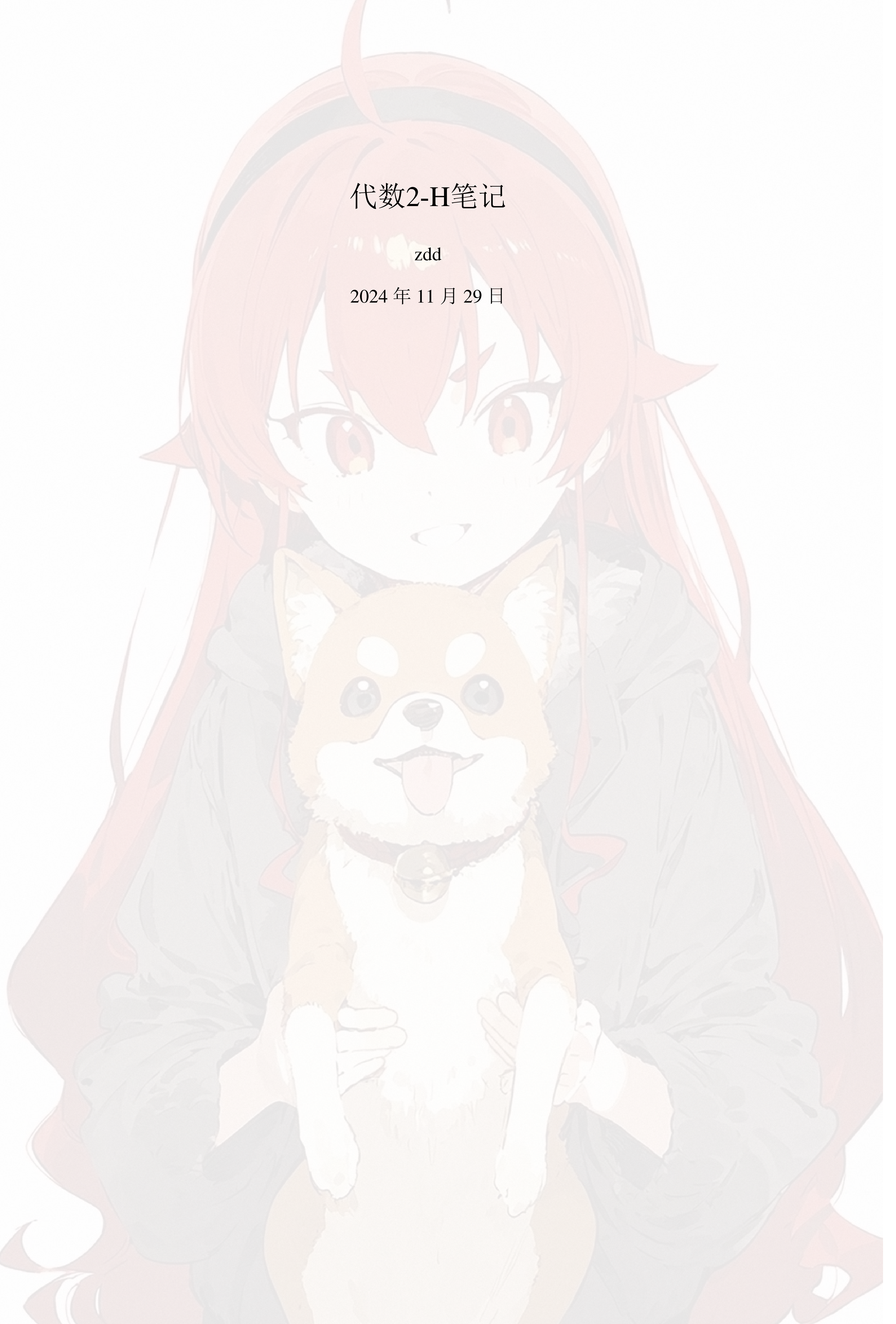
代数2-H笔记

zdd

2024 年 11 月 29 日



目录

1 域

1.1 域扩张

定义 1.1

$(F,+,\cdot)$ 称为**域(field)**，若满足：

- $a+b=b+a, a\cdot b=b\cdot a$;
- $(a+b)+c=a+(b+c),(a\cdot b)\cdot c=a\cdot(b\cdot c)$;
- $(a+b)\cdot c=a\cdot c+b\cdot c$;
- $\exists 0\in F,\forall a\in F,0+a=a$;
- $\exists 0\neq 1\in F,\forall a\in F,1\cdot a=a$;
- $\forall a\in F,\exists -a\in F,a+(-a)=0$;
- $\forall a\neq 0,\exists a^{-1}\in F,a\cdot a^{-1}=1$.

定义 1.2

E 是一个域，F 称为 E 的**子域(subfield)**，若 $F\subset E$，且对 E 中的运算构成域。称 E 是 F 的一个**扩张(extension)**。

设 F 是域，考虑自然同态 $f:\mathbb{Z}\to F$，则 $\ker f$ 为 (0) 或一个素理想 (p)。

若 $\ker f=(0)$，称 F 的**特征**是 0 且有嵌入映射 $\mathbb{Q}\to F$，称 $\mathbb{Q}$ 是 F 的素子域。

若 $\ker f=(p)$，称 F 的**特征**是 p 且有嵌入映射 $\mathbb{Z}/p\mathbb{Z}\to F$，称 $\mathbb{Z}/p\mathbb{Z}$ 是 F 的素子域。

定义 1.3

设有域扩张 E/F，$S\subset E$，记 $F(S)$ 为由 F 与 S 生成的子域，那么 $F(S)/F$ 是一个域扩张。若 S 只含一个元素 u，我们称 $F(u)$ 是 F 的一个**单扩张(simple extension)**，称 u 为 $F(u)$ 的**本原元(primitive element)**。

$u\in E$，考虑 $F(u)=\left\{\frac{f(u)}{g(u)}\middle| f,g\in F[x],g(u)\neq 0\right\}$。

我们有同态 $f:F[x]\to E,f(x)\mapsto f(u),f|_F=id_F$。由于 $F(u)$ 是一个域，故 $\ker f=(0)$ 或 $(g(x))$，其中 $g(x)$ 是不可约多项式。

若 $\ker f=(0)$，则 $F[x]\cong F[u]$；若 $\ker f=(g(x))$，则 $F(u)\cong F[u]\cong F(x)/(g(x))$。

定义 1.4

$u\in E$，若不存在 $h(x)\in F[x],h(u)=0$，则称 u 是 F 上的**超越元(transendental element)**，否则称为**代数元(algebraic element)**。若首一的不可约多项式 $g(x)$ 使 $g(u)=0$，则称之为 u 的极小多项式。

命题 1.1 (Kronecker's theorem)

F 是一个域，$h(x)\in F[x]$，则存在域扩张 E/F 使得 $h(x)$ 在 E 上有根。

证明. 不妨设 $h(x)$ 是不可约多项式，则 $F[x]/(h(x))$ 是满足条件的域扩张。 □

定义 1.5

设 E/F 是域扩张，若对 $\forall u \in E$ 均为代数元，则称 E/F 是**代数扩张(algebraic extension)**。否则称为**超越扩张(transendental extension)**。

定义 1.6

设 E/F 是域扩张，我们可以将 E 视作 F 上的线性空间，我们将这个线性空间的维数称作 E/F 的**度数(degree)**，记作 $[E:F]$。

若 $[E:F]=2, E=F(\alpha)$，则存在 $a,b,c \in F, a\alpha^2+b\alpha+c=0$。由于 $\alpha \notin F$，故 $a \neq 0$。不妨 $a=1.x^2+bx+c$ 是 α 的极小多项式。假设 $\mathrm{char}F \neq 2$，则 $(\alpha+b/2)^2=b^2/4-c \in F$。设 $\alpha'=\alpha+b/2$，则

$$E=F(\alpha)=F(\alpha'), {\alpha'}^2 \in F$$

命题 1.2

E/F 是域扩张，代数元 $u \in E$ 极小多项式为 $g(x)$，则 $[F(u):F]=\deg g$。进一步若 $[F(u):F]<\infty$，则 u 是 F 上代数元。

证明. 设 $n=\deg g$，则 $F(u) \cong F[x]/(g(x)) = F(1,x,\cdots,x^{n-1})$，故 $[F(u):F]=n=\deg g$。

进一步设 $[F(u):F]=n$，则存在 $a_0,\cdots,a_n \in F$，$a_0+a_1u+\cdots+a_nu^n=0$，故 u 是 F 上代数元。 □

推论 1.1

有限扩张都是代数扩张。

设域扩张 E/F，域 K 满足 E/K 和 K/F 都是域扩张，则称 K 为 E/F 的**中间域(intermediate field)**。

定理 1.1

设域扩张 $E/K/F$，则 E/F 是有限扩张当且仅当 E/K 和 K/F 均为有限扩张。事实上，$[E:F]=[E:K][K:F]$。

证明. “$\Longrightarrow$” 是显然的。

“$\Longleftarrow$”：设 E/K 和 K/F 都是有限扩张。取 K/F 的一组基 $u_1,\cdots,u_n$ 与 E/K 的一组基 $v_1,\cdots,v_n$，则 $\forall a \in E$，

$$\begin{aligned} a &= \sum_{i=1}^{m} a_i v_i, a_i \in K \\ &= \sum_{i=1}^{m} v_i \cdot \sum_{j=1}^{n} b_{i,j} u_j, b_{i,j} \in F \\ &= \sum_{i,j} b_{i,j} v_i u_j, b_{i,j} \in F \end{aligned}$$

即 E 是由 $\{v_i u_j\}$ 生成的，且线性不相关。因此

$$[E:F]=mn=[E:K][K:F]$$

□

推论 1.2

设域扩张 $E/K/F$，$[E:F]<\infty$，则 $[E:F]$ 被 $[E:K]$ 与 $[K:F]$ 整除。特别的，若 $[E:F]$ 是素数，则 $K=E$ 或 $K=F$。

定理 1.2 (Steinitz's theorem)

E/F 是一个有限域扩张，则 E/F 是单扩张当且仅当它只有有限个中间域。

证明. "$\Longrightarrow$"：设 $E=F(u)$，K 是中间域，则 $E=K(u)$。设 u 在 K 上的极小多项式是 $g(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_0, a_i\in K$。

令 $K'=F(a_0,a_1,\cdots,a_{n-1})\subset K$，$g'(x)$ 是 u 在 K' 上的极小多项式。

则 $g'(x)\mid g(x)$ 且

$$[E:K']=\deg g'(x)\le \deg g(x)=[E:K]\le[E:K']$$

于是我们有 $g'(x)=g(x), K=K'$。

设 $h(x)$ 是 u 在 F 上的极小多项式，则 $g(x)\mid h(x)$。注意到 K 由 g 唯一确定且 g 仅有有限个选择，因此 K 也只有有限个。

"$\Longleftarrow$"：我们先证明如下引理：

引理 1.1

$[E:F]<\infty$ 当且仅当 $E=F(u_1,\cdots,u_n)$，其中 u_i 是 F 上的代数元。

引理的证明. "$\Longleftarrow$"：

$$[E:F]=[F(u_1):F][F(u_1,u_2):F(u_1)]\cdots[E:F(u_1,\cdots,u_{n-1})]<\infty$$

"$\Longrightarrow$"：取 $u\notin F$，$[F(u):F]\le[E:F]<\infty$，故 u 是 F 上代数元。考虑 $E/F(u)$，有 $[E/F(u):F]<[E:F]$，归纳得 $E/F(u)=F(v_1,\cdots,v_m)$ 对某个 m，故 $E=F(u,v_1,\cdot,v_m)$。 □

□

1.2 代数扩张

定理 1.3

设域扩张 $K/E/F$，则 K/F 是代数扩张当且仅当 K/E 和 K/F 是代数扩张。

证明. “$\Longrightarrow$” 是显然的。

“$\Longleftarrow$”: 对 $u \in K$，设 $g(x) = x^n + a_1 x^{n-1} + \cdots + a_0 \in E[x]$ 是 a 的极小多项式，则 u 是 $F(a_0, \cdots, a_{n-1})$ 上的代数元，故

$$\begin{aligned}[F(u):F] &\leq [F(u, a_0, \cdots, a_{n-1}):F] \\ &= [F(u, a_0, \cdots, a_{n-1}):F(a_0, \cdots, a_{n-1})][F(a_0, \cdots, a_{n-1}):F] < \infty\end{aligned}$$

故 u 是 F 上的代数元。 □

定理 1.4

设域扩张 E/F，$K \subset E$ 是 E 中所有代数元构成的集合，则 K 是域。

证明. 对代数元 $\alpha, \beta \in K$，$F(\alpha, \beta)/F(\alpha)/F$ 是代数的，故 $F(\alpha, \beta)/F$ 是代数的。

即 $\alpha \pm \beta, \alpha \cdot \beta, \alpha^{-1}, \beta^{-1}$ 在 F 中都是代数元，进而 K 是域。 □

取 $E = \mathbb{R}$，$F = \mathbb{Q}$。注意到 $x^n - 2$ 在 $\mathbb{Q}$ 上不可约，取 $z = 2^{1/n}$，则

$$[K:\mathbb{Q}] \geq [\mathbb{Q}(z):\mathbb{Q}] = n$$

由 n 的任意性，$[K:\mathbb{Q}] = \infty$。

推论 1.3

若 u 是 K 上的代数元，则 $u \in K$。

证明. $K(u)/K/F$ 是代数扩张，所以 $K(u)/F$ 是代数扩张，这表示 u 是 F 上的代数元。 □

定义 1.7

设域扩张 E/K，若不存在域扩张 $E/K'/K$ 使得 K'/K 是代数扩张且 $K' \neq K$，则称 K 在 E 中是**代数封闭的(algebraically closed)**。

若 $E/K/F$ 满足 K 在 E 中是代数封闭的且 K/F 是代数扩张，则称 K 是 F 在 E 中的**代数闭包(algebraic closure)**。

事实上，$K = \left\{x \in E \middle| x是F上代数元\right\}$。

定义 1.8

K 是域，若 K 没有非平凡代数扩张，则称 K 是**代数封闭的**。

例 1.1

$\mathbb{R}$ 在 $\mathbb{C}$ 中的代数闭包是 $\mathbb{C}$。

设 K 是 $\mathbb{Q}$ 在 $\mathbb{R}$ 上的代数闭包，则 K 在 $\mathbb{R}$ 中是代数封闭的，在 $\mathbb{C}$ 中不是。

F 在 $F(t)/F$ 中是代数封闭的。

定义 1.9

F 是域，若 K/F 是代数扩张且 K 是代数封闭的，则称 K 是 F 的代数闭包。

定理 1.5

K 是域，则以下命题等价：

- K 是代数封闭的；
- $K[x]$ 中任一不可约多项式的次数等于 1；
- $K[x]$ 中任一次数大于零的多项式可分解为一次因子的乘积；
- $K[x]$ 中任一次数大于零的多项式都在 K 中至少有一个根。

定理 1.6

K 是代数封闭的，$F \subset K$ 是子域，则 F 在 K 中的代数闭包 $\bar{F}$ 是代数封闭的，即 $\bar{F}$ 是 F 的代数闭包。

证明. 设 $K'/\bar{F}$ 是代数扩张，$u \in K'$ 的极小多项式是 $g(x) \in \bar{F}[x]$。因为 $g(x) \in K[x]$，故 $g(x) = (x - x_1)\cdots(x - x_n), x_i \in K$。$x_i$ 是 $\bar{F}$ 上的代数元，故 $x_i \in \bar{F}$。而 u 又是其中一个 x_i，故 $u \in \bar{F}$，即 $K' = \bar{F}$。 □

定理 1.7

任一域 F 在同构意义下有唯一的代数闭包。

定义 1.10

域扩张 E/F，设 $\mathrm{End}(E/F)$ 为所有同态 $\varphi : E \to E$ 且 $\varphi|_F = id_F$ 组成的集合，$\mathrm{Aut}(E/F)$ 为所有同构 $\varphi : E \to E$ 且 $\varphi|_F = id_F$ 组成的集合。

命题 1.3

若 E/F 是代数扩张，则 $\mathrm{End}(E/F) = \mathrm{Aut}(E/F)$。

证明. 设 $\varphi \in \mathrm{End}(E/F)$。设 $u \in E$ 的极小多项式 $g(x)$，则 $\varphi(g(x)) = g(x)$。设 S 是 $g(x)$ 根的集合，则 $\varphi(S) \subset S$。由于两个域之间的任一非零同态都是单的，故 $\varphi(S) = S$，即 φ 是满射，故是同构。 □

1.3 尺规作图

在本节中我们讨论尺规作图问题。

记 $L(x,y)$ 为过两点 x 和 y 的直线，$C(x,r)$ 为以点 x 为圆心，长度 r 为半径的圆。

开始尺规作图之前，我们在平面上有 n 个点 $z_1,z_2,\ldots,z_n\in\mathbb{R}^2\cong\mathbb{C}$，其中 $z_1=(0,0),z_2=(0,1)$，即我们有了原点和单位长度。

令 $S_1=\{z_1,\ldots,z_n\}$。我们在 S_i 上通过如下规则作出 S_{i+1}：

- 添加两直线的交点 $L(x,y)\cap L(x',y')$；
- 添加两圆的交点 $C(x,|y-z|)\cap C(x',|y'-z'|)$；
- 添加直线与圆的交点 $L(x,y)\cap C(x',|y'-z'|)$。

于是有 $S_1\subset S_2\subset\ldots$ 并且 $S=\bigcup\limits_{i=1}^{\infty}S_i$ 是所有能用尺规作图作出来的点构成的集合。

显然 $\frac{1}{2^n}\mathbb{Z}[i]\subset S$，即 S 在 $\mathbb{C}$ 中是稠密的。

定理 1.8

我们有如下命题：

- $S\supset z_1,\cdots,z_n$ 是 $\mathbb{C}$ 的子域；
- $\forall a\in S$，我们有 $\bar{a}\in S$ 与 $\sqrt{a}\in S$；
- S 是 $\mathbb{C}$ 的满足如上条件的最小子域。

证明. 我们已经熟知如何用尺规作图对线段长度进行加减乘除与开根，以及对角进行加减与平分，故前两者是显然的。对于最后一个命题，设 F 是 C 的满足条件的子域，可以通过归纳验证 $S_i\subset F$。 □

定义 1.11

称 S 中的点是$z_1,\ldots,z_n$ **尺规导出的(constructible)**

定义 1.12

对于 $\mathbb{C}$ 的子域 F，一个域扩张 E/F 称为 F 上的**平方根塔(square root tower)**，若 E 形如 $F(u_1,\ldots,u_n)$ 并且 $u_i^2\in F(u_1,\ldots,u_{i-1})$。

进而我们可以看到 $[F(u_1,\ldots,u_i):F(u_1,\ldots,u_{i-1})]=1$ 或 2，所以 $[E:F]=2^k$ 对于某个正整数 k。

定理 1.9

给定 n 个点 $z_1,\ldots,z_n\in\mathbb{C}$，$F=\mathbb{Q}(z_1,\ldots,z_n,\bar{z}_1,\ldots,\bar{z}_n)$。则 $z\in\mathbb{C}$ 是尺规导出的当且仅当 z 被包含在 F 上的一个平方根塔里。

证明. 设 T 是平方根塔的集合。

一方面，容易验证 T 同 S 一样满足上述条件，故 $S \subset T$。

另一方面，通过归纳容易验证 T 中的点都是尺规导出的，故 $T \subset S$。

因此 $S = T$，得证。 □

推论 1.4

若 z 是尺规导出的，那么 z 是代数数，且若 $g(x)$ 是 z 在 F 上的极小多项式，则 $\deg g(x) = 2^k$，对于某个正整数 k。

例 1.2 (尺规作图三大问题)

倍立方问题：取 $F = Q, z = \sqrt[3]{2}$，z 在 F 上的极小多项式是 $g(x) = x^3 - 2$，$\deg g(x) = 3 \neq 2^k$，故不是尺规导出的。

三等分角问题：取 $F = Q, z = e^{i\pi/9}$，z 在 F 上的极小多项式是 $g(x) = x^3 - \frac{3}{4}x - \frac{1}{8}$，$\deg g(x) = 3 \neq 2^k$，故 $\frac{\pi}{3}$ 不能被三等分，更不用说一般的角了。

倍立方问题：取 $F = Q, z = \pi$，z 在 F 上不是代数元，自然不是尺规导出的。

1.4 分裂域

定义 1.13

f 是 F 上的首一多项式，域扩张 E/F 满足：存在 $r_1, \cdots, r_n \in E$，$f(x) = (x-r_1)\cdots(x-r_n)$ 且 $E = F(r_1, \cdots, r_n)$，则称 E 是 F 的**分裂域(splitting field)**。此时称 E 是多项式 $f(x)$ 的分裂域。

引理 1.2

我们有如下命题：

- 若 E 是 $f(x) \in F(x)$ 的分裂域，则 $[E:F] < \infty$；
- 域扩张 $E/K/F$，E/F 是 $f(x) \in F[x] \subset E[x]$ 的分裂域，则 E/K 是 $f(x)$ 的分裂域。

定理 1.10

$F[x]$ 中任一非零首一多项式均有分裂域。

证明. 对 f 的度数归纳。假设 f 在 F 上不可分，则存在不可约多项式 $g(x)$，$g(x) \mid f(x)$，$\deg g \geq 2$。由 Kronecker's theorem，存在域扩张 K/F 使得 $g(x) = (x-r_1)g'(x) \in K[x]$，则 $f(x) = (x-r_1)f'(x) \in K[x]$。由归纳假设知 $h(x)/K$ 有分裂域 E，则 E 是 $f(x)/F$ 的分裂域。 □

接下来我们想要证明分裂域在同构意义下是唯一的。

引理 1.3

$\eta : F \to F'$ 是域同构，则存在唯一的同构 $\tilde{\eta} : F[x] \cong F'[x]$。对不可约多项式 $g[x] \in F[x], g'(x) = \tilde{\eta}(g(x)) \in F'[x]$，存在唯一的同构 $\bar{\eta} : F[x]/(g(x)) \cong F'[x]/(g'(x))$ 且下图是交换的。

$$\begin{array}{llcl}
\eta : & F & \xrightarrow{\cong} & F' \\
& \downarrow & & \downarrow \\
\tilde{\eta} : & F[x] & \xrightarrow{\cong} & F'[x] \\
& \downarrow & & \downarrow \\
\bar{\eta} : & F[x]/(g(x)) & \xrightarrow{\cong} & F'[x]/(g'(x))
\end{array}$$

引理 1.4

$\eta : F \to F'$ 是同构，$E/F, E'/F'$ 是域扩张，E/F 的代数元 u 的极小多项式为 $g(x)$，令 $g'(x) = \eta(g(x))$，则存在 $\eta' : F(u) \to E'$ 使得下图交换：

$$\begin{array}{llcl}
\eta : & F & \xrightarrow{\cong} & F' \\
& \downarrow & & \downarrow \\
\eta' : & F(u) & \longrightarrow & E'
\end{array}$$

当且仅当 $g'(x)$ 在 E' 中有根。这样的扩张的个数与 $g'(x)$ 在 E' 中的根个数相同。

证明. “$\Longrightarrow$”：$g(u)=0$，故 $g'(\eta'(u))=\eta(g(\eta'(u)))=0$，即 $\eta'(u)$ 是 $g'(x)$ 在 E' 上的根。

“$\Longleftarrow$”：设 u' 是 $g'(x)$ 的任一根，由**引理 1.3**知我们知道下图交换：

$$\begin{tikzcd}
\eta: & F \arrow[rr, "\cong"] \arrow[d] & & F' \arrow[d] \\
\bar{\eta}: & F(u)\cong F[x]/(g(x)) \arrow[r, "\cong"] \arrow[rr, "\eta'"'] & F(u')\cong F[x]/(g'(x)) \arrow[r, phantom] & \\
& & & E'
\end{tikzcd}$$

$$\begin{tikzcd}
F \arrow[rr, "\cong"] \arrow[d] & & F' \arrow[d] \\
F(u)\cong F[x]/(g(x)) \arrow[r, "\cong"] \arrow[drr, "\eta'"] & F(u')\cong F[x]/(g'(x)) \arrow[d] & \\
& E' &
\end{tikzcd}$$

$\tilde{\eta}$ 与 η' 有一一对应，故 η' 存在且唯一。对于 $g'(x)$ 任一根对应的 η' 均不同，故这样的扩张的个数与 $g'(x)$ 在 E' 中的根个数相同。 □

定理 1.11

$\eta:F\to F'$ 是同构，$f(x)\in F[x], f'(x)=\tilde{\eta}(f(x))\in F'[x]$，$E/F$ 和 E'/F' 分别是 f/F 与 f'/F' 的分裂域，则有同构 $E\to E'$ 使得下图交换：

$$\begin{tikzcd}
F \arrow[r, "\eta"] \arrow[d] & F' \arrow[d] \\
E \arrow[r, "\cong"] & E'
\end{tikzcd}$$

进一步，这样的扩张个数不超过 $[E:F]$，取等当且仅当 $f'(x)$ 在 E' 中没有重根。

证明. 对 $[E:F]$ 归纳。设 $u\in F$ 的极小多项式为 $f(x)$ 的一个不可约因式 $g(x)$，$\deg g\geq 2$。由引理

$$\begin{aligned}
\#\{同构\eta_u:F(u)\to F'(u')\}&=\#\{g'(x)=\tilde{\eta}(g(x))的根\}\\
&\leq \deg g=[F(u):F]
\end{aligned}$$

考虑 E 和 E' 是 $f(x)/F(u)$ 和 $f'(x)/F'(u')$ 的分裂域。由归纳假设，对任意 η_u 存在至多 $[E:F(u)]$ 个扩张，取等当且仅当 $f'(x)\in F'(u')[x]$ 在 E' 上无重根。故扩张的总数至多 $[F(u):F][E:F(u)]=[E:F]$ 取等当且仅当 f' 在 E' 上无重根。

$$\begin{tikzcd}
F \arrow[r, "\eta"] \arrow[d] & F' \arrow[d] \\
F(u) \arrow[r, "\eta_u"] \arrow[d] & F'(u') \arrow[d] \\
E \arrow[r, "\cong"] & E'
\end{tikzcd}$$

□

推论 1.5

E/F 是 $f(x)\in F[x]$ 的分裂域，则

$$|\mathrm{Aut}_F(E)|\leq [E:F]$$

取等当且仅当 $f(x)$ 没有重根。

定理 1.7 的证明. 存在性：考虑

$$R = F[\{x_f\}_{f\in F[x]}] = \bigcup_{\substack{n\in\mathbb{N}^+ \\ \forall\{f_i\}_{i=1}^n\subset F[x]}} F[x_{f_1},\cdots,x_{f_n}]$$

设 I 是由 $\left\{f(x_f)\middle|f(x)\in F[x]\right\}$ 生成的理想。我们断言 $I\neq R$，故可以取极大理想 $\mathfrak{m}\supseteq I$。事实上，若 $I=R$，则存在 $g_1,\cdots,g_n\in R, f_1,\cdots,f_n\in F[x]$ 使得

$$1 = g_1\cdot f_1(x_{f_1})+\cdots+g_n\cdot f_n(x_{f_n})$$

由 Kronecker's theorem，存在域扩张 K/F 使得 $f_i(x)$ 在 K 中有根 $a_i, i=1,\cdots,n$，则我们取 $x_{f_i}=a_i$ 就有 $1=g_1\cdot f_1(a_1)+\cdots+g_n\cdot f_n(a_n)=0$，矛盾！

令 $E_1=R/\mathfrak{m}$ 是一个域，对 $f(x)\in F[x], f(\overline{x_f})=0\in E_1$。故 E_1 是 F 的代数扩张，则任意 $f\in F$ 均有一根在 E_1 中。

继续这个过程，我们得到了一列代数扩张：

$$F\to E_1\to E_2\to\cdots$$

令 $E=\bigcup_{n=1}^\infty E_i$，则 E/F 是代数扩张。对任意 $f(x)\in E[x]$，设 $f(x)\in E_n[x]$，则 f 在 $E_{n+1}\subset E$ 中有根，即 E 是代数闭的，这表示 E 是 F 的一个代数闭包。

唯一性：设 $\bar{F}/F, \bar{F}'/F$ 是 F 两个代数闭包。定义

$$S=\left\{(K,\varphi_K)\middle|\bar{F}/K/F, \varphi: K\to\bar{F}', \varphi|_F = id_F\right\}$$

首先 $(F, id_F)\in S$ 故 $S\neq\emptyset$。我们定义序关系 $(K,\varphi_K)\le(K',\varphi_{K'})$ 当且仅当 $K\subset K'$ 且 $\varphi_K=\varphi_{K'}|_K$，这是一个偏序关系。对于升链 $(K_1,\varphi_{K_1})\le(K_2,\varphi_{K_2})\le\cdots$ 有上界 $(\cup K_i, \lim\limits_{i\to\infty}\varphi_{K_i})$。由 Zorn 引理，我们知道 S 中存在极大元 (E,φ_E)。

若 $E\neq\bar{F}$，取 $u\in\bar{F}\setminus E$，我们有下图交换：

$$\begin{tikzcd} E(u') \arrow[r] & \bar{F}' \\ E \arrow[u] \arrow[ur, "\varphi_E"'] & \end{tikzcd}$$

矛盾！故 $E=\bar{F}$，我们有单射 $\varphi:\bar{F}\to\bar{F}'$，同样有单射 $\bar{F}'\to\bar{F}$，这表示 $\bar{F}\cong\bar{F}'$。 □

推论 1.6

设 $\tau: F\to E$，E 是代数封闭的，K/F 是代数扩张，则存在 $\varphi: K\to E$ 使得下图交换：

$$\begin{tikzcd} K \arrow[r, "\varphi"] & E \\ F \arrow[u] \arrow[ur, "\tau"'] & \end{tikzcd}$$

推论 1.7

$E=F(a_1,\cdots,a_n)$ 是代数扩张，则 $\left|\mathrm{Hom}_F(E,\bar{F})\right|\leq[E:F]$ 取等当且仅当所有 a_i 的极小多项式 $g_i(x)$ 都没有重根。

证明. 注意到

$$\left|\mathrm{Hom}_F(F(a_1),\bar{F})\right|=\#\left\{g_1(x)\text{在}\bar{F}\text{中的根}\right\}\leq[F(a_1):F]$$

取等当且仅当 $g_1(x)$ 无重根。固定 $\eta_1\in\mathrm{Hom}_F(F(a_1),\bar{F})$，同样有

$$\left|\mathrm{Hom}_{F(a_1)}(F(a_1,a_2),\bar{F})\right|\leq[F(a_1,a_2):F(a_1)]$$

故 $\left|\mathrm{Hom}_F(F(a_1,a_2),\bar{F})\right|\leq[F(a_1,a_2):F]$。继续下去就完成了证明。

$$\begin{tikzcd}
F \arrow[r] \arrow[d] & \bar{F} \\
F(a_1) \arrow[ur, "\eta_1"] \arrow[d] & \\
F(a_1,a_2) \arrow[uur, "\eta_2"] \arrow[d] & \\
\vdots \arrow[d] & \\
E \arrow[uuuur, "\eta"'] &
\end{tikzcd}$$

□

1.5 可分扩张

定义 1.14

域 F，$f(x) \in F[x]$ 称为**可分多项式(separable polynomial)**若 $f(x)$ 的每个不可约因子在 $f(x)$ 的分裂域中均无重根。

定义 1.15

域扩张 E/F，代数元 $u \in E$ 的极小多项式是可分多项式，则称 u 是 F 上的**可分元**。

定义 1.16

若 E/F 是代数扩张且 E 中每个元都是 F 上的可分元，则称 E 是 F 上的**可分扩张**。

定理 1.12

若 E/F 是代数扩张，则如下命题等价：

- E/F 是可分扩张；
- $E = F(\{a_i\}_{i \in I})$，其中 a_i 是 F 上的可分元；
- 若 $[E : F] < \infty$，我们有 $\left|\mathrm{Hom}_F(E, \bar{F})\right| = [E : F]$。

证明. (1) $\Longrightarrow$ (2) 是显然的。(2) $\Longrightarrow$ (3) 由**推论 1.7**即得。

(3) $\Longrightarrow$ (1)：对于代数元 u 的极小多项式 $g(x)$，我们有下图交换：

$$\begin{tikzcd} F \arrow[r] \arrow[d] & \bar{F} \\ F(u) \arrow[ur] \arrow[d] & \\ E \arrow[uur] & \end{tikzcd}$$

则

$$\left|\mathrm{Hom}_F(E, \bar{F})\right| \leq [E : F(u)] \cdot \#\left\{g(x)\text{在}\bar{F}\text{中的根}\right\} \leq [E : F]$$

故

$$\#\left\{g(x)\text{在}\bar{F}\text{中的根}\right\} = [F(u) : F]$$

即 $g(x)$ 无重根。 □

推论 1.8

若 E 是 $f(x)$ 的分裂域，则 E/F 是可分的 $\Longleftrightarrow$ $f(x)$ 是可分的 $\Longleftrightarrow$ $\mathrm{Aut}_F(E) = [E : F]$。

命题 1.4

域扩张 $E/K/F$，则 E/F 是可分的当且仅当 $E/K, K/F$ 是可分的。

证明. “$\Longrightarrow$” 是显然的。

“$\Longleftarrow$”：$\forall u\in E$，设 u 在 K 上的极小多项式为 $u^n+k_{n-1}u^{n-1}+\cdots+k_0=0$。则 u 在 $F(k_0,\cdots,k_{n-1})$ 上可分。注意到

$$\begin{aligned}\left|\mathrm{Hom}_F(F(k_0,\cdots,k_{n-1}),\bar{F})\right| &= [F(u,k_0,\cdots,k_{n-1}):F(k_0,\cdots,k_{n-1})][F(k_0,\cdots,k_{n-1}):F] \\ &= [F(u,k_0,\cdots,k_{n-1}):F]\end{aligned}$$

故 $F(u,k_0,\cdots,k_{n-1})$ 是可分的，这表示 u 是可分的，即 E/F 是可分的。 □

定义 1.17

域扩张 $E/K/F,E/K'/F$，记 K 和 K' 的**复合** KK' 为包含 K 和 K' 的 E 的最小子域。

代数(可分)扩张的复合还是代数(可分)扩张。

我们想知道哪些多项式是可分的。

定义 1.18

设 $f(x)=a_0+a_1x+\cdots+a_nx^n\in F[x]$，定义 f 的导数

$$f'(x)=a_1+2a_2x+\cdots+na_nx^{n-1}$$

当 $\mathrm{char}F=0$ 时，$f'(x)=0\Longleftrightarrow f(x)\in F$；

当 $\mathrm{char}F=p$ 时，$f'(x)=0\Longleftrightarrow f(x)=a_0+a_px^p+a_{2p}x^{2p}+\cdots=g(x^p)$。

定理 1.13

$f(x)\in F[x]$ 是可分的当且仅当 $(f(x),f'(x))=1$。

推论 1.9

$f\in F[x]$ 是首一不可约多项式，则若 $\mathrm{char}F=0$，$f(x)$ 总是可分的；若 $\mathrm{char}F=p$，f 可分当且仅当 $f(x)\neq g(x^p)$，$g(x)\in F[x]$。

进而特征为零的域都是可分的，下面我们考虑特征为 p 的域。我们在 F 上定义 Frobenius 同态：$\varphi:a\mapsto a^p$，记 $F^p=\mathrm{Im}\varphi$。

引理 1.5

x^p-a 是可约的当且仅当 $a\in F^p$。

证明. 若 $a\in F^p$，设 $a=b^p$，则 $x^p-a=(x-b)^p$ 可约。

若 x^p-a 可约，设 $x^p-a=f(x)g(x)$，考虑 x^p-a 的分裂域，则存在 $b\in E$，$b^p=a$，则 $x^p-a=(x-b)^p\in E[x]$，故 $f(x)=(x-b)^r\in E[x]$，其中 $0<r<p$。则 $b^r\in F$，由裴蜀定理我们可以得到 $b\in F$，即 $a\in F^p$。 □

定义 1.19

一个域 F 上任一多项式都是可分多项式，则称 F 是**完全域(complete)**。

由**推论 1.9**我们知道特征为零的域都是完全域。而对于特征为 p 的域，我们有如下定理：

定理 1.14

$\mathrm{char}F = p$，则 F 是完全域当且仅当 $F = F^p$。

证明. "$\Longrightarrow$"：若 F 是完全域，$\forall a \in F$ 且 $a \notin F^p$，考虑 $f(x) = x^p - a$，由**引理 1.5** 知 f 不是可分的，矛盾！故 $F = F^p$。

"$\Longleftarrow$"：若 $F = F^p$ 且 F 不是完全域，取不可分的不可约多项式 f，由**推论 1.9** 知 $f(x) = g(x^p) = \sum a_i x^{pi}$。由于 $F = F^p$，$a_i = b_i^p$，于是 $f(x) = (\sum b_i x^i)^p$，矛盾！ □

推论 1.10

有限域都是完备的。

证明. 由于 φ 是单射，我们有 $|F| \leq |F^p|$，即 $F = F^p$。 □

定义 1.20

域扩张 E/F，可以证明 E 中所有 F 上的可分元构成了 E 的一个子域，称为 F 在 E 中的**可分闭包(separable closure)**，记为 F^{sep}。

设 E/F 是代数扩张。若 $\mathrm{char}F = 0$，显然 $F^{\mathrm{sep}} = E$。

若 $\mathrm{char}F = p$，取 $u \in E \setminus F^{\mathrm{sep}}$，设 $g(x)$ 是 u 的极小多项式。由**推论 1.9** 我们有 $g(x) = g_1(x^p)$，$g_1(x)$ 是 u^p 的极小多项式。继续这个过程，若 $u^p \notin F^{\mathrm{sep}}$，我们可以继续构造 $g_2(x)$ 是 u^{p^2} 的极小多项式。这个过程最终会停止，即 $u^{p^n} \in F^{\mathrm{sep}}$ 对某个 $n > 0$。

定义 1.21

设 E/F 是代数扩张，称 $u \in E$ 是**完全不可分的(purely inseparable)**，若 $u^{p^n} \in F$ 对某个 $n > 0$。E/F 称为完全不可分的若 E 中每个元素都完全不可分。

由上面的讨论，E/F^{sep} 是完全不可分的。

设 E/F 是完全不可分的，取 $u \in E \setminus F$，设 u 在 F 上的极小多项式为 $g(x)$，设 n 是最小的正整数满足 $u^{p^n} \in F$，则 u 是 $x^{p^n} - u^{p^n} \in F[x]$ 的根，故 $g(x) \mid x^{p^n} - u^{p^n}$。

注意到 $x^{p^n} - u^{p^n} = (x-u)^{p^n}$，故 $g(x) = (x-u)^m = x^m - u^m$ 对某个 m，这表示 $u^m \in F$，进而 $u^{(m,p^n)} \in F$，由 n 的取法知 $m = p^n$。

这表示若 E/F 是完全不可分的且 $E \neq F$，则 E/F 是不可分的。

例 1.3

$\mathbb{Z}_p(t^{1/p})/\mathbb{Z}_p(t)$ 是完全不可分的。

定义 1.22

E/F 是代数扩张，$[F^{\mathrm{sep}}:F]$ 称作 E/F 的**可分次数(separable degree)**，$[E:F^{\mathrm{sep}}]$ 称作 E/F 的**不可分次数(inseparable degree)**。

命题 1.5

设 E/F 是有限扩张，则 $[E:F^{\mathrm{sep}}]=p^n$ 对某个 $n\geq 0$。特别的，若 E/F 是完全不可分的，$F=F^{\mathrm{sep}}$，故 $[E:F]=p^n$。

命题 1.6

若 $E/K, K/F$ 是完全不可分扩张，则 E/F 是完全不可分扩张。

证明. 对任意 $u\in E$，存在 m 使得 $u^{p^m}\in K$，则存在 n 使得 $(u^{p^m})^{p^n}\in F$，即 $u^{p^{m+n}}\in F$，故 u 是完全不可分的。 □

利用可分闭包我们可以推广**定理 1.12**：

命题 1.7

E/F 是有限扩张，则

$$\left|\mathrm{Hom}_F(E,\bar{F})\right|=[F^{\mathrm{sep}}:F]$$

证明. 即证对给定的 $\psi:F^{\mathrm{sep}}\to\bar{F}$，保持 F^{sep} 不变的扩张 $\varphi:E\to\bar{F}$ 是唯一的。

取 $u\in E\setminus F^{\mathrm{sep}}$，$u$ 是 $x^{p^i}-u^{p^i}$ 的根。故 $\varphi(u)$ 是 $x^{p^i}-\varphi(u^{p^i})=x^{p^i}-\psi(u^{p^i})$ 的根。

由于 $\psi(u^{p^i})\in\bar{F}$，故存在 $v\in\bar{F}, v^{p^i}=\psi(u^{p^i})$，则$x^{p^i}-\psi(u^{p^i})=(x-v)^{p^i}$，这表明 $\varphi(x)=v$。更进一步的，因为 $v_1^{p^i}-v_2^{p^i}=(v_1-v_2)^{p^i}$，故 v 是唯一的。

$$\begin{tikzcd}
F \arrow[r] \arrow[d] & \bar{F} \\
F^{\mathrm{sep}} \arrow[ur, "\psi"] \arrow[d] & \\
E \arrow[uur, "\varphi"'] &
\end{tikzcd}$$

□

推论 1.11

若 E/F 是完全不可分的，则 $\left|\mathrm{Hom}_F(E,\bar{F})\right|=1$。

1.6 正规扩张

引理 1.6

E/F 是 $f(x) \in F[x]$ 的分裂域，$u \in E$，$g(x)$ 是 u 的极小多项式，则 $g(x)$ 在 E 上可分。

证明. 设 K 是 $g(x)$ 在 E 上的分裂域，$r \in K$ 是 $g(x)$ 的一个根。我们有下图交换：

$$\begin{tikzcd} & F(u) \arrow[r] \arrow[d, "\varphi"] & E \arrow[d, "\tau"] \\ F \arrow[ur] \arrow[dr] & & \\ & F(r) \arrow[r] & E(r) \end{tikzcd}$$

这里 $\varphi : F(u) \to F(r), u \mapsto r$ 是同构，注意到 E 是 $f(x)$ 在 $F(u)[x]$ 上的分裂域，$E(r)$ 是 $\varphi(f(x)) \in F(r)[x]$ 的分裂域，故由**定理 1.11** 存在同构 $\tau : E \to E(r)$。故 $E(r) \cong E$，即 $r \in E$。 □

我们将分裂域推广：

定义 1.23

E/F 是代数扩张，E/F 称作正规扩张，若 F 上任意不可约多项式在 E 中或者无根或者根都在 E 中，则称 E 是 F 的正规扩张。

由**引理 1.6** 我们知道所有的分裂域都是正规的。

定理 1.15

E/F 是代数扩张，则如下命题等价：

- E/F 是正规的；
- 对任意 $\tau \in \mathrm{Hom}_F(E, \bar{F})$，$\tau(E) = E$；
- 嵌入映射 $\mathrm{End}_F(E) \to \mathrm{Hom}_F(E, \bar{F})$ 是一一对应的。

证明. (2) $\iff$ (3) 是显然的。

(1) $\implies$ (2)：设 $u \in E$ 的极小多项式为 $g(x)$，则 $\tau(g(u)) = g(\tau(u)) = 0$，故 $\tau(u)$ 是 $g(x)$ 的根。由于 E/F 是正规的，故 $\tau(u) \in E$，进而 $\tau(E) \subset E$，即 $\tau \in \mathrm{Hom}(E/F)$。由于 E/F 是代数的，由**命题 1.3** 知 $\tau \in \mathrm{Aut}(E/F)$，即 $\tau(E) = E$。

(2) $\implies$ (1)：设 $u \in E$ 的极小多项式为 $g(x)$，设 r 是 $g(x)$ 的另外一根。我们有下图交换：

$$\begin{tikzcd} & F(u) \arrow[r] \arrow[d, "\varphi"] \arrow[ddr] & E \arrow[dd, "\tau"] \\ F \arrow[ur] \arrow[dr] & & \\ & F(r) \arrow[r] & \bar{F} \end{tikzcd}$$

这里 φ 是同**引理 1.6** 定义的同构，由于 E 是 $F(u)$ 的代数扩张且 $\bar{F}$ 是 $F(u)$ 的代数闭包故 τ 存在。于是 $\tau(u)=\varphi(u)=r\in E$，这表示 $g(x)$ 在 E 上分裂，即 E/F 是正规的。 □

推论 1.12

- $E/K/F$ 是域扩张，若 E/F 是正规扩张，则 E/K 也是正规扩张。
- $E/K/F, E/K'/F$ 是域扩张，$K/F, K'/F$ 是正规扩张，则 KK'/F 也是正规扩张。

证明. (1)：由于 E/F 是正规的，由上定理对任意 $\tau\in\mathrm{Hom}_F(E,\bar{F}),\tau(E)=E$。因为 $\mathrm{Hom}_K(E,\bar{F})\subset\mathrm{Hom}_F(E,\bar{F})$，再次利用上定理，$E/K$ 是正规的。

(2)：注意到任意 $\tau\in\mathrm{Hom}_F(KK',\bar{F}),\tau\subset\mathrm{Hom}_F(K,\bar{F})\cap\mathrm{Hom}_F(K',\bar{F})$，故 $\tau(K')=K'$，进而 $\tau(KK')=KK'$，这表示 KK' 是正规的。 □

定理 1.16

- 一个有限扩张 E/F 是正规的当且仅当 E 是一个分裂域。
- 任一有限扩张被包含于一个正规扩张。

证明. (1)：“$\Longleftarrow$” 由**引理 1.6** 直接得出。“$\Longrightarrow$”：设 $E=F(u_1,\cdots,u_n)$，u_i 的极小多项式是 $g_i(x)$，则 E 是 $g_1(x)\cdots g_n(x)$ 的分裂域。

(2)：设 $E=F(u_1,\cdots,u_n)$，则 E 被 $g_1(x)\cdots g_n(x)$ 的分裂域包含，它是正规的。 □

定义 1.24

$K/E/F$ 是代数扩张，称 K 是 E/F 的正规闭包，若：

- K/F 是正规的。
- 若 $K/M/E$ 是域扩张且 M/F 是正规的，则 $K=M$。

命题 1.8

若 E/F 是有限扩张，设 $E=F(u_1,\cdots,u_n)$，u_i 的极小多项式是 $g_i(x)$，则 E/F 的正规闭包为 $g_1(x)\cdots g_n(x)$ 的分裂域并且在 F-同构意义下是唯一的。

例 1.4

$\mathbb{Q}(\sqrt{2})/\mathbb{Q},\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ 是正规的，但是 $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ 不是正规的，因为 x^4-2 在 $\mathbb{Q}$ 中不可约，x^4-2 在 $\mathbb{Q}(\sqrt[4]{2})$ 中有根但是不可分。由**命题 1.8** 知 $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ 的正规闭包是 $\mathbb{Q}(\sqrt[4]{2},\sqrt{-1})$

例 1.5

$\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q}$ 是 x^3-2 的分裂域，它是正规扩张，但是 $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ 不是正规的，因为 x^3-2 在其中有根但是不可分。

由上两例我们知道，域扩张 $E/K/F$，若 E/F 是正规的，K/F 不一定是正规的；若 $E/K,K/F$

是正规的，E/F 也不一定是正规的。这与正规子群的概念相似。我们将在后文中讲述这种相似的原因。

定义 1.25

E/F 是有限正规域扩张，$E/K/F$ 是域扩张，则 K/F 是正规的当且仅当 $\forall\sigma \in \mathrm{Aut}(E/F), \sigma(K) = K$。

证明. 证明同**定理 1.15**。 □

1.7 Galois 扩张

定义 1.26

一个有限正规可分域扩张 E/F 称为 **Galois 扩张**。

由我们前文的讨论，可以知道 E/F 是 Galois 扩张当且仅当它是一个可分多项式的分裂域。若 $\mathrm{char}F=0$，则 E/F 是 Galois 扩张当且仅当它是分裂域。

命题 1.9

$E/K/F$ 是有限扩张，若 E/F 是 Galois 扩张，则 E/K 也是 Galois 扩张。

定义 1.27

E/F 是域扩张，则 $\mathrm{Aut}(E/F)$ 有自然群结构，称为 E/F 的 Galois 群，记为 $\mathrm{Gal}(E/F)$。

回忆，若 E/F 是 Galois 扩张，则 $|\mathrm{Gal}(E/F)|=[E:F]$。更一般的，若 E/F 是分裂域，$E=F(u_1,\cdots,u_n)$，则 $\forall\sigma\in\mathrm{Gal}(E/F),\sigma(u_i)\in\{u_1,\cdots,u_n\}$，这表示我们有嵌入映射 $\mathrm{Gal}(E/F)\hookrightarrow S_n$。

命题 1.10

若 E/F 是有限扩张，则 $\mathrm{Gal}(E/F)$ 是有限的。

证明. 设 $E=F(u_1,\cdots,u_n)$，u_i 的极小多项式是 $g_i(x)$，则 $\forall\sigma\in\mathrm{Gal}(E/F)$，$\sigma(u_i)$ 是 $g_i(x)$ 的根，这样的选择是有限的。 □

定义 1.28

E 是域，G 是 $\mathrm{Aut}(E)$ 的有限子群。记

$$E^G=\left\{a\in E\middle|\sigma(a)=a,\forall\sigma\in G\right\}$$

易验证 E^G 是 E 的一个子域，称为 E 的 G **不变子域(G-invariant subfield)**。

定理 1.17

域扩张 E/F，则如下命题等价：

- E/F 是 Galois 扩张；
- E 是 F 上某个可分多项式的分裂域；
- $F=E^G$，其中 G 是 $\mathrm{Aut}(E)$ 的有限子群。

证明. (1) $\Longrightarrow$ (2) 由**定理 1.16** 即得。

(2) $\Longrightarrow$ (3)：我们来证 $F=E^G$，其中 $G=\mathrm{Gal}(E/F)$。我们先来证明如下引理：

引理 1.7

E/F 是有限扩张，则

$$\mathrm{Gal}(E/F)=\mathrm{Gal}(E/E^{\mathrm{Gal}(E/F)})$$

引理的证明. 一方面，$F\subseteq E^{\mathrm{Gal}(E/F)}$，故 $\mathrm{Gal}(E/F)\supseteq\mathrm{Gal}(E/E^{\mathrm{Gal}(E/F)})$。

另一方面，$\forall\sigma\in\mathrm{Gal}(E/F)$，由定义 $\sigma|_{E^{\mathrm{Gal}(E/F)}}=id$，则 $\sigma\in\mathrm{Gal}(E/E^{\mathrm{Gal}(E/F)})$，这表示 $\mathrm{Gal}(E/F)\subseteq\mathrm{Gal}(E/E^{\mathrm{Gal}(E/F)})$。 □

一方面我们显然有 $F\subseteq E^G$。另一方面，由上述引理 $\mathrm{Gal}(E/E^G)=\mathrm{Gal}(E/F)$。因为 E/F 是可分的，$|\mathrm{Gal}(E/F)|=[E:F]$，故 $\left|\mathrm{Gal}(E/E^G)\right|=[E:F]$。因为 $E/E^G/F$ 是域扩张，E/F 是可分的，我们有 E/E^G 是可分的，这表示 $\left|\mathrm{Gal}(E/E^G)\right|=[E:E^G]$。

综上 $E^G=F$。

(3) $\Longrightarrow$ (1)：我们先来证明如下引理：

引理 1.8 (Artin)

E 是域，G 是 $\mathrm{Aut}(E)$ 的有限子群，则 $[E:E^G]\leq|G|$。

引理的证明. □

由该引理，$[E:F]=[E:E^G]\leq|G|<\infty$。

$\forall u\in E$ 的极小多项式 $g(x)$，需要证明 $g(x)$ 在 E 中分裂且没有重根。设 $u_1,\cdots,u_n\in E$ 是 $g(x)$ 的所有不同根。令 $u=u_1,f(x)=(x-u_1)\cdots(x-u_n)$。

注意到对 $\forall\sigma\in G,\sigma(g(x))=g(x)$，故 $\sigma(\{u_1,\cdots,u_n\})=\{u_1,\cdots,u_n\}$，这表示 $\sigma(f(x))=f(x)$。由于 $F=E^G$，我们有 $f(x)\in F[x]$。$g(x)$ 在 F 上可分，故只能 $f=g$，即 $g(x)$ 在 E 上可分且没有重根。 □

推论 1.13

若 $G\leq\mathrm{Aut}(E)$，则 $\mathrm{Gal}(E/E^G)=G$ 且 $[E:E^G]=|G|$。

证明. 由**定理 1.17**，E/E^G 是 Galois 扩张，故 $[E:E^G]=\mathrm{Gal}(E/E^G)$。由 Artin's lemma $[E:E^G]\leq G$，但 $G\subseteq(E/E^G)$，故 $G=\mathrm{Gal}(E/E^G)$。 □

推论 1.14

E/F 是 Galois 扩张当且仅当 $F=E^{\mathrm{Gal}(E/F)}$。

证明. 令 $G=\mathrm{Gal}(E/F)$。一方面若 $F=E^G$，由**定理 1.17** E/F 是 Galois 扩张。另一方面，若 E/F 是 Galois 扩张，$[E:F]=|G|=[E:E^G]$，故 $F=E^G$。 □

推论 1.15

E/F 是有限扩张，则 $|\mathrm{Gal}(E/F)| \mid [E:F]$，取等当且仅当 E/F 是 Galois 扩张。

证明. $E/E^{\mathrm{Gal}(E/F)}/F$ 是域扩张，故

$$|\mathrm{Gal}(E/F)| = \frac{[E:F]}{[E^{\mathrm{Gal}(E/F)}:F]}$$

取等当且仅当 $E^{\mathrm{Gal}(E/F)} = F$，即$E/F$ 是 Galois 扩张。 □

例 1.6

- 考虑 Galois 扩张 $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$，则 $\left|\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})\right| = [\mathbb{Q}(\sqrt{2})/\mathbb{Q}] = 2$，故 $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \cong C_2$，这两个元素分别是 $\eta_1 = id$ 和 $\eta_2 : \sqrt{2} \to -\sqrt{2}$。
- $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ 是平凡群，即必须有 $\eta(\sqrt[3]{2}) = \sqrt[3]{2}$。
- 令 $\omega = e^{2\pi i/3}$，则 $x^3 - 2$ 的分裂域 $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$ 是 Galois 扩张。我们有 $[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] = 6$。注意到任意 $\eta \in \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$ 是 $\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$，故 $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}) \cong S_3$。
- 考虑 $(x^2-3)(x^2-2)$ 的分裂域 $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ 是 Galois 扩张，且 $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$。这四个元素是 $\eta : \sqrt{2} \to \pm\sqrt{2}, \sqrt{3} \to \pm\sqrt{3}$，故 $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) \cong C_2 \times C_2$。
- 考虑 $F = \mathbb{Z}_p(t)$，$f(x) = x^p - t$ 是不可分且不可约的，故 $f(x)$ 的分裂域 E/F 不是 Galois 的/事实上若 $u \in E$，$f(u) = 0$，则 $f(x) = (x-u)^p$，这表示任意 η，$\eta(u) = u$ 且 $E = F(u)$，这表示 $\mathrm{Gal}(E/F)$ 是平凡群。

1.8 Galois 对应

给定域扩张 E/F，$G=\mathrm{Gal}(E/F)$，令 $\Sigma=\left\{H \middle| H\leq G\right\}$，$\Omega=\left\{K \middle| E/K/F\right\}$。定义 $\varphi:\Sigma\to\Omega, H\mapsto E^H$，$\phi:\Omega\to\Sigma, K\mapsto \mathrm{Gal}(E/K)$。我们有如下基础推论：

- 若 $H_1\subset H_2$，则 $E^{H_1}\supset E^{H_2}$；
- 若 $K_1\subset K_2$，则 $\mathrm{Gal}(E/K_1)\supset \mathrm{Gal}(E/K_2)$；
- $H\subset \mathrm{Gal}(E/E^H)$；
- $K\subset E^{\mathrm{Gal}(E/K)}$。

现在我们来介绍**伽罗瓦理论基本定理(the fundamental theorem of Galois correspondence)**

定理 1.18

E/F 是 Galois 扩张，则如下命题成立：

- φ,ϕ 互为逆映射，即 $H=\mathrm{Gal}(E/E^H), K=E^{\mathrm{Gal}(E/K)}$；
- $H_1\subset H_2$ 当且仅当 $E^{H_2}\subset E^{H_1}$；
- $|H|=[E:E^H], [G:H]=[E^H:F]$；
- $H\lhd G$ 当且仅当 E^H/F 是正规扩张，这时还有 $\mathrm{Gal}(E^H/F)\cong G/H$。

证明. (1) 利用**推论 1.14** 和**推论 1.15**。

(2) 由(1)显然。

(3) 由**推论 1.14** 得$|H|=[E:E^H]$。进而

$$[G:H]=\frac{|G|}{|H|}=\frac{[E:F]}{[E:E^H]}=[E^H:F]$$

(4) 回忆 K/F 是正规的当且仅当 $\forall\eta\in\mathrm{Gal}(E/F),\eta(K)=K$。$H$ 是正规子群当且仅当 $\forall\eta\in\mathrm{Gal}(E/F),\eta H\eta^{-1}=H$，这等价于 $E^{\eta H\eta^{-1}}=E^H$，注意到：

$$x\in E^{\eta H\eta^{-1}}\iff \eta H\eta^{-1}x=x \overset{x=\eta(y)}{\iff} Hy=y\iff y\in E^H\iff x\in\eta(E^H)\Rightarrow E^{\eta H\eta^{-1}}=\eta(E^H)$$

故 H 正规$\iff\forall\eta\in\mathrm{Gal}(E/F),\eta(E^H)=E^H\iff E^H/F$ 是正规的。

接下来考虑 $\psi:G\to\mathrm{Gal}(E^H/F),\eta\mapsto\eta|_{E^H}$。由于 $\eta(E^H)=E^H$ 故是良定义的。$\ker\psi=\mathrm{Gal}(E/E^H)=H$。因为 E^H/F 是 Galois 扩张，$[G:H]=[E^H/F]=\mathrm{Gal}(E^H/F)$，故 ψ 是满射，进而 $G/H\cong\mathrm{Gal}(E^H/F)$，我们完成了证明。 □

推论 1.16

E/F 是有限可分扩张，则 E 是单扩张。

证明. 设 $E=F(u_1,\cdots,u_n)$，u_i 的极小多项式是 $g_i(x)$，考虑 $g_1(x)\cdots g_n(x)$ 的分裂域 E'，则 $E\subset E'$，且 E'/F 是 Galois 扩张。由 Galois 对应，E'/F 有有限的子域，则 E/F 也只有有限的子域。回忆Steinitz's theorem，我们完成了证明。 □

E' 被称为 E/F 的 **Galois 闭包(Galois closure)**。事实上，类似正规闭包的定义，我们可以对任一可分扩张 E/F 定义 Galois 闭包。

推论 1.17 (代数基本定理)

$\mathbb{C}$ 是代数闭的。

证明. $\forall f(x) \in \mathbb{C}[x]$，设 $g(x) = f(x)\bar{f}(x)\mathbb{R}[x]$，我们只需证 g 有一根。

设 g 的分裂域为 E，则 $E/\mathbb{R}$ 是 Galois 扩张。设 $n = [E : R]$，我们来证明 $n = 1$ 或 2。由 Sylow 定理，取 2-Sylow 子群 $H \leq \mathrm{Gal}(E/\mathbb{R})$。由于 $[G : H] = [E^H : \mathbb{R}]$ 是奇数，故 $E^H = \mathbb{R}(\alpha)$，其中 α 的极小多项式次数为奇数，即 $\alpha \in \mathbb{R}$，这表示 $E^H = \mathbb{R}$，故 $H = G$，$|G| = 2^k$。由于

$$G \supset G_1 \supset \cdots \supset G_k = 1$$

故

$$\mathbb{R} \overset{\deg 2}{\subset} E^{G_1} \overset{\deg 2}{\subset} \cdots \overset{\deg 2}{\subset} E^{G_k} = E$$

所以

$$\mathbb{C} \cong E^{G_k} = E^{G_2} = \cdots = E$$

即 $g(x)$ 在 $\mathbb{C}$ 上分裂，故 $\mathbb{C}$ 是代数闭的。

□

命题 1.11

设 $E/K, K/F$ 是 Galois 扩张，则有如下命题成立：

- EK/F 是 Galois 扩张；
- $\mathrm{Gal}(EK/K) \xrightarrow{\varphi} \mathrm{Gal}(E/E \cap K)$ 是同构，且 $[EK : E \cap K] = [EK : E][EK : K]$；
- $\mathrm{Gal}(EK/F) \xrightarrow{\phi} \mathrm{Gal}(E/F) \times \mathrm{Gal}(K/F)$ 是单射。当 $F = E \cap K$ 时是同构。

证明. (1)：EK/F 是一个可分多项式的分裂域。

(2)：$\eta \in \mathrm{Gal}(EK/K)$。若 $\eta \in \ker\varphi$，则 $\eta|_E = id$，进而 $\eta|_{EK} = id$，即 φ 是单射。$E^{\mathrm{Im}\varphi} = E \cap K$推出 $\mathrm{Im}\varphi = \mathrm{Gal}(E/E \cap K)$。

$$a \in E \subset EK, \mathrm{Im}\varphi(a) = a \iff a \in EK^{\mathrm{Gal}(EK/K)} = K \iff a \in E \cap K$$

故 $[EK : E \cap K] = [E : E \cap K][K : E \cap K] = [EK : K][EK : E]$

(3)：$\eta \in \ker\phi, \eta|_E, \eta|K = id$，故 $\eta|_{EK} = id$，即 ϕ 是单射。

若 $F = E \cap K$ 则 ϕ 是两个相同指数的有限集之间的单射，即 ϕ 是满射。 □

1.9 有限域

定理 1.19

$\forall n>0$，存在同构意义下唯一的域 F 满足 $|F|=p^n$

证明. 若 $|F|=p^n$，则 $\forall a\in F$，$a^{p^n}=a$，故 $x^{p^n}-x$ 在 F 上可分，即 F 是 $x^{p^n}-x/\mathbb{Z}_p$ 的分裂域，自然在同构意义下唯一。

下面我们来证明 $|F|=p^n$。由于 $\dfrac{\partial(x^{p^n}-x)}{\partial x}=-1$，故 $x^{p^n}-x$ 在 F 上无重根。记 K 是 f 在 F 中的所有根，则 $|K|=p^n$。考虑 Frobenius 自同构 φ，则 $K=F^{\varphi^n}$ 是 F 的子域，即 K 是指数为 p^n 的域。 □

Problem 1.1

可以通过计算得到 $\mathbb{Z}_p[x]$ 上的 n 次多项式中有不可约多项式

推论 1.18

E/F 是有限域的扩张，则 E/F 是 Galois 扩张。

证明. E/F 是分裂域，由于 F 有限，故 $F^p=F$，即 F 是完全域，进而 E/F 是 Galois 扩张。 □

定理 1.20

E/F 是有限域，$|F|=q,[E:F]=m$，则 $\mathrm{Gal}(E/F)\cong\mathbb{Z}_m$，即 $\mathrm{Gal}(E/F)$ 由 Frobenius 映射 η 生成。

证明. $E^*\cong\mathbb{Z}_{q^m-1}$，设 a 是 E^* 的生成元，$a^{q^m-1}=1$。设 $n=|\eta|$，则 $\eta^n(a)=a$，即 $a^{q^n-1}=1$，故 $q^n-1\geq q^m-1$，即 $n\geq m$。但 $n\leq m$，只能 $n=m$。即 $\mathrm{Gal}(E/F)=<\eta>$。 □

推论 1.19

$|E|=p^n$，E/F，$|F|=p^m$，则 $m\mid n$。

推论 1.20

$|E|=p^n$，$m\mid n$，则存在指数 p^m 的子域 $F\hookrightarrow E$，进而存在 $F[x]$ 中的 $\dfrac{n}{m}$ 次不可约多项式

1.10 分圆域

定义 1.29

$n \in \mathbb{Z}_{>0}$，$x^n - 1$ 在 F 上的分裂域称为 n 次**分圆域(cyclotomic field)**。

记 μ_n 是 $x^n - 1$ 所有根的集合。若 $\mathrm{char} F \nmid n$，则 $|\mu_n| = n$ 且 μ_n 是 F 的一个子群，进而 $\mu_n \cong \mathbb{Z}_n$。

定义 1.30

μ_n 的生成元称为**本原单位根(primitive roots of unity)**。

设 ξ 是本原单位根，$E = F(\xi)$。取 $\eta \in \mathrm{Gal}(E/F)$，$\eta$ 由 $\eta(\xi)$ 决定。于是我们有单同态：$\phi : \mathrm{Gal}(E/F) \to \mathrm{Aut}(\mu_n) \cong \mathrm{Aut}(\mathbb{Z}_n)$，由于 $\mathrm{Aut}(\mathbb{Z}_n)$ 是 Abel 群，故 $\mathrm{Gal}(E/F)$ 也是 Abel 群。于是我们有如下命题：

命题 1.12

E/F 是 n 次分圆域，则 $\mathrm{Gal}(E/F)$ 是 Abel 群。

定义 1.31

E/F 是 Galois 扩张，若 $\mathrm{Gal}(E/F)$ 是 Abel/循环群，则称 E/F 为 Abel/循环扩张。

设 $F = \mathbb{Q}$，E 是 F 上的 n 次分圆域，我们想要计算 $[E : F]$。

首先 $E = F(\xi_n)$，其中 $\xi_n = e^{2\pi i/n}$，令

$$\varphi_n(x) = \prod_{\substack{(k,n)=1 \\ 1 \le k \le n-1}} (x - \xi_n^k)$$

我们来证明 $\varphi_n(x)$ 是不可约整系数多项式。

注意到

$$x^n - 1 = \prod_{d|n} \prod_{\substack{(k,\frac{n}{d}) \\ 1 \le k \le \frac{n}{d}-1}} (x - \xi_n^{dk}) = \prod_{d|n} \varphi_{\frac{n}{d}}(x) = \prod_{d|n} \varphi_d(x)$$

对任意 $\eta \in \mathrm{Gal}(E/F)$，$\eta(\varphi_n(x)) = \varphi(x)$，故 $\varphi_n(x) \in \mathbb{Q}[x]$。

由于

$$x^n - 1 = \varphi_n(x) \prod_{d|n, d<n} \varphi_d(x)$$

故我们可以通过归纳证明 $\varphi_n(x) \in \mathbb{Z}[x]$。

定理 1.21

$\varphi_n(x)$ 在 $\mathbb{Q}[x]$ 中不可约。

证明. 由于 $\varphi_n(x)$ 是首一的，因此等价于证明在 $\mathbb{Z}[x]$ 中不可约。

设 $\varphi_n(x) = f(x)g(x)$，其中 $f, g \in \mathbb{Z}[x]$，且 $f(\xi_n) = 0$，f 不可约。

我们来证明对于任意素数 $p \neq n$，$f(\xi_n^p)=0$。若不然，$g(\xi_n^p)=0$，令 $h(x)=g(x^p)$，则 $h(x)\in\mathbb{Z}[x]$ 有一根 ξ_n，因此 $f(x)\mid h(x)$。

考虑自然映射 $\mathbb{Z}[x]\to\mathbb{Z}_p[x]$，则 $\bar{h}(x)=\bar{g}(x)=(\bar{g}(x))^p$，且 $\bar{f}(x)\mid(\bar{g}(x))^p$。于是 $\bar{\varphi}_n(x)$ 在 $\bar{f}(x)$ 的分裂域中有重根。但是 $\bar{\varphi}_n(x)'=nx^{n-1}$ 与 $\bar{\varphi}_n(x)$ 互素，矛盾！

将证明中的 ξ_n 换成 ξ_n^p 同样成立，于是我们可以得到对任意 $(k,n)=1$，$f(\xi_n^k)=0$，这表明 $\deg f\geq\varphi(n)=\deg\varphi_n$，故 $f=\varphi_n$ 即 φ_n 是不可约的。 □

由该定理我们可以得到 $[E:F]=[\mathbb{Q}(\xi_n):\mathbb{Q}]=\varphi(n)$。

例 1.7

考虑 $G=\mathrm{Gal}(\mathbb{Q}(\sqrt[5]{2},\xi_5)/\mathbb{Q})$，首先

$$[E:\mathbb{Q}]=[\mathbb{Q}(\sqrt[5]{2},\xi_5):\mathbb{Q}(\xi_5)][\mathbb{Q}(\xi_5):\mathbb{Q}]=5[\mathbb{Q}(\sqrt[5]{2},\xi_5):\mathbb{Q}(\xi_5)]$$

同样也有

$$[E:\mathbb{Q}]=4[\mathbb{Q}(\sqrt[5]{2},\xi_5):\mathbb{Q}(\sqrt[5]{2})]$$

因此 $|G|\geq 20$。注意到 $[\mathbb{Q}(\sqrt[5]{2},\xi_5):\mathbb{Q}(\xi_5)]\leq 4$，故 $|G|=20$。
由于 $|\mathrm{Gal}(E/\mathbb{Q}(\xi_5))|=5$，故 $\mathrm{Gal}(E/\mathbb{Q}(\xi_5)\cong\mathbb{Z}_5\leq G$.
由于 $\left|\mathrm{Gal}(E/\mathbb{Q}(\sqrt[5]{2}))\right|=4$，故 $\mathrm{Gal}(E/\mathbb{Q}(\sqrt[5]{2})\cong\mathbb{Z}_4\leq G$。
利用 Sylow 定理 $\mathbb{Z}_5\lhd G$ 且我们有 $\mathbb{Z}_4\cap\mathbb{Z}_5=e$，因此 $G\cong\mathbb{Z}_5\rtimes\mathbb{Z}_4$。

1.11 Kummer 理论

在本节中，我们设 F 是一个包含 x^n-1 的 n 个不同根的域。

命题 1.13

$E=F(\alpha)$，其中 $\alpha^n\in F^*$，则 E/F 是 m 次分圆域，其中 m 是 α^n 在 $F^*/(F^*)^n$ 中的阶。

证明. 设 $(\alpha^n)^m=\bar{1}\in F^*/(F^*)^n$，则 $\alpha^{mn}=a^n$，其中 $a\in F$，故 $\alpha^m=a\xi_n^i\in F$。

若 $0<m'<m,\alpha^{m'}\in F^*$，则 $(\alpha^{m'})^n\in(F^*)^n$，即 $\alpha^{m'}=\bar{1}\in F^*/(F^*)^n$，这与 α^n 的阶是 m 矛盾。于是 m 是最小的正整数使得 $\alpha^m\in F^*$。

设 α 在 F 中的极小多项式为 $g(x)$，则 $g(x)\mid x^m-\alpha^m$，因此 $g(x)=\prod_{i\in I}(x-\xi_n^i\alpha)$，其中 $I\subset\{0,1,\cdots,m-1\}$。进而 $\prod_{i\in I}(\xi_n^i\alpha)\in F^*$，即 $\alpha^{\deg g}=\alpha^{|I|}\in F^*$。这推出 $\deg g=m$，即 $|\mathrm{Gal}(E/F)|=[E:F]=m$。

设 $\varphi:\mathrm{Gal}(E/F)\to\mu_m,\eta\mapsto\eta(\alpha)/\alpha$，已验证良定义且 φ 是单同态。由于 $|\mathrm{Gal}(E/F)|=|\mu_m|$，我们有 $\mathrm{Gal}(E/F)\cong\mu_m$ 是一个指数为 m 的循环群。 □

定义 1.32

若 $E=F(\alpha),\alpha^n\in F$，则称 E/F 是**单根式扩张(simple radical extension)**。

定理 1.22 (Kummer's theorem)

E/F 是有限 Galois 扩张且 $\mathrm{Gal}(E/F)$ 是 n 阶循环群，则 $E=F(\alpha),\alpha^n\in F$。

证明. 设 η 是 $\mathrm{Gal}(E/F)$ 的生成元，设

$$\alpha=\sum_{i=1}^{n-1}\xi_n^i\eta^i(\beta),\beta\in E$$

我们先来证明可以取 $\beta\in E$ 使得 $\alpha\neq0$，为此需要如下引理：

引理 1.9 (Dedekind)

域 F，$\sigma_1,\cdots,\sigma_n\in\mathrm{Aut}(F)$，若 $c_i\in F$ 使得 $\sum\limits_{i=1}^n c_i\sigma_i=0$，则 $c_i=0,\forall i$。

引理的证明. 取最小的 n 使得结论不成立。则对任意 $a,x\in F$，

$$a\sum_{i=1}^n c_i\sigma_i(x)=\sum_{i=1}^n c_i\sigma_i(ax)=0$$

进而

$$\sum_{i=2}^n c_i(\sigma_i(a)-\sigma_1(a))\sigma_i(x)=0$$

由于 n 是最小的，因此对任一 $c_i\neq0$ 都有对应的 $\sigma_i=\sigma_1$，矛盾！ □

由引理我们取 $\beta \in E$ 使得 $\alpha \neq 0$，则 $\eta(\alpha) = \xi_n^{-1}\alpha \neq \alpha$。由于 $\alpha \notin F$ 且 $\eta(\alpha^n) = \alpha^n$，由 Galois 对应 $\alpha^n \in F$。考虑 $E/F(\alpha)$，由于 $\eta^i(\alpha) = \xi_n^{-i}\alpha$，我们有 $\mathrm{Gal}(E/F(\alpha)) = id$。由 Galois 对应，$E = F(\alpha)$。 □

推论 1.21

有如下一一对应：

$$\{n \text{ 次分圆扩张}(\bar{F}/)E/F\} \leftrightarrow \{F^*/(F^*)^n \text{阶为 } n \text{ 的子群}\}$$

证明. 设 $C = \langle\alpha\rangle$，其中 $\alpha \in F^*/(F^*)^n$ 阶为 n，由**命题 1.13** 可知 $E(\sqrt[n]{\alpha})/F$ 是 n 次分圆域。由Kummer's theorem 知这是一个满射。

若 $F(\alpha) = F(\beta)$，我们来证明 $\langle\bar{\alpha}^n\rangle = \langle\bar{\beta}^n\rangle$。设 $a = \alpha^n, b = \beta^n$，则 a, b 在 $F^*/(F^*)^n$ 中阶均为 n。考虑 $\mathrm{Gal}(F(\alpha)/F)$，设 η 是生成元，则 $\eta(\alpha)/\alpha, \eta(\beta)/\beta$ 都是本原单位根。令 $\eta(\alpha) = \xi_n^i\alpha$，则 $\eta^j(\alpha) = \xi_n^{ij}\alpha$，这表示 ξ_n^i 也是本原的。故 $\frac{\eta(\alpha)}{\alpha} = (\frac{\eta(\beta)}{\beta})^k$，其中 $(k, n) = 1$，进而 $\bar(a) = \bar(b)^k$，这表示 $\langle\bar{\alpha}^n\rangle = \langle\bar{\beta}^n\rangle$。 □

定义 1.33

一个有限 Abel 扩张 E/F 称作 **Kummer 扩张**，若 $\mathrm{Gal}(E/F)$ 的指数整除 n，其中指数是其所有元素阶的最小公倍数。

定理 1.23

E/F 是 Kummer 扩张当且仅当 $E = F(\sqrt[n]{a_1}, \cdots, \sqrt[n]{a_r})$。

证明. "$\Longleftarrow$"：若 $E = F(\sqrt[n]{a_1}, \cdots, \sqrt[n]{a_r})$ 则我们有自然单射：

$$\mathrm{Gal}(E/F) \hookrightarrow \mathrm{Gal}(F(\sqrt[n]{a_1})/F) \times \cdots \times \mathrm{Gal}(F(\sqrt[n]{a_r})/F)$$

且对每个 k，$\mathrm{Gal}(F(\sqrt[n]{a_k})/F)$ 均为指数整除 n 的循环群，这表示 E/F 是 Kummer 扩张。

"$\Longrightarrow$"：设 E/F 是 Kummer 扩张，且 $\mathrm{Gal}(E/F) \cong C_1 \times \cdots \times C_r$。

令 $H_i = \prod_{j\neq i} C_j$，则 $H_i \lhd \mathrm{Gal}(E/F)$，由 Galois 对应 E^{H_i}/F 是 Galois 扩张且

$$\mathrm{Gal}(E^{H_i}/F) \cong \mathrm{Gal}(E/F)/H_i \cong C_i$$

由上定理 $E^{H_i} = F(\sqrt[n]{a_i})$，其中 $a_i \in F^*$。

最后我们需要证明 $E = E^{H_1}\cdots E^{H_r}$，我们考虑 $r = 2$ 的情形，$E^{H_1} \cap E^{H_2} = F$，故

$$[E^{H_1}E^{H_2} : F] = [E^{H_1} : F][E^{H_2} : F] = |H_1||H_2| = |\mathrm{Gal}(E/F)| = [E : F]$$

这表示 $E = E^{H_1}E^{H_2}$。一般情形可由归纳证明。 □

1.12 根式可解性

定义 1.34

有限扩张 E/F 称为**根式扩张(radical extension)**，若存在一个**根塔(root tower)**：$F = F_1 \subset F_2 \subset \cdots \subset F_r = E$，其中 $F_{i+1} = F_i(d_i), d_i^{n_i} \in F$。

我们有如下基本推论：

命题 1.14

$E/K/F, E/K'/F$ 是域扩张，

- 若 E/F 是根式扩张，则 E/K 也是根式扩张；
- 若 $E/K, K/F$ 是根式扩张，则 E/F 是根式扩张；
- 若 $K/F, K'/F$ 是根式扩张，则 KK'/F 是根式扩张；
- 若 $\mathrm{char}F = 0$，E/F 是根式扩张，则 E/F 的正规闭包是根式扩张。

证明. 我们给出 (4) 的证明。设我们有根塔 $F \subset F(d_1) \subset \cdots \subset F(d_1, \cdots, d_r) = E$，$E/F$ 的正规闭包是 K。

设 $\mathrm{Aut}(K/F) = \delta_1 = id, \delta_2, \cdots, \delta_n$，考虑 K 的子域

$$K' = \bigcup_{\delta \in \mathrm{Aut}(K/F)} \delta(E) = \bigcup_{i,j} F(\delta_i(d_j))$$

则 K' 是 $\mathrm{Aut}(K/F)-$不变的，故 K'/F 是正规的，这表示 $K = K'$。于是我们有根塔：

$$\begin{aligned} F &\subset F(d_1) \subset F(d_1, \delta_2(d_1)) \subset \cdots \subset F(d_1, \delta_2(d_1), \cdots, \delta_n(d_1)) \triangleq F_1 \\ &\subset F_1(d_2) \subset F_1(d_2, \delta_2(d_2)) \subset \cdots \subset F_1(d_2, \delta_2(d_2), \cdots, \delta_n(d_2)) \triangleq F_2 \\ &\subset \cdots \\ &\subset F_n = K \end{aligned}$$

故 K/F 是根式扩张。 □

定义 1.35

设 $\mathrm{char}F = 0$，$f(x)$ 是 F 上的首一多项式。等式 $f(x) = 0$ 称作**根式可解的(solvable by radicals)**，若存在根式扩张 E/F，E 包含了 $f(x)$ 的分裂域。

定义 1.36

设 E_f 是 $f(x)/F$ 的分裂域，则 $\mathrm{Gal}(E_f/F)$ 称为 $f(x)$ 的 Galois 群，记为 $G_F(f)$。

定理 1.24 (Galois's criterion)

$f(x) = 0$ 根式可解当且仅当 $G_F(f)$ 可解。

回忆：我们称一个群是可解的当且仅当有正规子列：

$$\{1\} = G_0 \lhd G_1 \lhd \cdots \lhd G_r = G$$

使 G_i/G_{i-1} 是 Abel 的。由于简单 Abel 群是素数阶循环群，因此假设 G_i/G_{i-1} 是素数阶循环群。

注意到 G_i/G_{i-1} 是 Abel 群当且仅当 G_{i-1} 包含 $[G_i, G_i] = \left\langle [a,b] = aba^{-1}b^{-1} \middle| a, b \in G_i \right\rangle$。设 $G^{(0)} = G, G^{(i)} = [G^{(i-1)}, G^{(i-1)}]$，则 $G_{r-i} \supset G^{(i)}$。由于 $[G:G] \lhd G$，故 G 可解当且仅当 $G^{(r)} = 1$ 对某个 r 成立。

回忆如下结论：

- 可解群的子群/商群是可解的；
- 非交换单群是不可解的。

引理 1.10

域扩张 K/F，$f(x) \in F[x]$，则 $G_K(f) \leq G_F(f)$。

证明. 设 $f(x)/F$ 的分裂域为 $E_{f,F}$，$f(x)/K$ 的分裂域为 $E_{f,K}$。考虑映射 $\varphi : G_K(f) \to G_F(f), \eta \mapsto \eta|_{E_{f,F}}$，由于 η 在 F 上不变且将 f 根的集合映到自身，故该 φ 是良定义的且是同态。

若 $\eta|_{E_{f,F}} = id$，注意到 $\eta|_K = id$，我们有 $\eta = id$，故 φ 是单射。 □

接下来我们来证明 Galois 判别定理(Galois's criterion)。

证明. “$\Longleftarrow$”：设 $G_F(f)$ 是可解的。令 E 是 $f(x)/F$ 的分裂域，$[E : F] = n$。考虑 $E(\xi_n)/F(\xi_n)$，其为 $f(x)(x^n - 1)$ 的分裂域。由上引理，$\mathrm{Gal}(E(\xi_n)/F(\xi_n))$ 是 $\mathrm{Gal}(E/F)$ 的子群，而 $\mathrm{Gal}(E/F)$ 是可解的，设

$$\{1\} = G_0 \lhd G_1 \lhd \cdots \lhd G_r = \mathrm{Gal}(E(\xi_n)/F(\xi_n))$$

由 Galois 对应我们有

$$F \subset F(\xi_n) = E(\xi_n)^{G_r} \subset \cdots \subset E(\xi_n)^{G_1} \subset E(\xi_n)$$

是正规扩张。再由 Galois 对应有

$$\mathrm{Gal}(E(\xi_n)^{G_{i-1}}/E(\xi_n)^{G_i}) = G_i/G_{i-1}$$

是循环群，由Kummer's theorem，$E(\xi_n)^{G_{i-1}}/E(\xi_n)^{G_i}$ 是单根式扩张，进而上式为根塔，于是得到 $E(\xi_n)/F$ 是根式扩张。

“$\Longrightarrow$”：设我们有根塔 $F \subset F_1 \subset \cdots \subset F_r \subset K$，其中 $E \subset K$。由**引理 1.10** 我们可以将 K 换成其正规闭包，故不妨 K/F 是正规的。则

$$F \subset F(\xi_n) \subset F_1(\xi_n) \subset \cdots \subset F_r(\xi_n) \subset K(\xi_n)$$

是根塔，由**命题 1.13**， $F_i(\xi_n)/F_{i-1}(\xi_n)$ 是分圆扩张。

回忆我们已经证明 $F(\xi_n)/F$ 是 Abel 扩张，故我们有

$$\mathrm{Gal}(K(\xi_n)/F) \rhd \mathrm{Gal}(K(\xi_n)/F_1(\xi_n)) \rhd \cdots \rhd \mathrm{Gal}(K(\xi_n)/F_r(\xi_n)) \rhd \{1\}$$

利用 Galois 对应，

$$\mathrm{Gal}(K(\xi_n)/F_i(\xi_n))/\mathrm{Gal}(K(\xi_n)/F_{i+1}(\xi_n)) \cong \mathrm{Gal}(F_{i+1}(\xi_n)/F_i(\xi_n))$$

是循环群。故 $\mathrm{Gal}(K(\xi_n)/F)$ 是可解的，因此其子群 $\mathrm{Gal}(K/F)$ 也是可解的。 □

推论 1.22

考虑 $f(x) \in \mathbb{Q}[x], \deg f = n$ 不可约。

- $G_F(f) \leq S_n$，特别的，$n \leq 4$ 时 $f(x) = 0$ 根式可解。
- $n \geq 5$ 是素数，f 恰有两个非实根，$G_F(f) \cong S_n$，此时 $f(x) = 0$ 根式不可解。

证明. (1) 利用 S_n 可解当且仅当 $n \leq 4$ 即证。

(2) $n \mid |G_F(f)|$，则存在 $a \in G_F(f)$ 阶为 n，故 $a = (12\cdots n)$ 是 $n-$循环。

$\tau : \mathbb{C} \to \mathbb{C}, z \mapsto \bar{z}$，则$\tau \in G_F(f)$，故 $\tau = (ij)$，进而 $\langle a, \tau \rangle = S_n$，即 $G_F(f) = S_n$。 □

例 1.8

$f(x) = x^5 - 5x + 2 \in \mathbb{Q}[x]$，容易验证 $f(x)$ 不可约且有三个根，由上推论知根式不可解。

考虑 $f(x) = x^n - s_1x^{n-1} + s_2x^{n-2} - \cdots + (-1)^n s_n$，令 $x_1, \cdots, x_n$ 为 $f(x)$ 的根。由韦达定理我们知

$$s_1 = \sum x_i, s_2 = \sum_{i<j} x_i x_j, \cdots, s_n = \prod x_i$$

考虑 $S_n \curvearrowright F[x_1, \cdots, x_n]$，$s_i$ 在 S_n 作用下不变。s_i 被称为**初等对称多项式**。则 $F[x_1, \cdots, x_n]^{S_n}$ 是所有对称多项式。

我们有同构 $F[y_1, \cdots, y_n] \cong F[x_1, \cdots, x_n]^{S_n}, y_i \mapsto s_i$。

定理 1.25

$F = \mathbb{Q}(s_1, \cdots, s_n)$，则 $G_F(f) \cong S_n$

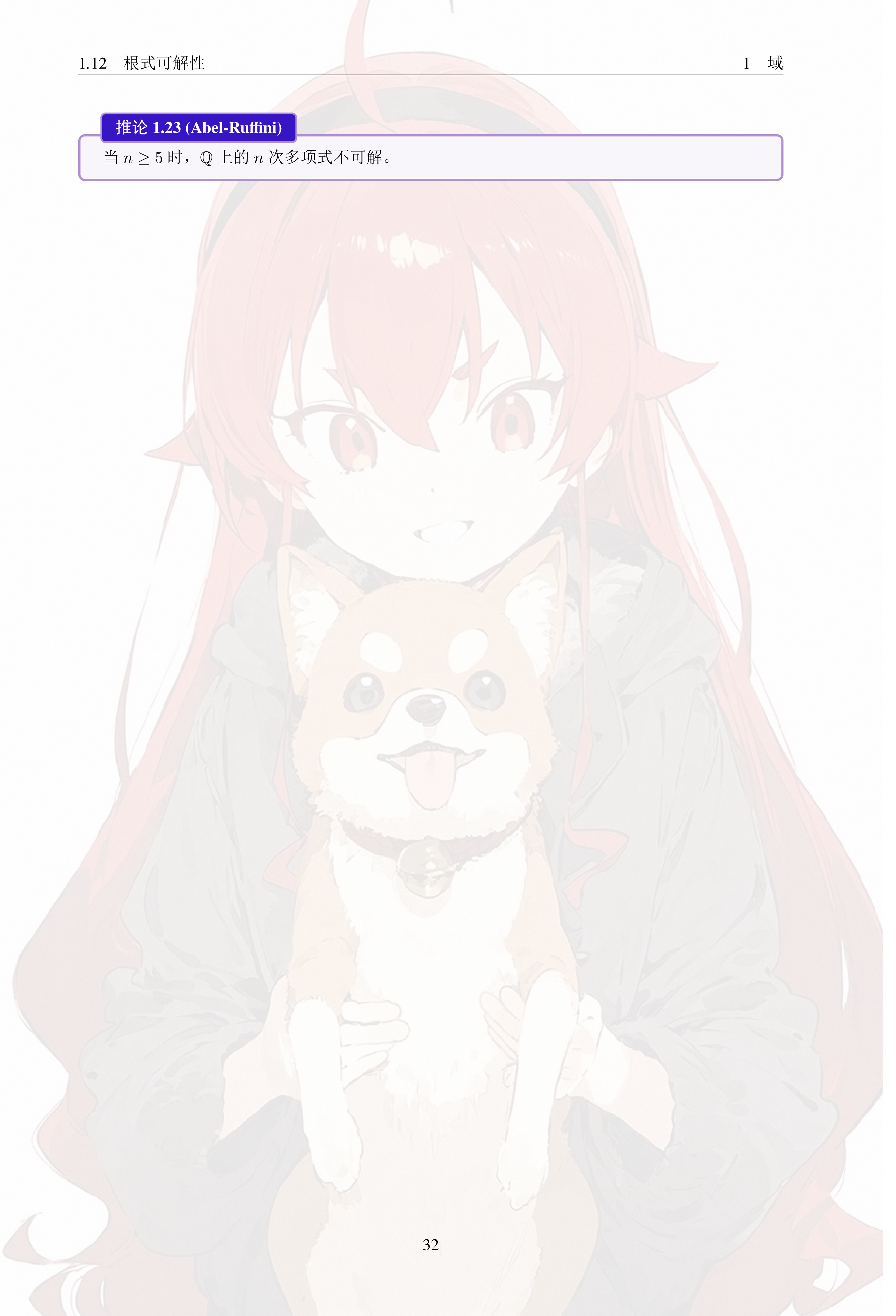
证明. 设 $x_1, \cdots, x_n$ 是 $f(x)$ 的根，则 $E_F(f) = F(x_1, \cdot, x_n)$。

$\forall \sigma \in S_n$，我们希望 $x_i \to x_{\sigma(i)}$ 是 $E_F(f)$ 的一个自同构。我们先证明 $\{x_i\}$ 代数独立。

若不然存在 $g \in F[y_1, \cdots, y_n], g(x_1, \cdots, x_n) = 0$，令 $h = \prod_{\sigma \in S_n} \sigma(g) \in F[y_1, \cdots, y_n]^{S_n}$，其中 $\sigma(g) = g(y_{\sigma(1)}, \cdots, y_{\sigma(n)})$，故 $h = h'(s_1^y, \cdots, s_n^y)$，由 $h(x_1, \cdots, x_n) = 0$ 得 $h'(s_1, \cdots, s_n) = 0$ 矛盾！ □

推论 1.23 (Abel-Ruffini)

当 $n \geq 5$ 时，$\mathbb{Q}$ 上的 n 次多项式不可解。



2 交换代数

2.1 环和理想

定义 2.1

$(R,+,\cdot)$ 称为**环(ring)**，若满足：

- $(R,+)$ 是交换群(这样R有零元素，记为0)
- $(xy)z = x(yz)$
- $x(y+z) = xy + xz$
- $(y+z)x = yz + zx$
- $xy = yx$
- $\exists 1 \in R, \forall x \in R, x1 = 1x = x$

定义 2.2

R 的子集称为**子环(subring)**，若它对 R 中的加法与乘法也构成环。
R 的子群 I 称为**理想(ideal)**，若满足 $\forall a \in R, x \in I, ax \in R$。

考虑 $\{I_i\}_{i\in J}$ 是 R 的所有理想，则 $\cap_{i\in J} I_i$ 也是 R 的理想。

定义 2.3

定义 $\sum_{i\in J} I_i = \left\{\sum_{i\in J'} a_i \middle| a_i \in I_i, J' \subset J\text{有限}\right\}$。
$I_1 \cdot I_2 = \left\{a_i b_j \middle| a_i \in I_1, b_j \in I_2\right\}$。
R, I 为理想，$R/I = \left\{\bar{a} = a + I \middle| a \in R\right\}$ 称为 **R 模 I 的商环**。

定义 2.4

对 $x \in R$：

- 称为**零因子(zero divisor)**若存在 $y \neq 0 \in R$ 使 $xy = 0$。
- 称为**幂零的(nilotent)**若存在 n 使得 $x^n = 0$。
- 称为**单位(unit)**若存在 $y \in R$ 使得 $xy = 1$。

环称为**整环(integral domain)**，若没有非零零因子。

定义 2.5

由单位生成的理想称为**单位理想(unit ideal)**。
由一个元生成的理想称为**主理想(principal ideal)**。
一个理想称为环 R 的**极大理想**，若它不被包含于任一其他 R 的理想。
一个理想 p 称为**素理想**，若 $xy \in \mathfrak{p}$ 能推出 $x \in \mathfrak{p}$ 或 $y \in \mathfrak{p}$。

命题 2.1

I 是素理想 $\iff R/I$ 是整环。

例 2.1

$k[x]$ 的理想均形如 $(f(x))$。

定理 2.1

任一非零理想、非单位理想、非单位元都包含于某一极大理想。

定义 2.6

所有幂零元构成的理想称作**幂零根(nilradical)**。
所有极大理想的交称作**Jacobson 根(Jacobson radical)**。

定理 2.2

幂零根等于所有素理想的交。
$\mathrm{Jacb}(R)$ 是所有满足 $\forall r \in R, 1 - ar$ 可逆的 a 构成的集合。

定义 2.7

$(I : J) = \left\{x \in R \middle| xJ \subset I\right\}$ 称为**商理想**。$(0 : J)$ 称作 J 的**零化理想(annihilator)**，记作 $\mathrm{Ann}(J)$。特别的，若 $J = (x)$，简记 $(I : J) = (I : x)$。
$r(I) = \left\{x \in R \middle| x^n \in I, n > 0\right\}$ 称作 I 的**根(radical)**。

例 2.2

$\bigcup\limits_{0 \neq x \in R} \mathrm{Ann}(x) = \{R\text{的零因子}\}$。$r(I) = \bigcap\limits_{I \subset \mathfrak{p}\ prime} \mathfrak{p}$。

2.2 模

定义 2.8

设R是一个交换环，M是一个交换群，$\mu : R \times M \to M$，我们把$\mu(r,x)$写作rx，若：

- $a(x+y) = ax + by$，
- $(a+b)x = ax + bx$，
- $(ab)x = a(bx)$，
- $1x = x$。

则称 M 为**R-模(R-module)**。
M 的子群称作**子模(submodule)**若 M 也是 R-模。

定义 2.9

两个 R-模 M, N 之间的映射 $f : M \to N$ 称为**同态(homomorphism)**，若满足 $f(x+y) = f(x) + f(y), f(ax) = af(x), \forall a \in R$。
称 f 是**同构(isomorphism)**若存在同态 $g : N \to M$ 满足 $f \circ g = id_N, g \circ f = id_M$。
$\ker f = f^{-1}(0)$ 是 M 的子模。
$\mathrm{coker} f = N/\mathrm{Im} f$ 是 R-模。
$\mathrm{Hom}_R(M,N)$ 为所有同态 $f : M \to N$ 构成的集合，也是一个 R-模

定义 2.10

$\{M_i\}_{i\in S}$ 是 M 的一列子模，定义

$$\sum_{i\in S} M_i = \left\{ \sum_{i\in S'} x_i \middle| x_i \in M_i, S' \subset S\text{有限} \right\}$$

称 M 是 $\{M_i\}_{i\in S}$ 的**直和**若每个元素表示方法唯一，记作 $M = \bigoplus_{i\in S} M_i$。

定义 2.11

M 是**自由的**若 $M = \bigoplus_{i\in S} M_i$ 且 $M_i \cong R$
称 M 是**有限生成的**若 $M = \sum_{1\le i\le n} R\cdot x_i, x_i \in M$。

定义 2.12

若 M 是有限生成自由模，则 $M \cong R^{\oplus n}$ 且 n 唯一，n 称为这个自由模的**维数(rank)**。

命题 2.2

M 有限生成 $\Longleftrightarrow$ 存在 $R^{\oplus n} \twoheadrightarrow M \Longleftrightarrow M$ 是 $R^{\oplus n}$ 的商模。

定义 2.13

M 是 R-模，I 是 R 的理想，定义 $IM=\left\{\sum_{i=1}^n a_ix_i \middle| a_i\in I, x_i\in M\right\}$。
N, N' 是 M 的子模，定义 $(N':N)=\left\{x\in R \middle| x\cdot N\subset N'\right\}$ 是 R 的一个理想，$(0:N)$ 记作 $\mathrm{Ann}(N)$。

定义 2.14

称 M 是**忠实的(faithful)** 若 $\mathrm{Ann}(M)=0$。

M 在 $R/\mathrm{Ann}(M)$ 是忠实的。

命题 2.3 (Cayley-Hamilton)

M 是有限生成 R-模，$\phi\in\mathrm{Hom}_R(M,M)$，$\phi(M)\subset I\cdot M$，则存在 $a_i\in I$ 使得

$$\phi^n+a_1\phi^{n-1}+\cdots+a_n=0\in\mathrm{Hom}_R(M,M)$$

证明. 设 M 生成元 $x_1,\cdots,x_n$，$M=\sum R\cdot x_i$，则 $\phi(x_i)=\sum_j a_{i,j}x_j, a_{i,j}\in I$，则

$$\sum_j(a_{i,j}-\delta_{i,j}\phi)x_j=0$$

进而 $(a_{i,j}-\delta_{i,j}\phi)_{n\times n}\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}=0$，故 $\det A(x_i)=0$。 □

若 $IM=M$，取 $\phi=id_M$，则存在 $a\in I,(1+a)M=0$。

引理 2.1 (Nakayama)

M 是有限生成模，理想 $I\subset\mathrm{Jacb}(R)$。若 $IM=M$ 则 $M=0$。更一般的，对 M 的子模 N，若 $M=N+IM$ 则 $M=N$。

证明. 存在 $a\in I$，$(1+a)M=0$，由于 $1+a$ 是单位，故 $M=0$。
对第二个结论，我们有 $I(M/N)=(IM+N)/N=M/N$。 □

推论 2.1

环 R，有限生成 R-模 M，$x_1,\cdots,x_n\in M$ 满足 $R/\mathfrak{m}\curvearrowright M/\mathfrak{m}M=\sum R\cdot\bar{x}_i$，则 $M=\sum Rx_i$。

证明. $N=\sum_i Rx_i$，则 $M=N+\mathfrak{m}M$，由 Nakayama 引理知成立。 □

定义 2.15

环 R 称为**局部的(local)**若它仅有一个极大理想 $\mathfrak{m}$，进而 $R\setminus\mathfrak{m}$ 中均是单位元，$R/\mathfrak{m}$ 称为 R 的**剩余类域(residue field)**。

推论 2.2

R是局部环，M 是有限生成 $R-$模，则我们可以将 $M/\mathfrak{m}M$ 看成 $R/\mathfrak{m}-$模，这是一个向量空间。若这个向量空间的基是 $x_1,\cdots,x_n$，则 $\{x_i\}$ 生成 M。

证明. 设 N 是由 $\{x_i\}$ 生成的子模，则 $N\to M/\mathfrak{m}M$ 是满射，这表示 $N+\mathfrak{m}M=M$，由 Nakayama 引理知 $N=M$。 □

推论 2.3

R 是局部环，$M=0$ 当且仅当 $M/\mathfrak{m}M=0$。$M\to N$ 是满射当且仅当 $M/\mathfrak{m}M\to N/\mathfrak{m}N$ 是满射。

2.2.1 正合性

定义 2.16

一个 R-模和 R-同态的序列

$$\cdots\to M_{i-1}\xrightarrow{f_i}M_i\xrightarrow{f_{i+1}}M_{i+1}\to\cdots$$

叫做在 M_i 处**正合(exact)**，若 $\mathrm{Im}(f_i)=\mathrm{Ker}(f_{i+1})$。

- $0\to M'\to M\to M''\to 0$ 称作短正合列；
- $0\to M'\to M\to M''$ 称作左正合列；
- $M'\to M\to M''\to 0$ 称作右正合列。

例 2.3

- $0\to M'\xrightarrow{f}M$ 是正合的当且仅当 f 是单射；
- $M\xrightarrow{g}M''\to 0$ 是正合的当且仅当 f 是满射；
- $$\cdots\to M_{i-1}\xrightarrow{f_i}M_i\xrightarrow{f_{i+1}}M_{i+1}\to\cdots$$
  是正合的当且仅当 $0\to\mathrm{Im}f_i\to M_i\to\mathrm{Ker}f_{i+1}\to 0$ 是正合的。

定义 2.17

正合列 $0\to M'\xrightarrow{f}M\xrightarrow{g}M''\to 0$ 称为**分裂的(split)**，若存在 $h:M''\to M$ 使得 $g\circ h=id_M$。

注意到 f,h 都是单射，故 M',M'' 可视作 M 的子模且由 $g\circ f=0$ 有 $M'\cap M''=\{0\}$。对任意 $x\in M$，$x=h(g(x))+(x-h(g(x))\in M''+M'$，故 $M=M'\oplus M''$。

命题 2.4

(1) $M' \to M \to M'' \to 0$ 是正合的当且仅当对任意 $R-$模 N，有

$$0 \to \mathrm{Hom}(M'', N) \to \mathrm{Hom}(M, N) \to \mathrm{Hom}(M', N)$$

是正合的。

(2) $0 \to N' \to N \to N''$ 是正合的当且仅当对任意 $R-$模 N 有

$$0 \to \mathrm{Hom}(M, N'') \to \mathrm{Hom}(M, N) \to \mathrm{Hom}(M, N')$$

是正合的。

证明. 我们只证明 (1)，(2) 是类似的。

设 $M' \to M \to M'' \to 0$ 是正合的。若 $M \to M'' \to N$ 是零的，由于 $M \to M'$ 是满射，故 $M'' \to N$ 是零。于是 $\mathrm{Hom}(M'', N) \to \mathrm{Hom}(M, N)$ 是单射。

若 $f : M \to N \in \mathrm{Im}(\mathrm{Hom}(M'', N) \to \mathrm{Hom}(M, N))$，则 $(M' \to M \to N) = (M' \to M \to M'' \to N) = 0$，故 $f \in \mathrm{Ker}(\mathrm{Hom}(M, N) \to \mathrm{Hom}(M', N))$。

另一方面若 $(M' \to M \to N) = 0$，由于 $M'' \cong M/\mathrm{Im}(M' \to M)$，故存在自然映射 $M'' \to N, (M \to N) = (M \to M'' \to N)$，故 $M \to N \in \mathrm{Im}(\mathrm{Hom}(M'', N) \to \mathrm{Hom}(M, N))$。

反过来是类似的，读者自证不难。 □

命题 2.5 (Snake lemma)

$$\begin{tikzcd}
0 \arrow[r, dashed] & \ker f' \arrow[r, dashed] \arrow[d] & \ker f \arrow[r, dashed] \arrow[d] & \ker f'' \arrow[d] \arrow[dddll, dashed, "\delta"] & \\
0 \arrow[r] & M' \arrow[r] \arrow[d, "f'"] & M \arrow[r] \arrow[d, "f"] & M'' \arrow[r] \arrow[d, "f''"] & 0 \\
0 \arrow[r] & N' \arrow[r] \arrow[d] & N \arrow[r] \arrow[d] & N'' \arrow[r] \arrow[d] & 0 \\
& \operatorname{coker} f' \arrow[r, dashed] & \operatorname{coker} f \arrow[r, dashed] & \operatorname{coker} f'' \arrow[r, dashed] & 0
\end{tikzcd}$$

是交换图。则存在正合列

$$0 \to \ker f' \to \ker f \to \ker f'' \xrightarrow{\delta} \operatorname{coker} f' \to \operatorname{coker} f \to \operatorname{coker} f'' \to 0$$

其中 δ 称为**边缘同态(boundary homomorphism)**。

证明. 我们这样给出 δ：对任意 $x'' \in M$，$f''(x'') = 0$，我们取 $x \in M$，$(M \to M'')(x) = x''$，则 $f(x) \in \ker(N \to N'')$，故存在唯一的 $x' \in N', x' \to f(x)$。令 $\delta(x'') = \overline{x'} \in \operatorname{coker} f'$，容易验证良定义，且 $\ker f \to \ker f'' \xrightarrow{\delta} \operatorname{coker} f' \to \operatorname{coker} f$ 正合 □

定义 2.18

设 S 是一些 $R-$模构成的集合，$\lambda : S \to \mathbb{Z}$ 称为**可加的(additive)**若对任意正合列 $0 \to M' \to M \to M'' \to 0$ 有 $\lambda(M) = \lambda(M') + \lambda(M'')$。

例 2.4

若 R 是域，则 $\lambda(M) = \dim_R(M)$ 是可加的。

引理 2.2

设 $0 \to M_0 \to M_1 \to \cdots \to M_n \to 0$ 是正合的，$M_i \in S$，λ 在 S 上可加，则

$$\sum_{i=0}^{n}(-1)^i\lambda(M_i) = 0$$

证明. $0 \to \mathrm{Im}f_i \to M_i \to \mathrm{Im}f_{i+1} \to 0$ 是正合的，故 $\lambda(M_i) = \lambda(\mathrm{Im}f_i) + \lambda(\mathrm{Im}f_{i+1})$。 □

2.2.2 张量积

定义 2.19

M, N, P 是 $R-$模，$f : M \times N \to P$ 称为 **$R-$双线性的($R-$bilinear)**，若任意 $x \in M$，$N \to P, y \mapsto f(x, y)$ 是 $R-$线性的且任意 $y \in N$，$M \to P, x \mapsto f(x, y)$ 是 $R-$线性的。

若 f 是 $R-$双线性的，则如下元素均为零：

$$(x + x', y) - (x, y) - (x', y), (x, y + y') - (x, y) - (x, y'), (ax, y) - a(x, y), (x, ay) - a(x, y) \tag{1}$$

定义 2.20

M, N 是 $R-$模，$C = \bigoplus_{(x,y)\in M\times N} R \cdot (x, y)$，$D \subset C$ 由 $(*)$ 生成。称 C/D 为 M 与 N 的张量积，记作 $M \otimes N$。

命题 2.6 (Universal property)

存在双线性映射 $g : M \times N \to M \otimes N, (x, y) \mapsto x \otimes y$ 使得对任意双线性映射 $f : M \times N \to P$，存在唯一的 R-线性映射 h 使下图交换：

$$\begin{tikzcd} M \times N \arrow[r, "f"] \arrow[d, "g"'] & P \\ M \otimes N \arrow[ur, "h"'] & \end{tikzcd}$$

证明. 对任意映射 $f : M \times N \to P$，我们有 $f' : C \to P, \sum a_{xy}(x, y) \mapsto \sum a_{xy}f(x, y)$，则 f 是双线性的当且仅当 $\ker f' \supset D$。故若 f 是双线性的，则存在唯一的 h，$f' = h \circ \pi$，其中 π 是投影映射 $C \to M \otimes N = C/D$，则 $f = h \circ g$。

$$\begin{tikzcd}
C \arrow[rd, "f'"] \arrow[dd, bend right=60, "\pi"'] & \\
M\times N \arrow[u] \arrow[r, "f"] \arrow[d, "g"] & P \\
M\otimes N \arrow[ru, "h"'] &
\end{tikzcd}$$

□

由此命题我们可以有如下张量积的定义：

定义 2.21

M,N 的张量积 T 是由双线性映射 $g:M\times N\to T$ 定义的模，对任意 $f:M\times N\to P$ 存在唯一的线性映射 $f':T\to P, f=f'\circ g$。

张量积的唯一性. 若我们有两个不同的张量积 T_1 和 T_2 与对应的双线性映射 g_1,g_2，由上定义存在 $h_1:T_1\to T_2, g_2=h_1\circ g_1$ 与 $h_2:T_2\to T_1, g_1=h_2\circ g_2$。则 $g_2=h_1\circ g_1=h_1\circ h_2\circ g_2$。由于 $h_1\circ h_2:T_2\to T_2$ 是线性的，由唯一性 $h_1\circ h_2=id_{T_2}$。同理 $h_2\circ h_1=id_{T_1}$，故 $T_1\cong T_2$。

$$\begin{tikzcd}
 & T_1 \arrow[dd, shift right, "h_1"'] \\
M\times N \arrow[ru, "g_1"] \arrow[rd, "g_2"'] & \\
 & T_2 \arrow[uu, shift right, "h_2"']
\end{tikzcd}$$

□

由 Universal property，我们可以定义 $M_1,\cdots,M_n$ 的张量积，由多线性映射 $g:M_1\times\cdots\times M_n\to M_1\otimes\cdots\otimes M_n, (x_1,\cdots,x_n)\mapsto x_1\otimes\cdots\otimes x_n$ 定义，对任意多线性映射 $f:M_1\times\cdots\times M_n\to P$，存在唯一的 R-线性映射 h 使下图交换：

$$\begin{tikzcd}
M_1\times\cdots\times M_n \arrow[r, "f"] \arrow[d, "g"'] & P \\
M_1\otimes\cdots\otimes M_n \arrow[ru, "h"'] &
\end{tikzcd}$$

设 M 由 $\{x_i\}_{i\in S}$ 生成，N 由 $\{y_i\}_{i\in S'}$ 生成，则

$$\sum a_{x,y}(x,y)=\sum a_{x,y}(\sum b_ix_i,\sum c_jy_j)=\sum a_{x,y}\sum b_ic_jx_i\otimes y_j$$

即 $M\otimes$ 由 $\{x_i\otimes y_j\}$ 生成。于是有如下推论：

推论 2.4

若 M,N 有限生成，则 $M\otimes N$ 也有限生成。

例 2.5

将 $\mathbb{Z}_m \otimes \mathbb{Z}_n$ 看成 $\mathbb{Z}-$模。我们来证 $\mathbb{Z}_m \otimes \mathbb{Z}_n \cong \mathbb{Z}_{(m,n)}$。
令 $d = (m,n)$，$\mathbb{Z}_m \otimes \mathbb{Z}_n$ 由 $1 \otimes 1$ 生成，$m(1 \otimes 1) = m \otimes 1 = 0, n(1 \otimes 1) = 1 \otimes n = 0$，故 $d(1 \otimes 1) = 0$。令 $f : \mathbb{Z}_m \times \mathbb{Z}_n \to \mathbb{Z}_d, (a,b) \mapsto ab$，这是双线性的，故由 Universal property 存在满射 $h : \mathbb{Z}_m \otimes \mathbb{Z}_n \to \mathbb{Z}_d$。这同时也是单射因为 $d(1 \otimes 1) = 0$。

例 2.6

设 M, N 分别为 m, n 维自由模且

$$M = \bigoplus_{i=1}^{n} Rx_i, N = \bigoplus_{j=1}^{m} Ry_j$$

令 $A = \bigoplus_{i=1}^n \bigoplus_{j=1}^m Rx_i \otimes y_j$。
考虑 $f : M \times N \to A, (\sum a_i x_i, \sum b_j y_j) \mapsto \sum a_i b_j (x_i \otimes y_j)$，这是双线性的，故我们可以构造 $f' : M \otimes N \to A, f' = f \circ g$。
另一方面我们自然有 $h : A \to M \otimes N, x_i \otimes y_j \mapsto x_i \otimes y_j$。可以验证 $f' \circ h = id_A, h \circ f' = id_{M \otimes N}$，故 $M \otimes N \cong A$ 是一个 mn 维的自由模。

例 2.7

$2 \otimes \bar{1} \in \mathbb{Z} \otimes \mathbb{Z}_2$，$2 \otimes \bar{1} = 2 \cdots 1 \otimes \bar{1} = 1 \otimes 2 \cdots \bar{1} = \bar{0}$，但在 $2\mathbb{Z} \otimes \mathbb{Z}_2$ 中 $2 \otimes \bar{1} \neq 0$。
故若 $M' \subset M, N' \subset N$，不一定有 $M' \otimes N' \subset M \otimes N$。
另一方面，若 $\sum x \otimes y = 0 \in M' \otimes N'$，则 $\sum x \otimes y = 0 \in M \otimes N$。

命题 2.7

M, N, P 是 $R-$模，则有如下命题成立：

- $M \otimes N \cong N \otimes M$
- $(M \otimes N) \otimes P \cong M \otimes (N \otimes P) \cong M \otimes N \otimes P$
- $(M \oplus N) \otimes P \cong (M \otimes P) \oplus (N \otimes P)$

证明. 这些同构分别由如下映射给出：

- $x \otimes y \mapsto y \otimes x$;
- $(x \otimes y) \otimes z \mapsto x \otimes (y \otimes z) \mapsto x \otimes y \otimes z$;
- $(x, y) \otimes z \mapsto (x \otimes z, y \otimes z)$。

□

设 M 是 $R-$模，N 是 $R, R'-$双模(满足 $(ax)b = a(xb)$)，P 是 $R'-$模，则

$$(M \otimes_R N) \otimes_{R'} P \cong M \otimes_R N \otimes_{R'} P$$

是 $R, R'-$双模

命题 2.8

同态 $f: M \to M', g: N \to N'$ 则

$$f \otimes g: \quad \begin{tikzcd} M \otimes N \arrow[r] & M' \otimes N' \\ M \times N \arrow[u, "x\otimes y"] \arrow[ur, "f(x)\otimes g(y)"'] & \end{tikzcd}$$

设 N 是 R–模，在范畴论中我们有函子

$$\text{Cat of R-module} \longrightarrow \text{Cat of R-module}$$

$$\begin{tikzcd} M \arrow[r] \arrow[d, "f"] & M \otimes N \arrow[d, "f\otimes id"] \\ M' \arrow[r] & M' \otimes N \end{tikzcd}$$

设 $\varphi: R \to R'$ 是环同态，则在 R' 上定义 $ra = \varphi(r)a$ 则是一个 R–模。对任意 R'–模 M'，定义 $ra = \varphi(r)a$ 则是一个 R–模，这称为**纯量限制(restriction of scalars)**。对任意 R–模 M，在 $M \otimes_R R'$ 上定义 $r(a \otimes x) = a \otimes rx$ 则是一个 R'–模，这称为**纯量扩张(extension of scalars)**。

命题 2.9

- 若 M' 在 R' 上有限生成，R' 在 R 上有限生成，则 M' 在 R 上有限生成；
- 若 M 在 R 上有限生成，则 $M \otimes_R R'$ 在 R' 上有限生成。

2.2.3 张量积的正合性

命题 2.10

$M' \to M \to M'' \to 0$ 正合，对任一 R–模 N 都有

$$M' \otimes N \to M \otimes N \to M'' \otimes N \to 0$$

正合。

推论 2.5

由于 $I \to R \to R/I \to 0$ 正合，故任意 R–模 M，$I \otimes M \to R \otimes M \to R/I \otimes M \to 0$ 正合。
注意到 $R \otimes M \cong M$，$I \otimes M \cong IM$，故 $(R/I) \otimes M \cong M/IM$。
特别的令 $M = R/J$，则 $R/I \otimes R/J \cong R/I + J$。

引理 2.3

M, N, P 是 R–模，则 $\mathrm{Hom}_R(M \otimes N, P) \cong \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P))$

证明. 下述两个映射互为逆映射：

$$\phi: \begin{matrix} f: M \otimes N \to P \mapsto M \to \mathrm{Hom}_R(N, P) \\ x \mapsto y \mapsto f(x \otimes y) \end{matrix}, \varphi: \begin{matrix} g: M \to \mathrm{Hom}_R(N, P) \mapsto M \otimes N \to P \\ x \otimes y \mapsto g(x)(y) \end{matrix}$$

□

命题2.10的证明. 由**命题2.4**我们希望

$$0 \to \mathrm{Hom}(M'' \otimes N, P) \to \mathrm{Hom}(M \otimes N, P) \to \mathrm{Hom}(M' \otimes N, P)$$

对任意 P 都正合，而由上述引理这等价于

$$0 \to \mathrm{Hom}(M'', \mathrm{Hom}(N, P)) \to \mathrm{Hom}(M, \mathrm{Hom}(N, P)) \to \mathrm{Hom}(M', \mathrm{Hom}(N, P))$$

正合，再次利用**命题2.4**我们完成了证明。 □

定义 2.22

一个 $R-$模 M 是**平坦的(flat)**，若对任意正合列

$$\cdots \to M_{i-1} \to M_i \to M_{i+1} \to \cdots$$

有

$$\cdots \to M \otimes M_{i-1} \to M \otimes M_i \to M \otimes M_{i+1} \to \cdots$$

也是正合的。

例 2.8

自由模是平坦的，任意有限生成平坦 $\mathbb{Z}-$模都是自由的。

命题 2.11

下述命题等价：

- M 是平坦的；
- 任意正合列 $0 \to N' \to N \to N'' \to 0$，$0 \to N' \otimes M \to N \otimes M \to N'' \otimes M \to 0$ 正合。
- 任意正合列 $0 \to N' \to N$，$0 \to N' \otimes M \to N \otimes M$ 正合。
- 任意有限生成模 N, N'，若 $0 \to N' \to N$ 正合，则 $0 \to N' \otimes M \to N \otimes M$ 正合。

证明. (1) $\Longrightarrow$ (2) 是显然的。

(2) $\Longrightarrow$ (1)：回忆若有正合列 $N_{i-1} \xrightarrow{f_i} N_i \xrightarrow{f_{i+1}} N_{i+1}$，则

$$0 \to \mathrm{Im} f_i \to N_i \to \mathrm{Im} f_{i+1} \to 0$$

也是正合的，进而 $0 \to \mathrm{Im} f_i \otimes M \to N_i \otimes M \to \mathrm{Im} f_{i+1} \otimes M \to 0$ 正合。我们有自然映射 $\mathrm{Im} f_{i+1} \to N_i$ 与 $N_i \to \mathrm{Im} f_i$，故s

$$\ker(f_{i+1} \otimes id_M) = \ker(N_i \otimes M \to \mathrm{Im} f_{i+1} \otimes M) = \mathrm{Im}(\mathrm{Im} f_i \otimes M \to N_i \otimes M) = \mathrm{Im}(f_i \otimes id_M)$$

$$\begin{tikzcd}
 & & & 0 \arrow[d] & 0 \\
 & & & \mathrm{Im} f_{i+1} \arrow[ur] \arrow[d] & \\
 & N_{i-1} \arrow[r, "f_i"] \arrow[d] & N_i \arrow[r, "f_{i+1}"] \arrow[ur] & N_{i+1} & \\
 & \mathrm{Im} f_i \arrow[ur] \arrow[d] & & & \\
0 \arrow[ur] & 0 & & &
\end{tikzcd}$$

(2) $\iff$ (3) 由**命题2.10**是显然的。

(3) $\implies$ (4) 是显然的。

(4) $\implies$ (3)：设 $M' \to M$ 是单射，我们来证明 $f \otimes 1 : M' \otimes N \to M \otimes N$ 也是单射。取 $x \in \ker(f \otimes 1)$，$x = \sum_{i=1}^n x_i \otimes y_i$，则 $(f \otimes 1)(x) = \sum_{i=1}^n f(x_i) \otimes y_i = 0$。取 $\tilde{M}'$ 由 $x_1, \cdots, x_n$ 生成，$\tilde{M}$ 由 $f(x_1), \cdots, f(x_n)$ 生成，则我们有单射 $f\big|_{\tilde{M}'} : \tilde{M}' \to \tilde{M}$，且 $(\tilde{f} \otimes 1)(x) = 0$，即 $x = 0 \in \tilde{M}' \otimes N$，即 $x = 0 \in M' \otimes N$，于是我们完成了证明。 □

命题 2.12

若 M 是 R 上的平坦模，则 $M \otimes_R R'$ 是 R' 上的平坦模。

证明. 由 $N_i \otimes_{R'} (R' \otimes_R M) \cong N_i \otimes_R M$ 即得。 □

定义 2.23

环 R' 由同态 $f : R \to R'$ 给出的 R–模结构称为一个 R 上的**代数**。

2.3 局部化

定义 2.24

给定环 R，乘性子集 $S \subset R$ 使得 $1 \in S$ 且若 $a, b \in S$ 则 $ab \in S$。我们定义 $R \times S$ 上的等价关系：$(a, s)\ (b, t) \leftrightarrow \exists u \in S, (at - bs)u = 0$。由该等价关系导出的等价类记为 $S^{-1}R$ 称为 R 对 S 的**分式环(ring of fractions)**。

我们记 (a, s) 为 $\frac{a}{s}$，分式环的结构由

$$\frac{a}{s} + \frac{a'}{s'} = \frac{as' + a's}{ss'}, \frac{a}{s} \cdot \frac{a'}{s'} = \frac{aa'}{ss'}$$

给出，单位为 $\frac{1}{1}$，零元为 $\frac{0}{S}$。

例 2.9

- 若 R 是整环，取 $S = R \setminus 0$，则 $S^{-1}R$ 称为 R 的分式域。
- 设 $\mathfrak{p}$ 是 R 的素理想，取 $S = R \setminus \mathfrak{p}$ 是乘性子集，我们称 $R_{\mathfrak{p}} = S^{-1}R$ 是在 $\mathfrak{p}$ 的**局部化(localization)**，且 $I = \left\{ \frac{x}{s} \middle| x \in \mathfrak{p}, s \in S \right\}$ 是 $R_{\mathfrak{p}}$ 的唯一极大理想，且 $R_{\mathfrak{p}}/I \cong R/\mathfrak{p}$ 是域。
- $f \in R, S = \{1, f, f^2, \cdots\}$，则 $S^{-1}R = \left\{ \frac{a}{f^n} \middle| a \in R, n \geq 0 \right\}$，记为 R_f。

我们有自然同态 $l : R \to S^{-1}R, x \mapsto \frac{x}{1}$。

命题 2.13 (Universal property)

设同态 $f : R \to R'$ 满足任意 $s \in S, f(s)$ 均为单位，则存在唯一的同态 $g : S^{-1}R \to R'$ 使得 $f = g \circ l$。

$$\begin{tikzcd} S^{-1}R \arrow[r, "g"] & R' \\ R \arrow[u, "l"] \arrow[ur, "f"'] & \end{tikzcd}$$

证明. 若 g 存在，则必须有 $g(\frac{a}{s})g(s) = g(a) = f(a)$，故 $g(\frac{a}{s}) = f(a)f^{-1}(s)$。

现在我们检验 g 是良定义的，即若 $u(as' - a's) = 0$，则 $g(\frac{a}{s}) = g(\frac{a'}{s'})$。这是因为 $0 = f(u(as' - a's)) = f(u)(f(a)f(s') - f(a')f(s)) = 0$ 且 $f(u)$ 是单位，故 $f(a)f(s') = f(a')f(s)$，即 $f(a)f^{-1}(s) = f(a')f^{-1}(s)$。同态是容易验证的。 □

推论 2.6

设同态 $f: R \to R'$，若有：

- $\forall s \in S$，$f(s)$ 是单位；
- 若 $f(a)=0$，则存在 $s \in S, as=0$；
- R' 可以写成 $f(a)f^{-1}(s)$，其中 $a \in R, s \in S$。

则 $R' \cong S^{-1}R$。

类似的，设 M 是一个 $R-$模，S 是 R 的乘性子集，我们可以定义 $M \times S$ 上的等价关系：$(a,s)\ (b,t) \longleftrightarrow \exists u \in S, (at-bs)u=0$，则 $S^{-1}M$ 是该等价关系导出的等价类，可以将 $S^{-1}M$ 看作一个 $S^{-1}R-$模。

命题 2.14

设 $f: M \to N$ 是一个 $R-$模同态，则 f 诱导了一个同态 $S^{-1}f: S^{-1}M \to S^{-1}N$。更进一步地，若 $g: P \to M$ 是同态，则 $S^{-1}f \circ S^{-1}g = S^{-1}(f \circ g)$。

证明. 定义 $S^{-1}f: \frac{a}{s} \to \frac{f(a)}{s}$。我们来检验 $S^{-1}f$ 是良定义的：若 $\frac{a}{s}=\frac{b}{t}$，则 $\exists u \in S, (at-bs)u=0$，故 $(f(a)t-f(b)s)u=0$，进而 $\frac{f(a)}{s}=\frac{f(b)}{t} \in S^{-1}N$。 □

注：S^{-1} 是一个 $R-$模范畴映到自身的函子。

命题 2.15

若 $M' \xrightarrow{f} M \xrightarrow{g} M''$ 是正合的，则$S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M''$ 是正合的。特别的，若 M' 是 M 的子模，则 $S^{-1}M'$ 是 $S^{-1}M$ 的子模。

证明. 首先 $S^{-1}g \circ S^{-1}f = S^{-1}(f \circ g)=0$，故 $\mathrm{Im} S^{-1}f \subset \ker S^{-1}g$。

另一方面，设 $\frac{a}{s} \in \ker S^{-1}g, \frac{g(a)}{s}=0 \in S^{-1}M''$，则存在 $u \in S, g(a)u=0$，即 $g(ua)=0 \in M''$。由正合性，$ua=f(b), b \in M'$，则 $\frac{a}{s}=\frac{au}{su}=\frac{f(b)}{su}=S^{-1}f(\frac{b}{su}) \in \mathrm{Im} S^{-1}f$。 □

推论 2.7

设 N, P 是 M 的子模，则：

- $S^{-1}(N+P)=S^{-1}N+S^{-1}P$；
- $S^{-1}(N \cap P)=S^{-1}N \cap S^{-1}P$；
- $S^{-1}(M/N) \cong S^{-1}M/S^{-1}N$；
- $S^{-1}(I \cdot J)=S^{-1}I \cdot S^{-1}J$，其中 I, J 是 R 的理想。

命题 2.16

设 $R-$模 M，则作为 $S^{-1}R-$模，$S^{-1}M \cong M \otimes_R S^{-1}R$。特别的，$S^{-1}R$ 是平坦 $R-$模。

证明. 定义 $\varphi : M \times S^{-1}R \to S^{-1}M, (m, \frac{a}{s}) \mapsto \frac{am}{s}$ 是 $R-$双线性的，故存在 $R-$同态 $f : M \otimes_R S^{-1}R \to S^{-1}M, m \otimes \frac{a}{s} \mapsto \frac{am}{s}$，这显然是满射。下证这是单射。

取 $\sum a_i \otimes \frac{x_i}{s_i} \in M \otimes_R S^{-1}R$。令 $s = \prod s_i$，则

$$\sum a_i \otimes \frac{x_i}{s_i} = \sum a_i x_i \otimes \frac{1}{s_i} = (\sum a_i x_i \frac{s}{s_i}) \otimes \frac{1}{s} := a \otimes a \otimes \frac{1}{s}$$

$a \otimes \frac{1}{s} \in \ker f \iff \frac{a}{s} = 0 \in S^{-1}M \iff \exists u \in S, ua = 0$，则 $a \otimes \frac{1}{s} = ua \otimes \frac{1}{us} = 0$，故 f 是单射。 □

推论 2.8

$S^{-1}M \otimes_{S^{-1}R} S^{-1}N \cong S^{-1}(M \otimes_R N)$

证明. 由上命题我们有

$$S^{-1}M \otimes_{S^{-1}R} S^{-1}N \cong M \otimes_R S^{-1}R \otimes_{S^{-1}R} S^{-1}N \cong M \otimes_R S^{-1}N$$

$$S^{-1}(M \otimes_R N) \cong M \otimes_R N \otimes_R S^{-1}R \cong M \otimes_R S^{-1}N$$

□

2.3.1 局部性质

本节我们讨论模的局部性质：

命题 2.17

M 是一个 $R-$模，则如下命题等价：

- $M=0$；
- 对任意素理想 $\mathfrak{p}$，$M_{\mathfrak{p}}=0$；
- 对任意极大理想 $\mathfrak{m}$，$M_{\mathfrak{m}}=0$。

证明. 只需证 (3) $\Longrightarrow$ (1)。设 $M\neq 0$，取 $0\neq a\in M$，则 $\mathrm{Ann}(a)$ 是 R 的真理想，故存在极大理想 $\mathfrak{m}\supset \mathrm{Ann}(a)$。由于 $\frac{a}{1}\neq 0$ 故 $M_{\mathfrak{m}}\neq 0$，矛盾！ □

命题 2.18

设 $f:M\to N$ 是 $R-$模同态，则如下命题等价：

- f 是单(满)射；
- 对任意素理想 $\mathfrak{p}$，$f_{\mathfrak{p}}:M_{\mathfrak{p}}\to N_{\mathfrak{p}}$ 是单(满)射；
- 对任意极大理想 $\mathfrak{m}$，$f_{\mathfrak{m}}:M_{\mathfrak{m}}\to N_{\mathfrak{m}}$ 是单(满)射；

证明. 我们只证明单射的情形。

注意到 $0\to \ker f\to M\to N$ 是正合的，故 $0\to(\ker f)_{\mathfrak{p}}\to M_{\mathfrak{p}}\to N_{\mathfrak{p}}$ 是正合的，即 $(\ker f)_{\mathfrak{p}}=\ker f_{\mathfrak{p}}$。由上命题知 $\ker f=0\Longleftrightarrow \forall\mathfrak{p},(\ker f)_{\mathfrak{p}}=0\Longleftrightarrow\forall\mathfrak{p},\ker f_{\mathfrak{p}}=0$。 □

命题 2.19

设 M 是一个 $R-$模，则如下条件等价：

- M 在 R 上平坦；
- 对任意素理想 $\mathfrak{p}$，$M_{\mathfrak{p}}$ 在 $R_{\mathfrak{p}}$ 上平坦；
- 对任意极大理想 $\mathfrak{m}$，$M_{\mathfrak{m}}$ 在 $R_{\mathfrak{m}}$ 上平坦。

证明. 利用 $N\otimes_{R_{\mathfrak{p}}}M_{\mathfrak{p}}\cong N\otimes_{R_{\mathfrak{p}}}R_{\mathfrak{p}}\otimes_R M\cong N\otimes_R M$ 即得。 □

2.3.2 理想的局限和扩张

我们来考虑分式环中的理想。

$f:R\to R'$ 是环同态。I 是 R 的理想，则 $f(I)$ 生成一个 R' 的理想，称为 I 的扩张，记为 I^e；J 是 R' 的理想，则 $f^{-1}(J)$ 是 R 的一个理想，称为 J 的局限，记为 J^c。容易验证如下性质：

引理 2.4

$I^{ec} \supset I, I^{ece} = I^e; J^{ce} \subset J, J^{cec} = J^c$。

由此引理，我们有：

$$C := \{R\text{的局限理想}\} = \left\{I \middle| I = I^{ec}\right\}$$

$$E := \{R'\text{的扩张理想}\} = \left\{J \middle| J = J^{ec}\right\}$$

且两者有一一对应。

回忆：对于分式环，我们有自然同态 $l : R \to S^{-1}R, x \mapsto \frac{x}{1}$。

命题 2.20

我们有如下命题：

- I 是 R 的理想，则 $I^e = S^{-1}I \subset S^{-1}R$；
- $S^{-1}R$ 任一理想 J 均为扩张理想，即 $J^{ce} = J$；
- I 是 R 的理想，则 $I^{ec} = \cup_{s\in S}(I : s)$；
- $I^e = (1) \iff I \cap S \neq \emptyset$ ‘
- I 是局限理想当且仅当 S 中元素均非 R/I 的零因子；
- $S^{-1}R$ 的素理想和 R 中与 S 不交的素理想有一一对应。特别的，$R_{\mathfrak{p}}$ 的素理想与 R 中包含 $\mathfrak{p}$ 的素理想有一一对应。
- S^{-1} 对理想的有限和、积、交、根交换。

证明. (1) $x \in I^e \iff x = \sum \frac{a_i}{s_i}, a_i \in I, s_i \in S \iff x = \frac{a}{s}, a \in I, s \in S$，即 $x \in S^{-1}I$

(2) $\frac{x}{s} \in J \Longrightarrow \frac{x}{1} \in J \Longrightarrow x \in J^c \to \frac{x}{s} \in J^{ce}$。又 $J^{ce} \supset J$，故 $J = J^{ce}$。

(3) $x \in I^{ec} \iff \frac{x}{1} \in I^e = S^{-1}I \iff \exists a \in I, s \in S, \frac{x}{1} = \frac{a}{s}$，即 $\exists u \in S, u(xs-a) = 0$，故 $xus = au \in I$，即 $\exists us \in S, x \in (I : us)$

(4) $1 \in I^{ec} \iff \exists s \in S, 1 \in (I : s)$，即 $I \cap S \neq \emptyset$。

(5) I 是局限$\iff I = I^{ec} \iff I \supset I^{ec}$，即(由(3))$\forall xs \in I$，我们有 $x \in I$，即 $\forall \bar{x}\bar{s} = 0 \in R/I$，$\bar{x} = 0 \in R/I$，即 s 不是 R/I 中的零因子。

(6) 一方面，若 $\mathfrak{q}$ 是 $S^{-1}R$ 中的素理想，则 $\forall ab \in \mathfrak{q}^c$，$\frac{a}{1}\frac{b}{1} \in \mathfrak{q}$，故 $\frac{a}{1} \in \mathfrak{q}$ 或 $\frac{b}{1} \in \mathfrak{q}$，即 $a \in \mathfrak{q}^c$ 或 $b \in \mathfrak{q}^c$，这表明 $\mathfrak{q}^c$ 是素理想，且由 (2) 和 (4) 知 $\mathfrak{q}^c \cap S = \emptyset$。

另一方面，若 $\mathfrak{p} \cap S = \emptyset$ 是 S 中的素理想，则 $S^{-1}R/S^{-1}\mathfrak{p} \cong S^{-1}(R/\mathfrak{p})$ 是整环，由于若 $\frac{a}{s}\frac{b}{t} = 0$，则存在 $u \in S, uab = 0 \in R/\mathfrak{p}$，且由于 $\mathfrak{p} \cap S = \emptyset$，故 $u \neq 0$，这表明 $ab = 0$，进而 $a = 0$ 或 $b = 0$，故 $\mathfrak{p}^e = S^{-1}\mathfrak{p}$ 是素理想。

(7) **推论2.7** 中已证明前三者。我们来证明 $S^{-1}(r(I)) = r(S^{-1}(I))$。

回忆，我们有 $r(I) = \cap_{I\subset\mathfrak{p}}\mathfrak{p}$，故 $S^{-1}(r(I)) = \cap_{I\subset\mathfrak{p}}S^{-1}\mathfrak{p}$。又 $S^{-1}\mathfrak{p}$ 包含了所有 $S^{-1}R$ 的素理想，故 $S^{-1}(r(I)) \subset r(S^{-1}I)$。

另一方面，若 $\frac{x}{s} \notin S^{-1}(r(I))$，则存在素理想 $\mathfrak{q} \supset I, x \notin \mathfrak{q}$，即 $\frac{x}{s} \notin S^{-1}\mathfrak{q}$，则 $\mathfrak{q} \cap S = \emptyset$，且 $\frac{x}{a} \notin r(S^{-1}I)$。 □

推论 2.9

设 $f: R \to R'$ 是环同态，$\mathfrak{p}$ 是 R 的素理想，则 $\mathfrak{p}$ 是 R' 中一个素理想的局限当且仅当 $\mathfrak{p}^{ec} = \mathfrak{p}$。

证明. 只需证“$\Longleftarrow$”。

令 $S = R \setminus \mathfrak{p}$，$f(S)$ 是乘性子集，我们有同态 $l: R' \to f(S)^{-1}R'$。令 $\mathfrak{q}'$ 是 $\mathfrak{p}^e$ 在 $f(S)^{-1}R$ 的扩张。由于 $\mathfrak{p}^{ec} = \mathfrak{p}$，$\mathfrak{p}^e \cap S = \emptyset$，我们有 $\mathfrak{q}' \neq (1) \in f(S)^{-1}R'$。设 $\mathfrak{m}$ 是包含 $\mathfrak{q}'$ 的极大理想，令 $\mathfrak{q} = l^{-1}(\mathfrak{m})$，则 $\mathfrak{q}$ 是素理想，$\mathfrak{q} \supset \mathfrak{p}^e$，$\mathfrak{q} \cap f(S) = \emptyset$，故 $\mathfrak{q}^c \supset \mathfrak{p}$ 且 $\mathfrak{q}^c \cap S = \emptyset$ 即 $\mathfrak{q}^c = \mathfrak{p}$。 $\square$

2.4 整相关性

定义 2.25

$R\subset R', x\in R'$ **在** R **上整(integral over** R**)**，若 x 是 R 上某个首一多项式的根。

例 2.10

R 中的元素都是 R 上的整元，$\mathbb{Q}$ 中在 $\mathbb{Z}$ 上的整元为 $\mathbb{Z}$。

例 2.11

域 F 上的代数元是整元。

命题 2.21

设 $R\subset R'$，如下命题等价：

- $x\in R'$ 在 R 上整；
- $R[x]$ 是有限生成 R–模；
- $R[x]$ 被包含于 R' 的子环，它是有限生成 R–模；
- 存在忠实的 $R[x]$–模 M 是有限生成 R–模。

证明. (1) $\Longrightarrow$ (2)：设 $x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0=0$，则 $R[x]$ 由 $\{1,x,\cdots,x^{n-1}\}$ 生成。

(2) $\Longrightarrow$ (3) $\Longrightarrow$ (4) 是显然的。

(4) $\Longrightarrow$ (1)：由于 $xM\subset M$，由 Caylay-Hamilton 定理，存在 $a_0,\cdots,a_{n-1}\in R$，使得 $(x^n+a_{n-1}x^{n-1}+\cdots+a_0)M=0$。由于 M 是忠实的，故 $x^n+a_{n-1}x^{n-1}+\cdots+a_0=0$。 □

推论 2.10

R' 中在 R 上整的元素构成了 R' 的一个子环。

证明. 首先我们先证明如下引理：

引理 2.5

M 在 B 上有限生成，B 是有限生成 R–模，则 M 在 R 上有限生成。

Lemma's proof. 若 M 在 B 上由 $\{a_1,\cdots,a_n\}$ 有限生成，B 由 $\{b_1,\cdots,b_m\}$ 有限生成，则 M 在 R 上由 $\{a_ib_j\}$ 有限生成。 □

推论 2.11

$a_1,\cdots,a_n$ 在 R 上整，则 $R[a_1,\cdots,a_n]$ 是有限生成 R–模。

由上结论，若 x,y 是整的，则 $R[x+y],R[xy]$ 被包含于 $R[x,y]\subset R'$，故 $x+y,xy$ 也是整的。 □

定义 2.26

$R\subset R'$，R' 中的整元构成的环 A 称为 R 在 R' 中的**整闭包(integral closure)**。若 $A=R$ 则称 R 在 R' 中**整闭的(integrally closed)**，若 $A=R'$ 则称 R' **在 R 上整(integral over R)**

定义 2.27

$f:R\to R'$ 称为**整的(integral)**，若 R' 在 $f(R)$ 上是整的，这时候我们称 R' 是**整R–代数(integral R-algebra)**。

注：回忆：我们称 R' 是**有限类的(finite type)**若存在 $x_1,\cdots,x_n\in f(R)$，R' 中任一元素可以被写成 $x_1,\cdots,x_m$ 的多项式，称 R' 是**有限的(finite)**若它是有限生成 R–模。若 R' 是整的且是有限类的，设 x_i 的极小多项式的次数为 d_i，则 R' 由 $\{x_i^{k_i}\}_{k_i\le d_i-1}$ 生成，故 R' 是有限的。反过来，若 R' 是有限的，由上命题 R' 是整的。因此：

$$\text{finite type + integral = finite}$$

命题 2.22

设 $R\subset R'$，R' 在 R 上整，则如下命题成立：

- 设 J 是 R' 中理想，$I=J^c=J\cap R$，则 R'/J 在 R/I 上整；
- 设 S 是 R 中乘性子集，则 $S^{-1}R'$ 在 $S^{-1}R$ 上整。

推论 2.12

设 $R\subset R'\subset R''$，R' 在 R 上整，R'' 在 R' 上整，则 R'' 在 R 上整。

证明. 设 $x\in R'',x^n+a_{n-1}x^{n-1}+\cdots+a_0=0$，$a_i\in R'$ 在 R 上整。故 $R[a_0,\cdots,a_{n-1}]$ 是有限生成 R–模，故 x 在 $R[a_0,\cdots,a_{n-1}]$ 上整，$R[x,a_0,\cdots,a_{n-1}]$ 在 $R[a_0,\cdots,a_{n-1}]$ 上有限生成，进而 $R[x,a_i]$ 在 $R[a_0,\cdots,a_{n-1}]$ 上有限生成，故 x 在 R 上整。 □

推论 2.13

$R\subset R'$，S 是 R 的乘性子集。设 A 是 R 的整闭包，则 $S^{-1}A$ 是 $S^{-1}R$ 的整闭包。

证明. 首先我们有 $S^{-1}A$ 在 $S^{-1}R$ 上是整的。取 $\frac{x}{s}\in S^{-1}R'$ 是整的，则有

$$(\frac{x}{s})^n+\frac{a_{n-1}}{s_{n-1}}(\frac{x}{s})^{n-1}+\cdots+\frac{a_0}{s_0}=0$$

其中 $a_i\in R$。两边乘 $(s\cdot s_1\cdots s_n)^n$ 有：

$$(x\cdot s_1\cdots s_n)^n+a_1\cdot s^{n-1}(x\cdot s_1\cdots s_n)^{n-1}+\cdots+\frac{a_n}{s}\cdot(s\cdot s_1\cdots s_n)^n=0$$

这表明 $x\cdot s_1\cdots s_n$在 R 上整故属于 A，进而 $\frac{x}{s}=\frac{x\cdot s_1\cdots s_n}{s\cdot s_1\cdots s_n}\in S^{-1}A$。 □

2.4.1 上升/下降定理

定理 2.3 (上升定理)

$R \subset R'$，R' 在 R 上整。设 I 是 R 的理想，$\mathfrak{p} \subset R$ 是包含 I 的素理想。I' 是 R' 的理想满足 $I' \cap R = I$。则存在 $\mathfrak{p}'$ 是 R' 的素理想满足 $\mathfrak{p}' \cap R = \mathfrak{p}$。

为证明该定理，我们先证明若干结论。

命题 2.23

$R \subset R'$ 是整环，R' 在 R 上整，则 R 是域 $\Longleftrightarrow$ R' 是域。

证明. “$\Longrightarrow$”：设 $x \neq 0 \in R'$，有 $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$，不妨 $a_0 \neq 0$，则 $x \cdot (x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1)(-a_0)^{-1} = 1$，故 $x^{-1} \in R'$，进而 R' 是域。

“$\Longleftarrow$”：设 $x \in R$，则 $x^{-1} \in R'$，有 $x^{-n} + a_{n-1}x^{-n+1} + \cdots + a_0 = 0$，故 $x^{-1} = -a_{n-1} - a_{n-2}x - \cdots - a_0x^{n-1} \in R$，进而 R 是域。 □

推论 2.14

$R \subset R'$，R' 在 R 上整，$\mathfrak{p}'$ 是 R' 的素理想，$\mathfrak{p} = \mathfrak{p}' \cap R$ 是 R 的素理想。则 $\mathfrak{p}'$ 是 R' 的极大理想 $\Longleftrightarrow$ $\mathfrak{p}$ 是 R 的极大理想。更进一步的，若 R' 的素理想 $\mathfrak{q}'$ 包含 $\mathfrak{p}'$，$\mathfrak{p}' \cap R = \mathfrak{q}' \cap R = \mathfrak{p}$，则 $\mathfrak{p}' = \mathfrak{q}'$。

证明. 第一个部分由 **命题 2.22** 和 **命题 2.23** 推出。

对于第二个部分，设 $S = R \backslash \mathfrak{p}, S^{-1}R = R_{\mathfrak{p}}$。设 $\mathfrak{n}, \mathfrak{p}''$ 分别是 $\mathfrak{p}, \mathfrak{p}'$ 的扩张。回忆 $\mathfrak{n}$ 是 $S^{-1}R$ 的极大理想，故 $\mathfrak{p}''$ 是极大的。类似的，设 $\mathfrak{q}''$ 是 $\mathfrak{q}'$ 的扩张，则 $\mathfrak{q}''$ 也是极大的且 $\mathfrak{q}'' \supset \mathfrak{p}''$，故 $\mathfrak{p}'' = \mathfrak{q}''$，由**命题 2.20**知 $\mathfrak{p}' = \mathfrak{q}'$。

$$
\begin{tikzcd}
R \arrow[r, hook] \arrow[d] & R' \arrow[d] \\
R_{\mathfrak{p}} \arrow[r, hook] & S^{-1}R'
\end{tikzcd}
$$

□

推论 2.15

$R \subset R'$，R' 在 R 上整，$\mathfrak{p}$ 是 R 的素理想，则存在 R' 的素理想 $\mathfrak{p}'$，$\mathfrak{p}' \cap R = \mathfrak{p}$。

证明. 同样考虑 $S = R \setminus \mathfrak{p}$，令 $\mathfrak{n}$ 是 $S^{-1}R'$ 的极大理想，由上推论我们有 $\mathfrak{m} = n \cap S^{-1}R$ 是极大的。注意到 $S^{-1}R$ 是局部环且其极大理想为 $S^{-1}\mathfrak{p}$，故 $\mathfrak{m} = S^{-1}\mathfrak{p}$。取 $\mathfrak{p}$ 为 $\mathfrak{n}$ 的局限即有素理想 $\mathfrak{p}'$ 满足 $\mathfrak{p}' \cap R = \mathfrak{p}$。 □

proof of going-up. 回忆 R'/I' 在 R/I 上整，$\bar{\mathfrak{p}}$ 是 R/I 的素理想。由上推论存在 R'/I' 中的素理想 $\overline{\mathfrak{p}'}$，$\overline{\mathfrak{p}'} \cap R/I = \bar{\mathfrak{p}}$。我们提升 $\overline{\mathfrak{p}'}$ 至 $\mathfrak{p}' \subset R'$，则 $\mathfrak{p}'$ 是素理想，$\mathfrak{p}' \supset I'$，$\mathfrak{p}' \cap R = \mathfrak{p}$。

$$\begin{tikzcd} R \arrow[r, hook] \arrow[d] & R' \arrow[d] \\ R/I \arrow[r, hook] & R'/I' \end{tikzcd}$$

□

定义 2.28

设 R 是整环，K 是 R 的分式域，则 R 称为整闭的若 R 在 K 中整闭。

例 2.12

UFD 是整闭的。

整闭是一种局部性质：

命题 2.24

R 是整环，则如下命题等价：

- R 是整闭的；
- 对任意素理想 $\mathfrak{p}$，R_p 是整闭的；
- 对任意极大理想 $\mathfrak{m}$，R_m 是整闭的。

证明. 设 K 是 R 的分式域，$A \subset K$ 是 R 在 K 中的整闭包。由**命题 2.22**，$A_\mathfrak{p}$ 是 $R_\mathfrak{p}$ 在 $K_\mathfrak{p} = K$ 中的整闭包。R 是整闭的当且仅当 $f : A \to R$ 是满射；$R_\mathfrak{p}$ 是整闭的当且仅当 $f_\mathfrak{p}$ 是满射。结合**命题 2.18**即证。 □

定义 2.29

对理想 $I \subset R \subset R'$，$x \in R'$ 称为**在 I 上整(integral over I)**，若存在 $a_i \in I$ 满足 $x^n + a_1x^{n-1} + \cdots + a_n = 0$。这样的元素构成了 I 的一个整闭包(这不一定构成环)。

命题 2.25

$R \subset R'$，A 是 R 的整闭包。设 I^e 是 I 在 A 中的扩张，则 I 在 R' 中的整闭包是 $r(I^e)$。特别的，I 的整闭包在加法和乘法运算下封闭。

证明. 设 $x \in R'$ 是 I 上的整元，则存在 $a_i \in I$，$x^n + a_1x^{n-1} + \cdots + a_n = 0$，则 $x^i \in A$，故 $x^n = -a_1x^{n-1} - \cdots - a_n \in I^e$，即 $x \in r(I^e)$。

反过来，若 $x \in r(I^e)$，则存在 n，$x^n \in I^e$。设 $x^n = a_1x_1 + \cdots + a_nx_n$，其中 $a_i \in A$，$x_i \in I$。考虑 $M = R[a_1, \cdots, a_n]$ 是有限生成 $R-$模，$x^nM \subset IM$，则由 Cayley-Hamilton 定理，x^n 是 I 上的整元，故 x 是 I 上的整元。 □

命题 2.26

$R \subset R'$ 是整环，R 是整闭的，K 是 R 的分式域。令 $x \in R'$ 是 $I \subset R$ 上的整元，则 x 在 K 上的极小多项式形如 $x^n + a_1 x^{n-1} + \cdots + a_n$，其中 $a_i \in r(I) \subset R$。

证明. 设 $L = K[x_1, \cdots, x_n]$ 是 $g(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ 的分裂域。注意到我们有 $h(x) = x^m + b_1 x^{m-1} + \cdots + b_m = 0, b_i \in I$，故 $g(x) \mid h(x)$。则 $h(x_i) = 0$，即 x_i 是 I 上整元。由上引理我们有 $x_i \in r(I^e) = r(I)$，由韦达定理有 $a_i \in r(I)$。 □

定理 2.4 (下降定理)

$R \subset R'$ 是整环，R 是整闭的，R' 在 R 上整。若有素理想 $\mathfrak{q} \subset \mathfrak{p} \subset R$，且素理想 $\mathfrak{p}' \subset R'$，$\mathfrak{p}' \cap R = \mathfrak{p}$，则存在 R' 的素理想 $\mathfrak{q}' \subset \mathfrak{p}'$，$\mathfrak{q}' \cap R = \mathfrak{q}$。

证明. 考虑 $R \subset R' \subset R'_{\mathfrak{p}'}$，我们来证明 $\mathfrak{q}$ 是 $R'_{\mathfrak{p}'}$ 的一个局限理想。由**推论 2.9**知只需证明 $\mathfrak{q}R'_{\mathfrak{p}'} \cap R \supset \mathfrak{q}$。首先显然 $\mathfrak{q}R'_{\mathfrak{p}'} \cap R \supset \mathfrak{p}$。

对任意 $\frac{x}{s} \in \mathfrak{q}R'_{\mathfrak{p}} \cap R, x \in \mathfrak{q}R', s \in R' \setminus \mathfrak{p}'$，则由于 $\mathfrak{q}R' \subset r(\mathfrak{q}^e)$，$x$ 在 $\mathfrak{q}$ 上整。令 K 是 R 的分式域，由**命题 2.26**知 x 在 K 上的极小多项式形如 $x^n + a_1 x^{n-1} + \cdots + a_n$，其中 $a_i \in r(\mathfrak{q}) = \mathfrak{q}$。

由于 $s = \frac{s}{x} \cdot x$，故 s 在 K 上的极小多项式形如 $s^r + a_1(\frac{s}{x})s^{r-1} + \cdots + a_n(\frac{s}{x})^n$。因为 s 在 R 上整，由**命题 2.26**我们有 $a_i(\frac{s}{x})^i \in R$。注意到 $a_i(\frac{s}{x})^i \cdot (\frac{x}{s})^i = a_i \in \mathfrak{q}$，若 $\frac{x}{s} \notin \mathfrak{q}$，则 $a_i(\frac{s}{x})^i \in \mathfrak{q} \Longrightarrow s^r \in \mathfrak{q}R' \subset \mathfrak{p}R' = \mathfrak{p}' \Longrightarrow s \in \mathfrak{p}'$，矛盾！

现在设 $\mathfrak{q} = \mathfrak{q}'' \cap R$，则 $\mathfrak{q}'$ 是 R' 的素理想，由**命题 2.20**知 $\mathfrak{q}' \subset \mathfrak{p}'$，且 $\mathfrak{q}' \cap R = \mathfrak{q}$。 □

2.4.2 赋值环

定义 2.30

设 R 是整环，K 是 R 的分式域。R 称为 K 的**赋值环(valuation ring)**，若对任意 $x \in K$，$x \in R$ 或 $x^{-1} \in R$。

注：令 U 为 R 的所有单位，考虑自然映射 $\nu : K^* \to K^*/U$。则我们可以定义其上序关系：$x \geq y$ 当且仅当 $x = yr$，其中 $r \in R$，即 $xy^{-1} \in R$。容易验证序关系是良定义的，且若 R 是赋值环，则这个序是完备的。

命题 2.27

R 是赋值环，则如下命题成立：

- R 是局部环；
- 若 $R \subset R' \subset K$，则 R' 是赋值环；
- R 是整闭的。

证明. (1)(2) 是显然的。

(3)：若 $x \in K$ 在 R 上整，设 $x^n + a_1 x^{n-1} + \cdots + a_n = 0$，$a_i \in R$。若 $x \notin R$，则 $x^{-1} \in R$，故 $x = -a_1 - a_2 x^{-1} - \cdots - a_n x^{1-n} \in R$，矛盾。 □

推论 2.16

若 R 是赋值环，则对任意 S，$S^{-1}R$ 是赋值环。

证明. 由 $R \subset S^{-1}R \subset K$ 即得。 □

定理 2.5

设 R 是域 K 的子环，$\bar{R}$ 是 R 在 K 中的整闭包，则

$$\bar{R} = \bigcap_{\substack{A\text{赋值环} \\ R \subset A}} A$$

证明. 一方面若 $x \in \bar{R}$，则 x 在 R 上整，故 x 在任意赋值环 $A \supset R$ 上整。由于 A 是整闭的，故 $\bar{R} \subset \cap_A A$。

另一方面，下次再写。 □

命题 2.28

$R \subset R'$ 是整环，R' 在 R 上有限生成。取 $0 \neq u' \in R'$，则存在 $0 \neq u \in R$ 使得对任意同态 $f : R \to F$，其中 F 是代数闭域，满足 $f(u) \neq 0$。则 f 可被延拓至 $f' : R' \to F$ 使得 $f'(u') \neq 0$。

证明. 由归纳我们可以假设 R' 仅由 x 生成。

若 x 在 R 上超越。令 $u' = a_n x^n + \cdots + a_0$，取 $u = a_n$。对任意 $f(a_n) \neq 0$，我们可以取 $f(x) \in F$ 不是 $f(a_n)X^n + \cdots + f(a_0) = 0$ 的根。我们这样扩张 f：

$$f(b_m x^m + \cdots + b_0) = f(b_m) f(x)^m + \cdots + f(b_0)$$

则由定义 $f(u') \neq 0$。

若 x 在 R 上代数。则 u' 在 R 上代数。令 K 是 R 的分式域，则 u'^{-1} 在 K 上是代数的。故存在 $b_i, c_i \in R$，$b_n x^n + \cdots + b_0 = 0$，$c_m u'^{-m} + \cdots + c_0 = 0$。取 $u = b_n c_m \in R$，则对任意 $f : R \to F$，$f(u) = \neq 0$，我们可以将其扩张为 $f' : R[u^{-1}] \to F, f'(u^{-1}) = f(u)^{-1}$。在**定理 2.5** 的证明中我们找到了 $R[u^{-1}]$ 的分式域 K 上的赋值环 A，$A \supset R[u^{-1}]$，f' 可以扩张为 $f'' : A \to F$。x 在 $R[u^{-1}]$ 上整，故由**定理 2.5**，$x \in A$，即 $R' \subset A$，特别的 $u' \in A$。由于 u'^{-1} 在 $R[u^{-1}]$ 上整，同理 $u'^{-1} \in A$，故 u' 是 A 中的单位。即 $f''(u') \neq 0$。现在取 f'' 在 R' 上的限制我们就完成了证明。

$$\begin{tikzcd}
R \arrow[r, "f"] \arrow[d] & F \\
R[u^{-1}] \arrow[ur, "f'"] \arrow[d] & \\
A \arrow[uur, "f''"] & R' \arrow[l] \arrow[uu]
\end{tikzcd}$$

□

推论 2.17 (Hilbert's Nullstellensatz)

- 设 k 是域，R 是有限生成 k–代数。若 R 是域，则 R 是 k 的有限扩张；
- 若 $k=\bar{k}$，则 $k[x_1,\cdots,x_n]$ 的极大理想形如 $(x_1-a_1,\cdots,x_n-a_n), a_i\in k$。

证明. (1)：取 $u'=1$，则任意 $k\to\bar{k}$ 可被扩张为 $R\to\bar{k}$。设 R 由 $a_1,\cdots,a_n$，则 a_i 是代数的，故 R 是有限扩张。

(2)：考虑 $k[x_1,\cdots,x_n]/\mathfrak{m}$，由 (1) 这是一个 k 的有限扩张，即 $k[x_1,\cdots,x_n]/\mathfrak{m}\cong k$。故对任意 x_i，存在 $a_i,\bar{x}_i=\bar{a}_i$，即 $x_i-a_i\in\mathfrak{m}$，故 $\mathfrak{m}\supset(x_1-a_1,\cdots,x_n-a_n)$。

相反的，考虑 $f:k[x_1,\cdots,x_n]\to k, p(x_1,\cdots,p_n)\mapsto p(a_1,\cdots,a_n)$，显然有 $\ker f=(x_1-a_1,\cdots,x_n-a_n)$ 是极大理想。 □

2.5 Noether 模和 Artin 模

定义 2.31

$R-$模 M 称为 Noether 模，若其满足升链条件：$M_1 \subset M_2 \subset \cdots \Longrightarrow \exists k, M_k = M_{k+1} = \cdots$。
$R-$模 M 称为 Artin 模，若其满足链降条件：$M_1 \supset M_2 \supset \cdots \Longrightarrow \exists k, M_k = M_{k+1} = \cdots$。

定义 2.32

环 R 称为 Noether/Artin 环若它对自身是 Noether/Artin 模。

例 2.13

有限群看作 $\mathbb{Z}-$模既是 Noether 也是 Artin 模。

例 2.14

- $\mathbb{Z}$ 是 Noether 的但不是 Artin 的；
- 任一域既是 Noether 也是 Artin 的；
- 任一 PID 是 Noether 的。

例 2.15

$k[x]$ 是 Noether 的但不是 Artin 的，$k[x_1, x_2, \cdots]$ 既不是 Noether 也不是 Artin 的。

例 2.16

Noether/Artin 环的子环不一定是 Noether/Artin 环，如 $k[x_1, x_2, \cdots]$ 的分式域是域。

后文中我们会证明任一 Artin 环均为 Noether 环。

命题 2.29

M 是 Noether 的当且仅当任意 M 的子模都是有限生成的。

证明. “$\Longrightarrow$”：令 N 是 M 的子模，若 N 不是有限生成的，设 $x_1 \in N, x_2 \in N \setminus Rx_1, x_3 \in N \setminus (Rx_1 + Rx_2), \cdots$，则我们有升链：

$$Rx_1 \subset Rx_1 + Rx_2 \subset \cdots$$

由于 M 是 Noether 的，故存在 n，$Rx_1 + Rx_2 + \cdots + Rx_n = Rx_1 + \cdots + Rx_{n+1}$，矛盾！

“$\Longleftarrow$”：对任意 $M_1 \subset M_2 \subset \cdots, M = \bigcup M_i$ 由一些 $x_1, \cdots, x_n$ 生成，则存在 a_i，$x_i \in M_{a_i}$，取 $m = \max a_i$，则 $M_m = M$。 □

命题 2.30

令 $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ 是短正合列。则 M 是 Noether/Artin 的当且仅当 M', M'' 均为 Noether/Artin 的。特别的，由于 $0 \to M' \to M' \oplus M'' \to M'' \to 0$ 是正合的，故 Noether/Artin 模的直和也是 Noether/Artin 的。

证明. 下次再补。 □

命题 2.31

R 是 Noether/Artin 环，M 是有限生成 $R-$模，则 M 是 Noether/Artin 模。令 I 是 R 的理想，则作为 $R-$模 R/I 是 Noether/Artin 的。

证明. 设 M 是 R^n 的商模，则我们有正合列

$$0 \to \ker f \to R^n \xrightarrow{f} M \to 0$$

由**命题 2.30**，我们有正合列 $0 \to I \to R \to R/I \to 0$，故 R/I 是 Noether/Artin 的。 □

定义 2.33

一个 $R-$模 M 称为单模，若它没有非平凡的子模。一个合成列是一列子模

$$M = M_0 \supsetneqq M_1 \supsetneqq M_2 \supsetneqq \cdots \supsetneqq M_n = 0$$

其中 M_i/M_{i+1} 是单模。n 称为这个合成列的长度。

命题 2.32

合成列的长度相同。

证明. 对 $R-$模 M，记 $l(M)$ 为其合成列中最小的长度。我们断言若 $N \subsetneqq M, l(M) < \infty$，则 $l(M) > l(N)$。

若该断言成立，则对任意序列 $M = M_0 \supsetneqq M_1 \supsetneqq M_2 \supsetneqq \cdots \supsetneqq M_n = 0$，我们有 $l(M) > l(M_1) > \cdots > l(M_n) = 0$，故 $l(M) \geq n$，但由定义 $l(M) \leq n$，故 $n = l(M)$。

现在我们来证明这个断言。取 M 的一个合成列，$M = M_0 \supset M_1 \supset M_2 \supset \cdots \supset M_l = 0$，其中 $l = l(M)$。则

$$N = M_0 \cap N \supset \cdots \supset M_l \cap N = 0$$

是 N 的合成列，这是因为 $M_i \cap N/M_{i+1} \cap N \subset M_i/M_{i+1}$ 是单的，故 $M_i \cap N = M_{i+1} \cap N$ 或 $M_i \cap N/M_{i+1} \cap N = M_i/M_{i+1}$。若第一种情况发生了，则我们可以删去一些项，这表示 $l(N) < l(M)$。否则我们可以归纳得到 $M_i = M_i \cap N$，这表明 $M = N$。 □

命题 2.33

M 有合成列当且仅当 M 既是 Noether 又是 Artin 的。

证明. “$\Longleftarrow$”：对全体子模用升链条件我们有极大子模 $M_1 \subset M$，M/M_1 是单的。类似的得到 $M_1 \supset M_2 \supset \cdots$，$M_i/M_{i+1}$ 是单的。再利用降链条件得到这个序列有限。

“$\Longrightarrow$”：设 M 有合成列，对任意 $M_1 \supset M_2 \supset \cdots$，$l(M_1) \le l(M_2) \le \cdots \le l(M)$ 有限，故存在 k，$l(M_k) = l(M_{k+1}) = \cdots$，即 $M_k = M_{k+1} = \cdots$，故是 Noether 的。Artin 同理。 □

注：若 $l(M) < \infty$，则任意序列 $M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_n = 0$ 可通过将 M_i/M_{i+1} 拆开扩张成合成列。

命题 2.34

定义在有限长度的 $R-$模上的 $l(M)$ 是加性函数。即对任意正合列 $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ 我们有 $l(M) = l(M') + l(M'')$。

证明. 对任意 M' 的合成列，$M' = M'_0 \supset M'_1 \supset \cdots \supset M'_m = 0$，任意 M'' 的合成列，$M'' = M''_0 \supset M''_1 \supset \cdots \supset M''_n = 0$，我们有

$$M = g^{-1}(M'') \supset g^{-1}(M''_1) \supset \cdots \supset g^{-1}(M''_n) = f(M') \supset f(M'_1) \supset \cdots \supset f(M'_m) = 0$$

是 M 的长度为 $m+n$ 的合成列。 □

推论 2.18

若环 R 满足 $(0) = \mathfrak{m}_1 \cdots \mathfrak{m}_n$，其中 $\mathfrak{m}_i$ 是极大理想，则 R 是 Noether 的当且仅当 R 是 Artin 的。

证明. 由于 $0 \to \mathfrak{m}_1 \to R \to R/\mathfrak{m}_1 \to 0$ 是正合列，R 是 Noether 的当且仅当 $\mathfrak{m}_1$ 和 $R/\mathfrak{m}_1$ 是 Noether 的，且 $R/\mathfrak{m}_1$ 在 R 上是 Noether 的当且仅当它在 $R/\mathfrak{m}_1$ 上是 Noether 的。类似的 $\mathfrak{m}_1$ 是 Noether 的当且仅当 $\mathfrak{m}_1/\mathfrak{m}_1\mathfrak{m}_2$ 在 $R/\mathfrak{m}_2$ 上是 Noether 的且 $\mathfrak{m}_1\mathfrak{m}_2$ 在 R 上是 Noether 的。继续这样下去我们有 R 是 Noether 的当且仅当对任意 i，$\mathfrak{m}_1 \cdots \mathfrak{m}_{i-1}/\mathfrak{m}_1 \cdots \mathfrak{m}_i$ 在 $R/\mathfrak{m}_i$ 上是 Noether 的。对 Artin 的讨论可以得到类似的结果。而由于 $R/\mathfrak{m}_i$ 是域，故我们可以将 Noether 替换成 Artin，便完成了证明。 □

2.5.1 诺特环

命题 2.35

R 是 Noether 环。

- 同态 $f: R \to R'$，R' 是有限生成 $R-$模，则 R' 是 Noether 的。特别的，若 f 是满射，则 R' 是 Noether 的；
- $S \subset R$ 是乘性子集，则 $S^{-1}R$ 是 Noether 的。特别的 $R_{\mathfrak{p}}$ 是 Noether 的。

证明. (1) $f(R) \cong R/\ker f$ 是 Noether 的。R' 是有限生成 $f(R)-$模，故是 Noether $f(R)-$模。因此 R' 是 Noether 的。

(2) 注意到 $S^{-1}R$ 中的理想均为扩张的，故升链条件显然成立。 □

例 2.17

数域所包含的全体代数整数形成的环是诺特环。

定理 2.6 (Hilbert basis theorem)

若 R 是 Noether 的，则 $R[x]$ 是 Noether 的。

证明. 由于 $R[X_1,\ldots,X_{n+1}]\simeq R[X_1,\ldots,X_n][X_{n+1}]$，断言化约到 $n=1$ 亦即环 $R[X]$ 的情形。给定理想 $\mathfrak{a}\subset R[X]$，我们将指出如何递归地构造一列元素 $f_1,\ldots,f_m\in\mathfrak{a}$ 使之生成 $\mathfrak{a}$ 进而导出 $R[X]$ 为 Noether 环。

对任意 $f=\sum\limits_{k=0}^{n}a_kX^k\in R[X],a_n\neq 0$，定义其领导系数为

$$\mathrm{in}(f):=a_n.$$

取 $f_1\in\mathfrak{a}\setminus\{0\}$ 使得 $\deg f_1$ 最小。今假设已选取 $f_1,\ldots,f_k\in\mathfrak{a}$，倘若 $\mathfrak{a}=\langle f_1,\ldots,f_k\rangle$ 则构造终止，否则选择 $f_{k+1}\in\mathfrak{a}$ 使得 (i) $f_{k+1}\in\mathfrak{a}\setminus\langle f_1,\ldots,f_k\rangle$；(ii) 在前述条件下 $\deg f_{k+1}$ 取最小可能的值. 置 $\alpha_i:=\mathrm{in}(f_i)$。由 R 的升链条件，理想 $\langle\alpha_1,\ldots\rangle$ 有一族生成元 $\alpha_1,\ldots,\alpha_m$。倘若上述构造可以走到第 $m+1$ 步，则有

$$\mathrm{in}(f_{m+1})=\sum_{i=1}^{m}u_i\alpha_i,\ u_1,\ldots,u_m\in R.$$

根据前 m 步的选取，对 $i=1,\ldots,m$ 皆有 $d_i:=\deg f_{m+1}-\deg f_i\geq 0$。显见

$$f_{m+1}-\sum_{i=1}^{m}u_if_iX^{d_i}\ \in\mathfrak{a}\setminus\langle f_1,\ldots,f_m\rangle$$

的次数严格小于 $\deg f_{m+1}$,此与 f_{m+1} 的选取矛盾。 □

注： 反复使用该定理我们有 $R[x_1,\cdots,x_n]$ 是 Noether 的。对任意有限生成 $R-$代数 R'，存在满射 $R[x_1,\cdots,x_n]\to R'$，故 R' 也是 Noether 的。

命题 2.36

$R\subset R'\subset R''$，R 是 Noether 的，R'' 是有限生成 $R-$代数，也是有限生成 $R'-$模，则 R' 是有限生成 $R-$代数。

证明. 我们来构造这样的 R_0：$R\subset R_0\subset R'\subset R''$ 使得 R'' 是有限生成 R_0-模，R_0 是有限生成 $R-$代数。这样由 Hilbert 基定理就有 R_0 是 Noether 的，故 R'' 是 Noether R_0-模，因此 R' 是有限生成 R_0-模。由于 R_0 是有限生成 $R-$代数，R' 也是有限生成 $R-$代数。

我们这样来构造 R_0：设 R'' 作为 $R-$代数由 $x_1,\cdots,x_m$ 生成，作为 $R-$模由 $y_1,\cdots,y_n$ 生成，则我们有

$$x_i=\sum_{j=1}^{n}a_{ij}y_j,a_{ij}\in R';y_iy_j=\sum_{k=1}^{n}a_{ijk}y_k,a_{ijk}\in R'$$

令 $R_0 = R[a_{ij}, a_{ijk}]$，这是一个有限生成 $R-$代数。对任意 $m \in R''$ 我们可以将它写成 y_i 的系数在 R_0 中的多项式，且由上关系可以将其写成 y_i 的线性表达式，即 R'' 是有限生成 R_0-模。 □

推论 2.19 (First part of Hilbert's Nullstellensatz)

k 是域，R 是有限生成 $k-$代数。若 R 是域，则也是 k 的有限扩张。

证明. 设 R 作为 $k-$代数由 $a_1, \cdots, a_n$ 生成，若 R 不是有限生成的，我们可以找到 $a_1, \cdots, a_r$ 在 k 上是代数不相关的，$a_{r+1}, \cdots, a_n$ 在 $R' = k(a_1, \cdots, a_r) \cong k(x_1, \cdots, x_r)$ 是代数的。则 R 是 R' 的有限扩张。由于 R 是有限生成 $R, k-$模，由上命题我们有 R' 在 k 上是有限生成的。

设 R' 由 $\frac{f_1}{g_1}, \cdots, \frac{f_m}{g_m}$ 生成，其中 $(f_i, g_i) = 1$，令 $h \in k[x_1, \cdots, x_r]$，满足 $(h, g_1, g_2, \cdots, g_m) = 1$，则 $\frac{1}{h}$ 不在 $k[\frac{f_1}{g_1}, \cdots, \frac{f_m}{g_m}]$ 中，矛盾！ □

2.5.2 准素分解

定义 2.34

R 是环，理想 $\mathfrak{q}$ 称为**准素的(primary)**，若 $\mathfrak{q} \neq (1)$ 且若 $xy \in \mathfrak{q}$，则 $x \in \mathfrak{q}$ 或 $y^n \in \mathfrak{q}$ 对某个 $n > 0$。等价的定义是 $R/\mathfrak{q} \neq 0$ 且其中零因子均幂零。

例 2.18

在 $\mathbb{Z}$ 中，$(0), (p^n)$ 是准素的。

在 $k[x, y]$ 中，(x^2, y) 是准素的，这是因为 $k[x, y]/(x^2, y) \cong k[x]/(x^2)$ 且 (x^2) 在 $k[x]$ 中是准素的。

命题 2.37

设 $\mathfrak{q}$ 是准素的，则 $r(\mathfrak{q})$ 是包含 $\mathfrak{q}$ 的极小素理想。

证明. Check directly by definition. □

若 $r(\mathfrak{q}) = \mathfrak{p}$，则称 $\mathfrak{q}$ 是 $\mathfrak{p}-$准素的。

例 2.19

$(x, y^2) \subset k[x, y]$，$r(x, y^2) = (x, y)$。

例 2.20

考虑 $R = k[x, y, z]/(xy - z^2)$，$\mathfrak{p} = (\bar{x}, \bar{z})$，$r(\mathfrak{p}^2) = \mathfrak{p}$，但 $\mathfrak{p}^2$ 不是准素的，因为 $\bar{x}\bar{y} = \bar{z}^2$，但 $\bar{x} \neq \mathfrak{p}^2$，$\bar{y} \neq r(\mathfrak{p}) = \mathfrak{p}$。

命题 2.38

若 $r(\mathfrak{q})$ 是极大的，则 $\mathfrak{q}$ 是准素的。特别的，对任意极大理想 $\mathfrak{m}$，$\mathfrak{m}^n$ 是准素的。

证明. $R/\mathfrak{q}$ 的幂零根是极大的，故 $R/\mathfrak{q}$ 有唯一的素理想，因此任意 $R/\mathfrak{q}$ 中的元素要么是单位的，要么是幂零的。 □

定义 2.35

I 的一个**准素分解(primary decomposition)**为 $I=\bigcap_{i=1}^n \mathfrak{q}_i$，其中 $\mathfrak{q}_i$ 是准素的，此时 I 称作**可分解的(decomposible)**。这样的分解称为极小的，若对任意 $i\neq j$，$r(\mathfrak{q}_i)\neq r(\mathfrak{q}_j)$ 且 $\bigcap_{k\neq i}\mathfrak{q}_k$ 不包含于 $\mathfrak{q}_i$。

引理 2.6

若 $\mathfrak{q}_1,\mathfrak{q}_2$ 是 $\mathfrak{q}-$准素的，则 $\mathfrak{q}_1\cap\mathfrak{q}_2$ 是 $\mathfrak{p}-$准素的。

证明. 首先 $r(\mathfrak{q}_1\cap\mathfrak{q}_2)=r(\mathfrak{q}_1)\cap r(\mathfrak{q}_2)$。若 $xy\in\mathfrak{q}_1\cap\mathfrak{q}_2$，$x\notin\mathfrak{q}_1\cap\mathfrak{q}_2$，不妨 $x\notin\mathfrak{q}_1$，则 $y\in r(\mathfrak{q}_1)=r(\mathfrak{q}_1\cap\mathfrak{q}_2)$，即 $\mathfrak{q}_1\cap\mathfrak{q}_2$ 是准素的。 □

由该引理我们知道准素分解总能化简为极小分解，然而下面给出的例子表明极小分解并不唯一。

例 2.21

$R=k[x,y]$，$I=(x^2,xy)=(x)\cap(x,y)^2=(x)\cap(x^2,y)$。

定理 2.7

I 是可分解的理想，$I=\bigcap_{i=1}^n\mathfrak{q}_i$ 是一个极小分解，设 $\mathfrak{p}_i=r(\mathfrak{q}_i)$，则

$$\{\mathfrak{p}_i\}=\left\{prime\ r(I:x)\middle|x\in R\right\}$$

由 I 唯一确定。

证明. 首先我们有 $r(I:x)=r(\bigcap_{i=1}^n\mathfrak{q}_i:x)=\bigcap_{i=1}^n r(\mathfrak{q}_i:x)$，为了计算 $r(\mathfrak{q}_i:x)$，我们需要如下引理：

引理 2.7

$\mathfrak{q}$ 是 $\mathfrak{p}-$准素理想，则

- 若 $x\in\mathfrak{q}$，则 $(\mathfrak{q}:x)=(1)$；
- 若 $x\notin\mathfrak{q}$，则 $(\mathfrak{q}:x)$ 是 $\mathfrak{p}-$准素的；
- 若 $x\notin\mathfrak{p}$，则 $(\mathfrak{q}:x)=\mathfrak{q}$。

证明. (1) 和 (3) 是显然的。对于 (2)，$y\in(\mathfrak{q}:x)\Longrightarrow xy\in\mathfrak{q}\Longrightarrow y\in r(\mathfrak{q})=\mathfrak{p}$，由于 $\mathfrak{q}\subset(\mathfrak{q}:x)$，故只能 $r(\mathfrak{q}:x)=\mathfrak{p}$。若 $yz\in(\mathfrak{q}:x),y\notin(\mathfrak{q}:x)$，则 $xyz\in\mathfrak{q},xy\notin\mathfrak{q}$，故 $z\in r(\mathfrak{q})=r(\mathfrak{q}:x)$，即 $(\mathfrak{q}:x)$ 是准素的。 □

由引理，$r(\mathfrak{q}:x)=\begin{cases}R, & x\in\mathfrak{q}_i;\\ \mathfrak{p}_i, & x\notin\mathfrak{q}_i.\end{cases}$ 故 $\bigcap_{i=1}^n r(\mathfrak{q}_i:x)=\bigcap_{x\notin\mathfrak{q}_i}\mathfrak{p}_i$。

一方面由于这个分解是极小的，我们可以找到 $x,x\notin\mathfrak{q}_i$，$x\in\bigcap_{j\neq i}\mathfrak{q}_j$，则 $(I:x)=\mathfrak{p}_i$。另一方面当 $r(I:x)$ 是素的，若 $r(I:x)\neq\mathfrak{p}_i$，我们可以取出 $y_i\notin r(I:x),y_i\in\mathfrak{p}_i$，则 $\prod y_i\in\bigcap\mathfrak{p}_i$，但因为 $r(I:x)$ 是素的，$\prod y_i\notin r(I:x)$，矛盾！ □

上面的 $\mathfrak{p}_i$ 称作**与 I 相伴的(associated)**，$\{\mathfrak{p}_i\}$ 中的最小元称作 I 的**伴随素理想(isolated prime ideals)**。

例 2.22

I 是准素的当且仅当只有一个伴随素理想。

命题 2.39

设 I 为可分解理想，则对任意素理想 $\mathfrak{p}\supset I$，$\mathfrak{p}$ 包含一个伴随素理想。

证明. 设 $\mathfrak{p}\supset I=\bigcap_{i=1}^n\mathfrak{q}_i$ 是一个极小分解，$r(\mathfrak{q}_i)=\mathfrak{p}_i$，则 $\mathfrak{p}=r(\mathfrak{p})\supset r(\bigcap_{i=1}^n\mathfrak{q}_i)\supset\bigcap_{i=1}^n r(\mathfrak{q}_i)=\bigcap_{i=1}^n\mathfrak{p}_i$，故 $\mathfrak{p}\supset\mathfrak{p}_i$，对某个 i。 □

命题 2.40

设 $I=\bigcap_{i=1}^n\mathfrak{q}_i$ 是一个极小准素分解，则 $\left\{\mathfrak{q}_i\middle|r(\mathfrak{q}_i\text{是极小的})\right\}$ 唯一确定。

证明. 详见 Atiyah。 □

现在我们来看 Noether 环的准素分解。

定义 2.36

理想 I 称为**不可约的(irreducible)**，若 $I=I_1\cap I_2$，则 $I=I_1$ 或 $I=I_2$。

例 2.23

I 是不可约的当且仅当 (0) 在 R/I 中不可约，任意素理想都是不可约的。

命题 2.41

对 Noether 环 R：

- 任意理想是有限个不可约理想的交；
- 任意不可约理想是准素理想；
- 任意理想有准素分解。

证明. (1)：设 $\Sigma=\{$不是有限个不可约理想的交$\}$，由 Noether 环的性质对每个升链都有上界，故由 Zorn 引理存在 Σ 的极大元 I。由于 I 是可约的，$I=I_1\cap I_2, I_1, I_2\notin\Sigma$，这是一个矛盾！

(2)：考虑商环，需要证明 (0) 是不可约的。若 $xy=0, y\neq 0$，我们有升链

$$\mathrm{Ann}(x)\subset\mathrm{Ann}(x^2)\subset\cdots$$

由 Noether 环的性质知存在 n，$\mathrm{Ann}(x^n)=\mathrm{Ann}(x^{n+1})=\cdots$。

对于 $a\in(x^n)\cap(y)$，设 $a=x^nb=cy$，则 $ax=cxy=0=x^{n+1}b$，故 $b\in\mathrm{Ann}(x^{n+1})=\mathrm{Ann}(x^n)$，即 $a=0$。由于 $y\neq 0, x^n=0$，$(x^n)\cap(y)=(0)$。

(3) 由 (1) 和 (2) 直接推出。 □

命题 2.42

R 是 Noether 环，I 是 R 的理想，则 I 包含一个 $r(I)$ 的幂。特别的，R 的幂零根是幂零的。

证明. 设 $r(I)$ 由 $x_1,\cdots,x_n$ 生成，其中 $x_i^{k_i}\in I$。令 $k=\sum_{i=1}^n(k_i-1)+1$，则 $r(I)^k\in I$。 □

推论 2.20

R 是 Noether 环，$\mathfrak{m}$ 是 A 的极大理想，则下述命题等价：

- $\mathfrak{q}$ 是 $\mathfrak{m}-$准素的；
- $\mathfrak{m}^n\subset\mathfrak{q}\subset\mathfrak{m}$，对某个 $n>0$；
- $r(\mathfrak{q})=\mathfrak{m}$。

证明. (1) $\Longrightarrow$ (2) 由上命题即得。

(2) $\Longrightarrow$ (3) 是因为 $\mathfrak{m}=r(\mathfrak{m}^n)\subset r(\mathfrak{q})\subset r(\mathfrak{m})=\mathfrak{m}$。

(3) $\Longrightarrow$ (1) 由**命题 2.38**即得。 □

命题 2.43

R 是 Noether 环，$I\neq(1)$，则伴随素理想=$\{(I:x)\}_{x\in R}$ 的素理想。

证明. 我们已证明伴随素理想是 $r(I:x)$ 中的素理想。另一方面，若 $(I:x)$ 是素理想，则 $r(I:x)=(I:x)$ 是相伴的。反过来，我们需要证明任意相伴的素理想 $\mathfrak{p}$ 对应的 $\mathfrak{q}$ 形如 $(I:y)$，其中 $y\in R$。

回忆对极小分解，$\mathfrak{p}=r(I:x)=\bigcap r(\mathfrak{q}_i:x)=\bigcap_{x\notin\mathfrak{q}_i}r(\mathfrak{q}_i)$。对任意 $x\notin I$，$x\in\bigcap_{\mathfrak{q}_i\neq\mathfrak{q}}\mathfrak{q}_i=I'$，则 $r(I:x)=\mathfrak{p}$。由**命题 2.42**知，存在 n，$\mathfrak{p}^n\subset\mathfrak{q}$。则 $I'\mathfrak{p}^n\subset I'\cap\mathfrak{q}=0$ 取这样最小的 n，则存在 $0\neq y\in I'\mathfrak{p}^{n-1}, y\mathfrak{p}=0$，即 $(I:y)\supset\mathfrak{p}$。因此 $\mathfrak{p}=(I:y)$，我们完成了证明。 □

-

2.5.3 Artin 环

命题 2.44

若 R 是 Artin 环，则任意素理想均是极大的，即幂零根与Jacobson根相等。

证明. 考虑 Artin 整环 $R' = R/\mathfrak{p}$，对任意 $0 \neq x \in R'$，我们有 $(x) \supset (x^2) \supset \cdots$，存在 n，$(x^n) = (x^{n+1})$，即存在 $y \in R'$，$x^n = x^{n+1}y$，故 $x^n(xy-1) = 0$，由于 □

定义 2.37

环 R 的 Krull 维数为素理想升链 $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ 长度 n 的最大值。

由上命题，若 R 是 Artin 的，则 $\dim R = 0$。

命题 2.45

Artin 环只有有限个极大理想。

证明. 考虑 $\Sigma = \{$极大理想的有限交$\}$，由 Artin 环的降链条件这个集合有极小元，记为 $I = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$。则对任意其他极大理想 $\mathfrak{m}$，$\mathfrak{m} \cap I = I$，故存在 i，$\mathfrak{m} = \mathfrak{m}_i$，取法有限。 □

命题 2.46

在 Artin 环中，幂零根是幂零的。

证明. 设 $\mathfrak{R}$ 是幂零根，由 Artin 环的升链条件存在 n，$\mathfrak{R}^n = \mathfrak{R}^{n+1} = \cdots$，记为 I，我们来证明 $I = 0$。若 $I \neq 0$，设 $\Sigma = \left\{J \middle| ideal J, I \cdots J \neq 0\right\}$，则 $I \in \Sigma$。由 Artin，Σ 有极小元，记为 I'，对任意 $x \in I', xI \neq 0$，$(x) \subset I'$，故 $I' = (x)$。$(xI)I = xI^2 = xI \neq 0$，故 $xI \in \Sigma$，这表明 $xI = (x)$。故存在 $y \in I \subset \mathfrak{R}$，$xy = x$。故存在 k，$y^k = 0$，$x = xy^k = 0$，矛盾！ □

定理 2.8

R 是 Artin 的当且仅当 R 是 Noether 的且 $\dim R = 0$。

证明. "$\Longrightarrow$"：设 R 是 Artin 的，则幂零根 $\mathfrak{R} = \bigcap_{i=1}^n \mathfrak{m}_i$。由上一个命题存在 k，$\prod_{i=1}^n \mathfrak{m}_i^k \subset (\bigcap_{i=1}^n \mathfrak{m}_i)^k = \mathfrak{R}^k = 0$，由**推论 2.18**知 R 是 Noether 的。

"$\Longleftarrow$"：设 R 是 Noether 的，(0) 有准素分解 $(0) = \cap \mathfrak{q}_i$。由于存在 n_i，$r(\mathfrak{q}_i)^{n_i} \subset \mathfrak{q}_i$，我们可以找到 n，$(0) = (\cap r(\mathfrak{q}_i))^n$。再由 $\dim R = 0$ 与 $r(\mathfrak{q}_i)$ 是素的知其均为极大理想，结合**推论 2.18**知 R 是 Artin 的。 □

上面定理说明了 Artin 环都是 Noether 环，但是 Artin 模不一定是 Noether 模。

例 2.24

考虑 $G \subset \mathbb{Q}/\mathbb{Z}$ 作为 $\mathbb{Z}-$模，取素数 p，$G = \frac{q}{p^n}$，其所有子模为 $(0) \subset \mathbb{Z} \subset \frac{\mathbb{Z}}{p} \subset \frac{\mathbb{Z}}{p^2} \subset \cdots$，故 G 是 Noether 模但不是 Artin 模。

例 2.25

设 R 是 Artin 局部环，极大理想为 $\mathfrak{m}$，则 $\mathfrak{m}$ 是幂零的，故 $x \in R$ 要么是单位，要么是幂零的。

例 2.26

R 是 Noether 局部环，极大理想为 $\mathfrak{m}$，若存在 n，$\mathfrak{m}^n = \mathfrak{m}^{n+1}$，由于 Noether 环的理想均有限生成，利用 Nakayama 引理，$\mathfrak{m}^n = 0$。对任意素理想 $\mathfrak{p}$，$\mathfrak{m}^n \subset \mathfrak{p}$，故 $\mathfrak{m} \subset r(\mathfrak{m}^n) \subset r(\mathfrak{p}) \subset \mathfrak{p}$，即 $\mathfrak{m} = \mathfrak{p}$。因此 $\mathfrak{m}$ 是唯一的素理想，由上定理，R 是 Artin 的。另外若 R 不是 Artin 的，则对任意 $\mathfrak{m}$，$\mathfrak{m}^n \neq \mathfrak{m}^{n+1}$。

例 2.27

维数为 0 的局部环不一定是 Noether 或者 Artin 的。考虑 $R = k[x_1, x_2, \cdots]/(x_1, x_2^2, x_3^3, \cdots)$，有唯一的素理想 $\mathfrak{p} = (\bar{x}_2, \bar{x}_3, \cdots)$，但 $(\bar{x}_1) \subset (\bar{x}_1, \bar{x}_2) \subset \cdots$ 不是稳定的。

定理 2.9 (Artin 环的结构定理)

任意 Artin 环 R 是有限个 Artin 局部环的直积，此直积在同构意义下是唯一的。

为了证明这个定理，我们需要介绍如下定义：

定义 2.38

环 R 的两个理想 I_1, I_2 称为**互素的(coprime)**，若 $I_1 + I_2 = (1)$。

引理 2.8

设 $I_1, \cdots, I_n \subset R$ 是理想，我们有自然同态 $\phi : R \to \prod R/I_i$，则：

- 若对任意 $i \neq j$，I_i 与 I_j 互素，则 $\cap I_i = \prod I_i$；
- ϕ 是满射当且仅当对任意 $i \neq j$，I_i 与 I_j 互素；
- ϕ 是单射当且仅当 $\cap I_i = (0)$。

证明. (1)：设结论对 $n-1$ 成立，即 $I = \cap_{i=2}^n I_i = \prod_{i=2}^n I_i$。我们来证明 I_1 与 I 互素。事实上对任意 $2 \leq i \leq n$，我们可以找到 $a_i \in I_1, b_i \in I_i, a_i + b_i = 1$。故 $I \ni \prod b_i = \prod(1 - a_i) \in 1 + I_1$，故 $1 \in I + I_1$。于是我们只需证明 $n = 2$ 的情形。事实上，我们有

$$I_1 \cdot I_2 \subset I_1 \cap I_2 = (I_1 \cap I_2)(I_1 + I_2) = (I_1 \cap I_2)I_1 + (I_1 \cap I_2)I_2 \subset I_1 \cdot I_2$$

故 $I_1 \cap I_2 = I_1 \cdot I_2$。

(2)：“$\Longrightarrow$”：$R \to R/I_1 \times R/I_2$ 是满射，故存在 a，$a \in I_i, a \in 1 + I_j$，即 $I_i + I_j = 1$。

“$\Longleftarrow$”：同 (1)，$I_1 + \cap_{i=2}^n I_i = (1)$，故对任意 $r_1 \in R/I_1$，我们可以找到 a_1，$\phi(a_1) = (r_1, 0, \cdots, 0)$。则对任意 $r = (r_1, \cdots, r_n), \phi(a_1 + \cdots + a_n) = r$，故 ϕ 是满射。

(3)：由 $\ker \phi = \cap I_i$ 显然。 □

定理 2.9 的证明. 存在性：我们有极小分解 $(0)=\mathfrak{q}_1\cap\cdots\cap\mathfrak{q}_n$，$r(\mathfrak{q}_i)\neq r(\mathfrak{q}_j)$ 是极大理想。故 $r(\mathfrak{q}_i)+r(\mathfrak{q}_j)=(1)$。则 $\mathfrak{q}_i+\mathfrak{q}_j=(1)$，故由上引理我们有同构

$$R\cong\prod R/\mathfrak{q}_i$$

唯一性：设 $R\cong\prod R_i$，其中 R_i 是 Artin 局部环。我们有自然投影 $\pi_i:R\to R_i$。令 $I_i=\ker\pi_i$，则 $(0)=\cap I_i$。我们希望这是一个极小分解。

首先 $r(I_i)=\pi_i^{-1}(r(0))$，其中 $r(0)$ 是 R_i 唯一的极大理想，因此 $r(I_i)$ 是极大的，故 I_i 是准素的。由上引理对任意 $i\neq j$，$I_i+I_j=(1)$，故 $r(I_i)+r(I_j)=(1)$，这表明 $r(I_i)\neq r(I_j)$。由于 $I_i+\cap_{j\neq i}I_j=(1)$，$\cap_{j\neq i}I_j$ 不包含于 I_i。

于是 $(0)=\cap I_i$ 是极小分解，由于任意素理想是极大的，故均为极小素理想。由**命题 2.40**知唯一。 □

命题 2.47

R 是 Artin 局部环且不是域，则如下条件等价：

- R 是 PID；
- 极大理想 $\mathfrak{m}$ 是主理想；
- $\dim_{R/\mathfrak{m}}\mathfrak{m}/\mathfrak{m}^2=1$。

证明. (1) $\Longrightarrow$ (2) $\Longrightarrow$ (3) 是显然的。下假设 (3) 成立。

由**推论 2.2**知 $\mathfrak{m}$ 是主理想，设为 (x)。由**命题 2.46**知存在 r，$I\subset\mathfrak{m}^r$ 但不被包含于 $\mathfrak{m}^{r+1}$，故存在 $y\in I, y=ax^r, a\notin\mathfrak{m}$。则 a 是 R 中的单位，故 $(x^r)\subset I$，即 $I=(x^r)$ 是主理想。 □

2.6 Dedekind 整环

我们在前文讨论了维数为 0 的 Noether 环。在本节中，我们来讨论维数为 1 的 Noether 整环.即任意非零素理想都是极大的。

命题 2.48

设 R 是 Noether 整环，$\dim R=1$，则任意非零、非单位的理想 I 可以唯一表示为 $I=\mathfrak{q}_1\cdots\mathfrak{q}_n$，其中 $\mathfrak{q}_i$ 是准素的且 $r(\mathfrak{q}_i)$ 是不相交的。

证明. 设 $I=\mathfrak{q}_1\cap\cdots\cap\mathfrak{q}_n$ 是极小分解，则 $r(\mathfrak{q}_i)\neq r(\mathfrak{q}_j)$ 是极大的。故 $r(\mathfrak{q}_i)+r(\mathfrak{q}_j)=(1)$，这表明 $\mathfrak{q}_i+\mathfrak{q}_j=(1)$。由**引理 2.8**知 $I=\prod\mathfrak{q}_i$。

反过来，若 $I=\prod\mathfrak{q}_i$，类似的有 $I=\cap\mathfrak{q}_i$，由于 $\dim R=1$ 故每个 $r(\mathfrak{q}_i)$ 均为相伴的。利用**命题 2.40**知唯一确定。 □

定义 2.39

K 是域，一个**离散赋值(discrete valuation)**是 K^* 上的一个满射 $\nu : K^* \to \mathbb{Z}$ 使得 $\nu(xy) = \nu(x)+\nu(y)$ 且 $\nu(x+y) \geq \min(\nu(x), \nu(y))$。令 $\nu(0) = +\infty$ 我们可以扩张 ν 到 K 上。可以验证 $R = \left\{x \middle| \nu(x) \geq 0\right\}$ 是 K 的子环，称为 K 的赋值环。一般的，整环 R 称为**离散赋值环(discrete valuation ring)**，即 DVR，若它是它的分式域的 DVR。

例 2.28

我们有 $\nu : \mathbb{Q}^* \to \mathbb{Z}, p^n \cdot \frac{a}{b} \mapsto n$，其中 $(a,p) = (b,p) = 1$，p 是固定的素数。则 $\mathbb{Q}$ 的 DVR 是局部化 $\mathbb{Z}_{(p)}$。类似的，对不可约多项式 $f(x) \in k[x]$，我们可以定义 $\nu : k(x)^* \to \mathbb{Z}, f^n(x) \cdot \frac{g(x)}{h(x)} \mapsto n$，则 $k(x)$ 的 DVR 是 $k[x]_{(f)}$。

我们有如下关于 DVR 的命题：

- 若 $\nu(x) = 0$，则 $\nu(x^{-1}) = 0$，故 $x^{-1} \in R$；反过来若 $\nu(x) > 0$ 则 $x^{-1} \notin R$。因此 $\nu(x) = 0$ 当且仅当 x 是 R 中的单位。
- 若 $\nu(x) = \nu(y) \geq 0$，则 $\nu(x/y) = 0$，故 $\frac{x}{y} \in R$，进而 $(x) \subset (y)$。类似的有 $(y) \subset (x)$，故 $(x) = (y) \subset R$。
- 对 R 的理想 I，取 $x \in I$ 使得 $\nu(x)$ 取到最小值。对任意 $y \in I$，$\nu(y) \geq \nu(x)$，故 $\frac{y}{x} \in R$，$y \in (x)$，即 $I = (x)$。于是 R 是 PID。
- 由上两个命题，我们有 R 的所有理想与 $\mathbb{Z}_{\geq 0}$ 之间的一一映射。
- 取 $\pi \in R, \nu(\pi) = 1$，则 $\nu(\pi^n) = n$。R 中所有理想满足降链：

$$(1) \supset (\pi) \supset (\pi^2) \supset \cdots$$

故 R 是 Noether 的。R 是极大理想为 (π) 的局部环且任意理想均为极大理想的幂，这表明 $\dim R = 1$。我们称 DVR 的极大理想的生成元为**uniformizer**。回忆任意赋值环都是整闭的，故任意 DVR 都是整闭的。

例 2.29

我们可以给出一个是赋值环但不是 DVR 的例子。

考虑 $R' = \bigcap_{n\geq 0} k[x^{\frac{1}{2^n}}] \subset \overline{k(x)}$，$K$ 是 R' 的分式域。考虑 $\nu : K^* \to \mathbb{Q}, f \mapsto \mathrm{ord}_0 f \in \mathbb{Q}$，可以验证这是一个赋值且它的赋值环是

$$R = \bigcup_{n\geq 0} k[x^{\frac{1}{2^n}}]_{(x^{\frac{1}{2^n}})}$$

然而 R 不是 Noether 的因为我们可以找到 x_n，$\nu(x_n) = \frac{1}{2^n}$，则

$$(x_1) \subset (x_2) \subset \cdots$$

不是稳定的，故 R 不是 DVR。

定义 2.40

极大理想为 $\mathfrak{m}$ 的 Noether 局部环 R 称为**正规局部环(regular local ring)**，若作为向量空间 $\dim R = \dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2$。显然 DVR 是正规局部环。

命题 2.49

R 是 Noether 局部整环，维数为 1，$\mathfrak{m}$ 是极大理想，$k = R/\mathfrak{m}$。则如下条件等价：

- R 是 DVR；
- R 是整闭的；
- $\mathfrak{m}$ 是主理想；
- R 是正规局部环；
- 任意非零理想均为 $\mathfrak{m}$ 的幂；
- 存在 x，任意非零理想均形如 (x^k)。

证明. 我们已经证明 $(1) \implies (2)$。

$(2) \implies (3)$：令 $0 \neq a \in \mathfrak{m}$，则 $r(a)$ 是非零素理想，由于 $\dim R = 1$ 故是极大理想，因此 (a) 是准素的。由**推论 2.20**知存在 k，$\mathfrak{m}^k \subset (a), \mathfrak{m}^{k-1} \not\subseteq (a)$。取 $b \in \mathfrak{m}^{k-1} \setminus (a)$，并取 $x = \frac{a}{b}$ 是 R 的分式环中的元素。$x^{-1} \notin R$，否则 $b = x^{-1}a \in \mathfrak{m}^k$。由条件 x^{-1} 不在 R 上整，于是 $x^{-1}\mathfrak{m}$ 不包含于 $\mathfrak{m}$，否则由 Cayley-Hamilton 定理知存在多项式 f，$f(x^{-1})\mathfrak{m} = 0$，即 $f(x^{-1})a = 0$，故 $f(x^{-1}) = 0$，矛盾！注意到 $x^{-1}\mathfrak{m} = \frac{b\mathfrak{m}}{a} \subset \frac{\mathfrak{m}^k}{a} \in R$，故 $x^{-1}\mathfrak{m} = R$，即 $\mathfrak{m} = Rx = (x)$。

$(3) \implies (4)$ 显然。

$(4) \implies (5)$：设 $\mathfrak{m}/\mathfrak{m}^2$ 由 x 生成，则 $\mathfrak{m} = (x)$。对任意理想 $I \neq 0, I \neq (1)$，则 $I \subset \mathfrak{m}$。同上存在 n，$\mathfrak{m}^n \subset I$，故可以找到 k，$I \subset \mathfrak{m}^k, I \not\subseteq \mathfrak{m}^{k+1}$。选取 $y \in I \setminus \mathfrak{m}^{k+1}$，则 $y = x^k z$，其中 $z \in R$ 且 $z \notin \mathfrak{m}$。于是 z 是 R 中的单位，且 $(y) = (x^k) = \mathfrak{m}^k$。

$(5) \implies (6)$：只需证明 $\mathfrak{m} = (x)$。利用 Nakayama 引理知 $\mathfrak{m} \neq \mathfrak{m}^2$。取 $x \in \mathfrak{m} \setminus \mathfrak{m}^2$，则由条件 $(x) = \mathfrak{m}^n$，于是 $(x) = \mathfrak{m}$。

$(6) \implies (1)$：容易验证 $\nu : a \mapsto n$ 若 $a = (x^n)$，这可以扩张成 R 的分式环上的赋值，且 $R = \{x : \nu(x) \geq 0\}$。 □

命题 2.50

R 是 Noether 整环，维数为 1，则如下条件等价：

- R 是整闭的；
- 任意准素理想是素理想的幂；
- 任意局部化 $R_{\mathfrak{p}}$ 是 DVR。

若 R 满足如上条件，我们称 R 是 **Dedekind 整环(D.D.)**。

证明. (1) $\iff$ (3)：由上一命题中的 (1) $\iff$ (2)，回忆我们有 R 是整闭的当且仅当任意局部化 $R_{\mathfrak{p}}$ 是整闭的。

(2) $\Longrightarrow$ (3)：由于 $R_{\mathfrak{p}}$ 是 Noether 局部整环维数为 1 且极大理想为 $\mathfrak{p}^e$，对任意 $R_{\mathfrak{p}}$ 的理想 I，存在 m，$(\mathfrak{p}^e)^m \subset I$，则 $I^c \supset \mathfrak{p}^m$。由上一命题中的 (1) $\iff$ (5) 我们有 $R_{\mathfrak{p}}$ 是 DVR。

(3) $\Longleftarrow$ (2)：设 $I \subset R$ 是准素的，$r(I) = \mathfrak{p}$。$I^e \subset R_{\mathfrak{p}}$，故由上一命题中的 (1) $\iff$ (5) 知存在 n，$I^e = (\mathfrak{p}^e)^n$。对素理想 $\mathfrak{q} \neq \mathfrak{p}$，$I_{\mathfrak{p}} = (\mathfrak{p}^n)_{\mathfrak{q}}$ 且 $I_{\mathfrak{p}} = (\mathfrak{p}^n)_{\mathfrak{p}}$，因此由**命题 2.18**知 $I = \mathfrak{p}^n$。 □

推论 2.21

R 是 Dedekind 整环，则任意非零理想能被唯一分解成素理想的乘积。

证明. 利用**命题 2.48**。 □

例 2.30

$k[x,y]$ 是 UFD 但不是 Dedekind 整环，因为 $\dim k[x,y] = 2$。

例 2.31

$\mathbb{Z}[\sqrt{13}]$ 是$\mathbb{Z}$ 在 $\mathbb{Q}(\sqrt{-13})$ 上的整闭包，故它是整闭的。由 Hilbert 基定理，这是 Noether 的，由上升定理我们得到 $\dim \mathbb{Z}[\sqrt{-13}] = \dim \mathbb{Z} = 1$。因此 $\mathbb{Z}[\sqrt{-13}]$ 是 Dedekind 整环。然而它不是 UFD 的因为 $14 = 2 \cdot 7 = (1+\sqrt{-13})(1-\sqrt{-13})$ 是两种分解。

例 2.32

一般的，代数数域上的整数环是 D.D.。

例 2.33

PID 是 D.D.。首先显然是 Noether 的且维数为 1。对任意局部化 $R_{\mathfrak{p}}$，也是 PID，故是 DVR，因此 R 是 D.D.。

命题 2.51

D.D. 是 PID 当且仅当是 UFD。

证明. 若 D.D. 是 UFD，设 $I = P_1 \cdots P_n \neq 0$。注意到对 $x \in P_i, x = a_1 \cdots a_m$，故 $(x) = (a_1)\cdots(a_m) \subset P_i$。$(a_i)$ 是素的，故存在 i，$(a_i) = P_i$。因此 $I = (a_1 \cdots a_m)$ 是主理想。反过来同理。 □

命题 2.52

R 是 D.D. 且仅有有限个素理想，则 R 是 PID。

证明. 设这些素理想是 $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$。对任意理想 $I \neq (0)$，我们有分解 $I = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_n^{a_n}$。故 $\mathfrak{p}_i^{a_i} \neq 0$，由 Nakayama 引理知存在 $x_i \in \mathfrak{p}_i^{a_i} \setminus \mathfrak{p}_i^{a_i+1}$。由于 $r(\mathfrak{p}_i^{a_i+1} + \mathfrak{p}_j^{a_j+1}) \supset \mathfrak{p}_i \bigcup \mathfrak{p}_j$，$\mathfrak{p}_i, \mathfrak{p}_j$ 是

极大的，我们有 $\mathfrak{p}_i^{a_i+1}+\mathfrak{p}_j^{a_j+1}=(1)$。

因此投影映射 $\pi: R\to\prod R/\mathfrak{p}_i^{a_i}$ 是满射，存在 $x\in I,\pi(x)=(\overline{x_1},\cdots,\overline{x_n})$，则 $(x)=\prod\mathfrak{p}_i^{a_i}=I$。 □

2.6.1 分式理想

定义 2.41

R 是整环，K 是分式域。K 的一个 $R-$子模 I 称为**分式理想(fractional ideal)**，若对某个 $0\neq x\in R$，$xI\subset R$。R 称为整理想若 $I\subset R$。

例 2.34

对任意 $u\in K$，uR 是分式理想，也称为主分式理想。

例 2.35

取 $R=\mathbb{Z}$，$\bigcap_{n\geq 0}\mathbb{Z}/2^n=\left\{\frac{x}{2^n}\middle| x\in\mathbb{Z},n\in\mathbb{N}\right\}$ 不是分式理想。

例 2.36

K 的任意有限生成子模均是分式理想。若 R 是 Noether 的，分式理想是有限生成的。

定义 2.42

子模 $I\subset K$ 称为**可逆的(invertible)**，若存在 $J\subset K, IJ=R$。

事实上 J 是唯一的，因为若 $IJ=R$，则 $J\subset(R:I)$。但 $(R:I)=(R:I)IJ\subset RJ=J$，故 $J=(R:I)$ 是由 I 唯一决定的。因此我们可以在可逆子模上定义群结构。

例 2.37

考虑 $R=\mathbb{Z}+2\sqrt{-1}\mathbb{Z}$，则 $K=\mathbb{Q}(\sqrt{-1})$，我们可以验证 $I=2\mathbb{Z}[\sqrt{-1}]$ 不可逆但是分式理想：注意到 $(R:I)=\mathbb{Z}[\sqrt{-1}]$，但 $(R:I)I\neq R$。然而它是可逆的，因为 $R=\mathbb{Z}[\sqrt{-1}]$ 且 $I^{-1}=\frac{1}{2}\mathbb{Z}[\sqrt{-1}]$。

命题 2.53

I 是 R 的分式理想，则如下条件等价：

- I 可逆；
- I 是有限生成的且对任意素理想 $\mathfrak{p}$，$I_{\mathfrak{p}}$ 在 $R_{\mathfrak{p}}$ 上可逆；
- I 是有限生成的且对任意极大理想 $\mathfrak{m}$，$I_{\mathfrak{m}}$ 在 $R_{\mathfrak{m}}$ 上可逆；

证明. (1) $\Longrightarrow$ (2)：$I_{\mathfrak{p}}\cdot(R:I)_{\mathfrak{p}}=R_{\mathfrak{p}}$，故 $I_{\mathfrak{p}}$ 是可逆的，且由上讨论知 I 有限生成。

(2) $\Longrightarrow$ (3) 是显然的。(3) $\Longrightarrow$ (1)：我们希望证明 $I\cdot(R:I)=R$，由于 $I\cdot(R:I)$ 是整理想，这需要证明 $I_{\mathfrak{m}}\cdot(R:I_{\mathfrak{m}})=R_{\mathfrak{m}}$。事实上这等价于证明 $(R:I)_{\mathfrak{m}}=(R_{\mathfrak{m}}:I_{\mathfrak{m}})$。

设 I 由 $x_1,\cdots,x_n$ 生成，则 $(R:I)=\bigcap_{i=1}^n(R:x_i)$，故

$$(R:I)_{\mathfrak{m}}=\bigcap_{i=1}^n(R:x_i)_{\mathfrak{m}},(R_{\mathfrak{m}}:I_{\mathfrak{m}})=\bigcap_{i=1}^n(R_{\mathfrak{m}}:\frac{x_i}{1})$$

故只需证明 $(R:x)_{\mathfrak{m}}=(R_{\mathfrak{m}},(x)_{\mathfrak{m}})$。注意到我们有正合列

$$0\to(R:x)\to R\xrightarrow{f}((x)+R)/R\to 0$$

其中 $f:y\mapsto xy+R$。故我们有正合列

$$0\to(R:x)_{\mathfrak{m}}\to R_{\mathfrak{m}}\xrightarrow{f_{\mathfrak{m}}}(x)_{\mathfrak{m}}+R_{\mathfrak{m}}/R_{\mathfrak{m}}\to 0$$

故 $(R:x)_{\mathfrak{m}}=\ker f_{\mathfrak{m}}=(R_{\mathfrak{m}},(x)_{\mathfrak{m}})$

□

命题 2.54

设 R 是局部整环，则 R 是 DVR 当且仅当任意非零分式理想是可逆的。此时任意分式理想都是主理想。

证明. “$\Longrightarrow$”：$xI\subset R$ 是 R 中的理想，故 $xI=(u)$ 是主理想，进而 $I=x^{-1}(u)$，于是 $I^{-1}=x(u^{-1})$ 是可逆的。

“$\Longleftarrow$”：由于 R 的任意整理想都是可逆的，因此是有限生成的，故 R 是 Noether 的。我们只需证明任意非零整理想都形如 $\mathfrak{m}^k$。

若该假设不成立，设 Σ 为所有不是 $\mathfrak{m}$ 幂的非零理想的集合，则由 Zorn 引理我们可以取出 Σ 中的最大元 I。注意到 $I\subset\mathfrak{m}$，故 $I\subset\mathfrak{m}^{-1}I\subset\mathfrak{m}^{-1}\mathfrak{m}=R$。

由于 $\mathfrak{m}^{-1}I$ 不是 $\mathfrak{m}$ 的幂，故 $I=\mathfrak{m}^{-1}I$，于是 $I=\mathfrak{m}I$，这由 Nakayama 引理知矛盾！ □

推论 2.22

R 是整环，则 R 是 D.D. 当且仅当 R 的任意非零分式理想是可逆的。

证明. “$\Longrightarrow$”：设 I 是分式理想，则由 R 是 Noether 的知 I 是有限生成的，且由上命题 $I_{\mathfrak{m}}$ 是可逆的。

“$\Longleftarrow$”：首先任意 R 的整理想是可逆的，因此是有限生成的，故 R 是 Noether 的。对任意素理想 $\mathfrak{p}$，$R_{\mathfrak{p}}$ 的任意分式理想 M 是可逆的，故 $A_{\mathfrak{p}}$ 是 DVR，则对任意素理想 $0\neq\mathfrak{p}\subset\mathfrak{p}$，我们有 $0\neq\mathfrak{q}_{\mathfrak{p}}\subset\mathfrak{p}_{\mathfrak{p}}$，故 $\mathfrak{q}_{\mathfrak{p}}=\mathfrak{p}_{\mathfrak{p}}$，这表明 $\mathfrak{q}=\mathfrak{p}$。因此 $\dim R=1$，由**命题 2.50**知是 D.D.。

□

设 $\mathcal{I}$ 是所有分式理想的集合，设 R 是 D.D.，则我们可以定义 $\mathcal{I}$ 上的群结构。设 I 是分式理想，$I_{\mathfrak{p}}$ 是 DVR $R_{\mathfrak{p}}$ 的分式理想，于是是主理想，故我们设 $I_{\mathfrak{p}}=(x)$，则我们可以定义 $\nu_{\mathfrak{p}}(I)=\nu_{\mathfrak{p}}(x)$，期中 $\nu_{\mathfrak{p}}$ 是 $R_{\mathfrak{p}}$ 上的赋值。于是我们得到了群同态 $\nu_{\mathfrak{p}}:\mathcal{I}\to\mathbb{Z}$，且若 $I\subset J$，则 $\nu_{\mathfrak{p}}(I)\geq\nu_{\mathfrak{p}}(J)$。

引理 2.9

$\nu_{\mathfrak{p}}(I)=0$ 仅对有限多个素理想 $\mathfrak{p}$ 不成立。

证明. 由于存在 $x\in K$，$(x)I=J\subset R$，我们有 $\nu_{\mathfrak{p}}(x)+\nu_{\mathfrak{p}}(I)=\nu_{\mathfrak{p}}(J)$。由于在 D.D. 中非零理想可唯一分解成素理想的乘积，故 $\nu_{\mathfrak{p}}(x),\nu_{\mathfrak{p}}(J)=0$ 仅对有限多个 $\mathfrak{p}$ 不成立，于是我们完成了证明。 □

由上引理我们有一个良定义的同态：

$$\phi:\mathcal{I}\to\bigoplus_{\mathfrak{p}\neq 0,\mathfrak{p}\ prime}\mathbb{Z}$$

事实上这是一个同构。对 $(a_{\mathfrak{p}})\in\oplus_{\mathfrak{p}}\mathbb{Z},\phi(\prod_{\mathfrak{p}}\mathfrak{p}^{a_{\mathfrak{p}}})=(a_{\mathfrak{p}})$，故 ϕ 是满射。若 $\phi(I)=0$，则 $I_{\mathfrak{p}}=R_{\mathfrak{p}}$ 对任意 $\mathfrak{p}$，故由局部性 $I=R=(1)$，于是 ϕ 是单射。

考虑 $\varphi:K^{*}\to\mathcal{I},x\mapsto(x)$，我们称 $\operatorname{coker}\varphi$ 为**理想类群(ideal class group)**，也称为**Picard 群**，对它的研究是代数数论的主题，我们这里浅尝辄止。

2.7 完备性

定义 2.43

一个 $R-$模的**反向系统(inverse system)**指的是 $R-$模序列 $\{M_n\}$ 与 $f_{n+1}: M_{n+1} \to M_n$。若每个 f_n 都是满的则称这个反向系统是**满系统**。
反向极限定义为 $\prod_n M_n$ 中所有满足 $f_{n+1}(a_{n+1}) = a_n$ 的 (a_n) 构成的集合，记为 $\varprojlim M_n$，这是一个 $R-$模。

由定义，我们有下图交换：

$$\begin{tikzcd}
 & \varprojlim M_\bullet \arrow[dl] \arrow[dr] & \\
M_{n+1} \arrow[rr, "f_{n+1}"] & & M_n
\end{tikzcd}$$

其中 $\varprojlim M_\bullet \to M_n$ 是自然投影。进一步我们有反向极限的万有性质，证明留作习题：

命题 2.55

对任意模 X 与同态 $\varphi_n : X \to M_n$ 使得 $f_{n+1} \circ \varphi_{n+1} = \varphi_n$，则存在唯一的同态 $g : X \to \varprojlim M_\bullet$ 使得下图交换：

$$\begin{tikzcd}
 & X \arrow[d, "g"] \arrow[ddl, "\varphi_{n+1}"'] \arrow[ddr, "\varphi_n"] & \\
 & \varprojlim M_\bullet \arrow[dl] \arrow[dr] & \\
M_{n+1} \arrow[rr, "f_{n+1}"] & & M_n
\end{tikzcd}$$

反过来，该性质唯一确定了反向极限。

定义 2.44

一个 R 的**滤链(filtration)**是序列 $M = M_0 \supset M_1 \supset M_2 \supset \cdots$。若 $IM_n \subset M_{n+1}$ 对任意 n 成立，则称为$I-$**滤链**。若 $IM_n = M_{n+1}$ 对充分大的 n 成立，则称为**稳定** $I-$**滤链**。

定义 2.45

M 对滤链 $M = M_0 \supset M_1 \supset \cdots$ 的**完备(completion)**是下反向系统的反向极限：

$$M/M_0 \leftarrow M/M_1 \leftarrow M/M_2 \leftarrow \cdots$$

记为 $\hat{M}$。
若 $M_{n+1} = IM_n$ 对任意 n 成立则称 $\hat{M}$ 为 $I - adic$ 完备。M 称为**完备的(complete)**若 $M \to \hat{M}, x \mapsto (\bar{x})_n$ 是同构。

注：从拓扑的角度看，我们可以讲 $M_1, M_2, \cdots$ 看作一组 M 的拓扑基，对序列 $(a_n)_n$，$a_m - a_n \in M_{\min m,n}$，故 $(a_n)_n$ 是 Cauchy 列，且两个等价的 Cauchy 列定义了同一个 $\hat{M}$ 中的元素。因此代数中的完备与拓扑中的完备概念相同。

例 2.38

考虑 $M=k[x]\supset(x)\supset(x^2)\supset\cdots$，则我们有 $\hat{M}\cong k[[x]]$。
类似的考虑 $\mathbb{Z}\supset p\mathbb{Z}\supset p^2\mathbb{Z}\supset\cdots$，我们称 $\hat{\mathbb{Z}}=\{\sum_{i=0}^{\infty}a_ip^i,0\le a_i\le p-1\}$ 为 $p-adic$环

命题 2.56

M 的 $I-adic$ 完备同构于对任意稳定 $I-$滤链的完备。

证明. 设我们有稳定 $I-$滤链 $0\leftarrow M/M_1\leftarrow M/M_2\leftarrow\cdots$。

首先 $M_n\supset IM_{n-1}\supset\cdots\supset I^nM$，我们有自然映射 $M/I^nM\to M/M_n$，这诱导了映射 $f:\varprojlim M/I^nM\to\varprojlim M/M_n$，反过来存在 c，对任意 $n>c$，$M_n=IM_{n-1}=\cdots=I^{n-c}M_c\subset I^{n-c}M$，故有自然映射 $M/I^kM\to M/M_{k+c}$，这诱导了映射 $g:\varprojlim M/M^n\to\varprojlim M/I^nM$。进一步我们可以验证 $f\circ g=id,g\circ f=id$，故我们完成了证明。 □

例 2.39

取 $R=\mathbb{Z}_2\otimes\mathbb{Z}_2$，$I=0\otimes\mathbb{Z}_2$，则 $I^n=I$，故 $\hat{R}=R/I=\mathbb{Z}_2\otimes 0$，且 $\ker(R\to\hat{R})=I$。

例 2.40

考虑 $R=\bigcup_n k[x^{1/2^n}]$，$I=\bigcup_n x^{1/2^n}k[x^{1/2^n}]$，则

$$I^{2^m}\supset\bigcup_n x^{1/2^{n-m}}k[x^{1/2^{n-m}}]=I$$

故 $I^{2^n}=I$，这表明 $I=I^n$。同样有 $\ker(R\to\hat{R})=I$。

定义 2.46

一个反向系统的正合列是满足下图交换的反向系统 $\{A_n\},\{B_n\},\{C_n\}$：

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A_{n+1} & \longrightarrow & B_{n+1} & \longrightarrow & C_{n+1} & \longrightarrow & 0\\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A_n & \longrightarrow & B_n & \longrightarrow & C_n & \longrightarrow & 0
\end{array}$$

命题 2.57

设 $0\to\{A_n\}\to\{B_n\}\to\{C_n\}$ 正合，则

$$0\to\varprojlim A_n\to\varprojlim B_n\to\varprojlim C_n$$

正合。进一步，若 $\{A_n\}$ 是满的，则

$$0\to\varprojlim A_n\to\varprojlim B_n\to\varprojlim C_n\to 0$$

正合。

证明. 设 $A=\prod A_n, B=\prod B_n, C=\prod C_n$，考虑 $d_A: A\to A, (a_n)\mapsto (a_n-f_{n+1}(a_{n+1}))$，则 $\varprojlim A_n=\ker d_A$，我们有下图交换：

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r] \arrow[d, "d_A"] & B \arrow[r] \arrow[d, "d_B"] & C \arrow[r] \arrow[d, "d_C"] & 0 \\ 0 \arrow[r] & A \arrow[r] & B \arrow[r] & C \arrow[r] & 0 \end{tikzcd}$$

由蛇引理，我们有正合列：

$$0\to \ker d_A\to \ker d_B\to \ker d_C\to \mathrm{coker} d_A\to \mathrm{coker} d_B\to \mathrm{coker} d_C\to 0$$

进一步若 $\{A_n\}$ 是满射，则 d_A 是满射，故 $\mathrm{coker} d_A=0$。 □

推论 2.23

设我们有正合列 $0\to M'\to M\to M''\to 0$，$M=M_o\supset M_1\supset\cdots$ 是 M 的滤链，这诱导了 M' 的滤链 $M'=M_0\cap M'\supset M_2\cap M'\supset\cdots$ 与 M'' 的滤链 $M''=\mathrm{Im}(M_0)\supset \mathrm{Im}(M_1)\supset\cdots$，于是我们有

$$0\to \hat{M}'\to \hat{M}\to \hat{M}''\to 0$$

是正合的。

证明. 在 $M'=M_n, M''=M/M_n$ 上使用上推论，我们有正合列

$$0\to \hat{M}_n\to \hat{M}\to M/M_n\to 0$$

□

2.7.1 分次环

定义 2.47

一个**分次环(graded ring)**是指一个环 R 及 R 的加法群的一组子群 $(R_n)_{n\geq 0}$ 使得 $R=\oplus_{n\geq 0}R_n$ 且 $R_m\cdot R_n\subset R_{m+n},\forall m,n\geq 0$。若 $x\in R_n$，我们称 n 为 x 的次数。由定义 R_0 是 R 的子环且 R_n 均为 R_0-模。

例 2.41

$R=k[x]=\oplus_{n\geq 0}kx^n$ 是分次环。

定义 2.48

R 是分次环。**分次 $R-$模**是指一个 $R-$模 M 及 M 的一组子群 $(M_n)_{n\geq 0}$ 使得 $M=\oplus_{n\geq 0}M_n$ 使得 $R_n\cdot M_m\subset M_{n+m},\forall m,n\geq 0$。
分次模 $M=\oplus M_n$ 与 $N=\oplus N_n$ 之间的同态是指 $R-$模同态 $f:M\to N$ 使得 $f(M_n)\subset N_n,\forall n$。

例 2.42

$R_+ = \oplus_{n\geq 1}R_n$ 是分次 $R-$模且是 R 的一个理想。

定义 2.49

一个 R 的理想 I 称为**齐次的(homogeneous)**，若它是分次 $R-$模，即 $I = \oplus_{n\geq 0}(I\cap R_n)$ 是分次的。$x\in R$ 称为**齐次元**若 $x\in R_n$ 对某个 n。
可以验证 I 是齐次的当且仅当它由齐次元生成。

若 I 是齐次的，则 $R/I = \oplus(R_n/I_n)$ 是分次环。

命题 2.58

分次环 R 是 Noether 的当且仅当 R_0 是 Noether 的且 R 是有限生成 R_0-代数。

证明. “$\Longleftarrow$” 由 Hilbert 基定理即得。

$\Longrightarrow$：首先由于 $R_0 = R/R_+$ 故 R_0 是 Noether 的。设 R_+ 由 $a_1,\cdot,a_n$ 有限生成，我们可以假设 a_i 是齐次的。现在我们来证明 $R = R_0[a_1,\cdots,a_n]$，这只需证明 $R_i\subset R_0[a_1,\cdots,a_n]$。

归纳证明之。对 $x\in R_{n+1}$，$x=\sum a_ix_i, x_i\in R, \deg x_i>0$。注意到 $\deg x_i = n+1-\deg a_i\leq n$，由归纳假设知 $x_i\in R_0[a_1,\cdots,a_n]$，故 $x\in R_0[a_1,\cdots,a_n]$。

□

对任意环 R 与理想 I，我们可以构造分次环 $R^*\oplus_{n\geq 0}I^n = R\oplus I\oplus I^2\oplus\cdots$。设 M 是 $R-$模且 (M_n)

引理 2.10

R 是 Noether 环，M 是有限生成 $R-$模，$(M_n)_n$ 是 $I-$滤链。设

$$M^* = \oplus_{n\geq 0}M_n,$$

且 M^* 是 R^*-分次模。则 M^* 是有限生成的当且仅当 $(M_n)_n$ 是稳定 $I-$滤链。

证明. 令 $M_n^* = M_0\oplus\cdots\oplus M_n\oplus IM_n\oplus I^2M_n\oplus\cdots$，则 M_n^* 是 R^*-模，且我们有链 $M_0^*\subset M_1^*\subset\cdots$ 且 $\bigcup_{n=0}^\infty M_n^* = M^*$。

一方面，若 M^* 是有限生成的，由于 R^* 是 Noether 的故 M^* 也是 Noether R^*-模，故存在 n，$M_n^* = M_{n+1}^*$，这表明 (M_n) 是稳定 $I-$滤链。

另一方面，若 (M_n) 是稳定 $I-$滤链，则存在 $M^* = M_n^*$。注意到 M_i 是有限生成的，且 M_n^* 作为 R^*-模由 $M_0,\cdots,M_n$ 生成，故 $M^* = M_n^*$ 是有限生成的，我们完成了证明。 □

引理 2.11 (Artin-Rees)

I 是 Noether 环 R 的理想，$N\subset M$ 均为有限生成模，则存在 $c>0$，使得 $I^nM\cap N = I^{n-c}(I^cM\cap N), n\geq c$。特别的，$N$ 的 $I-adic$ 完备同构于由 $(M_n)_n$ 诱导的 N 的完备。

证明. 注意到 $M^* = M \oplus IM \oplus I^2M \oplus \cdots$ 在 R^* 上有限生成，故是 Noether 的，因此 $N^* = N \oplus (IM \cap N) \oplus (I^2M \cap N) \oplus \cdots$ 在 R^* 上有限生成，进而 $(I^nM \cap N)_n$ 稳定。 □

推论 2.24

I 是 Noether 环 R 的理想，$0 \to M' \to M \to M'' \to 0$ 是有限生成 $R-$模的正合列，则 $0 \to \hat{M}' \to \hat{M} \to \hat{M}'' \to 0$ 是 $I - adic$ 完备的正合列。

命题 2.59

M 是有限生成 $R-$模，则 $\hat{R} \otimes_R M \to \hat{M}$ 是满射。若 R 是 Noether 的则是同构，特别的 $\hat{R}$ 是平坦 $R-$模。

证明. 设有

$$\begin{array}{ccccccccc} & & \hat{R} \otimes N & \longrightarrow & \hat{R}^{\oplus n} & \longrightarrow & \hat{R} \otimes M & \longrightarrow & 0 \\ & & \downarrow f & & \downarrow g & & \downarrow h & & \\ 0 & \longrightarrow & \hat{N} & \longrightarrow & \hat{R}^{\oplus n} & \longrightarrow & \hat{M} & \longrightarrow & 0 \end{array}$$

则

$$\ker f \to \ker g \to h \to \mathrm{coker} f \to \mathrm{coker} g \to \mathrm{coker} h \to 0$$

若 R 是 Noether 的，则 N 是有限生成的，故 $\mathrm{coker} f = 0$，因此 $\ker h = 0$，于是 $\hat{R} \otimes M \cong \hat{M}$。 □

推论 2.25

设 Noether 环 R 的 $I - adic$ 完备是 $\hat{R}$。

- $\hat{R} \otimes_R I \cong \hat{I} = \hat{R} \cdot I$；
- $\widehat{I^n} = (I^n)^e = (I^e)^n = \hat{I}^n$；
- $I^n/I^{n+1} \cong \widehat{I^n}/\widehat{I^{n+1}} \cong \hat{I}^n/\hat{I}^{n+1}$；
- $\hat{I}$ 被包含于 $\hat{R}$ 的 Jacb 根中；
- $\hat{R}$ 是 $\hat{I} - adic$ 完备的。

证明. (1) 由上命题即得，(2) 由 (1) 直接得到。

(3)：我们有正合列 $0 \to I^{n+1} \to I^n \to I^n/I^{n+1} \to 0$，这诱导了正合列 $0 \to \widehat{I^{n+1}} \to \widehat{I^n} \to \widehat{I^n/I^{n+1}} \to 0$，故 $\hat{I}^n/\hat{I}^{n+1} \cong \widehat{I^n}/\widehat{I^{n+1}} \cong I^n/I^{n+1}$。

(4) 由定义是显然的。

(5)： $\hat{I} = I \cdot \hat{R}$，故只需证明 $I \subset \mathrm{Jac}(\hat{R})$。对任意 $x \in I, a \in \hat{R}$，$(1 - ax)^{-1} = (ax) + (ax)^2 + \cdots \in \hat{R}$，这是因为 $(ax)^n \in \hat{I}^n$ 且 $\hat{R}$ 是 $\hat{I} - adic$ 完备的。于是 $x \in \mathrm{Jac}(\hat{R})$。 □

推论 2.26

R 是 Noether 局部环，极大理想为 $\mathfrak{m}$，则 $\hat{R}$ 是极大理想为 $\hat{\mathfrak{m}}$ 的局部环。

证明. 注意到 $\hat{R}/\hat{\mathfrak{m}} \cong R/\mathfrak{m}$ 是域，故 $\hat{\mathfrak{m}}$ 是极大理想。进一步 $\hat{\mathfrak{m}} \subset \mathrm{Jac}(\hat{R})$，故是唯一的极大理想。 □

定理 2.10 (Krull)

I 是 Noether 环 R 的理想，M 是有限生成 $R-$模，则 $M \to \hat{M}$ 的 ker 是 $E = \bigcap_n I^n M = \left\{x \in M \middle| 存在某个 a \in I, (1+a)x = 0\right\}$。

证明. 一方面若 $(1-a)x = 0$ 则 $x = ax = a^2x = \cdots$，故 $x \in E$。另一方面我们断言 $E = IE$。事实上，由 Artin-Rees：$E = I^{c+1}M \cap E = I \cdot (I^c M \cap E) = IE$。由 Hamilton-Cayley 定理知存在 $a \in I$，$(1+a)E = 0$。 □

推论 2.27

R 是 Noether 整环，$I \neq R$，则 $\bigcap_{n=0}^{\infty} I^n = 0$。

推论 2.28

R 是 Noether 环，$I \subset \mathrm{Jac}(R)$，$M$ 是有限生成 $R-$模，则 $\bigcap_{n=0}^{\infty} I^n M = 0$，特别的若 R 是局部的，$\mathfrak{m}$ 是极大的，则 $\bigcap_{n=0}^{\infty} \mathfrak{m}^n M = 0$。

推论 2.29

R 是 Noether 的，$\mathfrak{p}$ 是素理想，则 $R \to R_{\mathfrak{p}}$ 的 ker 是所有 $\mathfrak{p}-$准素理想的交。

证明. 由上推论我们有 $\bigcap_{n=0}^{\infty} (\mathfrak{p}R_{\mathfrak{p}})^n = 0$。回忆我们有 $S^{-1}R$ 的准素理想和 R 中与 S 不交的准素理想有一一对应，故

$$\ker(R \to R_{\mathfrak{p}}) = \bigcap_{\mathfrak{p}-\text{准素的}} \mathfrak{q}$$

□

定义 2.50

I 是环 R 的理想，定义 $G(R) = G_I(R) := \oplus_{n=0}^{\infty} I^n/I^{n+1}$，这是一个分次环。$M$ 是 $R-$模，$(M_n)_n$ 是 $I-$滤链，定义 $G(M) = \oplus_{n=0}^{\infty} M_n/M_{n+1}$，这是一个分次 $G(R)-$模。

命题 2.60

R 是 Noether 环，则

- $G_I(R)$ 是 Noether 的；
- $G_I(R) \cong G_{\hat{I}}(\hat{R})$；
- 若 M 是有限生成 $R-$模，$(M_n)_n$ 是稳定 $I-$滤链，则 $G(M)$ 是有限生成 $G(R)-$模。

证明. (1)：设 I 由 $x_1, \cdots, x_n$ 生成，则 $G_I(R) = (R/I)[x_1, \cdots, x_n]$，由 Hilbert 基定理知这是 Noether 的。

(2)：回忆我们有 $\widehat{I^n}/\widehat{I^{n+1}} \cong \hat{I}^n/\hat{I}^{n+1} \cong I^n/I^{n+1}$。

(3)：存在 m，对任意 $r \geq 0$，$I^r M_m = M_{m+r}$，则 $G(M)$ 由 $M/M_1, \cdot, M_{m-1}/M_m$ 生成，其中 M_{n-1}/M_n 是有限生成 $R-$模且 $I \cdot (M_{n-1}/M_n) = 0$，因此是有限生成 $R/I-$模，故是有限生成 $G(R)-$模，这表明 $G(M)$ 是有限生成 $G(R)-$模。 □

引理 2.12

$\phi : M \to N$ 是群同态，且与滤链 $(M_n), (N_n)$ 相容，则我们有自然诱导映射 $G(\phi) : G(M) \to G(N), \hat{\phi} : \hat{M} \to \hat{N}$。进一步我们有 $G(\phi)$ 是单(满)射可推出 $\hat{\phi}$ 是单(满)射。

证明. $G(\phi)$ 定义为 $G_n(\phi) : M_n/M_{n+1} \to N_n/N_{n+1}, x + M_{n+1} \mapsto \phi(x) + N_{n+1}, G(\phi) = \oplus G_n(\phi)$。

$\hat{\phi}$ 定义为 $\phi_n : M/M_n \to N/N_n, x + M_n \mapsto \phi(x) + N_n, \phi = \prod \phi_n$。

容易验证这是良定义的。于是我们有如下交换图：

$$\begin{tikzcd}
0 \arrow[r] & M_n/M_{n+1} \arrow[r] \arrow[d, "G_n(\phi)"] & M/M_{n+1} \arrow[r] \arrow[d, "\phi_{n+1}"] & M/M_n \arrow[r] \arrow[d, "\phi_n"] & 0 \\
0 \arrow[r] & N_n/N_{n+1} \arrow[r] & N/N_{n+1} \arrow[r] & N/N_n \arrow[r] & 0
\end{tikzcd}$$

由蛇引理我们有长正合列：

$$0 \to \ker G_n(\phi) \to \ker \phi_{n+1} \to \ker \phi_n \to \mathrm{coker} G_n(\phi) \to \mathrm{coker}\phi_{n+1} \to \mathrm{coker}\phi_n \to 0$$

若 $G(\phi)$ 是单射，则 $G_n(\phi)$ 是单射，$\ker G_n(\phi) = 0$，故 $\ker \phi_{n+1} \to \ker \phi_n$ 是单射。由于 $\ker \phi_0 = 0$，故由归纳易知 ϕ_n 是单射，进而 $\hat{\phi}$ 是单射。

若 $G(\phi)$ 是满射，则 $G_n(\phi)$ 是满射，$\mathrm{coker} G_n(\phi) = 0$，故 $\ker \phi_{n+1} \to \ker \phi_n$ 是满射。我们有如下交换图：

$$\begin{tikzcd}
0 \arrow[r] & \ker \phi_n \arrow[r] & M/M_n \arrow[r] & N/N_n \arrow[r] & 0 \\
0 \arrow[r] & \ker \phi_{n+1} \arrow[r] \arrow[u] & M/M_{n+1} \arrow[r] \arrow[u] & N/N_{n+1} \arrow[r] \arrow[u] & 0
\end{tikzcd}$$

由于 $\ker \phi_{n+1} \to \ker \phi_n$ 是满射，由**命题 2.57**知 $\hat{M} \to \hat{N} \to 0$ 是正合的，即 $\hat{\phi}$ 是满射。 □

命题 2.61

R 是 $I-adic$ 完备且我们有嵌入 $M\to\hat{M}$。

- 若 $G(M)$ 是有限生成 $G(R)-$模，则 M 是有限生成 $R-$模且 M 是完备的；
- 若 $G(M)$ 是 Noether 的，则 M 是 Noether 的。

证明. 设 $\bar{x}_1,\cdots,\bar{x}_n$ 生成 $G(M)$，$\bar{x}_i\in M_{n_i}/M_{n_{i+1}}$，则映射 $\phi_i:1\mapsto x_i$ 给出：

$$\begin{array}{ccccccccccc} R & \supset & R & \supset & \cdots & \supset & R & \supset & IR & \supset & \cdots \\ \downarrow & & \downarrow & & & & \downarrow & & \downarrow & & \\ M & \supset & M_1 & \supset & \cdots & \supset & M_{n_i} & \supset & M_{n_i+1} & \supset & \cdots \end{array}$$

我们可将第一行视作 $I-$滤链，ϕ_i 与该滤链相容。取直和，我们有 $\phi:R^{\oplus n}\to M$ 且 $G(\phi):G(R^{\oplus n})\to G(M)$ 是满射，这是因为 $G(M)$ 由 $\bar{x}_1,\cdots,\bar{x}_n$ 生成。故由上命题知 $\hat{\phi}:\widehat{R^{\oplus n}}\to\hat{M}$ 是满射。由于 R 是 $I-adic$ 完备的，$\widehat{R^n}\cong\hat{R}^n\cong R^n$。由于 $\hat{\phi}$ 是满射，$M\to\hat{M}$ 是满射，故我们有如下交换图：

$$\begin{tikzcd} R^{\oplus n} \arrow[r, "\cong"] \arrow[d, "\phi"] & \widehat{R^{\oplus n}} \arrow[d, "\hat{\phi}"] \\ M \arrow[r] & \hat{M} \end{tikzcd}$$

但由条件，这是单射，故 $M\cong\hat{M}$，即 M 是完备的。于是 ϕ 必须是满射，故 M 是有限生成 $R-$模。

(2)：我们想要证明任意 M 的子模 M' 均是有限生成 $R-$模。事实上 $G(M')$ 可以看成 $G(M)$ 的子模，这是有限生成的，且 $M'\to\hat{M}'$ 是 $M\to\hat{M}$ 的限制，这是单射。由 (1) 我们完成了证明。

□

推论 2.30

R 是 Noether 的，则 $\hat{R}_I$ 是 Noether 的且 $G_{\hat{I}}(\hat{R})$ 是 Noether 的。特别的 $R[[x]],R[[x_1,\cdots,x_n]]$ 是 Noether 的。

证明. R 是 Noether 的，由**命题 2.60**知 $G_I(R)$ 是 Noether 的，$G_I(R)\cong G_{\hat{I}}(\hat{R})$，且由上命题 $\hat{R}$ 是 Noether 的。特别的 $R[[x]]$ 对 $R[x]$ 是 $(x)-$完备的。利用归纳易得 $R[[x_1,\cdots,x_n]]$ 是 Noether 的。 □

推论 2.31

若 R 是 Noether 的，M 是有限生成 $R-$模，则 $\hat{M}_I$ 是 $\hat{I}-adic$ 完备且是 $I-adic$ 完备。

证明. 首先注意到 $\widehat{I^n}\widehat{M}=I^n\cdot\hat{R}\cdot\widehat{M}=I^n\widehat{M}$，故只需证明 $\hat{M}$ 是 $\hat{I}-adic$ 完备的。$\hat{M}$ 是有限生成 $\hat{R}-$模，于是由**命题 2.60**知 $G(\hat{M})$ 是有限生成 $G(\hat{R})-$模。现在只需验证 $\ker(\hat{M}\to\hat{\hat{M}})=0$。

由 Krull 定理

$$\ker(\hat{M}) \to \hat{\hat{M}} = \left\{ x \in \hat{M} \middle| \text{存在某个 } a \in \hat{I}, (1+a)x = 0 \right\}$$

设 $a = (\bar{a}_0, \bar{a}_1, \cdots), x = (\bar{x}_0, \bar{x}_1, \cdots)$，则 $(1+\bar{a}_n)\bar{x}_n = 0, (1+a_n)x_n \in I^n M$。$a_n x_n \in IM$，故 $x_n \in IM$，继续下去得到 $x_n \in I^n M$，即 $\bar{x}_n = 0$，故 $x = 0$。

□