第 7 章 多项式环

7.1 一元多项式环的概念及其通用性质

多项式定义：表达式 $f(x)=\sum_{i=0}^{n}a_ix^i$， $a_i\in F, 0\le n\in Z$，称为数域 F 上的多项式；

其中 a_ix^i 称为 f (x)的 i 次项。
若 $a_i=0$，表达式 f (x)中可以去掉 a_ix^i；若 $a_i=1$，$1x^i$ 可以简写为 x^i。
同样我们可以在表达式中增加系数为 0 的项。
若 $a_n\neq0$，称 a_nx^n 为 f (x)的首项；a_n 称为首项系数；n 称为 f (x)的次数，记为 deg f (x)=n。
若 $a_n=1$，称 f (x)为首一多项式。
若 n=0，f (x)=$a_0\neq0$，即 F 中的非零常数 a 是 0 次多项式。
若 f (x)表达式中 $a_i=0(i=0,1,\cdots,n)$，记 f (x)=0，称为 0 多项式，其次数定义为 deg 0= $-\infty$。

记 F[x]=$\left\{\sum_{i=0}^{n}a_ix^i \mid a_i\in F, 0\le n\in Z\right\}$表示属于 F 上的以 x 为未定元的多项式集合。

简称多项式集合 F[x]。

给定 $f(x)=\sum_{i=0}^{m}a_ix^i$， $g(x)=\sum_{i=0}^{n}b_ix^i\in F[x]$；

Define 加法：$f(x)+g(x)=\sum_{i=0}^{\max\{m,n\}}(a_i+b_i)x^i$；乘法：$f(x)g(x)=\sum_{k=0}^{m+n}(\sum_{i+j=k}a_ib_j)x^k$ 。

运算性质：1° 交换律：f+g=g+f，fg=gf；
2° 结合律：(f+g)+h=f+(g+h)，(fg)h=f(gh)；
3° 零元存在：∀f，∃0，s.t. f+0=f；
4° 负元存在：∀f，∃g，s.t. f+g=0；简记 g= −f，称 g 为 f 的负多项式；
5° 分配律：(f+g)h=fh+gh，h(f+g)=hf+hg；
6° 单位元存在：∀f，∃1，s.t. f1=1f=f。
多项式环定义：集合 F[x]，加法运算、乘法运算以及它们满足的运算律，统称为多项式环 F[x]，简称为多项式环 F[x]。
如果一个环的子集(对于原环的加法和乘法)也构成一个环,则称之为该环的子环。
次数与运算：f,g∈F[x]，则 deg(f+g)⩽max{deg f,deg g} and deg(fg)=deg f+deg g。
*称非空集合 R 为环，如果 R 上有两个运算：
加法“+”RxR→R and 乘法“•”RxR→R
满足如下性质：1° a+b=b+a；2° (a+b)+c=a+(b+c)；3° 零元存在；
4° 负元存在；5° (ab)c=a(bc)；6° (a+b)c=ac+bc，c(a+b)=ca+cb。
乘法满足交换律的环是交换环；单位元存在的环是有“1”的环。
多项式环的通用性：对于环 R，未定元 x，我们有 R[x]，我们有

R[x]=$\left\{\sum_{i=0}^{n}a_ix^i \mid a_i\in R, 0\le n\in Z\right\}$，称为 R 上的多项式环，环 R⊆环 R[x]。

定理：设 F 是一个数域，S 是一个有单位元的交换环，F 到 S 的一个子环有一个环同构映射。则对∀b∈S，有自然映射 $\varphi_a : F[x] \to S, f(x) \mapsto \varphi_a(f(x)) = f(a)$ 满足：

1° $\varphi_a(f(x)+g(x)) = f(a)+g(a)$；2° $\varphi_a(f(x)g(x)) = f(a)g(a)$。

且 φ_a 的像为 F[a]=$\left\{ \sum_{i=0}^{n} a_i a^i \mid a_i \in F, 0 \le n \in Z \right\}$。

7.2 整除性，带余除法

多项式整除定义：∀f(x),g(x)∈F[x]，g(x)≠0，称 g(x)整除 f(x)，如果存在 h(x)∈F[x]使得 f(x)=g(x)h(x)。记为 g(x)|f(x)，也称 g(x)是 f(x)的因式。

注：给定 f(x)∈F[x]，非零常数都是 f(x)的因式；把非零因式称为平凡因式。

性质 1：设 f(x),g(x),h(x)∈F[x]，g(x)h(x)≠0。若 h(x)|g(x)，g(x)|f(x)，那么 h(x)|f(x)。

相伴：f(x),g(x)∈F[x]，称 f(x)与 g(x)相伴，如果存在非零常数 c∈F，使得 f(x)=cg(x)。

两个多项式相伴⇔f(x)|g(x)，g(x)|f(x)。

推论：若 f(x)g(x)是首一多项式，则 f(x)=g(x)⇔f(x)|g(x)，g(x)|f(x)。

性质 2：设 f(x),g(x),h(x)∈F[x]，若 h(x)|f(x)，h(x)|g(x)，那么 h(x)|u(x)f(x)+v(x)g(x)，∀u(x),v(x)∈F[x]。

带余除法：∀f(x),g(x)∈F[x]，g(x)≠0，存在唯一的一组多项式 q(x),r(x)∈F[x]使得 f(x)=g(x)q(x)+r(x)；其中 deg r＜deg g。

推论：f(x)=(x-a)q(x)+f(a)（a∈F）。（该式看上去很奇怪，可以理解为拿 x-a 去除 f(x)，余数一定是 0 次或-∞次的某个常数）

推论：(x-a)|f(x)⇔f(a)=0，a∈F，f(x)∈F[x]。

命题：设 F⊂K 是数域，给定 f(x),g(x)∈F[x]，g(x)≠0，同样对于 f(x),g(x)∈K[x]；若在 K[x]中，g(x)|f(x)，那么在 F[x]中也有 g(x)|f(x)。（做带余除法证之）

同余：在 F[x]中，给定 g(x)≠0，称两个多项式 $f_1(x),f_2(x)$模 g(x)同余，如果 $g(x)|f_1(x)-f_2(x)$。记 $F[x] \big/ g(x)F[x] = \{\overline{f(x)} \mid f(x) \in F[x]\}$,其中 $\overline{f(x)} = f(x) + g(x)F[X] =$ {f(x)+g(x)h(x)|h(x)∈F[x]}。这也是一个环。（类比 mod N 同余类构成的一个有限环）

计算两个多项式的带余除法：辗转相除法。

7.3 最大公因式

公因式：设 f(x),g(x)∈F[x]，h(x)∈F[x]且≠0，称 h(x)是 f(x),g(x)的公因式，如果 h(x)|f(x)，h(x)|g(x)。特别地，任意非零常数∈F，c 是 f(x),g(x)的公因式。

最大公因式：设 f(x),g(x)∈F[x]，d(x)称为 f(x),g(x)的最大公因式，如果(1) d(x)|f(x)，d(x)|g(x)；(2)∀h(x)|f(x)，h(x)|g(x)，则 h(x)|d(x)。

命题：d(x)在相伴意义下唯一。记(f,g)=d，表示 f 与 g 的首“1”最大公因式。

定理：f(x)与 g(x)的最大公因式 d(x)存在，且存在 u(x),v(x)使得 fu+gv=d。

补充：若存在 u(x),v(x)使得 fu+gv=d，且 d|f and d|g，则 d 是 f,g 的最大公因式。

互素：设 f(x),g(x)∈F[x]，称 f(x)与 g(x)互素，如果(f(x),g(x))=1。

定理：f(x)与 g(x)互素的充要条件是存在 u(x),v(x)使得 fu+gd=1。

性质 1：f(x),g(x),h(x)∈F[x]，h(x)≠0，if h|fg with (h,f)=1，then h|g。

性质 2：f(x),g(x),h(x)∈F[x]，fg≠0，if f|h and g|h with (f,g)=1，then fg|h。

性质 3：$f(x),g(x),h(x)\in F[x]$，if $(f,h)=1$ and $(g,h)=1$，then $(fg,h)=1$。
推广：S 是正整数，$f_i\in F[x](i=1,2,\cdots,S)$，称 h 是 f_i 的因式，如果 $h|f_i$。
定义：设 S 是正整数。称 d 是 f_i 的最大公因式，如果(1) $d|f_i$；(2) $\forall h(x)|f_i(x)$，都有 $h|d$。
命题：d(x)在相伴意义下唯一。记$(f_1,\cdots,f_S)=d$，表示 $f_1,\cdots,f_S$ 的首“1”最大公因式。
命题：$(f_1,\cdots,f_S)=((f_1,\cdots,f_{S-1}),f_S)$。
定理：$f_1(x),\cdots,f_S(x)$的最大公因式 d(x)存在，且存在 $u_1(x),\cdots,u_S(x)$使得$\Sigma u_if_i=d$。
互素：设 $f_1(x),\cdots,f_S(x)\in F[x]$，称 $f_1(x),\cdots,f_S(x)$互素，如果$(f_1(x),\cdots,f_S(x))=1$。
定理：$f_1(x),\cdots,f_S(x)$互素的充要条件是存在 $u_1(x),\cdots,u_S(x)$使得$\Sigma u_if_i=1$。
区别：$f_1(x),\cdots,f_S(x)$两两互素条件比 $f_1(x),\cdots,f_S(x)$互素条件强得多！
定理：数域的扩大不改变最大公因式；从而不改变互素性。

7.4 不可约多项式，唯一因式分解定理

不可约多项式：称 $p(x)\in F[x]$是 F[x]中的不可约多项式，如果 p(x)只有平凡的因式。（如果 $h(x)|p(x)$，则 $h(x)=c$ 或者 $h(x)\sim p(x)$）
多项式因式分解的存在唯一性定理：设 $f(x)\in F[x]$，那么存在不可约多项式 $p_1(x),\cdots,p_s(x)$使得 $f(x)=p_1(x)\cdots p_s(x)$；若还有不可约多项式 $q_1(x),\cdots,q_t(x)$使得 $f(x)=q_1(x)\cdots q_s(x)$，那么 s=t，在不记因子的顺序条件下有 $p_i(x)$与 $q_i(x)$相伴。
命题：p(x)是 F[x]中的不可约多项式，$f(x)\in F[x]$，那么则 $p(x)|f(x)$或者$(p,f)=1$。
命题：p(x)是不可约多项式，$f(x),g(x)\in F[X]$，若 $p|fg$，则 $p|f$ or $p|g$。

唯一分解：$f(x)=cp_1(x)^{l_1}p_2(x)^{l_2}\cdots p_s(x)^{l_s}$。其中 $p_i(x)$是互不相同的不可约首“1”多项式，c 是 f(x)的首项系数。
定义：设 $p(x)\in F[x]$，称 p(x)是 F[x]中的素元，如果 p(x)满足性质：对任意 $f,g\in F[x]$，若 $p|fg$，那么 $p|f$ or $p|g$。
命题：在多项式环中，不可约多项式$\Leftrightarrow$素元。

7.5 重因式

多项式的重因式：设 $f(x),p(x)\in F[x]$，p(x)是 F[x]的不可约多项式，k 是一个正整数，称 p(x)是 f(x)的 k 重因式，如果 $p^k(x)||f(x)$。当 k=1 时，称 p(x)是 f(x)的单因式。

多项式的导数：设 $f(x)=\sum_{i=0}^{n}a_ix^i$，f(x)的导数定义为 $f'(x)=\sum_{i=1}^{n-1}ia_ix^{i-1}$。

导数运算满足：1°$(f+g)'=f'+g'$，$(fg)'=f'g+fg'$；2°$(af+bg)'=af'+bg'$。
求导运算是映射：$F[x]\to F[x]$，$f(x)\mapsto f'(x)$。
定理：p(x)是 f(x)的 k 重因式，那么 p(x)是 f'(x)的 k-1 重因式。若 k=1，则 p(x)与 f'(x)互素。
推论：p(x)是 f(x)的(k)重因式($k\geqslant 2$)的充要条件是 $p(x)|(f(x),f'(x))$。
推论：p(x)是 f(x)的单因式$\Rightarrow(p(x),f'(x))=1$。
推论：f(x)没有重因式$\Leftrightarrow(f(x),f'(x))=1$。

定理：设 $f(x)=cp_1^{m_1}\cdots p_s^{m_s}$，$f'(x)=p_1^{m_1-1}\cdots p_s^{m_s-1}h(x)$。其中$(h,p_i)=1,\forall i=1,\cdots,s$。

则$(f,f')=p_1^{m_1-1}\cdots p_s^{m_s-1}$，且 $f=cp_1\cdots p_s(f,f')$。

给定一个多项式，对它进行因式分解的步骤：
1°计算 f'(x)；2°计算$(f',f)=d$；3°若 d(x)=1，寻找 f(x)的不可约因子；若 $d(x)\neq 1$，

计算 f/(f,f')；4° f←f/(f,f')。
一般地，称映射 D:F[x]→F[x]为导子，如果(1)D(af+bg)=aD(f)+bD(g)；(2)D(fg)=D(f)g+D(g)f。
定理：重因式的有无不随数域扩大而改变。

7.6 多项式的根，复数域上的不可约多项式

多项式函数：设 F 是数域，映射φ:F→F 称为多项式函数，如果存在 f(x)∈F[x]使得φ(a)=f(a)。记 F 上的多项式函数集合为 F_{poly}。
定义 F_{poly} 中的代数运算：和：(P+Q)(a)=P(a)+Q(a)；积：(P・Q)(a)=P(a)Q(a)。
命题：多项式函数的和、积仍是多项式函数。
定理：多项式函数也是一个环。
命题：F[x]中的 n 次多项式至多有 n 个根(n≥0)。
命题：设 f,g∈F[x]是 n 次多项式，若有不同的 $a_1,\cdots a_{n+1}$ 使得 $f(a_i)=g(a_i)$，则 f=g。
令映射Φ：F[x]→F_{poly}，f↦Φ(f)，且Φ(f)(a)=f(a)，∀a∈F。则Φ是环同构映射（单射、满射，保持加法、乘法运算）。
Gauss 定理：对∀f(x)∈C[x]，存在 a∈C 使得 f(a)=0。
推论（唯一因式分解定理）：在复数域上，对∀f(x)∈C[x]，存在唯一的一组数 $a_1,\cdots,a_s$，使得 $f(x)=c(x-a_1)^{l_1}\cdots(x-a_s)^{l_s}$。
命题：在 C[x]中 f(x)没有重因式⇔ $f(x)=c(x-a)^m$。
Vieta 定理：设 $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0=(x-c_1)\cdots(x-c_n)$，则 $a_{n-1}=-(c_1+\cdots+c_n)$，$a_{n-k}=(-1)^k\sum\limits_{1\le i_1<\cdots<i_k\le n}c_{i_1}\cdots c_{i_k}$，$a_0=(-1)^nc_1\cdots c_n$。
总结：复数域上的不可约多项式只有一次多项式。
tips:检验 a 是一个多项式的根，可以利用(x-a)的带余除法。

7.7 实数域上的不可约多项式

实数域上的多项式：(1)ax+b∈R[x]不可约；(2)$ax^2+bx+bc$∈R[x]不可约⇔ $b^2-4ac\leqslant 0$；(3)在数学分析学过，奇次多项式一定有实根。
命题：f(x)∈R[x]，c∈C，若 f(c)=0，则 $f(\overline{c})=0$。即实多项式的非实根成对出现。
推论：f(x)∈R[x]，f(x)的非实根个数是偶数个。
定理：对 n 次多项式 f(x)∈R[x]，设 $r_1,r_2,\cdots,r_s$ 是 f(x)的全部实根，$c_1,\overline{c_1},\cdots,c_t\overline{c_t}$ 是 f(x)的全部复根，则 $f(x)=\prod\limits_{i=1}^{s}(x-r_i)\prod\limits_{i=1}^{t}(x-c_i)(x-\overline{c_i})=\prod\limits_{i=1}^{s}(x-r_i)\prod\limits_{i=1}^{t}(x^2-(c_i+\overline{c_i})x+c_i\overline{c_i})$。
容易证明：$x^2-(c_i+\overline{c_i})x+c_i\overline{c_i}\in$R[x]。（该分解也是唯一的）
定理：实多项式 p(x)不可约⇔ p(x)是一次多项式或者二次多项式 ax^2+bx+c，其中 $b^2-4ac<0$。
总结：实数域上的不可约多项式只有一次多项式和判别式＜0 的二次多项式。

7.8 有理数域上的不可约多项式

命题：任意 f(x)∈Q[x]，存在 g(x)∈Z[x]使得 f(x)与 g(x)相伴。
本原多项式：$g(x)=a_nx^n+\cdots+a_1x+a_0$∈Z[x]，且$(a_0,a_1,\cdots,a_n)=1$。
定理：两个本原多项式 g(x),h(x)在 Q[x]中相伴当且仅当 g(x)=±h(x)。

Gauss 引理：本原多项式的乘积仍然是本原多项式。
推论：若 f(x),g(x)∈Z[x]是本原多项式，且在 Q[x]中 g(x)|f(x)，则 f(x)=g(x)h(x)，则 h(x)是本原多项式。
定义：设 p(x)∈Z[x]，称 p(x)是不可约本原多项式，如果(1) p(x)是本原多项式；(2) p(x)在 Q[x]上不可约。
定理：任一本原多项式都可以唯一的分解为不可约本原多项式的乘积。（在相伴意义下）
定理：整系数多项式如果在 Q 上可约，则可分解为整系数多项式乘积。
定理：设 $f(x)=a_nx^n+\cdots+a_1x+a_0\in Z[x]$。如果 $x=\frac{s}{r}$(既约)是 f(x)的根，则 $s|a_0$，$r|a_n$。
Eisenstein 判别法：设 $f(x)=a_nx^n+\cdots+a_1x+a_0$ 是一个次数 n 大于零的整系数多项式，如果存在一个素数 p，使得 1° $p|a_i$，i=0,1,⋯,n-1；2° $p\nmid a_n$；3° $p^2\nmid a_0$。则 f(x)在 Q[x]上不可约。
命题：对于 f(x)∈F[x]，f(x)不可约⇔ f(x+a)不可约。
tips:关于整系数多项式可约性质的一些做法与注意事项。
1. 有有理根 c，从而推出 x-c|f(x)，可约；
2. 无有理根，并不能导出不可约；（这是因为因式不一定是一次的）
3. 直接或移位 Eisenstein 判别法导出不可约；
4. 整系数多项式在 Q[x]可约，就能分解成两个整系数多项式的乘积；（但这并不意味着一定有有理数根，因为因式完全有可能是高次幂的）
5. 利用 a_n,a_0 判别法判断是否有有理数根；有，则可约；无，则未必不可约。
tips:本原多项式的判别及用途。
1. 首项系数为“1”的整系数多项式一定是本原多项式；
2. 若某首“1”多项式有有理数根，由 a_n,a_0 判别法知其必为整数根；
3. 设该整数根为 c，则 f(x)=(x-c)h(x)，则 h(x)也是首“1”的本原多项式。

7.9 多元多项式环

设 $t_1,t_2,\cdots,t_n$ 是未知变元：$\sigma_1(t_1,\cdots,t_n)=\sum_{i=1}^{n}t_i,\sigma_i=\sum_{1\le k_1<\cdots<k_i\le n}t_{k_1}t_{k_2}\cdots t_{k_i},\sigma_n=t_1t_2\cdots t_n$；

$r(t_1,\cdots,t_n)=\prod_{1\le i<j\le n}(t_i-t_j)^2$。且所有函数与 $t_1,\cdots,t_n$ 的排列顺序无关。

给定域 F，$x_1,x_2,\cdots,x_n$ 是独立的未知变元。
定义：$F[x_1,x_2,\cdots,x_n]=F[x_1][x_2]\cdots[x_n]$。
一般地，设 R 是整环，R[x]也是整环。推论：环 $F[x_1,x_2,\cdots,x_n]$是整环。
$F[x_1,\cdots,x_n]$的元素 $f(x_1,\cdots,x_n)=\sum_{i_1,\cdots i_n}a_{i_1,\cdots,i_n}x_1^{i_1}\cdots x_n^{i_n}$ 有限和，$i_1,\cdots,i_n$ 是非负整数。

称 $a_{i_1,\cdots,i_n}x_1^{i_1}\cdots x_n^{i_n}$ 是 $F[x_1,\cdots,x_n]$中的单项式。

全次数：单项式 $a_{i_1,\cdots,i_n}x_1^{i_1}\cdots x_n^{i_n}$ 的全次数定义为 $i_1+i_2+\cdots+i_n$；

多项式 $f(x_1,\cdots,x_n)=\sum_{i_1,\cdots i_n}a_{i_1,\cdots,i_n}x_1^{i_1}\cdots x_n^{i_n}$ 的全次数 $\deg f=\max\{i_1+i_2+\cdots+i_n|a\neq0\}$.

全次数是 0 的项只有常数项。

齐次多项式：对自然数 m，称 $f(x_1,\cdots,x_n)$为 m 次齐次多项式，如果 a=0，当 $i_1+i_2+\cdots+i_n\neq m$ 时。
对 $f\in F[x_1,x_2,\cdots,x_n]$，则存在 m 次齐次多项式 f_m 使得 $f=f_0+f_1+\cdots+f_n$。
性质：$\deg f\pm g\leqslant\max\{\deg f,\deg g\}$，$\deg fg = \deg f + \deg g$。
字典顺序：$(i_1,\cdots,i_n)>(j_1,\cdots,j_n)$：存在 s 使得 $i_1=j_1,\cdots,i_s=j_s$，且 $i_{s+1}>j_{s+1}$。
首项：字典顺序最大的那项。
命题：$f,g\in F[x_1,\cdots,x_n]$，则首项(fg)=首项(f)*首项(g)。
给定 $f\in F[x_1,\cdots,x_n]$，定义函数：φ_f：$F^n\to F$，$(a_1,\cdots,a_n)\to f(a_1,\cdots,a_n)$称为 F^n 上对应于 F 的多项式函数。
定理：设 F 是数域，对任意 $f_1,f_2\in F[x_1,\cdots,x_n]$，若$\varphi_{f1}=\varphi_{f2}$，则 $f_1=f_2$。
推广：当 F 是无限域时，多项式环和多项式函数环同构。

7.10 对称多项式

设 F 是域，$F[x_1,x_2,\cdots,x_n]$是 F 上的以 $x_1,x_2,\cdots,x_n$ 为未定元的多项式环。定义：设 $f(x_1,\cdots,x_n)\in F[x_1,\cdots,x_n]$是对称多项式，如果 $f(x_1,\cdots,x_n)=f(x_{i1},\cdots,x_{in})$，对于$(1,2,\cdots,n)$的任一排列$(i_1,\cdots,i_n)$。
注：1° 常值多项式是对称多项式；
2° $\sigma_1(x_1,\cdots,x_n)=\sum_{i=1}^{n}x_i$；$\sigma_i(x_1,\cdots,x_n)=\sum_{1\le k_1<\cdots<k_i\le n}x_{k_1}\cdots x_{k_i}$；$\sigma_n(x_1,\cdots,x_n)=x_1\cdots x_n$；称为基本对称多项式；
令 S 是 $F[x_1,\cdots,x_n]$中的对称多项式的集合，容易验证 S 是 $F[x_1,\cdots,x_n]$的子环。
推论：设 $g(x_1,\cdots,x_n)\in F[x_1,\cdots,x_n]$，若 $f_1,\cdots,f_n\in S$，则 $g(f_1,\cdots,f_n)\in S$。
命题：设 S_n 表示 $F[x_1,\cdots,x_n]$对称多项式构成的子环，S_{n-1} 表示 $F[x_1,\cdots,x_{n-1}]$ 构成的子环。对任意 $f(x_1,\cdots,x_n)\in S_n$，则 $f(x_1,\cdots,x_{n-1})\in S_{n-1}$。
特别地，对于基本多项式，有$\sigma_i(x_1,\cdots,x_{n-1},0)=\sigma_i(x_1,\cdots,x_{n-1})$。
定理：设 $f(x_1,\cdots,x_n)\in S_n$，那么唯一存在 $g(x_1,\cdots,x_n)\in F[x_1,\cdots,x_n]$，使得 $f(x_1,\cdots,x_n)=g(\sigma_1,\cdots,\sigma_n)$。
Newton 公式：记 $s_i=x_1^i+\cdots+x_n^i$。有递推公式：
$1\leqslant k\leqslant n$ 时：$s_k-\sigma_1 s_{k-1}+\cdots+(-1)^{k-1}\sigma_{k-1}s_1+(-1)^k k\sigma_k=0$；
$k>n$ 时：$s_k-\sigma_1 s_{k-1}+\cdots+(-1)^{k-1}\sigma_{n-1}s_{k-n+1}+(-1)^k\sigma_n s_{k-n}=0$。
判断一个方程在复数域上有没有重根：$\prod_{1\le i<j\le n}(c_i-c_j)^2=$

$$\begin{vmatrix} n & \sum_{i=1}^{n}c_i & \cdots & \sum_{i=1}^{n}c_i^{n-1} \\ \sum_{i=1}^{n}c_i & \sum_{i=1}^{n}c_i^2 & \cdots & \sum_{i=1}^{n}c_i^{n} \\ \vdots & \vdots & & \vdots \\ \sum_{i=1}^{n}c_i^{n-1} & \sum_{i=1}^{n}c_i^{n} & \cdots & \sum_{i=1}^{n}c_i^{2n-2} \end{vmatrix}$$

上式记为某个方程的判别式 D(f)。
在上述讨论中，f(x)首项系数为 1。如果 f(x)首项系数为 a_n，先算出 $a_n^{-1}f(x)$的判别式，然后规定 f(x)的判别式为 $a_n^{2n-2}D(a_n^{-1}f)$。

7.11 模 m 剩余类环，域，域的特征

设 Z 是整数环，N 是正整数，称 $a,b\in Z$ 是模 N 同余的，如果 M|a-b。模 N 同余是 Z中的等价关系。记 a'表示模 N 与 a 的全体整数的等价类。
令 Z/NZ={a'|a∈Z}={0',1',⋯,(N-1)'}。规定加法运算：a'+b'=(a+b)'；乘法运算：a'・b'=(ab)'。
当 N 是合数时，Z/NZ 有零因子。
令$(Z/NZ)^x$={a'|(a,N)=1}。1° 乘法封闭；2° 满足结合律；3° 单位元 1'存在；4° 任意 $a'\in(Z/NZ)^x$，存在逆元 b'∈Z/NZ 使得 a'b'=1'。∴$(Z/NZ)^x$构成一个群。
当 N 是素数 p 时，$(Z/pZ)^x$所有非零元都是可逆元。

定义：设 F 是非空集合，有加法运算和乘法运算，称 F 是域，如果 F 是有单位元 1 的交换环，并且每个非零元都是可逆元。（域一定无零因子）
定义：F 中有单位元 1，若任意 $n\in Z$，$n\cdot 1\neq 0$，则称 F 是特征 0 域；若存在 $m\in Z$，$m\cdot 1=0$，则称 F 是有限特征 域。
命题：若 F 是有限特征域，那么存在唯一的素数 p 使得 $pa=0$，对任意 $a\in F$。
定义：若 F 是域，存在素数 $p\in Z$，使得 $pa=0$，任意 $a\in F$。则称 F 是特征 p 的域。
推论：任意的域，它们的特征要么是 0，要么是 p。
tips：两个元素相乘=0，那么他们一定都不可逆。
在 Z_p 上不可约的整系数多项式在 Q 上也不可约。

第 8 章 线性空间

8.1 线性空间的结构

设 F 是域，F^n 有两个运算：$F^n\times F^n\to F^n$，$(\alpha,\beta)\to\alpha+\beta$称为向量加法；$F\times F^n\to F^n$，$(a,\alpha)\to a\alpha$称为数量乘法。满足 8 个性质：
1°加法交换律；2°加法结合律；3°零元存在；4°负元存在；5°单位元存在；6°数乘结合律；7°数乘左分配律；8°数乘右分配律
定义：设 F 是域，V 是非空集合。有两个运算，一个加法运算$(V\times V\to V)$，一个数乘运算$(F\times V\to V)$，满足以上 8 个性质。称$(V,F,+,\cdot)$是一个线性空间，简称 V 是 F-线性空间。
例：数域、特征 p 域、F[x]、C 是 R-线性空间，F[x]/f(x)F[x]是 F-线性空间。
设 V 是 F-线性空间：1°零元唯一；2°负元唯一；3°$0\alpha=0$；4°$-\alpha=(-1)\alpha$；5°$k0=0$；6°若 $k\alpha=0$，则 $k=0$ 或$\alpha=0$
定义：设 F 是域，V 是 F-线性空间，1°设$\alpha_1,\cdots,\alpha_n\in V$，$a_i\in F$，称$\Sigma a_i\alpha_i\in V$称为向量$\alpha_i$的线性组合；2°对$\forall\alpha_i\in V$，$\beta\in V$，若存在 $a_i\in F$ 使$\beta=\Sigma a_i\alpha_i$，则β可由α_i线性表示；3°设$\alpha_1,\cdots,\alpha_n\in V$，称向量组是线性相关的，如果存在不全为 0 的 $a_i\in F$，使得$\Sigma a_i\alpha_i=0$；4°称向量组是线性无关的，如果$\Sigma a_i\alpha_i=0$ 则 $a_i=0$；
3*设$\{a_i\}(i\in I)$是 V 的向量组，称这个向量组线性相关，存在 I 的有限子集 I_A 使得$\{a_i\}(i\in I_A)$是线性相关的。
4*称向量组线性无关，如果对 I 的任意有限子集 I_A 都有$\{a_i\}(i\in I_A)$线性无关。
例：在线性空间 F[x]中，$1,x,\cdots,x^n$ 是 F-线性无关的。
命题：向量组$\{a_i\}(i\in I)$是线性相关的$\Leftrightarrow$存在 $i_0\in I$，使得 a_{i0} 可由$\{a_i\}(i\in I\backslash\{i_0\})$线性表示。
定义：设$\{a_i\}(i\in I)$是 V 的向量组，J 是 I 的子集，称向量组$\{a_i\}(i\in J)$是$\{a_i\}(i\in I)$的极大无关组，如果$\{a_i\}(i\in J)$线性无关，且对任意 $i\in I$，则 a_i 均可由$\{a_i\}(i\in J)$线性表示。
定义：设$\{a_i\}(i\in I)$,$\{\beta_i\}(i\in J)$是 V 的两个向量组，称它们等价，如果$\{a_i\}$可由$\{\beta_i\}$线性表示且$\{\beta_i\}$可由$\{a_i\}$线性表示。等价的向量组的极大线性无关组向量个数相同。
定义：设$\{a_i\}(i\in I)$是 V 的向量组，向量组的秩是极大线性无关组的向量个数。
定义：设$\alpha_1,\cdots,\alpha_n\in V$，则集合 $V=V_1\{\Sigma k_ia_i|k_i\in F\}$是一个 F-线性空间。由$\alpha_1,\cdots,\alpha_n$生成的 F-线性空间记为$<\alpha_1,\cdots,\alpha_n>$。
定义：设 V 是 F-线性空间，I 是一个集合，$\alpha_i\in V$，$i\in I$。称$\{a_i\}(i\in I)$是 V 的一组基，如果 1°$\{a_i\}(i\in I)$是线性无关的；2°任意$\beta\in V$，β可由$\{a_i\}(i\in I)$线性表示。如果 I 是有限，称 V 是有限维线性空间；如果 I 是无限的，就称为无限维线性空间。
例：F^n 是 n 维 F-线性空间；$M_{m\times n}(F)$是 $m\times n$ 维线性空间；C 是 Q-无限维空间；R 是无限维 Q-线性空间

定理：设$\alpha_1,\cdots,\alpha_n$是 V 的一组基，那么映射$\theta:V\to F^n$，$\alpha\to(a_1,a_2,\cdots,a_n)$(坐标)，则$\theta$是一个双射，保加法，保数乘。
过渡矩阵：$\alpha_1,\cdots,\alpha_n$和$\beta_1,\cdots,\beta_n$是 V 的两组基，则$(\beta_1,\cdots,\beta_n)=(\alpha_1,\cdots,\alpha_n)A$，其中 A 是可逆矩阵。
可以定义映射φ把$\{\beta_1,\cdots,\beta_n|\beta_1,\cdots,\beta_n$是 V 的基$\}$映射成 $A\in GLn(F)$(n 阶可逆矩阵群)
$A\in GLn(F)\Leftrightarrow$ A 的列(行)向量是 F^n 的基。

坐标变换公式：设$\alpha_1,\cdots,\alpha_n$和$\beta_1,\cdots,\beta_n$是 V 的两组基，对$\alpha\in V=\sum_{i=1}^{n}a_i\alpha_i=\sum_{i=1}^{n}b_i\beta_i$，

令$(\beta_1,\cdots,\beta_n)=(\alpha_1,\cdots,\alpha_n)T$ 的过渡矩阵，则有$(a_1,\cdots,a_n)^T=T(b_1,\cdots,b_n)^T$。

tips:一个线性空间的基可以是无限多个，但是所有元素都必须使用**有限**个基表出。

8.2 子空间及其交与和，子空间的直和

定义：设 V 是 F-线性空间，V 的非空子集 V_0 称为 V 的子空间，如果 V_0 在 V 的加法和数乘下仍然是一个线性空间。
命题：线性空间 V 的非空子集 V_0 是 V 的子空间的充分必要条件是 V_0 对于 V 的加法和数乘封闭。
命题：若 V 是 n 维 F-线性空间，U 是 V 的子空间，则 $\dim U\leqslant n$。
命题：设 U_1,U_2 是 V 的子空间，若 $U_1\subseteq U_2$，$\dim U_1=\dim U_2$，则 $U_1=U_2$。
命题：若 $\dim V=n$，则 V 中任意 n+1 个向量线性相关。
子空间运算：设 V_1 和 V_2 是 V 的子空间：$V_1\cap V_2$ 是 V 的子空间。V_1+V_2 是 V 的子空间。$(V_1+V_2=\{\alpha+\beta|\alpha\in V_1,\beta\in V_2\})$
定理：设 V_1,V_2 是 V 的一个子空间，则 $\dim(V_1\cap V_2)+\dim(V_1+V_2)=\dim V_1+\dim V_2$。
子空间的直和：设 V_1,V_2 是 V 的子空间，称 V 是 V_1 和 V_2 的直和，如果对任意的$\alpha\in V$，都存在唯一的一组向量$\alpha_1\in V_1,\alpha_2\in V_2$使得$\alpha=\alpha_1+\alpha_2$。(记为 $V=V_1\oplus V_2$)
命题：设 V_1,V_2 是 V 的子空间，下列条件是等价的：
1° V 是 V_1 和 V_2 的直和；2° V 中的零元素表示唯一；3° $V=V_1+V_2,V_1\cap V_2=0$；
4° $\dim V=\dim V_1+\dim V_2$
推广：设 V_i 是 V 的子空间，若 $V=\Sigma V_i$，称 V 是 V_i 的直和，如果对任意的$\alpha\in V$，存在唯一一组$\alpha_i\in V_i$使得$\alpha=\Sigma\alpha_i$，记为 $V=\oplus V_i$。

8.3 线性空间的同构

定义：设 V_1,V_2 是两个 F-线性空间，映射$\varphi:V_1\to V_2$称为 F-线性同构，如果 1° φ是双射；2° φ保运算：$\varphi(\alpha+\beta)=\varphi(\alpha)+\varphi(\beta)$，$\varphi(a\alpha)=a\varphi(\alpha)$。
同构映射的性质：1° $\varphi(0)=0$；2° $\alpha_1,\cdots,\alpha_s$线性相关$\Leftrightarrow\varphi(\alpha_1),\cdots,\varphi(\alpha_n)$线性相关。
推论：V_1 与 V_2 同构的充要条件是 $\dim V_1=\dim V_2$。
推论：任意 n 维 F-线性空间同构于 F^n，F-空间的线性同构构成它的一个等价关系。
命题：设 V_1,V_2 是 V 的子空间，$V=V_1\oplus V_2$ 的充要条件是 V 同构于 $V_1\times V_2$。
命题：设 V 是 F-线性空间，V_1 是 V 的子空间，则存在 V_2 是 V 的子空间，使得 $V=V_1\oplus V_2$。(注：这样的 V_2 并不唯一，这是因为**基的扩充方式有很多**)
(理解：R^2 为 V_1=xy 平面，想要扩充成 R^3，可以补充 V_2=Z 轴，也可以补充 V_2=任意一条不在 xy 平面上的直线)
若 $V=V_1\oplus V_2$，对任意$\alpha\in V$，存在唯一的$\alpha_1\in V_1,\alpha_2\in V_2$使得$\alpha=\alpha_1+\alpha_2$，则令映射$\pi_i$：$V\to V_i$，$\alpha\mapsto\alpha_i$是满射，保持线性运算，这类映射称为 V 沿直和分解的投影。

8.4 商空间

设 F 是域，V 是 F-线性空间，V_1 是 V 的子空间，称 V 的元素 α_1,α_2 关于 V_1 是等价的，如果 $\alpha_1-\alpha_2\in V_1$。

命题：V 中元素关于 V_1 的等价是 V 的等价关系。

记 V 关于 V_1 等价为 $\tilde{V_1}$，x_1 与 x_2 关于 V_1 等价，记为 $x_1 \overset{V_1}{\sim} x_2$。

定义 V 对于子空间 V_1 的商集 $V/V_1=\{\bar{v}=v+V_1 \mid v\in V\}$

在集合 V/V_1 中定义运算：对任意 $\alpha,\beta\in V$，规定：$\bar{\alpha}+\bar{\beta}=\overline{\alpha+\beta}$；$k\bar{\alpha}=\overline{k\alpha}$。

V/V_1 是 F-线性空间，称为 V 关于子空间 V_1 的商空间。

定理：设 V 是 n 维向量空间，V_1 是 V 的 k 维子空间，则 V/V_1 是 n-k 维空间。

定理：设 V_1 是 V 的子空间，$\alpha_1,\cdots,\alpha_k$ 是 V_1 的一组基，$\alpha_1,\cdots,\alpha_k,\alpha_{k+1},\cdots,\alpha_n$ 是 V 的一组基，则 $\overline{\alpha_{k+1}},\cdots\overline{\alpha_n}$ 是 V/V_1 的基。

定理：若 $V=V_1\oplus V_2$，则 $V/V_1=\{\bar{\alpha}\mid\alpha\in V_2\}$.

第 9 章 线性映射

9.1 线性映射及其运算

设 V_1,V_2 是 F-线性空间，映射 $\varphi:V_1\to V_2$ 称为 F-线性映射，如果 1° $\varphi(\alpha+\beta)=\varphi(\alpha)+\varphi(\beta)$；2° $\varphi(a\alpha)=a\varphi(\alpha)$，$a\in F$，$\alpha,\beta\in V_1$。（即：$\varphi(a\alpha+b\beta)=a\varphi(\alpha)+b\varphi(\beta)$）

命题：$\varphi:V_1\to V_2$ 是 F-线性的，那么 $\varphi(0)=0$；把线性组合映成线性组合。

设 F 是域，m,n 是正整数，$A\in M_{m\times n}(F)$，那么映射 $\varphi_A:F^n\to F^m$，$\alpha\to A\alpha$，则 φ_A 是 F-线性的。

命题：设 $\varphi:V_1\to V_2$，$\psi:V_2\to V_3$，那么 $\psi\circ\varphi$ 也是 F-线性的。

记 $Hom_F(V_1,V_2)$ 表示从 V_1 到 V_2 的 **F-线性映射**组成的集合。

若 $\varphi_1,\varphi_2\in Hom_F(V_1,V_2)$，定义：$(\varphi_1+\varphi_2)(\alpha)=\varphi_1(\alpha)+\varphi_2(\alpha)$，$(a\varphi)(\alpha)=a\varphi(\alpha)$，$\alpha\in V_1$，$a\in F$。

定理：$Hom_F(V_1,V_2)$ 在加法和数量乘法下是 F-线性空间。

当 $V_1=V_2=V$ 时，$Hom_F(V,V)$ 记为 $End_F(V)$，它的元素称为 V 的线性变换。

$End_F(V)$ 在“+”和“∘”是一个环。

映射 $\varphi:V\to V$，$\alpha\to a\alpha$ 是线性变换，称为纯量线性变换，记为 aI_V，其中 I_V 是恒等线性变换。

定义映射 $\varphi:F\to End_F(V)$，$a\to aI_V$ 是单射，把 F 与 FI_V 等同起来，$F\subset End_F(V)$。

由多项式环的通用性，对任意 $\varphi\in End_F(V)$，$F[\varphi]=\{f(\varphi)\mid f(x)\in F[x]\}$ 是 $End_F(V)$ 的子环，其中 $\varphi^0=I_V$，$f(\varphi)=a_0I_V+a_1\varphi+\cdots\cdots+a_n\varphi^n$。

9.2 线性映射的核与象

定义：设 $\varphi:V_1\to V_2$ 是 F-线性空间的线性映射，称 $\varphi^{-1}(0)$ 为 φ 的核。记为 $Ker(\varphi)$。

称映射 φ 的象为线性映射 φ 的象，记为 $Im(\varphi)$。

命题：线性映射 φ 的核 $Ker\ \varphi$ 是 V_1 的子空间、象 $Im\ \varphi$ 是 V_2 的子空间。

定理：设 $\varphi:V_1\to V_2$ 是 F-线性映射，那么 $\dim(Ker(\varphi))+\dim(Im(\varphi))=n$。

定理：设 φ 是线性映射，称象空间的维数为映射 φ 的秩。

推论 1：设 $\varphi:V_1\to V_2$ 是 F-线性映射，那么映射 $\varphi':V_1/Ker(\varphi)\to Im(\varphi)$，$\alpha+Ker(\varphi)\to\varphi(\alpha)$ 是 F-线性空间同构。

推论 2：任意$\beta\in\mathrm{Im}(\varphi)$，$\varphi^{-1}(\beta)=\{\alpha\in V_1|\varphi(\alpha)=\beta\}$；若$\alpha_0\in\varphi^{-1}(\beta)$，则$\varphi^{-1}(\beta)=\alpha_0+\mathrm{Ker}(\varphi)$。

9.3 线性映射的矩阵表示

定理：设 V_1,V_2 是有限维的 F-线性空间，$\alpha_1,\cdots,\alpha_n$ 是 V_1 的基，$\beta_1,\cdots,\beta_m$ 是 V_2 的基，则映射$\Phi:\mathrm{Hom}_F(V_1,V_2)\to M_{m\times n}(F)$，$\varphi\to A$，满足$(\varphi(\alpha_1),\cdots,\varphi(\alpha_n))=(\beta_1,\cdots,\beta_m)A$ 是 F-线性空间同构的。

定理：设 V_1,V_2 是有限维 F-线性空间，$\dim V_1=\dim V_2$，$\varphi:V_1\to V_2$ 是 F-线性映射，则φ是单射的充要条件是φ是满射。

引理：设 V_1,V_2 是 F-线性空间，$\alpha_1,\cdots,\alpha_n$ 是 V_1 的基，对任意$\beta_1,\cdots,\beta_n\in V_2$，都存在唯一的线性映射$\varphi:V_1\to V_2$ 使得$\varphi(\alpha_i)=\beta_i$。

定理：设 V 是 n 维 F-线性空间，$\alpha_1,\cdots,\alpha_n$ 是 V 的一组基，则映射$\Phi:\varphi\in\mathrm{End}_F(V)\to A\in M_n(F)$是环同构，其中$(\varphi(\alpha_1),\cdots,\varphi(\alpha_n))=(\alpha_1,\cdots,\alpha_n)A$。

在同构Φ下，n 阶可逆矩阵的集合 $GL_n(F)$的原象记为 $\mathrm{Aut}(V)=\{\varphi\in\mathrm{End}_F(V)|\varphi$是同构$\}$。

定理：设 V 是 n 维 F-线性空间，$\alpha_1,\cdots,\alpha_n$ 和$\beta_1,\cdots,\beta_n$ 是 V 的两组基，设$\varphi\in\mathrm{End}_F(V)$，$\varphi(\alpha_1,\cdots,\alpha_n)=(\alpha_1,\cdots,\alpha_n)A$，$\varphi(\beta_1,\cdots,\beta_n)=(\beta_1,\cdots,\beta_n)B$，设$(\beta_1,\cdots,\beta_n)=(\alpha_1,\cdots,\alpha_n)T$，$T\in GL_n(F)$，则 $B=T^{-1}AT$。

定理：设$\varphi:V_1\to V_2$ 是 F-线性空间同构，φ^{-1} 是φ的逆映射，则φ^{-1} 是线性同构。

9.4 线性变换的特征值与特征向量，线性变换可对角化的条件

定义：设$\varphi\in\mathrm{End}_F(V)$，设$\lambda\in F$，称$\lambda$是$\varphi$的特征值，如果存在$\alpha\in V(\alpha\neq 0)$，使得$\varphi(\alpha)=\lambda\alpha$，称$\alpha$是属于$\varphi$的特征向量。记 $V_\lambda=\{\alpha\in V|\varphi(\alpha)=\lambda\alpha\}$，当$\lambda$是$\varphi$的特征值时，$V_\lambda\neq 0$。

命题：V_λ是 V 的子空间。

定义：设$\varphi\in\mathrm{End}_F(V)$，$\alpha_1,\cdots,\alpha_n$ 是 V 的基，$\varphi(\alpha_1,\cdots,\alpha_n)=(\alpha_1,\cdots,\alpha_n)A$，定义$\varphi$的特征多项式为 $f_\varphi(\lambda)=f_A(\lambda)$。

定理：设$\varphi\in\mathrm{End}_F(V)$，$\alpha_1,\cdots,\alpha_n$ 是 V 的基，$\varphi(\alpha_1,\cdots,\alpha_n)=(\alpha_1,\cdots,\alpha_n)A$，那么：

1° λ是φ的特征值$\Leftrightarrow\lambda$是 A 的特征值；2° 映射$\alpha\in V_\lambda\to(F^n)_\lambda(\varphi_A)$是同构。

定义：称线性变换φ是可对角化的，如果存在 V 的一组基$\alpha_1,\cdots,\alpha_n$ 使得$\varphi(\alpha_i)=\lambda_i\alpha_i$。

定理：设$\varphi\in\mathrm{End}_F(V)$，$\alpha_1,\cdots,\alpha_n$ 是 V 的基，$\varphi(\alpha_1,\cdots,\alpha_n)=(\alpha_1,\cdots,\alpha_n)A$，则$\varphi$可对角化的充要条件是 A 可对角化。

定理：设$\varphi\in\mathrm{End}_F(V)$，下列条件等价：

1° φ可对角化；2° $f_\varphi(\lambda)=\prod_{i=1}^{s}(\lambda-\lambda_i)^{m_i},\dim V_{\lambda_i}=m_i$；3° $V=\oplus_{i=1}^{s}V_{\lambda_i}$。

命题：属于不同特征子空间的向量线性无关。

9.5 线性变换的不变子空间

定义：设$\varphi\in\mathrm{End}_F(V)$，$V_1$ 是 V 的子空间，称 V_1 是φ的不变子空间，如果对$\forall\alpha\in V_1$ 都有$\varphi(\alpha)\in V_1$。

命题：设$\varphi\in\mathrm{End}_F(V)$，则 1° $\mathrm{Ker}(\varphi)$、$\mathrm{Im}(\varphi)$；2° $\forall f(x)\in F[x]$，$\mathrm{Ker}(f(\varphi))$、$\mathrm{Im}(f(\varphi))$是φ-不变子空间。

定义：设$\varphi\in\mathrm{End}_F(V)$，$V_1$ 是φ-不变子空间，映射$\varphi|V_1:V_1\to V_1$，定义为对$\forall\alpha\in V_1$，$\varphi|V_1(\alpha)=\varphi(\alpha)$，称映射$\varphi|V_1$ 是φ在 V_1 上的限制，$\varphi|V_1\in\mathrm{End}(V_1)$。

命题：设$\varphi\in\mathrm{End}_F(V)$，$V_1$ 是φ-不变子空间，则映射$\varphi':V/V_1\to V/V_1$，$\alpha+V_1\to\varphi(\alpha)+V_1$ 是线性变换。称φ'是φ在商空间 V/V_1 上的诱导线性变换。

定理：设$\varphi\in\mathrm{End}_F(V)$，$V_1$ 是φ-不变子空间，$\varphi_1=\varphi|V_1$，φ'是φ的诱导线性变换，则 $f_\varphi(\lambda)=f_{\varphi_1}(\lambda)f_{\varphi'}(\lambda)$。（化归基-矩阵证明之）

定理：设 $V=V_1\oplus V_2$，$\varphi\in End_F(V)$，V_i 是φ-不变子空间，$\alpha_1,\cdots,\alpha_r$ 是 V_1 的基，$\alpha_{r+1},\cdots,\alpha_n$ 是 V_2 的基，$\varphi(\alpha_1,\cdots,\alpha_r)=(\alpha_1,\cdots,\alpha_r)A_1$，$\varphi(\alpha_{r+1},\cdots,\alpha_n)=(\alpha_{r+1},\cdots,\alpha_n)A_2$，这里 $A_1\in M_r(F)$，$A_2\in M_{n-r}(F)$，则$\varphi(\alpha_1,\cdots,\alpha_n)=(\alpha_1,\cdots,\alpha_n)\begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}$。

定理：设$\varphi\in End_F(V)$，$f(\lambda)=g(\lambda)h(\lambda)\in F[\lambda]$，若$(g(\lambda),h(\lambda))=1$，则 $Ker(f(\varphi))=Ker(g(\varphi))\oplus Ker(h(\varphi))$。

推论：设 $f(\lambda)\in F[\lambda]$，$f_i(\lambda)\in F[\lambda]$，且 $f(\lambda)=\prod_{i=1}^{s} f_i(\lambda)$，且$\{f_i\}$是两两互素的，那么对任意$\varphi\in End_F(V)$，则 $Kerf(\varphi)=\oplus_{i=1}^{s}Ker(f_i(\varphi))$。

推论：设 $A\in M_n(F)$，$f(\lambda)=\prod_{i=1}^{s}(\lambda-\lambda_i)^{m_i}$ 是 A 的特征多项式，则 $Ker\ f(A)=\oplus_{i=1}^{s}Ker\ (\lambda_i I-A)^{m_i}$。

定义：对于$\varphi\in End_F(V)$，$A\in M_n(F)$，若多项式 $f(x)\in F[x]$使得 $f(\varphi)=0(f(A)=0)$，称 $f(x)$ 是$\varphi(A)$的零化多项式。

9.6 Hamilton-Cayley 定理

定理：设 $A\in M_n(F)$，$f(\lambda)$是 A 的特征多项式，则 $f(A)=0$。

注：此定理的结果依赖于：1° $M_n(F)[x]=M_n(F[x])$；2° $(\lambda I-A)^*(\lambda I-A)=f(\lambda)I_n$。

推论：矩阵 A 或线性变换φ的特征多项式是它的零化多项式。

例：单位矩阵的零化多项式是λ-1。

分块对角矩阵的零化多项式是 $f(\lambda)=\prod_{i=1}^{s}(\lambda-\lambda_i)^{m_i}$ 或 $d(\lambda)=\prod_{i=1}^{s}(\lambda-\lambda_i)$。

9.7 线性变换的最小多项式

定义：设 $A\in M_n(F)$，$\varphi\in End_F(V)$，称 $A(\varphi)$的零化多项式 $d(\lambda)$为 A 的极小多项式，如果 1° $d(A)=0$，2° 任意 $f\in F[\lambda]$，若 $f(A)=0$，则有 $d(\lambda)|f(\lambda)$，3° 是首一的。

定理：A 可对角化的充要条件是 $d_A(\lambda)$没有重根。

定理：矩阵 $A\in M_n(F)$的 $f_A(\lambda),d_A(\lambda)$不随域的扩张而改变。若 F 是数域，$A\in M_n(F)$，$B\in M_n(F)$，若 A 与 B 相似，则 $d_A(\lambda)=d_B(\lambda)$。

定理：设 $A\in M_n(F)$，则 c 是 $d_A(\lambda)$的充分必要条件是 c 是 $f_A(\lambda)$的根($c\in C$)。

推论：设 $A\in M_n(F)$，$f_A(\lambda)=\prod_{i=1}^{s}(\lambda-\lambda_i)^{m_i}$，其中$\lambda_1,\cdots,\lambda_s$ 是 $f_A(\lambda)$的不同特征值，m_i 是正整数，那么 $d_A(\lambda)=\prod_{i=1}^{s}(\lambda-\lambda_i)^{e_i}$，其中 $1\leqslant e_i\leqslant m_i$。

推论：设 $A\in M_n(F)$，$f_A(\lambda)=\prod_{i=1}^{s}P_i(\lambda)^{m_i}$ 是 $f_A(\lambda)$在 $F[\lambda]$的不可约因式分解，则

$d_A(\lambda)=\prod_{i=1}^{s}P_i(\lambda)^{e_i}$，其中 $1\leqslant e_i\leqslant m_i$。

定理：设$\varphi\in End_F(V)$，$f_\varphi(\lambda)=\prod_{i=1}^{s}P_i(\lambda)^{m_i}$，$d_\varphi(\lambda)=\prod_{i=1}^{s}P_i(\lambda)^{e_i}$，$1\leqslant e_i\leqslant m_i$，

则 $V=\oplus_{i=1}^{s}Ker\,(P_i(\varphi))^{m_i})=\oplus_{i=1}^{s}Ker\,(P_i(\varphi))^{e_i})$。

定理：设 $V=\oplus_{i=1}^{s}V_i$，$\varphi\in End_F(V)$，V_i 是φ-不变子空间，$\varphi_i=\varphi|V$，则：

1° $f_\varphi(\lambda)=\prod_{i=1}^{s}f_{\varphi_i}(\lambda)$；$2^\circ$ $d_\varphi(\lambda)=[d_{\varphi_1}(\lambda),\cdots,d_{\varphi_s}(\lambda)]$。

定义：称 V 是φ-不可分解，如果不存在φ-不变子空间 V_1,V_2 使得 $V=V_1\oplus V_2$。

定理：设$\varphi\in End_F(V)$，$f_\varphi(\lambda)=d_\varphi(\lambda)=(\lambda-\lambda_0)^n$，则存在 V 的一组基$(\varphi-\lambda_0I)^{n-1}\alpha,(\varphi-\lambda_0I)^{n-2}\alpha,\cdots,(\varphi-\lambda_0I)\alpha$，$\alpha$使得$\varphi$在这组基下的矩阵是 $J_n(\lambda_0)$。

推论：设 $A\in M_n(F)$，若 $f_A(\lambda)=d_A(\lambda)=(\lambda-\lambda_0)^n$，则 A 相似于 $J_n(\lambda_0)$。

9.8 幂零变换的结构

定义：设 V 是 n 为 F-线性空间，$\varphi\in End_F(V)$，称φ是幂零线性变换，存在正整数 n_0 使得$\varphi^{n_0}=0$。

命题：φ是幂零线性变换，则φ的特征值为 0。

定义：幂零线性变换φ的最小多项式的次数称为φ的幂零指数。

定义：设$\varphi\in End_F(V)$是幂零线性变换，对向量$\alpha\in V$，若$\alpha,\varphi(\alpha),\cdots,\varphi^{l-1}(\alpha)$线性无关，且$\varphi^l(\alpha)=0$，记为 $Z(\alpha,\varphi)=\langle\alpha,\varphi(\alpha),\cdots,\varphi^{l-1}(\alpha)\rangle$是$\varphi$-不变子空间，称为$\varphi$-强循环子空间。

定理：令$\varphi|Z(\alpha,\varphi)=\varphi_0$，则 $Z(\alpha,\varphi)$不能写成两个φ-不变子空间的直和。

定理：设$\varphi\in End_F(V)$，e 是φ的幂零指数，那么存在$\alpha_1,\alpha_2,\cdots,\alpha_s\in V$ 使得 $V=\oplus_{i=1}^{s}Z(\alpha_i,\varphi)$。更确切地，存在 V 的一组基$\alpha_1,\varphi(\alpha_1),\cdots,\varphi^{l_1-1}(\alpha_1);\cdots;\alpha_s,\varphi(\alpha_s),\cdots,\varphi^{l_s-1}(\alpha_s)$使$\varphi$在这组基下的矩阵为 Jordan 形矩阵。

定理：设$\varphi\in End_F(V)$，$\varphi^n=0$，则存在$\alpha_i\in V$，使得 $V=\oplus_{i=1}^{s}Z(\alpha_i,\varphi)$。记 $dimZ(\alpha_i,\varphi)=t_i$，则$(t_1,t_2,\cdots,t_s)$是由$\varphi$唯一决定的（不考虑顺序）。

定理：$A\in M_n(F)$，$A^l=0$，那么 A 相似于 Jordan 形矩阵，在不考虑 Jordan 小块的顺序下唯一。

定理：记 N_i 是 i 阶 Jordan 小块的个数，则 $rank(A^k)=N_{k+1}+2N_{k+2}+\cdots+(n-k)N_n$；$N_k=rank(A^{k-1})+rank(A^{k+1})-2rank(A^k)$。

9.9 线性变换的 Jordan 标准形

定理：设 $A\in M_n(F)$，$f_A(\lambda)=\prod_{i=1}^{s}(\lambda-\lambda_i)^{m_i}$，那么 A 相似于一个分块 Jordan 矩阵。

更确切地，存在 Jordan 矩阵 $J_{n_{11}}(\lambda_1),\cdots,J_{n_{1t_1}}(\lambda_1),\cdots,J_{n_{s1}}(\lambda_s),\cdots,J_{n_{st_s}}(\lambda_s)$ 使得 A 相似

于 diag($J_{n_{11}}(\lambda_1),\cdots,J_{n_{1t_1}}(\lambda_1),\cdots,J_{n_{s1}}(\lambda_s),\cdots,J_{n_{st_s}}(\lambda_s)$)，其中$\sum_{j=1}^{t_i}J_{n_{ij}}=m_i$。

主对角元为λ_j 的 Jordan 块总数 $N_j=dimV-rank(A-\lambda_jI)$，

t 级 Jordan 块 $J_t(\lambda_j)$的个数 $N_j(t)=\mathrm{rank}(A-\lambda_j I)^{t+1}+\mathrm{rank}(A-\lambda_j I)^{t-1}-2\mathrm{rank}(A-\lambda_j I)^t$。
在不考虑 Jordan 块的顺序下 Jordan 标准型唯一。
在复数域上，任何一个矩阵都相似于它的 Jordan 标准型。
补：多项式环上的矩阵
$M_n(F[\lambda])=M_n(F)[\lambda]$
用 $A(\lambda)$表示 $M_n(F[\lambda])$中的元素。
称 $A(\lambda)$是可逆矩阵，如果存在 $B(\lambda)$使得 $A(\lambda)B(\lambda)=B(\lambda)A(\lambda)=I_n$。
若 $A(\lambda)$是可逆矩阵，则$|A(\lambda)|\in F^{\times}=F\backslash\{0\}$。
初等行列变换：交换行/列，把某一行/列乘上 F，把某一行/列的 F[λ]倍加到另一行/列。
初等矩阵：1°交换单位矩阵的行列；2°单位矩阵某一行/列数乘 F；3°单位矩阵某一行/列的 F[λ]倍加到另一行/列。
整数环类似：1°同理；2°数乘±1；3°整数倍。
定理：对 $A\in M_n(F[\lambda])$，存在首一多项式 $d_1(\lambda),\cdots,d_r(\lambda)$使得 A 经过若干次行初等变换和列初等变换化为 $\mathrm{diag}\{d_1(\lambda),\cdots,d_r(\lambda),0,\cdots,0\}$，且 $d_1(\lambda)|d_2(\lambda)|\cdots|d_r(\lambda)$。
定义 rank(A)=max{i|A 有 i 阶非零子式}。初等行列变换不改变矩阵的秩。
注：满秩矩阵不一定可逆。$\mathrm{rank}(\lambda I-A)=n$，但$\lambda I-A$ 不可逆；$\mathrm{rank}(\mathrm{diag}\{1,2\})=2$，但 $\mathrm{diag}\{1,2\}$不可逆。
推论：$A(\lambda)$是可逆矩阵，则 $A(\lambda)$经行列初等变换后化为单位矩阵，从而有：
$A(\lambda)\in M_n(F[\lambda])$可逆$\Leftrightarrow |A(\lambda)|\in F^{\times}=F\backslash\{0\}$。
定义：称 $A(\lambda),B(\lambda)$相抵，如果存在可逆矩阵 $P(\lambda),Q(\lambda)$使得 $P(\lambda)A(\lambda)Q(\lambda)=B(\lambda)$。
任何可逆矩阵都是初等矩阵的乘积。
定义：多项式矩阵的行列式因子：设 $A(\lambda)\in M_n(F[\lambda])$，若 $\mathrm{rank}(A(\lambda))=r$，对任意非负整数 $i\in\{1,2,\cdots,r\}$，定义 $D_i(\lambda)$是 $A(\lambda)$的所有 i 次子式的首一最大公因式。
$D_1(\lambda),\cdots,D_r(\lambda)\in F[\lambda]$称为 $A(\lambda)$的行列式因子组，由 $A(\lambda)$唯一确定；$D_i(\lambda)$称为 $A(\lambda)$的 i 阶行列式因子。
命题：设 $A(\lambda),B(\lambda)\in M_n(F[\lambda])$，假定 $B(\lambda)$是由 $A(\lambda)$经过一次初等行变换后得到的矩阵，则 $D_i(A(\lambda))=D_i(B(\lambda))$。
推论：若 $A(\lambda)$与 $B(\lambda)$相抵，则 $D(A(\lambda))=D(B(\lambda))$。
进而有 $D_i(\lambda)=\prod_{k=1}^{i}d_k(\lambda),d_i(\lambda)={D_i(\lambda)}\big/{D_{i-1}(\lambda)}$ 由 $A(\lambda)$唯一决定，称 $d_1(\lambda),\cdots,d_r(\lambda)$是 $A(\lambda)$的不变因子组，称 $\mathrm{diag}\{d_1(\lambda),\cdots,d_r(\lambda),0,\cdots,0\}$是 $A(\lambda)$的相抵标准型(Smith 标准型)。
定义：若 $A\in M_n(F)$，$\lambda I-A$ 的 Smith 标准型为 $\mathrm{diag}\{1,1,\cdots,1,d_1(\lambda),\cdots,d_s(\lambda)\}$。它的不变因子组为 $1,1,\cdots,1,d_1(\lambda),\cdots,d_s(\lambda)$，行列式因子组为 $1,1,\cdots,1,d_1(\lambda),\cdots,d_1(\lambda)\cdots d_s(\lambda)$，行列式等于不变因子的乘积。且$\Sigma(\deg d_i -1)=n-s$ 是 1 的个数，通常简称 $d_1(\lambda),\cdots,d_s(\lambda)$是 A 的不变因子组。
定理：设 $A\in M_n(F)$，$d_1(\lambda),\cdots,d_s(\lambda)$是 $A(\lambda)$的不变因子组，则$\lambda I-A$ 与矩阵 $\mathrm{diag}\{1,1,\cdots,d_1(\lambda),1,1,\cdots,d_2(\lambda),\cdots,1,1,\cdots,d_s(\lambda)\}$相抵。
定理：设 F 是域，$A,B\in M_n(F)$，那么 A 与 B 相似的充要条件是$\lambda I-A$ 与$\lambda I-B$ 相抵。
命题：矩阵 $J_n(a)$的不变因子组为 $1,1,\cdots,1,(\lambda-a)^n$。
定理：若 A 的不变因子组为 $d_1(\lambda),\cdots,d_s(\lambda)$，则 $d_s(\lambda)$是 A 的最小多项式。
定义：对 $f(\lambda)=\lambda^n+a_1\lambda^{n-1}+\cdots+a_{n-1}\lambda+a_n$，定义矩阵 $A_{f(\lambda)}$称为 $f(\lambda)$的相伴矩阵。

其中 $A_{f(\lambda)}=\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_n \\ 1 & 0 & 0 & \cdots & 0 & -a_{n-1} \\ 0 & 1 & 0 & \cdots & 0 & -a_{n-2} \\ & & \cdots & & \cdots & \\ 0 & 0 & 0 & \cdots & 0 & -a_2 \\ 0 & 0 & 0 & \cdots & 1 & -a_1 \end{pmatrix}$。

定义：设 A∈$M_n(F)$，不变因子组为 $d_1(\lambda),\cdots,d_s(\lambda)$，设 $d_j(\lambda)=\prod_{i=1}^{k}(\lambda-\lambda_i)^{n_{ij}}$,j=1,2,⋯,s，

则称$\{(\lambda-\lambda_i)^{n_{ij}}$ |i=1,2,⋯,k,j=1,2,⋯,s}构成的有重类称为 A 的初等因子组。

定理：设 A∈$M_n(F)$，若 $f_A(\lambda)=d_A(\lambda)=\prod_{i=1}^{k}(\lambda-\lambda_i)^{m_i}$ ，则 A 的 Jordan 标准型为

diag{$J_{m1}(\lambda_1),J_{m2}(\lambda_2)\cdots,J_{mk}(\lambda_k)$}。
即：如果特征多项式是最小多项式，Jordan 各块只有一块。
推论：A,B∈$M_n(F)$，则下列条件等价：1°A,B 相似；2°A 与 B 有相同的不变因子组；3°A 与 B 有相同的行列式因子组；4°A 与 B 有相同的初等因子组。

定理：设 A∈$M_n(F)$，$f_A(\lambda)=\prod_{i=1}^{k}(\lambda-\lambda_i)^{m_i}$ ，若 $d_j(\lambda)=\prod_{i=1}^{k}(\lambda-\lambda_i)^{n_{ij}}$,j=1,2,⋯,s，则 A

相似于 diag{$J_{m_{11}}(\lambda_1),\cdots,J_{m_{1k}}(\lambda_k),\cdots,J_{m_{s1}}(\lambda_1),\cdots,J_{m_{sk}}(\lambda_k)$}
计算：(1)λI-A 的 Smith 标准型；(2)把不变因子组分解一次因式的乘积，写出相应的 Jordan 块，把它们对角地拼在一起，就构成 A 的 Smith 标准型。
这个算法给出了：(1)相似的判别法；(2)Jordan 标准型的算法；(3)最小多项式不随数域扩大而改变。

9.10 线性函数与对偶空间

一般地，R^n 上的线性函数空间是 $Hom_R(R^n,R)$，这是线性空间 R^n 到 R^1 的线性映射构成的向量空间。
定义：设 F 是一个域，V 是 F-线性空间，V 的对偶空间定义为 V*=Hom_F(V,F)，元素称为 V 上的 F-线性函数。V 和 V*都是 F-线性空间，若 dim_FV=n，则 dim_FV*=n。
定义：设 V 的一组基为$\alpha_1,\alpha_2,\cdots,\alpha_n$，设$\alpha_i^*(\alpha_j)=\delta_{ij}$，则称$\alpha_1^*,\alpha_2^*,\cdots,\alpha_n^*$是$\alpha_1,\alpha_2,\cdots,\alpha_n$的对偶基。则 1° ∀α∈V，$\alpha=\Sigma\alpha_i^*(\alpha)\alpha_i$；2° ∀f∈V*，则 $f=\Sigma f(\alpha_i)\alpha_i^*$。
命题：设 V 是 F-线性空间，$\alpha_1,\cdots,\alpha_n$，$\beta_1,\cdots,\beta_n$ 是 V 的两组基，设$(\beta_1,\cdots,\beta_n)=(\alpha_1,\cdots,\alpha_n)T$，那么$(\beta_1^*,\cdots,\beta_n^*)=(\alpha_1^*,\cdots,\alpha_n^*)(T^t)^{-1}$。
定理：设 V_1,V_2 是 F-线性空间，则存在映射$\varphi\in Hom_F(V_1,V_2)\to\varphi^*\in Hom_F(V_2^*,V_1^*)$是 F-线性空间同构，其中对 $f\in V_2^*$，$\varphi^*(f)=f\circ\varphi$。
定理：若 $V_1=V_2=V$，则$\varphi,\psi\in End_F(V)$，则$(\varphi\circ\psi)^*=\psi^*\circ\varphi^*$。
定理：给定 V 的一组基$\alpha_1,\cdots,\alpha_n$，$\varphi(\alpha_1,\alpha_2,\cdots,\alpha_n)=(\alpha_1,\alpha_2,\cdots,\alpha_n)A$，则 $\varphi^*(\alpha_1^*,\alpha_2^*,\cdots,\alpha_n^*)=(\alpha_1^*,\alpha_2^*,\cdots,\alpha_n^*)A^t$。
定理：设 V 是 F-线性空间，存在 F-线性单射 l:V→V**,v→l(v)，l(v)∈Hom_F(V*,F)定义为 f∈V*，l(v)(f)=f(v)。

第 10 章 具有度量的线性空间

10.1 双线性函数

定义：对一般的域 F，一般 F-线性空间 V，V 上的双线性函数是一个映射，$f:V\times V\to F$，满足：$\forall \alpha_1,\alpha_2,\beta_1,\beta_2,\alpha,\beta\in V$，$k_1,k_2\in F$，

1° $f(k_1\alpha_1+k_2\alpha_2,\beta)=k_1f(\alpha_1,\beta)+k_2f(\alpha_2,\beta)$；2° $f(\alpha,k_1\beta_1+k_2\beta_2)=k_1f(\alpha,\beta_1)+k_2f(\alpha,\beta_2)$。

一般地，对 F-线性空间 V，记 BL(V)表示 V 上的 F-双线性函数的集合。

$0\in BL(V)$，$\forall f_1,f_2\in V$，定义 f_1+f_2 为$(f_1+f_2)(\alpha,\beta)=f_1(\alpha,\beta)+f_2(\alpha,\beta)$，从而 $f_1+f_2\in BL(V)$。

$\forall f\in V$，$a\in F$，定义 af 为$(af)(\alpha,\beta)=af(\alpha,\beta)$，从而 $af\in BL(V)$。

在上面的定义下，BL(V)是一个 F-线性空间。

定理：设$\alpha_1,\alpha_2,\cdots,\alpha_n$ 是 V 的一组基，那么映射 $A:BL(V)\to M_n(F)$，$f\to(f(\alpha_i,\alpha_j))_{n\times n}$ 是 F-线性空间同构，且 $f(\alpha,\beta)=X^TA(f)Y$，这里 X,Y 表示α,β在基$\alpha_1,\alpha_2,\cdots,\alpha_n$ 下的坐标。

定理：设$\alpha_1,\alpha_2,\cdots,\alpha_n$ 是 V 的一组基，则对$\forall f\in BL(V)$，都有 $f(\alpha,\beta)=X^T(f(\alpha_i,\alpha_j))Y$，其中 X,Y 是$\alpha,\beta$在基$\alpha_1,\alpha_2,\cdots,\alpha_n$ 下的坐标。

定义：设 $f\in BL(V)$，$\alpha_1,\alpha_2,\cdots,\alpha_n$ 是 V 的一组基，称矩阵 $A(f)=(f(\alpha_i,\alpha_j))$关于基$\alpha_1,\alpha_2,\cdots,\alpha_n$ 的度量矩阵。

定理：设 $f\in BL(V)$，$\alpha_1,\alpha_2,\cdots,\alpha_n,\beta_1,\beta_2,\cdots,\beta_n$ 是 V 的两组基，A(f),B(f)分别是 f 关于基$\alpha_1,\alpha_2,\cdots,\alpha_n,\beta_1,\beta_2,\cdots,\beta_n$ 的度量矩阵，$P\in GL_n(F)$是从基$\alpha_1,\alpha_2,\cdots,\alpha_n$ 到$\beta_1,\beta_2,\cdots,\beta_n$ 的过度矩阵，则 $B(f)=P^TA(f)P$。

定理：双线性函数在不同基的度量矩阵合同。

定义：设 BL(V)，f 的秩是它的度量矩阵的秩，记为 r(f)。

在合同关系下，矩阵有标准型。对给定的双线性函数，合同标准型对应的基是值得研究的。

定义：$L_f:V\to V^*,\alpha\to f(\alpha,\cdot)$，$R_f:V\to V^*,\alpha\to f(\cdot,\alpha)$。这两个映射是线性的。

定理：设 $f\in BL(V)$，则 $r(f)=r(L_f)=r(R_f)$。

推论：若 $f\in BL(V)$，$r(f)=n$，则 $L_f,R_f:V\to V^*$都是同构。

反对称矩阵的秩是偶数，反对称矩阵合同于 $\mathrm{diag}\{\begin{pmatrix}0&1\\-1&0\end{pmatrix},\cdots,\begin{pmatrix}0&1\\-1&0\end{pmatrix},0,\cdots,0\}$。

定义：称双线性函数 f 是对称的，如果 $f(\alpha,\beta)=f(\beta,\alpha)$；称双线性函数 f 是反对称的，如果 $f(\alpha,\beta)=-f(\beta,\alpha)$。

定理：双线性函数 f 的对称性与度量矩阵对称性相同。

定理：设 $f\in BL(V)$，f 是对称的双线性函数，则存在 V 的一组基$\alpha_1,\alpha_2,\cdots,\alpha_n$ 使得$(f(\alpha_i,\alpha_j))=\mathrm{diag}\{c_1,c_2,\cdots,c_f,0,0\}$，其中 $c_i\neq0$，$r=r(f)$。

10.2 欧几里得空间

定义：设 V 是 R-线性空间，$f:V\times V\to R$ 是对称双线性函数，且 $f(\alpha,\alpha)\geqslant0$，取等号$\Leftrightarrow\alpha=0$。

定理：任何有限 n 维欧式空间都同构于 $R^n\Leftrightarrow$ n 维欧式空间一定存在一组基$\varepsilon_1,\cdots,\varepsilon_n$ 使得它的度量矩阵是单位矩阵。

定义：设 V 是 n 维欧式空间，$\varepsilon_1,\cdots,\varepsilon_n$ 称为 V 的标准正交基，如果$(\varepsilon_i,\varepsilon_j)=\delta_{ij}$。

定理：对任意$\alpha,\beta\in V$，V 是欧式空间，则$(\alpha,\beta)^2\leq(\alpha,\alpha)(\beta,\beta)$。

定理：正交的向量组线性无关。

定义：$\varepsilon_1,\cdots,\varepsilon_n$ 是 V 的标准正交基，则 $\alpha=\sum_{i=1}^{n}(\alpha,\varepsilon_i)\varepsilon_i$ 称为α的傅里叶展开。

10.3 正交补，正交投影

定义：设 V 是欧式空间，W 是 V 的子空间，$\varepsilon_1,\cdots,\varepsilon_r$ 是 W 的标准正交基，称映射 $P_W:V\to W$，$\alpha\to P_W(\alpha)=\sum_{i=1}^{r}(\alpha,\varepsilon_i)\varepsilon_i$ 是 V 到 W 的正交投影。

定理：设 V 是欧式空间，W 是 V 的子空间，对$\forall\alpha\in V$，都有$|\alpha-P_W(\alpha)|\leqslant|\alpha-\beta|$。

定义：考虑方程 $AX=\beta$的解，通常这个方程无解，称 $X=(c_1,c_2,\cdots,c_n)$是方程的最小二乘解，如果$||AX-\beta||$取最小值。

定理：设 A 的列向量为$\alpha_1,\alpha_2,\cdots,\alpha_n$，令 $W=<\alpha_1,\alpha_2,\cdots,\alpha_n>$，则$||AX-\beta||$取最小值当且仅当 $AX=P_W(\beta)\Leftrightarrow\beta-AX\perp W\Leftrightarrow X$ 是方程组 $A^TAX=A^T\beta$的解。

10.4 正交变换与对称变换

定义：设 V 是欧式空间，设$\varphi:V\to V$ 是线性变换，称φ是正交变换，如果$(\varphi(\alpha),\varphi(\beta))=(\alpha,\beta)$。它是欧式空间的等距变换。

命题：设$\varphi\in O(V)$，其中 V 是 n 维欧式空间，$\varepsilon_1,\cdots,\varepsilon_n$ 是 V 的标准正交基。设 A_φ 是φ在基$\varepsilon_1,\cdots,\varepsilon_n$ 下的矩阵，即是$\varphi(\varepsilon_1,\cdots,\varepsilon_n)=(\varepsilon_1,\cdots,\varepsilon_n)A_\varphi$，则 A_φ是正交矩阵。

定理：$\varphi\in O(V)\Leftrightarrow A_\varphi$是正交矩阵。

命题：正交矩阵的实特征值只能是±1。

定理：设 A 是 n 阶正交矩阵，则 A 的特征多项式 $f_A(\lambda)=(\lambda-1)^s(\lambda+1)^t\prod_{i=1}^{v}(\lambda^2-2\cos\theta_i\lambda+1)^{P_i}$，且 A 相似于 $\mathrm{diag}\{I_s,-I_t,\begin{pmatrix}\cos\theta_i & \sin\theta_i\\ -\sin\theta_i & \cos\theta_i\end{pmatrix}\}$。

命题：设 V 是欧式空间，$\varphi\in O(V)$，W 是φ-不变子空间，则 $W^\perp$也是φ-不变子空间。

命题：设 V 是实线性空间，$\varphi:V\to V$ 是 R-线性变换，如果φ没有实特征值，则存在 2 维φ-不变子空间。

Riesz 表示定理：设 V 是数域 F 上的有限维非退化的正交空间，那么对$\forall f\in V^*$，存在$\alpha\in V$，使得 $f(\beta)=L(\alpha)(\beta)=(\beta,\alpha)$。称线性函数 f 可由$\alpha$表示。

定理：设 V 是有限维欧式空间，$\varphi\in End_R(V)$，那么存在唯一的$\varphi^*\in End_R(V)$，使得对任意$\alpha,\beta\in V$，都有$(\varphi(\alpha),\beta)=(\alpha,\varphi^*(\beta))$，这里的$\varphi^*$称为$\varphi$的伴随。

定义：设 V 是有限维欧式空间，$\varphi\in End_R(V)$，称φ是对称变换，如果$\varphi^*=\varphi$。即对任意$\alpha,\beta\in V$，都有$(\varphi(\alpha),\beta)=(\alpha,\varphi(\beta))$。

定理：φ是对称变换的充要条件是它的变换矩阵 A_φ是对称矩阵。

定理：对称线性变换可正交对角化。

命题：设 V 是欧式空间，φ是对称线性变换，V_1 是φ-不变子空间，则 $V_1^\perp$也是φ-不变的。

10.6 正交空间与辛空间

定义：设 V 是 F-线性空间，$f\in BL(V)$，称(V,f)是度量空间。当 f 是对称时，称(V,f)是正交空间；当 f 是反对称时，称(V,f)是辛空间；对一般的 f，称(V,f)是度量空间。记 V 上的对称双线性函数空间为 SBL(V)，反对称双线性函数空间为 ASBL(V)。

命题：设 F 是域，$\mathrm{char}F\neq2$，则 $BL(V)=SBL(V)\oplus ASBL(V)$。

定理：设(V,f)是正交空间，$r(f)=r$，那么存在 V 的一组基$\alpha_1,\alpha_2,\cdots,\alpha_n$ 使得 f 在这组基下的度量矩阵为 $\mathrm{diag}\{c_1,\cdots,c_r,0,\cdots,0\}$，$c_i\neq0\in F$。

定义：设(V,f)是正交空间，$\alpha,\beta\neq0\in V$，称α与β正交，如果 $f(\alpha,\beta)=0$。

推广：设$\alpha_1,\cdots,\alpha_s$ 是(V,f)中的非零向量组，若 $f(\alpha_i,\alpha_j)=0$，$i\neq j$，称$\alpha_1,\cdots,\alpha_s$ 是 V 中的正交向量组。

定义：设(V,f)是正交空间，$\alpha_1,\cdots,\alpha_n$ 是 V 的一组基，且$\alpha_1,\cdots,\alpha_n$ 是正交的，那么称$\alpha_1,\cdots,\alpha_n$ 是(V,f)的正交基。
定理：正交空间(V,f)有一组正交基。
定理：设(V,f)是正交空间，$\alpha_1,\cdots,\alpha_n$ 是 V 的正交基，它的度量矩阵为 $\mathrm{diag}\{c_1,\cdots,c_r,0,\cdots,0\}$，那么 $V=\langle\alpha_1,\cdots,\alpha_r\rangle\oplus\langle\alpha_{r+1},\cdots,\alpha_n\rangle$。
定义：设(V,f)是正交空间，W 是 V 的子空间，令 $f|W:W\times W\to F$，$(\alpha,\beta)\to f(\alpha,\beta)$是 $W\times W$ 上的双线性函数，且是对称的。
命题：设(V,f)是正交空间，W 是 V 的子空间，那么(W,f|W)也是正交空间。
定理：设(V,f)是正交空间，$\alpha_1,\cdots,\alpha_n$ 是 V 的正交基，且 f 关于$\alpha_1,\cdots,\alpha_n$ 的度量矩阵为 $\mathrm{diag}\{c_1,\cdots,c_r,0,\cdots,0\}$，那么 $\mathrm{Ker}\ L_f = \mathrm{Ker}\ R_f = \langle\alpha_{r+1},\cdots,\alpha_n\rangle = \mathrm{Rad}_f(V)$。
定理：设(V,f)是正交空间，存在 V 的子空间 V_1，使得 $V=V_1\oplus\mathrm{Rad}_f(V)$，且 $f|V_1$ 是非退化的，$f|\mathrm{Rad}_f(V)=0$。
定义：设(V,f)是正交空间，V_1,V_2 是 V 的子空间，称 V 是 V_1 与 V_2 的正交直和，如果 $V=V_1\oplus V_2$，且任意$\alpha\in V_1,\beta\in V_2$ 都有 $f(\alpha,\beta)=0$，记为 $V=V_1\perp V_2$。
定义：设(V,f)是正交空间，V_1 是 V 的子空间，令 $V_1^{\perp}=\{\alpha\in V|f(\alpha,\beta)=0,\ \forall\beta\in V_1\}$是 V 的子空间，称为 V_1 在 V 中的正交补。
命题：设(V,f)是正交空间，那么 $V^{\perp}=\mathrm{Rad}_f(V)$。
定理：设(V,f)是正交空间，r(f)=r，则存在 V 的子空间 V_1 使得 $V_1\perp V^{\perp}$，且 $f|V_1$ 是非退化的，$r(f|V_1)=r$。
命题：设(V,f)是正交空间，V_1,V_2 是 V 的子空间，$V_1\subseteq V_2$，则 $V_2^{\perp}\subseteq V_1^{\perp}$。
引理：设(V,f)是正交空间，V_1 是 V 的非退化子空间，则 $V=V_1\perp V_1^{\perp}$。（对偶空间+维数证明）
定理：设(V,f)是正交空间，r(f)=r，则存在 V 的一组正交基$\alpha_1,\cdots,\alpha_n$ 使得 f 在$\alpha_1,\cdots,\alpha_n$ 下的度量矩阵为 $\mathrm{diag}\{c_1,\cdots,c_r,0,\cdots,0\}$。
当 F=R 时，设(V,f)是实数域 R 上的非退化正交空间，那么存在正交基使得 f 的度量矩阵为 $\mathrm{diag}\{I_p,-I_q\}$。

补：双曲空间与 Witt 定理

定义：设(V,f)是正交空间，$\alpha\neq0\in V$，若 $f(\alpha,\alpha)=0$，则称α是迷向向量。
V 中的迷向向量构成的集合 m(V)不是 V 的子空间，但若$\alpha\in m(V)$，$k\alpha\in V$，从而迷向向量是 V 的锥。
定义：称(V,f)是非退化的双曲空间，存在 V 的一组基$\alpha_1,\alpha_2,\cdots,\alpha_p,\alpha_{-1},\alpha_{-2},\cdots,\alpha_{-p}$ 使得 f 在这组基下的度量矩阵为$\begin{pmatrix}0 & I_p\\ I_p & 0\end{pmatrix}$。当 p=1 时称为双曲平面。
定义：设(V,f)是正交空间，称(V,f)是反迷向(定性)的，如果对$\forall\alpha\in V$，$f(\alpha,\alpha)=0\Rightarrow\alpha=0$。
容易知道，任意的非退化双曲空间都是偶数维的。
命题：任意双曲空间都有双曲平面的正交直和。
命题 1：1 维非退化正交空间一定是反迷向的。
命题 2：2 维非退化正交空间要么是反迷向的，要么是双曲平面。即是：非退化二维正交空间有迷向向量一定是双曲平面。
设(V,f)是非退化正交空间，$\dim V\geqslant2$，若$\alpha,\beta\in V$，满足 $f(\alpha,\alpha)f(\beta,\beta)=0$，但 $f(\alpha,\beta)\neq0$，那么$\langle\alpha,\beta\rangle$是 V 的双曲平面。
Witt 分解定理：设(V,f)是非退化正交空间，则存在 V 的双曲子空间 H_s 与反迷向子空间 D，使得 $V=H_s\perp D$，且 S 是由 f 唯一决定的。

此即：A=diag$\{\begin{pmatrix} 0 & I_s \\ I_s & 0 \end{pmatrix}, c_1, c_2, \cdots, c_{n-2s}\}$

定义：是个(V_1,f_1),(V_2,f_2)是域 F 上的正交空间，一个映射$\varphi:(V_1,f_1)\to(V_2,f_2)$称为等距/保距同构，如果 1° φ是线性同构；2° 对$\forall\alpha,\beta\in V_1$，$f_1(\alpha,\beta)=f_2(\varphi(\alpha),\varphi(\beta))$。
当 $V_1=V_2$，$f_1=f_2$ 时，等距同构也称为等距变换。
1° 等距变换的复合是等距变换；2° 单位映射是等距变换；3° 等距变换的逆也是等距变换。
从而(V,f)的等距变换在映射的复合下构成一个群，记为 $O(V,f)\subseteq GL(V)$。
定理：维数相同的非退化双曲空间等距同构。
唯一性定理叙述为：设(V_1,f_1),(V_2,f_2)是两个非退化的正交空间，如果$\varphi:(V_1,f_1)\to(V_2,f_2)$是等距同构，$V_1=H_{s1}\perp D_1$，$V_2=H_{s2}\perp D_2$，那么 $S_1=S_2$。
特殊情形：设(V,f)是非退化的正交空间，若 $V=H_{s1}\perp D_1=H_{s2}\perp D_2$，则 $S_1=S_2$。
Witt 消去定理：设(V_1,f_1),(V_2,f_2)是两个非退化正交空间，$\varphi:(V_1,f_1)\to(V_2,f_2)$是等距同构，且 $V_1=U_1\perp W_1$，$V_2=U_2\perp W_2$，$f|V_i,f|W_i$ 是非退化的，若$\varphi_1:(U_1,f|U_1)\to(U_2,f|U_2)$是等距同构，则存在$\varphi_2:(W_1,f|W_1)\to(W_2,f|W_2)$是等距同构。
设 charF$\neq$2，假定(V,f)是非退化的正交空间镜面对称映射，设η是(V,f)的非迷向向量，则 $V=\langle\eta\rangle\perp\langle\eta\rangle^{\perp}$。考虑映射：$M_\eta:V\to V$，$\alpha\to M_\eta(\alpha)=\alpha-2\dfrac{f(\alpha,\eta)}{f(\eta,\eta)}\eta$。
命题：映射 $M_\eta\in O(V,f)$。
Witt 扩充定理：设(V,f)是有限维非退化正交空间，W 是 V 的子空间，$\varphi_1:W\to V$ 是等距单射，则存在$\varphi\in O(V,f)$，使得$\varphi|W=\varphi_1$。
双曲扩张定理：n 维双曲空间的任意 r 维全迷向子空间都可以扩充成为 2r 维双曲空间。