抽象代数

主讲教师：邱德荣

记录人：许晓宇(1.1-1.4)，赵玲钰(1.5-2.2),李雪芳(2.3-2.7), 张钰(2.8-3.3),
马明扬(3.4-3.7),李航(3.8-4.3),吴传传(4.4-5.2)

目录

1 群 **3**
1.1 集合上的等价关系 . . . 3
1.2 群 . . . 4
1.3 群同态基本定理 . . . 7
1.4 群作用 . . . 11
1.5 *Sylow*定理（有限群“结构”定理） . . . 13
1.6 自由*Abel*群 . . . 16
1.7 有限生成*Abel*群 . . . 17

2 环与模 **18**
2.1 一些简单定义 . . . 18
2.2 子结构 . . . 19
2.3 理想、模、分式环 . . . 21
2.4 . . . 24
2.4.1 几类重要的特殊环 . . . 24
2.4.2 UFD唯一分解环或唯一析因环 . . . 25
2.4.3 分式环(环的局部化方法) . . . 26
2.5 分式环 . . . 28
2.6 反向极限与正向极限(在集合上) . . . 29
2.6.1 正向集(directed portialy ordered set) . . . 29
2.7 模 . . . 32
2.8 正合列 . . . 37
2.9 $A-$模复型 . . . 38
2.10 范畴和函子的简介 . . . 39
2.11 模的张量积 外积 对称积 . . . 43
2.12 分式模 . . . 48

3 域论 **50**
3.1 域的代数扩张 . . . 50
3.2 代数扩张与单代数扩张结构 . . . 52
3.3 代数闭包(1) . . . 56
3.4 代数闭包(2) . . . 57
3.5 分裂域 正规扩张 . . . 61
3.6 正规扩张 可分扩张 . . . 65
3.7 有限域 . . . 71
3.8 不可分扩张 . . . 73

4 Galois理论 **77**
4.1 有限Galois理论 77
4.2 Galois理论的若干应用 80
4.2.1 关于多项式根式解的Galois定理 80
4.2.2 古希腊四大数学难题 83
4.3 域的无限Galois扩张 84
4.4 例题 86

5 环与模的链条件 **88**
5.1 环与模的链条件 88
5.2 域的Galois扩张例子选讲 93

1 群

1.1 集合上的等价关系

集合的分类:如果非空集合S的一组非空子集$\{S_\lambda|\lambda\in I\}$,$I$为指标集,满足下列条件:

(1)$S=\bigcup_{\lambda\in I}S_\lambda$;

(2)$S_\lambda\cap S_\mu=\emptyset,\lambda\neq\mu,\lambda,\mu\in I$;

则$\{S_\lambda\}$叫做S的一个分类.

Definition 1.1. **关系**:非空集合S上的一个关系指的是任意一个子集$R\subset S\times S$.$(a,b)\in S\times S$,a与b有关系R,即 $(a,b)\in R$,也记为aRb.

特别地，当R为$S\times S$或$\emptyset$时,为平凡关系.

$R_1,R_2\subset S\times S$,$R_1\circ R_2\triangleq\{(a,b)\in R$:存在$c\in S$,使得$(a,c)\in R_1,(c,b)\in R_2\}$

$$a\xrightarrow{R_1}c\xrightarrow{R_2}b$$

Definition 1.2. **等价关系**:设R是非空集合S上的一个关系.如果满足如下条件:

(1)(自反性) $(a,a)\in R(\forall a\in S)$

(2)(对称性) 若$(a,b)\in R$,则 $(b,a)\in R$

(3)(传递性) 若$(a,b)\in R$且$(b,c)\in R$,则$(a,c)\in R$,

则称R为S上的等价关系.记为aRb或$(a,b)\in R$或$a\equiv_R b$.

Example 1.1. 取$S=\mathbb{Z}$

(1)$\mathbb{Z}=\mathbb{Z}_{>0}\cup\mathbb{Z}\cup\mathbb{Z}_{<0}$,$a\sim b$:要么$a,b$都为0,要么$a,b$同号.

(2)$\mathbb{Z}=2\mathbb{Z}\cup(2\mathbb{Z}+1)$,$a\sim b$:$a,b$同奇偶性.

(3)$n>1,\mathbb{Z}=n\mathbb{Z}\cup(n\mathbb{Z}+1)\cup\cdots\cup(n\mathbb{Z}+n-1)=\overline{0}\cup\overline{1}\cup\cdots\cup\overline{(n-1)}$

$$a\sim_n b\Leftrightarrow n|(a-b)\Leftrightarrow a\equiv b(mod\ n)$$

$$\mathbb{Z}/\sim_n=\{\overline{0},\overline{1},\cdots,\overline{(n-1)}\}$$

设R是S上一个等价关系,对应的分类:$S=\bigcup_{a\in S}[a]$,其中$[a]=\{b\in S:b\sim_R a\}$

Proposition 1.1. 给定非空集合S,则S上的分类与等价关系可以互相导出.

证明. (1)$S=\bigcup_{i\in\wedge}S_i$是$S$上一个分类,即$S_i\subset S$且对$\forall i,j\in\wedge$如果$S_i\cap S_j\neq\emptyset$,则$S_i=S_j$,于是定义$S$上的一个关系$R$如下:

$$(a,b)\in R\overset{\triangle}{\Longleftrightarrow}\text{存在}i\in\wedge,\text{使得}a,b\in S_i.$$

①$\forall a,(a,a)\in R$.事实上,$a\in S=\bigcup_{i\in\wedge}S_i$,则$a\in S_i$,对某个$i$,即$(a,a)\in R$.

②$(a,b)\in R\to(b,a)\in R$.

③设$(a,b)\in R,(b,c)\in R$.由$(a,b)\in R$知,存在$i\in\wedge$,使得$a,b\in S_i$.由$(b,c)\in R$知,存在$j\in\wedge$,使得$b,c\in S_j$.于是$b\in S_i\cap S_j$,即$S_i\cap S_j\neq\emptyset$.故$S_i=S_j$,$a,c\in S_i$,即$(a,c)\in R$.

因此R是S上的一个等价关系.

(2)设R是S上的一个等价关系.则$S=\bigcup_{a\in S}[a]$.其中$[a]\triangleq \overline{a}=\{b\in S:(b,a)\in R\}$

①$a\in[a]$.覆盖成立.

②对$\forall a,b\in S$.如果$[a]\cap[b]\neq\emptyset$.下证$[a]=[b]$.

由所设,有$c\in[a]\cap[b]$.即$c\sim a$且$c\sim b$,则$a\sim b$.即$a\in[b]$.且$b\in[a]$.因此$[a]=[b]$.

(3)$S=\bigcup_{i\in\wedge}S_i\Rightarrow R\Rightarrow$分类$S=\bigcup_{a\in S}[a]_R$,则对任取$a\in S$,有 $a\in S_i$,对某个i,即$S_i=[a]$. □

Definition 1.3. **偏序关系**:设R是非空集合S上的一个关系.如果满足如下条件:

(1)(自反性) $(a,a)\in R(\forall a\in S)$,

(2)(反对称性) 若$(a,b)\in R$且$(b,a)\in R$,则$a=b$,

(3)(传递性) 若$(a,b)\in R$且$(b,c)\in R$,则$(a,c)\in R$,

则称R为S上的一个偏序关系*(partial order)*,(S,R)称为一个偏序集.

Example 1.2. $(\mathbb{R},\leq),(S,\subset)$

Lemma 1.1. *Zorn*引理 设$(S,\leq)$是一个偏序集,如果S中的每个全序子集在S中都有上界,则S中存在极大元.

1.2 群

Definition 1.4. 设G是带有一个运算"$*$"的一个非空集合.如果下述条件成立:

(1)(结合律) $(a*b)*c=a*(b*c),\forall a,b,c\in G$;

(2)(单位元) 存在$e\in G$,使得$a*e=e*a=a(\forall a\in G)$;

(3)(逆元) $\forall a\in G$,存在$b\in G$,使得$a*b=b*a=e$,并记$b=a^{-1}$;

则称$(G,*)$是一个群.

如果还满足交换律:$a*b=b*a(\forall a,b\in G)$,则称$(G,*)$是一个**交换群**$(abelian)$.

Example 1.3.

(1)$(\mathbb{Z},+)$;

(2)$(\mathbb{Z},\times)$ 不是群,除$1,-1$外，其他元素无逆元;

(3)$M_n(\mathbb{R},+)$ $\mathbb{R}$上的全体n级矩阵对普通加法构成的群;

$M_{m\times n}(\mathbb{R},+)$;

(4)$GL_n(\mathbb{R},\cdot)$ $\mathbb{R}$上的全体n级可逆矩阵对矩阵乘法构成的群，称为**一般线性群**;

(5)$SL_n(\mathbb{R},\cdot)$ $\mathbb{R}$上的全体行列式为1的n级矩阵对矩阵乘法构成的群，称为**特殊线性群**;

(6)$\mathcal{U}_n=\{a\in\mathbb{C}:a^n=1\}$ x^n-1在$\mathbb{C}$中的全部根对普通乘法构成群，称为n次单位根群,$(\mathcal{U},\cdot)$;

(7)

$$X\xrightarrow{f}Y\xrightarrow{g}Z$$

$$g\circ f$$

令$S=X\neq\emptyset$,$Perm(S)=I(S)=\{f:f是S到自身的一一到上的变换\}$,则$P(S)$关于变换的合成构成一个群,称为$S$上的变换群.

$(S_n,\circ)$ n次对称群,元素个数为$n!$.

$V\xrightarrow{f}W$为线性映射.证明其为单射的方法:①$f(\alpha)=f(\beta)\Rightarrow\alpha=\beta$,②$kerf=f^{-1}(0)=\{0\}$;

(8)$(\mathbb{Z}/n\mathbb{Z},+)$ $\mathbb{Z}/n\mathbb{Z}=\{\overline{0},\overline{1},\cdots,\overline{(n-1)}\}$ $\overline{a}+\overline{b}\triangleq\overline{a+b}$

$(\mathbb{Z}/n\mathbb{Z})^*=\{\overline{a}:a\in\mathbb{Z},(a,n)=1\}$

$((\mathbb{Z}/n\mathbb{Z})^*,\cdot)$ 此群元素个数为$\varphi(n)$.

内部:子结构

外部:群同态

Definition 1.5. 子群:对于群$G\neq\emptyset$,非空子集$H\subset G$称为G的一个子群,如果H在G中的运算下也是一个群,此时记为$H\leq G$.

下列条件等价:

(1)①单位元 $e\in H$,

②封闭性 $\forall a,b\in H,a\cdot b\in H$,

③逆元 $a^{-1}\in H$.

(2)$H\neq\emptyset$.$\forall a,b\in H,ab^{-1}\in H$. (验证子群的方法)

G的平凡子群:$\{e\},G$.

子群的交与并 $H,K\leq G$.

$H\cup K\not\leq G$

反例:$H=\{[0],[3]\},K=\{[0],[2],[4]\}$,易知$H\cup K$不满足封闭性.

$H\cap K\leq G$

一般地，设$H_i\leq G(i\in\wedge)$,则$H=\bigcap_{i\in\wedge}H_i\leq G$

证明. ①$e\in H_i(i\in\wedge)\Rightarrow e\in H$.

②$\forall a,b\in H$,有$a,b\in H_i(\forall i\in\wedge)\Rightarrow a\cdot b\in H_i(\forall i\in\wedge)\Rightarrow a\cdot b\in H$.

③$\forall a\in H\Rightarrow a\in H_i(\forall i\in\wedge)\Rightarrow a^{-1}\in H_i\Rightarrow a^{-1}\in\bigcap_{i\in\wedge}H_i=H$.

$\Longrightarrow H\leq G$. □

子集生成的子群:

问题:群G，$\emptyset\neq S\subset G$,G中是否有子群包含S,若有,最小者是?

令$\mathscr{F}=\{H\leq G:H\supset S\}$.显然,$G\in\mathscr{F}$,即$\mathscr{F}\neq\emptyset$.记$\langle S\rangle=\bigcap_{H\in\mathscr{F}}$,则$\langle S\rangle$是$G$中包含$S$的最小子群.

即(1)$\langle S\rangle\leq G$(子群对取交封闭)

(2)设$H\leq G$,且$S\subset H$,则$H\supset\langle S\rangle$.

称$\langle S\rangle$为S在G中生成的子群.

定义 特别地，对群G,如果有$a\in G$,使得$G=\langle a\rangle$,则称G为一个**循环群**.

易知$\forall$群G,$a\in G$,$\langle a\rangle\leq G$.

群的阶:$|G|$.

Definition 1.6. **元素的阶**:$a \in G, |\langle a\rangle|$称为元素$a$的阶.

注: 群$(G,\cdot)$, $G=\langle a\rangle, e=a^0, a\in G, a^2, a^3, \cdots \in G$,其中$a^n = \underbrace{a*\cdots*a}_{n}(n\in\mathbb{Z}_{>0})$,则$a^{-1}, a^{-2}, \cdots \in G$,则$a^{\mathbb{Z}} \triangleq \{a^m : m\in\mathbb{Z}\}$.

事实:$\langle a\rangle = a^{\mathbb{Z}}$.

证明. (1)$\langle a\rangle \supset a^{\mathbb{Z}}$,

(2)只需说明$a^{\mathbb{Z}}$是子群.(显然) □

结论:若有群$(G,\cdot)$,$\forall a\in G$,则有$\langle a\rangle = a^{\mathbb{Z}}$.

另一方面, 有满同态$f:\mathbb{Z}\to\langle a\rangle, m\mapsto a^m$.

Example 1.4. $(\mathbb{Z},+)=\langle 1\rangle$

群$(G,\cdot)$,$H,K\subset G$,定义$H\cdot K=\{hk : h\in H, k\in K\}$,易知$H\cdot K\subset G$;另一方面,有$G=HG=\bigcup_{a\in G} H\cdot a$.其中$H\cdot a\subset G$

事实:$\{Ha : a\in G\}$给出了G上的一个分类.

证明. (1)$\bigcup_{a\in G} H\cdot a = G$;

(2)任取$a,b\in G$,如果$Ha\cap Hb\neq\emptyset$,则有$Ha=Hb$.事实上,由所设,有$c\in Ha\cap Hb$,即$c=h_1a=h_2b$.其中$h_1,h_2\in H$.下证$Ha=Hc$.

对$\forall h\in H, ha = h(h_1{}^{-1}c) = (hh_1{}^{-1})c\in Hc$即$Ha\subset Hc$.同理$hc=hh_1a=(hh_1)a\in Ha$,即$Hc\subset Ha$.因此,$Ha=Hc$.同理可证$Hb=Hc$,所以$Ha=Hb$. □

于是从上述讨论, 得到了G关于H的一个(右)陪集分类.$G=\bigcup_{a\in G}Ha=\bigcup_{a\in G}[a]$.其中$Ha$称为$a$所在的右陪集.(显然$a=ea\in H$)由前述,上述分类必对应于$G$上的一个等价关系$\sim$. 即$\forall a,b\in G, a\sim b\Leftrightarrow Ha=Hb\Leftrightarrow ab^{-1}\in H$.

记所得的商集为$G/H=\{Ha : a\in G\}=\{[a] : a\in G\}=\{\overline{a} : a\in G\}, [a]=\overline{a}\triangleq Ha$.

注意:$a,b\in G, Ha=Hb\Leftrightarrow ab^{-1}\in H$.

同样地,$G=GH=\bigcup_{a\in G} aH$是G上的一个分类.称为G关于H的左陪集分类.

注意:$a,b\in G, aH=bH\Leftrightarrow a^{-1}b\in H$.

商集$H\setminus G(\triangleq G/H)=\{aH : a\in G\}=\{\overline{a} : a\in G\}$ 且有$|G/H|=|\sum_{a_i\in G} a_iH=|\frac{|G|}{|H|}$,为此只需证$f:H\Rightarrow aH, h\mapsto ah$既单又满,易证.

称$|G/H|=\frac{|G|}{|H|}$为G关于H的$index$(指数),记之为(G:H).且有$|G|=|H|\cdot(G:H)$.$|G|=(G:\{e\})$

设$H\leq G$(群),$G/H=\{aH : a\in G\}$(左商集),问:是否可在G/H中引进某个运算,使得$(G/H,\cdot)$是一个群.

取$aH,bH\in G/H$,要使$aH*bH=abH\in G/H$成立,必须满足对$\forall a\in G$,都有$aH=Ha$.

Definition 1.7. 设$H\leq G$(群),如果对$\forall a\in G$,都有$aH=Ha$,则称H是G的一个正规子群.记之为$H\triangleleft G$.

显然$\{e\}$与G是G的两个平凡的正规子群.特别地,交换群中的任一子群均是正规的.

Proposition 1.2. 设$H \leq G$,则下列陈述等价.

(1)$H \triangleleft G$;

(2)$\forall h \in H, a \in G$,有$aha^{-1} \in H$;

*(3)*对$\forall a \in G, aHa^{-1} \subset H$;

(4)$aHa^{-1} = H, (\forall a \in G)$.

证明. (2)⇒(4)

$aHa^{-1} \subset H, h = a(a^{-1}ha)a^{-1}$,则有$a^{-1}ha = (a^{-1})h(a^{-1})^{-1} \in H$. □

事实:设$H \triangleleft G$,则按下述方式引进G/H上的运算·构成一个群,称之为G关于H的商群.

$$G/H = \{aH : a \in G\} = \{\overline{a} : a \in G\}, \overline{a} = aH(= Ha)$$

任取$a, b \in G, \overline{a}, \overline{b} \in G/H$.规定$\overline{a} \cdot \overline{b} = \overline{a \cdot b}$(即$aH \cdot bH \triangleq (a \cdot b)H$)

$aH \cdot bH = Ha \cdot bH = H(a \cdot b)H = (a \cdot b)HH \Rightarrow H^2 = H(H \leq G), H^2 = \{h_1h_2 : h_1, h_2 \in H\}$

1.3 群同态基本定理

Definition 1.8. 设G_1, G_2是两个群,$f : G_1 \to G_2$ 是一个映射.如果f满足如下条件:

(1)$f(e_1) = e_2$;

(2)$f(a \cdot b) = f(a) \cdot f(b), \forall a, b \in G_1$.

则称f为从G_1到G_2的一个*(群)*同态.

由$f(a^{-1}) \cdot f(a) = f(a^{-1} \cdot a) = f(e_1) = e_2$知$f(a^{-1}) = f(a)^{-1} \in G_2$.

Example 1.5. 群$(\mathbb{R}, +)$和$(S^1, \cdot)$,其中$S^1 = \{z \in \mathbb{C} : |z| = 1\}$, 令$f : \mathbb{R} \Rightarrow S^1, a \mapsto e^{2\pi ia}$,则$f$是一个群同态.

(1)$f(0) = e^{2\pi i0} = 1$.

(2)$f(a + b) = e^{2\pi i(a+b)} = e^{2\pi ia} \cdot e^{2\pi ib} = f(a)f(b)$.

特别地, 当f是满射,单射或一一到上的映射时,分别称f为满同态, 单同态或同构.

设$f : G \Rightarrow H$是群同态,则$f(e) = e$,记$kerf = f^{-1}(e) = \{a \in G : f(a) = e\}$,称之为$f$的核$(kernel)$.

(1)$kerf \leq G$

证明. 任取$a, b \in kerf$,则$f(a) = f(b) = e$.

于是

$$f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} = e \Rightarrow ab^{-1} \in kerf$$

.

进一步,$\forall a \in G, b \in kerf$.则$f(b) = e$.于是$f(aba^{-1}) = f(a)f(b)f(a)^{-1} = f(a)ef(a)^{-1} = e \Rightarrow aba^{-1} \in kerf$. 故$kerf \triangleleft G$,于是有商群$G/kerf$.

于是$f:G\to G/H$(单位元为$\overline{e}=H$),$a\mapsto\overline{a}(=aH)$,

$$f(ab)=abH=aH\cdot bH=f(a)\cdot f(b),f(e)=eH=H$$

$$kerf=f^{-1}(\overline{e})=\{a\in G:f(a)=\overline{e}\}=\{a\in G:aH=H\}=H$$

$$\overline{f}:G/kerf\to H,\overline{a}\mapsto f(a).$$

下证映射$\overline{f}$为良定义的，即与代表元选取无关.

$$a_1,a_2\in G,\overline{a_1}=\overline{a_2}\Rightarrow a_1kerf=a_2kerff\Rightarrow {a_1}^{-1}a_2\in kerf$$

即

$$f({a_1}^{-1}a_2)=e,f({a_1}^{-1})f(a_2)=e\Rightarrow f(a_1)=f(a_2).$$

□

$$\overline{f}:G/kerf\to H,\overline{a}\mapsto f(a),\overline{f}(\overline{a})\overset{\triangle}{=}f(a).(\forall a\in G)$$

事实:证明$\overline{f}$为群同态.

证明. $\overline{f}(\overline{e})=\overline{f(e)}=f(e)=e$

$\overline{f}(\overline{a}\overline{b})=\overline{f}(\overline{ab})=f(ab)=f(a)f(b)=\overline{f}(\overline{a})\overline{f}(\overline{b})$ □

Lemma 1.2. **引理**:群同态$f:G\to H$是单的,$\Leftrightarrow kerf=\{e\}$.

$ker\overline{f}=\{\overline{e}\}$

$\overline{a}\in ker\overline{f}\Leftrightarrow\overline{f}(\overline{a})=e$,即$f(a)=e\Rightarrow a\in kerf\Rightarrow\overline{a}=\overline{e}\Rightarrow ker\overline{f}=\{\overline{e}\}$

问题:$G=\langle a\rangle=a^{\mathbb{Z}}$,令$f:\mathbb{Z}\to a^{\mathbb{Z}},m\mapsto a^m$,

(1)$kerf=\{1\}$,

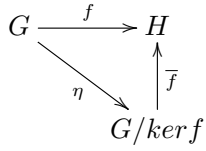
(2)$H\leq(\mathbb{Z},+),H=\{n\mathbb{Z},n\in\mathbb{N}\}$.

Theorem 1.1. **群同态基本定理**

设$f:G\to H$是一个群同态,则

(1)$kerf=f^{-1}(e)\triangleleft G,imf=f(G)\leq H$.

(2)f诱导出群同态$\overline{f}:\overline{G}=G/kerf\simeq imf\to H$,使得下图交换,



即$f=\overline{f}\circ\eta$,其中$\eta:G\to\overline{G},a\mapsto\overline{a}=akerf,\overline{f}:\overline{G}\to H,\overline{a}\mapsto f(a),ker\overline{f}=\{\overline{0}\}$.

Corollary 1.1. **推论**:设G是一个群,$H,K\triangleleft G$.如果$H\subset K$,则$K/H\triangleleft G/H$,且有群同构$(G/H)/(K/H)\simeq G/K$.

证明. 令$f: G/H \to G/K, aH \mapsto aK$,

则f是一个映射:设$aH = bH(a, b \in G)$,则$a^{-1}b \in H$.由于$H \subset K$.故$a^{-1}b \in K$.即$aK = bK$,也即$f(aH) = f(bH)$.

又显然,

$$f(aH \cdot bH) = f(abH) = abK = aK \cdot bK = f(aH) \cdot f(bH)$$

即f是一个群同态,且显然是满的.

于是有群同态基本定理,得

$$\begin{aligned} kerf &= \{aH \in G/H : f(aH) = eK\} \\ &= \{aH \in G/H : aK = eK\} \\ &= \{aH \in G/H : a \in K\} \\ &= K/H \triangleleft G/H \end{aligned}$$

且$(G/H)/(K/H) \simeq f(G/H)$,即$(G/H)/(K/H) \simeq G/K$. □

Definition 1.9. *(子群的正规化):*设$H \leq G$*(*群*)*,定义

(1)$N_G(H) = \{g \in G : gHg^{-1} = H\}$

事实:①$N_G(H) \leq G$,

②$H \triangleleft N_G(H)$.

称$N_G(H)$为H在G中的正规化子$(normilirer)$.

任取$H, K \leq G$,若$HK = KH$,即$hK = Kh$,所以$h \in N_G(K)$即$H \subset N_G(K)$.

(2a)G的中心.$C(G) = \{a \in G : ab = ba(\forall b \in G)\}$,易证$C(G) \triangleleft G$.

*(2b)*中心化子:设$S \subset G$,定义S在G中的中心化子为$C_G(S) = \{a \in G : ab = ba(\forall b \in S\}$.

*(3)*非交换群的交换化*(*即$Abel$化*)*:设G是一个群*(*非交换*)*,由交换群性质$ab = ba$,即$(ab)(ba)^{-1} = e = aba^{-1}b^{-1}$得到换位子定义:

G的换位子群:对于$a, b \in G$.记$[a, b] = aba^{-1}b^{-1}$,称为一个换位子.且记$S = \{[a, b] : a, b \in G\}$.令$[G : G] = \langle S \rangle$为$S$生成的子群,称$[G, G]$为$G$的换位子群.

事实:$[G : G] \triangleleft G$.

称商群$G/[G : G]$为G的交换化,记之为$G^{ab} \triangleq G/[G : G]$.

事实:(1)G^{ab}是一个交换群.

(2)满足如下所谓"泛性质":对任意交换群H及群同态$g : G \to H$,则存在唯一的群同态$\rho : G^{ab} \Rightarrow H$,使得$g = \rho \circ f$(试比较$kerf$与$kerg$的关系)

Corollary 1.2. 设$H, K \leq G$,且$H \subset N_G(K)$,则

(1)$HK \leq G$,且$K \triangleleft HK$

*(2)*有群同构$HK/K \simeq H/H \cap K$.

证明. 令$f:H\to HK/K,h\mapsto hK(\forall h\in H)$,易知$f$是一个群满同态.又

$$\begin{aligned}kerf&=\{h\in H:f(h)=eK\}\\&=\{h\in H:hK=K\}\\&=\{h\in H:h\in K\}\\&=H\cap K\end{aligned}$$

由群同态基本定理,知$H\cap K=kerf\triangleleft H$,且$H/H\cap K\simeq f(H)=HK/K$即$H/H\cap K\simeq HK/K$. □

(循环群的结构)

设$G=\langle a\rangle$是一个循环群,则$G=a^{\mathbb{Z}}=\{a^m:m\in\mathbb{Z}\}$令$f:(\mathbb{Z},+)\to G=a^{\mathbb{Z}},m\mapsto a^m$,显然$f$是一个群满同态,于是由群同态基本定理,得$\mathbb{Z}/kerf\simeq G$

事实:$(\mathbb{Z},+)=\langle 1\rangle=\langle -1\rangle$是一个无限循环群.

$H\leq\mathbb{Z},H=n\mathbb{Z}=\langle n\rangle(n\in\mathbb{Z})$

$(1)H=\{0\}$

$(2)H\neq\{0\}$,此时$H\cap\mathbb{Z}_{\geq 1}\neq\emptyset$.取$H$中的最小正整数$n$,则断言$H=n\mathbb{Z}=\langle n\rangle(=\langle -n\rangle)$.

对$\forall m\in H$,有带余数除法知,$m=qn+r$,其中$q,r\in\mathbb{Z}$且$0\leq r<n.r=m-qn\in H$.由n的最小性知$r=0$,即$m=qn\in n\mathbb{Z}\Rightarrow H\subset n\mathbb{Z}\subset H\Rightarrow H=n\mathbb{Z}$,因此$kerf=n\mathbb{Z}$.

$$G=\langle n\rangle\simeq\mathbb{Z}/kerf=\mathbb{Z}/n\mathbb{Z}$$

(1)无限循环群:$G\simeq\mathbb{Z}$,

(2)有限循环群:$G\simeq\mathbb{Z}/n\mathbb{Z}=\{\overline{0},\overline{1},\cdots,\overline{(n-1)}\}(n\neq 0)$.

事实:$G=\langle a\rangle$是一个循环群.$|G|=n$

元素阶的性质:$a\in G$,a的阶$o(a)$为n.

$$o(a)=n\Leftrightarrow n=|\langle a\rangle|\Leftrightarrow n\text{是使得}a^n=e\text{的最小正整数.}$$

$$\Leftrightarrow\begin{cases}(1)a^n=e\\(2)a^m=e\Leftrightarrow n|m\end{cases}$$

对$\forall b\in G,b=a^r$,则$o(b)=o(a^r)=\frac{n}{(r,n)}$,此外,当$H\leq G,\#H=m$且$m|n$,则$H=\langle a^{\frac{n}{m}}\rangle$.

Example 1.6. *(1)*群$(\mathbb{R},+)$和$(S^1,\cdot)$,其中$S^1=\{z\in\mathbb{C}:|z|=1\}$,令$f:\mathbb{R}\Rightarrow S^1,a\mapsto e^{2\pi ia}$,则$f$是一个群满同态.$kerf=(\mathbb{Z},+)$,且有$(\mathbb{R}/\mathbb{Z},+)\simeq(S^1,\cdot)$,以及$\mathbb{R}^n/\mathbb{Z}^n\simeq S^n=S^1\times S^1\times\cdots S^1$.

(2)$G=GL_n(\mathbb{R})$,则$det:G\to\mathbb{R}^*=\mathbb{R}\setminus\{0\},S\mapsto detA=|A|$,则$kerdet=\{A\in GL_n\mathbb{R}:detA=1\}=SL_n(\mathbb{R}),SL_n(\mathbb{R})\triangleleft GL_n(\mathbb{R})$,且$GL_n(\mathbb{R})/SL_n(\mathbb{R})\simeq GL_1(\mathbb{R})=\mathbb{R}^*$

(3)$f:(\mathbb{Z},+)\to(2\mathbb{Z},+),a\mapsto 2a$.则$f(3\mathbb{Z})=6\mathbb{Z}$,且有$\mathbb{Z}/3\mathbb{Z}\simeq f(\mathbb{Z})/f(3\mathbb{Z})=2\mathbb{Z}/6\mathbb{Z}\simeq\mathbb{Z}/3\mathbb{Z}$,但$\mathbb{Z}/2\mathbb{Z}\ncong\mathbb{Z}/4\mathbb{Z}$

所以,对于一般的群同态$f:G_1\to G_2$,当H_1是G_1的正规子群,则有$G_1/H_1\simeq f(G_1)/f(H_1)$.

1.4 群作用

$|G|=n$,由算术基本定理$n=p_1{}^{e_1}\cdots p_r{}^{e_r}$,$p_i$为素数.

重要工具:群作用$(actions\ of\ groups)$

Definition 1.10. 设G是一个群,S是一个非空集合,G对S的一个作用,指的是满足下述条件的映射$*:G\times S\to S$:

(条件):(1)$e\cdot s=s(e\in G$是单位元$,s\in S)$

(2)$(a*b)*c=a*(b*c)(\forall a,b\in G,s\in S)$

Example 1.7. $\forall a\in G,f_a:S\to S,s\mapsto as$,且易证$f_a$为置换(即$f_a\in Perm(S)$),$f:G\to Perm(S),a\mapsto f_a$为群同态.此时$G\times S\to S,(a,s)\mapsto as=f(a)(s)=f_a(s)$.

设$G\times S\to S$是个群作用,则该作用给出了S上的如下一个等价关系:$\sim_G$:

对于$s_1,s_2\in S$,定义:$s_1\sim_G s_2\overset{\triangle}{\Longleftrightarrow}$存在$a\in G$,使得$s_2=as_1$.

事实:$\sim_G$是S上的一个等价关系.于是有对应的分类,

商集:

$$S/G=\{[s]:s\in G\}=\{\overline{s}:s\in G\}$$

$$t\in[s]\Leftrightarrow t=as(\exists a\in G),$$

即

$$[s]=G\cdot s=\{as:a\in G\}$$

称$[s]$为s所在的$G-$轨道.

$$S=\bigcup_{s\in S}G\cdot s$$

特别地,如果$\sharp S<+\infty$,则可选取$s_1,s_2,\cdots,s_r\in S$使得$S=[s_1]\cup\cdots\cup[s_r]=G\cdot s_1\cup\cdots\cup G\cdot s_r$.

于是得计数公式:

$$|S|=\sum_{i=1}^{r}|G\cdot s_i|$$

每个轨道元素个数:

令$G_s=\{a\in G:as=s\}$

事实:$G_s\leq G$.

称G_s为S在G中的稳定子群$(stablizer)$.

$$\phi:G/G_s\to G\cdot s,\overline{a}\mapsto as(\forall a\in G)$$

(1)ϕ是$well-defined$:

设$\overline{a_1}=\overline{a_2}(a_1,a_2\in G)$,则${a_1}^{-1}a_2\in G_s$,即${a_1}^{-1}a_2s=s\Rightarrow a_1({a_1}^{-1}a_2)s=a_1s$,即$a_2s=a_1s(\phi(\overline{a_1})=\phi(\overline{a_2}))$

(2)显然ϕ是满射,下证ϕ是单射:

设$a_1,a_2\in G$且$\phi(\overline{a_1})=\phi(\overline{a_2})$,则

$$a_1s=a_2s\Rightarrow {a_2}^{-1}a_1s=s\Rightarrow {a_2}^{-1}a_1\in G_s\Rightarrow\overline{a_2}=\overline{a_1}$$

.

结论:$\phi: G/G_s \to G\cdot s, \phi$是双射,于是$|G\cdot s| = |G/G_s| = (G:G_s)$.

计数公式(稍精细些):群G作用在有限集S上,有$G-$轨道分类:$S = G\cdot s_1 \cup \cdots \cup G\cdot s_r$.

(计数公式):$|S| = \sum_{i=1}^r |G\cdot s_i| = \sum_{i=1}^r (G:G(s_i)$

Example 1.8. *(1)*G为群,取$S=G, G\times S\to S, (a,s)\mapsto as$,

*(2)*当$H\le G$.则$S = G/H = \{aH : a\in G\}$且$G\times S\to S, (a,bH)\mapsto abH$.

Definition 1.11. **共轭关系**:设G是一个群,$a,b\in G$.如果存在$c\in G$,使得$cac^{-1}=b$,则称a与b共轭.

事实:共轭关系是一个等价关系.

$G/\sim = \{[a]: a\in G\}$,其中$[a] = \{bab^{-1} : b\in G\}$是$G$中$a$所在的共轭类.则$G = \bigcup_{a\in G}[a]$.而$[a] = \{a\} \Leftrightarrow a\in C(G)$,所以有$|G| = |C(G)| + \sum_{i=1}^r \sharp[a_i], a_i\notin C(G)$

用群作用的观点:取$S=G, G\times S\Rightarrow S, (a,s)\mapsto asa^{-1}$,易证$e\cdot s = s, (a*b)*s = a*(b*s)$,

任取$s\in S = G$,则有

$$G\cdot s = \{asa^{-1} : a\in G\} = [s]$$

则由$G = C(G) + \bigcup_{a\in G}^r [s_i]$得

$$\begin{aligned} |S| &= \sharp C(G) + \sum_{i=1}^r |[s_i]| \\ &= \sharp C(G) + \sum_{i=1}^r |G\cdot s_i| \\ &= \sharp C(G) + \sum_{i=1}^r (G:G_{s_i}) \end{aligned}$$

$$G_{s_i} = \{a\in G : as_ia^{-1} = C_G(s_i)\} \Rightarrow |S| = |C(G)| + \sum_{i=1}^r (G:C_G(s_i))$$

当$H\le K$,有$S = \{gHg^{-1} : g\in G\}$,即$G\times S\Rightarrow S, (a,bHb^{-1})\mapsto a*(bHb^{-1}) \triangleq a(bHb^{-1})a^{-1}$

则$G_H = \{g\in G : gHg^{-1} = H\} = N_G(H)$.

复习:(群作用)

群G作用于$S(\neq\emptyset)$上,即

$$G\times S\Rightarrow S$$

$$S/G = S/\sim_G = \{[s] : s\in S\}$$

$$s_1, s_2\in S, s_1\sim_G s_2 \Leftrightarrow \text{存在} a\in G, \text{使得} as_1 = s_2$$

$[s] = G\cdot s = \{as : a\in G\}$: s所在的G轨道，且有$S = \bigcup_{s\in S} G\cdot s$,

当$\sharp S < +\infty$时,选择$s_1, s_2, \cdots, s_r\in S$使得$S = [s_1]\cup\cdots\cup[s_r] = G\cdot s_1\cup\cdots\cup G\cdot s_r$.

轨道计数公式:$|S| = \sum i = 1^r |G\cdot s_i| = \sum i = 1^r (G:G(s_i)$

特别地,对于

$$s\in G, [s] = G\cdot s = \{s\} \Leftrightarrow a\cdot s = s(\forall a\in G) \Leftrightarrow G_s = G$$

此时称s为G的一个不动点.

1.5 $Sylow$定理（有限群“结构”定理）

Definition 1.12. 设p是素数,G是一个有限群,如果$|G|$是p的幂,则称G为一个p群.

Definition 1.13. 设G是一个n阶群,p是一个给定的素数,且$p|n$.于是有唯一的$r \in Z_{\geq 0}$使得$p^r||n$,称G的任意一个阶为p^r的子群为G的$Sylow$-子群.

Theorem 1.2. ***(有限子群$Sylow$定理)***

设G是一个n阶群,p是一个素数,且$p|n$,记$n = p^r m, r \in Z_{\geq 1}$,且$p \nmid m$.则

(1)G的任一个p子群必包含于G的某个$Sylow-p$子群中.

(2)G的$Sylow-p$子群互相共轭.

*(3)*记S为G的全部$Sylow-p$子群组成的集合,则$|S| \equiv 1(mod \quad p)$.

(4)$|S| \mid m$.

设H是一个p群,p是素数,H作用在集合$S(\neq \emptyset)$上.

s是一个$H-$固定点 $\Longleftrightarrow hs = s(\forall h \in H) \Longleftrightarrow H_s = H$.

$1=|[s]|=|H : H_s|$

s不是$H-$固定点 $\Longleftrightarrow (H : H_s) > 1 \Longleftrightarrow p|(H : H_s)$

记S_f={ $s \in S$:s是H固定点}

则 $S=S_f \bigcup H_{s1} \bigcup \cdots \bigcup H_{sr}$

$|S|=|S_f|+ \prod_{i=1}^{r} |H_{si}|=|S_f|+ \prod_{i=1}^{r}(H : H_{si}) \quad \Rightarrow |S| \equiv |S_f|(mod \quad p)$ (因为$p|(H : H_{si}), i = 1,\cdots,r$)

综上,得

Proposition 1.3. 设p是一个素数,H是一个p群,S是一个$H-$集.记S_f={ $s \in S$:s是H固定点}. 则$|S_f| \equiv |S|(mod \quad p)$.

证明. （有限子群$Sylow$定理）

(1)设H是G的一个p子群，P是G的一个$Sylow-p$子群.令S=$\{aPa^{-1} : a \in G\}$.于是S是一个自然的$G-$集（在共轭作用下），且是可迁的.

$$G \times S \to S$$
$$(a, bPb^{-1}) \to a(bPb^{-1})b^{-1}$$

于是$|S| = |[P]| = (G : G_p)$,其中$G_P = \{a \in G : aPa^{-1} = P\} = N_G(P)$ (即P是G中的正规化子).

$\Rightarrow |S| = (G : G_P) = (G : N_G(P))$

又$P \subset N_G(P) \subset G$

$\Rightarrow (G : N_G(P))|(G : P) = m$

$\Rightarrow p \nmid (G : N_G(P))$,即$p \nmid |S|$

又显然S也是一个$H-$集合,记$S_f(H) = \{s \in S : h*s = s(\forall h \in H)\}$,则由前述命题,得$|S_f(H)| \equiv |S|(mod \quad p)$.

由上述结论,$p \nmid |S|$,$\Rightarrow p \nmid |S_f(H)|$.

特别地,$S_f(H) \neq \emptyset$,也即

S中必有$H-$固定点,不妨设其中一个为P'.于是,对$\forall h \in H$,有$hP'h^{-1} = P'$,即$h \in N_G(P')$.因此$H \subset N_G(P')$.

由群同态基本定理,得$H/H \bigcap P' \simeq HP'/P'$,$\Rightarrow (H : H \bigcap P') = (HP' : P')$.

由于$P' \subset HP' \subset G$且$(HP' : P')|(G : P') = m$

$\Rightarrow (H : H \bigcap P')|m$

$\Rightarrow (H : H \bigcap P')||H| = p^t \quad (1 \leq t \leq r)$

$\Rightarrow (H : H \bigcap P')|(m, p^t) = 1$

$\Rightarrow (H : H \bigcap P') = 1$

$\Rightarrow H \bigcap P' = H$

$\Rightarrow H \subset P'$

(2)任取G的一个$Sylow - p$子群H.下证$H \in S$.

与上述（1）的证明中的讨论一样,即S作为一个$H-$集,必有固定点,取其中一个为Q,于是有$H \subset N_G(Q)$,$\Rightarrow H \subset Q$.

但$|H| = |Q| = p^r$.故$H = Q \in S$.

(3)同理,S也是一个$p-$集,且S有且仅有一个$P-$固定点,即P自身:

$$Q \in S_f \iff aQa^{-1} = Q(\forall a \in P),\text{即}a \in N_G(Q) \Rightarrow P \subset N_G(Q) \Rightarrow P \subset Q \Rightarrow Q = P$$

因此,由前面关于p群作用的固定点结果,$|S| \equiv \#S_f(mod \quad p)$,即$|S| \equiv 1(mod \quad p)$.

(4)S作为一个$G-$集,有$|S| = |\{aPa^{-1} : a \in G\}| = (G : N_G(P))|(G : P) = m$

□

循环群:(1)$G \simeq (Z, +)$可作其生成元的元素为1,-1,$< 1 >=< -1 >$.(2)$G =< a >$,$\circ(a) = n$,$G \simeq (Z/nZ, +)$.$< a >=< a^r > \iff (r, n) = 1$,则$r$有$\phi(n)$个.

Example 1.9. *(1)*$Z/6Z =< \overline{1} >=< \overline{5} >$

(2)$(Z/nZ)^* = \{\overline{a} : (a, n) = 1\}$

置换群:

$S = \{a_1, \cdots, a_n\} \longrightarrow \{1, 2, \cdots, n\}$

$P(S) = Perm(S)$,$\sigma \in P(s)$

$$\begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$$

$\sigma \circ \tau$：先用τ作用,再用σ作用.$(i_1 \dots i_r)$是r循环.

可解群:

$G \supset G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_n = \{e\}$,且$G_{i+1} \lhd G_i \ (i = 0, \dots, n-1)$,$G_i/G_{i+1}$是交换的.

幂零群一定是可解群.

有限生成*Abel*群结构

(1)有限*Abel*群

设A是一个n阶$Abel$群,$(A,+)$,p是素数,$p|n$.A的$Sylow-p$子群有且只有一个,记之为$A(p)$.

$A(p)=\{a\in A:\exists r\in Z_{\geq 0},\to p^r a=0\}$,称之为$A$的$p-primary$($p$准素)子群.

$n={p_1}^{e_1}\dots{p_s}^{e_s}.p_1,\dots,p_s$是两两互异的素数,$e_1,\dots,e_s\in Z_{\geq 0}$.

对应地,有A的p_i-准素子群$A(p_i)$.

注记:一般地,对于$Abel$群A及$n\in Z_{\geq 1}$,记$A[n]=\{a\in A:na=0\}$,$A[n]\leq A$,

于是$A(p)=\bigcup\limits_{m\in Z_{\geq 0}}A[p^m]=\bigcup\limits_{m=0}^{\infty}A[p^m]$.　$A[1]=\{0\}$.

(2)$Abel$群的直和

$A=A_1\oplus A_2$:(1)$A=A_1+A_2$　(2)表示法唯一:$a=a_1+a_2=a_1'+a_2'\Rightarrow a_1=a_1',a_2=a_2'$.$A_1\bigcap A_2=\{0\}$.

Theorem 1.3. 设A是一个n阶$Abel$群,且$n={p_1}^{e_1}\dots{p_r}^{e_r},p_1,\dots,p_r$是两两互异的素数,$e_1,\dots,e_r\in Z_{\geq 1}$.则$A=A(p_1)\oplus\dots\oplus A(p_r)=\bigoplus\limits_{i=1}^{r}A(p_i)$.

证明. 先证$A(p_1)\bigcap\sum\limits_{i=2}^{r}A(p_i))=\{0\}$

任取其中一个元素α,则$\alpha\in A(p_1)$且$\alpha=\sum\limits_{i=2}^{r}a_i,a_i\in A(p_i)$.

记$\circ(a_i)=p_i^{t_i}\quad(i=2,\dots,r).\circ(\alpha)=p_1^{t_1}$.

令$t=max\{t_i:i=2,\dots,r\}$,则$(p_2,\dots,p_r)^t\alpha=(p_2,\dots,p_r)^t(\sum\limits_{i=2}^{r}a_i)=0$.

$p_1^{t_1}\alpha=0\Rightarrow\circ(\alpha)|(p_1^{t_1},(p_2,\dots,p_r)^t)=1\Rightarrow\circ(\alpha)=1\Rightarrow\alpha=0$.

不妨设$n=p^{e_1}q^{e_2}$,下证$A=A(p)+A(q)$.

$(p^{e_1},q^{e_2})=1\iff\exists u,v\in Z\to up^{e_1}+vq^{e_2}=1$.

则对A中任意元素a有$a=1\cdot a=(up^{e_1}+vq^{e_2})\cdot a=up^{e_1}a+vq^{e_2}a\in A(p)+A(q)$.

□

设$(A,+)$是$Abel$群,$a\in A,n\in Z_{>0}$,则$na=a+\dots+a$(n个a).

若$n\in Z_{\geq 1}$,记$A[n]=\{a\in A:na=0\}$,p是素数,$A[p^n]=\{a\in A:p^na=0\}$,$A(p)=\bigcup\limits_{n\in Z_{>0}}A[p^n]$ 是A的$p-$准素子群$(p-primary)$,$A[1]=\{0\}$.

事实:A交换$\Rightarrow A=\bigoplus\limits_{p}A(p)$,其中$p$取遍所有素数.

特别地,当$|A|<+\infty$,即A是一个有限$Abel$群,记$|A|=n={p_1}^{e_1}\dots{p_r}^{e_r}.p_1,\dots,p_r$是两两互异的素数,$e_1,\dots,e_r\in Z_{\geq 1}$.

此时,$A=A(p_1)\oplus\dots\oplus A(p_r)$

事实:p是素数,有限p群必是循环p子群的直和,即

$A=A(p)\simeq Z/p^{r_1}Z\oplus\dots\oplus Z/p^{r_s}Z$.（不妨设$r_1\leq\dots\leq r_s$),其中$s$在同构意义下不变,称之为$A$的$p-$秩$(rank)$.　$p-rank(A)=s$.

若$A=Z/p^rZ$　$p-rank(A)=1$.

$A[p]=\{a\in A:pa=0\}=\{\overline{m}:p\overline{m}=\overline{0}\}=\{\overline{a}:a\in p^{r-1}Z\}=p^{r-1}Z/p^rZ$.

即$A[p] = p^{r-1}Z/p^rZ \simeq Z/pZ = F_p$,即$dim_{F_p}A[p] = 1 = dim_{F_p}A/pA, p - rank(A) = dim_{F_p}A[p]$.

由$A = Z/p^rZ$,有$pA = pZ/p^rZ \leq A$,商群$A/pA = (Z/p^rZ)/(pZ/p^rZ) \simeq Z/pZ = F_p$.

事实:设p是素数,A是一个有限*Abel*群,则

$$p - rankA = p - rankA(p) = dim_{F_p}A[p] = dim_{F_p}A/pA.$$

1.6 自由*Abel*群

Definition 1.14. 设A是一个*Abel*群,$\emptyset \neq S \subset A$,如果下述条件成立:

*(1)*对$\forall \alpha \in A$,都有$\alpha = \sum\limits_{s\in S} a_s \cdot S$,其中$a_s \in Z$,且对几乎所有*(*即除有限个外*)*的$s \in S, a_s = 0$.

*(2)*上述*(1)*中的表示法唯一.

则称S为A的一组基,此时也称A为一个自由*Abel*群.

Example 1.10. *1.*$A = (Z, +), S = \{1\}$

*2.*设$x_1, \ldots, x_n$是一组未定元,令$A = Z_{x_1} \oplus \cdots \oplus Z_{x_n}$

Lemma 1.3. 7.2$(P40)$ 设$f : A \to A'$是一个群满同态,其中A, A'都是*Abel*群,且A'是自由的,则存在A的一个子群C,使得$f|_C : C \simeq A'$,且$A = C \oplus kerf$.

证明. 取A'的一组基$S' = \{x'_i\}_{i\in I}$,且对每个$i \in I$,取定一个$x_i \in A$,使得$f(x_i) = x'_i$(因f是满射),并记$S = \{x_i : i \in I\}$.

(1)下证S中的元素是$Z-$线性无关的.为此,令$\sum\limits_{i\in I} a_ix_i = 0$,其中$a_i \in Z, i \in I$,且对几乎所有的$i \in I, a_i = 0$. $\Rightarrow 0 = f(\sum\limits_{i\in I} a_ix_i) = \sum\limits_{i\in I} a_if(x_i) = \sum\limits_{i\in I} a_ix'_i \Rightarrow a_i = 0, (\forall i \in I)$. 于是,令$C =< S >$为$A$中由$S$生成的子群,则$C$是以$S$为一组基的自由*Abel*群.

(2)下证$C \bigcap kerf = \{0\}$.任取$\alpha \in C \bigcap kerf$,有$\alpha = \sum\limits_{i\in I} a_ix_i (a_i \in Z$,且除有限个外均取0),且$0 = f(\alpha) = f(\sum\limits_{i\in I} a_ix_i) = \sum\limits_{i\in I} a_if(x_i) = \sum\limits_{i\in I} a_ix'_i \Rightarrow a_i = 0, (\forall i \in I)$,即$\alpha = 0$.

(3)下证$A = C \oplus kerf$.任取$\alpha \in A, f(\alpha) \in A', f(\alpha) = \sum\limits_{i\in I} a_ix'_i$(有限和), 即$f(\alpha) = \sum\limits_{i\in I} a_if(x_i) = f(\sum\limits_{i\in I} a_ix_i) \Rightarrow f(\alpha - \sum\limits_{i\in I} a_ix_i) = 0 \Rightarrow \alpha - \sum\limits_{i\in I} a_ix_i \in kerf \Rightarrow \alpha \in C + kerf$.

□

Theorem 1.4. 7.3$(P41)$ 自由*Abel*群A的非平凡子群是自由的,且其基的基数$\leq$ A的基的基数.由此即知,A中任两组基的基数均相等,称该基数为A的秩$(rank)$.

证明. (为简单证,只考虑基的基数$< +\infty$的情形),即只考虑有限生成的自由*Abel*群.

(对基的基数用归纳法)

$r = 1$时显然,$Z \simeq nZ(n \neq 0)$.

现设$A = Z_{\alpha_1} \oplus \cdots \oplus Z_{\alpha_n}$(即$\{\alpha_1, \ldots, \alpha_n\}$是$A$的一组自由基). 令

$$f : A \to Z_{\alpha_1}(\text{即投影到第一个分量})$$
$$\sum_{i\in I} a_i\alpha_i \to a_1\alpha_1$$

显然,f是一个群满同态.由群同态基本定理,$A/kerf \simeq Z_{\alpha_1} \Rightarrow kerf = Z_{\alpha_1} \oplus \cdots \oplus Z_{\alpha_n}$.

设$B \leq A$.将f限制在B上,得 $f|_B : B \to Z_{\alpha_1}$.

注意到$Z_{\alpha_1} \simeq Z$,故$im(f|_B)$作为Z_{α_1}的子群有以下两种情形:

(1)$im(f|_B) = 0$.由群同态基本定理得 $B/ker(f_B) \simeq im(f|_B) = 0 \Rightarrow B = ker(f|_B) \subset kerf$

由归纳假设,B是自由的,且B的基的基数$\leq n-1 < n$.

(2)$im(f|_B) \neq 0$,此时$im(f|_B) \simeq Z$,即$f|_B$是满的. 于是由前述引理7.2知B中有一个子群C,使得$C \simeq Z_{\alpha_1}$,且$B = ker(f|_B) \oplus C$.

由归纳假设,$ker(f|_B) \subset kerf = Z_{\alpha_2} \oplus \cdots \oplus Z_{\alpha_n}$知 B是自由的(因为$ker(f|_B)$是自由的,C也是自由的),且 B的基的基数=$ker(f|_B)$的基的基数+C的基的基数$\leq n-1+1 = n$.

□

1.7 有限生成*Abel*群

Definition 1.15. 设A是一个*Abel*群,令$A_{tors} = \{a \in A : \exists m \in Z_{\geq 1} \to ma = 0\}$.

事实:$A_{tors} \leq A$,称A_{tors}为A的挠子群($torsion \quad subgroup$).特别地,当$A_{tors} = \{0\}$时,我们称A为一个$torsion - free$群.

事实:A/A_{tors}是一个$torsion - free$群.

证明. 任取$\alpha = \overline{a} \in A/A_{tors}$,其中$a \in A$.假设有$m \in Z_{\geq 1}$,使得$m\alpha = \overline{0}$ 即$m\overline{a} = \overline{0}, \overline{ma} = \overline{0} \iff ma \in A_{tors} \Rightarrow \exists n \in Z_{\geq 1}, s.t., nma = 0 \Rightarrow a \in A_{tors} \Rightarrow \alpha = \overline{a} = 0$.

□

Theorem 1.5. 8.4($P45$)*:对于有限生成Abel群A.*$torsion - free \iff free$.

证明. 不妨设$A \neq 0$.

设S是A的一个生成元集,($S \neq \emptyset$)即$A = \underset{s \in S}{\oplus} Z_s, |S| < +\infty$.

则可取A在S中的如下一个极大$Z-$线性无关组$x_1, \ldots, x_n$,即

(1)$a_1x_1 + \cdots + a_nx_n = 0 (a_i \in Z, i = 1, \ldots, n) \Rightarrow a_i = 0 (i = 1, \ldots, n)$

(2)对$\forall x \in A$,有不全为0的整数$a_0, a_1, \ldots, a_n \in Z, s.t., a_0x + a_1x_1 + \cdots + a_nx_n = 0$

令$B = Z_{x_1} \oplus \cdots \oplus Z_{x_n}$,则$B$是$A$的一个秩$n$的自由*Abel*子群. 特别地,$\forall s \in S$,都有不全为0的整数$a_0, a_1, \ldots, a_n \in Z, s.t., a_0s + a_1x_1 + \cdots + a_nx_n = 0$.

此时,$a_0 \neq 0 \Rightarrow a_0s = -a_1x_1 - \cdots - a_nx_n \in B$.由于$|S| < +\infty$,故有$m \in Z_{\geq 1}, s.t., ms \in B (\forall s \in S)$.

对$\forall \alpha \in A$,有$\alpha = \sum\limits_{s \in S} a_s \cdot s, a_s \in Z$,于是$m\alpha = \sum\limits_{s \in S} a_s \cdot (ms) \in B$, 即$mA \leq B$.

由前述结论,可知mA是自由*Abel*群.又显然

$$A \simeq mA$$
$$a \to ma$$

(因为$ma = 0 \iff a = 0$, A是$torsion - free$.)

□

Theorem 1.6. 8.5(*P*46)*:*设A是一个有限生成*Abel*群,则$A \simeq A_{tors} \oplus A_f$,其中$A_{tors}$是$A$的$torsion$子群,是一个有限群; A_f是一个自由*Abel*群,且$A_f \simeq Z^r = Z \oplus \cdots \oplus Z(r$个$), r = rank(A_f), A \simeq A_{tors} \oplus Z^r$.

证明. $A = \sum\limits_{s\in S} Z_s$.$S$是$A$的一个生成元集,$|S| < +\infty$.

令$F = \bigoplus\limits_{s\in S} Z_s$,则$F$是一个以$S$为一组基的自由*Abel*群,且有一个自然的群满同态

$$f : F = \bigoplus_{s\in S} Z_s \to \sum_{s\in S} Z_s$$
$$\bigoplus_{s\in S} a_s \cdot s \to \sum_{s\in S} a_s \cdot s$$

$f^{-1}(A_{tors})$作为F的子群,是一个有限生成的自由*Abel*群 $\Rightarrow A_{tors} = f(f^{-1}(A_{tors}))$是$A$的有限生成子群 $\Rightarrow A_{tors}$是有限群.

前面已证A/A_{tors}是一个有限生成$torsion-free$ *Abel*群, 故A/A_{tors}是一个有限生成自由*Abel*群,即$A/A_{tors} \simeq Z^r.r \in Z_{\geq 1}$.

再用引理7.2及群满同态,$g : A \to A/A_{tors} \simeq Z^r. \Rightarrow A = A_{tors} \oplus C, C \simeq Z^r$.

□

2 环与模

2.1 一些简单定义

Example 2.1. $(Z, +, \times)$*(*两个运算*)*

(1)$(Z, +)$是一个交换群

(2)$(Z, \times)$是一个半群,$\times$满足结合律

*(3)*分配律*:*$(a + b) \cdot c = a \cdot c + b \cdot c$

Definition 2.1. 环$(Ring)$*:*$(R, +, \times)$ $R \neq \emptyset$

(1)$(R, +)$是一个*Abel*群

(2)R对乘法"$\times$"封闭且满足结合律

*(3)*分配律*:*$(a + b) \cdot c = a \cdot c + b \cdot c$

特殊元素:$1 \in R, 1 \cdot a = a \cdot 1 = a(\forall a \in R)$

Definition 2.2. 模*:*设R是一个环*(*含1*)*,$(M, +)$是一个交换群,且有R对M的如下作用*:*

$$R \times M \to M$$
$$(a, \alpha) \to a \cdot \alpha$$

满足如下条件*(*公理*):*

(1)$(a_1a_2)\alpha = a_1(a_2\alpha)$ $(\forall a_1, a_2 \in R, \alpha \in M)$

(2)$1 \cdot \alpha = \alpha(\forall \alpha \in M)$;$0 \cdot \alpha = 0(\forall \alpha \in M)$; $a \cdot 0 = 0(\forall a \in A)$

(3)$(a_1 + a_2)\alpha = a_1\alpha + a_2\alpha; a(\alpha_1 + \alpha_2) = a\alpha_1 + a\alpha_2(a_1, a_2, a \in R, \alpha, \alpha_1, \alpha_2 \in M)$

则称M为一个R模$(R - module)$.

Definition 2.3. 一些特殊环:

1.(1)$(R,+,\cdot)$是一个交换环;(2)$(R\setminus\{0\},\cdot)$是一个乘法群,则称R是一个域

2.(1)$(R,+,\cdot)$是一个非交换环;(2)$(R\setminus\{0\},\cdot)$是一个群,则称R是一个除环$(skew\quad ring)(division\quad ring)$

Example 2.2. 1.域:$Q,R,C.Q(x)=\{\frac{f}{g}:f,g\in Q[x],且g\neq 0\}$(有理分式域).$(Q,+,\cdot),(Q\setminus\{0\},\cdot)$

2.域F上的多项式环$F[x]$.

3.$Gauss$整数环$Z[i]=\{a+bi:a,b\in Z\}$

4.$Z[\sqrt{-3}]=\{a+b\sqrt{-3}:a,b\in Z\}$

5.$(Mn(R),+,\cdot)(n>1)$

$Mn(R)=Hom_R(R^n,R^n)=End_R(R^n)$

$GLn(R)=Mn(R)^*$

Definition 2.4. (1)对于环$(R,+,\cdot)$(含1).记$R^\times(=R^*)=\{a\in R:\exists b\in R,s.t.,ab=ba=1\}$

事实:$(R^\times,\cdot)$是一个群,称为环R的(乘法)单位群.

(2)零因子:环R,$a\in R$.称为一个零因子，如果有$b\in R\setminus\{0\},s.t.,ab=0$.

Definition 2.5. 一个不含非零幂零元的交换环称为一个既约环$(reduced\quad ring)$.

2.2 子结构

Definition 2.6. **子环**:R是一个含1的环,$R_0\leq R$是R的子环,$1\in R_0$.$(R_0,+,\cdot)$是一个含1的环.

Definition 2.7. **理想**: 设$(R,+,\cdot)$是一个含1的环,I是R的一个加法子群,如果I还满足如下条件:

(对乘法的吸收性):对$\forall a\in R,b\in I$,都有$ab,ba\in I$,则称I是R的一个理想$(ideal)$,记之为$I\lhd R$.

环的商:设R是一个含1的环,$I\lhd R$.

(1)有加法商群$R/I:(R,+)/(I,+)\quad \overline{a}+\overline{b}=\overline{a+b}(\forall a,b\in R)$.

(2)在R/I中引进乘法"$\cdot$"如下:

$$\overline{a}\cdot\overline{b}=\overline{a\cdot b}(\forall a,b\in R)$$

$$\overline{a_1}=\overline{a_2}\iff a_1-a_2\in I\Rightarrow(a_1-a_2)b\in I(\forall b\in R)即a_1b-a_2b\in I\Rightarrow\overline{a_1b}=\overline{a_2b}.$$

结论:$(R/I,+,\cdot)$是一个环.

Definition 2.8. **环同态**设R_1,R_2是含1的环,$f:R_1\to R_2$是一个映射,如果f保运算,即

(1)$f(a+b)=f(a)+f(b)(\forall a,b\in R_1)$

(2)$f(ab)=f(a)f(b)(\forall a,b\in R_1)$

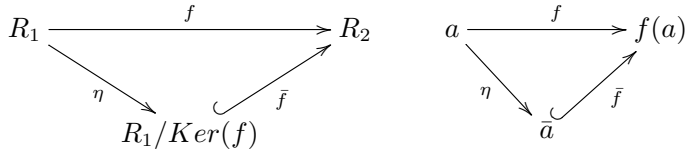
(3)$f(1)=1$

Theorem 2.1. **环同态基本定理**设R_1,R_2是含1的环,$f:R_1\to R_2$是一个环同态,则

(1)f的核$kerf=f^{-1}(0)=\{a\in R_1:f(a)=0\}$是$R_1$的理想,即$kerf\lhd R_1,imf=f(R_1)\leq R_2$.

(2)有环同构$R_1/kerf\simeq imf$,故有交换图

$$f = \overline{f} \circ \eta$$



$$\overline{f} : R/kerf \to R_2$$
$$\overline{a} \to f(a)$$
$$\overline{f}(\overline{a}) = \overline{f}(\overline{b}), a, b \in R_1 \Rightarrow f(a) = f(b) \Rightarrow f(a-b) = 0 \Rightarrow a - b \in kerf \Rightarrow \overline{a} = \overline{b}.$$

事实:环同态$f : R_1 \to R_2$是单一同态 $\iff$ $kerf = \{0\}$.

$(R, +, \cdot)$是含1交换环

平凡理想:0与R

理想的交:I, J

$$(I \bigcap J, +)$$
$$b \in I \bigcap J, \forall a \in R$$
$$ab \in I, ab \in J \Rightarrow ab \in I \bigcap J$$

结论:理想对取"交"封闭.

Definition 2.9. 子集生成的理想:$\emptyset \neq S \subset R$(环),记$\mathscr{F}(S) = \{I : I \lhd R, I \supset S\}$, 令$< S >= \bigcap\{I : I \lhd R, I \supset S\} = \bigcap\limits_{I \in \mathscr{F}(S)} I$

特别地,可由一个元素生成的理想称为一个主理想.$I =< a > (a \in R)$.

$(R, +, \cdot)$环(含1),$a \in R \Rightarrow Ra, aR, RaR \subset < a >, Ra = \{ra : r \in R\}$

$RaR \subset < a >, \alpha \in RaR \iff \alpha = r_1 a r_1' + r_2 a r_2' + \cdots + r_n a r_n'$

又$RaR \lhd R, RaR \supset < a >$,故$< a >= RaR$.

特别地,当R是含1交换环时,$< a >= Ra(= aR), < a_1, \ldots, a_n >= Ra_1 + \cdots + Ra_n$.

$< \emptyset >= \{0\}$

R是含1交换环.I, J. $I \bigcap J \lhd R, I \bigcup J$不一定是理想. $< I \bigcup J > \subset I + J \subset K, K \lhd R$且$K \supset I \bigcup J, a \in I, b \in J, a + b \in K$.

Proposition 2.1. 设$(R, +, \cdot)$是一个含*1*的交换环.

*(1)*对$\forall a \in R, < a >= Ra$.

(2)$I_1, \ldots, I_n \lhd R$,则$< I_1 \bigcup \cdots \bigcup I_n >= I_1 + \cdots + I_n$.

更一般地,对R的任一簇理想$\{I_\alpha\}_{\alpha \in \Lambda}$,有$< \bigcup\limits_{\alpha \in \Lambda} I_\alpha >= \sum\limits_{\alpha \in \Lambda} I_\alpha$.

Definition 2.10. 设R是含*1*交换环,$I \lhd R$,称I是R的一个极大理想,如果下述条件成立:

(1)$1 \notin I$(即$I \neq R$),也即I是R的真理想*(proper)*.

(2)(极大性)如果$J \lhd R$,且$I \subset J \subset R$则$J = I$或$J = R$.

Theorem 2.2. 含*1*交换环必有极大理想.由此可知,该环中的任一个真理想必包含于某个极大理想中.

证明. (*Zorn*引理的引用)

令$S = \{I \lhd R : 1 \notin I\}, 0 \in S$,故$S \neq \emptyset$,且$S$在集合的"包含$\subset$"关系下是一个偏序集.

任取S中的一个全序子集$(Chain)\{I_\alpha\}_{\alpha\in\Lambda}$, 即对$\forall\alpha, \beta \in \Lambda, I_\alpha \subset I_\beta$或$I_\beta \subset I_\alpha$.

令$J = \bigcup\limits_{\alpha\in\Lambda} I_\alpha$.断言:$J$是$R$的一个真理想.

事实上,对$\forall a, b \in J$,则$a \in I_\alpha, b \in I_\beta$(对某个$\alpha, \beta \in \Lambda$).

由所设,不妨设$I_\alpha \subset I_\beta$,则$a, b \in I_\beta \Rightarrow a + b \in I_\beta$且对$\forall c \in R, ca \in I_\beta \Rightarrow a + b \in J$且$ca \in J \Rightarrow J$是理想.

又$1 \notin J$,假如不然,由$1 \in J \Rightarrow 1 \in I_\alpha$(对某个$\alpha \in \Lambda$),矛盾!

综上,J是$\{I_\alpha\}_{\alpha\in\Lambda}$在$S$中的一个上界,故由$Zorn$引理,命题得证.

□

练习:

1.Z中的所有理想,极大理想.

2.$Z/24Z$中的所有理想,极大理想.

2.3 理想、模、分式环

A是一个含1交换环

Definition 2.11. **(素理想):** $I \rhd A$真理想, 满足条件: $a, b \in A$ 若$ab \in I$, 则$a \in I$或$b \in I$,称I是A的一个素理想

Example 2.3. $A = Z, I \rhd A$是素理想$\Longleftrightarrow I = \langle n\rangle$其中$n = p(p$是素数$)$或$n = 0$

Example 2.4. $B = F[x]$,F是域,$\mathcal{P} \rhd B$是素理想$\Longleftrightarrow \mathcal{P} = \langle p(x)\rangle$其中$p(x)$是$F[x]$的不可约多项式$Z[x]$不是$PID($主理想整环$)$(因为$I = \langle 2, x\rangle$不是由一个元素生成的主理想)

商环

设A是含1交换环, $\mathcal{M} \rhd A$是极大理想,$\overline{A} = A/\mathcal{M}$ 。$\forall\bar{a} \in \bar{A}(a \in A), \bar{a} = \bar{0} \Longleftrightarrow a \in \mathcal{M}$, 故有$\forall\bar{a} \neq \bar{0} \Longleftrightarrow a \notin \mathcal{M}$, 从而$\mathcal{M} \subsetneq \{a + \mathcal{M}\} \subseteq A$。由$\mathcal{M}$是极大理想, 所以$A =< a + \mathcal{M} >= \langle a\rangle + \mathcal{M}$。因为$1 \in A, \exists x \in \langle a\rangle, y \in \mathcal{M}$,即$x = ax_1, x_1 \in A$ 有$1 = x + y = ax_1 + y$, 从而有$\bar{1} = \overline{ax_1 + y} = \bar{a}\bar{x}_1 + \bar{y}$。因为$y \in \mathcal{M}$, 所以有$\bar{y} = \bar{0}$, 从而$\bar{1} = \bar{a}\bar{x_1}$, 即$\bar{a}$在$\bar{A}$中可逆。 $\bar{A}$在任一个非零元$\bar{a}$都有逆, 故$\bar{A} = A/\mathcal{M}$是域。

Proposition 2.2. **(极大理想的判别)** 设A是交换环*(*含*1)*, $I \rhd A$真理想, 则I是A的极大理想$\Longleftrightarrow A/I$是一个域

证明. "$\Rightarrow$" (必要性)记$\bar{A} = A/I, \forall\bar{a} \in \bar{A}\backslash\{0\}(a \in A)$, 则 $a \in I$。令$J = \langle\{a\} \cup I\rangle = \langle a\rangle + I$, 则$J \rhd A$且$I \subsetneq J \subseteq A$。由$I$是极大理想, 故$J = A$,即$A = \langle a\rangle + I$。由于$1 \in A$, 所以$\exists x = ax_1 \in$

$\langle a\rangle$，其中$x_1 \in A, y \in I$，于是有$1 = x + y = ax_1 + y$，从而在A中有$\bar{1} = \overline{ax+y} = \bar{a}\bar{x} + \bar{y} = \bar{a}\bar{x}$，(因为$y \in I$，所以$\bar{y} = \bar{0}$)即$\bar{1} = \bar{a}\bar{x}$，所以$\bar{a}$在$\bar{A}$中可逆，故$\bar{A}$是一个域。
“$\Leftarrow$” (充分性)任取$J \rhd A$，使得$I \subseteq J \subseteq A$。若$J \neq I$(下证$J = A$)，则有$x \in J \backslash I$，于是在$\bar{A}$中，$\bar{a} \neq \bar{0}$，由于$\bar{A}$是域，故$\exists y \in A$，使得$\bar{x}\bar{y} = \bar{1}$，即$\overline{xy} = \bar{1}$，从而$1 - xy \in I$，即$1 \in xy + I \subseteq J$。故$J = A$ □

记号:$I \rhd A, \bar{A} = A/I, a, b \in A, \bar{a} = \bar{b} \Longleftrightarrow a - b \in A$,也记为$a \equiv b(\mathrm{mod} I)$

Proposition 2.3. **（素理想的判别）**设A是交换环*(含1)*，$I \rhd A$真理想，则I是A的素理想$\Longleftrightarrow$ A/I是一个整环*(证明作为课后练习)*

记号:常记(1)spec$A$=$\{\mathcal{P}$—$\mathcal{P}$是A的素理想$\}$ (2)Max$A$=$\{\mathcal{M} \mid \mathcal{M}$是$A$的极大理想$\}$

Corollary 2.1. *在含1交换环A中,极大理想也是素理想*

Definition 2.12. *设A是交换环(含1),定义$J(A) = \bigcap_{m \in Max(A)} m$,称它为$A$的Jacobson根*

Definition 2.13. **（幂0元）** *设A是交换环(含1),$a \in A$,如果有$\exists n \in Z_{\geq 1}$,使得$a^n = 0$，则称a为A一个幂0元。记$N(A)$=$\{a \in A$—a是A的幂0元$\}$*

Proposition 2.4. *$N(A) \rhd A$,称$N(A)$为A的幂0根。(nipotant radical),有时也称$N(A)$=rad(A)*

(证明用于课后练习)
当N(A)=0时，称A是既约环

Proposition 2.5. *$N(A/N(A))$=$\{\bar{0}\}$,即$A/N(A)$是既约的(rediced)*

证明. 任取$\bar{a} \in \mathrm{N}(A/\mathrm{N}(A))(a \in A)$，则$\exists n \in Z_{\geq 1}$,使得$\bar{a}^n = \bar{0}$，即有$\overline{a^n} = \bar{0}$，故$a^n \in \mathrm{N}(A)$。从而$\exists m \in Z_{\geq 1}$,使得$(a^n)^m = 0$，即$a^{nm} = 0$，故有$a \in \mathrm{N}(A)$，从而$\bar{a} = \bar{0}$。所以N$(A/\mathrm{N}(A))$=$\{\bar{0}\}$。 □

Proposition 2.6. *设A是交换环(含1),则$N(A)$=$\bigcap_{\mathcal{P} \in spec(A)} \mathcal{P}$*

证明. 首先证N$(A) \subseteq \bigcap_{\mathcal{P} \in spec(A)} \mathcal{P}$。 $\forall a \in \mathrm{N}(A) \exists n \in Z_{\geq 1}$,使得$a^n = 0 \in \mathcal{P} (\forall \mathcal{P} \in spec(A))$。由于$\mathcal{P}$是素理想,所以$a \in \mathcal{P}$。故有N$(A) \subseteq \bigcap_{\mathcal{P} \in spec(A)} \mathcal{P}$。
下证$\bigcap_{\mathcal{P} \in spec(A)} \mathcal{P} \subseteq$N$(A)$。任取$a \in A/\mathrm{N}(A)$,则$\forall n \in Z_{\geq 1}$,有$a^n \neq 0$。令

$$\varepsilon = \{I \rhd A | n \cap a^{Z_{\geq 1}} = \varnothing\} = \{I \rhd A | a^n \notin I, \forall n \in Z_{\geq 1}\},$$

显然$\langle 0\rangle \in \varepsilon$,则$\varepsilon \neq \varnothing$。因为在通常的包含关系下，$(\varepsilon, \subseteq)$构成一个偏序集。故任取$\varepsilon$中的一个全序子集$\{I_\alpha\}_{\alpha \in \Lambda}$，令$J = \cup_{\alpha \in \Lambda} I_\alpha$。由于$\{I_\alpha\}_{\alpha \in \Lambda}$有包含关系,从而$J \rhd A$。
下证$J \in \varepsilon$,即证$J \cap a^{Z_{\geq 1}} = \varnothing$。若不然,则有$a^m \in J (\exists m \in Z_{\geq 1})$。由于$J = \cup_{\alpha \in \Lambda} I_\alpha$,则$\exists \alpha \in \Lambda$,使得$a^m \in I_\alpha$与$I_\alpha \in \varepsilon$矛盾。从而$J \cap a^{Z_{\geq 1}} = \varnothing$，故$J \in \varepsilon$,即$J$是全序子集$\{I_\alpha\}_{\alpha \in \Lambda}$在$\varepsilon$中的上界。由Zorn引理,$\varepsilon$必有极大元。设$J$为是一个$\varepsilon$的极大元,且$J \in specA$,即$J$是素理想。从而$\forall x, y \in A, xy \in J$,有$x \in J$或$y \in J$。若不然$x \notin J$且$y \notin J$,有$\langle x\rangle + J \supsetneqq J, \langle y\rangle + J \supsetneqq J$。由$J$的极大

性得$\langle x\rangle + J \notin \varepsilon, \langle y\rangle + J \notin \varepsilon$。又由$\varepsilon$的定义,$\exists m, n \in Z_{\geq 1}$使得$a^m \in \langle x\rangle + J, a^n \in \langle y\rangle + J$。从而$a^{mn} = a^m a^n \in (\langle x\rangle + J)(\langle y\rangle + J) \subseteq \langle xy\rangle + J$(因为$xy \in J$)与$J \in \varepsilon$矛盾。所以$J \in specA$，故$\forall a \in A/\mathrm{N}(A)$，有$a \notin J, J \rhd A$是素理想，所以$a \notin \bigcap_{\mathcal{P}\in spec(A)} \mathcal{P}$。故$a \in \bigcap_{\mathcal{P}\in spec(A)} \mathcal{P}$，从而$b \in \mathrm{N}(A)$,即$\bigcap_{\mathcal{P}\in spec(A)} \mathcal{P} \subseteq \mathrm{N}(A)$。
综上$\mathrm{N}(A)=\bigcap_{\mathcal{P}\in spec(A)} \mathcal{P}$ □

$I \rhd A$,

$$A \twoheadrightarrow \bar{A} = A/I$$
$$I \longmapsto J/I$$

$\mathrm{N}(A/I)=\bigcap_{\mathcal{P}\in spec(A/I)} \mathcal{P}=\bigcap_{\mathcal{P}\in spec(A),\mathcal{P}\supset I} \mathcal{P}$

Definition 2.14. 设A是交换环*(含1)*,$I \rhd A$,定义$\sqrt{I}$ =*rad(I)*,称之为的I根
rad(I)=$\sqrt{I} \triangleq \{a \in A | \exists n \in Z_{\geq 1}$,使得$a^n \in I\}$

显然$I \subset \sqrt{I}, rad(I) \rhd A$(课后练习) 特别的,当rad($I$)=$I$时,称$I$是$A$的一个根理想,rad(rad($I$))=rad($I$
$\sqrt{I}$,即rad(I)是一个根理想

证明. 显然$\sqrt{I} \subset \sqrt{\sqrt{I}}$,下证$\sqrt{\sqrt{I}} \subset \sqrt{I}$。$\forall a \in \sqrt{\sqrt{I}}, \exists m \in Z_{\geq 1}$，使得$a^m \in \sqrt{I}$。也$\exists n \in Z_{\geq 1}$，使得$a^{mn} = a^{nm} \in I$。故有$a \in \sqrt{I}$，即$\sqrt{I} = \sqrt{\sqrt{I}}$ □

特别的，$\sqrt{0}$ =N(A)。

Proposition 2.7. 设A是交换环*(含1)*,$I \rhd A$，则$\sqrt{I}$ =*rad(I)*=$\bigcap_{\mathcal{P}\in spec(A),\mathcal{P}\supset I} \mathcal{P}$。记$A$的*Jaobson radical*为$J(A)=\bigcap_{m\in MaxA} m$。

Proposition 2.8. 设A和$J(A)$如上，则$x \in J(A) \iff 1 - xy \in A^* = u(A)(\forall y \in A)$，其中$u(A)$是指$A$的乘法单位群。$u(A)$=$\{a \in A | \exists b \in A$，使得$ab = 1\}$。

证明. “⇐”：若$x \notin J(A) = \bigcap_{m\in MaxA} m$，则存在$\mathcal{M} \in$Max$A$，使得$x \notin \mathcal{M}$。则$\mathcal{M} \subsetneqq \langle x\rangle + \mathcal{M}$，从而$\langle x\rangle + \mathcal{M} = A$，即存在$y \in A, m \in \mathcal{M}$，使得$1 = m + xy$。故$1 - xy = m \in \mathcal{M}$与$1 - xy \in u(A)$矛盾。所以$x \in J(A)$。
“⇒”：若$1 - xy \notin u(A)$，则$\langle 1 - xy\rangle \neq A$。即存在$\mathcal{M}'$是极大理想，使得$\langle 1 - xy\rangle \subsetneq \mathcal{M}'$。从而$1 - xy \in \mathcal{M}'$，故$1 \in xy + \mathcal{M}'$。由于$x \in J(A) = \bigcap_{m\in MaxA} m$，从而有$x \in \mathcal{M}'$，即$xy \in \mathcal{M}'$，故$1 \in xy + m' \subset \mathcal{M}'$,这与$\mathcal{M}'$是极大理想矛盾。所以$1 - xy \in u(A)$。 □

Theorem 2.3. 中国剩余定理*(Chinese Remainder thm)* 设A是一个含*1*交换环，$I_1, I_2, \ldots I_n \rhd A$，且这些理想两两互素，即$I_j + I_k = \langle 1\rangle = A(\forall j, k \in \{1, 2, \ldots n\}, j \neq k)$，则
(1)$I_1 I_2 \ldots I_n = I_1 \cap I_2 \cap \cdots \cap I_n$
(2)$A/I_1 \cap I_2 \cap \cdots \cap I_n \simeq A/I_1 \times A/I_2 \times \cdots \times A/I_n$
换言之，

$$\phi : A \to A/I_1 \times A/I_2 \times \cdots \times A/I_n$$
$$a \longmapsto (a + I_1, a + I_2, \ldots, a + I_n)$$

是一个环满同态，且*ker(*ϕ*)*=$I_1 \cap I_2 \cap \cdots \cap I_n$。

Definition 2.15. 设A是一个含*1*交换环，$I \triangleright A, J \triangleright A$。若有$I+J=A$，则称$I$与$J$互素。

Example 2.5. $A=Z[x], p=\langle 2\rangle, q=\langle x\rangle$。由于$Z[x]/\langle x\rangle \simeq \mathbb{Z}$是整环，得$q \triangleright A$是素理想。$p=\langle 2\rangle$显然也是素理想，$p+q=\langle 2\rangle+\langle x\rangle=\langle 2,x\rangle$。考虑

$$\begin{array}{ccccc} \mathbb{Z}[X] & \overset{\phi}{\twoheadrightarrow} & \mathbb{Z} & \overset{\psi}{\twoheadrightarrow} & \mathbb{Z}/2\mathbb{Z} \\ f(x) & \mapsto & f(0) & \mapsto & \overline{f(0)} \\ & & m & \mapsto & \overline{m} \end{array}$$

则$\eta=\psi\circ\phi$: $\mathbb{Z}[x]\to\mathbb{Z}/2\mathbb{Z}=\{\bar{0},\bar{1}\}$环满同态，且$ker\eta$=$\{f(x)\in\mathbb{Z}[x] \mid \overline{f(0)}=\bar{0}\}$=$\{f(x)\in\mathbb{Z}[x] \mid 2|f(0)\}$=$\langle 2,x\rangle$,则$\mathbb{Z}[x]/\langle 2,x\rangle \simeq \mathbb{Z}/2\mathbb{Z}$是域，因此$m=\langle 2,x\rangle=q+p$是极大理想。但显然$1\notin\langle 2,x\rangle$，从而$q$与$p$并不是互素的。

Definition 2.16. A,B是两个含*1*交换环，令$A\times B$=$\{(a,b) \mid a\in A, b\in B\}$，则$A\times B$是一个环*(*按照分量相加，相乘*)*，称之为两个环的乘积。

$$\begin{aligned} \phi: A &\to A/I_1\times A/I_2\times\cdots\times A/I_n \\ a &\longmapsto (a+I_1, a+I_2, \ldots, a+I_n) \end{aligned}$$

显然是一个同态，下面说明是满的，即任意的$(a_1+I_1, a_2+I_2, \ldots, a_n+I_n)\in A/I_1\times A/I_2\times\cdots\times A/I_n$，存在$a\in A$，使得$\phi(a)=(a_1+I_1, a_2+I_2, \ldots, a_n+I_n)$，即$(a_1+I_1, a_2+I_2, \ldots, a_n+I_n)=(a+I_1, a+I_2, \ldots, a+I_n)$，从而有，即是方程组的解。

Example 2.6. $A=\mathbb{Z}$，$I_1=\langle 2\rangle, I_2=\langle 3\rangle, I_3=\langle 5\rangle$

$$\begin{cases} x\equiv a_1 \pmod{\langle 2\rangle} \\ x\equiv a_2 \pmod{\langle 3\rangle} \\ x\equiv a_3 \pmod{\langle 5\rangle} \end{cases}$$

有解$x=a$.

2.4

2.4.1 几类重要的特殊环

A是一个含1交换环

Definition 2.17. **（局部环）***:*只有一个极大理想的含*1*交换环，就称为局部环。

Proposition 2.9. 设A是一个局部环，m是A的极大理想，则$A^\times=u(A)=A\backslash m$

证明. 因为$a\in A$，存在$b\in A$，使得$ab=1$，所以$aA=\langle a\rangle=A$，故$a\notin m$，即$a\in A\backslash m$，从而有$u(A)\subset A\backslash m$。若$aA\neq A$，由$\langle a\rangle\triangleright m$，且$A$是局部环，只有唯一极大理想$m$，则$\langle a\rangle\subset m$，从而$a\in m$。即由$a\notin A^\times$，有$a\in m$。综上有$A^\times=u(A)=A\backslash m$。 □

Fact: $I \triangleright A$,若$A\backslash I = A^\times$，则A是一个局部环且I是它的唯一一个极大理想。

Example 2.7. 由$\mathbb{Q}\backslash\{0\} = u(\mathbb{Q})$，得$\mathbb{Q}$是一个局部环。

Fact: 任一个域都是局部环。下面举一个不是域但是是局部环的例子。 $A = \{\frac{b}{a} \mid (a,b) = 1, a, b \in \mathbb{Z}, 2 \nmid a\}$。由于$A^\times = u(A) = \{\frac{b}{a} \mid a, b \in \mathbb{Z}, (a,b) = 1, 2 \nmid ab\}$，$m = \{\frac{b}{a} \mid a, b \in \mathbb{Z}, (a,b) = 1, 2 \mid b, 2 \nmid a\} = 2A$，所以$A\backslash m = u(A)$。又$A/2A \cong \mathbb{Z}/2\mathbb{Z} \cong \mathbb{F}_2$, 所以，$2A$是$A$的极大理想且是唯一的，故$A$是局部环。

Example 2.8. $A = \mathbb{Z}/4\mathbb{Z}$，$m = 2\mathbb{Z}/4\mathbb{Z}$.$A$是一个局部环,且$A/m \cong \mathbb{Z}/2\mathbb{Z}$,所以$A$是$m$的唯一极大理想。

2.4.2 UFD唯一分解环或唯一析因环

Definition 2.18. **不可约元**:设A是一个含*1*交换环，$a \in A$且$a \neq 0, a \notin A^\times$，如果下述条件成立:$a = bc, b, c \in A$，有$b \in A^\times$,或者$c \in A^\times$，则称$a$是$A$一个不可约元。

Definition 2.19. ***UFD***:设A是一个整环，如果A中任一个非*0*非单位元都可分解为有限个不可约元之积，且在不计单位顺序下，上述分解是唯一的，则称A是一个*UFD*。

Example 2.9. $\mathbb{Z}$是个*UFD*。

Example 2.10. F是域，$F[x], F[x_1, x_2, \ldots, x_n]$是*UFD*。

Proposition 2.10. 设A是*UFD*,$\pi \in A$，π是一个不可约元，则$\langle\pi\rangle \triangleright A$是素理想。

证明. 对任意$ab \in \langle\pi\rangle$分，则存在$c \in A$，有$ab = c\pi$。由于$ab \in A$，A是UFD，则由唯一分解性，a中必有分解元π或者b分解出因子π，即$a \in \langle\pi\rangle$，或者$b \in \langle\pi\rangle$，从而$\langle\pi\rangle \triangleright A$是素理想。 □

记号:若$a = bc$，记$b \mid a, c \mid a$。

Proposition 2.11. *PID*必是*UFD*。

Example 2.11. *PID*:$\mathbb{Z}, F[x]$，其中F是域，$\mathbb{Z}[\sqrt{-1}] = \{a + b\sqrt{-1} \mid a, b \in \mathbb{Z}\}$
不是*PID*:$\mathbb{Z}$。*(*因为$\langle 2, x\rangle$不是主理想*)*。

环的特征

A是一个含1交换环。

$$\begin{aligned} f : \mathbb{Z} &\to A \\ 1 &\longmapsto 1_A \end{aligned}$$

f是一个环同态，且ker(f)=$n\mathbb{Z}$。所以有

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} &\hookrightarrow A \\ \bar{a} &\longmapsto f(a) \end{aligned}$$

因为$n\bar{a}=0$，所以对任意的$a\in A, na=0$。
情形1:char$A$=0(A的特征为0),此时$\mathbb{Z}\subset A, n\in\mathbb{Z}, a\in A$,由$na=0$，得$n=0$或者$a=0$。
情形2:char$A$=n($n\in\mathbb{Z}_{\geq 1}$)，n是使得对任意的$a\in A, na=0$成立的最小正整数。此时A的素环为$\mathbb{Z}/n\mathbb{Z}$

Example 2.12. $A=\mathbb{Z}/6\mathbb{Z}$,则$charA=6$。
$A=\mathbb{Z}/6\mathbb{Z}[x]$,则$charA=6$。特别的，当$A$是一个整环时，$chA=0$或者$p(p$是素数$)$。当$chA\neq 0$时，

$$f:\mathbb{Z}\to A$$
$$1\longmapsto 1_A$$

$ker(f)=n\mathbb{Z}(n\in\mathbb{Z})$，从而有$\mathbb{Z}/n\mathbb{Z}\subset A$子环，由于$A$是整环，故$A$无零因子，即$\mathbb{Z}/n\mathbb{Z}$无零因子，所以$n$为素数。

2.4.3 分式环(环的局部化方法)

设A是含1交换环，S是A的一个非空子集，如果S满足:
(1)$1\in S$
(2)$a,b\in S$，则$ab\in S$
则称S为A的一个乘法闭子集。由此可构造如下集合，

$$A\times S=\{(a,s)\mid a\in A, s\in S\}$$

在其中引入如下关系" "

$$(a_1,s_1)\hat{}(a_2,s_2)\in A\times S\Leftrightarrow\exists t\in S, t(s_2a_1-s_1a_2)=0$$

Fact: 上述定义的" "是$A\times S$上的一个等价关系(验证作为课后练习)。现考虑商集$A\times S/\hat{}$。对于$(a,s)\in A\times S$，将(a,s)的上述等价类$\overline{(a,s)}\triangleq\frac{a}{s}$。且记$A\times S/\hat{}=S^{-1}A$ 在中引入如下运算(一般取$0\notin S$,若$0\in S$,则$S^{-1}A=\{0\}$)
加法:$\frac{a_1}{s_1}+\frac{a_2}{s_2}\triangleq\frac{a_1s_2+a_2s_1}{s_1s_2}(a_1,a_2\in A, s_1,s_2\in S)$
乘法:$\frac{a_1}{s_1}\Delta\frac{a_2}{s_2}\triangleq\frac{a_1a_2}{s_1s_2}$(验证上述定义的有效性，课外练习)
结论:$(S^{-1}A,+,\Delta)$是一个含1交换环，称A为关于S的分式环

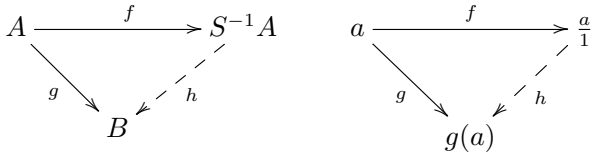
$$f:A\to S^{-1}A$$
$$a\longmapsto\frac{a}{1}$$

是环同态 $ker(f)=\{a\in A\mid\frac{a}{1}=0=\frac{0}{1}\}$=$\{a\in A$ |存在$t\in S$,使得$t(1\Delta a-1\Delta 0)=0\}$=$\{a\in A\mid ta=0\}$

Theorem 2.4. ***分式环的泛性质(univerasity)*** 设S是环A($一个含1交换环$)的一个乘法封闭子集，则典范同态

$$f:A\to S^{-1}A$$
$$a\longmapsto\frac{a}{1}$$

有如下泛性质:任意一个环同态g,$g: A \to B$,如果$g(S) \subset B^\times = u(B)$,则存在唯一的环同态$h: S^A \to B$使得下图可交换:



证明. 存在性:令

$$h: S^{-1} \to B$$
$$\frac{a}{s} \longmapsto g(a)\Delta g(s)^{-1}$$

需要证明h是良好定义的,对任意$\frac{a_1}{s_1} = \frac{a_2}{s_2} \in S^{-1}A$,则$h(\frac{a_1}{s_1}) = g(a_1)\Delta g(s_1)^{-1}, h(\frac{a_2}{s_2}) = g(a_2)\Delta g(s_2)^{-1}$,由于$\frac{a_1}{s_1} = \frac{a_2}{s_2}$,则存在$t \in S$，使得$t(s_2a_1 - s_1a_2) = 0$, 所以

$$g(t(s_2a_1 - s_1a_2))g(t)g(g(s_2a_1) - g(a_2s_1)) = 0.$$

因为$t \in S$,所以$g(t)$可逆，故有$g(s_2)g(a_1) - g(s_1)g(a_2) = 0$,从而$g(s_2)g(a_1) = g(s_1)g(a_2)$，即$g(s_2)^{-1}g(a_2) = g(s_1)^{-1}g(a_1)$,所以$h(\frac{a_1}{s_1}) = h(\frac{a_2}{s_2})$。从而$h$是良好定义的，即这样的环同态$h$是存在的。唯一性:显然。 □

Fact:特别的，S不含A中的零因子时，

$$f: A \to S^{-1}A$$
$$a \longmapsto \frac{a}{1}$$

是一个单一的环同态，实际上$ker(f) = \{a \in A \mid \frac{a}{1} = 0\} = \{a \in A \mid \exists t \in S, ta = 0\} = \{0\}$

Example 2.13. A是整环,则$S = A\backslash\{0\}$是一个A的乘法封闭子集，此时分式环$S^{-1}A$是一个域，称为的分式商域。

证明. 显然$S^{-1}A$已经是一个分式环了，任意的$\alpha \neq 0 \in S^{-1}A$,即$0 \neq \alpha = \frac{a}{s}, a \in A, s \in S$。由于$\alpha = \frac{a}{s} = 0$当且仅当存在$t \in S$使得$ta = 0$。又由于$S$无零因子，所以$a = 0$，所以$\alpha = 0$当且仅当$a = 0$,故$\alpha = \frac{a}{s} \neq 0$当且仅当$a \neq 0$,即$a \in S$，于是$\frac{s}{a} \in S^{-1}A$。显然$\alpha\Delta\frac{s}{a} = \frac{a}{s}\Delta\frac{s}{a} = 1$,所以$\alpha$在$S^{-1}A$中可逆。从而$S^{-1}A$是一个域。 □

Example 2.14. $\mathbb{Z}, S = \mathbb{Z}\backslash\{0\}, \mathbb{Q} = S^{-1}\mathbb{Z}, A = \mathbb{Q}[x], S = \mathbb{Q}[x]\backslash\{0\}, S^{-1}A = \mathbb{Q}(x) = \{fracfg \mid f, g \in \mathbb{Q}[x], g \neq 0\}$,$A$是任一个含1交换环，则它的乘法封闭子集$S$可取为:
(1)$S = \{1\}$，则$S^{-1}A = A$。
(2)$\forall a \in A\backslash N(A), S = \{a^m \mid m \in \mathbb{Z}_{\geq 0}\}$
(3)$\forall p \in spec(A)$,由于$ab \in p$当且仅当 $a \in p$或者$b \in p$,则$ab \notin p$当且仅当$a \notin p$且$b \notin p$,所以$S = A\backslash p = \{a \in A \mid a \notin p\}$是一个乘法封闭子集。记$p$对应的分式环为$A_p = S^{-1}A$。 $I \triangleright A, \bar{A} = A/I$,

$$A \overset{\phi}{\twoheadrightarrow} A/I = \bar{A}$$

结论:$\bar{A}$的理想均形如J/I，其中$J \triangleright A$，且$I \subset J$。

Example 2.15. $\mathbb{Z}/4\mathbb{Z}, \langle 24\rangle \subset J \triangleright \mathbb{Z}$,所以$J$可以取:

$$\mathbb{Z}, 2\mathbb{Z}, 3\mathbb{Z}, 4\mathbb{Z}, 6\mathbb{Z}, 8\mathbb{Z}, 12\mathbb{Z}, 24\mathbb{Z}.$$

从而$\mathbb{Z}/24\mathbb{Z}$的理想为:

$$\mathbb{Z}/24\mathbb{Z}, 2\mathbb{Z}/24\mathbb{Z}, 3\mathbb{Z}/24\mathbb{Z}, 4\mathbb{Z}/24\mathbb{Z}, 6\mathbb{Z}/24\mathbb{Z}, 8\mathbb{Z}/24\mathbb{Z}, 12\mathbb{Z}/24\mathbb{Z}, 24\mathbb{Z}/24\mathbb{Z}.$$

素理想为:

$$2\mathbb{Z}/24\mathbb{Z}, 3\mathbb{Z}/24\mathbb{Z},$$

极大理想为:

$$2\mathbb{Z}/24\mathbb{Z}, 3\mathbb{Z}/24\mathbb{Z}$$

典范同态

$$\begin{aligned} f : A &\to S^{-1}A \\ I &\longmapsto S^{-1}I \end{aligned}$$

其中$I \triangleright A$,若$S \cap I \neq \varnothing$，则存在$a \in S$且$a \in I$，即$\frac{a}{a} = 1$在$S^{-1}I$中可逆，所以$S^{-1}I = S^{-1}A$。故若需要$S^{-1}I$是真理想，则需要$S \cap I = \varnothing$。

2.5 分式环

Theorem 2.5. 设S是含1交换环A的一个乘法封闭子集，则映射

$$\begin{aligned} \psi : \{P \in spec(A) \mid P \cap S = \varnothing\} &\to spec(S^{-1}A) \\ P &\longmapsto S^{-1}P \end{aligned}$$

是一个双射。

证明. 先证明任意$P \in spec(A)$,若$P \cap S = \varnothing$,则

$$\psi(p) = S^{-1}P = \{\frac{a}{s} \mid a \in P, s \in S\} \in spec(S^{-1}A).$$

先证明$S^{-1}P$是$S^{-1}A$的理想，其中$a_1, a_2 \in P, s_1, s_2 \in S$,

$$\frac{a_1}{s_1} + \frac{a_2}{s_2} = \frac{s_2a_1 + s_1a_2}{s_1s_2},$$

由于$s_2a_1 + s_1a_2 \in P, s_1, s_2 \in S$，所以$\frac{a_1}{s_1} + \frac{a_2}{s_2} \in S^{-1}P$ 对任意的$c \in A, s \in S, \frac{c}{s} \in S^{-1}A$,

$$\frac{c}{s} \cdot \frac{a_1}{s_1} = \frac{ca_1}{ss_1}$$

,由于$P \triangleright A$,得$ca_1 \in P$,从而$\frac{c}{s} \cdot \frac{a_1}{s_1}$,即$S^{-1}P \triangleright S^{-1}A$。

下证是$S^{-1}P$素理想。任意$\frac{a_1}{s_1}, \frac{a_2}{s_2} \in S^{-1}A, a_1, a_2 \in A; s_1, s_2 \in S$且$\frac{a_1}{s_1} \cdot \frac{a_2}{s_2} \in S^{-1}P$,即

$$\frac{a_1 a_2}{s_1 s_2} = \frac{a}{s}, a \in P, s \in S.$$

则存在$s' \in S$使得$s'(sa_1a_2 - s_1s_2a) = 0$,从而$s'sa_1a_2 = s's_1s_2a \in P$。

由于$S \cap P = \varnothing$,所以$s's \notin P$。又由于P是素理想,所以$a_1a_2 \in P$,得$a_1 \in P$或者$a_2 \in P$,从而$\frac{a_1}{s_1} \in S^{-1}P$或者$\frac{a_2}{s_2} \in S^{-1}P$,故$S^{-1}P$素理想。即$P \in spec(A)$,所以，$\psi$是有意义的。

再证明ψ是满的。任取$\beta \in spec(S^{-1}A)$,令

$$P = \{a \in A \mid \text{存在} s \in S, \text{使得} \frac{a}{s} \in \beta\},$$

下证$P \in spec(A)$，即P是A的一个素理想。首先证$P \triangleright A$。任取$a, b \in P$, 则存在$s_1, s_2 \in S$,使得$\frac{a}{s_1}, \frac{b}{s_2} \in \beta$,于是

$$\frac{a}{1} = \frac{s_1}{1} \cdot \frac{a}{s_1} \in \beta, \frac{b}{1} = \frac{s_2}{1} \cdot \frac{b}{s_2} \in \beta,$$

有$\frac{a}{1} + \frac{b}{1} = \frac{a+b}{1} \in \beta$,所以$a + b \in P$。又对任一个$c \in A$, $\frac{c}{1}\Delta\frac{a}{s_1} \in \beta$,即$\frac{ca}{s_1} \in \beta$,故$ca \in P$,从而$P \triangleright A$。

下证P满足素性条件。设$a, b \in A$且$ab \in P$。由定义存在$s \in S$,使得$\frac{ab}{s} \in \beta$, 即$\frac{a}{1}\Delta\frac{b}{s} \in \beta$。由于$\beta \in spec(S^{-1}A)$,则$\frac{a}{1} \in \beta$或者$\frac{b}{s} \in \beta$,从而$a \in P$或者$b \in P$,综上$P \in spec(A)$且$\psi(P) = \beta = S^{-1}P$,即$\psi$是满的。

下证ψ是单的。设$P_1, P_2 \in spec(A)$且$P_i \cap S = \varnothing (i = 1, 2)$。若$\psi(P_1) = \psi(P_2)$,则$S^{-1}P_1 = S^{-1}P_2$。下证$P_1 = P_2$即可。

任意$a_1 \in P_1$,有$\frac{a_1}{1} \in S^{-1}P_1 = S^{-1}P_2$,即$\frac{a_1}{1} = \frac{a_2}{s}, a_2 \in P_2, s \in S$。所以存在$s' \in S$使得$s'(sa_1 - a_2) = 0$,故有$s'sa_1 = sa_2 \in P_2$。由于$S \cap P_2 = \varnothing$，所以$a_1 \in P_2$,即$P_1 \subset P_2$;同理可得$P_2 \subset P_1$。综上$P_1 = P_2$,故$\psi$是单的。从而$\psi$是双射。

□

Example 2.16. 设A是含*1*交换环，$P \in spec(A)$是一个素理想，$S = A\backslash P$是一个乘法封闭子集，记关于S的分式环$S^{-1}A = A_P$，*(*有时称A_P为A关于P的局部化或者局部环*)*，$spec(A_P) = \{S^{-1}P \mid P_1 \in spec(A), P_1 \subset P\}$。特别的， $S^{-1}P$且是A_P中唯一的极大理想，故A_P是一个局部环。$S^{-1}P = (S^{-1}A)P = PA_P$，从而$A_P/PA_P$是一个域，称之为模$P$的剩余类域。

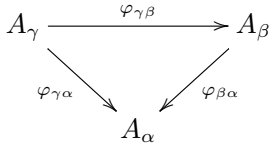
Example 2.17. 设A是含*1*交换环，$f \in A\backslash N(A)$，令$S_f = \{f^n \mid n \in \mathbb{Z}_{\geq 0}\} = \{1, f, f^2, f^3 \dots\}$，$S_f$是$A$的一个乘法封闭子集。对应的分式环$S_f^{-1}A$记为$A_f$。$spec(A_f) = \{S_f^{-1}P \mid P \in spec(A), P \cap S_f = \varnothing\}$。记$V(f) = \{P \mid P \in spec(A), f \in P\}$，所以$spec(A_f) = \{S_f^{-1}P \mid P \in spec(A), f \notin P\} \triangleq D(f) = spec(A)\backslash V(f)$。

2.6 反向极限与正向极限(在集合上)

2.6.1 正向集(directed portialy ordered set)

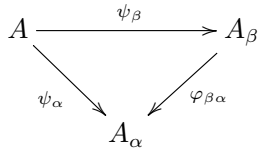
Definition 2.20. 设$(S, \leq)$是一个非空偏序集，对任意$i, j \in S$存在$k \in S$，使得$i \leq k, j \leq k$，则称$(S, \leq)$是一个正向集。

Definition 2.21. 反向系 设$(\Lambda,\leq)$是一个正向集，$\{A_\alpha\}_{\alpha\in\Lambda}$是一个集合簇，若对任意的$\alpha,\beta\in\Lambda$，当$\alpha\leq\beta$时，有映射$\varphi_{\beta\alpha}:A_\beta\to A_\alpha$且满足下列条件
(1)$\varphi_{\alpha\alpha}=id_{A_\alpha}$*(恒等映射)*，$\forall\alpha\in\Lambda$
*(2)*对任意的$\alpha,\beta,\gamma\in\Lambda$，若$\alpha\leq\beta\leq\gamma$，则有下图可交换

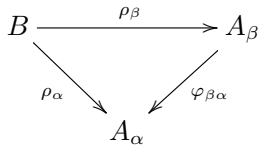


则称$\{(A_\alpha,\varphi_{\alpha\beta})\}$为定义在正向集$(\Lambda,\leq)$上的反向系。

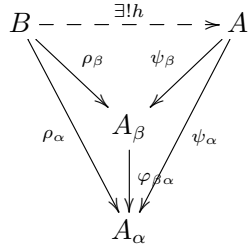
射影(反向)极限的构造 设$\{(A_\alpha,\varphi_{\beta\alpha})\}_\Lambda$是正向集$(\Lambda,\leq)$上的一个反向系，如果$A$是一个集合且对任意$\alpha\in\Lambda$，都有映射$\psi:A\to A_\alpha$满足对任意的$\alpha,\beta\in\Lambda$，若$\alpha\leq\beta$，则有下图可交换



如果还具备以下泛性质(universality)
设有集合B以及映射$\rho_\alpha:B\to A_\alpha(\forall\alpha\in\Lambda)$，如果$(B,\rho_\alpha)_{\alpha\Lambda}$满足



则存在唯一映射$h:B\to A$使得下面图表可交换



则称A是反向系$\{(A_\alpha,\varphi_{\beta\alpha})\}_{\alpha\in\Lambda}$的反向极限，记为$A=\varprojlim_\alpha A_\alpha$ 对于上述反向系$\{(A_\alpha,\varphi_{\beta\alpha})\}_{\alpha\in\Lambda}$，及其反向极限$A=\varprojlim_\alpha A_\alpha$。由构造可知$A=\varprojlim_\alpha A_\alpha=\{(x_\alpha)_{\alpha\in\Lambda}\mid\forall\alpha,\beta\in\Lambda,\alpha\leq\beta,x_\alpha\in A_\alpha,x_\alpha=\phi_{\beta\alpha}(x_\beta)\}$，特别的$\varprojlim_\alpha A_\alpha\subset\prod_{\alpha\in\Lambda}A_\alpha$。

Example 2.18. 取$\Lambda=\mathbb{Z}_{\geq1}$，当$m\mid n$时，定义为$m\leq n$。对任意$n\in\Lambda$，令$A_n=\mathbb{Z}/n\mathbb{Z}$*(模$n$的剩余类加群)*。对于任意的$m,n\in\Lambda$，若$m\leq n$，则令

$$\varphi_{nm}:\mathbb{Z}/n\mathbb{Z}\to\mathbb{Z}/m\mathbb{Z}$$
$$a+n\mathbb{Z}\longmapsto a+m\mathbb{Z}$$

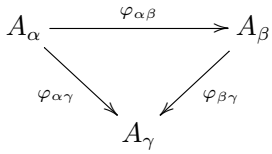
则$(A_n=\mathbb{Z}/n\mathbb{Z},\varphi_{nm})$是$(\Lambda,\leq)$上的一个反向系，其射影极限$\varprojlim_n\mathbb{Z}/n\mathbb{Z}\triangleq\hat{\mathbb{Z}}$

$\mathbb{Z} = \varprojlim_n \mathbb{Z}/P^n\mathbb{Z}$,($P$进整数)，$\mathbb{Z}_P \subset \prod_{n=1}^{\infty} \mathbb{Z}/P^n\mathbb{Z}$子集，$\Lambda = \mathbb{Z}_{\geq 1}, m \leq n$，则$(\Lambda, \leq)$是正向集。令$A_n = \mathbb{Z}/P^n\mathbb{Z}$，

$$\begin{aligned} \varphi_{nm} : \mathbb{Z}/P^n\mathbb{Z} &\to \mathbb{Z}/P^m\mathbb{Z} \\ a + P^n\mathbb{Z} &\longmapsto a + P^m\mathbb{Z} \end{aligned}$$

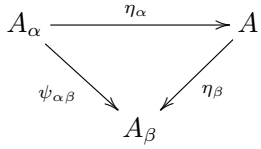
正向极限的定义和构造

Definition 2.22. 正向系 设$(\Lambda, \leq)$是一个正向集，$\{A_\alpha\}_{\alpha\in\Lambda}$是一个集合簇，若对任意的$\alpha, \beta \in \Lambda$，当$\alpha \leq \beta$时，有映射$\varphi_{\alpha\beta} : A_\alpha \to A_\beta$且满足下列条件
(1)$\varphi_{\alpha\alpha} = id_{A_\alpha}$*(*恒等映射*)*，$\forall \alpha \in \Lambda$
*(2)*对任意的$\alpha, \beta, \gamma \in \Lambda$，若$\alpha \leq \beta \leq \gamma$，则有下图可交换

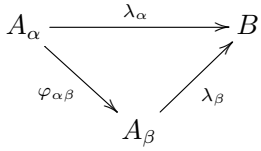


则称$\{(A_\alpha, \varphi_{\alpha\beta})\}$为定义在正向集$(\Lambda, \leq)$上的正向系。

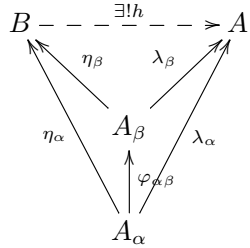
射影(正向)极限的构造 设$\{(A_\alpha, \varphi_{\alpha\beta}$是正向集$(\Lambda, \leq)$上的一个正向系，如果$A$是一个集合且对任意$\alpha \in \Lambda$，都有映射$\eta_\alpha : A_\alpha \to A$满足对任意的$\alpha, \beta \in \Lambda$，若$\alpha \leq \beta$，则有下图可交换



如果A还具备以下泛性质(universality)
设有集合B以及映射$\lambda_\alpha : A_\alpha \to B(\forall \alpha \in \Lambda)$，如果$(B, \lambda_\alpha)_{\alpha\Lambda}$满足



则存在唯一映射$\rho : A \to B$使得下面图表可交换



则称A是正向系$\{A_\alpha\}_{\alpha\in\Lambda}$的正向极限，记为$A = \varinjlim_\alpha A_\alpha$

Example 2.19. $\varinjlim_n \mathbb{Z}/n\mathbb{Z} = \mathbb{Q}/\mathbb{Z}$，其中

$$\begin{aligned}\varphi_{nm} : \mathbb{Z}/n\mathbb{Z} &\to \mathbb{Z}/m\mathbb{Z}\\ a + n\mathbb{Z} &\longmapsto \frac{m}{n}a + m\mathbb{Z}\end{aligned}$$

则$\{\mathbb{Z}/n\mathbb{Z}, \varphi_{nm}\}$构成正向系，其正向极限$\varinjlim_n \mathbb{Z}/n\mathbb{Z} = \mathbb{Q}/\mathbb{Z}$。

Example 2.20. $p \in \mathbb{C}, \Lambda$=$\{$开领域$U|\ p \in \mathbb{C}\}$,$U \le V \Leftrightarrow V \subset U$。对每个$U \in \Lambda$，令$F_U$ =$\{f \mid f$在U上的解析函数$\}$。若$U \le V \Leftrightarrow V \subset U$，

$$\begin{aligned}\varphi_{UV} : F_U &\to F_V\\ f &\longmapsto f\mid_V\end{aligned}$$

则$\{(F_U, \varphi_{UV})\}$是$(\Lambda, \le)$上的一个正向系，其正向极限记为$O_p = \varinjlim_{U\in\Lambda} F_U$
具体构造$\varinjlim_\alpha A_\alpha$，令$\widetilde{A} = \bigcup_{\alpha\in\Lambda} A_\alpha$，在$\widetilde{A}$中引入如下关系:$x, y \in \widetilde{A} \Rightarrow x \in A_\alpha, y \in A_\beta$。设$x \sim y$当且仅当存在$\gamma \in \Lambda$，使得$\varphi_{\alpha\gamma}(x) = \varphi_{\beta\gamma}(y)$。对于$\bar{f}, \bar{g} \in O_p = \varinjlim_{U\in\Lambda} F_U, \bar{f} \in F_U, \bar{g} \in F_V$，则$\bar{f} = \bar{g}$当且仅当存在$W \subset U \cap V$使得$f\mid_W = g\mid_W$

2.7 模

Definition 2.23. 设A是一个含*1*交换环，M是一个加法群，称M是一个$A-$模，如果有作用

$$\begin{aligned}A \times M &\to M\\ (a, \alpha) &\longmapsto a\Delta\alpha\end{aligned}$$

且满足“相关公理”*(*类似于向量空间中的公理*)*

子模

Definition 2.24. 设M是一个$A-$模，$N \subset M$,若N满足如下条件*:*
(1)N是M的加法子群
*(2)*对$a \in A, x \in N$有$ax \in N$
则称N是M的一个$A-$子模，记之为$N \le M$。

如果模M的子模只有0和M，则称M是一个单模

子模的交

设M是一个$A-$模，$M_\alpha \le M, \alpha \in \Lambda$，则$\cap_{\alpha\in\Lambda} \le M$

证明. 显然$\cap_{\alpha\in\Lambda}$是M子群，对任意的$x \in \cap_{\alpha\in\Lambda}, a \in A$，则有任意$\alpha \in \Lambda, x \in \cap_{\alpha\in\Lambda}$,得$\forall\alpha \in \Lambda, ax \in M_\alpha$，即$\forall\alpha \in \Lambda, ax \in \cap_{\alpha\in\Lambda} M_\alpha$，所以$\cap_{\alpha\in\Lambda}$是$M$子群。

□

注:子模的交仍是子模，但子模的并不一定是子模。

Example 2.21. $V = \mathbb{R}^2$,W_1=$\{x$轴$\}$,W_2=$\{y$轴$\}$，所以W_1, W_2是V的线性子空间，且$W_1 \cap W_2 = \{0\}$也是线性子空间，但$W_1 \cup W_2$ =$\{x$轴$\cup y$轴$\}$不是线性子空间。

生成模

设M是一个$A-$模，$S \subset M, S \neq \varnothing$，令$\langle S\rangle = \cap_{N\leq M, N\supset S}$，则$\langle S\rangle$是$M$中包含$S$的最小子模，称之为由$S$生成的子模。特别的，由一个元素生成的模$\langle x\rangle$为包含$x$的最小子模。

Fact:$N = \langle x\rangle = Ax$，显然$\langle x\rangle$是$Ax$的子模，而对任意一个子模$N'$，且$x \in N'$，由任意$a \in A$，有$ax \in N'$，得到$Ax \subset N'$，即$Ax$是包含$x$的最小子模。所以有$A\langle x\rangle = \langle x\rangle$

推广到有限个:$x_1, x_2, \ldots, x_n \in M, \langle x_1, x_2, \ldots, x_n\rangle = Ax_1 + Ax_2 + \cdots + Ax_n$

子模的和

$N, L \leq M, N + L \triangleq \{x + y \mid x \in N, y \in L\}$.

则$N + L =< N \cup L >$.

一般地，$N_1, N_2, \cdots, N_r \leq M$,则 $N_1 + \cdots + N_r = \{x_1 + \cdots + x_r | x_i \in N_i, i = 1, \cdots, r\}$.则

$$N_1 + \cdots + N_r =< N_1 \cup \cdots \cup N_r >$$

$$\sum_{\alpha\in\Lambda} N_\alpha =< \cup_{\alpha\in\Lambda} N_\alpha > (\text{里面的元素} \sum x_\alpha \text{为有限和})$$

设A是环，$I \lhd A$.则

$(1)(I, +) \leq (A, +)$,加法子群;

$(2)A \times I \to I$

$(a, \alpha) \mapsto a\alpha$,即$I$是一个$A-$模。

有限生成模

Definition 2.25. 设M是一个$A-$模，如果有$x_1, \cdots, x_n \in M$使得

$$M =< x_1, \cdots, x_n >= Ax_1 + Ax_2 + \cdots + Ax_n.$$

则称M是一个有限生成$A-$模。

自由模

Definition 2.26. *(基)*设M是一个$A-$模，如果存在$\{x_\alpha\}_{\alpha\in\Lambda}$使得如下条件成立:

*(1)*对$\forall x \in M$,都有$a_\alpha \in A(\forall\alpha \in \Lambda)$使得

$$x = \sum_{\alpha\in\Lambda} a_\alpha x_\alpha (\text{其中只有有限个}\alpha\text{使得}a_\alpha \neq 0).$$

*(2)*上述表示法唯一*(*等价于*0*表示法唯一*)*。

则称$\{x_\alpha\}$为M的一组$A-$基,此时称M是一个自由$A-$模*(*即有一组$A-$基的模，称为一个自由的$A-$模*)*.

例1.A是环(含1交换环)，$n \in \mathbb{Z}_{\geq 1}$。令$M = A^n$(卡氏积)，$x \in M, x = (x_1, \cdots, x_n), x_i \in A(\forall 1, \cdots, n)$

$$A \times M \to M$$

$$(a, x) \mapsto a \cdot x := (ax_1, \cdots, ax_n).$$

则显然$M = A^n$是一个自由$A-$模(因为$\epsilon_1 = (1, 0, \cdots, 0), \cdots, \epsilon_n = (0, \cdots, 0, 1)$是$M$的一组$A-$基)。

Definition 2.27. 设M,N是$A-$模，$f:M\to N$是一个映射，称f是一个$A-$模同态。如果f是$A-$线性，即

$$f(a\alpha+b\beta)=af(\alpha)+bf(\beta)(\forall a,b\in A,\alpha,\beta\in M).$$

若f是模同态，

- f是单的，称f是单同态;
- f是满的，称f是满同;
- f即单又满，则称f为一个模同构，此时亦称M与N同构，记之为$M\overset{f}{\cong}N$.

商模

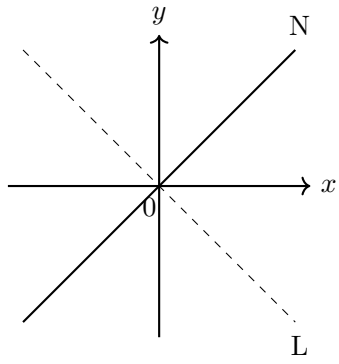
Proposition 2.12. 设M是一个$A-$模,$N\leq M$,则M/N是M关于N的商模。

证明. 规定$a\cdot\bar{x}:=\overline{ax}$.

下证这是良好定义的：设$x,x'\in M$,且$\bar{x}=\overline{x'}$,则$x-x'\in N$,由于$N\leq M$,对任意$a\in A$,$a(x-x')\in N\Rightarrow ax-ax'\in N\Rightarrow\overline{ax}=\overline{ax'}$.

显然M/N已是商群，再加上上面定义的模结构，成为一个模。 □

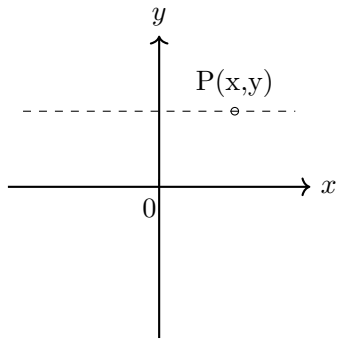
例 $M=\mathbb{R}^2,N=\mathbb{R}\alpha,\alpha=(1,1)$,则$M/N=L$.



$N=\mathbb{R}\alpha,\alpha=(1,0)$,则$M/N=y$轴。设$P=(x,y)$

$$\begin{aligned}\overline{(x,y)}=\bar{P}&=P+N\\&=(x,y)+\{(x',0)|x'\in\mathbb{R}\}\\&=\{(x+x',y)|x'\in\mathbb{R}\}\\&=\text{距离}x\text{轴长度为}y,\text{且与}y\text{轴平行}\\&=\overline{(0,y)}\end{aligned}$$

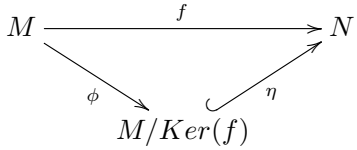
从而M/N是y轴。



Theorem 2.6. *(模同态基本定理)*设$f : M \to N$是一个$A-$模同态，则 *(1)*$f(M) = im(f) \leq N$,*(2)*f的核$Kerf = f^{-1}(0) \leq M$. *(3)*f导出模同构

$$\bar{f} : M/Ker(f) \simeq im(f)$$
$$\bar{a} \longmapsto f(a), \forall a \in M.$$

即有交换图



$f = \eta \circ \phi$.

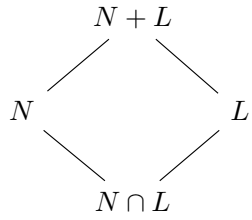
证明. (1)(2)显然成立。

(3)$\bar{f}$呈满射也显然，下证$\bar{f}$是单的。若$\forall \bar{x_1}, \bar{x_2} \in Im(f)$,且有$\bar{f}(\bar{x_1}) = \bar{f}(\bar{x_2})$. 则

$$f(x_1) = f(x_2) \Rightarrow f(x_1 - x_2) = 0 \Rightarrow x_1 - x_2 \in Ker(f) \Rightarrow \bar{x_1} = \bar{x_2}.$$

于是$\bar{f}$是单的。显然$\bar{f}$是模同态，于是$\bar{f}$是模同构。 □

Corollary 2.2. 设M是一个$A-$模，$N, L \leq M$,则有模同构



$(N + L)/N \cong L/(N \cap L)$.

Corollary 2.3. M是$A-$模，$N, L \leq M$,且$N \subseteq L$(则$N \leq L$),则$L/N \leq M/N$，且有模同构

$$(M/N)/(L/N) \cong M/L.$$

设M,N是$A-$模，记$Hom_A(M,N)=\{f:|f:M\to N$是一个模同态$\}$。$Hom_A(M,N)$上有加法以及同态的复合，构成一个非交换环。

$End_A(M)=\{f|f:M\to M$是一个模同态$\}$. $(End_A(M),+,\circ)$是一个环，其中"$\circ$"是映射的合成。

Lemma 2.1. *设M是有限生成$A-$模，$I\lhd A,\phi\in End_A(M)$,如果$\phi(M)\in IM$,则存在$a_0,a_1,\cdots,a_{n-1}\in I$使得*

$$\phi^n+a_{n-1}\phi^{n-1}+\cdots+a_1\phi+a_0=0.$$

证明. 由M是有限生成$A-$模，设$\alpha_1,\cdots,\alpha_n$是M的一组生成元，则$\phi(\alpha_1),\cdots,\phi(\alpha_n)\in IM=I\alpha_1+\cdots+I\alpha_n,\Rightarrow\phi(\alpha_1,\cdots,\alpha_n)=(\alpha_1,\cdots,\alpha_n)B,B\in M_n(I)$.

令

$$\begin{aligned}f(x)&=det(xE_n-B)\\&=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0.\end{aligned}$$

其中$a_0,a_1,\cdots,a_{n-1}\in I$. 类似于"高代"中Hamilton-Kayley定理的证明可得$f(\phi)=0$. 即 $\phi^n+a_{n-1}\phi^{n-1}+\cdots+a_1\phi+a_0=0$. □

Corollary 2.4. *设M是一个有限生成$A-$模，$I\lhd A$,如果$IM=M$,则存在$x\in A$使得$x\equiv 1(mod\ I)$且$x\cdot M=0$.(x零化M中的所有元素)*

证明. 在上一引理中，取$\phi=id$(恒等映射)且有$\phi(M)=M=IM$成立。则由上述引理，$\exists a_0,\cdots,a_{n-1}\in I$使得

$$id+a_{n-1}id^{n-1}+\cdots+a_1id+a_0=0\in End_A(M),$$

$\Rightarrow 1+a_{n-1}+\cdots+a_1+a_1=0$.令 $x=1+a_{n-1}+\cdots+a_1+a_0$,则$xM=0M=0$,且$x\in A$,有$x-1=a_{n-1}+\cdots+a_1+a_0\in I$.即$x\equiv 1(mod\ I)$。 □

Lemma 2.2. *(NaKayama引理1)设M是有限生成$A-$模，J是A的Jacobson根，$I\lhd A$且$I\subseteq J$,若$IM=M$，则$M=0$.*

证明. 由上述推论，$\exists x\in A$使得

$$x\equiv 1(mod\ I)\quad 且xM=0.$$

即$x-1\in I,\Rightarrow x=1+y,\exists y\in I\subseteq J$,即$y\in J\Rightarrow x=1+y\in u(A)$,$x$可逆。

从而$M=x^{-1}(xM)=x^{-1}0=0$. □

Lemma 2.3. *(Nakayama引理2)设M是有限生成$A-$模,$N\leq M,I\lhd A$且$I\subseteq J(A)$(J是A的Jacobson根),若$N+IM=M$,则$N=M$.*

证明. 考虑商模M/N.首先有$I\cdot(M/N)=(IM+N)/N$.

由于$a\bar{x}\in I\cdot(M/N)(a\in I,\bar{x}\in M/N)$,$ax\in IM+N,\Rightarrow\overline{ax}\in(IM+N)/N$.

$\overline{ax+y}\in(IM+N)/N(a\in I,x\in M,y\in N),\overline{ax+y}=\overline{ax}+\overline{y}=\overline{ax}=a\bar{x}\in I\cdot(M/N)$.

$\Rightarrow I\cdot(M/N)=(IM+N)/N.$

由于M是有限生成，$\Rightarrow M/N$也是有限生成，又由

$$N+IM=M\Rightarrow I(M/N)=(IM+N)/N=M/N.$$

由M/N是有限生成，由$NaKayama$引理$1\Rightarrow M/N=0\Rightarrow M=N.$ □

例：设A是一个局部环，M是一个生成$A-$模，m是A的唯一理想，$mM\leq M, A/m=F.$

M/mM是一个$F-$向量空间，若有限，取$\bar{x}_1,\cdots,\bar{x}_n$是其一组基，则$x_1,\cdots,x_n$是$M$的生成元(是一组基)

M是$A-$模，$I\lhd A, IM=0$,则M可看作一个$A/I-$模

$$A/I\otimes M\to M$$
$$(\bar{a},x)\mapsto \bar{a}\cdot x=\overline{ax}$$

Nakayama引理推论 A是一个局部环，$\mathfrak{m}$是它的极大理想，如果有$x_1,x_2,\cdots,x_n\in M$,使得$\bar{x_1},\bar{x_2},\cdots,\bar{x_n}\in M/\mathfrak{m}M$,是$M/\mathfrak{m}M$作为域$A/\mathfrak{m}$上线性空间的一组基，则$M=<x_1,\cdots,x_n>$.

证明. 令$N=<x_1,\cdots,x_n>$是M中由$x_1,\cdots,x_n$生成的$A-$子模，下证$M=N$.

为此,任取$x\in M$,则$\bar{x}\in M/\mathfrak{m}M$,由所设，有

$$\bar{x}=\bar{a}_1\bar{x}_1+\bar{a}_2\bar{x}_2+\cdots+\bar{a}_n\bar{x}_n$$

其中$a_1,\cdots,a_n\in A,\bar{a}_i\in A/\mathfrak{m}(i=1,\cdots,n)$. 即

$$\bar{x}=\overline{a_1x_1+\cdots+a_nx_n}\in M/\mathfrak{m}M$$
$$\Rightarrow x-(a_1x_1+\cdots+a_nx_n)\in\mathfrak{m}M$$

注意到$a_1x_1+\cdots+a_nx_n\in N=<x_1,\cdots,x_n>$,故$x\in N+\mathfrak{m}M\Rightarrow M\subset N+\mathfrak{m}M\Rightarrow M=N+\mathfrak{m}M.$
由于A是局部环，$\mathfrak{m}$是它的唯一的极大理想，所以A的$Janbous$根$J(A)=\mathfrak{m}$, 故由$Nakayama$引理,得$M=N.$ □

2.8 正合列

设A是一个含1交换环，M,N,L是A-模，$M\xrightarrow{f}N\xrightarrow{g}L$.设$f,g$是$A$-模同态，则$f$与$g$的合成是从$M$到$L$的模同态.

设$f:M\to N$是一个A-模同态，$K=kerf\leqslant M$,$K\xrightarrow{\eta}N\xrightarrow{f}L$，$f$与$\eta$的合成是0，$K$中元映到$N$中是0.

$L\leqslant M,\bar{M}=M/L$,我们有$L\xrightarrow{g}M\xrightarrow{f}M/L$,其中$g$是单射，且$g(L)=L, kerf=L$,则有$img=kerf$,即上面的列在$M$上正合.

$0\to L\xrightarrow{g}M\xrightarrow{f}M/L\xrightarrow{h}0$是一个短正合列，因为$kerh=M/L$,且$f$是满射，有$imf=M/L$

只要$L\to M$是单射，则在前面加个$0\to L\to M$,其就为一个正合列.

事实:设有模同态$L\xrightarrow{f}M, M\xrightarrow{g}N$,则$f$是单射$\Leftrightarrow 0\to L\xrightarrow{f}M$是正合列，$g$是满射$\Leftrightarrow M\xrightarrow{g}N\to 0$是正合列.

Definition 2.28. （模的正合列）：设有一个模同态，则$\cdots \to M_{n-1} \xrightarrow{f_{n-1}} M_n \xrightarrow{f_n} M_{n+1} \xrightarrow{f_{n+1}} \cdots$是一个正合列，如果它在任一个$M_n$处均正合，即$imf_{n-1} = kerf_n$.

设$f : M \to N$是一个A-模同态（任何一个模同态都能给出下面一个正合列）

$0 \to K \xrightarrow{g} M \xrightarrow{f} N \xrightarrow{h} N/f(M) \to 0$是一个$A-$模正合列，因为$K = kerf \leqslant M, f(M) \leqslant N, imf = kerh = f(M)$

2.9 $A-$模复型

设有一$A-$模同态列

$$\overline{M} : \cdots \to M_{n-1} \xrightarrow{f_{n-1}} M_n \xrightarrow{f_n} M_{n+1} \xrightarrow{f_{n+1}} \cdots,$$

如果在任意的M_n处，都有$f_n o f_{n-1} = 0$(对任意的n),则称它是一个（上）复型.

Definition 2.29. 上述列是一个A-模上复型，即$f_n o f_{n-1} = 0$(对任意的n)，等价的,$imf_{n-1} \subseteqq kerf_n$

Definition 2.30. 定义：$H^n(\overline{M}) = \frac{kerf_n}{imf_{n-1}}$，称之为上复型$\overline{M}$的第$n$个上同调群（此处，它也是个$A-$模）

对偶地，对于A-模下复型

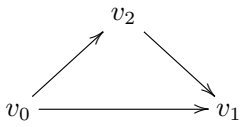
$$\overline{M_0} : \cdots \to M_{n+1} \xrightarrow{f_{n+1}} M_n \xrightarrow{f_n} M_{n-1} \xrightarrow{f_{n-1}} \cdots,$$

即对任意的n有$f_n o f_{n+1} = 0$成立，我们定义$H^n(\overline{M_0}) = \frac{kerf_n}{imf_{n+1}}$是第n个下同调群.

例：设X拓扑空间。则一个n-单形形如$< v_1, v_2 \cdots, v_n >$，其中$v_1 - v_0, v_2 - v_0 \cdots, v_n - v_0$是线性无关的.

令$C_n(K(x))$代表由X中所有n-单形生成的自由$Abel$群。则$C_0(K(x)) = ZX$.

$v_0 \longrightarrow v_1$　　$< v_0, v_1 >$边缘算子　$\alpha_1(< v_0, v_1 >) = \alpha_1(< v_1, v_2 >)$



$\alpha_1(< v_0, v_1 >, v_2) =< v_1, v_2 > - < v_0, v_2 > + < v_0, v_1 >$

一般地，$\alpha_n(< v_0, v_1 \cdots, v_n >) = \sum_{i=0}^{n} (-1)^i < v_0, v_1 \cdots, v_{i-1}, \widehat{v_i}, v_{i+1}, \cdots, v_n >$

得到$Z-$模复形（即$Abel$群下复形）：

$$\cdots \to C_n(K(x)) \xrightarrow{\alpha_n} C_{n-1}(K(x)) \xrightarrow{\alpha_{n-1}} \cdots$$

事实：$\alpha_n \circ \alpha_{n-1} = 0$. 例如

$$\begin{aligned}
\alpha^2(v_0, v_1, v_2) &= \alpha_1 \circ \alpha_2(v_0, v_1, v_2) = \alpha_1(\alpha_2(v_0, v_1, v_2)) \\
&= \alpha_1(< v_1, v_2 > - < v_0, v_2 > + < v_0, v_1 >) \\
&= \alpha_1(< v_1, v_2 >) - \alpha_1(< v_0, v_2 >) + \alpha_1(< v_0, v_1 >) \\
&=< v_2 > - < v_1 > -(< v_2 > - < v_0 >) + (< v_1 > - < v_0 >) \\
&= 0.
\end{aligned}$$

定义：$H_n(Z,X)=H_n(K(\tilde{X}))=\frac{ker\alpha_{n-1}}{im\alpha_n}$.

$n-$单形

2.10 范畴和函子的简介

Definition 2.31. 一个范畴$\mathscr{C}$指的是如下要素：

$C1$ 一类对象（$objects$）$O(\mathscr{C}), A\in\mathscr{C}(A\in O(\mathscr{C}))$

$C2$ 对$\mathscr{C}$中任意两个对象的有序对A,B对应于一个集合$Mor(A,B)$称之为从A到B的态射集

满足如下公理

$A1$ 对每个$A\in\mathscr{C}$，有一个特别的元素$1_A\in Mor(A,A)$

$A2$ 对任意的$A,B,C\in\mathscr{C}$

$$Mor_{\mathscr{C}}(A,B)\times Mor_{\mathscr{C}}(B,C)\longrightarrow Mor_{\mathscr{C}}(A,C)$$
$$(f,g)\longmapsto gof$$

且满足结合律

$A3$ 对任意的$f\in Mor_{\mathscr{C}}(A,B)$

$$A\xrightarrow{1_A}A\xrightarrow{f}B, fo1_A=f,$$
$$A\xrightarrow{f}B\xrightarrow{1_B}B, 1_Bof=f.$$

例1.集合范畴Set:

对象：集合,态射集：对任意的$A,B\in Set$;$Mor(A,B)=Map(A,B)$=$\{f:A\longrightarrow B$是一个映射$\}$

例2.群范畴G_P:

对象：群,态射集：$G,H\in G_P$,$Mor(G,H)=Hom(G,H)$.

例3.模范畴:

设A是一个含1交换环，$A-$模范畴$A-Mod$,对象：$A-Mod, M$,态射：A-同态,$M,N\in A-Mod$,$Mor_{A-Mod}(M.N)=Hom_A(M,N)$.

子范畴

Definition 2.32. 设$\mathscr{C}$是范畴，若$\mathscr{D}\in\mathscr{C}$,则 $ob(\mathscr{D})\subset ob(\mathscr{C})$,且对任意$A,B\in ob(\mathscr{D})$有$Mor_{\mathscr{D}}(A,B)\subset Mor_{\mathscr{C}}$.

完全子范畴

Definition 2.33. $\mathscr{D}\in\mathscr{C}$（子范畴）

如果对任意的$A,B\in\mathscr{D}$,都有$Mor_{\mathscr{D}}(A,B)=Mor_{\mathscr{C}}$则称$\mathscr{D}$是$\mathscr{C}$的完全子范畴.

例如：$G_P\leqslant Set$是子范畴，但不是完全子范畴.

函子

Definition 2.34. 设$\mathscr{C}$和$\mathscr{D}$是两个范畴，对应$F:\mathscr{C}\longrightarrow\mathscr{D}$,则对任意的$A\in\mathscr{C}$都有$F(A)\in\mathscr{D}$

对任意的$A,B\in\mathscr{C}$有

$$Mor_{\mathscr{C}}(A,B)\longrightarrow Mor_{\mathscr{D}}(F(A),F(B))$$

$$f\longmapsto F(f)$$

满足

$A1$:对任意的$A\in\mathscr{C}$，有$F(1_A)=1_{F(A)}$.

对任意的$A,B,C\in\mathscr{C},f\in Mor_{\mathscr{C}}(A,B),g\in Mor_{\mathscr{C}}(B,C),A\xrightarrow{f}B\xrightarrow{g}C$有

$$F(A)\xrightarrow{F(f)}F(B)\xrightarrow{F(g)}F(C).$$

即有

$$F(gof)=F(g)oF(f).$$

称上述F为$\mathscr{C}$到$\mathscr{D}$的共变函子.

对偶的，反变函子$F:\mathscr{C}\longrightarrow\mathscr{D}$,

$$F:Mor_{\mathscr{C}}(A,B)\longrightarrow Mor_{\mathscr{D}}(F(B),F(A))$$

$$f\longmapsto F(f)$$

对任意的$A,B,C\in\mathscr{C},f\in Mor_{\mathscr{C}}(A,B),g\in Mor_{\mathscr{C}}(B,C),A\xrightarrow{f}B\xrightarrow{g}C$有

$$F(A)\xleftarrow{F(f)}F(B)\xleftarrow{F(g)}F(C),$$

即有

$$F(gof)=F(f)oF(g).$$

函子的自然变换

Definition 2.35. 设F,G是范畴$\mathscr{C}$到$\mathscr{D}$的两个共变函子，如果对任意的$A\in\mathscr{C}$有

$$l_A\in Mor_{\mathscr{D}}(F(A),G(A)),l_B\in Mor_{\mathscr{D}}(F(B),G(B)).$$

其中$F(f)\in Mor_{\mathscr{D}}(F(A),F(B)),G(f)\in Mor_{\mathscr{D}}(G(A),G(B))$使得

$$l_BoF(f)=G(f)ol_A.$$

即下图交换

$$\begin{array}{ccc} F(A) & \xrightarrow{l_A} & G(A) \\ {\scriptstyle F(f)}\downarrow & & \downarrow{\scriptstyle G(f)} \\ F(B) & \xrightarrow{l_B} & G(B). \end{array}$$

特别的，如果l_A都是同构的（对任意的$A\in\mathscr{C}$），则F,G也是同构的.

范畴的同构与等价

如果存在函子$F:\mathscr{C}\longrightarrow\mathscr{D}$与$G:\mathscr{D}\longrightarrow\mathscr{C}$使得$GoF=1_{\mathscr{C}},FoG=1_{\mathscr{D}}$则称范畴$\mathscr{C}$与$\mathscr{D}$是**同构**的.

如果存在函子$F:\mathscr{C}\longrightarrow\mathscr{D}$与$G:\mathscr{D}\longrightarrow\mathscr{C}$使得$GoF\backsimeq 1_{\mathscr{C}},FoG\backsimeq 1_{\mathscr{D}}$则称范畴$\mathscr{C}$与$\mathscr{D}$是**等价**的.

$A-$**模范畴**(A是一个含1交换环)

对$M,N\in A-mod$,$A-$模同态是单的.$Mor_{A-mod}(M,N)\triangleq Hom_A(M,N)$.

对任意的$f,g\in Hom_A(M,N)$,定义$f+g\in Hom_A(M,N)$如下

$$(f+g)(x)\triangleq f(x)+g(x)(x\in M).$$

事实：$(Hom_A(M,N),+)$是一个Abel群.

现固定$M\in A-mod$,

记$F_M=Hom_A(M,-):\quad A-mod\longrightarrow\mathscr{A}b$(Abel群范畴）

$$N\longmapsto F_M(N)$$

其中$F_M(N)=Hom_A(M,-)(N)\triangleq Hom_A(M,N)$.

根据上述的关系，对于$N,L\in A-mod,F_M(N),F_M(L)\in\mathscr{A}b$我们有

$N\xrightarrow{f}L\qquad F_M(N)=Hom_A(M,N)\xrightarrow{F_M(f)}F_M(L)=Hom_A(M,L)$

对于$g:M\longrightarrow N,fog:M\longrightarrow L$有

$$F_M(f)(g)=Hom_A(M,f)(g)=f\circ g.$$

对于$h:M\longrightarrow N,N\xrightarrow{f}L\xrightarrow{g}K$有

$$F_M(g\circ f)=F_M(g)\circ F_M(f).$$

因为对任意的$h\in Hom_A(M,N)$,

$$F_M(g\circ f)(h)=g\circ f\circ h=g\circ(F_M(f)(h))=F_M(g)(F_M(f)(h))=F_M(g)\circ F_M(f)(h),$$

即$F_M(g\circ f)=F_M(g)\circ F_M(f)$.

共变函子

$$Hom_A(M,-):A-mod\longrightarrow\mathscr{A}b$$
$$N\longmapsto Hom_A(M,N)$$

反变函子

固定N,

$$G_N\triangleq Hom_A(-,N):A-mod\longrightarrow\mathscr{A}b$$
$$M\longmapsto Hom_A(M,N),$$

对于$L \xrightarrow{f} M$我们有

$$Hom_A(M,N) \xrightarrow{G_N(f)} Hom_A(L,N).$$

对于$L \xrightarrow{f} M \xrightarrow{g} N$,

$$Hom_A(-,N)(f) = G_N(f): \quad Hom_A(M,N) \longrightarrow Hom_A(L,N),$$
$$g \longmapsto gof,$$

即

$$G_N(f)(g) = gof, g \in Hom_A(M,N),$$

$$Hom_A(-,N)(f)(g) = gof,$$

即$Hom_A(-,N)$是一个反变函子.

A是一个合1交换环,$A-$模范畴,$A-Mod$.取$M \in A-$ Mod. 共变函子 $\mathrm{Hom}_A(M,-) \triangleq h_M$, 反变函子 $\mathrm{Hom}_A(-,N)$

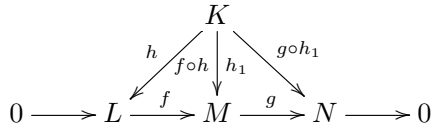
$A-$模的一个短正合列

$$0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0 \qquad (\star)$$

表示 $(i)f$单； $(ii)g$满；$(iii)Imf = kerg$.

任取$K \in A-\mathrm{mod}$用$h_K = \mathrm{Hom}_A(K,-)$作用$(\star)$。

我们有



$h_K(L) = \mathrm{Hom}_A(K,L)$

$$0 \to \mathrm{Hom}_A(K,L) \to \mathrm{Hom}_A(K,M) \to \mathrm{Hom}_A(K,N) \qquad (\star\star)$$

Proposition 2.13. *$(\star)$是一个正合列⇒$(\star\star)$是正合列.*

即

$$0 \to h_k(L) \xrightarrow{h_k(f)} h_k(M) \xrightarrow{h_k(g)} h_k(N)$$

是*Abel*群正合列。

证明. 先证$h_k(f)$是单射.

$\forall h \in h_k(L)$，使得$h_k(f)(h) = 0$,即$h_k(f)(h) = f \circ h = 0$。故对$\forall \alpha \in M$，有$f \circ h(\alpha) = 0 \Rightarrow f(h(\alpha)) = 0$。由于

$$0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$$

是正合的，故f单射. 于是$h(\alpha) = 0$. 由α的任意性得到$h = 0$.即$h_k(f)$ 是单射。

下证在$h_k(m)$处正合,即$Im\,(h_k(f)) = \ker\,(h_k(g))$.
由于$(\star)$正合,故有

$$\mathrm{g}\circ\mathrm{f} = 0 \;\Rightarrow gofoh = 0 \Rightarrow g\circ(foh) = 0.$$

$\therefore\,(h_k(g)\circ h_k(f))(h) = 0$.由$h$是任取的,$\Rightarrow h_k(y)\circ h_k(t) = 0, \therefore Im(h_k(f)) \subseteq (ker(h_k(g))$.

下证 $\ker\,(h_k(g)) \subset I_m\,(h_k(f))$.为此取 $h' \in \ker\,(h_k(g))$，则$h_k(g)\,(h') = goh' = 0$. 也即$\forall x \in K$，均有

$$g\circ h'(x) = 0 \Rightarrow g\circ h'(x) = 0 \Rightarrow h'(x) \in kerg.$$

$h'(x) \in M$, 由于$\mathrm{kerg} = Imf$,即有的$y \in L$,使得$h'(x) = f(y)$.

于是定义

$$h : k \to L$$

$$x \mapsto y$$

易验证$h \in h_k(L)$。

即$h' = f\circ h, \therefore h'(x) = f(y) = f\circ h(x) = f(h(x))$,且$h_k(f)(h) = f\circ h = h'$ 由此得到$h' \in Im(h_k(f)) \Rightarrow \ker\,h_k(g) \subset Im(h_k(f))$。

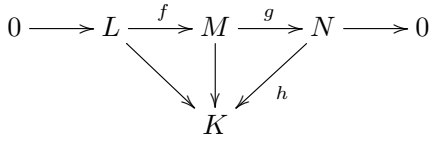
综上，$Kerh_k(g) = Im(h_k(t))$.

因此可由短正合列$(\star) \Rightarrow (\star\star)$是左正合的。 □

此时称$h_k = \mathrm{Hom}_A\,(k,\,)$呈一个左正合函子(不能像证右边正合)

$\mathrm{Hom}_A\,(\mathrm{M},\mathrm{J})$与$\mathrm{Hom}_A(-, M)$均呈左正合。

取$K \in A - Mod$,由



得到左正合列

$$0 \to \mathrm{Hom}_A(N,K) \to \mathrm{Hom}_A(M,K) \to \ \mathrm{Hom}\ _A(L,K).$$

2.11 模的张量积 外积 对称积

$M \xrightarrow{f} N$ A-线性(A-模同态)

向量空间 F/V (下域) V为节上的向量空间

$V \backsimeq R^n$ R实数欧式空间

内积 $\langle,\rangle$

$$V \times V \longrightarrow R$$

$$(\alpha,\beta) \mapsto \langle\alpha,\beta\rangle$$

1. $\langle a_1\alpha_1 + a_2\alpha_2, \beta\rangle = a_1\langle\alpha_1,\beta\rangle + a_2\langle d_2,\beta\rangle$;

2. $\langle \alpha, \quad b_1\beta_1 + b_2\beta_2 \rangle = b_1\langle \alpha, \beta_1 \rangle + b_2\langle \alpha, \beta_2 \rangle$

$\mathbb{R}$-双线性

固定α, $\langle \alpha, - \rangle$:

$$V \to \mathbb{R}$$

$$\beta \mapsto \langle \alpha, \beta \rangle$$

$m \times N \to L$ $\quad M \xrightarrow{f} N$ A线性

$(\alpha, \beta) \longmapsto f(\alpha, \beta)$

定义：设$M, N, L \in A - mod.$ A是含1交换环，称映射$f : M \times N \to L$为一个双线性映射，如果下述条件成立。

1. $f(a_1x_1 + a_2x_2, y) = a_1 f(x_1, y) + a_2 f(x_2, y)$

2. $f(x, b_1y_1 + b_2y_2) = b_1 f(x, y_1) + b_2 f(x_1y_2)$

$\forall a_1, a_2, b, b_2 \in A, \quad x_1, x_2 \in M, y_1, y_2 \in N$

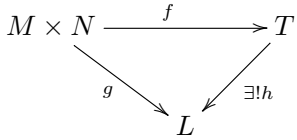
即f对每个分量都是$A-$线性的。

此处固空$x \in M$，则$f(x, -)$：$N \to L, y \longmapsto f(x, y)$是$A-$线性的。 $M \otimes N$

"双线性"作为一个属性，找一个最基本的.

Theorem 2.7. *设$M, N \in A - Mod$.(A是一个含1交换环)，则存在一个对(pairs)(T, f),其中$T \in A - Mod$。 $f : M \times N \xrightarrow{f} T$.是一个$A-$双线性的。使得如下"泛性质"满足。*

(泛性质)对$\forall L \in A - Mod$及双线性映射$g : M \times N \to L$, 则存在唯一一个A-线性映射$h : T \to L$, 使$g = h \circ f$.即下图交换



且上述满足泛性质的(T, f)在同构定义下唯一记$T \triangleq M \otimes_A N$. 称为$M$和$N$的张量积。

证明. 以$M \times N$中全体元素为基作一个自由$A-$模,记为$F \triangleq A^{(M \times N)} = \oplus_{\alpha \in M \times N} A$. 故$x \in F \Leftrightarrow x = \sum a_{m,n}(m, n)$,其中$a_{m,n} \in A$ 除有限个均为0.(表示法唯一)

在F中令F_0为有形式如下的元素生成的$A-$子模:

$$(m_1 + m_2, n) - (m_1, n) - (m_2, n),$$

$$(m, n_1 + n_2) - (m, n_1) - (m, n_2),$$

$$(am, n) - a(m, n), (m, bn) - b(m, n).$$

于是令$T = F/F_0$. 则T满足的双线性的"泛性质" □

记号：将上述构造的$T \triangleq M \otimes_A N$. $\quad M \times N \xrightarrow{f} M \otimes_A N$

$$(m.n) \mapsto (m, n)$$

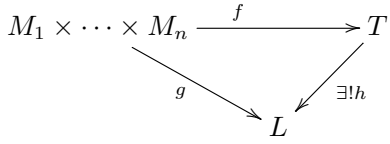
更一般的，任给$M_1, \cdots, M_n \in A - Mod$有$n-$重维映射。

$$f = M_1 \times \cdots \times M_n \to N$$

$$\begin{aligned} &f(\alpha_1, \cdots, \alpha_{i-1}, a_i \cdot \alpha_i + a_i' \alpha_i', \alpha_{i+1}, \cdots, \alpha_n) \\ &= a_i f(\alpha_1, \cdots, \alpha_i, \cdots, \alpha_n) + a_i' f(\alpha_1, \cdots, \alpha_i', \cdots, \alpha_n) \end{aligned}$$

即f对每个分量均是线性的(多重线性映射).

张量积对$M_1 \times \cdots \times M_n \xrightarrow{f \quad linear} T$，对$M_1 \times \cdots \times M_n \xrightarrow{g} L$都存在唯一的线性映射$h : T \longrightarrow L$，使得$g = hof$. 即有下面交换图



记$T = M_1 \otimes_A M_2 \otimes_A \cdots \otimes_A M_n$ 性质：

1. $M \otimes_A N = N \otimes_A N$;
2. $M \otimes_A A \simeq M$;
3. $(M \otimes_A N) \otimes_A L \simeq M \otimes_A (N \otimes_A L)$;
4. $M \otimes_A (N \oplus_A L) \simeq (M \otimes_A N) \oplus (M \otimes_A L)$.

例1. V, W分别是$\mathbb{R}$上的m, n维向量空间，则$dim_{\mathbb{R}}(W \otimes V) = mn$.
$v \xrightarrow{f} \mathbb{R}$
$\int : \mathscr{C}[a, b] \longrightarrow \mathbb{R}$($\mathscr{C}[a, b]$是[a,b]上的连续函数的全体)
$f \mapsto \int_{[a,b]} f = \int_a^b t dx$

对称.设$V, W \in A - Mod$,

$$V \times V \cdots \times V \xrightarrow{f} W$$
$$n\text{重}$$

若(1)f是n-重线性的. (2)$f(x_{\sigma(1)}, x_{\sigma(2)} \cdots x_{\sigma(n)}) = f(x_1 \cdots x_n)(\forall \sigma \in S_n)$. 则称$f$为$n$**重对称函数**.

外积.设$V, W \in A - Mod$

$$V \times V \cdots \times V \xrightarrow{f} W$$
$$n\text{重}$$

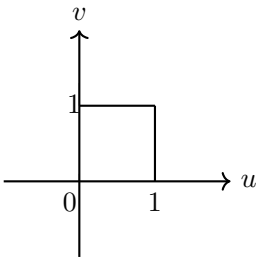
(1) f是n-重线性映射。

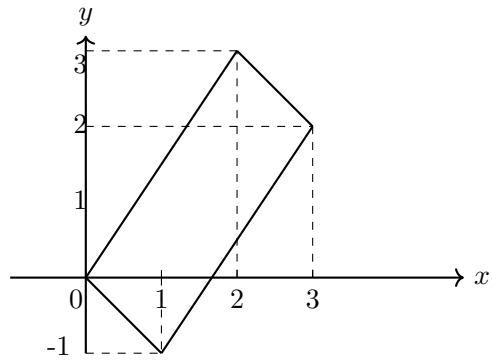
(2) f是交错的。$f(x_{\sigma(1)}, x_{\sigma(2)} \cdots x_{\sigma(n)}) = \operatorname{sgn}(\sigma) \cdot f(x_1 \cdot x_n)$. 其中$\sigma \in S_n$($n$次对称群)

$$\operatorname{sgn}(\sigma) = \begin{cases} 1 & \text{当}\sigma\text{是偶置换,} \\ -1 & \text{当}\sigma\text{是奇置换.} \end{cases}$$

外积：$\phi : V \times V \times \cdots \times V \xrightarrow{\phi} \wedge^n V = V \wedge V \wedge \cdots \wedge V$是一$n$重交错线性映射，若对任意$V \times V \times \cdots \times V \xrightarrow{f} W$存在唯一的$g : \wedge^n V \longrightarrow W$使得$f = g \circ \phi$ 则称$\wedge^n V$为V的n次外积。

例1





$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ -1 & 3 \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix}$$

$$\therefore \begin{cases} x = u + 2v & dx = du + 2dv \\ y = -u + 3v & dy = -du + 3dv \end{cases}$$

$$\begin{aligned} S(\Delta) &= \iint_{\Delta} dxdy \\ &= \iint_{\Delta} (du + 2dv) \wedge (-du + 3dv) \\ &= \iint_{\Delta} (3 + 2) du \wedge dv \\ &= 5 \iint_{\Delta} dudv = 5 \end{aligned}$$

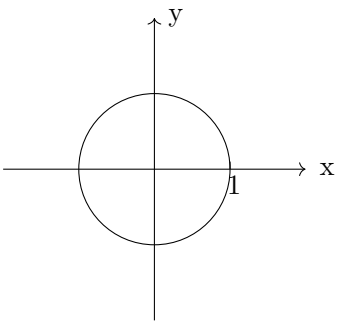
$du \wedge du = -du \wedge du$
$\Rightarrow du \wedge du = 0$

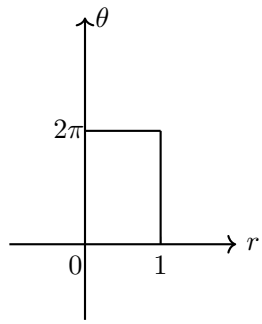
另一种方法求面积

$$\left\| \begin{matrix} 1 & 2 \\ -1 & 3 \end{matrix} \right\| = |5| = 5 \qquad J = \left| \frac{\partial(x,y)}{\partial(u,v)} \right| = \begin{vmatrix} 1 & 2 \\ -1 & 3 \end{vmatrix} = 5$$

$$-\iint_{\Delta} dxdy = \iint_{D} J dudv = 5 \iint_{D} dudv = 5.$$

例2.计算区域$D, 0 \le r \le 1, 0 \le \theta \le 2\pi$的面积。





$D: x^2+y^2 \le 1$ $\Delta: 0 \le r \le 1, 0 \le \theta \le 2\pi$

解:进行坐标变换$\begin{cases} x = r\cos\theta & 0 \le \theta \le 2\pi \\ y = r\sin\theta & 0 \le r \le 1 \end{cases}$,于是

$$\begin{aligned} S(\Delta) &= \iint_{\Delta} dxdy = \iint_{D} d(r\cos\theta) \wedge d(r\sin\theta) \\ &= \iint_{D} (\cos\theta dr - r\sin\theta d\theta) \wedge (\sin\theta dr + r\cos\theta d\theta) \\ &= \iint_{D} r\cos\theta^2 dr d\theta - r\sin^2\theta d\theta dr \\ &= \iint_{D} r(\cos\theta^2 + \sin^2\theta) dr d\theta \\ &= \iint_{D} r dr d\theta \\ &= \int_0^{2\pi} d\theta \int_0^1 r dr = 2\pi \cdot \frac{1}{2} = \pi \end{aligned}$$

一般地，设D是$\mathbb{R}^n$中区域，$x_1, x_2, \cdots, x_n$是D上坐标，进行坐标变换$\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ $A \in M_n(\mathbb{R}), y_i = a_{i1}x_1 + \cdots + a_{in}x_n, (1 \le i \le n)$，得到$\mathbb{R}^n$中区域$D'$,则

$$\begin{aligned} vol(D') &= \int \cdots \int_{D'} dy_1 \wedge \cdots \wedge dy_n \\ &= \int \cdots \int_{D} d(a_{11}x_1 + \cdots a_{1n}x_n) \wedge \cdots \wedge d(a_{n1}x_1 + \cdots + a_{nn}x_n) \\ &= |A| \int \cdots \int_{D} dx_1 \wedge dx_2 \wedge \cdots \wedge dx_n \end{aligned}$$

$|A| = J = \left|\frac{\partial(y_1 \cdots y_n)}{\partial(x_1 \cdots x_n)}\right|$.

2.12 分式模

A环(交换环)
S是A的乘法封闭子集$S \subset A$,

$$S^{-1}A = \left\{ \frac{a}{s} | a \in A, s \in S \right\}.$$

设$M \in A - Mod$，分式模为

$$S^{-1}M = \left\{ \frac{x}{s} | x \in M, s \in S' \right\}.$$

$\frac{x_1}{s_1} = \frac{x_2}{s_2} \Leftrightarrow \exists t \in S$使得$t(s_2x_1 - s_1x_2) = 0.$
有自然映射

$$A \to S^{-1}A$$
$$a \mapsto \frac{a}{1}$$

这样$S^{-1}A$可看成一个$A - Mod.$
由定义，$\frac{x_1}{s_1} \sim \frac{x_2}{s_2}(x_1, x_2 \in M, s_1, s_2 \in S^{-1} \Leftrightarrow \exists t \in S$使得$t(s_2x_1 - s_1x_2) = 0$。易知“$\sim$”是$S \times M$中的一个等价关系. $\frac{x}{s}$即为$(s, x) \in S \times M$关于“$\sim$”的等价类.
定义$S^{-1}M$中加法为 “+”: $\frac{x_1}{s_1} + \frac{x_2}{s_2} \triangleq \frac{s_2x_1 + s_1x_2}{s_1s_2}$.
数乘($S^{-1}A$对$S^{-1}M$的作用):

$$S^{-1}A \times S^{-1}M \to S^{-1}M$$
$$\left(\frac{a}{s}, \frac{x}{t}\right) \mapsto \frac{a}{s}\frac{x}{t} \triangleq \frac{ax}{st} \quad (\forall a \in A, s, t \in S, x \in M)$$

$\therefore S^{-1}M \in S^{-1}A - Mod.$
即上述构造所得$S^{-1}M$是一个$S^{-1}A$-模，称为M关于S的**分式模**。
事实：设A, B是交换环,$f : A \to B$是一个环同态
则：$\begin{array}{l} A \times B \to B \\ (a, b) \mapsto a \star b \end{array}$ (注：若A, B是非交换环，则$f(A) \subset C(B)$)
其中$a \star b \triangleq f(a) \cdot b.$ 于是易验证$(B, +, \star)$是一个$A-$模，此时也称B为一个$A-$代数.
若B与C为$A-$代数，则可定义

$$B \bigotimes_A C$$
$$(b_1 \bigotimes c_1)(b_2 \bigotimes c_2) = (b_1b_2) \bigotimes (c_1c_2)$$
$$\Rightarrow B \bigotimes_A C \text{也是一个} A - \text{代数.}$$

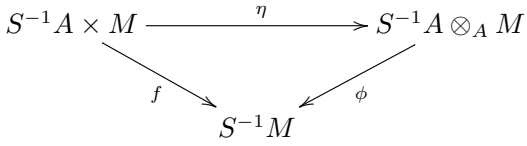
Theorem 2.8. 设A是含1交换环，S是A的一个乘法封闭子集，$M \in A - Mod$,则

$$S^{-1}A \otimes_A M \cong S^{-1}M.$$

证明. 首先，令

$$f : S^{-1}A \times M \to S^{-1}M$$
$$\left(\frac{a}{s}, x\right) \mapsto \frac{ax}{s} \in M.$$

$\because M \in A-Mod, f(\frac{a}{s}, x_1) \triangleq \frac{ax}{s} (\forall \frac{a}{s} \in S^{-1}A, x \in M)$. 易验证，$f$是$A-$双线性映射，从而由张量积的泛性质: $\exists!$的$A-$线性映射$\phi = S^{-1}A \otimes_A M \to S^{-1}M$, 使得$f = \phi \circ \eta$,即下图交换



$$\phi : S^{-1}A \otimes_A M \to S^{-1}M$$
$$\frac{a}{s} \otimes_A x \mapsto \frac{ax}{s}$$

下证ϕ是一个同构。

由于$\forall s \in S, x \in M$,有$\frac{x}{s} = f(\frac{1}{s} \otimes x)$,从而$\phi$是满射。

下证ϕ是一个单射。为此，任取$\alpha \in S^{-1}M$有$\alpha = \sum_{i=1}^{n} \frac{a_i}{s_i} \otimes x_i$,其中$a_i \in A, s_i \in S, x_i \in M, (i-1, \cdots, n)$。令$s = s_1 \cdots s_n$, $s' = \frac{s}{s_i}$,

$$\begin{aligned}
\alpha = \sum_{i=1}^{n} \frac{a_i}{s_i} \otimes x_i &= \sum_{i=1}^{n} \frac{a_i s'}{s} \otimes x_i = \sum_{i=1}^{n} \frac{1}{s} \times (a_i s' x_i) \\
&= \frac{1}{s} \sum_{i=1}^{n} 1 \otimes (a_i s' x_i) \\
&= \frac{1}{s} \left(1 \otimes \sum_{i=1}^{n} (a_i s' x_i) \right) \\
&= \frac{1}{s}(1 \otimes x) \qquad \text{其中} x = \sum_{i=1}^{n} a_i s' x_i \\
&= \frac{1}{s} \otimes x.
\end{aligned}$$

$$\begin{aligned}
\therefore \alpha = \frac{1}{s} \otimes x \in Ker\theta &\Leftrightarrow 0 = \phi(\alpha) = \phi(\frac{1}{s} \otimes x) = \frac{x}{s} = 0 \\
&\Leftrightarrow \exists t \in S, \text{使得} t(x \cdot 1 - s \cdot 0) = tx = 0
\end{aligned}$$

故

$$\begin{aligned}
\alpha = \frac{1}{s} \otimes x &= \frac{t}{st} \otimes x \\
&= \frac{1}{st} \otimes tx = \frac{1}{st} \otimes 0 = 0
\end{aligned}$$

$\Rightarrow ker\phi = 0 . \because \phi$是单的。从而$\phi$呈同构。 □

上述构造所得$S^{-1}M$是一个$S^{-1}A$-模，称为M关于S的分式模.

Jordan-Holder定理

Definition 2.36. 设$M \in A-mod$, 如果有序列

$$M = M_0 \subsetneqq M_1 \subsetneqq M_2 \cdots \subsetneqq M_n = 0(\star)$$

其中$M_i \leq M(i = 0, 1, 2 \cdots n)$, 且$M_i/M_{i+1}$均是单$-A$模$(i = 0, 1, \cdots, n-1)$，则称$(\star)$为一个合成列*(comprosition serise)*. M_i/M_{i+1}称为M的合成因子，其中n标为M的长度*(length)*记为$l(M) = n$.

Theorem 2.9. *(Jordan-Holder)* 设$M \in A - Mod$，如果M有合成列，则M的所有h合成列都有相同的长度，且他们的合成因子在相差一个置换下的对应互相同构。

把合成因子M_i/M_{i+1}作直和$M' = \bigoplus_{i=1}^{n} M_i/M_{i+1}$,当$M$不是半单时，可由$M'$去找合成列。

3 域论

3.1 域的代数扩张

域$F, (F, +, \cdot), u(F) = F^* = F/0$,子域$F_i \leqslant F$其中$i \in I$,$\cap F_i \leqslant F$.

证明：由于$0, 1 \in F_i, \forall i \in I, \Rightarrow 0, 1 \in \bigcap_{i\in I} F_i$.

而$\forall a, b \in F_i, i \in I, \Rightarrow a + b \in F_i, \forall i \in I \Rightarrow a + b \in \bigcap_{i\in I} F_i$

$$ab \in F_i, \forall i \in I \Rightarrow ab \in \bigcap_{i\in I} F_i$$

$\bigcap_{i\in I} F_i \leqslant F$是$F$的子域。

$\alpha \in F$,则$\alpha^2, \alpha^3 \ldots \alpha^n \in F\ (\forall n \in N)$, $a_0 \cdot 1 + a_1 \cdot \alpha + 1 + a_n\alpha^n \in F$. 令$f(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n \in F$，即$\alpha \in F, f(\alpha) \in F$.

若$g(x) \in F[x], g(\alpha) \neq 0$，则$\dfrac{f(\alpha)}{g(\alpha)} \in F$

F是域，F上的关于x的多项式环$F[x]$， F上的关于x的有理分式域$F(x)$，如$\mathbb{R}(x)$，$\mathbb{C}(x)$

一般地，F上关于$x_1 \cdots x_n$的多项式环为$F[x_1 \cdots x_n]$;F上关于$x_1 \cdots x_n$的有理分式域$F(x_1 \cdots x_n)$.

固定一个域k，任取k的一个子域F，任取$\alpha \in k$. 问题：k中包含F与α的最小子域是？

答案：$F(\alpha) = \{h(\alpha) \mid h \in F(x) \mid h(\alpha) \text{ 有意义 }\} = \left\{ \dfrac{f(\alpha)}{g(\alpha)} \middle| f, g \in F[x] \text{ 且 } g(\alpha) \neq 0 \right\}$

$F(\alpha) \triangleq \bigcap_{\substack{E\in k \\ E\supset FU(\alpha)}} E$，称$F(\alpha)$为$F$添加$k$中元$\alpha$生成的子域。

同理，

$$\begin{aligned} F(\alpha_1, \alpha_2) &= \{h(\alpha_1, \alpha_2) \mid h \in F(x_1, x_2), h(\alpha_1, \alpha_2) \text{ 有意义 }\} \\ &= \left\{ \frac{f(\alpha_1, \alpha_2)}{g(\alpha_1, \alpha_2)} \mid f, g \in F[x_1, x_2] \text{ 且 } g(\alpha_1, \alpha_2) \neq 0 \right\} \end{aligned}$$

对于$\alpha_1 \cdots \alpha_n \in k$

$$F(\alpha_1 \cdots \alpha_n) = \left\{ \frac{f(\alpha_1 \cdots \alpha_n)}{g(\alpha_1 \cdots \alpha_n)} \middle| f, g \in F[x_1 \cdots x_n] \text{ 且 } g(\alpha_1 \cdots \alpha_n) \neq 0 \right\}$$

设$F \leqslant k$子域，$S' \subset k$子集，$S \neq \varnothing$，$F(S)$为k中既包含F又包含S'的最小子域，

$$F(S) = \left\{ \frac{f(\alpha_1 \cdots \alpha_n)}{g(\alpha_1 \cdots \alpha_n)} \middle| n \in N, \alpha_1 \cdots \alpha_n \in S, f, g \in F[\alpha_1 \cdots \alpha_n], g(\alpha_1 \cdots \alpha_n) \neq 0 \right\}$$

每个元素都可只加S中的有限个元即可得到。

固定k域，$F_1, F_2 \leq k$是k的两个子域. 问：k中既包含F_1又包含F_2的最小子域是？

答：$F_1(F_2) = F_2(F_1) \triangleq F_1F_2$称之为$F_1$与$F_2$的合成（域）。

类似地，对于k的子域F_i $(i = 1, \cdots, n)$，F_i的合成记为$F_1 \cdots F_n$代数扩张。

域扩张：设F, k是域，如果$F \subset k$，则知F为k的子域，k是F的一个扩域，则k可作为F模$\Rightarrow k$可作为F向量空间。

此时，k是F上一个向量空间，$F \times k \longrightarrow k$，$(a, b) \longmapsto ab$

Definition 3.1. 设k/F是一个域扩张$(F \subset k)$，称$\dim_F^k$为其扩张次数，记之为$[k : F] \triangleq \dim_F^k$

当$[k : F] = n < +\infty$时，称k/F为一个n次扩张。

当$[k : F] = +\infty$时，称k/F为一个无限扩张。

Definition 3.2. 设k/F是一个域扩张，$\alpha \in k$，如果有$f(x) \in F[x] \mid \{0\}$，使得$f(\alpha) = 0$，则称α在F上代数，也称α是一个F代数元。

若这样的非零多项式不存在，则称α是F上的数据元。

此时，$f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in F[x] \mid \{0\}$，$a_0, \cdots, a_n \in F$，$n = \deg f, a_n \neq 0$，且显然$n > 0$。

Definition 3.3. 设k/F是一个域扩张，如果k中任一元素均是下一代数元，则称k/F是一个代数扩张。

Theorem 3.1. 域的有限扩张均是代数扩张，即对于域扩张k/F，如果$[k : F] < +\infty$，则k/F是一个代数扩张。

证明. 设$[k : F] = n < +\infty, \forall \alpha \in k$（只需证$\alpha$是$F$一代数元即可）

则$1, \alpha_1, \cdots, \alpha_n$是$F$一线性相关的（$\because \dim_F^k = n$）

$\therefore$存在不全为0的$a_0 \cdots a_n \in F$，使得

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$$

令$f(x) = 1 + a_1x + \cdots + a_nx^n \in F[x] \mid \{0\}$，且$f(\alpha) = 0$

$\therefore \alpha$是F一代微元，

$\therefore k/F$是代数扩张。 □

Theorem 3.2. 设域$F \subset E \subset k$，如果E/F，k/E都是有限扩张，则k/F是有限扩张，且$[k : F] = [k : E][E : F]$

证明. 设$[E:F]=m,[k:E]=n$，则$\dim_F^F=m$，$\dim_E^k=n$. 取$\{x_1,\cdots,x_m\}$是E上的一组F-基; $\{y_1,\cdots,y_n\}$是k上的一组E-基.

下证$\{x_iy_j\}_{\substack{1\leqslant i\leqslant m\\1\leqslant j\leqslant n}}$是$k$的一组$F$-基.

$\forall\alpha\in k$，有$\alpha=\sum\limits_{j=1}^{n}x_jy_j$，其中$b_j\in E$，而$\forall b_j\in E$，有$b_j=\sum\limits_{i=1}^{m}a_{ij}x_i$，其中$a_{ij}\in F$

$$\Rightarrow\alpha=\sum_{j=1}^{n}b_jy_j=\sum_{j=1}^{n}\left(\sum_{i=1}^{m}a_{ij}x_i\right)y_j$$
$$=\sum_{j=1}^{n}\sum_{i=1}^{m}a_{ij}x_iy_j.$$

$\therefore k$中任一元素都可用$\{x_iy_j\}_{\substack{1\leqslant i\leqslant m\\1\leqslant j\leqslant n}}$ F-线性表出

设

$$\sum_{i=1}^{m}\sum_{j=1}^{n}a_{ij}x_iy_j=0,a_{ij}\in F,$$

则

$$\sum_{j=1}^{n}\left(\sum_{i=1}^{m}a_{ij}x_i\right)y_j=0.$$

由于$\sum\limits_{i=1}^{m}a_{ij}^{\in F}x_i^{\in E}\in E$，由$\{y_1,\cdots,y_n\}$线性无关$\Rightarrow\sum\limits_{i=1}^{m}a_{ij}x_i=0(\forall j)$，由于$a_{ij}\in F$，$\{y=x_1,\cdots,x_m\}$是$E$上关于$F$的一组基$\Rightarrow a_{ij=0}$,于是$a_{ij=0}(i=1,\cdots,m,1\leqslant j\leqslant n)$.

从而$\{x_iy_j\}_{\substack{1\leqslant i\leqslant m\\1\leqslant j\leqslant n}}$是一组$k$的$F$-基. 且有$[k:F]=[k:E][E:F]=mn$. □

同理设域扩张$F=F_0\subset F_1\subset\cdots\subset F_n$，则

$$[F_n:F]=[F_n:F_{n-1}][F_{n-1}:F_{n-2}]\cdots[F_1:F]$$

Theorem 3.3. *(单代数扩张结构定理）设k/F是一个域扩张，$\alpha\in k$且α是F-代数元，则$F(\alpha)=F[\alpha]$且$[F(\alpha):F]=n<+\infty$。特别地，$F(\alpha)/F$是代数扩张，其中n为α在F上极小多项式的次数。*

3.2 代数扩张与单代数扩张结构

域的特征：F域,有整数环到F的自然嵌入

$$\phi:\mathbb{Z}\to F$$
$$1\mapsto 1_F$$

则$\ker\phi=<n>$, $n\in\mathbb{Z}\geqslant 0$.于是 $Z/\ker\phi\hookrightarrow F$子域$\Rightarrow$ $\ker\phi$ 是$\mathbb{Z}$中极大理想，或0。

域F的特征，若$\mathrm{ch}(F)=0$,则$\mathbb{Z}\subset F$，又域有逆元，$\mathbb{Q}\subset F$，即$\mathbb{Q}$是F的最小子域(或称素子域)

若$\mathrm{ch}(F)=p$（素数），此时$F_p=\mathbb{Z}/p\mathbb{Z}\subset F$，即$F_p$为$F$的素子域。

Theorem 3.4. *(域的单代数扩张结构):设k/F是一个域扩张，$\alpha\in k$，记$E=F(\alpha)$*

(1) 存在F上唯一一个首 *1* 不可约多项式$P_\alpha(x)\in F[x]$，使得$P_\alpha(x)=0$，记$n=\deg P_\alpha(x)$

(2) $E=F(\alpha)=F[x]$且$\{1,\alpha,\alpha^2,\cdots,\alpha^{n-1}\}$是$E$的一组$F$-基，特别地，$[F(\alpha):F]=\deg P_\alpha(x)$，称上述$P_\alpha(x)$为$\alpha$在$F$上的极小多项式（书上记之为$P_\alpha(x)=I_{rr}(\alpha,F,x)$）

先给出一个引理及证明，利用引理去证明定理 1。

Lemma 3.1. 设α，k/F如上述定理，记$I=\{f(x)\in F[x]\mid f(\alpha)=0\}$，则$I=\langle P_\alpha(x)\rangle$是一个素理想，其中$P_\alpha(x)\in F[x]$是$F$上一个首 *1* 的不可约多项式。

证明. 令

$$\begin{aligned}\phi: F[x]&\longmapsto k\\ f(x)&\longmapsto f(\alpha)\end{aligned}$$

则ϕ是环同态，且$\ker\phi=\{f\in F[x]\mid f(\alpha)=0\}=I$

于是由环同态基本定理，有

$$F[x]/I\backsimeq Im(\phi)\leqslant k\text{ 子环}$$

因为k是域，故$F[x]/I$是整环$\Rightarrow$ I是素理想。

又$F[x]$是一个PID，由于α是F-代数元，故$\exists\ f\in F[x]-\{0\}$，使得$f(\alpha)=0$，即$I\neq 0\Rightarrow I$是极大理想。

从而I是由一个不可约多项式生成(把首项系数化为 1，得到的理想也相同)记为$P_\alpha(x)$，即$I=\langle P_\alpha(x)\rangle$ □

定理的证明

证明. （1）由上述引理即得

（2）设$P_\alpha(x)$为（1）中所给的α在F上的极小多项式，$n=\deg P_\alpha(x)$，于是可设$P_\alpha(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in F[x]$

下证$F(x)=F[\alpha]$.

为此，任取$\beta\in F(\alpha)$，则$\beta=\dfrac{f(\alpha)}{g(\alpha)},f,g\in F[x]$，且$g(\alpha)\neq 0$. 由极小多项式的性质，$P_\alpha(x)\nmid g(x)$. 又$P_\alpha(x)$不可约，则$(P_\alpha(x),g(x))=1$，又$F[x]$是PID，$\therefore$有$u(x),v(x)\in F[x]$，使得

$$\begin{aligned}&u(x)P_\alpha(x)+v(x)g(x)=1\\ \Rightarrow\ &u(\alpha)P_\alpha(\alpha)+v(\alpha)g(\alpha)=1\\ \Rightarrow\ &v(\alpha)g(\alpha)=1\\ \Rightarrow\ &\frac{1}{g(\alpha)}=u(\alpha)\\ \Rightarrow\ &\beta=\frac{f(\alpha)}{g(\alpha)}=f(\alpha)\cdot v(\alpha)\in F[\alpha]\\ \Rightarrow\ &F(\alpha)\subset F[\alpha]\end{aligned}$$

显然$\Rightarrow F(\alpha)\supset F[\alpha]\Rightarrow F(\alpha)=F[\alpha]$.

下证$\{1,\alpha,\cdots,\alpha^{n-1}\}$是$E$的一组$F$-基.

由带余除法有$f(x)=g(x)P_\alpha(x)+r(x)$，其中$g(x)\cdot r(x)\in F[x]$，且$r(x)=0$或$\deg r(x)<\deg P_\alpha(x)=n$

于是

$$\beta=f(\alpha)=gf(\alpha)P_\alpha(\alpha)+r(\alpha)=r(\alpha)\in F+F\alpha+\cdots+F\alpha^{n-1}$$

即β可由$\{1,\alpha,\cdots,\alpha^{n-1}\}$的$F$-线性表述。

下证$\{1,\alpha,\cdots,\alpha^{n-1}\}$线性无关。

设$b_0+b_1\alpha+\cdots+b_{n-1}\alpha^{n-1}=0$，其中$b_0,\cdots,b_{n-1}\in F$. 令$g(x)=b_0+b_1x+\cdots+b_{n-1}x^{n-1}\in F[x]$, 则$g(\alpha)=0$，从而$P_\alpha(x)\mid g(x)$. 由于$\deg g(x)=n-1<\deg P_\alpha(x)$

$$\Rightarrow g(x)=0\Rightarrow b_0=b_1=\cdots=b_{n-1}=0,$$

从而$\{1,\alpha,\cdots,\alpha^{n-1}\}$是线性无关的。

综上，$\{1,\alpha,\cdots,\alpha^{n-1}\}$是$E$的一组$F$-基。 □

Definition 3.4. 设k/F是一个域扩张，如果有$\alpha_1,\cdots,\alpha_n\in k$，使得$k=F(\alpha_1,\cdots,\alpha_n)$，则称$k$是$F$的一个有限生成扩域，或称$k/F$是一个有限生成扩张。

证明. “$\Longleftarrow$” $k=F(\alpha_1,\cdots,\alpha_n)=F[\alpha_1,\cdots,\alpha_n]$，其中$\alpha_1,\cdots,\alpha_n\in k$都是$F$-代数元

$$k=F[\alpha_1,\cdots,\alpha_{n-1}][\alpha_n],F[\alpha_1,\cdots,\alpha_{n-1}]=F[\alpha_1,\cdots,\alpha_{n-2}][\alpha_{n-1}]$$

$$\cdots$$

$$\begin{aligned}\Rightarrow\ [k:F]&=[k:F[\alpha_1,\cdots,\alpha_{n-1}]]\\&=[F[\alpha_1,\cdots,\alpha_{n-1}]:F[\alpha_1,\cdots,\alpha_{n-2}]]\cdots[F[\alpha_2,\alpha_1]:F[\alpha_1]]\\&<+\infty.\end{aligned}$$

“$\Longrightarrow$” 由于$[k:F]=n<+\infty$，故k作为F的向量空间有一组基. 设$\alpha_1,\cdots,\alpha_n$为k的一组F-基

于是

$$k=F\alpha_1+F\alpha_2+\cdots+F\alpha_n\subset F[\alpha_1,\cdots,\alpha_n]\subset k(\Leftarrow\because\alpha_1,\cdots,\alpha_n\in k,F\subset k)$$

即$k=F[\alpha_1,\cdots,\alpha_n]$. 从而$k$是$F$上一个有限生成的代数扩张。 □

Example 3.1. $F=Q\left(\sqrt[3]{2}\right)=Q\left(\sqrt[3]{2}\right)$, $\alpha=\dfrac{1}{2-\sqrt[3]{2}+\sqrt[3]{4}}\in F$，找$f(x)\in Q[x]$，使得$\alpha=f\left(\sqrt[3]{2}\right)$

解： $\sqrt[3]{2}$在Q中的极小多项式为$P(x)=x^3-2$，不可约的

而令$g(x)=x^2-x+2$，则$g\left(\sqrt[3]{2}\right)=\sqrt[3]{4}-\sqrt[3]{2}+2$，即$\alpha=\dfrac{1}{g\left(\sqrt[3]{2}\right)}$

对$P(x)$与$g(x)$作辗转粗除法

$$\begin{aligned}
P(x)=x^3-2&=(x+1)\left(x^2-x+2\right)-x-4\\
g(x)&=(-x-4)(-x+5)+22\\
\Rightarrow 22&=g(x)+(x+4)(-x+5)\\
&=g(x)+[(x+1)g(x)-P(x)](-x+5)\\
&=g(x)+\left(-x^2+4x+5\right)g(x)-P(x)(-x+5)\\
&=\left(-x^2+4x+6\right)g(x)-P(x)(-x+5)\\
\Rightarrow 22&=\left(-\sqrt[3]{4}+4\sqrt[3]{2}+6\right)g(\sqrt[3]{2})-P(\sqrt[3]{2})(-\sqrt[3]{2}+5)\\
&=\left(-\sqrt[3]{4}+4\sqrt[3]{2}+6\right)g(\sqrt[3]{2})\\
\Rightarrow \alpha&=\frac{1}{g\left(\sqrt[3]{2}\right)}=\frac{1}{22}\left(-\sqrt[3]{4}+4\sqrt[3]{2}+6\right)
\end{aligned}$$

$\therefore$取$f(x)=\dfrac{1}{22}\left(-x^2+4x+6\right)$即可得到$\alpha=f\left(\sqrt[3]{2}\right)$ □

Proposition 3.1. 设有域扩张$F\subset E\subset k$，则k/F是代数扩张$\Longleftrightarrow$ E/F, k/E都是代数扩张。

证明. “$\Longrightarrow$” 若k/F是代数扩张，则$\forall\ \alpha\in k$，α在F上代数，则自然在E上也代数，$\therefore$ k/E是代数扩张。由于$\forall\ \alpha\in E$，自然$\alpha\in k$，由于k/F是代数扩张，则α在F上的代数元，则E/F是代数扩张。

$\Longleftarrow$” 任取$\alpha\in k$，下证α是F-代数元。

由于k/E是代数扩张，则α是E-代数元，则有

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in E[x]\mid\{0\}$$

使得$f(\alpha)=0$。

令

$$E_1=F\left[a_0,\cdots,a_n\right]=F\left(a_0,\cdots,a_n\right),$$

则$f(x)\in E_1[x]$且α在E_1代数。由于$a_0,\cdots,a_n\in E$，又E/F是代数扩张，则$a_0,\cdots,a_n$在F上代数。则$E_1=F\left[a_0,\cdots,a_n\right]/F$是一个有限扩张.

综上，$\left[E_1(\alpha):F\right]=\left[E_1(\alpha):E_1\right]\left[E_1:F\right]<+\infty$. 从而$E_1(\alpha)/F$是代数扩张 .

$\therefore$ α在F上代数，由α的任一性, $\Rightarrow$ k/F是代数扩张 . □

3.3 代数闭包(1)

$\alpha \in k$ 域扩张

$|$ $f(x) \in F[x]$，使得$f(\alpha)=0$, $\tau|F=\sigma$

F

τ为σ延拓

σ为τ在F上的限制

设$f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0 \in F[x]$， $0=f(\alpha)=\alpha^n+a_{n-1}\alpha^{n-1}+\cdots+a_1\alpha+a_0$

$$\begin{aligned}0=\tau(0)=\tau(f(\alpha))&=\tau\left(\alpha^n+a_{n-1}\alpha^{n-1}+\cdots+a_1\alpha+a_0\right)\\&=\tau(\alpha)^n+\tau(a_{n-1})\tau(\alpha)^{n-1}+\cdots+\tau(a_1)\tau(\alpha)+\tau(a_0)\\&=\tau(\alpha)^n+\sigma(a_{n-1})\tau(\alpha)^{n-1}+\cdots+\sigma(a_1)\tau(\alpha)+\sigma(a_0)\end{aligned}$$

即

$$\tau(\alpha)^n+\sigma(a_{n-1})\tau(\alpha)^{n-1}+\cdots+\sigma(a_1)\tau(\alpha)+\sigma(a_0)=0.$$

令

$$g(x)=x^n+\sigma(a_{n-1})x^{n-1}+\cdots+\sigma(a_1)x+\sigma(a_0),$$

即$g(\tau(\alpha))=0$，即$\tau(\alpha)$是$g(x)$的一个根. 常记$g(x) \triangleq f^\sigma(x)$ $f^0(\tau(\sigma))=0$,$f^\tau(\tau(\sigma))=0$.

Definition 3.5. 设k/F是一个域扩张，L是一域，$\sigma:\ F \longrightarrow L$与$\tau:\ k \longrightarrow L$均是域同态，如果$\tau|F=\sigma$，则称$\tau$是$\sigma$在$k$上的拓展或$\sigma$是$\tau$在$F$上的限制。

特别地，当$F \subset L$，且σ是恒等嵌入（即$\sigma(\alpha)=\alpha\ \forall\ \alpha \in F$）时，如果$\tau|F=\sigma$，则称$\tau$是$k$到$L$的一个$F$-嵌入。

设$K \xrightarrow{\tau} L, K \longrightarrow F, F \xrightarrow{id} L$

τ是k到L的一个F-嵌入，$\alpha \in k$且是一个F-代数元，则$\tau(\alpha)$也是F-代数元($\because f^\tau(x)=f^\sigma(x)=f(x)$，从而$\alpha$与$\tau(\alpha)$的极小多项式是相同的，故都是$F$-代数元)。

Lemma 3.2. 设k/F是一个代数扩张，$\sigma: k \longrightarrow k$是一个$F$-嵌入，则$\sigma$是$k$上的一个自同构。

证明. ：由于域嵌入必是单的，故只须让σ是一个满射即可.

为此，任取$\alpha \in k$（找到α的原像）, 由k/F是代数扩张，则设α在F上的极小多项式$P_\alpha(x) \in F[x]$. 令

$$S=\{\beta \in k \mid P_\alpha(\beta)=0\},$$

则$\alpha \in S$. 又令$E=F(S)=F[S]$, 则k/F是一个有限扩张. 任取$\beta \in S$，有$P_\alpha(\beta)=0$. 于是$\sigma(P_\alpha(\beta))=0$，即$P_\alpha(\sigma(\beta))=0$.

$$\Rightarrow \sigma(\beta) \in S \Rightarrow \sigma(S) \subset S$$

$\sigma(E) \subset E$（下证事实上$\sigma(E)=E$，只需证维数相等）.

设$r_1, r_2, \cdots, r_n$是E的一组F-基, 则$\sigma(r_1), \cdots, \sigma(r_n) \in \sigma(E)$.下证它是$\sigma(E)$的一组$F$-基.

设

$$a_1\sigma(r_1)+\cdots+a_n\sigma(r_n)=0,$$

其中$a_1,\cdots,a_n\in F$, 则

$$\sigma\left(a_1r_1+\cdots+a_nr_n\right)=0.$$

由于σ是单的，从而$a_1r_1+\cdots+a_nr_n=0$.

又$\because\ r_1,\cdots,r_n$是E的一组F-基$\Rightarrow\ a_1=a_2=\cdots=a_n=0$ 即$\sigma\left(r_1\right),\cdots,\sigma\left(r_n\right)$线性无关 .

$\therefore \dim_F\sigma(E)\geqslant n$，又$\therefore \dim_F\sigma(E)\leqslant\dim_F E=n$. 则$\dim_F\sigma(E)=n$,即$\sigma(E)=E$. 由$\alpha\in S\subset E$,所以存在$\alpha_1\in E\subset K$使得$\sigma(\alpha_1)=\alpha$, 即$\alpha$为$\alpha_1$在$\sigma$下的原像. 从而$\sigma:K\longrightarrow K$是满的.

故σ是同构.

□

3.4 代数闭包(2)

K/F是一个数域扩张，$F\overset{\sigma}{\hookrightarrow}K$ 嵌入，对于多项式$F[x]$中多项式

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in F[x]$$

定义$\sigma f(x)$为

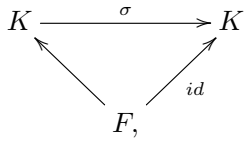
$$\sigma f(x)\overset{\triangle}{=}f^\sigma(x)=\sigma(a_n)x^n+\sigma(a_{n-1})x^{n-1}+\cdots+\sigma(a_1)x+\sigma(a_0)\in\sigma(F)[x]\subset K[x].$$

设有$\alpha\in F$ 使得 $f(\alpha)=0$, 则

$$\begin{aligned}f^\sigma(\sigma(\alpha))&=\sigma(a_n)\sigma(\alpha)^n+\sigma(a_{n-1})\sigma(\alpha)^{n-1}+\cdots+\sigma(a_1)\sigma(\alpha)+\sigma(a_0)\\&=\sigma(a_n\alpha^n+a_{n-1}\alpha^{n-1}+\cdots+a_1\alpha+a_0)\\&=a_n\alpha^n+a_{n-1}\alpha^{n-1}+\cdots+a_1\alpha+a_0\\&=0.\end{aligned}$$

即$\sigma(\alpha)$是f^σ上的一个根.

如下图



$F\subset K,\sigma:K\longrightarrow K$是一个$F$˘嵌入, 且$\sigma|_F=id$.设$f(x)\in F[x],\alpha\in K$。若$f(\alpha)=0$, 则由于$\sigma(f(x))=f^\sigma(x)=f(x)$(因为$\sigma|_F=id_F$)，故

$$0=\sigma(0)=\sigma(f(\alpha))=f^\sigma(\alpha)=f(\sigma(\alpha)),$$

即$f(\sigma(\alpha))=0$. 从而$\sigma(\alpha)$也是$f(x)$的一个根。

$\sigma(f(\alpha))=f(\sigma(\alpha))$, 考虑

$$\sigma(\frac{f(\alpha)}{g(\alpha)})=\frac{f^\sigma(\sigma(\alpha))}{g^\sigma(\sigma(\alpha))},$$

从而得到

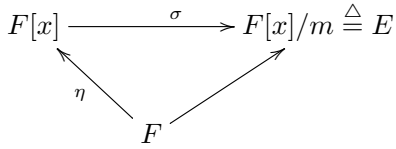
$$\sigma(\frac{f(\alpha)}{g(\alpha)}) = \frac{f(\sigma(\alpha))}{g(\sigma(\alpha))}.$$

问：F是一个域，$f(x) \in F[x], degf > 0$是否有F的扩域E，使得f在E中有根？

由于$F[x]$是PID，则任意一个多项式

$$f(x) = P_1(x)^{e_1} \cdots P_r(x)^{e_r}$$

其中$P_i(x)$在F上不可约. 不妨设f在F上不可约，$f(x) \in F[x]$.令$m =< f > \lhd F[x]$，则m是极大理想



显然σ为满射,此时E为域，F直接看作E的子域，从而可把E看作F的扩域, 由于$f(x) \in m$，故在$E = F[x]/m$中$\overline{f(x)} = \overline{0}$. 将$f(x)$展开如下：

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \in F[X],$$

于是我们有：

$$\begin{aligned}\overline{0} = \overline{f(x)} &= \overline{a_n x^n + \cdots + a_1 x + a_0} \\ &= \overline{a_n}\overline{x}^n + \cdots + \overline{a_1}\overline{x} + \overline{a_0}\end{aligned}$$

即在E中（注意到$\overline{a_i} = a_i, i = 1 \cdots n, F \hookrightarrow E$ ）

继而得到：

$$\overline{0} = a_n\overline{x}^n + \cdots + a_1\overline{x} + \overline{a_0}$$

此时$\overline{x} \in E$,即$f(\overline{x}) = \overline{0}$,也即$f$在$E$中有根.

Theorem 3.5. *设F是一个域，$f(x) \in F[X]$,且$degf > 0$,则存在一个F扩域E,使得f在E中有根.(证明上面已给出)*

Corollary 3.1. *设F是一个域，$f_1(x) \cdots f_n(x) \in F[X]$,且$degf_i > 0, i = 1 \cdots n$,则存在一个$F$扩域$E$,使得$f_1(x) \cdots f_n(x)$在$E$中均有根.*

证明. 由上述定理，存在一个F扩域E_1,使得$f_1(x)$在E_1中有根，此时

$$f_2(x) \in F[X] \subset E_1[X],$$

又由上述定理，存在E_1扩域E_2,使得$f_2(x)$在E_2中有根.依次下去，得到E_{n-1}扩域E_n,使得$f_n(x)$在E_n中有根.

即$f_1(x) \cdots f_n(x)$在E_n中有根. □

Definition 3.6. 代数封闭域（*algebraically field*）

设K是一个域,如果K上任意一个次数大于*0*的多项式，均在K中有根，则称K是一个代数封闭域.

事实 设K是一个代数封闭域,$f(x) \in K[X]$,且$n = degf > 0$,则$f(x)$在K中有且只有n个根.(重根按重数计算)

证明. 由所设，$f(x)$在K中有根，取其一为α_1,即$\alpha_1 \in K$,,满足$f(\alpha) = 0$,此时由带余除法可知，

$$(x - \alpha_1)|f(x),$$

即:

$$f(x) = (x - \alpha_1) \cdot g(x),$$

其中$g(x) \in K[X]$,且次数为$n - 1$.

(1)若$n - 1 = 0$,则$f(x)$在K中有一个根，结论显然成立.

(2)若$n - 1 > 0$,此时$g(x)$在K中有一个根α_2,此时有：

$$g(x) = (x - \alpha_2) \cdot h(x),$$

其中$h(x) \in K[X]$,且次数为$n - 2$,即:

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdot h(x)$$

依次做下去，得到：

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n),$$

故$f(x)$在K中有且只有n个根.(重根按重数计算) □

Theorem 3.6. 任一个域均包含于一个代数封闭域 .

证明. (Artin)

设k是一个域,令：

$$S_0 = \{f(x) \in k[X], degf > 0\},$$

对每个$f \in S_0$,都给f对应于一个未定元，记之为X_f,记

$$S = \{X_f : f \in S_0\}.$$

令$A = K[S]$是k上关于未定元集S的多项式环.注意到，对每个$f \in S_0$,都有$f(X_f) \in A$,令：

$$I =< f(X_f) : f \in S_0 >,$$

为A中由所有$f(X_f)(f \in S_0)$生成的理想.

下证：I是A的真理想，即证$1 \notin I$,

反证，若$1 \in I$,就有

$$1 = g_1 f_1(X_{f_1}) + \cdots + g_n f_n(X_{f_n}) \tag{1}$$

其中$g_1\cdots g_n\in A, f_1\cdots f_n\in S_0, g_1\cdots g_n\in A$是$\{X_f\}_{f\in S_0}$中有限个变量的多项式.(虽然$A$中的变量个数是无限的，但每个多项式$g_i$的变量个数是有限的)

对于$f_i(X_{f_i})\in k[X_f], i=1\cdots n$,由上述定理可知，存在$k$的扩域$E_1$,使得$f_i(X_{f_i})$在$E_1$中均有根，不妨取其根为$\alpha_i\in E$,(即$f_i(\alpha_i)=0$),将$\alpha_i$代入（1）中,得到：

$$1=g_1(\alpha_1)f_1(\alpha_1)+\cdots+g_n(\alpha_n)f_n(\alpha_n)=0,$$

矛盾!

因此I是A的真理想，故有A的一个极大理想m,使得$I\subset m$.令$K_1=A/m$,则K_1是一个域，从而如下图所示：

$$\begin{array}{ccc} A=K[S] & \xrightarrow{\quad\sigma\quad} & K_1=A/m \\ & \nwarrow \quad \nearrow & \\ & k & \end{array}$$

其中σ显然为满射，K_1可看作是k的一个扩域.任取$f\in S_0, f(X_f)\in I\subset m$. 从而有$\overline{f(X_f)}=\overline{0}\in A/m=K_1$,即$f(\overline{X_f})=\overline{0}$,也即$\overline{X_f}$是$f$在$K_1$中的一个根.

对于K_1按上述步骤，可构造K_1的一个扩域K_2，使得K_1中的任一次数≥ 0的多项式，在K_2中均有根.依此类推，可得到域的扩张链如下：

$$k\subset K_1\subset\cdots\subset K_n\subset\cdots,$$

其中K_n中次数大于0的多项式均在K_n-1中有根.令$K=\bigcup\sum_{i=1}^{\infty}K_i$,则显然$K$是一个域，且$k\subset K$.

下证：K是代数封闭域.

为此任取$f(x)\in K[X]$,且$degf>0$,则由上述构造可知，存在$n\in Z_{\geq 0}$,使得$f(x)\in K_n[X]$,于是$f(x)$在$K_{n+1}[X](\subset K)$中与根，故K是代数封闭域. □

Theorem 3.7. *设k是一个域，则存在域K,使得K是代数封闭域，且K/k是代数扩张，称K是k的一个代数闭包.*

证明. 由前面的定理可知，k包含于一个代数封闭域E中，令$K=\{\alpha\in E,\alpha$是一个k—代数元$\}$,则K是一个域，且K/k是一个代数扩张.

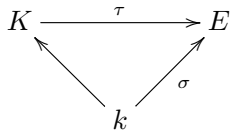
下证：K是代数封闭域.

为此任取$f(x)\in K[X]$,且$degf>0$,则$f(x)\in E[X]$,由于E是代数封闭域，故f在E中有根，取其一为α,即$\alpha\in E, f(\alpha)=0$

显然α是一个K—代数元,即$K[\alpha]/K$是一个代数扩张，又由于K/k是一个代数扩张，进而可知$K[\alpha]/k$是一个代数扩张.即α是一个k—代数元,从而可知$\alpha\in K$,因此K是代数封闭域，K是k的一个代数闭包（同构意义下） □

E是代数封闭域,K/k是一个代数扩张,$\sigma: k\to E$,问是否存在$\tau; K\to E$,使得$\tau|_k=\sigma$.正如下图

所示：



简化模型 $K = k(\alpha)$是k上的单代数扩张，设α在k上的极小多项式为$P_\alpha(x) \in k[X]$,从而有$P_\alpha^\sigma(x) \in \sigma(k)[X] \subset E[X]$,且有$P_\alpha^\tau(x) \in E[X]$.

由$P_\alpha(\alpha) = 0$推出$0 = \tau(P_\alpha(\alpha)) = P_\alpha^\tau(\tau(\alpha)) = P_\alpha^\sigma(\tau(\alpha))$,即$\tau(\alpha)$是$P_\alpha^\sigma$在$E$中的一个根.

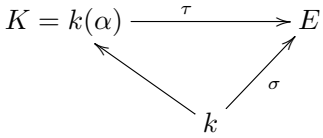
反之，$\beta \in E$,且$P_\alpha^\sigma(\beta) = 0$,令

$$\tau; k(\alpha) \to E, \quad \alpha \longmapsto \beta$$

从而有对应

$$g(\alpha) \longmapsto g^\sigma(\tau(\alpha)) = g^\sigma(\beta)$$

继而下图成立：



Proposition 3.2. *设E是代数封闭域,$k \subset E$,α是一个k—代数元,$P_\alpha(x) \in k[X]$是k上的极小多项式，则$k(\alpha)$到E中的k-嵌入的个数$=P_\alpha(x)$中全部互异根的个数$\leq degP_\alpha(x)$.*

Proposition 3.3. *设K/k是一个代数扩张，E是一个代数封闭域，$\sigma; k \to E$是一个域嵌入，则σ可延拓到K上，即有域嵌入*

$$\tau : K \to E$$

使得$\tau|_k = \sigma$.

3.5 分裂域 正规扩张

回顾：设k是代数封闭域，$,f(x) \in k[X]$,且$n = degf > 0$,,则$f(x)$在k中有根，从而就有n个根.(重根按重数计算)

设F是一个域，$f(x) \in F[X]$,且$n = degf > 0$,,则$f(x)$在F中至多有n个根.

代数闭包：K/k是一个域扩张（1）K/k是代数扩张；（2）K是代数封闭的，则称K是k的一个代数闭包.

取E为代数封闭域，且$k \subset E$,令： $k^\alpha = \{\alpha \in E, \alpha$是一个$k$—代数的$\}$,则$k^\alpha$是$k$的一个代数闭包.

Proposition 3.4. *设k是代数封闭域，且K/k是一个代数扩张，则$K = k$.(代数闭域只有平凡的代数扩张)*

证明. 任取$\alpha \in K, \alpha$是一个k—代数元，α在k上的极小多项式为,$P_\alpha(x) \in k[X]$,则$degP_\alpha(x) > 0$,于是$P_\alpha(x)$在k中完全分解.特别地，$\alpha \in k$ □

Proposition 3.5. 设E为代数封闭域，k是一个域，则k到E的任何一个嵌入，$\sigma; k \to E$均可延拓到k的任何一个代数扩域K上，即对于任意代数扩张K/k,存在嵌入：

$$\tau; K \to E,$$

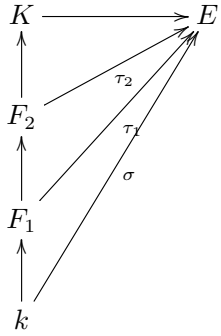
使得$\tau|_k = \sigma$.

证明. 取$S = \{(F, \tau) : F$是K/k的中间域,$\tau; F \to E$,且$\tau|_k = \sigma$显然$(k, \sigma) \in S, S \neq \phi$.

在S中引入如下关系：对于$(F_1, \tau_1), (F_2, \tau_2) \in S$，定义$(F_1, \tau_1) \leq (F_2, \tau_2)$，如果$F_1 \subset F_2$，且满足$\tau_2|_{F_1} = \tau_1$.

易验证，“$\leq$”是S上的一个偏序关系，即$(S, \leq)$是一个非空偏序集.

如下图：

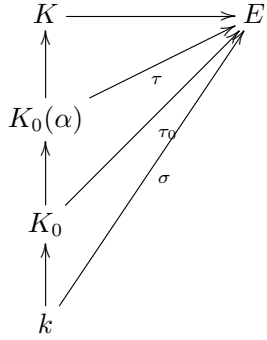


任取S上的一个全序子集$\{(F_i, \tau_i)\}_{i \in I}$,令$L = \bigcup_{i \in I} F_i$,则$L$是$K/k$的一个中间域，此时我们令：

$$\tau; L \to E \quad \alpha \longmapsto \tau_i(\alpha)$$

其中$\alpha \in F_i$,对任意的$\alpha \in L$,则τ是一个嵌入.

证明思路如下图：



该嵌入是良好定义的.如果$\alpha \in F_i$,且$\alpha \in F_j$,则不妨设$F_i \subset F_j$,此时$\tau_i = \tau_j|_{F_i}$,从而有$\tau(\alpha) = \tau_i(\alpha) = \tau_j|_{F_i}(\alpha) = \tau_j(\alpha)$.且对任意的$\alpha \in K$,有$\alpha \in F_i$（对于任意的$i \in I$)进而有

$$\tau(\alpha) = \tau_i(\alpha) = \sigma(\alpha),$$

即$\tau|_k = \sigma$.可以推出$(L, \tau) \in S$,且显然有$\tau|_{F_i} = \tau_i$,即$(F_i, \tau_i) \leq (L, \tau)(i \in I)$成立.也即$(L, \tau)$是$\{(F_i, \tau_i)\}_{i \in I}$在$S$中的一个上界.

因此由$Zorn$引理可知，S中有极大元，设其中的一个极大元为(K_0, τ_0).

下证：$K = K_0$.

假若不然，则有$\alpha \in K, \alpha \notin K_0$,由所设$\alpha$是一个$k$—代数元,从而$\alpha$也是一个$K_0$—代数元,故$K_0(\alpha)/K_0$是一个单代数扩张.

由前面的定理得τ_0可延拓到$K_0(\alpha)$上,即有嵌入

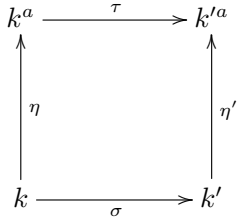
$$\tau' : K_0(\alpha) \to E,$$

使得$\tau'|_{K_0=\tau_0}$.显然有$\tau'|_k = \tau_0|_k = \sigma$,故$(K_0(\alpha), \tau') \in S$.但$(K_0, \tau_0) \leq (K_0(\alpha), \tau')$,但$K_0 \neq K_0(\alpha)$与$K_0$的极大性矛盾.

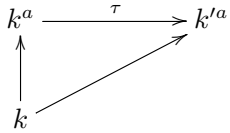
因此$K = K_0$. □

取E为代数封闭域，且$k \subset E$,令$k^a = \{\alpha \in E, \alpha$是一个$k$—代数元$\}$,则$k^a$是$k$的一个代数闭包.

设k, k'是域，$\sigma : k \to k'$为同态应射同态映射；$\eta : k \to k^a$为恒等嵌入；$\eta' : k' \to k'^a$为恒等嵌入.如图所示：



则σ可延拓到k^a上，即有域嵌入$\tau : k^a \to k'^a$,使得$\tau|_k = \sigma$.即有：



Corollary 3.2. 任一个域k的代数闭包在k—同构下是唯一的，即对于k的两个的代数闭包K_1与K_2,都有域同构：

$$\sigma : K_1 \to K_2,$$

使得$\sigma|_k = id.$(即K_1与K_2是k—同构的)

Proposition 3.6. 域F的任一个有限乘法子群都是循环的.

证明. 设$G \subset F^*$是一个有限群，且$|G| > 1$，由有限$Able$群结构定理可知，只需证G是一个P群的情形.（P是素数）此时记$|G| = p^n (n \in Z_{\geq 1})$,令$S = \{m \in Z_{\geq 0}$:存在$a \in G$,使得$\sigma(a) = p^m\}$,则$S \neq \phi$,且对于任意$m \in S$,有$m \leq n$.由S是一个有限集合，故S中有最大整数，记之为r,且有$b \in G$,使得$\circ(b) = p^r$,显然$r \leq n$.

于是对任意的$\alpha \in G$,记$\circ(\alpha) = p^s, s \in Z_{\geq 0}$,则$s \leq r$.于是就有$\alpha^{p^r} = (\alpha^{p^s})^{p^{r-s}} = 1^{p^{r-s}} = 1$.因此，$G$中元素均是$X^{p^r} - 1$的根.

因为$G \subset F^*$,而$X^{p^r} - 1$在F中至多有p^r个根，可以推出$|G| \leq p^r$,即$p^n \leq p^r \leq p^n$,从而得到$r = n$,进而得到$\circ(b) = p^n$.

故$G =< b >$. □

分裂域 正规扩张

设k是一个域，$f(x) \in k[X]$,且$n =, degf > 0$,取k^a为k的一个代数闭包，则$f(x)$在k^a中可完全分解为：

$$f(x) = a(x - \alpha_1) + \cdots + (x - \alpha_n)$$

令$K = k(\alpha_1 \cdots \alpha_n) \subset k^a$.

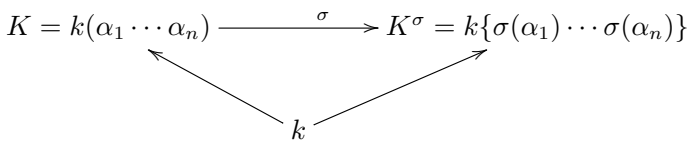
事实:上述K是k^a/k中使得$f(x)$在其中可完全分解的最小中间域.若$\alpha_1 \cdots \alpha_n \in K'$,则可以得到$K = k(\alpha_1 \cdots \alpha_n) \subset K'$,称$K$为$f$在$k$上的一个分裂域.我们有：

$$K = k(\alpha_1 \cdots \alpha_n) \to K^\sigma = k\{\sigma(\alpha_1) \cdots \sigma(\alpha_n)\}$$

从而我们有对应：

$$\{\alpha_1 \cdots \alpha_n\} \longmapsto \{\sigma(\alpha_1) \cdots \sigma(\alpha_n)\}$$

从而我们有下图：



分裂域是在k—同构意义下是唯一的.

对于两个多项式的分裂域，$f_1, f_2 \in k(x)$,f_1的根为$\alpha_1 \cdots \alpha_m$； f_2的根为$\beta_1 \cdots \beta_n$； 我们得到$E_1 = k(\alpha_1 \cdots \alpha_m), E_2 = k(\beta_1 \cdots \beta_n)$,则有：

$$\begin{aligned} E = E_1E_2 &= E_1(E_2) = E_2(E_1) \\ &= k(\alpha_1 \cdots \alpha_m)k(\beta_1 \cdots \beta_n) \\ &= k(\alpha_1 \cdots \alpha_m\beta_1 \cdots \beta_n) \end{aligned}$$

Definition 3.7. *(分裂域)* 设K是一个域,$\{f_i\}_{i\in I}$是k上的一簇多项式，取定k^a为k的一个代数闭包,$\{f_i\}_{i\in I}$
在k^a/k中的分裂域是指K:$k \subset K \subset k^a$,且满足：

（1）每个$f_1, (i = 1 \cdots n)$在K中完全分解；

（2）对k^a/k的任一个中间域E,如果k^a/k在E中完全分解，有$K \subset E$；

具体地,令$S = \{\alpha \in k^a$:存在$i \in I$,使得$f_i(\alpha) = 0$,则有$K = k(S)$.注意到：分裂域是在k—同构意义下是唯一的.

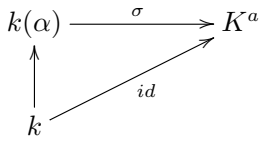
考虑不可约多项式，设k是一个域,$f(x) \in k[X]$,且f在k上不可约，从而有：

$$f(x) = a(x - \alpha_1) + \cdots + (x - \alpha_n)$$

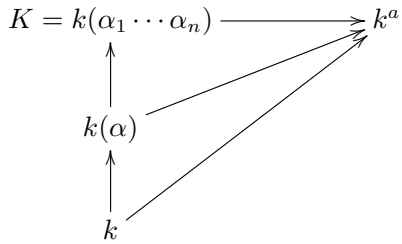
$\alpha_1 \cdots \alpha_n \in k^a$,令$S = \{\alpha_1 \cdots \alpha_n\}$, 我们有映射：

$$\sigma : k(\alpha) \to k^a \quad \alpha \longmapsto \sigma(\alpha),$$

由$f(\sigma(\alpha))=0$,可知：$\sigma(\alpha)\in\{\alpha_1\cdots\alpha_n\}$我们有下图：



进而我们考虑下图：



取$K=k(\alpha_1\cdots\alpha_n)$为$f$在$k^a/k$中的分裂域，对于映射

$$\tau:K\to\tau(K)\quad \tau|_k=id,$$

我们有:$f^\tau(x)=f(x)$,推出$0=\tau(0)=\tau(f(\alpha_i))=f(\tau(\alpha_i))$,从而推出$\tau(\alpha_i)\in S$,进而有$\tau(K)\subset k(S)=K$,即$\tau(K)=K$.

又由于K/k是代数扩张，故τ是满的，从而$\tau\in Aut_k(K)$为K到自身的一个k-嵌入. 即有下图：

$$\tau:K\to K\quad \tau|_k=id.$$

Definition 3.8. （正规扩张）设K/k是一个域的代数扩张，k^a为k的一个代数闭包,如果K到自身的k-自同构，则称K/k是一个正规扩张.

Definition 3.9. 设k是一个域, $\alpha\beta\in k^a$.如果在k上的不可约多项式，$P(x)\in k[X]$,使得$P(\alpha)=P(\beta)=0$,则称α与β是k-共轭的.(极小多项式相同，即多项式的根之间为k-共轭元.)

Definition 3.10. $\alpha\sim\beta\in k^a\iff$ 极小多项式相同,(固定一个代数闭包的情形下，给一个$\alpha\in k$,则就对应于一个极小多项式.)则"$\sim$"是一个等价关系.

$k^a/\sim=\{k-$共轭类$\}$

3.6 正规扩张 可分扩张

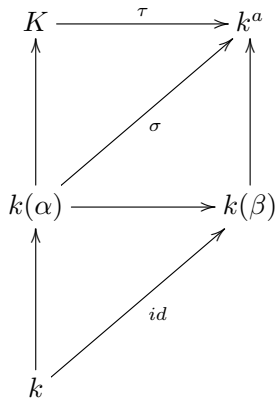
Theorem 3.8. 设K/k是一个域的代数扩张，k^a是k的包含K一个代数闭包,则下列陈述等价：

（1）K到k^a的任一个k-嵌入均是K的一个k-自同构，即$\sigma(K)=K$.

（2）$k[X]$中的任一不可约多项式f如果在K中有一个根，则f在K中完全分解.（即K包含$\alpha\in k^a$的同时也包含α的在k^a中的全部共轭元.）

（3）K是k上一簇多项式在k上的分裂域.

证明. （1）$\Longrightarrow$（2）证明思路如下图：



设$f(x) \in k[X]$为k上的一个不可约多项式，且有$\alpha \in K$.使得$f(\alpha) = 0$

下证：$f(x)$在k^a中的任一个根β都必在K中.

事实上，对于上述的$\beta \in k^a$,令

$$\sigma : k(\alpha) \to k^a \quad \alpha \longmapsto \beta,$$

则$\sigma : k(\alpha) \to k^a$是一个$k$-嵌入.

由于$K/k(\alpha)$是代数的，故σ可延拓为

$$\tau : K \to k^a,$$

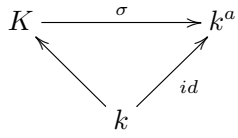
即$\tau|_{k(\alpha)} = \sigma$.

显然τ也是一个k-嵌入，由所设，$\tau(K) = K$.特别地，$\beta = \sigma(\alpha) = \tau(\alpha) \in K$,故$K$包含$\alpha$的全部共轭元.

（2）$\Longrightarrow$（3）取$S = \{P(x) \in k[X], P(x)$是某个$\alpha \in K$在$k$上的不可约多项式$\}$,则$K$是$S$在$k$上的分裂域.

（3）$\Longrightarrow$（1）设K是多项式簇$\{f_i\}_{i\in I} \subset k[X]$在$k$上的分裂域.(其中$deg f_i > 0$)

任取K到k^a的任一个k-嵌入如下：



下证$\sigma(K) = K$.

下面只需证：$\sigma(K) \subset K$.

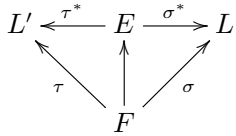
为此任取$\alpha \in K$，由所设，有$f_i \subset k[X]$，使得$f_i(\alpha) = 0$,从而有$\sigma(f_i(\alpha)) = 0$,即$f_i(\sigma(\alpha)) = 0 \Rightarrow \sigma(\alpha) \in K \Rightarrow \sigma(\alpha) \subset K$.故$\sigma(K) = K, \sigma$是$K \to K$的自同构. □

Theorem 3.9. *(1)* 设K/k是一个域的正规扩张，对k的任一个扩域F，则FK/K也是正规的；

（2）设$k \subset E \subset K$,如果K/k是正规的，则K/E也是正规的；

（3）设K_1, K_2均是k的代数扩张，且$K_1, K_2 \subset L$，如果$K_1/k, K_2/k$均是正规的，则K_1K_2/k, $K_1 \cap K_2/k$均是正规的.

可分扩张 E/F是一个代数扩张，L, L'是F的两个代数封闭域，则有下图：

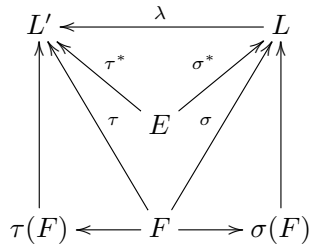


设$\sigma : F \to L$是一个嵌入，$\tau : F \to L'$,令：$S(\sigma) = \{\sigma^* : E \to L$嵌入，且$\sigma^*|_F = \sigma\}$,$S(\tau) = \{\tau^* : E \to L'$嵌入，且$\tau^*|_F = \tau\}$.

事实：

$$S(\sigma) \longleftrightarrow S(\tau) \quad \sigma^* \longmapsto \tau^*$$

不妨令$\tau^* = \lambda \circ \sigma^*$，则有下图：



其中λ是$\tau \circ \sigma^{-1} : \sigma(F) \to L'$到$L'$上的延拓.

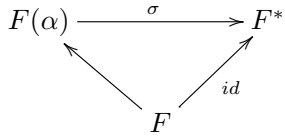
任取$\alpha \in F$,$\tau^*(\alpha) = \lambda\sigma^*(\alpha) = \lambda\sigma(\alpha) = \tau \circ \sigma^{-1}\sigma(\alpha) = \tau(\alpha)$,故$\tau^*|_F = \tau$.

Definition 3.11. 设E/F是一个代数扩张，F^a是F的一个代数闭包，任取一个F-嵌入$\sigma : F \to F^a$,令$S(\sigma) = \{\sigma^* : E \to F^a$嵌入，且$\sigma^*|_F = \sigma\}$.定义$E/F$的可分次数为$[E : F]_s \overset{\triangle}{=} \# S(\sigma)$.特别地$\sigma = id$

$$\begin{aligned}[E : F]_s &= \#S(id) \\ &= \#\{\sigma^* : E \to F^*, \sigma^*|_F = id\}\end{aligned}$$

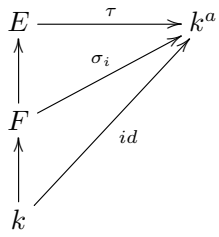
即为$\#\{E$到F^*的全部F-嵌入$\}$.

例如：$E = F(\alpha)$为一个单代数扩张，$\alpha \in F^a$,则$[E : F]_s = \alpha$在F上的极小多项式全部互异根（根在F^a中）的个数.即有：



Theorem 3.10. 设有域扩张$k \subset F \subset E$,则有$[E : k]_s = [E : F]_s[F : k]_s$.

证明. 令$S_E = \{\tau : E \to k^a$嵌入，且$\tau|_k = id\}$,$S_F = \{\sigma : F \to k^a$嵌入，且$\sigma|_k = id\}$,即有：



设$S_F = \{\sigma_1 \cdots \sigma_m\}$,对每一个$\sigma_i \in S_F$,记$S_{E/F}(\sigma_i) = \{\tau : E \to k^a$嵌入，且$\tau|_F = \sigma_i\}$,则$\#S_{E/F}(\sigma_i) = [E : F]_s$,且有$S_E \subset \{\tau : E \to k^a$嵌入，且$\tau|_F = \sigma_i$,对每个$i \in \{1 \cdots n\}\} \triangleq T$

任取$\tau \in S_E$,则$\tau|_F$是F 到k^a的一个k-嵌入，$\tau|_F = \sigma_i$,对某个$i \in \{1 \cdots n\}$,从而得到$S_E \subset T$,因此$S_E = T$.

故我们得到：$[E : k]_s = \#S_E = \#T = m\#S_{E/F}(\sigma_i) = [E : F]_s[F : k]_s$. □

Theorem 3.11. 设K/k是一个域的有限扩张，则$[E : k]_s \le [E : k]$.*(即可分次数≤扩张次数)*

证明. 由所设，$K = k(\alpha_1 \cdots \alpha_n)$,其中$\alpha_1 \cdots \alpha_n \in K$.于是有：

$$k \subset k(\alpha_1) \subset k(\alpha_1, \alpha_2) \subset \cdots \subset k(\alpha_1 \cdots \alpha_n) = K,$$

其中 $k(\alpha_1 \cdots \alpha_i) = k(\alpha_1 \cdots \alpha_{i-1})(\alpha_i)$.

由前面的结果有：

$$\begin{aligned}[k(\alpha_1 \cdots \alpha_i) : k(\alpha_1 \cdots \alpha_{i-1})]_s &= [k(\alpha_1 \cdots \alpha_{i-1})(\alpha_i) : k(\alpha_1 \cdots \alpha_{i-1})]_s \\ &\le [k(\alpha_1 \cdots \alpha_i) : k(\alpha_1 \cdots \alpha_{i-1})].\end{aligned}$$

于是我们得到：

$$\begin{aligned}[K : k]_s &= [K : k(\alpha_1 \cdots \alpha_{n-1})]_s \cdots [k(\alpha_1) : k]_s \\ &\le [K : k(\alpha_1 \cdots \alpha_{n-1})] \cdots [k(\alpha_1) : k] \\ &= [K : k].\end{aligned}$$

□

Proposition 3.7. 设$K = k(\alpha)$是k的单代数扩张，则K/k是可分的$\iff \alpha$是可分代数元.

证明. $[K : k]_s = [k(\alpha) : k]_s = P_\alpha(x)$在$k^a$中互异根的个数.

故：K/k可分$\iff [K : k]_s = [K : k] = degP_\alpha(x)$=$P_\alpha(x)$在$k^a$中互异根的个数$\iff P_\alpha(x)$在$k^a$中无重根$\iff P_\alpha(x)$为可分的$\iff \alpha$为$k$上的可分代数元. □

Definition 3.12. 设k是一个域，k_a是k的一个代数闭包，$\alpha \in k^a$,称α为k上的可分代数元.如果α在k上的极小多项式是可分的.

注：多项式可分$\iff$它无重根；

Proposition 3.8. 域的代数扩张K/k是可分的$\Longleftrightarrow$ K中的每个元素均是k上的可分代数元.特别地，对于有限扩张K/k有：K/k可分$\Longleftrightarrow K=k(\alpha_1\cdots\alpha_n),\alpha_1\cdots\alpha_n\in K$为$k$上的可分代数元.

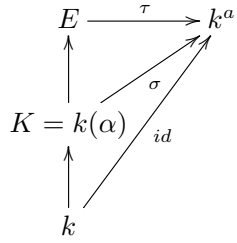
正规闭包

回忆一下正规扩张，$K/k,K=k(\alpha),\alpha\in K$单代数扩张，$\alpha$在$k$上的极小多项式为：

$$P_\alpha(x)=(x-\alpha_1)\cdots(x-\alpha_n),\quad \alpha_1=\alpha\in K$$

记E为$P_\alpha(x)$在k上的分裂域（$\subset k^a$）,则E是k^a中包含$k(\alpha)$的最小正规扩域,称E是$k(\alpha)/k$的一个正规闭包.

由于K/k是正规扩张，从而在K上完全分裂，$\tau(\alpha)\in E,E/k$正规，$\tau|_K=\sigma\Rightarrow\tau(\alpha)=\sigma(\alpha)=\alpha_i$,对某个$i\in\{1\cdots n\}$,即有下图：



一般地，任一个代数扩张K/k在k^a中均有一个正规闭包k',即：（1）k'/k是正规的（$k'\subset k^a$）;(2)设$E\subset k^a,E/k$是正规的，且$E\supset K$,则$E\supset K'$.

Theorem 3.12. **本原元（*primtive element*）**

设K/k是域的有限扩张，则：K是k的单代数扩张$\Longleftrightarrow$ K/k只有有限个中间域.特别地,域的有限可分扩张必是单代数扩张，此时$K=k(\alpha),\alpha$称为K/k的一个本原元.

证明. (1)" $\Leftarrow$ "(充分性)若k是有限域，则由K/k是有限扩张$\Rightarrow$ K是有限域，则K^*是循环群，记$K^*=<\alpha>,\alpha\in K,\alpha\neq\{0\}$,从而推出$K=k(\alpha)$.则$K$为单扩张.

若k是无限域，设K/k只有有限多个中间域，由于K/k是有限扩张，不妨$K=k(\alpha,\beta)$.对任意的$c\in k^*$,有中间域:

$$E_c=k(\alpha+c\beta),$$

由所设K/k只有有限个中间域，但$c\in k^*$是无限的，从而有$c_1,c_2\in k^*,c_1\neq c_2$,使得$k(\alpha+c_1\beta)=k(\alpha+c_2\beta)\triangleq E$.于是$\alpha+c_1\beta,\alpha+c_2\beta\in E$,从而推出$(c_1-c_2)\beta\in E$.又由于$c_1\neq c_2\Rightarrow c_1-c_2\neq0\Rightarrow\frac{1}{(c_1-c_2)}(c_1-c_2)\beta\in E$.即$\beta\in E$,进而我们有$\alpha=(\alpha+c_1\beta)-c_1\beta\in E$.即

$$K=k(\alpha,\beta)\subset E\subset K,$$

故$K=E=k(\alpha+c\beta)$.

" $\Rightarrow$ "(必要性)设$K=k(\alpha)$是k的一个单代数扩张，设$P_\alpha(x)$为α在k上的极小多项式，记$S=\{$中间域$E:k\subset E\subset K\}$,对每个$E\in S,\alpha$也是E上的代数元，记α在E上的极小多项式为$P_{\alpha,E}(x)$，则显然有$P_{\alpha,E}(x)|P_\alpha(x)$,(因为$P_\alpha(x)$也是$E$上的多项式，且$P_\alpha(\alpha)=0$.)

记$T=\{P_{\alpha,E}(x):E\in S\}$,则$\#T<+\infty$.令：

$$\phi:S\to T\quad E\mapsto P_{\alpha,E}(x).$$

下证：ϕ是一个单射.

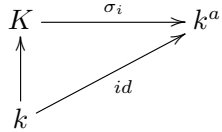
对于$P_{\alpha,E}(x)\in T,(E\in S)$,令$F$为$k$上添加$P_{\alpha,E}(x)$的全部系数所得的扩域，则$k\subset F\subset E$.此时$P_{\alpha,E}(x)\in F(X)$,且为$F$上不可约多项式.

又显然$K=k(\alpha)=E(\alpha)=F(\alpha)\Rightarrow[K:E]=degP_{\alpha,E}(x);[K:F]=degP_{\alpha,E}(x)$,从而推出$[K:E]=[K:F]$,又由于$F\subset E$,即可得到$E=F$.由此可知$\phi$是一个单射.

故有$\#S\leq\#T<+\infty$,即S是一个有限集，从而K/k中的中间域只有有限个. □

（2）下证：域的有限可分扩张必是单代数扩张，$\#k=+\infty$.

证明. 证法一（书上），设$[K:k]=n$,不妨设$K=k(\alpha,\beta),(\alpha,\beta\in K)$,由所设$[K:k]_s=n$,取$k$的代数闭包$k^a$,使得$k^a\subset K$.此时$K$到$k^a$共有$n$个不同的$k$-嵌入$\sigma_1\cdots\sigma_n$.即：



令$f(x)=\prod_{1\leq i\neq j\leq n}\{(\sigma_i\alpha+x\sigma_i\beta)-(\sigma_j\alpha+x\sigma_j\beta)\}$,则$f(x)\neq0$.(不是零多项式)

假若不然，则有上述$i,j,i\neq j$,使得$\sigma_i\alpha+x\sigma_i\beta=\sigma_j\alpha+x\sigma_j\beta$,即满足$\sigma_i\alpha=\sigma_j\alpha,\sigma_i\beta=\sigma_j\beta$,从而对于$\sigma_i,\sigma_j:K\to k^a$,我们得到：$\sigma_i=\sigma_j$,与所设矛盾，故$f(x)\neq0$.

设$f(x)$在k^a中至多有有限个根（零点），故在k中也只有有限个零点.但$\#k=+\infty.$，从而存在$c\in k^*$,使得$f(c)\neq0$.于是$(\sigma_i\alpha+c\sigma_i\beta)-(\sigma_j\alpha+c\sigma_j\beta)\neq0$,也即$\sigma_i\alpha+c\sigma_i\beta\neq\sigma_j\alpha+c\sigma_j\beta,(i\neq j)$.注意到$\sigma_i\alpha+c\sigma_i\beta=\sigma_i(\alpha+c\beta),(i=1\cdots n)$,而$\sigma_i$是$K$到$k^a$的$k$-嵌入，故$\sigma_i(\alpha+c\beta)$均是$\alpha+c\beta$的$k$-共轭元，从而推出$[k(\alpha+c\beta):k]_s\geq n$.

另一方面，$k(\alpha+c\beta)\subset K$,即有：

$$n=[K:k]=[K;k]_s\geq[k(\alpha+c\beta):k]=[k(\alpha+c\beta):k]_s\geq n,$$

故有，$K=k(\alpha+c\beta)$. □

证明. 证法二（构造法）把满足上面条件的c找出

不妨设$K=k(\alpha,\beta)$,取定k的一个代数闭包k^a,使得$k^a\subset K$,分别设α,β在k^a中的全部共轭元为$\alpha=\alpha_1\cdots\alpha_m,\beta=\beta_1\cdots\beta_n$,令

$$S=\{\frac{\alpha_i-\alpha_j}{\beta_l-\beta_k}|1\leq i\neq j\leq m,1\leq l\neq k\leq n\},$$

显然S是一个有限集.

由所设，k是一个无限域，故有$c\in k^*$,使得$c\notin S$,又设$f(x),g(x)\in k[X]$是α,β在k上的极小多项式，记$r=\alpha+c\beta=\alpha_1+c\beta_1\in K$,令$h(x)=f(r-cx)$,则$h(x)\in k[r][X]\subset K[X]$,则$h(\beta_1)=f(r-c\beta_1)=f(\alpha_1)=0$,可以推出$\beta_1$是$h(x)$的一个根，又$\beta_1$也是$g(x)$的一个根，而$h(\beta_j)\neq0,(j=$

$2\cdots n)$,若不然，$h(\beta_j)=0\Rightarrow f(r-c\beta_j)=0$,而$f(x)$的根为$\alpha_1\cdots\alpha_m$,进而有$r-c\beta_j=\alpha_i$,对某个$i=1\cdots m$,即

$$\alpha_1+c\beta_1-c\beta_j=\alpha_i\Rightarrow\alpha_1-\alpha_i=c(\beta_j-\beta_1)\Rightarrow c=\frac{\alpha_1-\alpha_i}{\beta_j-\beta_1}\Rightarrow c\in S,$$

矛盾!

由于$g(x),h(x)\in k[r][X]$,且由上述讨论可知，$g(x),h(x)$的最大公因式为$(x-\beta_1)$,即$(g(x),h(x))=x-\beta_1$,由辗转相除法可知：$x-\beta_1\in k[r][X]\Rightarrow\beta=\beta_1\in k[r]$,又由于$r=\alpha+c\beta\Rightarrow\alpha=r-c\beta\in k[r]\Rightarrow k(\alpha,\beta)=K\subset k[r]\subset K$,故

$$K=k(r)=k(\alpha,\beta).$$

□

Example 3.2. $K=Q(\sqrt{-1},\sqrt{-2})=Q(r)$,求$r$.

解：由于$K=Q(\sqrt{-1})(\sqrt{-2})$,而$\sqrt{-1}$的$Q$-共轭元为$\pm\sqrt{-1}$,$\sqrt{2}$的$Q$-共轭元为$\pm\sqrt{2}$,$[Q(\sqrt{-1}):Q]=2,[Q(\sqrt{-1})(\sqrt{-2}):Q(\sqrt{-1})]=2$.(这是由于$\sqrt{-2}\notin Q(\sqrt{-1})$,如若不然$\sqrt{-2}=a+b\sqrt{-1},a,b\in Q\Rightarrow 2=a^2-b^2+2ab\sqrt{-1}$.左边属于$Q$,右边属于$C$,但不属于$Q$,从而矛盾,故$\sqrt{-2}\notin Q(\sqrt{-1}),\Rightarrow[Q(\sqrt{-1})(\sqrt{-2}):Q(\sqrt{-1})]=2$.)故有$[K:Q]=4$.

K/Q是有限可分，故有本原元,从而有：

$$S=\{\pm\frac{\sqrt{-1}-(-\sqrt{-1})}{\sqrt{2}-(-\sqrt{2})}\}=\{\pm\frac{\sqrt{-1}}{\sqrt{2}}\}.$$

取$c=1$即满足条件.即有：

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

3.7 有限域

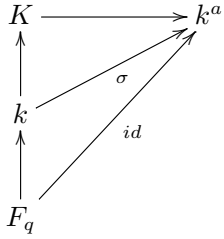
设k是一个有限域，此时k的特征$char(k)=p$,(p为素数)即为p元域，$F_p\subset k$.换言之F_p是k的素子域,显然，k/F_p是有限扩张（即有限域的有限扩张）.

不妨设$[k;F_p]=n,\Rightarrow k=|F_p|^n=p^n$,记$k=F_q,F_q=p^n$.取$k$的一个代数闭包$k^a$,则$G=F_q^*$是一个$q-1$阶循环群，可以推出存在$\alpha\in F_q^*$,有$\alpha^{q-1}=1\Rightarrow\alpha^q=\alpha$(任意$\alpha\in F_q$).即$\alpha$是多项式$x^{q-1}-1$在$k^a$中的一个根.

$k=F_q\subset\{x^q-x$在k^a中的根$\}.\Rightarrow q=\#k\le\#\{x^q-x$在$k^a$中的根$\}\le q$,从而有$k=\{x^q-x$在$k^a$中的根$\}$,且$x^q-x$在$k$中是可分的，由于$f(x)=x^q-x\Rightarrow f'(x)=qx^{q-1}-1=-1,(f(x),f'(x))=1$.

设K,k均为有限域，且$k\subset K$,记$char(k)=p$,(p为素数)，由前述讨论可知：$\#k=p^m,\#K=p^n,(m,n\in Z_{\ge1})$.记$[K;k]=r\in Z_{\ge1}$,则$p^n=|K|=|k|^r=(p^m)^r\Rightarrow n=mr\Rightarrow m|n$.即若有限域有包含关系，其指数定有整除关系.

事实上，设K,k均为有限域，且$k\subset K$，则K/k是一个可分的单代数扩张.由于$|k|=p^m,|K|=p^n.\Rightarrow k=\{x^{p^m}-x在k^a中的全部根\}=x^{p^m}-x在F_q上的分裂域,\Rightarrow k/F_q也是正规扩张\Rightarrow K/k也是正规扩张$，即有：



设$char(k)=p,(p为素数).令$：

$$\phi:k\to k\quad \alpha\mapsto\alpha^p,$$

则$\phi\in Aut_{F_p}(k)是k到自身的一个自同构.$

由于任意$\alpha,\beta\in k,有$：

$$\phi(\alpha+\beta)=(\alpha+\beta)^p=\alpha^p+\beta^p=\phi(\alpha)+\phi(\beta),$$

且满足：

$$\phi(\alpha\beta)=(\alpha\beta)^p=\alpha^p\beta^p=\phi(\alpha)\phi(\beta),$$

ϕ是一个域同态，又由于其是$x^{p^m}-x在F_p$上的分裂域，ϕ是自同构，即$\phi\in Aut(k).$

Definition 3.13. 称上述映射$\phi:k\to k为k上的Frobenious$自同构，记为$Frob_k.$

事实：$\phi是k到自身的F_p$-自同构，任意的$\alpha\in F_p\Rightarrow\phi(\alpha)=\alpha^p=\alpha.易知Aut_{F_p}(k)$关于映射的合成是一个群.

首先有$\#Aut_{F_p}(k)=[k:F_p]=m,\phi\in Aut_{F_p}(k)=\{\sigma:\sigma是k到自身的F_p$-自同构$\}.任意的\alpha\in k,$

$$\phi(\alpha)=\alpha^p,$$

$$\phi^2(\alpha)=\phi(\phi(\alpha))=\phi(\alpha^p)=\phi(\alpha)^p=\alpha^{p^2},$$

即有:

$$\phi^r(\alpha)=\alpha^{p^r},$$

特别地，

$$\phi^m(\alpha)=\alpha^{p^m}=\alpha,(\alpha\in k)$$

即$\phi^m=id.\Rightarrow\circ(\phi)|m.$

又记$\circ(\phi)=r,则\phi^r=id.于是任意的\alpha\in k,有\phi^r=\alpha=id(\alpha)\Rightarrow\alpha^{p^r}=\alpha\Rightarrow k\subset\{x^{p^r}-x在k^a中的全部根\}.$

进而有$p^m\le p^r\Rightarrow m\le r|m\Rightarrow r=\circ(\phi)=m\Rightarrow Aut_{F_p}(k)=<\phi>=<Frob_{F_p}>.$

故$Aut_{F_p}(k)是由Frobenious元生成的m阶循环群.$

一般地，对于有限域扩张$K/k,char(k)=p,(p为素数)，Aut_k(K)=<Frob_K>=<\phi_K>.$

$$Frob_K : K \to K \quad \alpha \mapsto \alpha^{p^m} = \alpha^{|k|},$$

且有$\circ(\phi_K) = \#Aut_k(K) = [K : k] = \frac{n}{m}$.

故$Aut_k(K)$是一个$[K : k]$阶循环群.

3.8 不可分扩张

设 $K|k$ 是单代数扩张, $K = k(\alpha)$, α在k上极小多项式为$f(x) \in k[x]$. 设$deg(f) = n$,则$\{1, \alpha, \cdots, \alpha^{n-1}\}$ 是K的一组$k-$基,$K = k(\alpha) = k[\alpha]$.

取定k的代数闭包k^a,设$\alpha_1, \cdots, \alpha_m$是$f(x)$在$k^a$中的全部互异根，$\alpha_i$的重数记为$r_i$, 则在$k^a$中，有

$$f(x) = (x - \alpha_1)^{r_1} \cdots (x - \alpha_m)^{r_m},$$

其中$m = [K : k]_s$(可分次数)。K到k^a的$k-$嵌入共有m个，分别记为$\sigma_1, \cdots, \sigma_m$,取定$\alpha = \alpha_1$,不妨设$\sigma_i(\alpha) = \alpha_i$,将$\sigma_i$延拓为$k^a$上的一个$k-$自同构，记之为$\tau_i$,于是有 $\tau_i|_K = \sigma_i$,

$$\tau_i(f(x)) = (x - \tau_i(\alpha_1))^{r_1} \cdots (x - \tau_i(\alpha_m))^{r_m},$$

即

$$\begin{aligned}(x - \alpha_1)^{r_1} \cdots (x - \alpha_i)^{r_i} \cdots (x - \alpha_m)^{r_m} \\ = (x - \alpha_i)^{r_1} \cdots (x - \tau_i(\alpha_m))^{r_m}\end{aligned}$$

由此可得$r_i = r_1 (i = 1, \cdots, m)$.即极小多项式的所有根在代数闭包$k^a$中有相同的重数。特征为零的域上不可约多项式无重根.因此若f有重根，则$char(k) = p$，其中p为某一素数。同时注意到由于f有重根，故$(f, f') \neq 1$,但由于f不可约且 $deg(f') < deg(f)$,f'只能为零，这就说明f是形如$f(x) = g(x^p)$的多项式(其中$g(x) \in k[x]$,且由于$f(x)$为$k[x]$中不可约多项式，$g(x)$也是$k[x]$中不可约多项式.). 于是α^p是$g(x)$的一个根。重复上述过程，最终，我们可以找到最小的整数$r \geq 0$，使得α^{p^r}是$k[x]$中一个可分不可约多项式$h(x)$的根，且

$$f(x) = h(x^{p^r}).$$

设$h(x)$在k^a中的分解为$h(x) = (x - \beta_1) \cdots (x - \beta_s)$, 令$\gamma_i \in k^a (i = 1, \cdots, s)$使得$\gamma_i^{p^r} = \beta_i$, 设$t = r_1 = \cdots = r_m$ 则

$$\begin{aligned}f(x) &= (x - \alpha_1)^t \cdots (x - \alpha_m)^t \\ &= (x^{p^r} - \gamma_1^{p^r}) \cdots (x^{p^r} - \gamma_s^{p^r}) \\ &= (x - \gamma_1)^{p^r} \cdots (x - \gamma_s)^{p^r}\end{aligned}$$

由一元多项式分解的唯一性知$m = s, t = p^r$.

于是

$$f(x) = (x - \alpha_1)^{p^r} \cdots (x - \alpha_s)^{p^r}.$$

由

$$[k(\alpha):k]=deg(f)=s\cdot p^r=[k(\alpha):k]_s\cdot p^r$$

知$[k(\alpha):k]_s|[k(\alpha):k]$,它们的商$\frac{[k(\alpha):k]}{[k(\alpha):k]_s}=p^r$称为$k(\alpha)|k$的**不可分次数**,记之为$[k(\alpha):k]_i$.
令$\beta=\alpha^{p^r}$,则$h(\beta)=h(\alpha^{p^r})=f(\alpha)=0$,由于$h(x)$是首一不可约多项式，于是$h(x)$是$\beta$在$k[x]$上的极小多项式.因$h(x)$无重根， $[k(\alpha^{p^r}):k]=[k(\alpha^{p^r}):k]_s=deg(h(x))=s$. 由域扩张的次数传递公式知$[k(\alpha):k(\alpha^{p^r})]=\frac{n}{[k(\alpha^{p^r}):k]}=\frac{n}{s}=p^r$.同样可得到

$$[k(\alpha):k(\alpha^{p^r})]_s=\frac{[k(\alpha):k]_s}{[k(\alpha^{p^r}):k]_s}=\frac{s}{s}=1.$$

于是$[k(\alpha):k(\alpha^{p^r})]_i=p^r$. 注意到$k(\alpha)=k(\alpha^{p^r})(\alpha)$,令$a=\alpha^{p^r}\in k(\alpha^{p^r})$, 则$x^{p^r}-a$是$\alpha$在$k(\alpha^{p^r})$上的极小多项式，该极小多项式只有一个根$\alpha$且重数为$p^r$.

Definition 3.14. 设k是域，$char(k)=p>0$, k^a是k的一个代数闭包，设$\alpha\in k^a$,如果有$r\in\mathbb{Z}_{\geq 0}$使得 $\alpha^{p^r}\in k$,则称α为k上的一个**纯不可分元**。

Proposition 3.9. 设K/k是一个代数扩张，$char(k)=p>0$,则下列陈述等价:
(i)$[K:k]_s=1$.
(ii)K中任一元素均是k上纯不可分元。
*(iii)*对$\forall\alpha\in K$, α在k上的极小多项式均形如$x^{p^r}-a, a\in k, r\in\mathbb{Z}_{\geq 0}$.
(iv)K是在k上添加若干个纯不可分元生成。
称满足上述命题中等价条件的域扩张K/k为一个**纯不可分扩张**。

证明. $(i)\Rightarrow(ii)$任取$\alpha\in K$,由$[k(\alpha):k]_s|[K:k]_s=1$知 $[k(\alpha):k]_s=1$,由此知α在k上极小多项式必形如 $x^{p^r}-a\in k[x]$,由此$\alpha^{p^r}\in k$,即α是k上纯不可分元。
$(ii)\Rightarrow(iii)$设$\alpha\in K$是k上的纯不可分元，即有$\exists r\in\mathbb{Z}_{\geq 0}, x^{p^r}-a\in k[x]$,使得$\alpha^{p^r}=a\in k$,不妨设$r$是满足该条件的最小的非负整数，令$f(x)=Irr(\alpha,k,x)$为$\alpha$在$k$上的不可约多项式(极小多项式)，则$f(x)|x^{p^r}-a$. 由于

$$x^{p^r}-a=x^{p^r}-\alpha^{p^r}=(x-\alpha)^{p^r},$$

$f(x)=(x-\alpha)^m$,其中$m=p^st\leq p^r, s\leq r, p\nmid t$.对$f(x)$进行二项式展开，

$$\begin{aligned}f(x)&=(x-\alpha)^{p^st}\\&=(x^{p^s}-\alpha^{p^s})^t\\&=x^{p^st}-t\cdot\alpha^{p^s}x^{p^s(t-1)}+\cdots+(-1)^t\alpha^{p^st}\in k[x],\end{aligned}$$

因此$t\cdot\alpha^{p^s}\in k$,由$p\nmid t$,而$char(k)=p$得到t在k中可逆，于是$\alpha^{p^s}=b\in k$.由r的极小性得到$r\leq s$.又由上面知$s\leq r$,因此$r=s, t=1$.即 $f(x)=x^{p^r}-a$.即$x^{p^r}-a$是α在k上的不可约多项式。
$(iii)\Rightarrow(iv)$显然地.
$(iv)\Rightarrow(i)$任取K到k的某一代数闭包$\bar{F}$的 $k-$嵌入，设K由在k上纯不可分元$\{\alpha_i\}_{i\in I}$生成，则

$$f_i(X)=Irr(\alpha_i,k,X)$$

是α_i在k上的极小多项式，由于α_i是纯不可分元, 存在$r \in \mathbb{Z}_{\geq 0}, a \in k$使得$\alpha_i^{p^r} = a_i \in k$，因此$f_i(X)|(X^{p^r} - a_i)$,即$f(X)$只有唯一根$\alpha_i$,任意$K$到$\bar{F}$的$k$嵌入$\tau$把元素映到其共轭元，但任意$\alpha_i$的共轭元只有自身,于是$\tau$是恒等映射,即$[K:k]_s = 1$. □

Proposition 3.10. 设$K|k$是一个代数扩张，K_0为K中所有在k上可分的代数扩张的合，则$K_0|k$是可分扩张，$K|K_0$是纯不可分的。也称K_0为k在K中的可分闭包。

证明. $K|k$的可分子扩张的复合仍是可分扩张，于是$K_0|k$是可分扩张；若$char(k) = 0$,则显然$K_0 = K$,若$char(k) = p$,则任给$\alpha \in K$,存在非负整数n使得α^{p^n}在k上可分的，于是$\alpha^{p^n} \in K_0$,即$K|K_0$是纯不可分扩张。 □

Corollary 3.3. 对于上述命题中$K|k$为有限扩张的情形,有

$$[K:k]_s = [K_0:k],$$
$$[K:k]_i = [K:K_0].$$

证明.

$$\begin{aligned}[K:k]_s &= [K:K_0]_s \cdot [K_0:k]_s \\ &= 1 \cdot [K_0:k]_s \\ &= [K_0:k].\end{aligned}$$

$$\begin{aligned}[K:k]_i &= [K:K_0]_i \cdot [K_0:k]_i \\ &= [K:K_0]_i \cdot 1 \\ &= [K:K_0].\end{aligned}$$

□

Corollary 3.4. 设$K|k$是域的正规扩张，K_0是k在K中的可分闭包，则$K_0|k$也是正规扩张。

证明. 设k^a是k的一个代数闭包，任取K_0到k^a的一个$k-$嵌入σ,下面证明$\sigma(K_0) = K_0$,从而$K^0|k$是正规扩张.

σ可延拓到K上，记为$\tau : K \to k^a$.由于$K|k$是正规扩张，$\tau(K) = K$.任取$\alpha \in K_0$, α在k上极小多项式$P_\alpha(X) \in k[X]$无重根,而$\tau(\alpha) = \sigma(\alpha)$在$k$上极小多项式也是$P_\alpha(X)$，于是$\tau(\alpha)$在$k$上也可分，从而$\tau(\alpha) \in K_0$,即$\tau(K_0) \subseteq K_0 \Rightarrow \sigma(K_0) = K_0$. □

Corollary 3.5. 设$E|k$是域的一个有限扩张，$p = char(k) > 0$,若$E^p \cdot k = E$,则$E|k$是可分的。反之，如果$E|k$是可分，则$E^{p^r}k = E(\forall r \in \mathbb{Z}_{\geq 1})$.

证明. $\Rightarrow$:设E_0是k在E中的极大可分扩张，$E|k$是有限扩张，因此对$\forall \alpha \in E$,存在固定的$m \in \mathbb{Z}_{\geq 1}$使得$\alpha^{p^m} \in E_0$,于是$E^{p^m} \subseteq E_0$.

另一方面，

$$\begin{aligned} & E^p k = E \\ \Rightarrow\ & E^p = (E^p k)^p = E^{p^2} k^p \\ \Rightarrow\ & E^{p^2} k^{p+1} = E^p k = E \\ \Rightarrow\ & E^{p^2} k \supseteq E^{p^2} k^{p+1} = E \supseteq E^{p^2} k \\ \Rightarrow\ & E = E^{p^2} k \end{aligned}$$

如此归纳下去便得到$E = E^{p^n} k (n \in \mathbb{Z}_{\geq 1})$, 但$E^{p^m} k \subseteq E_0 k = E_0$,于是$E \subseteq E_0 \subseteq E$,即$E_0 = E$, $E|k$是可分的。

$\Leftarrow$:设$E|k$可分，则$E|E^p k$是可分.又对任意$\alpha \in E$,有$\alpha^p \in E^p \subseteq E^p k$，于是$E|E^p k$是纯不可分的.故$E = E^p k$.由上面证明可得对任意$r \in \mathbb{Z}_{\geq 1}, E^{p^r} \cdot k = E$. □

Proposition 3.11. 设$K|k$是域的一个正规扩张，令$G = Aut_k(K)$是K到自身的$k-$自同构，又记

$$K^G = \{\alpha \in K | \sigma(\alpha) = \alpha, \forall \sigma \in G\}.$$

则K^G是$K|k$的中间域，且$K^G|k$是纯不可分的，$K|K^G$是可分的。又设K_0是k在K中的可分闭包，则$K_0 K^G = K, K_0 \cap K^G = k$.

证明. 任取$\sigma \in Aut_k(K), \sigma|_k = id$,于是$k \subseteq K^G$,即$K^G$是$K|k$的中间域。

(1)下证$K^G|k$是纯不可分的。

为此，任取$\alpha \in K^G$,取定k的一个代数闭包k^a，使得$k^a \supseteq k$. 任取$k(\alpha)$到k^a的$k-$嵌入$\sigma : k(\alpha) \to k^a$，将$\sigma$延拓到$K$上，记之为$\tau : K \to k^a$.由所设$K|k$是正规扩张，则$\tau(K) = K$.即$\tau$是一个$K$到自身的$k-$嵌入，于是$\tau \in G$, $\sigma(\alpha) = \tau(\alpha) = \alpha (\forall \alpha \in K^G)$. 这就说明$\sigma = id$,即$k(\alpha)$到自身的$k-$嵌入只有唯一的恒等映射。从而$[k(\alpha) : k]_s = 1$，$\alpha$是$k$上的纯不可分元，令$\alpha$跑遍$K^G$可得$K^G|k$是纯不可分扩张。

(2)证明$K|K^G$是可分的，方法用$Serge\ Lang : Algebra.P_{264}$Artin定理的证明。

(3)若K_0是k在K中的可分闭包，则$K_0|k$是可分的，于是 $K_0 \cap K^G|k$是可分的，又由于$K^G|k$是纯不可分的，于是 $K_0 \cap K^G|k$是纯不可分的.综上，$K_0 \cap K^G = k$.

(4)由$K|K^G$是可分的，$K|(K^G \cdot K_0)$也是可分的，又因 K_0是k在K中的可分闭包，故$K|(K^G K_0)$是纯不可分的，于是 $K = K^G K_0$. □

Example 3.3. *(1)*设p是素数，p元域$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$中，任意$\alpha \in \mathbb{F}_p, \alpha^p = \alpha$,于是$\mathbb{F}_p^p = \mathbb{F}_p$.

(2)$F = \mathbb{F}_p[x]$中，因x不能表示出某个多项式的p 次方,故$F^p \neq F$.

Definition 3.15. 设k是一个域，

*(1)*当$char(k) = 0$时，称k是一个*perfect*域。

*(2)*当$char(k) = p > 0$时，如果$k^p = k$,则称k是一个*perfect*域。

Corollary 3.6. 设k是一个*perfect* 域，则k的任意代数扩张都是可分扩张，k的任意代数扩张都是$perfect$.

证明. 设$K|k$是域的代数扩张，任取$\alpha \in K$,设E是$k(\alpha)|k$在K中的正规闭包，记$G = Aut_k(E)$,则$E^G|k$是纯不可分的.

对于任意$\beta \in E^G$有$\beta^{p^r} \in k$，即$\beta^{p^r} = a \in k$. 由于k是perfect,有$b \in k$使得$a = b^p$,于是$\beta^{p^{r-1}} = b \in k$,继续下去可得到$\beta \in k$,于是$E^G \subseteq k$，但又因 $E^G \supseteq k$,故$E^G = k$。这就得到$E|k$是可分的，α 在k上是可分的，由于α是任意的，于是$K|k$是可分扩张.

□

4 Galois理论

4.1 有限Galois理论

设$K|k$是域的一个代数扩张，令$G = Gal(K|k) = Aut_k(K)$,则G是一个群，称为$K|k$的Galois群。任取$H \leq G$(子群),令

$$K^H = \{\alpha \in K | \sigma(\alpha) = \alpha, \forall \sigma \in H\},$$

结论:$k \subseteq K^H \subseteq K, K^H$是一个域。
证:任取$\alpha, \beta \in K^H$,对任意$\sigma \in H, \sigma(\alpha) = \alpha, \sigma(\beta) = \beta$,于是

$$\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta) = \alpha + \beta \Longrightarrow \alpha + \beta \in K^H$$
$$\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta) = \alpha\beta \Longrightarrow \alpha\beta \in K^H$$

若$\alpha \in K^H$,设$\beta = \alpha^{-1} \in K$, 由$\alpha\beta = 1$,得$\sigma(\alpha)\sigma(\beta) = \alpha\beta = 1$.于是$\sigma(\beta) = \beta$，即$\beta \in K^H$.综上，$K^H$是一个域。

Definition 4.1. 设$K|k$是一个域的代数扩张，如果$K|k$既是可分的，也同时是正规的，则称$K|k$是一个 *Galois*扩张。

设$K|k$是一个n次*Galois*扩张，$n = [K : k]$.则$|Gal(K|k)| = [K : k]_s = [K : k]$.

Theorem 4.1. （***Artin***）设k是一个域，$G \subseteq Aut(K)$是一个有限子群，令$k = K^G$,则$K|k$是一个*Galois*扩张，且其*Galois*群为$Gal(K|k) = G$.

证明. 任取$\alpha \in K$,设α的$G-$轨道为

$$G \cdot \alpha = \{\sigma_1\alpha, \sigma_2\alpha, \cdots, \sigma_r\alpha\}.$$

不妨设$\sigma_1 = id$,显然,对任意$\tau \in G, \tau G\alpha = G\alpha$,即

$$\{\tau\sigma_1\alpha, \tau\sigma_2\alpha, \cdots, \tau\sigma_r\alpha\}.$$

令$f(x)=(x-\sigma_1\alpha)\cdots(x-\sigma_r\alpha)$, 则

$$\begin{aligned} f^\tau(x)&=(x-\tau\sigma_1\alpha)\cdots(x-\tau\sigma_r\alpha)\\ &=f(x)\end{aligned}$$

这就说明$f(x)\in K^G[x]=k[x]$.显然，由于$\sigma_1=id, f(\alpha)=0$. 而$\sigma_1\alpha,\cdots,\sigma_r\alpha$两两不同，故$f(x)$无重根，即可分。从而$\alpha$是$k$上的可分元，由$\alpha$的任意性，$K|k$是可分的。

又设α在k上的极小多项式为$P_\alpha(x)$,则$P_\alpha|f(x)$,于是α的$k-$共轭元必属于$\{\sigma_1\alpha,\cdots,\sigma_r\alpha\}\subseteq K$,于是$\sigma(K)\subseteq K$,即$K|k$是正规扩张.综上，$K|k$是$Galois$扩张.

下证$Gal(K|k)=G$.设$|G|=n$,首先由定义易知$G\subseteq Gal(K|k)$. 又由上述证明可知，对任意$\alpha\in K$,有

$$[k(\alpha):k]=degP_\alpha(x)\leq degf(x)\leq|G|=n,$$

由此下述引理可证得$[K:k]\leq n$.于是$|Gal(K|k)|\leq n$.综上，$Gal(K|k)=G$. □

Lemma 4.1. 设$E|k$是可分代数扩张，若存在固定地正整数n使得对任意 $\alpha\in E,[k(\alpha):k]\leq n$.则$E|k$是有限扩张，且$[E:k]\leq n$.

证明. 不妨设m是k的单代数扩张的最大次数，即有$\alpha\in K$,使得 $[k(\alpha):k]=m$,且$\forall\beta\in K,[k(\beta):k]\leq m$. 下面说明$K=k(\alpha)$。
若不然，存在$\beta\in K-k(\alpha)$,由本原元定理，存在$\gamma\in K$使得$k(\alpha,\beta)=k(\gamma)$.于是

$$k\subseteq k(\alpha)\subsetneqq k(\alpha)(\beta)=k(\gamma).$$

由$k(\gamma)|k$是单代数扩张，$[k(\gamma):k]\leq m$,这与$k(\alpha)\subsetneqq k(\gamma)$矛盾！故$K=k(\alpha)$,进而$[K:k]=m\leq n$. □

Lemma 4.2. 设$K|k$是$Galois$扩张，$G=Gal(K|k)$,则$K^G=k$.

证明. 显然，$k\subseteq K^G$.下证$K^G\subseteq k$.

对任意$\alpha\in K^G$,任取$k(\alpha)$到K的一个$k-$嵌入，则σ可延拓为$k-$嵌入$\tau:K\to K$, 即$\tau\in G,\tau|_{k(\alpha)}=\sigma$.由所设 $\sigma(\alpha)=\tau(\alpha)=\alpha(\forall\alpha)\in K^G$.于是$\sigma=id$.由$k(\alpha)|k$是可分扩张，$[k(\alpha):k]=[k(\alpha):k]_s=1$.即$k(\alpha)=k$,由于$\alpha\in K^G$是任意，故$K^G\subseteq k$.综上，$K^G=k$. □

Theorem 4.2. ***Galois*理论基本定理***(*有限扩张情形*).*设$K|k$是域的n次$Galois$扩张,其$Galois$群为$G=Gal(K|k)$,用S表示所有k和K的中间域组成的集合，J表示G的所有子群组成的集合。令

$$\begin{aligned}\phi:&S\to J\\ &E\mapsto Gal(K|E)\end{aligned}$$

则*(1)*ϕ是一个双射，特别地，$K^{Gal(K|k)}=k$.
*(2)*设$k\subseteq E_1\subseteq E_2\subseteq K$,则对应地，有$\phi(E_1)\supseteq\phi(E_2)$.反之，如果 $1\leq H_1\leq H_2\leq G$,则$\phi^{-1}(H_1)\supseteq\phi^{-1}(H_2)$,
*(3)*对于中间域$E,k\subseteq E\subseteq K$, $E|k$是$Galois$扩张当且仅当$\phi(E)\triangleleft G$,此时

$$Gal(E|k)\cong G/\phi(E)\cong G/Gal(K|E).$$

*(4)*设有中间域$k \subseteq E_i \subseteq K(i=1,2)$，则

$$\phi(E_1 \cap E_2) =< \phi_(E_1) \cup \phi(E_2) >$$
$$\phi(E_1E_2) = \phi(E_1) \cap \phi(E_2)$$

*(5)*设中间域$k \subseteq E_1 \subseteq E_2 \subseteq K$,则 $E_2|E_1$是$Galois$的当且仅当$\phi(E_2) \lhd \phi(E_1)$.此时有

$$Gal(E_2|E_1) \cong \phi(E_1)/\phi(E_2) = Gal(K|E_1)/Gal(K|E_1).$$

证明. (1)任取$E \in S$,由于$K|k$是Galois扩张，$K|E$是Galois扩张，即$Gal(K|E) \in J$，从而ϕ是良定义的。

下证ϕ是单射。设对于中间域$k \subseteq E_i \subseteq bK(i=1,2)$,若有$\phi(E_1) = \phi(E_2)$,即

$$Gal(K|E_1) = Gal(K|E_2).$$

由上一引理得,$E_1 = K^{Gal(K|E_1)}, E_2 = K^{Gal(K|E_2)}$.由此$E_1 = E_2$,即$\phi$是单射.

下证ϕ是满射。任取$H \leq G$,令$E = K^H$,此时由$Artin$定理，$K|E$是Galois扩张，且$Gal(K|E) = H$,显然E是中间域，且$\phi(E) = H$.故ϕ是满射.

综上，ϕ是双射。

(2)若$k \subseteq E_1 \subseteq E_2 \subseteq K$, $\phi(E_1) = Gal(K|E_1), \phi(E_2) = Gal(K|E_2)$. 任取$\sigma \in Gal(K|E_2)$, 则$\sigma|_{E_2} = id$,从而$\sigma|_{E_1} = id$.于是$\sigma \in Gal(K|E_1)$.这便是$\phi(E_1) \supseteq \phi(E_2)$.

同样可得:若$1 \leq H_1 \leq H_2 \leq G$,则$\phi^{-1}(H_1) \supseteq \phi^{-1}(H_2)$.

(3)若$k \subseteq E \subseteq K$,且$E|k$是正规的，令

$$\psi : Gal(K|k) \to Gal(E|k)$$
$$\sigma \mapsto \sigma|_E,$$

则显然ψ是群同态，下证ψ是满射.任取$\sigma \in Gal(E|k)$,将σ延拓为K到k的代数闭包k^a的$k-$嵌入τ,由于$K|k$是正规扩张，故$\tau(K) = K$,从而$\tau \in Gal(K|k)$,于是$\psi(\tau) = \sigma$,即ψ是满射。

另一方面,

$$ker(\psi) = \{\sigma \in Gal(K|k) | \psi(\sigma) = id\} \subseteq Gal(K|E).$$

又$\forall \sigma \in Gal(K|E)$,则$\psi(\sigma) = \sigma|_E = id$,于是$Gal(K|E) \subseteq Ker\psi$.故$Gal(K|E) = ker\psi$.此时，$Gal(K|E)$是$Gal(K|k)$的正规子群，且由群同态基本定理得

$$Gal(K|k)/Gal(K|E) \cong Gal(E|k).$$

反过来，若$E|k$不是正规扩张，则存在E到K的$k-$嵌入λ使得$\lambda E \neq E$,将λ延拓成K的$k-$子同构,仍记为λ(因$K|k$是正规扩张,$\lambda(K) = K$),于是

$$Gal(K|\lambda E) = \lambda Gal(K|E)\lambda^{-1}.$$

$Gal(K|\lambda E)$与$Gal(K|E)$共轭但不相同(因对应的中间域不同)，这就说明$Gal(K|E)$不是$Gal(K|k)$的正规子群。

(4)若中间域$k \subseteq E_i \subseteq K(i=1,2)$，则

$$\begin{aligned} & E_1 \supseteq E_1 \cap E_2, E_2 \supseteq E_1 \cap E_2 \\ \Rightarrow & \psi(E_1) \subseteq \psi(E_1 \cap E_2), \psi(E_2) \subseteq \psi(E_1 \cap E_2) \\ \Rightarrow & < \psi(E_1) \cup \psi(E_2) > \subseteq \psi(E_1 \cap E_2) \end{aligned}$$

下证

$$\psi(E_1 \cap E_2) \subseteq \psi(E_1) \cup \psi(E_2) := H_0 = H_1 \cup H_2.$$

由于$H_0 \supseteq H_1, H_0 \supseteq H_2$,

$$\begin{aligned} & K^{H_0} \subseteq K^{H_1}, K^{H_0} \subseteq K^{H_1} \\ & \Rightarrow H_0 \subseteq K^{H_1} \cap K^{H_2} = E_1 \cap E_2 \\ & \Rightarrow H_0 \supseteq Gal(K|E_1 \cap E_2) = \psi(E_1 \cap E_2) \\ & \Rightarrow < \psi(E_1) \cup \psi(E_2) > \supseteq \psi(E_1 \cap E_2) \\ & \Rightarrow \psi(E_1 \cap E_2) = < \psi(E_1) \cup \psi(E_2) > \end{aligned}$$

(5)这是(3)的直接推论：运用(3)于域扩张$E_1 \subseteq E_2 \subseteq K$. □

4.2 Galois理论的若干应用

4.2.1 关于多项式根式解的Galois定理

Example 4.1. $f(x) = x^4 - 6x^2 + 7 \in \mathbb{Q}[x]$.
令$t = x^2$, $f(x) = 0 \Rightarrow t = \frac{6 \pm \sqrt{8}}{2} = 3 \pm \sqrt{2} \Rightarrow x = \pm\sqrt{3 \pm \sqrt{2}}$.考虑下列域扩张

$$k := \mathbb{Q} \subseteq k_1 := \mathbb{Q}(\sqrt{2}) \subseteq k_2 := \mathbb{Q}(\sqrt{2})(\sqrt{3+\sqrt{2}}) \subseteq k_3 := \mathbb{Q}(\sqrt{2})(\sqrt{3+\sqrt{2}})(\sqrt{3-\sqrt{2}})$$

则

$$\begin{aligned} & k_3 = k_2(\sqrt{3-\sqrt{2}}), k_2 = k_2(\sqrt{3+\sqrt{2}}), k_1 = k(\sqrt{2}), \\ & (\sqrt{3-\sqrt{2}})^2 \in k_2, (\sqrt{3+\sqrt{2}})^2 \in k_1, (\sqrt{2})^2 \in k = \mathbb{Q}. \end{aligned}$$

Definition 4.2. 设k是一个域，$f(x) \in k[x]$,称f在k上**可根式解**：如果存在k的扩域序列

$$k \subseteq k_1 \subseteq \cdots \subseteq k_r$$

使得k_r包含f的分裂域，且k_r是k的一个根式扩张，即有

$$k_r = k(\alpha_1, \cdots, \alpha_r), k_i = k_{i-1}(\alpha_i),$$

且$\alpha_i^{n_i} \in k_{i-1}$对某一正整数$n_i$成立.

Definition 4.3. 设$K|k$是一个域扩张.如果有域扩张序列

$$k = k_0 \subseteq k_1 \subseteq \cdots \subseteq k_r = K$$

及$n_1, \cdots, n_r \in \mathbb{Z}_{>0}$使得 $K = k(\alpha_1, \cdots, \alpha_r), k_i = k_{i-1}(\alpha_i)$且$\alpha_i^{n_i} \in k_{i-1}(i = 1, \cdots, r)$,则称$K$是$k$的一个根式扩张。若记$n = n_1 \cdots n_r$,则 $\alpha_i^n \in k_{i-1}$,此时称K是k的$n-$**根式扩张**(n不是唯一的).

性质:设$K|E$和$E|k$均是根式扩张，则$K|k$也是根式扩张。

证明. 由$K|E$和$E|k$是根式扩张，有

$$k = k_0 \subseteq k_1 \subseteq \cdots \subseteq k_r = E,$$

满足$k_i = k_{i-1}(\alpha_i), \alpha_i^n \in k_{i-1}$.

$$E = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_s = K,$$

满足$E_i = E_{i-1}(\beta_i), \beta_i^m \in E_{i-1}$.于是

$$k = k_0 \subseteq k_1 \subseteq \cdots \subseteq k_r = E = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_s = K$$

就满足$K|k$的根式扩张的条件。即$K|k$是根式扩张。 □

Theorem 4.3. 设$K|k$是域的有限扩张，且L是$K|k$的一个正规闭包(选定k的一个代数闭包k^a).如果$K|k$是根式扩张，则$L|k$也是根式扩张.

证明. 由$K|k$是有限扩张，则设$K = k(\alpha_1, \cdots, \alpha_r)$.对$r$用归纳法。

当$r = 1$时，简记$K = k(\alpha)$,因为L是$K|k$的正规闭包，故$L = k(\alpha_1, \cdots, \alpha_s)$,其中$\alpha_1, \cdots, \alpha_s$是$\alpha$的全部$k-$共轭元。由所设，$K|k$是一个$n-$根式扩张，于是$\alpha^n = a \in k$(对某个$a \in k$),即$\alpha$是$k$上多项式$x^n - a$的一个根，于是$P_\alpha(x)|(x^n - a)$,故$\alpha_1, \cdots, \alpha_s$都是$x^n - a$的根，即$\alpha_i^n = a \in k$. $L|k$是$n-$根式扩张。

现对于$K = k(\alpha_1, \cdots, \alpha_r)$,记$E = k(\alpha_1, \cdots, \alpha_{r-1})$,并设$E|k$的正规闭包为$L_1$,则由$E$是$k$的根式扩张，及归纳假设$L_1|k$也是根式扩张，又设$L$是$K|k$的正规闭包，则$L = L_1(\beta_1, \cdots, \beta_s)$,其中$\beta_1 = \alpha_r, \beta_1, \cdots, \beta_s$是$\alpha_r$的全部$k-$共轭元。

任取β_i,令

$$\sigma_i : k(\alpha_r) \to k^a$$
$$\alpha_r \mapsto \beta_i$$

则σ_i是$k(\alpha_r)$到k^a的一个$k-$嵌入，σ可延拓成L到k^a的一个$k-$嵌入τ_i，由所设$K|k$是根式扩张，而$K = E(\alpha_r)$,于是 $\alpha_r^n = \gamma \in E$对于某一$n \in \mathbb{Z}_{>0}$成立。由于$E \subseteq L_1$，而$L_1$是一正规闭包，故

$$(\tau_i(\alpha_r))^n = \tau_i(\alpha_r^n) = \tau(\gamma) = \tau_i|_{L_1}(\gamma) \in L_1.$$

于是$\beta_i^n \in L_1(i = 1, \cdots, s)$. 即$L|L_1$是根式扩张，又$L_1|k$是根式扩张，故$L|k$是根式扩张。 □

Definition 4.4. 设G是群，若存在G的子群列

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_r = \{1\},$$

使得$G_{i+1} \trianglelefteq G_i$,且$G_i/G_{i-1}$是$Abel$群，则称$G$是可解群.

Theorem 4.4. ***(Galois)***设k是一个域，$char(k) = 0, f(x) \in k[x]$，$K$是$f(x)$在$k$上的分裂域。则$f$可根式解当且仅当$Gal(K|k)$是可解群.

证明. $\Rightarrow$)由f可根式解，K包含于某个k的根式扩域E中，又取$E|k$的正规闭包$L|k$,由前述定理可知$L|k$也是根式扩张。
不妨设$L|k, E|k$均是$n-$次根式扩张。即有域的扩张序列

$$k = k_0 \subseteq k_1 \subseteq \cdots \subseteq k_r = E \subseteq L,$$

其中$k_i = k_{i-1}(\alpha_i), \alpha_i^n \in k_{i-1}(i = 1, \cdots, r), L = E(\alpha), \alpha^n \in E.$
记$G = Gal(L|k)$为$L|k$的Galois群，且记$H_i = Gal(L|k_i)(i = 1, \cdots, r)$,即有子群序列

$$\{1\} \subseteq H_r \subseteq H_{r-1} \subseteq \cdots \subseteq H_1 \subseteq H_0 = G.$$

为简记，设k包含n次本原单位根ξ_n。

考虑扩张k_i/k_{i-1},由于$k_i = k_{i-1}(\alpha_i), \alpha_i^n \in k_{i-1}$,又$\xi_n \in k \in k_{i-1}$. 则由$Kummer$扩张结果可知,$k_i/k_{i-1}$是一个循环扩张(即$Gal(k_i|k_{i-1})$是循环群)。由$Galois$理论知$H_i \triangleleft H_{i-1}$(正规子群),且

$$H_{i-1}/H_i \cong Gal(k_i|k_{i-1})$$

是循环群。即$G = Gal(L|k)$是一个可解群，G的商群$Gal(K|k)$也是可解群$(Gal(K|k) \cong G/Gal(L|K))$.

$\Leftarrow$)设$Gal(K|k)$是一个可解群，则有子群序列

$$G = Gal(K|k) = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_r = \{e\}.$$

其中$G_{i+1} \triangleleft G_i$,且$G_i/G_{i+1}(i = 0, \cdots, r-1)$是Abel群. 记$n = [K : k]$,且设$k$包含一个$n$次本原单位根$\xi_n$. 记$k_i = K^{G_i}$,则由$Galois$理论，可得$K$的子群序列

$$k = k_0 \subseteq k_1 \subseteq \cdots \subseteq k_r = k,$$

且$k_i|k_{i-1}$是Abel扩张(因为$Gal(k_i|k_{i-1}) \cong G_{i-1}/G_i$是Abel群). 又由所设$\sigma^n = id(\forall \sigma \in G)$,故每个$k_i/k_{i-1}$均为指数为$n$的Abel扩张，由Kummer理论可知$k_i|k_{i-1}(i = 1, 2, \cdots, r)$是一个根式扩张,从而$K|k$是根式扩张，即$f$可根式解。 □

Kummer理论：若有根式扩张$k(\sqrt[n]{\alpha})(\alpha \in k)$(Kummer扩张)，且$\xi_n \in k$,则Kummer扩张一定是循环扩张。

4.2.2 古希腊四大数学难题

1.化圆为方。 2.倍立方。 3.三等分角。 4.正多边形的作图问题。

方法：作图工具只有直尺与圆规.

(1)直线相交:l_1与l_2相交，

$$\begin{cases} a_1x+b_1y+c_1=0 \\ a_2x+b_2y+c_2=0 \end{cases}$$

其中$a_i,b_i,c_i\in\mathbb{Q},i=1,2$.若有交点$P$,则$P\in\mathbb{Q}\times\mathbb{Q}$.

(2)直线与圆相交:

$$\begin{cases} a_1x+b_1y+c_1=0 \\ x^2+y^2+cx+dy+e=0 \end{cases}$$

其中$a_1,b_1,c_1,c,d,e\in\mathbb{Q}$. 若有交点$P$,则$P=(x_0,y_0)\in\mathbb{Q}(\sqrt{\Delta})\times\mathbb{Q}(\sqrt{\Delta}),0\leq\Delta\in\mathbb{Q}$.

Proposition 4.1. 设$\alpha\in R$,则α可尺规构作当且仅当有域扩张序列

$$\mathbb{Q}=k_0\subseteq k_1\subseteq\cdots\subseteq k_r,$$

使得$[k_i:k_{i-1}]\leq 2(i=1,\cdots,r)$,且$\alpha\in k_r$.特别地,$\alpha\in k_r$且$[k_r:\mathbb{Q}]=2^s(s\in\mathbb{Z}_{\geq 0})$,即$\alpha$必为代数数。

问题1:化圆为方(π=正方形的面积?)

解：无解.原因:π是超越数。如若不然，则有$\mathbb{Q}$的某个2^s次扩域k,使得$\pi\in k$,由此得到π是代数数，矛盾!

问题2：倍立方(2=正方形的体积?)

解：无解.问题等价于$\sqrt[3]{2}$是否尺规构作.由于$\sqrt[3]{2}$是3次代数数，$[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3$,而3不是2的幂，从而$\sqrt[3]{2}$不可尺规构作。

问题3：三等分角。

首先，θ可尺规构作当且仅当$cos\theta,sin\theta$均可尺规构作.

解：一般情况下无解。例$\beta=60^0,\theta=\frac{\beta}{3}=20^0$.

$$\begin{aligned} \frac{1}{2}&=cos60^0=cos(3\theta)=cos(2\theta+\theta) \\ &=cos2\theta cos\theta-sin2\theta sin\theta \\ &=(2cos^2\theta-1)cos\theta-2sin^2\theta cos\theta \\ &=2cos^3\theta-cos\theta-2cos\theta+2cos^3\theta \\ &=4cos^3\theta-3cos(\theta) \end{aligned}$$

即$cos\theta$是多项式$f(x)=8x^3-3x-1$的根，而$f(x)$在$\mathbb{Q}$上不可约，于是$[\mathbb{Q}(cos\theta):\mathbb{Q}]=3$,但3不是2的方幂，故$cos\theta$不可尺规作出。

问题4：正多边形作图问题。

解:正n边形可尺规作出当且仅当$\frac{2\pi}{n}$可尺规作出，又等价于 $cos\frac{2\pi}{n}, sin\frac{2\pi}{n}$可尺规作出。

令$\xi_n = e^{\frac{2\pi i}{n}} = cos\frac{2\pi}{n} + isin\frac{2\pi}{n}(n > 2)$,则$\xi_n^{-1} = cos\frac{2\pi}{n} - isin\frac{2\pi}{n}$.于是

$$cos\frac{2\pi}{n} = \frac{\xi_n + \xi_n^{-1}}{2} \in \mathbb{Q}(\xi_n + \xi_n^{-1}) \subseteq R.$$

由$\xi_n \notin \mathbb{Q}(\xi_n + \xi_n^{-1})$得$\mathbb{Q}(\xi_n) \supsetneq \mathbb{Q}(\xi_n + \xi_n^{-1})$,于是

$$[\mathbb{Q}(\xi_n) : \mathbb{Q}(\xi_n + \xi_n^{-1})] \geq 2.$$

又因ξ_n是多项式$f(x) = x^2 - (\xi_n + \xi_n^{-1})x + 1 \in \mathbb{Q}(\xi_n + \xi_n^{-1})[x]$的根，故

$$[\mathbb{Q}(\xi_n) : \mathbb{Q}(\xi_n + \xi_n^{-1})] \leq 2.$$

综上，

$$[\mathbb{Q}(\xi_n) : \mathbb{Q}(\xi_n + \xi_n^{-1})] = 2.$$

Theorem 4.5. *正n边形可尺规构作当且仅当$\phi(n)$(欧拉函数)是2的幂。*

证明. 正n边形可尺规构作$\Leftrightarrow\frac{2\pi}{n}$可尺规作出$\Leftrightarrow cos\frac{2\pi}{n}, sin\frac{2\pi}{n}$可尺规作出 $\Leftrightarrow [\mathbb{Q}(cos\frac{2\pi}{n}) : \mathbb{Q}]$是2的幂。

而

$$\begin{aligned}\phi(n) &= [\mathbb{Q}(\xi_n) : \mathbb{Q}] \\ &= [\mathbb{Q}(\xi_n) : \mathbb{Q}(cos\frac{2\pi}{n})][\mathbb{Q}(cos\frac{2\pi}{n}) : \mathbb{Q}] \\ &= 2[\mathbb{Q}(cos\frac{2\pi}{n}) : \mathbb{Q}].\end{aligned}$$

由此即知命题成立。 □

4.3 域的无限Galois扩张

设$K|k$是无限Galois扩张，一般我们就取K是k的代数闭包。记$G = Gal(K|k)$,对于中间域$k \subset E \subset K$记$H_E = Gal(K|E)$.定义集合 $\mathcal{I} = \{E : E是K|k的中间域，且E|k是有限Galois扩张\}$. $\mathcal{N} = \{H : H = Gal(K|E), E \in \mathcal{I}\}$.

Proposition 4.2. (1) $\cap_{H\in\mathcal{N}} H = \{e\}$.(2) $\cap_{H\in\mathcal{N}} \sigma H = \{\sigma\}(\forall\sigma \in G)$.

证明. (1)任取$\sigma \in \cap_{H\in\mathcal{N}} H$,对任意$\alpha \in K$，设$E$是$k(\alpha)|k$在$K|k$中的正规闭包，则$E \in \mathcal{I}, H_E = Gal(K|E) \in \mathcal{N}$,特别地$\sigma \in H_E$,对$\alpha \in E, \sigma(\alpha) = \alpha$,由$\alpha$的任意性，$\sigma = id$,即$\sigma$在$K$是恒等映射.

(2)

$$\begin{aligned}\forall\tau \in \cap_{H\in\mathcal{N}}\sigma H &\Rightarrow \tau \in \sigma H(\forall H \in \mathcal{N}) \\ &\Rightarrow \sigma^{-1}\tau \in H(\forall H \in \mathcal{N}) \\ &\Rightarrow \sigma^{-1}\tau \in \cap_{H\in\mathcal{N}} = e \\ &\Rightarrow \sigma = \tau \\ &\Rightarrow \cap_{H\in\mathcal{N}}\sigma H = \{\sigma\}(\forall\sigma \in G).\end{aligned}$$

□

Proposition 4.3. 设$H_1, H_2 \in \mathcal{N}$,则$H_1 \cap H_2 \in \mathcal{N}$.

证明. 由$\mathcal{N}$的定义，存在$E_1, E_2 \in \mathcal{I}$使得$H_1 = Gal(K|E_1), H_2 = Gal(K|E_2)$.由于$E_1E_2|k$是有限Galois扩张$E_1E_2 \in \mathcal{I}$.由Galois理论知$H_1 \cap H_2 = Gal(K|E_1E_2)$于是$H_1 \cap H_2 \in \mathcal{N}$.
定义G上的$Krull$拓扑：规定$\{\sigma H : \sigma \in G, H \in \mathcal{N}\}$为$G$上的一个拓扑基。即$G$中子集$H'$为开集当且仅当$H'$为上述拓扑基元素之并。 □

Theorem 4.6. *G在上述拓扑基下为$Hausdorff$,紧致且完全不连通的拓扑群。*

证明. (i)完全不连通(能写成两个非空开子集的不交并，连通子集只有单点集)。
设$X \subset G$,且$|X| \geq 2$,取$\sigma, \tau \in X$,且$\sigma \neq \tau$. 由$\cap_{H\in\mathcal{N}}\sigma H = \{\sigma\}$知$\tau \notin \cap_{H\in\mathcal{N}}\sigma H$,从而$\exists H_0 \in \mathcal{N}$使得$\tau \notin \sigma H_0$,即 $\tau \in G - \sigma H_0$ 注意到

$$X = X \cap G = X \cap (\sigma H_0 \cup (G - \sigma H_0)) = (X \cap \sigma H_0) \cup (X \cap (G - \sigma H_0))$$

G关于子群H有陪集分解$G = \cup_{i\in I}\sigma_i H$,由此知若$H$是开集，由于$G$是拓扑群，对任意$\sigma \in G$,$\sigma H$为开集，从而$H$为其所有非平凡陪集的补集，为闭集。注意到$\sigma \in X \cap \sigma H_0, \tau \in X \cap (G - \sigma H_0)$,且$\sigma H_0, G - \sigma H_0$均为开集，这就得到$X$是完全不连通的。特别地，$G$是完全不连通的，此处还可以看出, G是hausdorff空间。

□

另证:若$\sigma, \tau \in G$且$\sigma \neq \tau$,则存在有限Galois子扩张$E|k$使得$\sigma|_E \neq \tau|_E$(注意到任取$x \in K$,必存在包含x的$K|k$的有限Galois子扩张$E|k$,例如E取$k(x)|k$在$K|k$中的代数闭包。若对任意有限Galois子扩张$E|k$有$\sigma|_E = \tau|_E$,则对任意$x \in K, \sigma(x) = \tau(x)$.矛盾！)因此$\sigma Gal(K|E) \neq \tau Gal(K|E)$,因此$\sigma Gal(K|E) \cap \tau Gal(K|E) = \emptyset$.
对于G的紧性,这里先省略证明。

注:设G关于闭子群H有陪集分解$G = \cup_{i\in I}\sigma_i H$，则由$G$的紧致性,$H$是$G$的开子集当且仅当$(G : H)$有限。

Theorem 4.7. 设$H \leq G$,记$H' = Gal(K|K^H)$,则$H' = \bar{H}$*(H在G中的闭包.)*

证明. 显然，$H \leq H'$.下证H'为G中的闭集,只需证$G - H'$为开集.

任取$\sigma \in G - H'$,必有$\alpha \in K^H$使得$\sigma(\alpha) \neq \alpha$.对于$\alpha \in K$,有$E \in \mathcal{I}$使得$\alpha \in E$,于是取$H_0 = Gal(K|E) \in \mathcal{N}$.对于$\forall \tau \in H_0$,有$\tau\alpha = \alpha$,于是$\sigma(\tau\alpha) = \sigma\alpha \neq \alpha$,即

$$\sigma\tau(\alpha) \neq \alpha \Rightarrow \sigma\tau \in G - H' \Rightarrow \sigma H_0 \in G - H' \Rightarrow G - H \quad is \quad open \Rightarrow H' is \quad closed.$$

下证$\bar{H} = H'$.需证$\forall \sigma \in H', N \in \mathcal{N}$.都有$\sigma N \cap H \neq \emptyset$.
由定义，取$E \in \mathcal{I}$使得$N = Gal(K|E)$,令$H_0 = \{\rho|_E : \rho \in H\}$,于是$K^{H_0} = K^H \cap E$,由有限Galois基本定理到$H_0 = Gal(E|K^H \cap E)$,由$\sigma \in H', \sigma|_{K^H} = id$,因此$\sigma|_E \in H_0$.存在$\rho \in H$使得$\rho|_E = \sigma|_E$.于是$\sigma^{-1}\rho \in Gal(K|E) = N$，即$\rho \in \sigma N \cap H$.$\sigma N \cap H \neq \emptyset$. □

Proposition 4.4. 设$K|k$是无限$Galois$扩张，任取$K|k$的一个中间域，则$H_E = Gal(K|E)$是G的一个闭子群。

证明. $H_E \leq G$,则$K^{Gal(K|E)} = E \Rightarrow H_E = Gal(K|E) = Gal(K|K^{H_E}) = \bar{H}_E$. □

Theorem 4.8. 无限*Galois*扩张基本定理:设$K|k$是无限$Galois$扩张，令$G = Gal(K|k)$, $\mathcal{I}_0 = \{E : E是K|k的中间域\}$, $\mathcal{N}_0 = \{H|H是G的子群\}$.定义映射

$$\varphi : \mathcal{I}_0 \to \mathcal{N}_0$$
$$E \mapsto Gal(K|E)$$

则φ是一个双射。
(1)$E|k$是$Galois \Leftrightarrow H_E = Gal(K|E) \triangleleft G$.
*(2)*对于$E \in \mathcal{I}_0, [E : k] \leq +\infty \Leftrightarrow H_E = Gal(K|E)$是$G$的开子群。*(*若$H$是开子群，则任意$\sigma \in G$,$\sigma H$也是开子群，从而由陪集分解 $G = \cup_{i\in I}\sigma_i H$,知$H$也是闭子群.此时再由$G$的紧致性知$[G : H] \leq +\infty$.反之，若已知$H$是闭集，则由$[G : H] \leq +\infty$知$H$是开集*)*。

4.4 例题

例F_p(p是素数)。

Example 4.2. 分圆域$K = Q(\zeta_n)$,其中$\zeta_n = e^{2i\pi/n} = \cos 2\pi/n + i \sin 2\pi/n \in C$. ζ_n是n次本原单位根，也是代数元. 问：K/Q是否为$Galois$扩张*?*

答：由$char(Q) = 0$知,K/Q是可分的。ζ_n是$x^n - 1$的根. 事实上，K是$x^n - 1$在Q上的分裂域，即K/Q是正规的，因此K/Q是$Galois$扩张。记其$Galois$群为$G = Gal(K/Q)$。

(1)设ζ_n在Q上的极小多项式为$f(x)$，则$f(x) \mid x^n - 1$。
任取$\sigma \in G$，$\sigma(\zeta_n)$⇒是ζ_n的一个共轭元。且$\sigma(\zeta_n)$=$(\zeta_n)^k$, 对某个$k \in \{0, 1, 2, \ldots, n-1\}$.

$$\sigma(\zeta_n)的阶 = r \Rightarrow \sigma(\zeta_n) = 1 \Rightarrow \sigma(\zeta_n^r) = 1 \Rightarrow \zeta_n^r = \sigma(1) = 1 \Rightarrow r = n.$$

注：ζ 是n次本原单位根$\Leftrightarrow$ ζ的阶是n,即$\zeta \in \mathbb{C}^*$且是$\mathbb{C}^*$中的一个阶为n的数，比如上述ζ_n.

$$\circ(\sigma(\zeta_n)) = \circ(\zeta_n^k) = \frac{n}{(n,k)} = n \Leftrightarrow (n,k) = 1.$$

即对$k \in \{0, 1, 2, \ldots, n-1\}$,$\zeta_n^k$是$n$次本原单位根$\Leftrightarrow (n,k) = 1$. 于是，$f(x) = \prod\limits_{k=1,(n,k)=1}^{n} (x - \zeta_n^k)$
显然，$deg(f(x)) = \phi(n)$(Euler函数)称上述$f(x)$为n次分圆多项式，常记之为$f(x) \doteq \phi_n(x)$, 特别地，当$n = p$是一个素数时，

$$\phi_p(x) = \prod_{k=1,(k,p)=1}^{p} (x - \zeta_p^k) = \prod_{k=1}^{p-1} (x - \zeta_p^k) = \frac{x^p - 1}{x - 1} = x^{p-1} + \ldots + x + 1.$$

$\#Gal(K/Q) = [K:Q] = deg(\phi_n(x)) = \phi_n(x)$.(比如$n = p$素数时，$[Q(\zeta_p):Q] = p-1$).

(2)计算$Gal(K/Q)$.

$\forall \sigma \in Gal(K/Q)$, $\sigma : K = Q(\zeta_n) \longrightarrow Q(\zeta_n)$. 事实：$\sigma(\zeta_n)$必是$n$次本原单位根，故$\sigma(\zeta_n) = \zeta_n^k, k \in (\mathbb{Z}/n\mathbb{Z})^*$. 而$\sigma \longrightarrow \overline{k}$建立了Gal(K/Q)到$(\mathbb{Z}/n\mathbb{Z})^*$的映射.
结论：$K = Q(\zeta_n), G$同上，有$(\mathbb{Z}/n\mathbb{Z})^* \backsimeq G = Gal(K/Q)$.

证明. 令

$$\psi : (Z/nZ)^* \longrightarrow Gal(K/Q)$$
$$\overline{k} \longmapsto \sigma_k : \zeta_n \longmapsto \zeta_n^k.$$

群同态：即证明$\psi(\overline{kl}) = \psi(\overline{kl}) = \sigma_k\sigma_l$.

$$\sigma_{kl}(\zeta_n) = \zeta_n^{kl} = (\zeta_n^l)^k = \sigma_k(\sigma_l(\zeta_n)) = (\sigma_k \circ \sigma_l)(\zeta_n).$$

即$\sigma_{kl} = \sigma_k \circ \sigma_l$. 也即$\psi(\overline{kl}) = \psi(\overline{k}) \circ \psi(\overline{l})$
ψ是单的：阶数一样，故证明是双射只需证单。
设$\overrightarrow{k} \in ker\psi$,则$\psi(\overline{k}) = \sigma_k = id$. 即

$$\sigma_k(\zeta_n) = \zeta_n^k = \zeta_n \Rightarrow \zeta_n^{k-1} = 1 \Rightarrow n|(k-1) \Rightarrow k \equiv 1 \pmod{n},$$

即$\overline{k} = \overline{1}. \Rightarrow ker(\psi) = \{\overline{1}\}$.
又$\#Gal(K/Q) = \phi(n) = \#(Z/nZ)^*$,故$\phi$也是满的，从而有$G = Gal(K/Q) \backsimeq (\mathbb{Z}/n\mathbb{Z})^*$. □

$O_k = Z[\zeta_n] \to PID$?

Example 4.3. $K = Q(\sqrt{-1}, \sqrt{2})|Q$是$Galois$扩张？

(1)K/Q是否均$Galois$扩张？
$charQ = 0 \Rightarrow K/Q$可分。
$\alpha = \sqrt{-1}, \beta = \sqrt{2}$。它们在$Q$上的极小多项式分别是:$P_\alpha(x) = x^2+1$, 根为：$\sqrt{-1}, -\sqrt{-1}$;$P_\beta(x) = x^2-2$,根为：$\sqrt{2}, -\sqrt{2}$. $K = Q(\pm\sqrt{-1}, \pm\sqrt{2})$是$\{P_\alpha, P_\beta\}$在Q上的分裂域.$\Rightarrow$ K/Q是正规的,从而K/Q是Galois的，记$G = Gal(K/Q)$. 于是$\#G = [K:Q] = 4, Q \subset Q(\sqrt{-1}) \subset Q(\sqrt{-1}, \sqrt{2}) = K$
(2)计算Galois群
$\forall \sigma \in G, K = Q(\alpha, \beta), \sigma(\alpha) \in \{\sqrt{-1}, -\sqrt{-1}\}, \sigma(\beta) \in \{\sqrt{2}, -\sqrt{2}\}$.
确定：$\sigma : (\alpha, \beta) \longmapsto (\sigma(\alpha), \sigma(\beta))$, $\sigma : (\sqrt{-1}, \sqrt{2}) \longmapsto (\sigma(\sqrt{-1}), \sigma(\sqrt{2}))$.有下列四种情形：

$$a : \sqrt{-1} \longmapsto \sqrt{-1}, \sqrt{2} \longmapsto \sqrt{2}, \text{此时}\sigma = id;$$

$$b : \sqrt{-1} \longmapsto \sqrt{-1}, \sqrt{2} \longmapsto -\sqrt{2}, \text{记为}\sigma_1;$$

$$c : \sqrt{-1} \longmapsto -\sqrt{-1}, \sqrt{2} \longmapsto \sqrt{2}, \text{记为}\sigma_2;$$

$$d : \sqrt{-1} \longmapsto -\sqrt{-1}, \sqrt{2} \longmapsto -\sqrt{2}, \text{记为}\sigma_3;$$

于是$G=\{1,\sigma_1,\sigma_2,\sigma_3\},\sigma_1^2=\sigma_2^2=\sigma_3^2=id,\sigma_3=\sigma_1\sigma_2$,可知

$$G=<\sigma_1,\sigma_2>=<\sigma_1>\times<\sigma_2>\backsimeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}.$$

G的子群为：$\{1\},<\sigma_1>,<\sigma_2>,<\sigma_1\sigma_2>=<\sigma_3>$, G对应的中间域为K.

$$K^{<\sigma_1>}=K^{\sigma_1}=Q(\sqrt{-1}),K^{\sigma_2}=Q(\sqrt{2}),K_3^{\sigma}=Q(\sqrt{-2}).$$

5 环与模的链条件

5.1 环与模的链条件

Theorem 5.1. 设A是一个含幺交换环，M是一个A-模，则下列陈述等价：
*(1)(ACC)(*升链条件*)*：对M中的任意子模升链（可数链） $M_1\subset M_2\subset\ldots\subset M_n\subset\ldots$ 则*(*)*式是稳定的，即存在$n\in Z_{\geq 1},\ddot{}M_n=M_{n+1}=\ldots$
*(2)(*极大条件*)*任意一个由M的子模构成的非空集合均有极大元。*(*集合的包含关系*)*
*(3)(*有限生成条件*)*M的任一子模均是有限生成A-模。

Definition 5.1. 对于$M\in A$-模，如果M满足上述定理的条件，则称M是一个*Noether* A-模。

证明. (1)⇒(2)设$\mathscr{M}$是M的一个子模非空集簇，要证$\mathscr{M}$中含极大元。(反证)假若不然，任取$M_1\in\mathscr{M}$,则M_1不是$\mathscr{M}$中极大元，故有$M_2\in\mathscr{M}\Rightarrow M_1\subsetneqq M_2$.同理，$M_2$也不是$\mathscr{M}$中极大元，故有$M_3\in\mathscr{M}\Rightarrow M_2\subsetneqq M_3$.以此类推即可得到M中一个无限长子模链。$M_1\subsetneqq M_2\subset M_3\subsetneqq\ldots$与所设矛盾！
(2)⇒(3) 任取子模N≤ M,不妨设N≠ 0，下证N是有限生成的。为此，令 $\mathscr{M}=\{L:L\leq N$,且L是有限生成的$\}$.显然，$0\in\mathscr{M}$,故，$\mathscr{M}\neq\Phi$, 由所设，$\mathscr{M}$中含极大元，设其一为N_0. 只需证$N_0=N$。假若$N_0\neq N$，即$N_0\subsetneqq N$。于是有$\alpha\in N\setminus N_0$,令$L_0=<N_0,\alpha>=N_0+A\alpha$则，$L_0\leq N$,且$L_0$是有限生成的，故$L_0\in\mathscr{M}$.但$N_0\subsetneqq L_0$，这与$N_0$的极大性矛盾！因此，$N=N_0$是有限生成的。
(3)⇒(1),任取M的一个可数子模升链，$M_1\subset M_2\subset\ldots$,令$N=\bigcup\limits_{i=0}^{\infty}M_i$,则$N\leq M$,有所设，N是有限生成A-模，即$N=<\alpha_1,\alpha_2,\ldots\alpha_m>=A\alpha_1+\ldots+A\alpha_m,(\alpha_1,\ldots\alpha_m\in N)$由$\alpha_1,\ldots\alpha_m\in N=\bigcup\limits_{i=0}^{\infty}M_i$,故有$r\in Z_{\geq 1}\Rightarrow\alpha_1,\ldots\alpha_m\in M_r\Rightarrow N=<\alpha_1,\alpha_2,\ldots\alpha_m>\subset M_R\subset N\Rightarrow N=M_r\Rightarrow M_r\subset M_{r+k}\subset N=M_r\Rightarrow M_{r+k}=M_r(\forall k\in Z_{\geq 0})$ □

对偶地，有Artin 模

Theorem 5.2. 设A是一个含*1*交换环，M是一个A-模，则下列条件等价：
(1)(DCC)M的任一个可数子模降链均稳定的，即对任一个子模链, $M_1\subset M_2\subset\ldots$则有$n\in Z_{\geq 1}$,使得$M_n=M_{n+1}=\ldots$
*(2)(*极大条件*).*有M的子模构成的任一非空集簇均有极小元。

Noether 模，Artin 模

Definition 5.2. 设A是一个含1交换环，如果A是一个$Noether\ A-$模，则称A是$Noether$ 环。

等价地，A是$Noether$环$\Leftrightarrow$ A的理想均是有限生成的。
对偶地，A是$Artin$环$\Leftrightarrow$ A作为A模是一个Artin模。

Example 5.1. 整数环$\mathbb{Z}Noether$环 (1)满足$acc, I_1 \subset I_2 \subset \ldots I_i = (a_i), (a_1) \subset (a_2) \subset \ldots, (a_1) \subset (a_2) \Leftrightarrow (a_2|a_1), (p) \subset (p), <1>=\mathbb{Z}$.
(2)不满足dcc. 例：$(2) \supset (2^2) \supset (2^3) \supset \ldots$ 可无限下去$(倍)$ 结论：$\mathbb{Z}$是$Noether$环，但不是$Artin$环。

Example 5.2. $G = (\mathbb{Q}/\mathbb{Z}, +)$,(注：$\mathbb{Q}/\mathbb{Z} = (\mathbb{R}/\mathbb{Z})_{tor}$).

$(\mathbb{Z}, +) \subset (\mathbb{R}, +), \mathbb{R}/\mathbb{Z} = [0, 1)$(作为集合)$\simeq (S^1, \cdot)$单位圆.
$(\mathbb{R}/\mathbb{Z}, +)_{tors} = \overline{a} : a \in \mathbb{R}, \circ(a) < \infty$.
设p是一个素数，G的$Sylow - p$子群

$$G(p) = \{a \in G : \circ(a)是p的幂\} = p^{-1}Z/Z \cup p^{-2}Z/Z \cup \ldots = \bigcup_{n=0}^{\infty} p^{-n}Z/Z,$$

$p^{-n}Z/Z \subset p^{-(n+1)}Z/Z, p^{-1}Z/Z \subsetneqq p^{-2}Z/Z \subsetneqq \ldots$(无限升链)
$\Rightarrow Q/Z$不是$NoetherZ-$模。

Example 5.3. $A = k[x]$(k域)A是$PID \Rightarrow$ A是$Noether$的，但A不是$Artin$的,$(x) \supsetneqq (x^2) \supsetneqq \ldots$

Example 5.4. $A = k[x_1, x_2, \ldots]$
A不是$Artin$环,$(x_1) \supsetneqq (x_1^2) \supsetneqq \ldots$; A也不是$Noether$ 环,$(x_1) \subsetneqq (x_1, x_2) \subsetneqq \ldots$
注：A是整环，设F是它的分式域，即$F = FracA$，F是$Noether$的(域中的理想只有0和本身)，$A \subset F$,A不是$Noether$ 的.

(环)Noether性质对子结构不封闭
(模)但M是$NoetherA-$模，$N \subseteq M$，则N也是$NoetherA-$模.原因：子模的子模是子模，N的子模是M的子模$\Rightarrow$有限生成.
$MNoetherA-$模，$N \leq M, NNoether$!
$L \leq N \Rightarrow L \leq M$子模的子模是子模
$M/N, A \times M/N \longrightarrow M/N, (a, \overline{m}) \longmapsto \overline{am}$
$\overline{M} = M/N, \overline{M_1} \leq \overline{M_2} \leq \ldots, N \leq M_i \leq M, \overline{M_i} = M_i/N$
$\Rightarrow M_1 \leq M_2 \leq \ldots$
验证：$\forall \alpha \in M_1, \overline{\alpha} \in \overline{M_1} \subset \overline{M_2} \Rightarrow \overline{\alpha} = \overline{\beta}$ 对某个$\beta \in M_2$.即$\alpha - \beta \in N, \alpha - \beta = \gamma \in N \subset M_2 \Rightarrow \alpha = \beta + \gamma \in M_2$
$\exists n \in Z_{\geq}1$使得$M_n = M_{n+1} = \ldots \Rightarrow \overline{M_n} = \overline{M_n + 1} = \ldots \Rightarrow \overline{M} = M/N$是Noether的.

Theorem 5.3. 设A是交换环,$L,N,M \in A\text{-}Mod$.且有正合列$0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$,则$M$是$Noether$模$L$与$N$均是$Noether\ A$-模。$Artin$仍成立。

证明. $\Rightarrow$ 任取$L_1 \leq L_2$,则$L_1 \leq M$，由所设，知L_1是有限生成的，故是Noether模。任取N的一个子模升链$N_1 \leq N_2 \leq \ldots$则有M的子模升链$f(L) \subset g^{-1}(N_1) \leq g^-1(N_2) \leq \ldots$ 由所设，$\exists m \in Z_{\geq}1$, 使得$g^{-1}(N_m) = g^{-1}(N_m + 1) = \ldots \Rightarrow N_m = g(g^{-1}(N_m)) = g(g^{-1}(N_m + 1)) = N_{m+1} = \ldots \Rightarrow$ N是个Noether A-模。

$\Leftarrow$ 任取M的一个可数子模升链$M_1 \leq M_2 \leq \ldots$ 于是有L中的子模升链$f^{-1}(M_1) \leq f^{-1}(M_2) \leq \ldots$ 及N中的子模升链$g(M_1) \leq g(M_2) \leq \ldots$ 由所设，存在k使得$f^{-1}(M_k) = f^{-1}(M_k + 1) = \ldots$ 且$g(M_k) = g(M_k + 1) = \ldots$

下证$M_k = M_{k+1} = \ldots$,只需证$M_{k+1} \subset M_k$.

为此，任取$\alpha \in M_{k+1}$则$g(\alpha) \in g(M_k + 1) = g(M_k)$即$g(\alpha) = g(\beta)$,对某个$\beta \in M_k$. 也即$g(\alpha - \beta) = 0 \Rightarrow \alpha - \beta \in ker(g) = im(f) = f(L)$即有$\gamma \in L$,使得 $alpha - \beta = f(\gamma)$,又$alpha - \beta \in M_{k+1}$,故$\gamma \in f^{-1}(M_k + 1) = f^{-1}(M_k) \Rightarrow f(\gamma) \in M_k \Rightarrow \alpha = \beta + f(\gamma) \in M_k \Rightarrow M_{k+1} \subset m_k$.从而有$M_{k+1} = M_k$

同理可证$M_{k+1} = M_{k+2} = \ldots$ 因此，M是Noether A-模。 □

Corollary 5.1. *M是Noether模$\Rightarrow M \bigoplus M$是Noether的。*

$$0 \longrightarrow M \longrightarrow M \bigoplus M \longrightarrow M \longrightarrow 0.$$
$$\alpha \longmapsto (\alpha, 0),$$
$$(\alpha, \beta) \longmapsto \beta.$$

Corollary 5.2. *设$M_i (1 \leq i \leq r)$是Noether A-模，则$\bigoplus_{i=1}^{r} M_i$也是Noether模。*

证明. 归纳法：

$$0 \longrightarrow M_1 \longrightarrow M_1 \oplus M_2 \longrightarrow M_2 \longrightarrow 0$$
$$a_1 \longmapsto (a_1, 0),$$
$$(a_1, a_2) \longmapsto a_2.$$

$\Rightarrow M_1 \oplus M_2$是Noether的。

$0 \longrightarrow M_1 \oplus M_2 \longrightarrow M_1 \oplus M_2 \oplus M_3 \longrightarrow M_3 \longrightarrow 0$

一般地.

$$0 \longrightarrow \bigoplus_{i=1}^{r-1} M_i \longrightarrow \bigoplus_{i=1}^{r} M_i \longrightarrow M_r \longrightarrow 0$$

特别地，当M是一个Noether模时，$M^n = M^{\oplus n}$是Noether的。

$M \oplus \ldots \oplus M = M \times \ldots \times M$ □

例.X是紧的Hausdorff拓扑空间，且$\#X = +\infty$.$C(X) = \{f : f是X上的实值函数\}, f : X \longrightarrow R$连续，显然，$(C(X), +, \cdot)$是一个含幺交换环，令$B_1 \supsetneqq B_2 \supsetneqq \ldots$ 是X中一个严格闭子集降链，又令$I_n \lhd C(X)$,且$I_1 \subsetneqq I_2 \subsetneqq I_3 \subsetneqq \ldots$(理想的无限升链)$\Rightarrow C(X)$不是Noether环。

Proposition 5.1. *Noether环上的有限生成模必是Noether模。*

证明. 设A是Noether环，M是一个有限生成A-模，即$M = A\alpha_1 + A\alpha_2 + \ldots + A\alpha_r, \alpha_1, \ldots$ fi$\alpha_r \in M$. 显然有A-模满同态$\Phi : A^r \longrightarrow M, (a_1, \ldots, a_r) \longmapsto a_1\alpha_1 + \ldots + a_r\alpha_r$.由所设，A是Noether环，故A也是一个Noether A-模，于是A^r也是Noether A-模，从而M是Noether的。 □

设M∈ A-Mod，设有子模降链：$M = M_0 \supset M_1 \supset \ldots \supset M_r = \{0\}(*)$,且$M_i/M_{i+1}$ 是单模，$(i = 0, 1, \ldots, r-1)$此时称$(*)$是M的一个合成列，称r为M的长度，记为r=L(M)，这样的M就成为是一个有限长模.(Jordan-Holder 定理)

Theorem 5.4. 设A是一个交换环，M∈ A-Mod,则M是有限长模⇔ M既是$Noether$模，也是$Artin$模。

证明. ⇒ 显然，M是有限长模则不可能有无限升链，也不可能有无限降链。⇐ $M \neq 0$.令$\mathscr{N}$={N:N≤ M且N≠ M}≠ ∅.则$0 \in \mathscr{N}$，由于M 是Noether模，故$\mathscr{N}$中含极大元，取其中一个为M_1，则M/M_1是单模，且M_1 也是Noether的。当M_1=0 时，已证;当$M_1 \neq 0$时，则对M_1用上述讨论可得$M_2 \leq M_1, M_2 \neq M_1$,且$M_1/M_2$是单的，以此类推，可得M的子模的严格降链：$M = M_0 \supsetneqq M_1 \supsetneqq M_2 \supsetneqq \ldots (*)$
由所设，M是Artin的，故$(*)$必是稳定的，从而由上述讨论可知，$\exists r \in Z_{\geq}1$,使得M_r=0.因此得M的合成列：$M = M_0 \supset M_1 \supset \ldots \supset M_r = \{0\}$ □

Theorem 5.5. *(Hilbert基本定理) Noether*环上的多项式环必是*Noether*环。具体言之，设A是一个*Noether*环，$x_1, \ldots, x_n$是n个未定元，则A 上的多项式环$A[x_1, \ldots, x_n]$是*Noether*环。

证明. 只需证$A[x]$是$Noether$环，其中x是未定元。为此任取$A[x]$中一个非零理想$\mathscr{A}$，令$I = \{a \in A : \exists f \in \mathscr{A},$ 使得a是f的首项系数}则$I \lhd A$.事实上，显然$0 \in I$,设$a, b \in I$,则有$f, g \in \mathscr{A}$.使得a, b分别是f, g的首项系数。不妨设

$$f(x) = ax^m + \ldots,$$

$$g(x) = bx^n + \ldots.$$

且设$m \geqslant n$，则$f(x) + g(x)x^{m-n} \in \mathscr{A}$且其首项系数均为$a + b$.$I \lhd A$. 由所设，$A$是$Noether$环，故$I$是有限生成的，即$I =< a_1, \ldots, a_s >$,其中$a_1, \ldots, a_s \in A$. 由所设，对每个$a_i, \exists f_i \in \mathscr{A}$,使得$a_i$是$f_i$的首项系数。记$m_i = deg(f_i), m = max\{m_i : i = 1, \ldots, s\}$(规定$deg0 = \infty$)记$\mathscr{A}' =< f_1, \ldots, f_s >$(在$A[x]$中生成)，显然$\mathscr{A} = \mathscr{A}'$. 又记$\mathscr{B} = A + Ax + \ldots + Ax^{m-1}$是由$\{1, x, \ldots, x^{m-1}\}$生成的$A-$模. 任取$f \in \mathscr{A}$,如果$deg(f) < m$,则$f \in b$.如果$deg(f) = n \geq m$.此时设$f$的首项系数为$a$.则$a \in I$, 于是有$a = c_1a_1 + \ldots + c_sa_s$, 其中$c_1, \ldots, c_s \in A$.令$g(x) = f(x) - \sum_{i=1}^{s} c_ix^{n-mi}f_i$. 则$g(x) \in \mathscr{A}$,但此时$deg(g(x)) < n$.以此类推，有限步后，可得$f(x) = h(x) + l(x)$,其中$h(x) \in \mathscr{A}', l(x) \in \mathscr{A} \cap \mathscr{B}$,(因为$f, h \in \mathscr{A} \Rightarrow l \in \mathscr{A}$) 即$f(x) \in \mathscr{A}' + (\mathscr{A} \cap \mathscr{B}) \Rightarrow \mathscr{A} \subset \mathscr{A}' + (\mathscr{A} \cap \mathscr{B}) \Rightarrow \mathscr{A} = \mathscr{A}' + (\mathscr{A} \cap \mathscr{B})$ 注意到A是Noether环，$\mathscr{B}$是有限生成$A-$模，故$\mathscr{B}$是Noether $A-$模⇒ $\mathscr{A} \cap \mathscr{B}$也是$Noether A-$模，故有$g_1, \ldots, g_t \in \mathscr{A} \cap \mathscr{B}$,使得 $\mathscr{A} \cap \mathscr{B} = Ag_1 + \ldots + Ag_t \Rightarrow \mathscr{A} = \mathscr{A}' + Ag_1 + \ldots + Ag_t \subset \mathscr{A}' + A[x]_{g_1} + \ldots + A[x]_g \subset \mathscr{A}. \Rightarrow \mathscr{A} =< f_1, \ldots, f_s, g_1, \ldots, g_t >$. □

Hilbert基定理

设A是Noether环，则A上的多项式环$A[x_1,\ldots,x_n]$也是Noether环。

Proposition 5.2. *A与B是交换环，$A\subset B$，设A是Noether环，B是有限生成$A-$模，则B是一个Noether环。*

证明. 任取$I\lhd B$ (理想)，由所设，B是有限生成$A-$模，另一方面，显然I是B的一个$A-$子模，$(A\subset B)$.从而I 使有限生成A模，即有$I=A\alpha_1+\ldots+A\alpha_m$.其中$\alpha_1,\ldots,\alpha_m\in I\subset B$.于是$I=A\alpha_1+\ldots+A\alpha_m\subset B\alpha_1+\ldots+B\alpha_m\subset I\Rightarrow I=B\alpha_1+\ldots+B\alpha_m$即$I$是$B$中有限生成理想，因此$B$是一个Noether环。 □

Proposition 5.3. *设A是一个交换环，S是A的一个乘法闭子集，如果A是一个Noether环，则分式环$S^{-1}A$也是Noether环。*

证明. 任取$S^{-1}A$中理想J，则$J=S^{-1}I$,其中$I\lhd A$。由所设，I是有限生成的，即$I=A\alpha_1+\ldots+A\alpha_m$,其中$\alpha_1,\ldots,\alpha_m\in A.\Rightarrow J=S^{-1}I,=S^{-1}A\alpha_1+\ldots+S^{-1}A\alpha_m$.即$J$是$S^{-1}A$的有限生成理想$\Rightarrow$ $S^{-1}A$ 是Noether环。特别地，任取$P\in Spec(A)$(A的素理想集)，$A_p=S^{-1}A$,其中$A=A\setminus P$. □

Corollary 5.3. *A是Noether环，则A_p是Noether环。*

多项式及多项式组的零点(system)

1.一个变量

$f(x)\in R[x].f(x)=x^2-2x+1,y=ax^2+bx+c(a>0).R$不是代数封闭域

$y=f(x),2\nmid deg(f)$,图像一定过x轴,$x\to+\infty,2\nmid n$. 2.两个变量的情形

$f(x,y)=ax+by+c.(a,b,c\in R,a,b$不同时为0) $f(x,y)=0,f(p)=0,f(x,y)=x^2+y^2-r^2,$

$f(x,y)=x^2+y^2+1.$

设k是一个代数封闭域，考虑k上的多项式环，$A=k[x_1,\ldots,x_n].f\in A,k^n$为$k$上$n$维仿射空间。记$Z(f)=\{p=(a_1,\ldots,a_n)\in k^n:f(p)=0\}$.同样地，任取$I\subset A,Z(I)=\{p\in k^n:f(p)=0,(\forall f\in I)\}$,称$Z(f)$为$f$在$k$上的零点集。显然，$Z(1)=Z(c)=\varnothing(c\in k^*),Z(0)=k^n.$

$f\in A$,令$I=I(f)=<f>=Af$,为f在A中生成的理想。$Z(f)=Z(<f>)=Z(Af),p\in Z(f)\Rightarrow f(p)=0\Rightarrow p\in Z(<f>)=Z(Af),\forall g\in<f>$,有$g=fh,h\in A.g(p)=f(p)h(p)=0.$

事实上:(1)$Z(f)=Z(<f>)$.(2)任取$S\subset A,S\neq\varnothing$,有$Z(S)=Z(<S>)$.

对$\forall a\lhd A,Z(a).$

Proposition 5.4. *对A中的任一真理想a，有$Z(a)\neq\varnothing$.*

Theorem 5.6 (Hilbert零点定理(Hilbert's Nullstellensatz)). *设k是一个代数封闭域，$A=k[x_1,\ldots,x_n]$是k上的多项式环，$a\lhd A$是A的一个真理想。$f\in A\setminus 0$,如果$Z(f)\subset Z(a)$,即$f(p)=0(\forall p\in Z(a))$.则存在$r\in Z_{\geqslant}1$, 使得$f^r\in A$.(即$f\in\sqrt{a}=rad(a)-a$的根理想)。*

证明. 引入一个变量y，令$B=k[x_1,\ldots,x_n,y]$,为方便记，简记$X=[x_1,\ldots,x_n]$,在B中考虑由a与$(1-fy)$生成的理想a'，即$a'=<a\cup(1-fy)>$(在B中)。断言：$a'=<1>$.假若不然，则a'为B中的真

理想，于是$Z[a'] \neq \varnothing$.特别地，有$P = (a_1, \ldots, a_n, b) \in k^n \times k$,且$(1 - fy)(P_0) = 1 - f(p_0)b = 0(*)$但另一方面，有所设，$P_0 \in Z(a) \subset Z(f)$,故有$f(P_0) = 0$,与$(*)$矛盾！因此，$a' =< 1 >$.于是

$$1 = g_1h_1 + \ldots + g_sh_s + (1 - fg)h.(**)$$

其中$g_i = g_i(x) = g_i(x_1, \ldots, x_n) \in a, h_i = h_i[x, y] \in B, h = h(x, y) \in B, X = (x_1, \ldots, x_n)$.在$(**)$中取$y = \frac{1}{f}$,得

$$1 = g_1(x)h_1(x, \frac{1}{f}) + \ldots + g_s(x)h_s(x, \frac{1}{f}) = \frac{1}{f^r}(g_1(x)f_1(x) + \ldots + g_s(x)f_s(x)),$$

$\Rightarrow f^r = g_1(x)f_1(x) + \ldots + g_s(x)f_s(x) \in a.$ □

5.2 域的Galois扩张例子选讲

Example 5.5. *(三次扩域)*

设$f(x) = x^3 + ax + b \in \mathbb{Q}[x]$,是$\mathbb{Q}$上不可约多项式，设$\alpha_1 = \alpha, \alpha_2, \alpha_3$为$f(x)$在$C$中的全部根，令$k = \mathbb{Q}(\alpha)$,则$[K : \mathbb{Q}] = deg(f) = 3$.又记$K = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$为$f$在$\mathbb{Q}$上的分裂域。$K/\mathbb{Q}$是$Galois$的$\Leftrightarrow k = K$.

(1)$K/\mathbb{Q}$是$Galois$的记$G = Gal(K/\mathbb{Q})$,任取$\sigma \in G : \alpha_1 \longmapsto \sigma(\alpha_1), \alpha_2 \longmapsto \sigma(\alpha_2), \alpha_3 \longmapsto \sigma(\alpha_3)$.

$$f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3) = x^3 + ax + b$$

$$f(x) = \sigma(f(x)) = (x - \sigma(\alpha_1))(x - \sigma(\alpha_2))(x - \sigma(\alpha_3)).$$

σ 只作用在系数上。

$\Rightarrow (\sigma(\alpha_1), \sigma(\alpha_2), \sigma(\alpha_3))$是$(\alpha_1, \alpha_2, \alpha_3)$的一个置换，于是有映射

$$G \longrightarrow S_3, \sigma \longmapsto (\sigma(1), \sigma(2), \sigma(3)).$$

且显然是单一群同态.像相同原像相同.$\Rightarrow \#G||S_3| = 6 \Rightarrow |G| = 3$或6.

令$S = (\alpha_1 - \alpha_2), (\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1)$, f的判别式即是$\Delta = S^2$,(注：一般地，对于多项式$f(x) = a\prod_{i=1}^{n}(x - \alpha_i)$,则$\sigma(f) = \prod_{1 \leqslant i \leqslant j}(\alpha_i - \alpha_j)^2$

如：$f(x) = x - \alpha$,

$$f(x) = x^2 + ax + b = (x - \alpha_1)(x - \alpha_2).\Delta = a^2 - 4b,$$

$$\Delta = (\alpha_1 - \alpha_2)^2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 = (-a)^2 - 4b = a^2 - 4b.$$

$\delta = (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1), \sigma(\delta) = (\sigma(\alpha_1) - \sigma(\alpha_2))(\sigma(\alpha_2) - \sigma(\alpha_3))(\sigma(\alpha_3) - \sigma(\alpha_1)) = \delta$ 或$-\delta$

且$\sigma(\delta) = \delta \Leftrightarrow \sigma \in A_3$(偶置换),

$sigma(\Delta) = \sigma(\delta^2) = \Delta(\Delta \in \mathbb{Q})$多项式系数在哪里，$\Delta$ 就在哪里。

$\sigma(\Delta) = \Delta(\forall \sigma \in G) \Rightarrow \Delta \in K^G = \mathbb{Q}$

由上述讨论可知

$$\delta \in \mathbb{Q} \Leftrightarrow \delta \in K^G \Leftrightarrow \sigma(\delta) = \delta(\forall \sigma \in G) \Leftrightarrow G = A_3.$$

又$\delta \in \mathbb{Q} \Leftrightarrow \Delta = \delta^2 \in \mathbb{Q}^2$

结论：对于上述$k = \mathbb{Q}(\alpha), K/\mathbb{Q}$是Galois扩张$\Leftrightarrow k = K \Leftrightarrow G = Gal(K/\mathbb{Q}) = A_3 \Leftrightarrow \Delta \in \mathbb{Q}^2$(即$\delta \in \mathbb{Q}$).

对于上述$f(x) = x^3 + ax + b, \Delta(f) = -4a^3 - 27b^2$.

例如，(1)取$f(x) = x^3 - x - 1, f(\alpha) = 0.\Delta(f) = -4(-1)^3 - 27 = 4 - 27 = -23$不属于$\mathbb{Q}^2$。故$\mathbb{Q}(\alpha)/\mathbb{Q}$不是Galois 扩张。对于$f$在$\mathbb{Q}$上的分裂域$K$，有$Gal(K/Q), \simeq S_3$.

(2)$f(x) = x^3 - 3x + 1, \Delta(f) = -4(-3)^3 - 27 = 81 = 9^2 \in \mathbb{Q}^2$.$\mathbb{Q}(\alpha)/\mathbb{Q}$是Galois的且$Gal(\mathbb{Q}(\alpha)/\mathbb{Q}) = A_3$.

Example 5.6. 设$f(x) = x^4 - 2 \in \mathbb{Q}[x]$.

则$f(x)$在$\mathbb{Q}$上不可约(爱森斯坦判别法，$p = 2$)，记$\alpha = \sqrt[4]{2}$,则f在C中的所有根为 $\alpha, i\alpha, i^2\alpha, i^3\alpha (i = \sqrt{-1})$,于是$f$在$\mathbb{Q}$上的分裂域为$K = \mathbb{Q}(\alpha, i\alpha, i^2\alpha, i^3\alpha) = \mathbb{Q}(\alpha, i) = \mathbb{Q}(\beta)$.

$K/\mathbb{Q}$是$Galois$扩张且$[K : \mathbb{Q}] = [K : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \times 4 = 8, K = \mathbb{Q}(\alpha, i) = \mathbb{Q}(\alpha)(i)$.

记$G = Gal(K/\mathbb{Q})$,下面计算G，任取$\sigma' \in G$

$$\sigma' : K \longrightarrow K, \sigma'(\alpha, i) \longmapsto (\sigma'(\alpha), \sigma'(i)),$$
$$\sigma'(\alpha) = \{\alpha, i\alpha, i^2\alpha, i^3\alpha\}, \sigma'(i) = \{i, -i\}.$$

令

$$\tau : i \longmapsto -i, \alpha \longmapsto \alpha,$$
$$\sigma : i \longmapsto i, \alpha \longmapsto i\alpha.$$

于是$\tau, \sigma \in G = Gal(K/Q)$且$\tau^2 = id$

$$\sigma(i) = \sigma^2(i) = \sigma^3(i) = \ldots = i;$$
$$\sigma^2(\alpha) = \sigma(i\alpha) = \sigma(i)\sigma(\alpha) = i(i\alpha) = -\alpha = i^2\alpha;$$
$$\sigma^3(\alpha) = \sigma(\sigma^2(\alpha)) = \sigma(-\alpha) = -\sigma(\alpha) = -i\alpha = i^3\alpha;$$
$$\sigma^4(\alpha) = \sigma(\sigma^3(\alpha)) = \sigma(-i\alpha) = -i\sigma(\alpha) = \alpha.$$

即$\sigma^4 = id$.故在G中，阶$\circ(\tau) = 2, \circ(\sigma) = 4$,事实：$G =< \sigma, \tau >$,且$\#G = 8$(由扩张次数即知)

$G \supset < \sigma, \tau >, G \supset < \sigma >$,但$\tau$ 不属于$< \sigma >$,故 $\# < \sigma, \tau >> 4. \Rightarrow \# < \sigma, \tau > \geqslant 8$

G中的二阶元:$\circ(\tau) = 2, \circ(\sigma^2) = 2, \circ(\tau\sigma^2) = 2, \circ(\sigma^2\tau) = 2, \circ(\sigma\tau) = 2.$

关系：

$$\tau\sigma\tau^{-1} = \tau\sigma\tau = \sigma^{-1} = \sigma^3.$$

G共有五个二阶子群，分别为：

$$< \tau >, < \sigma^2\tau >, < \sigma^2 >, < \sigma\tau >, < \sigma^3\tau >$$

所对应的中间域分别为：

$$Q(\alpha), Q(i\alpha), Q(\alpha^2 + i), Q((i+1)\alpha), Q((i-1)\alpha).$$

G共有三个四阶子群，分别为：

$$< \tau, \sigma^2 >, < \sigma >, < \sigma^2, \tau\sigma >,$$

所对应的中间域分别为：

$$Q(\sqrt{2}), Q(i), Q(\sqrt{-2}).$$

Example 5.7. 设k是一个域，$t_1, \ldots, t_n$是n个在k上代数无关的元,(未定元)考虑域$K = k(t_1, \ldots, t_n)$,显然，n次对称群S_n可作用于集合$\{t_1, \ldots, t_n\}$上，即对$\forall \sigma \in S_n$,令 $\sigma(t_1, \ldots, t_n) = (t_{\sigma(1)}, \ldots, t_{\sigma(n)})$由此导出，$K$到自身的一个$k-$自同构，仍记为$\sigma$.即$\sigma \in Aut_k(K)$,事实上，得到单一群同态$S_n \hookrightarrow Aut_k(K)$于是，可把$S_n$ 看作$Aut_k(K)$的子群.令$E = K^{S_n}$,则由$Artin$定理可知，K/E是$Galois$的.且$Gal(K$ S_n.

$f \in E \Leftrightarrow \sigma(f) = f(\forall \sigma \in S_n)$其中 $\sigma(f(t_1, \ldots, t_n)) = f(t_{\sigma(1)}, \ldots, t_{\sigma(n)})$即$f$是关于$t_1, \ldots, t_n$的对称多项式$\Rightarrow$ $f = g(s_1, \ldots, s_n)$,其中$g \in K, s_1, \ldots, s_n$是关于$t_1, \ldots, t_n$的全部初等对称多项式$\Rightarrow$ $E = k(s_1, \ldots, s_n)$.

另一方面，对$\forall h \in k(s_1, \ldots, s_n)$,显然有$\sigma(h) = h(\forall \sigma \in S_n) \Rightarrow k(s_1, \ldots, s_n) \subset E$,因此$E = k(s_1, \ldots, s_n)$, 即

$$K^{S_n} = k(t_1, \ldots, t_n)^{S_n} = k(s_1, \ldots, s_n),$$

又，令$f(x) = (x - t_1) \ldots (x - t_n)$,则$K = k(t_1, \ldots, t_n)$是$f$在$k$上的分裂域，$f$可分，$f(x) \in F[x]$,其中$E = k(s_1, \ldots, s_n) \Rightarrow K/E$ 是$Galois$扩张，且$Gal(K/E) = S_n$.
*(Galois逆问题).*任给一个有限群H，是否有有理数域$\mathbb{Q}$的$Galois$扩张K，使得$Gal(K/\mathbb{Q}) = H$?

Example 5.8. 复数域$\mathbb{C}$是一个代数封闭域.*(代数基本定理)*

证明. 3个事实:(0)任意非负实数均是某个实数的平方.$\alpha \in R_{\geqslant 0}, \alpha = \beta^2$
(1)奇次数实系数多项式必有实数根.(用连续性)
(2)$R(i)$中任意元素在$R(i)$中均有一个平方根.(假设不知是$\mathbb{C}$)即$\forall \alpha = a + bi \in R(i)(a, b \in R)$都有$\alpha = (c + di)^2$,其中$c^2 = \frac{a+\sqrt{a^2+b^2}}{2}, d^2 = \frac{-a+\sqrt{a^2+b^2}}{2}$
下证$R(i)$是代数封闭的.

为此，任取$R(i)$中一个有限扩域K，则K/R是有限扩张，设L是K/R的一个正规闭包，记$G = Gal(L/R)$，显然,$2 = [R(i) : R]|[L : R]$.即$2|\#G$.令H为G的$Sylow - 2$子群，记E为L对R的对应于H的中间域，则$2 \nmid [E : R]$,即E为R 的奇数次扩张，又由本原元素定理，$E = R[\alpha]$,对某个$\alpha \in E$,设α 在R上的极小多项式为$P_\alpha(x)$. 则$P_\alpha(x) \in R[x], 2 \nmid deg(P_\alpha(x))$,且$P_\alpha(x)$在$R$上不可约，于是由前面的事实(1)可知，$deg(P_\alpha(x)) = 1$,即$\alpha \in R \Rightarrow E = R \Rightarrow G = H$,即$G$是一个$2-$群，记$\#G = 2^r$,下证$r = 1$.
为此，记$G_0 = Gal(L/R(i))$,则$\#G_0 = 2^{r-1}$.假若$r - 1 > 0$,则G_0由一个2^{r-2}阶子群H_0,且令$E_0 = L^{H_0}$,则$[E : R(i)] = [G_0 : H_0] = 2$,即$E_0$是$R(i)$的二次扩域，与事实(2)矛盾.$\Rightarrow$ $r = 1 \Rightarrow L = R(i) \Rightarrow K = R(i)$,即$R(i)$是代数封闭的。 □

Example 5.9. 设p是一个素数，$f(x) \in \mathbb{Q}$是$\mathbb{Q}$上的p次不可约多项式，如果f恰有两个非实的复根，则f在$\mathbb{Q}$上的分裂域的$Galois$群即是S_p*(p次对称群)*。

证明. 用到如下事实：S_p可由p-循环$(12\dots p)$与任一个对换生成.($S_P =< 12\dots p, tau > \tau = (mn)$是个对换),记$K$为$f$在$\mathbb{Q}$上的分裂域，且设$\alpha$为$f$在$\overline{\mathbb{Q}}$中的一个根，并记$F = \mathbb{Q}(\alpha)$,则$[F:\mathbb{Q}] = degf = p \Rightarrow p|[K:\mathbb{Q}] = \#G$,其中$G = Gal(K/\mathbb{Q})$,即$G$中含有$p$阶元，又$G \leqslant S_p$,由置换群的性质可知，$S_p$中的$p$阶元必与$p$轮换$(12\dots p)$共轭，又由所设，$f(x)$有$p-2$个实根 $\alpha_1, \dots \alpha_{p-2}$, 及一对共轭复根$\beta, \overline{\beta}$.

令

$$\tau : K \longrightarrow K$$

$$\alpha_i \longmapsto \alpha_i$$

$$\beta \longmapsto \overline{\beta}$$

$$\overline{\beta} \longmapsto \beta$$

则$\tau \in S_n$,是一个对换$\Rightarrow G = S_p$. □

如$f(x) = x^5 - 4x + 2$,则f在$\mathbb{Q}$上的分裂域K的Galois群即为S_5.

$f'(x) = 5x^4 - 4, x = \pm\sqrt[4]{\frac{4}{5}}$.

$f''(x) = 20x^3, f''(-\sqrt[4]{\frac{4}{5}}) < 0$极大值点，$f''(\sqrt[4]{\frac{4}{5}}) > 0$极小值点。