例1.设$f(x)\in Q[x]$是不可约首一多项式，$\alpha_1,\cdots,\alpha_n$是它的$n$个根，称$d(f)=\prod_{1\le r<s\le n}(\alpha_r-\alpha_s)^2$是多项式$f(x)$的判别式，定义等幂和为$s_k=\sum_{i=1}^n\alpha_i^k$.则

$$d(f)=\begin{vmatrix} s_0 & s_1 & \cdots & s_{n-1} \\ s_1 & s_2 & \cdots & s_n \\ \vdots & \vdots & & \vdots \\ s_{n-1} & s_n & \cdots & s_{2n-2} \end{vmatrix}$$

只需注意到$\prod_{1\le r<s\le n}(\alpha_r-\alpha_s)$是范德蒙德行列式$(\alpha_i^j)(1\le i\le n,0\le j\le n-1)$的值.
设$f(x)=x^n+ax+b$是$Q[x]$中的不可约多项式，求证：

$$d(f)=(-1)^{n(n-1)/2}[(-1)^{n-1}(n-1)^{n-1}a^n+n^nb^{n-1}].$$

证明:需用到牛顿公式.设$f(x)$是有理数域$Q$上的$n$次多项式,$\alpha_1,\cdots,\alpha_n$是它的$n$个根，$\sigma_k(1\le k\le n)$是基本对称多项式，即$\sigma_k=\sum_{1\le i_1<i_2<\cdots<i_k\le n}x_{i_1}x_{i_2}\cdots,x_{ik}$ 牛顿公式为
当$k\ge n$时，

$$s_k-s_{k-1}\sigma_1+s_{k-2}\sigma_2+\cdots+(-1)^ks_{k-n}\sigma_n=0;$$

当$k<n$时，

$$s_k-s_{k-1}\sigma_1+\cdots+(-1)^{k-1}s_1\sigma_{k-1}+(-1)^kk\sigma_k=0.$$

具体地，对于多项式$f(x)=x^n+ax+b$,基本对称多项式为$\sigma_i=0(1\le i\le n-2),\sigma_{n-1}=(-1)^{n-1}a,\sigma_n=(-1)^nb$.再根据牛顿公式 ,等幂和为

$$s_0=n,s_i=0(1\le i\le n-2,n+1\le i\le 2n-3),s_{n-1}=-(n-1)a,s_n=-nb,s_{2n-2}=(n-1)a^2$$

于是

$$d(f)=\begin{vmatrix} n & 0 & \cdots & \cdots & -(n-1)a \\ 0 & 0 & \cdots & -(n-1)a & -nb \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & -(n-1)a & -nb & \cdots & \cdots \\ -(n-1)a & -nb & \cdots & \cdots & (n-1)a^2 \end{vmatrix}$$

计算该行列式即得到结论。
例2.设$\zeta_m=e^{\frac{2\pi i}{m}}(m\in Z_{\ge 0})$,证明:$\mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n)=\mathbb{Q}(\zeta_{(m,n)})$,这里$(m,n)$是$m,n$的最大公约数.
证明:首先易知$\mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n)\supseteq\mathbb{Q}(\zeta_{(m,n)})$.
令$l=[m,n],d=(m,n),F=\mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n)$
任取$f\in Gal(\mathbb{Q}(\zeta_l)/\mathbb{Q}(\zeta_n))$.$f$必形如映射

$$f_k:\mathbb{Q}(\zeta_l)\to\mathbb{Q}(\zeta_l),\zeta_l\mapsto\zeta_l^k,(k,l)=1,k\equiv 1(mod\quad n)$$

因$F$是$\mathbb{Q}(\zeta_n)$的子域，$f_k$保持$F$不变，另有$(k,l)=1,l=[m,n]\Rightarrow(k,m)=1$,于是$f_k$在$\mathbb{Q}(\zeta_m)$上的限制是自同构，从而有$f_k|_{\mathbb{Q}(\zeta_m)}\in Gal(\mathbb{Q}(\zeta_m)/F)$. 因此

$$|Gal(\mathbb{Q}(\zeta_l)/\mathbb{Q}(\zeta_n))|=\frac{\varphi(l)}{\varphi(n)}=\frac{\varphi(m)}{\varphi(d)}\le[\mathbb{Q}(\zeta_m):F].$$

由域扩张的乘积公式($[L:F]=[L:E][E:F]$)得到$[F:\mathbb{Q}]\le\varphi(d)$,再由$[\mathbb{Q}(\zeta_d):\mathbb{Q}]=\varphi(d)$及$\mathbb{Q}(\zeta_d)\subseteq F$得到$\mathbb{Q}(\zeta_d)=F$.

例3.设$\theta$是多项式$f(x)=x^3+x^2-2x+8\in\mathbb{Q}[x]$的一个根，$K=\mathbb{Q}(\theta)$,则
i)$d_k(1,\theta,\theta^2)=-4\cdot 503$.
ii)证明:$\theta^{'}=4/\theta\in\mathcal{O}_K$,$\{1,\theta,\theta^{'}\}$是域$K$的一组整基,并且$d(K)=-503$.
iii)对于每个$\alpha\in\mathcal{O}_K$, $\{1,\alpha,\alpha^2\}$不可能是域$K$的一组整基.
证明:(1)类似例1即可得到结论。
(2)根据行列式的性质即得。
(3)设$\theta$是$f(x)$的一根，则可验证$\{1,\theta,\beta=(\theta+\theta^2)/2\}$是一组整基，若$\alpha\in\mathcal{O}_K$,且$\{1,\alpha,\alpha^2\}$是域$K$的一组整基，不妨设$\alpha=a+b\theta+c\beta$,由于$\{1,\alpha,\alpha^2\}$是域$K$的一组整基当且仅当$\{1,(\alpha-a),(\alpha-a)^2\}$是域$K$的一组整基,因此，我们不妨设$a=0$.利用$\theta$是$f(x)$的根，我们得到

$$(b\theta+c\beta)^2=-8bc-2c^2+(2bc-b^2-\frac{c^2}{2})\theta+(2b^2-c^2)\beta$$

从而

$$(1,\alpha,\alpha^2)=(1,\theta,\beta)A$$

其中

$$A=\begin{vmatrix}1 & 0 & -8bc-2c^2\\ 0 & b & 2bc-b^2-\frac{c^2}{2}\\ 0 & c & 2b^2-c^2\end{vmatrix}$$

整基之间变换矩阵的行列式为±1. 于是

$$\pm 1=detA=2b^3-bc^2-2bc^2+b^2c+\frac{c^3}{2}=2b^3-3bc^2+b^2c+\frac{c^3}{2}$$

于是$b,c$是整数，$c$只能是偶数，但此时行列式也为偶数，矛盾！从而对于每个$\alpha\in\mathcal{O}_K$,$\{1,\alpha,\alpha^2\}$不可能是域$K$的一组整基.
(d-uple embedding)设$n,d>0$, $M_0,M_1,\cdots,M_N$ 是$n+1$个变量$x_0,x_1,\cdots,x_n$的次数为$d$的首一多项式，于是$N=C_{n+d}^n-1$.定义映射$\nu_d:\mathbb{P}^n\to\mathbb{P}^N$为

$$(x_0,x_1,\cdots,x_n)\mapsto(M_0(x_0,x_1,\cdots,x_n),M_1(x_0,x_1,\cdots,x_n),\cdots,M_N(x_0,x_1,\cdots,x_n)).$$

则i)定义映射$\theta:K[y_0,\cdots,y_N]\to K[x_0,\cdots,x_n]$ $f(y_0,\cdots,y_N)\mapsto f(M_0,M_1,\cdots,M_N)$,令$\mathfrak{a}=ker(\theta)$，则$\mathfrak{a}$是齐次素理想.
证明:设$f(y_0,\cdots,y_N)\in\mathfrak{a}$,由于$K[y_0,\cdots,y_N]$是分次环，可令$f=\sum_i f_i$,其中$f_i$是$i$次齐次多项式，于是$f(M_0,M_1,\cdots,M_N)=\sum_i f_i(M_0,M_1,\cdots,M_N)=0$.这就得到$f_i(M_0,M_1,\cdots,M_N)=0$,即$f_i\in\mathfrak{a}$.于是$\mathfrak{a}=\oplus_i\mathfrak{a}\cap K[y_0,\cdots,y_N]_i$,于是$\mathfrak{a}$是齐次理想。
若$f,g\in K[y_0,\cdots,y_N]$且$\theta(fg)=\theta(f)\theta(g)=0$，由于$k[x_0,\cdots,x_n]$为整环，故必有$\theta(f)=0$或$\theta(g)=0$，即$f\in\mathfrak{a}$或$g\in\mathfrak{a}$,从而$\mathfrak{a}$是素理想.
下面来刻画$\nu_d$的像。首先说明记号，由于$M_i$是关于$x_0,x_1,\cdots,x_n$的$d$次单项式，从而

$$M_i=x_0^{i_0}x_1^{i_1}\cdots x_n^{i_n},$$

把右边记为$x^{I_i}, I_i=(i_0,i_1,\cdots,i_n)$, 于是每个$M_i$对应一个$I_i$,把映射$\nu_d$的像中$M_i(x_0,\cdots,x_n)$所在$\mathbb{P}^N$中的分量命名为$z_{I_i}$.于是$\mathbb{P}^N$中的元素可用$(z_{I_0},z_{I_1},\cdots,z_{I_N})$表示，这里只是用$I_k(k=0,\cdots,N)$代替了$0,1,2,\cdots,N$,只是记号的改变。

命题1：映射$\nu_d:\mathbb{P}^n\to\mathbb{P}^N$的像为投射簇

$$W=V(\{z_Iz_J-z_Kz_L:I,J,K,L\in\mathbb{N}^{n+1},I+J=K+L\}).$$

这里指标的加法定义为:若$I=(i_0,i_1,\cdots,i_n), J=(j_0,\cdots,j_n)$,则$I+J:=(i_0+j_0,\cdots,i_n+j_n)$.

证明:首先由于$x^Ix^J-x^Kx^L=x^{I+J}-x^{K+L}=0$知$z_Iz_J-z_Kz_L$在$\nu_d(\mathbb{P}^n)$上恒为零.于是$\nu_d(\mathbb{P}^n)\subseteq W$.

为了证明$W\subseteq\mathbb{P}^n$，构造映射$\phi:W\to\mathbb{P}^n$使得$\phi\circ\nu_d=id_{\mathbb{P}^n},\nu_d\circ\phi=id_W$.

设$z=[\cdots:z_I:\cdots]\in W$,则$z_{(d,0,\cdots,)},z_{(0,d,\cdots)},\cdots,z_{(0,\cdots,0,d)}$中必有一非零元，否则由$W$的定义可得$z$的所有分量都是零,与$\mathbb{P}^N$中分量全部为零的点矛盾。事实上,设

$$z_{(d,0,\cdots,)}=z_{(0,d,\cdots)}=\cdots=z_{(0,\cdots,0,d)}=0,z_{(i_0,i_1,\cdots,i_n)}\neq 0.$$

不是一般性可以设$i_0\neq 0$,且对于$j_0>i_0$都有$z_{(j_0,j_1,\cdots,j_n)}=0$.由于$i_0<d$,因此存在指标，设为$d>i_1>0$,由$W$的中元素满足的方程知$z^2_{(i_0,i_1,\cdots,i_n)}=z_{(i_0+1,i_1-1,\cdots,i_n)}z_{(i_0-1,i_1+1,\cdots,i_n)}$.从而$z_{(i_0+1,i_1-1,\cdots,i_n)}\neq 0$,矛盾!

令$U_i=\{z\in W|z_{(0,\cdots,d^i,\cdots)}\neq 0\}$.(这里$(0,\cdots,d^k,\cdots)$表示指标$j_0=0,\cdots,j_i=d,\cdots,$)从而$U_i$是$W$的一组覆盖。

定义映射$\phi_i:U_i\to\mathbb{P}^n$

$$z\mapsto[z_{(1,0,\cdots,d-1^i),0,\cdots,0}:z_{(0,1,\cdots,d-1^i),0,\cdots,0}:\cdots,z_{(0,\cdots,d-1^i),0,\cdots,1}]$$

下面验证$\phi_i$和$\phi_j$在$U_i\cap U_j$上是相等的，由等式

$$z_{(0,\cdots,1^a,\cdots,d-1^j,\cdots,0)}z_{(0,\cdots,d^i,\cdots,0)}=z_{(0,\cdots,1^a,\cdots,d-1^i,\cdots,0)}z_{(0,\cdots,1^i,\cdots,d-1^j,\cdots,0)},$$

得到

$$z_{(0,\cdots,1^a,\cdots,d-1^j,\cdots,0)}=\frac{z_{(0,\cdots,1^i,\cdots,d-1^j,\cdots,0)}}{z_{(0,\cdots,d^i,\cdots,0)}}z_{(0,\cdots,1^a,\cdots,d-1^i,\cdots,0)},$$

因此$\phi_i$和$\phi_j$在$U_i\cap U_j$上是相等的。

将$\phi_i$结合在一起可得到映射$\phi:W\to\mathbb{P}^n$,定义为:若$z\in U_i$，则$\phi(z)=\phi_i(z)$.

复合映射是$\phi\circ\nu_d:\mathbb{P}^n\to\nu_d(\mathbb{P}^n)\to\mathbb{P}^n$

$$[x_0:\cdots:x_n]\mapsto\nu_d(x)\mapsto[x_0x_i^{d-1}:\cdots:x_nx_i^{d-1}]=[x_0:\cdots:x_n],$$

即是恒等映射。

同样地，容易验证$\nu_d\circ\phi:\nu_d(\mathbb{P}^n)\to\mathbb{P}^n\to\nu_d(\mathbb{P}^n)$是$W$上的恒等映射。

于是$\nu_d$是满射，从而$W=\nu_d(\mathbb{P}^n)$.

注意到由于$z_Iz_J-z_Kz_L\in\mathfrak{a}$于是$V(\mathfrak{a})\subseteq W$,其次易见$\nu_d(\mathbb{P}^n)\subseteq V(\mathfrak{a})$,于是$V(\mathfrak{a})=W=\nu_d(\mathbb{P}^n)$.

命题2:如果$Y\subseteq\mathbb{P}^n$是投射簇，那么$\nu_d(Y)$是$\nu_d(\mathbb{P}^n)$的子投射簇.

证明:对于映射$\nu_d::\mathbb{P}^n\to\mathbb{P}^N$，我们可以将其看作仿射空间上映射$\hat{\nu_d}:\mathbb{A}^{n+1}\to\mathbb{A}^{\binom{n+d}{d}}$, $[x_0,\cdots,x_n]\mapsto$

$[\cdots,x^I,\cdots,]$诱导得出的.将$K[\cdots,z_I,\cdots]$上的多项式$g(z)$与映射$\hat{\nu_d}$复合便得到$K[x_0,\cdots,x_n]$上的一个多项式$g\circ\hat{\nu_d}(x)$.
注意到下面事实：设$F$是多项式环$K[x_0,\cdots,x_n]$中的一个多项式，那么

$$V(F)=V(x_0F,x_1F,\cdots,x_nF)\subseteq\mathbb{P}^n.$$

因此若$Y=V(F_1,\cdots,F_r)\subseteq\mathbb{P}^n$,且$deg(F_i)=m_i(i=1,\cdots,r)$,则取$a$满足$ad>m_i$对任意$i$成立，于是就存在$ad$次齐次多项式$G_1,\cdots,G_s$使得$Y=V(G_1,\cdots,G_s)$.
进一步，存在$a$次齐次多项式$H_i(i=1,\cdots,r)$使得$G_i=H_i\circ\hat{\nu_d}$成立。由定义

$$y\in\nu_d(Y)\Leftrightarrow y=\nu_d(x),G_i(x)=0,\forall i.$$

但是$G_i(x)=H_i\circ\hat{\nu_d}(x)$,因此$x\in Y\Leftrightarrow\nu_d(x)\in V(H_1,\cdots,H_s)$.综上$\nu_d(Y)=\nu_d(\mathbb{P}^n)\cap V(H_1,\cdots,H_s)$.
上述命题说明$\nu_d$是开映射,从而命题1中$\phi$是连续映射.反过来，设$W$是$\nu_d$中闭集，从而存在多项式环$K[y_0,y_1,\cdots,y_N]$中齐次函数$H_i(i=1,\cdots,n)$使得$W=\nu_d(\mathbb{P}^n)\cap V(H_1,\cdots,H_n)$,易验证$\nu_d(\mathbb{P}^n)\cap V(H_1,\cdots,H_n)=\nu_d(V(H_1\circ\nu_d,\cdots,H_n\circ\nu_d))$,于是$\phi(W)=\phi\nu_d(V(H_1\circ\nu_d,\cdots,H_n\circ\nu_d))=V(H_1\circ\nu_d,\cdots,H_n\circ\nu_d)$,这就说明$\phi$是开映射，从而$\nu_d$连续.
**segre embedding 定义：**Segre embedding定义为映射

$$\sigma_{n,m}:\mathbb{P}^n\times\mathbb{P}^m\to\mathbb{P}^{(n+1)(m+1)-1}$$

**命题3：**设$E/F,K/E$是域扩张，则$E/F,K/E$是代数扩张当且仅当$K/F$是代数扩张。
证明:若$K/F$是代数扩张,则易证明$E/F,K/E$是代数扩张。反过来任取$\alpha\in K$,由于$K/E$是代数扩张，因此有$E[X]$中多项式$f(X)$使得$f(\alpha)=0$.设$f(X)=a_0+a_1X+a_2X^2+\cdots+a_nX^n,a_i\in E$,则$\alpha$是$F(a_0,\cdots,a_n)$上代数元，从而$F(a_0,\cdots,a_n)(\alpha)$是$F(a_0,\cdots,a_n)$的有限扩张。注意到$E/F$是代数扩张，从而$F(a_0,\cdots,a_n)/F$是有限扩张。综上，$F(a_0,\cdots,a_n)(\alpha)/F$是有限扩张，于是$\alpha$是$F$上代数元，即$K/F$是代数扩张。
**命题4：**设$K/F$是代数扩张，$\tau:K\to K$是$F$嵌入，即$\tau|_F=id_F$,则$\tau$是$K$的自同构.
证明:任取$\alpha\in K$,设$P(x)$是其在$F$上的最小多项式，令$S=\{\alpha\in K|P(\alpha)=0\},E=F(S)$,则$\tau(E)\subseteq E$.由于$E/F$是有限生成代数扩张，$E/F$是有限扩张，设$\alpha_0=1,\alpha_1,\cdots,\alpha_{n-1}$是$E$的一组$F$基，由于$\tau$是单射，我们可以得到$\tau(\alpha_0),\cdots,\tau(\alpha_{n-1})$线性无关，从而$dim_F\tau(E)\geq n$,但是$\tau(E)\subseteq E,dim_FE=n$,于是$\tau(E)=E$.由于$\alpha$是任取的，这就说明$\tau$是域$K$的子同构。

设$f(X)$是$\mathbb{Z}[x]$中首一多项式，而$g(x)\in\mathbb{Q}[x]$是$f(x)$的首一多项式因子，求证$g(x)\in\mathbb{Z}[x]$.
证明：设$g(x)=x^m+\frac{b_{m-1}}{a_{m-1}}x^{m-1}+\cdots+\frac{b_0}{a_0}$,其中$a_i,b_i\in\mathbb{Z}$且$(a_i,b_i)=1$.令$a=[a_0,a_1,\cdots,a_{m-1}]$,即$a$为$a_0,a_1,\cdots,a_{m-1}$的最小公倍数，则

$$(a,a\frac{b_0}{a_0},\cdots,a\frac{b_{m-1}}{a_{m-1}})=1$$

于是多项式 $h(x)=ax^m+a\frac{b_{m-1}}{a_{m-1}}x^{m-1}+\cdots+a\frac{b_0}{a_0}$是本原多项式，而$g(x)=\frac{1}{a}h(x)$,设$f(x)=g(x)p(x)$,同样地，有本原多项式$q(x)$使得$p(x)=\frac{1}{b}q(x)$,于是$f(x)=\frac{1}{ab}h(x)q(x)$，由$Gauss$引理

$h(x)q(x)$为本原多项式，$f(x)$为首一多项式，从而也是本原多项式，于是$ab=1$,从而$a=b=1$,这就说明$g(x)=h(x)\in\mathbb{Z}[x]$.

2.4设$A$是环，$(X,O_X)$是概型，我们有一一对应

$$Hom(X,SpecA)\rightarrow Hom(A,O_X(X))$$