模

2025 年 5 月 2 日

目录

1 模和范畴

这个章节我们讲$R-$模，其中R是交换环。若R是主理想整环，则有限生成的$R-$模分类诶出了一切有限生成阿贝尔群的分类。且由典范型构成的有限维向量空间上一切线性变换的分类。在之后，引入非交换环之后，定义这些环上的模，它们将用来证明每个$p^m q^n$阶有限群都是可解群。其中p, q是素数。

2 模

一个$R-$模指的是"环R上的向量空间"。在向量空间的定义中，允许标量在R中而不是在域中。

2.1 定义：模

设R是交换环，$R-$模是指配置了标量乘法$R \times M \to M$的加法阿贝尔群M，其中标量乘法记为

$$(r, m) \mapsto rm$$

且使得下列公理对一切$m, m' \in M$和$r, r', 1 \in R$都成立：

1 $r(m + m') = rm + rm'$

2 $(r + r')m = rm + r'm$

3 $(rr')m = r(r'm)$

4 $1m = m$

注： 若上述R是非交换的，则称M为左$R-$模

例子：

- 域k上的每个向量空间都是$k-$模
- 每个阿贝尔群都是$Z-$模

2.2 定义

若R是环且M,N是$R-$模，则如下定义的函数$f:M\to N$称为 $R-$同态（或者$R-$映射）：

- $f(m+m')=f(m)+f(m')$
- $f(rm)=rf(m)$

对一切$m,m'\in M$和一切$r\in R$成立，若$R-$同态是双射，则说他是$R-$同构。记为$M\cong N$。

注： 若f是$R-$同构，则逆f^{-1}也是$R-$同构

2.2.1 例子

1 $Z-$模是阿贝尔群，且每个群的同态是$Z-$映射。

2 设$T:V\to V$是域k上向量空间V的一个线性变换，现在设$v_1,\cdots,v_n$是V的基。并设A是T关于这个基的矩阵，我们证明两个$k[x]-$模，V^T和$(k^n)^A$同构[1]

定义$\varphi:V\to k^n$为$\varphi(v_i)=e_i$，其中$e_1,\cdots,c_n$是k^n的标准基。线性变换φ是向量空间的同构，为了证明φ是$k[x]-$映射，只需要证明$f(x)\in k[x]$和一切$v\in V$有$\varphi(f(x)v)=f(x)\varphi(v)$。现在

$$\begin{aligned}\varphi(f(x)v_i)&=\varphi(T(v_i))\\&=\varphi\left(\sum a_{ji}v_j\right)\\&=\sum a_{ji}\varphi(v_j)\\&=\sum a_{ji}e_j,\end{aligned}$$

为A的第i列。对于另一方面，

$$f(x)\varphi(v_i)=A\varphi(v_i)=Ae_i$$

是关于A的第i列。因此对一切$v\in V$有$\varphi(f(x)v)=f(x)\varphi(v)$。最后，只需要对$\deg(f)$用归纳法就可以证明完了

下述命题推广了上述例子2

[1] $V^T=T(V),(k^n)^A=Ak^n$

2.3 命题

设V是域k上的向量空间，并设$T,S:V\to V$是线性变换。则例2的$k[x]-$模V^T和V^S是$k[x]-$同构的当且仅当存在向量空间的同构$\varphi:V\to V$使得

$$S=\varphi T\varphi^{-1}$$

证明： 若$\varphi:V^T\to V^S$是$k[x]-$同构，则$\varphi:V\to V$是向量空间的同构使得对一切$v\in V$和$f(x)\in k[x]$有

$$\varphi(f(x)v)=f(x)\varphi(v)$$

特别的，若$f(x)=x$，则

$$\varphi(xv)=x\varphi(v)$$

那么对于两个线性变换T,S，有

$$\varphi(T(v))=S(\varphi(v))$$

因此

$$\varphi T=S\varphi\Rightarrow S=\varphi T\varphi^{-1}$$

反之，在$\deg(f)\leq 1$的特殊情况中假定$\varphi(f(x)v)=f(x)\varphi(v)$，因为

$$\varphi(xv)=\varphi(T(v))=S\varphi(v)=x\varphi(v)$$

最后也是，对$\deg(f)$用归纳法即可证明$\varphi(f(x)v)=f(x)\varphi(v)$

2.4 命题

设k是域，并设A,B是元素在k中的$n\times n$矩阵。则例2中的$k[x]-$模$(k^n)^A$和$(k^n)^B$是$k[x]-$同构的当且仅当存在非奇异矩阵P使得

$$B=PAP^{-1}$$

证明： 我们定义$T:k^n\to k^n$为$T(y)=Ay$，其中$y\in k^n$是列向量，我们有$k[x]-$模$(k^n)^A$，同样的，定义$S:k^n\to k^n$为$S(y)=By$，并记相应的$k[x]-$模为$(k^n)^B$。命题2.3告诉了我们同构$\varphi:V^T\to V^S$满足

$$\varphi(Ay)=B\varphi(y)$$

注意定义2.2，这是一个线性变换。那么存在矩阵P使得$\varphi y = Py$。上述等式变为

$$PAy = BPy$$

就有$PA = BP$。也就是$B = PAP^{-1}$

反之，非奇异矩阵P给出$B = PAP^{-1} \Rightarrow BP = AP$注意$\varphi y = Py$。就有$\varphi : (k^n)^A \to (k^n)^B$是一个$k[x]-$模同构

2.5 定义

若M和N是$R-$模，则

$$\mathrm{Hom}_R(M, N) = \{一切M \to N的R-同态\}$$

若$f, g \in \mathrm{Hom}_R(M, N)$，则定义$f + g : M \to N$为

$$f + g : m \mapsto f(m) + g(m)$$

2.6 命题

若M, N是$R-$模，其中R是交换环，则$\mathrm{Hom}_R(M, N)$是$R-$模,其中加法如定义2.5一样，标量乘法由

$$rf : m \mapsto f(rm)$$

给出。此外并带有分配律：若$p : M' \to M$和$q : N \to N'$，则对一切$f, g \in \mathrm{Hom}_R(M, N)$有

$$(f + g)p = fp + gp, \quad q(f + g) = qf + qg$$

证明： 略，验证定义即可。注意需要用到R的交换性。

我们现在证明对阿贝尔群和对向量空间建立的这些结构也可以用到模上。一般来说，子模指的是一个较大的$R-$模中的$R-$模。如果有$s, s' \in S$和$r \in R$，则$s + s'$和rs在S中和在M中有同样的意义。

2.7 定义：子模

若M是$R-$模，则M的子模N指的是M的加法子群N，它在标量运算下封闭，只要$n \in N$和$r \in R$就有$rn \in N$，记为$N \subseteq M$

例子

- 真子模指的是$N \subseteq M$时有$N \neq M$。
- $Z-$模的子模是子群，而向量空间的子模是子空间。
- 若J是R中的理想，M是$R-$模，则

  $$JM = \left\{ \sum_i j_i m_i : j_i \in J, m_i \in M \right\}$$

  是M的子模
- 若$\{S_i : i \in I\}$是模M的子模族，则$\cap_{i \in I} S_i$也是M的子模。
- 若M是$R-$模和$m \in M$，那么m生成的子模指的是

  $$\langle m \rangle = \{rm : r \in R\}$$

  更一般的。若X是$R-$模M的子集，则

  $$\langle X \rangle = \left\{ \sum r_i x_i : r_i \in R, x_i \in X \right\}$$

  是X中一切$R-$线性组合的集合，称它为X生成的子模。

2.8 定义: 有限生成

我们说模M是有限生成的，若M是一个有限集生成的，即存在有限集合$X = \{x_1, \cdots, x_n\}$使得$M = \langle X \rangle$。

若把X看做是一组基，那么一个由X生成的线性空间就是由X有限生成的。

2.9 定义：核

若$F : M \to N$是$R-$模之间的$R-$映射，则

$$\ker f = \{m \in M : f(m) = 0\}$$

并且

$$\mathrm{im} f = \{n \in N : \exists m \in M \text{ s.t. } n = f(m)\}$$

容易验证$\ker f$是M的子模，并且$\mathrm{im} f$是N的子模，假设$M = \langle X \rangle$，即M由子集X生成，进一步假设N是模切$f, g : M \to N$是$R-$同态，若f, g在X上一致[2]。则$f = g$

2.10 定义：商模

若N是$R-$模M的子模，则商模指的是商群M/N附有标量乘法

$$r(m + N) = rm + N$$

可以简单验证由函数$m \mapsto m + N$给出的自然映射$\pi : M \to M/N$是$R-$映射.

[2]即对一切$x \in X$有$f(x) = g(x)$

2.11 定理：第一同构定理

若$f : M \to N$是模的$R-$映射，则存在$R-$同构

$$\varphi : M/\ker f \to \mathrm{im} f$$

它由

$$\varphi : m + \ker f \mapsto f(m)$$

给出

证明： 若单纯把M和N看做是阿贝尔群，则群的第一同构定理讲的是$\varphi : M/\ker f \to \mathrm{im} f$是阿贝尔群的同构。现在，$\varphi$是$R-$映射：$\varphi(r(m+N)) = \varphi(rm+N) = f(rm)$，但因为$f$是$R-$映射，所以正如我们需要的，$f(rm) = rf(m) = r\varphi(m+N)$

2.12 第二同构定理

若S和T是模M的子模，则存在$R-$同构

$$S/(S \cap T) \to (S+T)/T$$

证明： 令$\pi : M \to M/T$是自然映射，那么$\ker \pi = T$，现在，定义$h = \pi \mid S$，从而有$h : S \to M/T$，就有

$$\ker h = S \cap T$$

由群的第二同构定理，那么$\mathrm{im} h$里面有一些形如$s+T$的代表元，那么h可以由$h : S \to (S+T)/T$定义，应用第一同构定理在h上就有了我们要的东西了。

2.13 第三同构定理

若$T \subseteq S \subseteq M$是子模的塔，则存在$R-$同构

$$(M/T)(S/T) = M/S$$

证明： 定义映射$g : M/T \to M/S$是陪集扩大，即

$$g : m + T \mapsto m + S$$

g是良定义的，若$m + T = m' + T$，则$m - m' \in T \subseteq S$，从而有$m + S = m' + S$，此外

$$\ker g = S/T$$

那么所有$m + S$组成商群M/S，因此

$$\mathrm{im} g = M/S$$

应用第一同构定理就可以证明完了。

2.14 对应定理

若T是模M的子模，则存在双射

$$\varphi : \{对所有中间子模S, T \subseteq S \subseteq M\} \to \{M/T的子模\}$$

它由

$$S \mapsto S/T$$

给出。此外，在M中有$S \subseteq S'$当且仅当在M/T中$S/T \subseteq S'/T$

$$\begin{tikzcd}
M \arrow[dr] \arrow[dd, dash] & \\
& M/T \arrow[dd, dash] \\
S \arrow[dr] \arrow[dd, dash] & \\
& S/T \arrow[dd, dash] \\
S' \arrow[dr] \arrow[dd, dash] & \\
& S'/T \arrow[dd, dash] \\
T \arrow[dr] & \\
& \{0\}
\end{tikzcd}$$

证明； 每个模都是加法群，所以每个子模都是子群。利用群的对应定理，对φ的部分是保持包含关系的单射。并且在M中有$S \subseteq S'$当且仅当M/T中有$S/T \subseteq S'/T$。最后简单验证一下加法同态即可。

$$s, s' \in S \Rightarrow (s + T)(s' + T) = ss' + T \in S'/T$$

2.15 命题

$R-$模M是循环模当且仅当有某个理想I使得$M \cong R/I$

证明： 若M是循环的，那么有$m \in M$使得$M = \langle m \rangle$。定义$f : R \to M$为$f(r) = rm$。现在因为M是循环的，所以f是满的。他的核是某个理想I，[3]利用第一同构定理就有$R/I \cong M$ 反过来，R/I是循环的，生成元是$1 + I$。和循环模同构的模是循环模。

2.16 定义：单模

称模M为单模（或不可约），若$M \neq \{0\}$且M没有非零真子模，即模M的子模只有M和$\{0\}$。

我们讲一些简单的推论，

推论1 阿贝尔群G是单模当且仅当存在一个素数p使得$G \cong I_p$

推论2 $R-$模M是单模当且仅当$M \cong R/I$，其中I是极大理想。

证明： 利用对应定理，若非单模，则M有其他子模存在，使得R/I中存在其他的商模，但M是单模使得R/I无其他的子模存在，因此I是极大理想。

2.17 定义：直和

若S, T是$R-$模，其中R是交换环，那么它们的直和是指笛卡尔积$S \times T$配备坐标形式的运算：

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

和

$$r(s, t) = (rs, rt)$$

其中$s, s' \in S, t, t' \in T, r \in R$。并把直和记为$S \sqcup T$

存在单射$R-$映射$\lambda_S : S \to S \sqcup T$和$\lambda_T : T \to S \sqcup T$分别由$s \mapsto (s, 0)$和$t \mapsto (0, t)$定义。

[3]用了如下定理：若I是交换环R中的理想，那么有环A和同态$\pi : R \to A$使得$I = \ker \pi$

2.18 命题

对$R-$模M,S,T，下列称述命题是等价的：

- $S\sqcup T\cong M$
- 存在单射$R-$映射$i:S\to M$和$j:T\to M$使得
$$M=\mathrm{im}i+\mathrm{im}j\text{和}\mathrm{im}i\cap\mathrm{im}j=\{0\}$$
- 存在$R-$映射$i:S\to M$和$j:T\to M$使得对每个$m\in M$有唯一的$s\in S,t\in T$满足
$$m=is+jt$$
- 存在$R-$映射$i:S\to M,j:T\to M,p:M\to S,q:M\to T$满足
$$pi=1_S,qj=1_T,pj=0,qj=0,ip+jq=1_M$$
注意：我们称i,j是内射，p,q是投射，等式$pi=1_S$和$qj=1_T$表明映射i,j必是单射。因此$\mathrm{im}i\cong S,\mathrm{im}j\cong T$，且映射$p,q$是满射、

证明： 我们设$\varphi:S\sqcup T$是同构并定义$i=\varphi\lambda_S$为如上定义的单射。并且定义$j=\varphi\lambda_T$，那么i,j都是单射的复合。因此也是单射。因此，若$m\in M$，则存在唯一的有序对$(s,t)\in S\sqcup T$使得$m=\varphi((s,t))$

$$m=\varphi((s,t))=\varphi((s,0)+(0,t))=i(s)+j(t)=is+jt\in\mathrm{im}i+\mathrm{im}j$$

现在，若$x\in\mathrm{im}i+\mathrm{im}j$，那么存在$s\in S,t\in T$使得$is=jt$。但$\varphi$是同构，有$(s,0)=(0,t)$，那么$s=0=t$，有$x=0$且$\mathrm{im}i\cap\mathrm{im}j=\{0\}$

2 $\Rightarrow$3：给定$m\in M$，由命题2可知$m=is+jt$。现在证明唯一即可。设$m=is'+jt'$，那么$i(s-s')+j(t-t')\in\mathrm{im}i+\mathrm{im}j=\{0\}$，所以只有$i(s-s')=0,j(t-t')=0$。由于$i,j$是单射，因此$s=s',t=t'$

3$\Rightarrow$ 4 若$m\in M$，则有$s\in S,t\in T$唯一使得$m=is+it$，于是

$$p(m)=s,q(m)=t$$

定义的函数是良定义的。容易验证前4个等式成立。而对于最后一个等式，若$m\in M,m=is+jt$，那么

$$ip(m)+jq(m)=is+it=m$$

最后，由$4 \to 1$有

定义$\varphi : S \sqcup T \to M$为$\varphi : (s,t) = is + jt$。$\varphi$是$R-$映射。现在，由于$1_M ip + jq$，所以$\varphi$是满射。最后证明$\varphi$是单射。设$\varphi((s,t)) = 0$，从而$is = -jt$。由于$s = pis = -pjt = 0$。而$-t = -qjt = qis = 0$就是我们需要的东西了。

2.19 定义：内直和

设S和T是模M的子模，若$M \cong S \sqcup T$且$i : S \to M$和$j : T \to M$是包含映射，则称M是S和T的内直和，记为

$$M = S \oplus T$$

2.20 命题

对$R-$模M以及其子模S, T，下列条件是等价的

- $M = S \oplus T$
- $S + T = M$且$S \cap T = \{0\}$
- 对每个$m \in M$都有唯一的形如$m = s + t$的表达式，其中$s \in S$且$t \in T$

证明： 定义i, j是包含映射，用定义就可以在命题2.18得出。

2.21 定义：直和项

称模M的一个子模S为M的直和项，若存在M的子模使得$M = S \oplus T$

2.22 定义：收缩

若S是$R-$模M的子模，则把S称为M的收缩核，若存在叫收缩的$R-$同态$\rho : M \to S$使得对一切$s \in S$有$\rho(s) = s$

2.23 命题

模M的子模是直和项当且仅当存在收缩$\rho : M \to S$

证明： 令$i: S \to M$是包含映射，为了证明$M - S \oplus T$，其中$T = \ker \rho$，若$m \in M$，则$m = (m - \rho m) + \rho m$。而$\rho m \in \mathrm{im}\rho = S$。有$\rho\rho m = \rho m$，应用$\rho$在$(m - \rho m) = \rho m - \rho\rho m = 0$。所以$M = S + T$ 另一方面，因为$\ker \rho = T = \{0\}$，所以$m \in S$有$m \neq 0$，否则若$s \in S \cap T$则有$T \neq 0$由此可得$M = S \oplus T$

反过来，若$M = S \oplus T$，则$m = s + t$是唯一表示的，$s \in S, t \in T$。所以$\rho : s + t \mapsto s$定义的$\rho : M \to S$是收缩映射

2.24 命题

若$M = S \oplus T$和$S \subseteq A \subseteq M$，则$A = S \oplus (A \cap T)$

证明 设$\rho : M \to S$是收缩映射$s + t \mapsto s$. 由于$S \subseteq A$，从而限制$\rho \mid A : A \to S$也是收缩，且$\ker \rho \mid A = A \cap T$。

2.25 定义：外直和(有限个子模)

设$S_1, \cdots, S_n$是$R-$模，定义外直和

$$S_1 \sqcup \cdots \sqcup S_n$$

为这样的$R-$模，他的底集是笛卡尔积$S_1 \times \cdots \times S_n$，运算为

$$(s_1, \cdots, s_n) + (s_1', \cdots, s_n') = (s_1 + s_1', \cdots, s_n + s_n')$$

和

$$r(s_1, \cdots, s_n) = (rs_1, \cdots, rs_n)$$

2.26 定义：内直和（有限个）

设M是模，若$S_1, \cdots, S_n$是M的子模，且每个$m \in M$存在唯一形式如$s_1 + \cdots + s_n$的表达式，其中对一切$i = 1, \cdots, n$有$s_i \in S_i$，则定义M是内直和

$$M = S_1 \oplus \cdots \oplus S_n$$

并且可以证明内直和可以由外直和定义得到。

2.27 定义：序列

我们定义$R-$映射和$R-$模的序列

$$\cdots \to M_{n+1} \xrightarrow{f_{n+1}} M_n \xrightarrow{f_n} M_{n-1} \to \cdots$$

为正合列，且对一切$n, \mathrm{im} f_{n+1} = \ker f_n$

2.28 命题

1 序列$0 \to A \xrightarrow{f} B$是正合列当且仅当$f$是单射

2 序列$B \xrightarrow{g} C \to 0$是正合的当且仅当$g$是满射。

3 序列$0 \to A \xrightarrow{h} B \to 0$是正合的当且仅当$h$是同构。

证明：

- $0 \to A$的象是$\{0\}$，结合正合性，就有$\ker f = \{0\}$，因此f是单射，其次。给定$f : A \to B$，存在正合列$\ker f \to A \xrightarrow{f} B$，若$f$是单射，$\ker f \to 0$只能是$\ker f = \{0\}$
- $C \to 0$的核是C，正合性给出$\mathrm{im} g = C$。所以g是满射。反之，给定$g : B \to C$，存在正合列$B \xrightarrow{g} C \to C/\mathrm{im} g$

> 定义$f : M \to N$是映射，它的余核记为$\mathrm{coker} f$，定义为$\mathrm{coker} f = N/\mathrm{im} f$
>
> 命题：映射$f : M \to N$是满射当且仅当$\mathrm{coker} f = \{0\}$
>
> **证明：** 当f是满射时，$\mathrm{im} f = N$。它的余核为$N/\mathrm{im} f = n + \mathrm{im} f, n \in N$ 所以它实际上只有一个元素也就是$0 + N = N$，所以它是一个零模、因此$N/\mathrm{im} f = 0$.
>
> 反过来，现在$\mathrm{coker} f = \{0\} = N$，因此$\mathrm{im} f = N$是满射。

，所以，若g是满射，$C = \mathrm{im} g$且$C/\mathrm{im}\ g = 0$，

- 1命题证明h是单射当且仅当$0 \to A \xrightarrow{f} B$，而命题2给出$A \xrightarrow{h} B \to 0$是正合列，所以$h$是同构当且仅当$0 \to A \xrightarrow{h} B \to 0$是正合列

2.29 短正合列

一个短正合列指的是形如

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

的正合列，我们称这个短正合列为A和C扩张

2.30 命题

- 若$0 \to A \xrightarrow{f} B \xrightarrow{g}\to C \to 0$是短正合列，则

$$A \cong \mathrm{im} f, \quad B/\mathrm{im} f \cong C$$

- 若$T \subseteq S \subseteq M$是子模的塔，那么存在正合列

$$0 \to S/T \xrightarrow{f} M/T \xrightarrow{g} M/S \to 0$$

证明：

- 由于f是单的，所以有同构$A \to \mathrm{im} f$。第一同构定理给出$B/\ker g \cong \mathrm{im} g$，利用正合性，有$\ker g = \mathrm{im} f$和$\mathrm{im} g = C$，所以$B/\mathrm{im} f \cong C$
- 第二个命题是第三同构定理的复述，定义$f : S/T \to M/T$为包含映射，再定义$g : M/T \to M/S$为陪集的扩大。g是满射。就有$\ker g = S/T = \mathrm{im} f$。

2.31 定义：

称短正合列

$$0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0$$

分裂，若存在映射$j : C \to B$使得$pj = 1_C$

2.32 命题

如果短正合列

$$0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0$$

分裂，则$B \cong A \sqcup C$

证明： 我们证明$B = \mathrm{im}i \oplus \mathrm{im}j$，其中$j : C \to B$满足$pj = 1_C$。若$b \in B$，则因$pj = 1_C$，利用命题2.23，只需要找出收缩$p$的范围即可。

定义$b - jpb$为不包含任何$\mathrm{im}p$的元素，现在我们证明$p(b - jpb) = 0$，有$p(b-jpb) = pb - pj(pb)$，因为$pj = 1$，所以上述式子是0，就有$pb \in C, b - jbp \in \ker p$, 并且$\ker p \cong \mathrm{im}f$。因此存在$a \in A$使得$ia = b - jpb$，因此$B = \mathrm{im}i + \mathrm{im}j$.剩下只需要证明$\mathrm{im}i \cap \mathrm{im}j = \{0\}$。若$ia = x = jc$，则$pi = 0$有$px = pia = 0$，又有$pj = 1_C$，所以$px = pjc = c$，因此$x = jc = 0$有$B \cong A \sqcup C$

上述命题的逆命题是不成立的，注意$A = \langle a \rangle$和$B = \langle b \rangle$还有$\langle c \rangle$是阶为$2, 4, 2$的循环群，若定义$i : A \to B$为$i(a) = 2b$，定义$p : B \to C$为$p(b) = c$。则$0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0$是正合列，但它不分裂。$\mathrm{im}i = \langle 2b \rangle$甚至不是$B$的子群。

2.33 命题

- 交换环R是诺特环当且仅当有限生成$R-$模M的每个子模是有限生成的。
- 若R是PID且M可以由n个元素生成，则M的每个子模可以由n个或者少于n个的元素生成。

证明： 假设一个有限生成$R-$模的每个子模也是有限生成的，特别的，若R是循环模，那么它自身就是有限生成的。而R的子模本身是理想，所以每个理想就是有限生成的。即R是诺特环。

反之，对$n \geq 1$应用归纳法，其中$M = \langle x_1, \cdots, x_n \rangle$，当$n = 1$，则$M$是循环的，命题2.15给出一个理想$I$使得$M \cong R/I$。若$S \subseteq M$，则对应定理给出$I \subseteq J \subseteq R$和$S \cong J/I$，由于$R$是诺特环，则$J$是有限生成的。从而$J/I$也是有限生成的。

现在，对$n \geq 1$和$M = \langle x_1, \cdots, x_n, x_{n+1} \rangle$，我们考虑正合列

$$0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$$

其中$M' = \langle x_1, \cdots, x_n \rangle$，而$M'' = M/M'$，其中$i$是包含映射，而$p$是自然映射。可以简单验证$M''$是循环的，因为$M''$由$x_{n+1} + M'$生成。若$S \subseteq M$是子

模，就有正合列

$$0 \to S \cap M' \to S \to S/(S \cap M') \to 0$$

有$S \cap M' \subseteq M'$，根据归纳假设，它是有限生成的，现在用第二同构定理，有$S/(S \cap M') \cong (S + M')/M' \subseteq M/M'$

引入习题

设$0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0$是短正合列。

证明若A, C是有限生成的，则B也是有限生成的。

证明： 利用命题2.30的1，有$A \cong \mathrm{im} f$和$B/\mathrm{im} f \cong C$，由于A, C有限生成，那么由i是单的和p是满的并且有限可知B也是有限生成的。

由归纳假设，M/M'有限，那么$S/(S \cap M')$是有限的，利用上述习题可知S是有限生成的。

对第二个命题，对$n \geq 1$归纳证明，若M是循环的，有$M \cong R/I$，若存在$S \subseteq M$，就存在一个包含I的理想J使得$S \cong J/I$，由于R是PID，所以J是主理想，有J/I是循环的。

对于归纳步骤和1一样，我们考虑正合列

$$0 \to S \cap M' \to S \to S(S \cap M') \to 0$$

其中$M = \langle x_1, \cdots, x_n, x_{n+1} \rangle$。和$M' = \langle x_1, \cdots, x_n \rangle$。由归纳假设，$S \cap M'$是可以被$n$个或少于$n$个的元素生成的。最后，$S \cap (S \cap M') \cong (S + M')/M' \subseteq M/M'$，由归纳假设，$M/M'$是$x_{n+1} + M'$生成的循环模。所以由基础步骤上，现在$S/(S \cap M')$被$M/M'$包含。那么就存在一个循环模和$S/(S \cap M')$是同构的，因此$S/(S \cap M')$是循环的。利用上述习题可知$S$是可以被$n+1$个或者少于$n+1$个的元素生成的

下一个命题我们证明代数整数的和还有积都是代数整数，若α和β是代数整数，不难给出以$\alpha + \beta$和$\alpha\beta$为根的首一多项式。

2.34 命题

设$\alpha \in \mathbb{C}$,定义$\mathbb{Z}[\alpha] = \{g(\alpha) : g(x) \in \mathbb{Z}[x]\}$

1、 $\mathbb{Z}[\alpha]$是$\mathbb{C}$的子环

2、 复数α是代数整数当且仅当$\mathbb{Z}[\alpha]$是有限生成的加法阿贝尔群

3、 一切代数整数的集合是$\mathbb{C}$的子环。

证明：

1 首先取$g(x) = 1$为常数多项式，现在$1 = g(\alpha)$就有$1 \in \mathbb{Z}[\alpha]$。若$f(\alpha), g(\alpha) \in \mathbb{Z}[\alpha]$。那么$f + g = h(\alpha) \in \mathbb{Z}[\alpha]$中。而$fg \in \mathbb{Z}[z]$，所以$\mathbb{Z}[\alpha]$是$\mathbb{C}$的子环

2 设α是代数整数，那么就存在首一多项式$f(x) \in \mathbb{Z}$以α为根。我们断言，若$\deg(f) = n$，则$Z[\alpha] = G$，其中G是满足$m_i \in \mathbb{Z}$的一切线性组合$m_0 + m_1\alpha + \cdots + m_{n-1}a^{n-1}$的集合。那么有$G \subseteq \mathbb{Z}[\alpha]$

对于反包含，$u \in \mathbb{Z}[\alpha]$的元素形如$u = g(\alpha)$，其中$g(x) \in \mathbb{Z}[x]$。由于f首一，带余除法给出$q, r \in \mathbb{Z}[x]$使得$g = qf + r$，其中$r(x) = 0$或者$\deg(r) < \deg(f) = n$。所以

$$u = g(\alpha) = q(\alpha)f(\alpha) + r(\alpha) = r(\alpha) \in G$$

由此$\mathbb{Z}[\alpha]$这个加法群是有限生成的。

反之，我们设$\mathbb{Z}[\alpha]$有一有限生成的加法群，即$\mathbb{Z}[\alpha] = \langle g_1, \cdots, g_m \rangle$是阿贝尔群，那么每个$g_j$都是$\alpha$的幂的$\mathbb{Z}-$线性组合。设$m$是$g$中会出现的最大幂次，由于$\mathbb{Z}[\alpha]$是交换环，那么$a^{m+1} \in Z[\alpha]$。从而可以表示为一些较小$\alpha$的次幂的$\mathbb{Z}-$线性组合。例如有 $a^{m+1} = \sum_{i=0}^{m} b_i a^i$，其中$b_i \in \mathbb{Z}$。那么$\alpha$就是$x^{m+1} - \sum_{i=0}^{m} b_i x^i$的根，由于$f(x)$是$\mathbb{Z}[x]$中的首一多项式，那么$\alpha$是代数整数。

3 假设α, β是代数整数。设α是n次首一多项式$f(x) \in \mathbb{Z}[x]$的根，而β是次数为m的首一多项式$g(x) \in \mathbb{Z}[x]$的根。那么$\mathbb{Z}[\alpha\beta]$是$G = \langle \alpha^i\beta^j : 0 \leq i < n, 0 \leq j < m \rangle$的加法子群。由于$G$是有限生成的，子群$\mathbb{Z}[\alpha\beta]$是有限生成的，利用命题1的结果就有$Z[\alpha\beta]$是$\mathbb{C}$的子环。其次$\mathbb{Z}[\alpha+\beta] = \{\langle \alpha^i\beta^j : i + j \leq n + m - 1 \rangle\}$的加法子群，则$\alpha + \beta$也是代数整数。