, 使得 $tc\in S$. 因此, $as'\cdot(tc)=a's\cdot(tc)$, 即 $(as',ss')\sim(a's',ss')$ 在 A_S 中成立, 即 $\frac{a}{s}=\frac{a'}{s'}$ 在 A_S 中成立. 所以, ϕ 为单射. 对于任意的 $\frac{a}{s}\in A_{\widehat{S}}$, 因为 $s\in\widehat{S}$, 存在 $c\in A$, 使得 $sc\in S$. 因此, 有

$$\phi(\frac{ac}{sc})=\frac{ac}{sc}=\frac{a}{s}.$$

所以, ϕ 为满射. 综上, ϕ 为环同构. □

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:

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

证明: 设 A,B,S,T,φ 如题设. 定义映射 $\psi: A_S\to B_T$, 对于任意的 $\frac{a}{s}\in A_S$, 令

$$\psi(\frac{a}{s})=\frac{\varphi(a)}{\varphi(s)}.$$

下面验证 ψ 为环同态且图表交换.

(良定义) 如果 $\frac{a}{s}=\frac{a'}{s'}$, 则存在 $t\in S$, 使得 $as'\cdot t=a's\cdot t$. 应用 φ, 有

$$\varphi(a)\varphi(s')\varphi(t)=\varphi(a')\varphi(s)\varphi(t).$$

由于 $\varphi(t)\in T$, 所以

$$\psi(\frac{a}{s})=\frac{\varphi(a)}{\varphi(s)}=\frac{\varphi(a')}{\varphi(s')}=\psi(\frac{a'}{s'}).$$

因此, ψ 良定义.

(环同态) 对于任意的 $\frac{a}{s}, \frac{b}{t} \in A_S$, 有

$$\begin{aligned}\psi(\frac{a}{s}+\frac{b}{t})&=\psi(\frac{at+bs}{st})=\frac{\varphi(at+bs)}{\varphi(st)}\\&=\frac{\varphi(a)\varphi(t)+\varphi(b)\varphi(s)}{\varphi(s)\varphi(t)}\\&=\frac{\varphi(a)}{\varphi(s)}+\frac{\varphi(b)}{\varphi(t)}=\psi(\frac{a}{s})+\psi(\frac{b}{t}),\end{aligned}$$

$$\begin{aligned}\psi(\frac{a}{s}\cdot\frac{b}{t})=\psi(\frac{ab}{st})&=\frac{\varphi(ab)}{\varphi(st)}\\&=\frac{\varphi(a)\varphi(b)}{\varphi(s)\varphi(t)}\\&=\frac{\varphi(a)}{\varphi(s)}\cdot\frac{\varphi(b)}{\varphi(t)}=\psi(\frac{a}{s})\cdot\psi(\frac{b}{t}).\end{aligned}$$

因此, ψ 为环同态. 对于任意的 $a\in A$, 有

$$\psi(\iota_A(a))=\psi(\frac{a}{1})=\frac{\varphi(a)}{\varphi(1)}=\frac{\varphi(a)}{1}=\iota_B(\varphi(a)).$$

因此, 图表交换. □

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,$I_S=\left\{\frac{a}{s}\middle|\ a\in I,s\in S\right\}$. 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, $(\iota^{-1}(J))_S=J$.

证明: 设 $I\subset A$ 为理想, I_S 为 $\iota(I)$ 在 A_S 中生成的理想.

(理想的刻画) 设 $K=\{\frac{a}{s}\mid a\in I,s\in S\}$.

先证明 $I_S\subset K$. 对于任意的 $a\in I$, 有 $\iota(a)=\frac{a}{1}\in I_S$. 对于任意的 $\frac{b}{t}\in A_S$, 有

$$\frac{b}{t}\cdot\frac{a}{1}=\frac{ba}{t}.$$

因为 I 为理想, 所以 $ba\in I$. 因此, $\frac{ba}{t}\in K$. 由理想的定义, 知 $I_S\subset K$.

再证明 $K\subset I_S$. 对于任意的 $\frac{a}{s}\in K$, 有 $a\in I$. 因为 $\iota(a)=\frac{a}{1}\in I_S$, 所以

$$\frac{a}{s}=\frac{a}{1}\cdot\frac{1}{s}\in I_S.$$

因此, $K\subset I_S$.

综上, $I_S=K=\{\frac{a}{s}\mid a\in I,s\in S\}$.

进一步证明, $I_S=A_S$ 当且仅当 $S\cap I\neq\emptyset$.

如果 $I_S=A_S$, 则 $1_{A_S}=\frac{1}{1}\in I_S$. 根据上面的等式, 存在 $a\in I$, $s\in S$, 使得 $\frac{a}{s}=\frac{1}{1}$. 根据等价关系的定义, 存在 $t\in S$, 使得 $a\cdot 1\cdot t=1\cdot s\cdot t$, 即 $at=st$. 因为 $t,s\in S$, 所以 $st\in S$. 由因为 $a\in I$, 所以 $at\in I$. 因此, $at=st\in S\cap I$. 反之, 如果 $S\cap I\neq\emptyset$, 则存在 $s\in S\cap I$. 对于任意的 $\frac{a}{t}\in A_S$, 有

$$\frac{a}{t}=\frac{as}{ts}.$$

因为 $s\in I$, 所以 $as\in I$. 因此, $\frac{as}{ts}\in I_S$. 所以, $A_S\subset I_S$. 由理想的定义, 知 $I_S\subset A_S$, 从而 $I_S=A_S$.

综上, $I_S=A_S$ 当且仅当 $S\cap I\neq\emptyset$.

设 $J \subset A_S$ 为理想. 下面证明 $(\iota^{-1}(J))_S = J$.

先证明 $(\iota^{-1}(J))_S \subset J$. 对于任意的 $\frac{a}{s} \in (\iota^{-1}(J))_S$, 有 $a \in \iota^{-1}(J)$, 即 $\iota(a) = \frac{a}{1} \in J$. 因为 J 为理想, 所以

$$\frac{a}{s} = \frac{a}{1} \cdot \frac{1}{s} \in J.$$

因此, $(\iota^{-1}(J))_S \subset J$.

再证明 $J \subset (\iota^{-1}(J))_S$. 对于任意的 $\frac{a}{s} \in J$, 有

$$\iota(a) = \frac{a}{1} = \frac{a}{s} \cdot \frac{s}{1} \in J,$$

即 $a \in \iota^{-1}(J)$. 因此,

$$\frac{a}{s} \in (\iota^{-1}(J))_S.$$

所以, $J \subset (\iota^{-1}(J))_S$

综上, $(\iota^{-1}(J))_S = J$. □

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.

证明：设 $\mathfrak{p} \subset A$ 为素理想且 $\mathfrak{p} \cap S = \emptyset$. 由 A9) 知, $\mathfrak{p}_S$ 为 $\iota(\mathfrak{p})$ 在 A_S 中生成的理想且 $\mathfrak{p}_S = \{\frac{a}{s} \mid a \in \mathfrak{p}, s \in S\}$, 下面证明 $\mathfrak{p}_S$ 为素理想.

对于任意的 $\frac{a}{s}, \frac{b}{t} \in A_S$, 如果 $\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st} \in \mathfrak{p}_S$, 则存在 $u \in S$, 使得 $ab \cdot u \in \mathfrak{p}$ ($\frac{ab}{st} = \frac{abu}{stu} \in \mathfrak{p}_S$). 因为 $\mathfrak{p}$ 为素理想, 并且 $u \notin \mathfrak{p}$ ($u \in S$ 且 $\mathfrak{p} \cap S = \emptyset$), 所以 $ab \in \mathfrak{p}$. 所以 $a \in \mathfrak{p}$ 或 $b \in \mathfrak{p}$. 因此, $\frac{a}{s} \in \mathfrak{p}_S$ 或 $\frac{b}{t} \in \mathfrak{p}_S$. 所以, $\mathfrak{p}_S$ 为素理想.

设 $\mathfrak{q} \subset A_S$ 为素理想. 下面证明 $\iota^{-1}(\mathfrak{q})$ 为 A 中唯一满足 $\mathfrak{p}_S = \mathfrak{q}$ 的素理想.

先证明 $\iota^{-1}(\mathfrak{q})$ 为素理想. 对于任意的 $a, b \in A$, 如果 $ab \in \iota^{-1}(\mathfrak{q})$, 则 $\iota(ab) = \frac{ab}{1} \in \mathfrak{q}$. 因为 $\mathfrak{q}$ 为素理想, 所以 $\frac{a}{1} \in \mathfrak{q}$ 或 $\frac{b}{1} \in \mathfrak{q}$. 因此, $a \in \iota^{-1}(\mathfrak{q})$ 或 $b \in \iota^{-1}(\mathfrak{q})$. 所以, $\iota^{-1}(\mathfrak{q})$ 为素理想.

再证明 $\mathfrak{p}_S = \mathfrak{q}$ 的唯一性. 如果存在素理想 $\mathfrak{p}' \subset A$, 使得 $\mathfrak{p}'_S = \mathfrak{q}$, 则对于任意的 $a \in \iota^{-1}(\mathfrak{q})$, 有 $\iota(a) = \frac{a}{1} \in \mathfrak{q} = \mathfrak{p}'_S$. 根据上面的等式, 存在 $s \in S$, 使得 $as \in \mathfrak{p}'$. 因为 $s \notin \mathfrak{p}'$（否则 $\mathfrak{p}'_S = A_S$）, 所以 $a \in \mathfrak{p}'$. 因此, $\iota^{-1}(\mathfrak{q}) \subset \mathfrak{p}'$. 对于任意的 $a \in \mathfrak{p}'$, 有 $\iota(a) = \frac{a}{1} \in \mathfrak{p}'_S = \mathfrak{q}$. 因此, $a \in \iota^{-1}(\mathfrak{q})$. 所以, $\mathfrak{p}' \subset \iota^{-1}(\mathfrak{q})$. 综上, $\iota^{-1}(\mathfrak{q}) = \mathfrak{p}'$.

综上, $\iota^{-1}(\mathfrak{q})$ 为 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.

证明：根据 A10), $A_{\mathfrak{p}}$ 中的素理想与 A 中与 S 不交的素理想一一对应. 因为 $S = A - \mathfrak{p}$, 所以与 S 不交的素理想只有 $\mathfrak{p}$ 一个. 因此, $A_{\mathfrak{p}}$ 中只有一个素理想, 即 $\mathfrak{p}_S$. 又极大理想都是素理想;

而对于 $A_\mathfrak{p}$ 中的任意理想 $I \neq A_\mathfrak{p}$, 存在极大理想 $\mathfrak{m} \neq A_\mathfrak{p}$ 使得 $I \subset \mathfrak{m}$. 由于 $A_\mathfrak{p}$ 中只有一个极大理想 $\mathfrak{p}_S$.

由此可知, $\mathfrak{p}_S$ 为 $A_\mathfrak{p}$ 的唯一极大理想. 所以, $A_\mathfrak{p}$ 为局部环. □

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

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

证明: 定义映射 $\phi : (A/I)_{\pi(S)} \to A_S/I_S$, 对于任意的 $\frac{a+I}{s+I} \in (A/I)_{\pi(S)}$, 令

$$\phi(\frac{a+I}{s+I}) = \frac{a}{s} + I_S.$$

下面验证 ϕ 为环同构.

(良定义) 如果 $\frac{a+I}{s+I} = \frac{a'+I}{s'+I}$, 则存在 $t+I \in \pi(S)$, 使得

$$(a+I)(s'+I)(t+I) = (a'+I)(s+I)(t+I),$$

由此得到 $(as'-a's)t \in I$, 即存在 $i \in I$, s.t.

$$(as'-a's)t = i,$$

其中 $t \in S$. 由此可知,

$$\frac{a}{s} - \frac{a'}{s'} = \frac{as'-a's}{ss'} = \frac{i}{ss't} \in I_S,$$

从而 $\frac{a}{s} + I_S = \frac{a'}{s'} + I_S$. 所以, ϕ 良定义.

(环同态) 对于任意的 $\frac{a+I}{s+I}, \frac{b+I}{t+I} \in (A/I)_{\pi(S)}$, 有

$$\begin{aligned}
\phi(\frac{a+I}{s+I} + \frac{b+I}{t+I}) &= \phi(\frac{(a+I)(t+I)+(b+I)(s+I)}{(s+I)(t+I)}) \\
&= \frac{at+bs}{st} + I_S \\
&= \frac{a}{s} + I_S + \frac{b}{t} + I_S = \phi(\frac{a+I}{s+I}) + \phi(\frac{b+I}{t+I}), \\
\phi(\frac{a+I}{s+I} \cdot \frac{b+I}{t+I}) &= \phi(\frac{(a+I)(b+I)}{(s+I)(t+I)}) \\
&= \frac{ab}{st} + I_S \\
&= (\frac{a}{s} + I_S) \cdot (\frac{b}{t} + I_S) = \phi(\frac{a+I}{s+I}) \cdot \phi(\frac{b+I}{t+I}).
\end{aligned}$$

因此, ϕ 为环同态.

(双射性) 如果 $\phi(\frac{a+I}{s+I}) = \phi(\frac{a'+I}{s'+I})$, 则

$$\frac{a}{s} + I_S = \frac{a'}{s'} + I_S.$$

根据商理想的定义, 存在 $t \in S$, 使得

$$(as' - a's)t \in I.$$

因为 $t \in S$, 所以 $st \in S$. 因此, 有

$$(as' - a's)t = i$$

对某个 $i \in I$. 由此可知,

$$(a+I)(s'+I)(t+I) = (a'+I)(s+I)(t+I).$$

因为 $t + I \in \pi(S)$, 所以

$$\frac{a+I}{s+I} = \frac{a'+I}{s'+I}.$$

所以, ϕ 为单射. 对于任意的 $\frac{a}{s} + I_S \in A_S/I_S$, 有

$$\phi(\frac{a+I}{s+I}) = \frac{a}{s} + I_S.$$

所以, ϕ 为满射.

综上, ϕ 为环同构. $\square$

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

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

证明: 定义映射 $\phi : A[X]\big/(1-fX) \to A_f$, 对于任意的 $g(X) + (1-fX) \in A[X]\big/(1-fX)$, 令

$$\phi(g(X) + (1-fX)) = g(\frac{1}{f}).$$

下面验证 ϕ 为环同构.

(良定义) 如果 $g(X) + (1-fX) = h(X) + (1-fX)$, 则 $g(X) - h(X) \in (1-fX)$. 即存在 $q(X) \in A[X]$, 使得 $g(X) - h(X) = q(X)(1-fX)$. 因此,

$$g(\frac{1}{f}) - h(\frac{1}{f}) = q(\frac{1}{f})(1 - f \cdot \frac{1}{f}) = q(\frac{1}{f}) \cdot 0 = 0.$$

所以, $\phi(g(X) + (1-fX)) = g(\frac{1}{f}) = h(\frac{1}{f}) = \phi(h(X) + (1-fX))$. 因此, ϕ 良定义.

(环同态) 对于任意的 $g(X) + (1-fX), h(X) + (1-fX) \in A[X]/(1-fX)$, 有

$$\begin{aligned}
\phi((g(X) + (1-fX)) + (h(X) + (1-fX))) &= \phi((g(X) + h(X)) + (1-fX)) \\
&= (g+h)(\frac{1}{f}) = g(\frac{1}{f}) + h(\frac{1}{f}) \\
&= \phi(g(X) + (1-fX)) + \phi(h(X) + (1-fX)),
\end{aligned}$$

$$
\begin{aligned}
\phi((g(X)+(1-fX))\cdot(h(X)+(1-fX))) &= \phi((g(X)h(X))+(1-fX)) \\
&= (gh)(\frac{1}{f}) = g(\frac{1}{f})\cdot h(\frac{1}{f}) \\
&= \phi(g(X)+(1-fX))\cdot\phi(h(X)+(1-fX)).
\end{aligned}
$$

因此, ϕ 为环同态.

(双射性) 如果 $\phi(g(X)+(1-fX)) = \phi(h(X)+(1-fX))$, 则 $g(\frac{1}{f}) = h(\frac{1}{f})$. 设 $d(X) = g(X)-h(X)$, 则 $d(\frac{1}{f}) = 0$. 因此, $d(X)$ 在 $X = \frac{1}{f}$ 处有根, 即 $1-fX$ 整除 $d(X)$. 所以, 存在 $q(X)\in A[X]$, 使得 $d(X) = q(X)(1-fX)$. 因此, $g(X)+(1-fX) = h(X)+(1-fX)$. 所以, ϕ 为单射. 对于任意的 $\frac{a}{f^n}\in A_f$, 令 $g(X) = aX^n \in A[X]$. 则有

$$\phi(g(X)+(1-fX)) = g(\frac{1}{f}) = a(\frac{1}{f})^n = \frac{a}{f^n}.$$

所以, ϕ 为满射.

综上, ϕ 为环同构. □

注: 完全可以用同构定理来证明, 这里相当于干了很多重复无意义的事.

定义映射 $\psi : A[X]\to A_f$, 对于任意的 $g(X)\in A[X]$, 令

$$\psi(g(X)) = g(\frac{1}{f}).$$

显然, ψ 为环同态. 并且 $\ker(\psi) = (1-fX)$, 因为 $g(\frac{1}{f}) = 0$ 等价于 $g(X)$ 在 $X = \frac{1}{f}$ 处有根, 即 $1-fX$ 整除 $g(X)$. 由同构定理, 有

$$A[X]\big/(1-fX) \xrightarrow{\simeq} \mathrm{Im}(\psi).$$

下面证明 $\mathrm{Im}(\psi) = A_f$. 对于任意的 $\frac{a}{f^n}\in A_f$, 令 $g(X) = aX^n\in A[X]$. 则有

$$\psi(g(X)) = g(\frac{1}{f}) = a(\frac{1}{f})^n = \frac{a}{f^n}.$$

因此, $\mathrm{Im}(\psi) = A_f$. 综上, 有

$$A[X]\big/(1-fX) \xrightarrow{\simeq} A_f.$$

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

假设 $d \in \mathbb{Z}$ 不是完全平方数。令

$$\mathbb{Z}[\sqrt{d}] = \{x + y\sqrt{d} \mid x, y \in \mathbb{Z}\}, \quad \mathbb{Q}[\sqrt{d}] = \{x + y\sqrt{d} \mid x, y \in \mathbb{Q}\}$$

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

证明：先证明 $\mathbb{Z}[\sqrt{d}]$ 为环. 对于任意的 $x_1 + y_1\sqrt{d}, x_2 + y_2\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, 有

$$(x_1 + y_1\sqrt{d}) + (x_2 + y_2\sqrt{d}) = (x_1 + x_2) + (y_1 + y_2)\sqrt{d} \in \mathbb{Z}[\sqrt{d}],$$

$$(x_1 + y_1\sqrt{d}) \cdot (x_2 + y_2\sqrt{d}) = (x_1x_2 + y_1y_2d) + (x_1y_2 + x_2y_1)\sqrt{d} \in \mathbb{Z}[\sqrt{d}].$$

因此, $\mathbb{Z}[\sqrt{d}]$ 在加法和乘法下封闭. 显然, 加法和乘法满足交换律和结合律, 且乘法对加法分配. 零元为 $0 + 0\sqrt{d}$, $x + y\sqrt{d}$ 的加法逆元为 $-x - y\sqrt{d}$. 所以, $\mathbb{Z}[\sqrt{d}]$ 为环.

再证明 $\mathbb{Z}[\sqrt{d}]$ 为整环. 直接利用 B4) 中定义的" 范数" 函数 $N : \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}$, 如果 $N(zw) = 0$, 则 $N(z)N(w) = 0$, 从而 $N(z) = 0$ 或 $N(w) = 0$. 因为 $N(x + y\sqrt{d}) = x^2 - dy^2 = 0$ 的唯一整数解为 $x = 0, y = 0$, 所以 $z = 0$ 或 $w = 0$. 因此, $\mathbb{Z}[\sqrt{d}]$ 为整环.

再证明 $\mathbb{Q}[\sqrt{d}]$ 为 $\mathbb{Z}[\sqrt{d}]$ 的分式域.

根据讲义上类似地构造 $\mathbb{Z}[\sqrt{d}]$ 的分式域, 那么 $\mathrm{Frac}(\mathbb{Z}[\sqrt{d}])$ 中的元素形如 $\frac{x_1+y_1\sqrt{d}}{x_2+y_2\sqrt{d}}$, 其中 $x_1, y_1, x_2, y_2 \in \mathbb{Z}$ 且 $x_2 + y_2\sqrt{d} \neq 0$. 下面证明 $\mathrm{Frac}(\mathbb{Z}[\sqrt{d}]) = \mathbb{Q}[\sqrt{d}]$. 先证明 $\mathrm{Frac}(\mathbb{Z}[\sqrt{d}]) \subset \mathbb{Q}[\sqrt{d}]$. 对于任意的 $\frac{x_1+y_1\sqrt{d}}{x_2+y_2\sqrt{d}} \in \mathrm{Frac}(\mathbb{Z}[\sqrt{d}])$, 有

$$\begin{aligned}\frac{x_1 + y_1\sqrt{d}}{x_2 + y_2\sqrt{d}} &= \frac{(x_1 + y_1\sqrt{d})(x_2 - y_2\sqrt{d})}{(x_2 + y_2\sqrt{d})(x_2 - y_2\sqrt{d})} \\ &= \frac{(x_1x_2 - y_1y_2d) + (x_2y_1 - x_1y_2)\sqrt{d}}{x_2^2 - y_2^2d}.\end{aligned}$$

因为 $x_1, y_1, x_2, y_2 \in \mathbb{Z}$ 且 $x_2 + y_2\sqrt{d} \neq 0$, 所以 $x_2^2 - y_2^2d \neq 0$. 因此, $\frac{x_1+y_1\sqrt{d}}{x_2+y_2\sqrt{d}} \in \mathbb{Q}[\sqrt{d}]$. 所以, $\mathrm{Frac}(\mathbb{Z}[\sqrt{d}]) \subset \mathbb{Q}[\sqrt{d}]$. 再证明 $\mathbb{Q}[\sqrt{d}] \subset \mathrm{Frac}(\mathbb{Z}[\sqrt{d}])$. 对于任意的 $x + y\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$, 设 $x = \frac{a}{b}$, $y = \frac{c}{e}$, 其中 $a, b, c, e \in \mathbb{Z}$ 且 $b, e \neq 0$. 则有

$$\begin{aligned}x + y\sqrt{d} &= \frac{a}{b} + \frac{c}{e}\sqrt{d} \\ &= \frac{ae + bc\sqrt{d}}{be}.\end{aligned}$$

因为 $ae + bc\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ 且 $be \in \mathbb{Z} - \{0\}$, 所以 $x + y\sqrt{d} \in \mathrm{Frac}(\mathbb{Z}[\sqrt{d}])$. 所以, $\mathbb{Q}[\sqrt{d}] \subset \mathrm{Frac}(\mathbb{Z}[\sqrt{d}])$.

综上, $\mathrm{Frac}(\mathbb{Z}[\sqrt{d}]) = \mathbb{Q}[\sqrt{d}]$. 而两者上的加法与乘法运算是一致的. 因此, $\mathbb{Q}[\sqrt{d}]$ 为 $\mathbb{Z}[\sqrt{d}]$ 的分式域. $\square$

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

证明：设 $d \in \mathbb{Z}$ 不是完全平方数.

如果 $d<0$, 则 $\sqrt{d}=i\sqrt{|d|}$. 因此, 对于任意的 $x+y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, 有

$$x+y\sqrt{d}=x+yi\sqrt{|d|}.$$

由此可知, $\mathbb{Z}[\sqrt{d}]$ 为 $\mathbb{C}$ 中的格点. 因为格点是离散的, 所以 $\mathbb{Z}[\sqrt{d}]$ 在 $\mathbb{C}$ 中离散.

如果 $d>0$, 我们可以使用连分式技巧, 取到一列有理数 $\{\frac{p_n}{q_n}\}$ 使得

$$|\sqrt{d}-\frac{p_n}{q_n}|<\frac{1}{q_n^2}.$$

即

$$|q_n\sqrt{d}-p_n|<\frac{1}{q_n}.$$

于是 $\forall a \in \mathbb{R}$, 取 $k_n=\lfloor\frac{a}{q_n\sqrt{d}-p_n}\rfloor$, 则有

$$|k_n(q_n\sqrt{d}-p_n)-a|=\left|\lfloor\frac{a}{q_n\sqrt{d}-p_n}\rfloor(q_n\sqrt{d}-p_n)-a\right|<|q_n\sqrt{d}-p_n|<\frac{1}{q_n},$$

又 $\lim_{n\to\infty}\frac{1}{q_n}=0$, 所以 $\lim_{n\to\infty}k_n(q_n\sqrt{d}-p_n)=a$. 因此, $\mathbb{Z}[\sqrt{d}]$ 在 $\mathbb{R}$ 中稠密. □

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

证明：下面证明环 $\mathbb{Z}[\sqrt{d}]$ 的自同构群 $\mathrm{Aut}(\mathbb{Z}[\sqrt{d}])$ 恰有 2 个元素.

设 $\sigma \in \mathrm{Aut}(\mathbb{Z}[\sqrt{d}])$. 我们可以将 $1, \sqrt{d}$ 视为 $\mathbb{Z}[\sqrt{d}]$ 的一组 “基”, 因此只需要考虑 $\sigma(1)$ 与 $\sigma(\sqrt{d})$ 即可. 因为 σ 为环同构, 所以

$$\sigma(1)=1.$$

设 $\sigma(\sqrt{d})=a+b\sqrt{d}$, 其中 $a, b \in \mathbb{Z}$. 则有

$$\sigma(\sqrt{d})^2=\sigma(d)=d.$$

因此,

$$(a+b\sqrt{d})^2=a^2+2ab\sqrt{d}+b^2d=d.$$

由此可知,

$$a^2+b^2d=d,$$

$$2ab=0.$$

如果 $b=0$, 则 $a^2=d$, 与 d 不是完全平方数矛盾. 因此, $a=0$. 所以, $b^2d=d$. 因为 $d\neq 0$, 所以 $b^2=1$. 因此, $b=1$ 或 $b=-1$.

如果 $b=1$, 则 $\sigma(\sqrt{d})=\sqrt{d}$. 如果 $b=-1$, 则 $\sigma(\sqrt{d})=-\sqrt{d}$. 因此, 环 $\mathbb{Z}[\sqrt{d}]$ 的自同构群 $\mathrm{Aut}(\mathbb{Z}[\sqrt{d}])$ 恰有 2 个元素, 即恒等映射和共轭映射. □

注：这里以及 B5) 中都讨论了 $d<0$ 情形.

B4) 对任意的 $z \in \mathbb{Q}[\sqrt{d}]$ ，我们定义 $N(z)=z\cdot\bar{z}$。证明，对任意的 $a,b \in \mathbb{Q}[\sqrt{d}], N(a\cdot b)=N(a)\cdot N(b)$ 并且 $N(\mathbb{Z}[\sqrt{d}]) \subset \mathbb{Z}$ 。据此证明：$\mathbb{Z}[\sqrt{d}]^\times=\{z\in\mathbb{Z}[\sqrt{d}] \mid N(z)=\pm1\}$ 。

证明: 先证明对任意的 $a,b\in\mathbb{Q}[\sqrt{d}]$, 有 $N(a\cdot b)=N(a)\cdot N(b)$. 设 $a=x_1+y_1\sqrt{d}, b=x_2+y_2\sqrt{d}$, 其中 $x_1,y_1,x_2,y_2\in\mathbb{Q}$. 则有

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

$$N(b)=(x_2+y_2\sqrt{d})(x_2-y_2\sqrt{d})=x_2^2-dy_2^2.$$

因此,

$$\begin{aligned}N(a\cdot b)&=N((x_1+y_1\sqrt{d})(x_2+y_2\sqrt{d}))\\&=N((x_1x_2+y_1y_2d)+(x_1y_2+x_2y_1)\sqrt{d})\\&=(x_1x_2+y_1y_2d)^2-d(x_1y_2+x_2y_1)^2\\&=(x_1^2-dy_1^2)(x_2^2-dy_2^2)=N(a)\cdot N(b).\end{aligned}$$

再证明 $N(\mathbb{Z}[\sqrt{d}])\subset\mathbb{Z}$. 对于任意的 $z=x+y\sqrt{d}\in\mathbb{Z}[\sqrt{d}]$, 其中 $x,y\in\mathbb{Z}$. 则有

$$N(z)=(x+y\sqrt{d})(x-y\sqrt{d})=x^2-dy^2\in\mathbb{Z}.$$

因此, $N(\mathbb{Z}[\sqrt{d}])\subset\mathbb{Z}$. 下面证明 $\mathbb{Z}[\sqrt{d}]^\times=\{z\in\mathbb{Z}[\sqrt{d}]\mid N(z)=\pm1\}$. 设 $z\in\mathbb{Z}[\sqrt{d}]^\times$. 则存在 $w\in\mathbb{Z}[\sqrt{d}]$, 使得 $z\cdot w=1$. 因此,

$$N(z)\cdot N(w)=N(z\cdot w)=N(1)=1.$$

因为 $N(z),N(w)\in\mathbb{Z}$, 所以 $N(z)=\pm1$. 反之, 设 $z\in\mathbb{Z}[\sqrt{d}]$, 且 $N(z)=\pm1$. 则有

$$N(z)=z\cdot\bar{z}=\pm1.$$

因此,

$$z\cdot(\pm\bar{z})=1.$$

所以, $z\in\mathbb{Z}[\sqrt{d}]^\times$. 综上, $\mathbb{Z}[\sqrt{d}]^\times=\{z\in\mathbb{Z}[\sqrt{d}]\mid N(z)=\pm1\}$. □

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

证明：如果 $d<0$, 则对于任意的 $z=x+y\sqrt{d}\in\mathbb{Z}[\sqrt{d}]^\times$, 有

$$N(z)=x^2-dy^2=\pm1.$$

因为 $d<0$, 所以 $x^2+|d|y^2=\pm 1$. 因此, 当 $d\leqslant -2$ 时, $y=0$ 且 $x=\pm 1$. 所以, $\mathbb{Z}[\sqrt{d}]^\times=\{\pm 1\}$; 当 $d=-1$ 时, $\mathbb{Z}[\sqrt{d}]^\times=\{\pm 1,\pm i\}$ □

如果 $d>0$, 则对于任意的 $z=x+y\sqrt{d}\in\mathbb{Z}[\sqrt{d}]^\times$, 有

$$N(z)=x^2-dy^2=\pm 1.$$

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

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

证明：设 $z=x+y\sqrt{2}\in\mathbb{Z}[\sqrt{2}]^\times\cap(1,3)$, 其中 $x,y\in\mathbb{Z}$. 则有

$$N(z)=x^2-2y^2=\pm 1.$$

因为 $1<x+y\sqrt{2}<3$, 对 x^2-2y^2 的值进行讨论.

如果 $x^2-2y^2=1$, 则有 $\frac{1}{3}<x-y\sqrt{2}<1$. 从而得到 $\frac{2}{3}<x<2$, 所以 $x=1$. 由此得到 $y=1$. 因此, $z=1+\sqrt{2}$.

如果 $x^2-2y^2=-1$, 则有 $-1<x-y\sqrt{2}<-\frac{1}{3}$. 从而得到 $0<x<\frac{4}{3}$, 所以 $x=1$. 由此得到 $y=1$. 但是, $1+\sqrt{2}$ 不满足 $x^2-2y^2=-1$, 矛盾.

综上, $\mathbb{Z}[\sqrt{2}]^\times\cap(1,3)=\{1+\sqrt{2}\}$. □

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

证明：先证明 $\mathbb{Z}[\sqrt{2}]^\times=\{\pm(1+\sqrt{2})^k\mid k\in\mathbb{Z}\}$. 设 $z=x+y\sqrt{2}\in\mathbb{Z}[\sqrt{2}]^\times$, 其中 $x,y\in\mathbb{Z}$.

若 $z>0$. 设 k 为满足 $(1+\sqrt{2})^k<z\leqslant(1+\sqrt{2})^{k+1}$ 的最大整数. 则有

$$1<\frac{z}{(1+\sqrt{2})^k}\leqslant 1+\sqrt{2}.$$

因为 $\frac{z}{(1+\sqrt{2})^k}\in\mathbb{Z}[\sqrt{2}]^\times$, 根据 B6), 有

$$\frac{z}{(1+\sqrt{2})^k}=1+\sqrt{2}.$$

因此, $z=(1+\sqrt{2})^{k+1}$. 如果 $z<0$. 设 k 为满足 $-(1+\sqrt{2})^{k+1}\leqslant z<-(1+\sqrt{2})^k$ 的最大整数. 则有

$$1<\frac{z}{-(1+\sqrt{2})^k}\leqslant 1+\sqrt{2}.$$

因为 $\frac{z}{-(1+\sqrt{2})^k}\in\mathbb{Z}[\sqrt{2}]^\times$, 根据 B6), 有

$$\frac{z}{-(1+\sqrt{2})^k}=1+\sqrt{2}.$$

因此, $z=-(1+\sqrt{2})^{k+1}$. 综上, $\mathbb{Z}[\sqrt{2}]^\times=\{\pm(1+\sqrt{2})^k\mid k\in\mathbb{Z}\}$.

定义映射 ϕ:

$$\mathbb{Z}[\sqrt{2}]^\times\to\mathbb{Z}\times{}^{\mathbb{Z}}\!/_{2\mathbb{Z}},\quad (1+\sqrt{2})^k\mapsto(k,\bar{0}),\quad -(1+\sqrt{2})^k\mapsto(k,\bar{1}).$$

下面验证 ϕ 为群同构.

(群同态) 对于任意的 $z_1, z_2 \in \mathbb{Z}[\sqrt{2}]^{\times}$, 设 $z_1 = \epsilon_1(1+\sqrt{2})^{k_1}$, $z_2 = \epsilon_2(1+\sqrt{2})^{k_2}$, 其中 $\epsilon_1, \epsilon_2 \in \{\pm 1\}$ 且 $k_1, k_2 \in \mathbb{Z}$. 则有

$$\begin{aligned}
\phi(z_1 \cdot z_2) &= \phi(\epsilon_1\epsilon_2(1+\sqrt{2})^{k_1+k_2}) \\
&= (k_1+k_2, \bar{\delta}), \quad 其中\delta = \begin{cases} 0, & 如果\epsilon_1\epsilon_2 = 1; \\ 1, & 如果\epsilon_1\epsilon_2 = -1. \end{cases} \\
&= (k_1, \overline{\epsilon_1}) + (k_2, \overline{\epsilon_2}) \\
&= \phi(z_1) + \phi(z_2).
\end{aligned}$$

因此, ϕ 为群同态.

(双射性) 如果 $\phi(z_1) = \phi(z_2)$, 则有 $(k_1, \overline{\epsilon_1}) = (k_2, \overline{\epsilon_2})$. 因此, $k_1 = k_2$ 且 $\overline{\epsilon_1} = \overline{\epsilon_2}$. 所以, $\epsilon_1 = \epsilon_2$. 因此, $z_1 = z_2$. 所以, ϕ 为单射. 对于任意的 $(k, \bar{e}) \in \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, 设 $e = 0$ 或 $e = 1$. 如果 $e = 0$, 则有

$$\phi((1+\sqrt{2})^k) = (k, \bar{0}) = (k, \bar{e}).$$

如果 $e = 1$, 则有

$$\phi(-(1+\sqrt{2})^k) = (k, \bar{1}) = (k, \bar{e}).$$

所以, ϕ 为满射. 综上, ϕ 为群同构. □

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?

证明: 根据 B4) 与 B7), $\mathbb{Z}[\sqrt{2}]^{\times} = \{z \in \mathbb{Z}[\sqrt{2}] \mid N(z) = \pm 1 \Leftrightarrow z = x + y\sqrt{2}, x^2 - 2y^2 = \pm 1\} = \{\pm(1+\sqrt{2})^k \mid k \in \mathbb{Z}\}$. 下面分别讨论 Pell 方程 $x^2 - 2y^2 = 1$ 和 $x^2 - 2y^2 = -1$ 的所有整数解.

设 $z = \epsilon(1+\sqrt{2})^k \in \mathbb{Z}[\sqrt{2}]^{\times}$, 其中 $k \in \mathbb{Z}, \epsilon = \pm 1$. 则有

$$N(z) = N(\epsilon(1+\sqrt{2})^k) = \epsilon(1+\sqrt{2})^k \cdot \epsilon(1-\sqrt{2})^k = \epsilon^2(-1)^k = (-1)^k.$$

又 $N(z) = x^2 - 2y^2 = \pm 1$. 因此, 当 k 为偶数时, $N(z) = 1$; 当 k 为奇数时, $N(z) = -1$.

综上, Pell 方程 $x^2 - 2y^2 = 1$ 的所有整数解为

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

其中 $m \in \mathbb{Z}$; Pell 方程 $x^2 - 2y^2 = -1$ 的所有整数解为

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

其中 $m \in \mathbb{Z}$. □

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 $\lim_{n\to\infty} z_n = 0$ 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）

证明：先证明 Dirichlet 引理. 设 $\alpha \in \mathbb{R}$ 且 M 为正整数. 考虑数列 $\{k\alpha\}_{k=0}^{M}$ 在区间 $[0,1)$ 中的小数部分. 将区间 $[0,1)$ 划分为 M 个子区间 $[0, \frac{1}{M}), [\frac{1}{M}, \frac{2}{M}), \ldots, [\frac{M-1}{M}, 1)$. 根据抽屉原理, 存在 i, j 满足 $0 \leqslant i < j \leqslant M$, 使得 $k_i\alpha$ 与 $k_j\alpha$ 的小数部分落在同一子区间内. 设 $q = j - i \leqslant M$, p 为 $k_j\alpha$ 与 $k_i\alpha$ 的小数部分之差的整数部分. 则有

$$|p - q\alpha| < \frac{1}{M}.$$

即, Dirichlet 引理成立.

下面证明存在序列 $\{z_n\}_{n\geqslant 1} \subset \mathbb{Z}[\sqrt{d}] - \{0\}$, 使得 $\lim_{n\to\infty} z_n = 0$ 且 $\{N(z_n)\}_{n\geqslant 1}$ 是有界的. 设 M 为正整数. 根据 Dirichlet 引理, 存在整数 p_n 和正整数 $q_n \leqslant M$, 使得

$$|p_n - q_n\sqrt{d}| < \frac{1}{M}.$$

定义 $z_n = p_n - q_n\sqrt{d}$. 则有

$$|z_n| = |p_n - q_n\sqrt{d}| < \frac{1}{M}.$$

因此, 当 $M \to \infty$ 时, $\lim_{n\to\infty} z_n = 0$. 下面证明 $\{N(z_n)\}_{n\geqslant 1}$ 是有界的. 对于任意的 $n \geqslant 1$, 有

$$N(z_n) = (p_n - q_n\sqrt{d})(p_n + q_n\sqrt{d}).$$

因为 $q_n \leqslant M$, 所以 $|p_n| < |q_n\sqrt{d}| + \frac{1}{M} \leqslant M\sqrt{d} + \frac{1}{M}$. 因此,

$$|N(z_n)| = |p_n - q_n\sqrt{d}||p_n + q_n\sqrt{d}| < \frac{1}{M}\left(2M\sqrt{d} + \frac{1}{M}\right) = 2\sqrt{d} + \frac{1}{M^2}.$$

由此可知, $\{N(z_n)\}_{n\geqslant 1}$ 是有界的.

综上, 存在序列 $\{z_n\}_{n\geqslant 1} \subset \mathbb{Z}[\sqrt{d}] - \{0\}$, 使得 $\lim_{n\to\infty} z_n = 0$ 且 $\{N(z_n)\}_{n\geqslant 1}$ 是有界的. $\square$

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 $w_n\bar{w}_m \in k\mathbb{Z}[\sqrt{d}]$ 。（提示：考虑 w_n 在 $\mathbb{Z}[\sqrt{d}]/k\mathbb{Z}[\sqrt{d}]$ 中的像）

证明：根据 B9), 存在序列 $\{z_n\}_{n\geqslant 1} \subset \mathbb{Z}[\sqrt{d}] - \{0\}$, 使得 $\lim_{n\to\infty} z_n = 0$ 且 $\{N(z_n)\}_{n\geqslant 1}$ 是有界的.

因为 $\{N(z_n)\}_{n\geqslant 1}$ 是有界的, 所以存在整数 k, 使得无穷多个 z_n 满足 $N(z_n) = k$. 设这些 z_n 构成子序列 $\{u_n\}_{n\geqslant 1}$.

因为 $\mathbb{Z}[\sqrt{d}]/k\mathbb{Z}[\sqrt{d}]$ 为有限集, 所以存在子序列 $\{w_n\}_{n\geqslant 1} \subset \{u_n\}_{n\geqslant 1}$, 使得对任意的 $n, m \geqslant 1$, 有

$$w_n \equiv w_m \mod k\mathbb{Z}[\sqrt{d}].$$

因此,

$$w_n - w_m \in k\mathbb{Z}[\sqrt{d}].$$

由此可知,

$$w_n\bar{w}_m - w_m\bar{w}_m = (w_n - w_m)\bar{w}_m \in k\mathbb{Z}[\sqrt{d}].$$

因为 $N(w_m) = k$, 所以 $w_m\bar{w}_m = k$. 因此,

$$w_n\bar{w}_m \in k\mathbb{Z}[\sqrt{d}].$$

综上, 存在子序列 $\{w_n\}_{n\geqslant 1}$ 以及整数 k, 使得对任意的 $n, m \geqslant 1$, 我们有 $N(w_n) = k$ 并且 $w_n\bar{w}_m \in k\mathbb{Z}[\sqrt{d}]$. $\square$

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

证明：根据 B10), 存在序列 $\{w_n\}_{n\geqslant 1} \subset \mathbb{Z}[\sqrt{d}] - \{0\}$ 以及整数 k, 使得对任意的 $n, m \geqslant 1$, 我们有 $N(w_n) = k$ 并且 $w_n\bar{w}_m \in k\mathbb{Z}[\sqrt{d}]$.

设 $n > m \geqslant 1$. 则有

$$w_n\bar{w}_m \in k\mathbb{Z}[\sqrt{d}].$$

因此, 存在整数 $l_{n,m} = x_n + y_n\sqrt{d}$, 其中 $x_n, y_n \in \mathbb{Z}$, 使得

$$w_n\bar{w}_m = kl_{n,m}.$$

定义

$$v_{n,m} = \frac{w_n}{w_m} = \frac{kl_{n,m}}{w_m\bar{w}_m} = l_{n,m}.$$

则有 $u_{n,m} \in \mathbb{Z}[\sqrt{d}]$. 下面证明 $u_{n,m} \in \mathbb{Z}[\sqrt{d}]^{\times}$. 由于 $N(w_n) = k$ 且 $N(w_m) = k$, 所以

$$N(u_{n,m}) = N\left(\frac{w_n}{w_m}\right) = \frac{N(w_n)}{N(w_m)} = \frac{k}{k} = 1.$$

根据 B4), 有 $u_{n,m} \in \mathbb{Z}[\sqrt{d}]^{\times}$.

于是固定 m, 可知对于任意的 $n > m \geqslant 1$, $u_{n,m} \in \mathbb{Z}[\sqrt{d}]^{\times}$. 因为 $\lim_{n\to\infty} w_n = 0$, 所以 w_n 可以取到无限个不同的值. 因此, $u_{n,m} = \frac{w_n}{w_m}$ 也可以取到无限个不同的值. 综上, $\mathbb{Z}[\sqrt{d}]^{\times}$ 是无限集. $\square$

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

证明：设 $0 < a < b < \infty$. 设 $z = x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]^{\times} \cap (a, b)$, 其中 $x, y \in \mathbb{Z}$. 则有

$$N(z) = x^2 - dy^2 = \pm 1.$$

类似 B6) 的分析, 对 $x^2 - dy^2$ 的值进行讨论.

如果 $x^2 - dy^2 = 1$, 则有

$$a < x + y\sqrt{d} < b,$$
$$\frac{1}{b} < x - y\sqrt{d} < \frac{1}{a}.$$

因此, x 与 y 满足以下不等式组:

$$a + \frac{1}{b} < 2x < b + \frac{1}{a},$$
$$a - \frac{1}{b} < 2y\sqrt{d} < b - \frac{1}{a}.$$

因为 x, y 为整数, 所以 x, y 只能取有限个值. 对于每一个确定的 y, x 也只能取有限个值. 而对于每一对 (x, y), 都对应着唯一的 z. 因此, $\mathbb{Z}[\sqrt{d}]^\times \cap (a, b)$ 是有限的.

$x^2 - dy^2 = -1$ 的情况是完全类似的. 综上, 对任意的 $0 < a < b < \infty$, $\mathbb{Z}[\sqrt{d}]^\times \cap (a, b)$ 是有限的. 因此, $\mathbb{Z}[\sqrt{d}]^\times \cap (0, \infty)$ 是乘法群 $(0, \infty)$ 的离散子群. □

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 $\mathbb{Z}[\sqrt{d}]^\times \cap (0, \infty)$ 。特别地，$\mathbb{Z}[\sqrt{d}]^\times \simeq \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. （注意到：对任意的 $u \in \mathbb{Z}[\sqrt{d}]^\times - \{\pm 1\}$ ，四个点 $\pm u, \pm \bar{u}$ 在区间 $(-\infty, -1), (-1, 0), (0, 1), (1, \infty)$ 中各有一个）

证明：由于 $\mathbb{Z}[\sqrt{d}]^\times$ 是无限集 (见 B11)), 所以 $\exists\ u \neq \pm 1 \in \mathbb{Z}[\sqrt{d}]^\times$. 注意到对任意的 $u \in \mathbb{Z}[\sqrt{d}]^\times - \{\pm 1\}$ ，四个点 $\pm u, \pm \bar{u}$ 在区间 $(-\infty, -1), (-1, 0), (0, 1), (1, \infty)$ 中各有一个, 这是因为 $N(u) = u\bar{u} = \pm 1$. 因此, $\exists\ v \in \mathbb{Z}[\sqrt{d}]^\times \cap (1, \infty)$.

根据 B12), $\mathbb{Z}[\sqrt{d}]^\times \cap (0, \infty)$ 为乘法群 $(0, \infty)$ 的离散子群. 因此, 存在 $\eta_d \in (1, \infty)$, 使得 η_d 为 $\mathbb{Z}[\sqrt{d}]^\times \cap (1, \infty)$ 中的最小元素.

下面证明 η_d 生成了 $\mathbb{Z}[\sqrt{d}]^\times \cap (0, \infty)$. 设 $u \in \mathbb{Z}[\sqrt{d}]^\times \cap (0, \infty)$. 则存在整数 k, 使得

$$(\eta_d)^k < u \leqslant (\eta_d)^{k+1}.$$

从而有

$$1 < \frac{u}{(\eta_d)^k} \leqslant \eta_d.$$

因为 $\frac{u}{(\eta_d)^k} \in \mathbb{Z}[\sqrt{d}]^\times \cap (1, \infty)$, 以及 η_d 的定义, 所以 $\frac{u}{(\eta_d)^k} = \eta_d$. 因此,

$$u = (\eta_d)^{k+1}.$$

综上, $\mathbb{Z}[\sqrt{d}]^\times \cap (0, \infty)$ 是由 η_d 生成的. 特别地, $\mathbb{Z}[\sqrt{d}]^\times \simeq \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. 这是因为 $\mathbb{Z}[\sqrt{d}]^\times$ 可以被分解为绝对值和符号的乘积, 而绝对值部分是由 η_d 生成的, 符号部分是由 -1 生成的. 因此, $\mathbb{Z}[\sqrt{d}]^\times \simeq \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. □

练习题

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.

证明：设 $a^n = 0$ 且 b^{-1} 为 b 的逆元.

(1) 证明 $a + b$ 可逆. 因为 $ab = ba$, 所以

$$(a+b)(b^{-1} - b^{-1}ab^{-1} + b^{-2}a^2b^{-1} - \cdots + (-1)^{n-1}b^{-(n-1)}a^{n-1}b^{-1}) = 1.$$

因此, $a + b$ 可逆.

(2) 证明 $a + b$ 是幂零元. 设 $a^m = 0, b^n = 0$. 因为 $ab = ba$, 所以

$$(a+b)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} a^k b^{n+m-k}.$$

当 $k \geqslant n$ 时, $a^k = 0$; 当 $k < n$ 时, $b^{n+m-k} = 0$. 因此, $(a+b)^{n+m} = 0$. 由此可知, $a + b$ 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，$1 - ba \in A^\times$。

证明：设 $(ab)^n = 0$.

(1) 证明 ba 是幂零元. 有

$$(ba)^{n+1} = b(ab)^n a = 0.$$

由此可知, ba 是幂零元.

(2) 给出 $(1-ab)^{-1}$ 与 $(1-ba)^{-1}$ 之间的联系. 有

$$(1-ba)(1+b(1-ab)^{-1}a) = 1 - ba + b(1-ab)^{-1}a - bab(1-ab)^{-1}a = 1.$$

因此,

$$(1-ba)^{-1} = 1 + b(1-ab)^{-1}a.$$

(3) 证明如果 $1 - ab \in A^\times$, 那么, $1 - ba \in A^\times$. 由 (2) 可知, $(1-ba)^{-1} = 1 + b(1-ab)^{-1}a$. 因此, $1 - ba \in A^\times$. □

注：这给出了著名的“交换律” $(1-ab)^{-1} = 1 + b(1-ba)^{-1}a$ 的非交换环版本.

我们在高等线性代数的课程中已经见过这个等式在矩阵环中的应用. 当时也许不太理解这个等式的来历. 现在我们看到，这个等式实际上是非交换环中的一个普遍现象.

并且等式也不是”注意到”的, 而是因为

$$(1-ab)(1+ab+(ab)^2+\cdots+(ab)^{n-1}) = 1-(ab)^n = 1,$$

$$(1-ba)(1+ba+(ba)^2+\cdots+(ba)^n) = 1-(ba)^{n+1} = 1,$$

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

证明：一方面, 设 $a\in\mathfrak{Nil}(A)$. 则存在 $n\geqslant 1$, 使得 $a^n=0$. 对任意的素理想 $\mathfrak{p}\in\mathrm{Spec}(A)$, 因为 $0\in\mathfrak{p}$ 且 $\mathfrak{p}$ 为理想, 所以 $a^n\in\mathfrak{p}$. 由于 $\mathfrak{p}$ 为素理想, 所以 $a\in\mathfrak{p}$. 因此, $a\in\bigcap_{\mathfrak{p}\in\mathrm{Spec}(A)}\mathfrak{p}$. 由此可知, $\mathfrak{Nil}(A)\subseteq\bigcap_{\mathfrak{p}\in\mathrm{Spec}(A)}\mathfrak{p}$.

另一方面, 设 $a\in\bigcap_{\mathfrak{p}\in\mathrm{Spec}(A)}\mathfrak{p}$. 考虑所有与 S 相交为空的理想的集合

$$\mathcal{I}=\{\mathfrak{a}\mid\mathfrak{a}\text{ 为理想且}\mathfrak{a}\cap S=\varnothing\},$$

其中 $S=\{a^n\mid n\geqslant 1\}$. 显然, $\mathcal{I}$ 非空, 因为零理想 $\{0\}\in\mathcal{I}$. 对于 $\mathcal{I}$ 中任意的链 $\{\mathfrak{a}_i\}_{i\in I}$, 定义 $\mathfrak{a}=\bigcup_{i\in I}\mathfrak{a}_i$. 则 $\mathfrak{a}$ 为理想且 $\mathfrak{a}\cap S=\varnothing$. 因此, 根据 Zorn 引理, 存在包含 a 的极大理想 $\mathfrak{m}$. 因为 $\mathfrak{m}$ 为极大理想, 所以 $\mathfrak{m}$ 为素理想. 由此可知, $a\notin\mathfrak{m}$. 这与 $a\in\bigcap_{\mathfrak{p}\in\mathrm{Spec}(A)}\mathfrak{p}$ 矛盾. 因此, $a\in\mathfrak{Nil}(A)$. 由此可知, $\bigcap_{\mathfrak{p}\in\mathrm{Spec}(A)}\mathfrak{p}\subseteq\mathfrak{Nil}(A)$。

综上, $\mathfrak{Nil}(A)=\bigcap_{\mathfrak{p}\in\mathrm{Spec}(A)}\mathfrak{p}$. □

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 $b\in A, 1-ab\in A^\times$。

证明：设 $a\in J(A)$. 对任意的 $b\in A$, 如果 $1-ab\notin A^\times$, 则存在极大理想 $\mathfrak{m}\in\mathrm{SpecMax}(A)$, 使得 $1-ab\in\mathfrak{m}$. 因为 $a\in J(A)$, 所以 $a\in\mathfrak{m}$. 因此, $ab\in\mathfrak{m}$. 由此可知, $1=(1-ab)+ab\in\mathfrak{m}$. 这与 $\mathfrak{m}$ 为理想矛盾. 因此, 对任意的 $b\in A$, 有 $1-ab\in A^\times$.

设对任意的 $b\in A$, 有 $1-ab\in A^\times$. 如果 $a\notin J(A)$, 则存在极大理想 $\mathfrak{m}\in\mathrm{SpecMax}(A)$, 使得 $a\notin\mathfrak{m}$. 因为 $\mathfrak{m}$ 为极大理想, 所以存在 $b\in A$, 使得 $1-ab\in\mathfrak{m}$. 由此可知, $1-ab\notin A^\times$. 这与对任意的 $b\in A$, 有 $1-ab\in A^\times$ 矛盾. 因此, $a\in J(A)$.

综上, $a\in J(A)$ 当且仅当对任意的 $b\in A$, 有 $1-ab\in A^\times$. □

5. A 是环，I 是双边理想。那么，我们有如下的一一对应

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

证明：设 J 为 A 的左理想且 $J\supset I$. $\forall j+I\in {}^{J}\!/\!_{I}$ 且 $\forall a+I\in {}^{A}\!/\!_{I}$. 因为 J 为左理想, 所以 $aj\in J$. 因此,

$$(a+I)(j+I)=aj+I\in {}^{J}\!/\!_{I}.$$

由此可知, ${}^{J}\!/\!_{I}$ 为 ${}^{A}\!/\!_{I}$ 的左理想.

设 K 为 ${}^{A}\!/\!_{I}$ 的左理想. 定义 $J=\{a\in A\mid a+I\in K\}$. 则 $J\supset I$. $\forall a_1,a_2\in J$ 且 $\forall r\in A$. 因为 K 为左理想, 所以

$$(a_1+I)+(a_2+I)=(a_1+a_2)+I\in K,$$

$$(r+I)(a_1+I)=ra_1+I\in K.$$

因此, $a_1+a_2\in J$ 且 $ra_1\in J$. 由此可知, J 为 A 的左理想且 $J\supset I$. 所以该映射是满射.

设 J_1,J_2 为 A 的左理想且 $J_1,J_2\supset I$. 如果 ${J_1}/{I}={J_2}/{I}$, 则 $\forall j_1\in J_1$, 有 $j_1+I\in {J_1}/{I}={J_2}/{I}$. 因此, 存在 $j_2\in J_2$, 使得 $j_1+I=j_2+I$. 由此可知, $j_1-j_2\in I\subset J_2$. 因此, $j_1\in J_2$, 从而 $J_1\subset J_2$. 同理可得 $J_2\subset J_1$. 由此可知, $J_1=J_2$. 所以该映射是单射.

综上, 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。

证明: 设 $J\subset B$ 为理想. 定义 $\varphi^{-1}(J)=\{a\in A\mid\varphi(a)\in J\}$. 则 $\varphi^{-1}(J)\subset A$. 设 $a_1,a_2\in\varphi^{-1}(J)$ 且 $r\in A$. 则有

$$\varphi(-a_1)=-\varphi(a_1)\in J,$$

$$\varphi(a_1)+\varphi(a_2)=\varphi(a_1+a_2)\in J,$$

$$\varphi(r)\varphi(a_1)=\varphi(ra_1)\in J.$$

因此, $-a_1,a_1+a_2\in\varphi^{-1}(J)$ 且 $ra_1\in\varphi^{-1}(J)$. 又由环同态易知 $0\in\varphi^{-1}(J)$. 由此可知, $\varphi^{-1}(J)\subset A$ 为理想. □

注: 可以看出, 证明理想中证明加法子群时重要的是封闭性.

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。

证明: 设 $\mathfrak{q}\subset B$ 为素理想. 定义 $\varphi^{-1}(\mathfrak{q})=\{a\in A\mid\varphi(a)\in\mathfrak{q}\}$. 则 $\varphi^{-1}(\mathfrak{q})\subset A$ 为理想. 设 $a_1,a_2\in A$, 且 $a_1a_2\in\varphi^{-1}(\mathfrak{q})$. 则有

$$\varphi(a_1)\varphi(a_2)=\varphi(a_1a_2)\in\mathfrak{q}.$$

因为 $\mathfrak{q}$ 为素理想, 所以 $\varphi(a_1)\in\mathfrak{q}$ 或 $\varphi(a_2)\in\mathfrak{q}$. 因此, $a_1\in\varphi^{-1}(\mathfrak{q})$ 或 $a_2\in\varphi^{-1}(\mathfrak{q})$. 由此可知, $\varphi^{-1}(\mathfrak{q})\subset A$ 为素理想.

下面利用 $\mathbb{Z}\to\mathbb{Q}$ 的自然映射说明极大理想的逆像未必是极大的. 设 $\varphi:\mathbb{Z}\to\mathbb{Q}$ 为自然映射. 则 φ 为环同态. 设 $\mathfrak{m}=\{0\}\subset\mathbb{Q}$. 则 $\mathfrak{m}$ 为极大理想. 由此可知,

$$\varphi^{-1}(\mathfrak{m})=\{a\in\mathbb{Z}\mid\varphi(a)\in\mathfrak{m}\}=\{a\in\mathbb{Z}\mid a=0\}=\{0\}.$$

显然, $\{0\}\subset\mathbb{Z}$ 不是极大理想. 综上, 极大理想的逆像未必是极大的. □

注: 请注意域的理想只有零理想与自身.

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 $I \subset \mathfrak{p}_{i_0}$ 。

证明：我们使用数学归纳法证明该命题. 当 $n=1$ 时, 显然成立. 假设当 $n-1$ 时命题成立. 现在证明当 n 时命题也成立. 若 $\exists\, 1 \leqslant k \leqslant n, \text{s.t. } I \subset \bigcup_{i=1, i\neq k}^n \mathfrak{p}_i$, 则根据归纳假设, 存在 $i_0 \in \{1,2,\ldots,n\}\backslash\{k\}$, 使得 $I \subset \mathfrak{p}_{i_0}$. 若 $\forall\, 1 \leqslant k \leqslant n, I \not\subset \bigcup_{i=1, i\neq k}^n \mathfrak{p}_i$, 则对每个 $1 \leqslant k \leqslant n$, 存在 $a_k \in I$, 使得 $a_k \notin \bigcup_{i=1, i\neq k}^n \mathfrak{p}_i$. 因为 $a_k \in I \subset \bigcup_{i=1}^n \mathfrak{p}_i$, 所以 $a_k \in \mathfrak{p}_k$. 定义

$$a = a_1 a_2 \cdots a_{n-1} + a_n,$$

则 $a \in I$. 一方面, 因为 $\forall\, 1 \leqslant k \leqslant n-1, a_k \notin \mathfrak{p}_n$, 所以 $a_1 a_2 \cdots a_{n-1} \notin \mathfrak{p}_n$. 又 $a_n \in \mathfrak{p}_n$, 从而 $a \notin \mathfrak{p}_n$. 另一方面, $\forall\, 1 \leqslant k \leqslant n-1$, 有 $a_k \in \mathfrak{p}_k$, 所以 $a_1 a_2 \cdots a_{n-1} \in \mathfrak{p}$. 因为 $a_n \notin \mathfrak{p}_k$, 所以 $a \notin \mathfrak{p}_k$. 于是这与 $I \subset \bigcup_{i=1}^n \mathfrak{p}_i$ 矛盾. 综上, 存在 i_0, 使得 $I \subset \mathfrak{p}_{i_0}$. □

注：归纳法的使用中, k 只是一个 symbol, 它可以代表任意一个从 1 到 n 的整数. 同样的运用可以参考作业 3 中的 B5).

本题中 a 的构造上课出现过.

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 $I_{i_0} = \mathfrak{p}$ 。

证明：我们使用数学归纳法证明该命题. 当 $n=1$ 时, 显然成立. 假设当 $n-1$ 时命题成立. 现在证明当 n 时命题也成立. 若 $\exists\, 1 \leqslant k \leqslant n, \text{s.t. } \bigcap_{i=1, i\neq k}^n I_i \subset \mathfrak{p}$, 则根据归纳假设, 存在 $i_0 \in \{1,2,\ldots,n\}\backslash\{k\}$, 使得 $I_{i_0} \subset \mathfrak{p}$. 若 $\forall\, 1 \leqslant k \leqslant n$, $\bigcap_{i=1, i\neq k}^n I_i \not\subset \mathfrak{p}$, 则对每个 $1 \leqslant k \leqslant n$, 存在 $a_k \in \bigcap_{i=1, i\neq k}^n I_i$, 使得 $a_k \notin \mathfrak{p}$. 定义

$$a = a_1 a_2 \cdots a_n,$$

则 $a \notin \mathfrak{p}$ 但 $a \in \bigcap_{i=1}^n I_i$. 这与 $\bigcap_{i=1}^n I_i \subset \mathfrak{p}$ 矛盾. 综上, 存在 i_0, 使得 $I_{i_0} \subset \mathfrak{p}$.

特别地, 如果 $\bigcap_{i=1}^n I_i = \mathfrak{p}$, 则 $I_{i_0} \subset \mathfrak{p} = \bigcap_{i=1}^n I_i \subset I_{i_0}$. 因此, $I_{i_0} = \mathfrak{p}$. □

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。

证明：设 $I+J=A$. 则存在 $a \in I$ 且 $b \in J$, 使得 $a+b=1$. 对任意的 $n \geqslant 1$, 有

$$(a+b)^{2n} = \sum_{k=0}^{2n} \binom{2n}{k} a^k b^{2n-k} = 1.$$

因为 $\forall\, 0 \leqslant k \leqslant 2n$, $a^k b^{2n-k} \in I^n + J^n$(对于 $0 \leqslant k \leqslant n$, $a^k \in I^n$; 对于 $n < k \leqslant 2n$, $b^{2n-k} \in J^n$), 所以 $1 \in I^n + J^n$. 由此可知, 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。

证明： 设 $x, y \in \mathbf{Z}_S(A)$ 且 $r \in A$. 则对任意的 $s \in S$, 有

$$xs = sx,$$
$$ys = sy,$$

因此,

$$\begin{aligned}(-x)s &= -(xs) = -(sx) = s(-x),\\ (x+y)s &= xs + ys = sx + sy = s(x+y),\\ (ry)s &= r(ys) = r(sy) = (rs)y = (sr)y = s(ry).\end{aligned}$$

由此可知, $-x, x+y \in \mathbf{Z}_S(A)$ 且 $xy \in \mathbf{Z}_S(A)$. 显然, $0, 1 \in \mathbf{Z}_S(A)$. 综上, $\mathbf{Z}_S(A)$ 为 A 子环. $\square$

12. K 是域，$A = K[X]$ 是 K 上的多项式环，V 是 K 一线性空间。给定线性映射 $T \in \mathrm{End}_K(V)$ 可以给出 V 上的一个 $K[X]$ 一模的结构：

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

证明，V 上的每一个 $K[X]$ 一模的结构都恰好有某个 $T \in \mathrm{End}_K(V)$ 使得上述关系成立。

证明： 设 V 为 $K[X]$-模. 定义 $T : V \to V$ 为 K-线性映射, 使得对任意的 $v \in V$, 有

$$T(v) = X \cdot v.$$

则对任意的 $P(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in K[X]$ 且 $v \in V$, 有

$$\begin{aligned}P(T)(v) &= (a_nT^n + a_{n-1}T^{n-1} + \cdots + a_1T + a_0)(v)\\ &= a_nT^n(v) + a_{n-1}T^{n-1}(v) + \cdots + a_1T(v) + a_0v\\ &= a_nX^n \cdot v + a_{n-1}X^{n-1} \cdot v + \cdots + a_1X \cdot v + a_0 \cdot v\\ &= P(X) \cdot v.\end{aligned}$$

由此可知, V 上每一个 $K[X]$-模的结构都恰好有某个 $T \in \mathrm{End}_K(V)$ 使得上述关系成立. $\square$