抽象代数

主讲人：北京大学　徐茂智
打字人：北京大学　龚诚欣

第 1 章　群、环、体、域的基本概念

1.0 预备知识

定义：集合到自身的映射称为变换。
集合 A,B 的笛卡儿积：a∈A，b∈B，构成集合(a,b)，记为 A×B。
集合 A 上的一个二元运算是 A×A→A 的一个映射。
A 上的一个二元关系定义为 A×A 的子集。（注意：不需要映射到 A 本身！）
二元关系 R 如果满足：1° 反身性，即 aRa；2° 对称性，即 aRb⇔bRa；3° 传递性，即 aRb，bRc⇒aRc，则称 R 为 A 上的一个等价关系，互相等价的元素组成的 A 的子集构成一个等价类。任意两个不同等价类的交为空集，从而 A 等于所有等价类的无交并。等价关系用"~"表示，A 中等价类组成的集合记为 A/~。

1.1 群的基本概念

定义：非空集合 G 上定义了一个二元关系 $\cdot$，满足：1° 结合律，即$(a\cdot b)\cdot c=a\cdot(b\cdot c)$；2° 幺元存在，即存在 e∈G 使得 $e\cdot a=a\cdot e=a$；3° 逆元存在，$\forall a,\exists b$ 使 $a\cdot b=b\cdot a$；则称 G 关于运算 $\cdot$ 构成一个群，记为$(G,\cdot)$。
交换群：满足 $a\cdot b=b\cdot a$，又称 Abel 群。
群的幺元唯一，逆元唯一，且满足消去率（由逆元存在保证）。
阶：群所含元素的个数，记为|G|。|G|有限称为有限群，否则称为无限群。
群的示例：n 次单位根群；剩余类群；一般线性群，$GL_n(K)$，n 阶可逆阵；特殊线性群，$SL_n(K)$，n 阶行列式 1 的矩阵；正交群；酉群；图形 T 的对称群，二面体群；全变换群，S(M)，非空集合 M 到自身的双射。
对称群：M 是有 n 个元素的集合，S(M)称为 n 级对称群，记为 S_n。
n 元置换：$\sigma(j)=\sigma_j$，记为$\begin{pmatrix}1 & 2 & \cdots & n\\ \sigma_1 & \sigma_2 & \cdots & \sigma_n\end{pmatrix}$。

轮换：$\sigma\in S_n, i_1,\cdots,i_t\in\{1,2,\cdots,n\}$，如果$\sigma(i_k)=i_{k+1}$(规定$i_{t+1}=i_1$)，那么称$\sigma$是一个轮换，规定 t 为该轮换的长度。长度为 2 的轮换称为对换。两个轮换$(i_1,\cdots,i_t)$和$(j_1,\cdots,j_s)$称为不相交的，如果 $i_k\neq j_m$，$\forall$ k,m。
不相交的轮换满足交换律。
对称群中任一不等一幺元的元素都可以唯一地分解为不相交的轮换的乘积。又因为轮换可以分解为对换的乘积，从而任意置换都可以分解为对换的乘积。
任一给定的置换分解为对换的乘积时出现的对换的个数的奇偶性不变。（这是因为每出现一次对换，逆序数改变一个奇数）。偶置换关于映射的乘法下也构成群，称为 n 级交错群，记为 A_n。
设 H 为群 G 的非空子集，如果 H 在 G 的运算下构成群，则称 H 为 G 的子群，记作 H≤G。子群的等价命题：1° 任意 a,b∈H，$a\cdot b\in H$ 且 $a^{-1}\in H$；2° 任意 a,b∈H，$ab^{-1}\in H$（或 $a^{-1}b\in H$）。
注意：证明子群时请先验证非空性。

群的乘积：H,K 是 G 的子集，规定 H,K 的积为 HK={hk|h∈H,k∈K}。如果 K={a}，简记为 aH 或 Ha。规定 $H^{-1}=\{h^{-1}|h\in H\}$，$H^n=\{h_1h_2\cdots h_n|h_i\in H\}$。

从而 H 是子群的充要条件是：1° $H^2\subseteq H$ 且 $H^{-1}\subseteq H$；2° $HH^{-1}\subseteq H$（或 $H^{-1}H\subseteq H$）。

设 G 是群，$M\subseteq G$，称 G 的所有包含 M 的子群的交为由 M 生成的子群，记作<M>。

<M>={e,$a_1a_2\cdots a_n$|$a_i\in M\cup M^{-1}$，n=1,2,⋯}。
如果<M>=G，我们称 M 为 G 的一个生成系，或称 G 可由 M 生成。仅由一个元素生成的群叫做循环群，由有限多个元素生成的群叫做有限生成群。
定义<a>的阶为元素 a 的阶，记作 o(a)。o(a)是满足 $a^n=e$ 的最小正整数，$a^{o(a)}=e$。
用子群 H 给出 G 上的一个等价关系~，a~b：存在 h∈H，使得 a=bh。
陪集：H≤G，形如 aH 的子集称为 H 的左陪集，Ha 的子集称为 H 的右陪集，分别记为 G/H 和 H\G。
注意：aH 的陪集代表 a 可以有很多。如果 b∈aH，那么 aH 也可以用 bH 来表示，这是因为 bH=aHH=aH。

显然 $G=\overset{*}{\bigcup_{aH}}aH$。（等价类的无交并）。H 的左陪集的个数称为 H 在 G 中的指数，记为|G:H|。注意到 f:H→aH，h→ah 是双射（定义知满射，$ah_1=ah_2$ 左乘 a^{-1} 知单射）。从而左右陪集个数相等。
Lagrange 定理：设 G 是有限群，H≤G，则|G|=|G:H||H|。特殊地，取 H={a}，由于必有 o(a)||G|，从而必有 $a^{|G|}=e$。

正规子群：H≤G，如果 aH=Ha，∀a∈G，称 H 为 G 的正规子群，记为 $H\trianglelefteq G$。（使得左陪集的乘积仍是左陪集）。显然{e}和 G 都是正规子群。如果没有其他正规子群，则称 G 为单群。
正规子群的等价条件：1° $a^{-1}Ha=H$，∀a∈G；2° $a^{-1}ha\in H$，∀h∈H，a∈G。
商群：设 G 是群，H 是正规子群，则 H 的陪集在乘法下构成群，称为 G 关于 H 的商群，记作 G/H。
例：Z/nZ={0+nZ,1+nZ,⋯,n-1+nZ}相当于：对于任意元素 k∈{0,1,⋯,n-1}，k+nZ 随着 Z 的变化把所有 mod n 余 k 的数都过了一遍，从而商群只有 n 个元素。
群同态：群 G→群 G_1 的映射 f 保持群运算，即 f(ab)=f(a)f(b)。单射称为单同态，满射称为满同态，双射称为同构，记为≅。
以后我们用 End(G)表示 G 的自同态的集合，用 Aut(G)表示自同构的集合。End(G)是一个幺半群，而 Aut(G)是自同构群；若 G 是 Abel 群，则 End(G)构成一个环。
容易验证，群同态 f 把幺元映射成幺元，把 a 的逆元映射成 f(a)的逆元。
我们把 f(G)称为映射 f 的像，记为 Im f；把 e_1 的原像称为 f 的核，记为 Ker f。
G→G_1 的群同态 f 单的充要条件是 Ker f ={e}。
f 是 G→G_1 的群同态，则 Im f 是 G_1 的子群，Ker f 是 G 的正规子群。
同态基本定理：f:G→G_1 是群同态，则 G/Ker f≅Im f。
推论：若 f:G→G_1 是满同态，则 G/Ker f≅G_1。
左平移：任一 a∈G，存在变换 L(a):G→aG，g→ag 称为 a 引起的 G 的左平移。容易看出 $L(a)L(a^{-1})=L(a^{-1})L(a)=id_G$。L(G)≤S(G)。
Cayley 定理：任一群都同构于某一集合上的变换群。（将 a 映射成 L(a)）上述的

L(G)称做群 G 的左正则表示。类似定义右平移与右正则表示。
典范同态：设 G 是群，H 是 G 的正规子群，则 g:G→G/H，a→aH 是群同态，称为 G 到 G/H 的典范同态。
第一同构定理：在典范同态(G→G/H,a→aH)下，1° G 的包含 H 的子群与 G/H 的子群在 g 下一一对应；2° 在此对应下，正规子群对应于正规子群；3° 若有 K 是 G 的正规子群且 $H\subseteq K$，则 $G/K\cong(G/H)/(K/H)$。

第二同构定理：设 G 是群，H 是 G 的正规子群，K 是 G 的子群，则 1° HK 是 G 的子群，$H\cap K$ 是 K 的正规子群；2° $(HK)/H\cong K/(H\cap K)$。
直和：设 G_1,G_2 是群，在笛卡尔积 $G_1\times G_2$ 上定义运算为按分量进行，即对于 $(a_1,b_1),(a_2,b_2)\in G_1\times G_2$，定义 $(a_1,b_1)(a_2,b_2)=(a_1a_2,b_1b_2)$，则 $G_1\times G_2$ 在此运算下构成群，称为 G_1 与 G_2 的直和，记为 $G_1\oplus G_2$，G_1 和 G_2 称为 $G_1\oplus G_2$ 的直和因子。
定理：设 G 是群，H,K 是 G 的正规子群，G=HK，则下述四条等价：1° 映射 $f:H\oplus K\to G$，$(h,k)\to hk$ 是同构；2° G 的任一元素表为 H 与 K 的元素的乘积的表示法唯一；3° G 的幺元表为 H 与 K 的元素的乘积的表示法唯一；4° $H\cap K=\{e\}$。
推广：设 G 是群，$H_1,H_2,\cdots,H_n$ 是 G 的正规子群，$G=H_1H_2\cdots H_n$，则下述四条等价：1° 映射 $f:H_1\oplus H_2\oplus\cdots\oplus H_n\to G$，$(h_1,h_2,\cdots,h_n)\to h_1h_2\cdots h_n$ 是同构；2° G 的任一元素表为 $H_1,H_2,\cdots,H_n$ 的元素的乘积的表示法唯一；3° G 的幺元表为 $H_1,H_2,\cdots,H_n$ 的元素的乘积的表示法唯一；4° $H_i\cap(H_1,H_2,\cdots,H_{i-1},H_{i+1},\cdots,H_n)=\{e\}$。
G_1,G_2 是 $G_1\oplus G_2$ 的正规子群。
一般而言，设 $G_i(i\in I$ 是指标集)是群，令 G 为集合 G_i 的笛卡尔积，在 G 上定义运算为按分量进行，所得到的群称为 G_i 的直积，记为 $\prod_{i\in I}G_i$，G_i 称为 G 的直积因子。
群 G 的子群 $\{(\cdots,a_i,\cdots)\mid a_i\in G_i$,除有限多个 i 之外都有 $a_i=e_i\}$ 构成 $\prod_{i\in I}G_i$ 的子群，此子群称为 G_i 的直和，记为 $\coprod_{i\in I}G_i$。当 I 为有限集时，直积与直和的概念一致。
注意：在群同态 $f_i:G_i\to\prod_{i\in I}G_i$，$a_i\to(\cdots,e,a_i,e,\cdots)$中，直和的任一元素都可以表为 f_i 像的和，但当 I 是无限集时直积却不具有这样的性质。

1.2 环的基本概念

设 R 是一个非空集合，在它上面定义了“+”，“·”两种运算，满足：1° (R,+) 构成 Abel 群；2° 乘法结合律；3° 乘法单位元存在；4° 乘法分配律。则称 R 是一个环，记为(R;+, ·)或 R。如果环 R 还满足乘法交换律，则称该环为交换环。
设 R 是一个环，则 1° 0a=a0=0；2° (-a)b=a(-b)=-(ab)。
设 R 是一个环，如果 ab=1，则称 a 是右可逆的，b 是 a 的一个右逆元；称 b 是左可逆的，a 是 b 的一个左逆元。如果 ab=ba=1，则称 a 是可逆的，b 是 a 的一个逆元。
设 R 是一个环，如果 a 既有左逆元又有右逆元，则 a 左逆元与右逆元相等，并称 a 可逆。
设 R 是一个环，对于 $a\in R$，如果存在一个 $b\neq0\in R$ 使得 ab=0，则称 a 是 R 的一个左零因子；类似定义右零因子。如果 a 是左零因子或右零因子，则称 a 是零因子。
设 R 是一个没有非零零因子的交换环，且 R 中至少包含两个元素 0 和 1，则称 R

是一个整环或整区。

设 R 是一个环，如果子集 $S\subseteq R$ 如果按照 R 的运算构成环，且要么 S 包含 1_R 要么 S={0}，则称 S 为 R 的一个子环。

设 R 是一个环，I 是 R 的加法子群，并且对于任意的 $r\in R$ 都有 $rI\subset I$($Ir\subset I$)，则称 I 是 R 的一个左（右）理想。如果 I 同时是左理想和右理想，则称 I 为 R 的一个（双边）理想。容易看出，子环的交是子环，理想的交、和是理想。

设 R 是一个环，$M\subset R$，则称 R 的所有包含 M 的理想的交为由 M 生成的理想，记为(M)。容易看出，$(M)=\{0, \sum_{finite} r_i m_i + m_j r_j + r_k' m_k r_k''\}$。如果 R 是幺环，则$(M)=\{0, \sum_{finite} r' m r''\}$；如果 R 是交换幺环，则$(M)=\{0, \sum_{finite} rm\}$。规定$(\phi)=\{0\}$。

如果(M)=I，则称 M 是 I 的一个生成系（生成元集）。由有限个元素生成的理想称为有限生成理想，一个元素生成的理想称为主理想。

设 R 是一个环，I 是 R 的一个理想，则陪集集合 $R/I=\{r+I|r\in R\}$在下列运算：1°$(r+I)+(s+I)=(r+s)+I$；2°$(r+I)(s+I)=(rs)+I$；上构成一个环，称为 R 关于 I 的商环。如果 I=R，则 $R/I=\{\overline{0_R}\}$是零环；如果 I＜R，则 $R/I=\{\overline{0_R}, \overline{1_R}, \cdots\}$。

环 R 到环 R_1 的映射 $f:R\to R_1$，如果满足对于任意 $a,b\in R$ 都有 $f(ab)=f(a)f(b)$,$f(a+b)=f(a)+f(b)$且 f(1)=1，则称 f 是环 R 到环 R_1 的一个同态。环同态 f 如果又是单射（满射）则称 f 是单（满）同态，既单又满的同态称为同构。如果存在环 R 到环 R_1 的同构映射，则称 R 和 R_1 是同构的，记为 $R\sim R_1$。

对于一个同态 $f:R\to R_1$，用 im f 或 f(R)表示 f 的像，而称 $Ker(f)=\{a|f(a)=0\}$。则 im f $\leqslant R_1$，ker f 是 R 的理想。

设 $f:R\to R_1$ 是环同态，则 f 是单射当且仅当 ker f={0}，这里 0 是 R 的零元。

同态基本定理：设 $f:R\to R_1$ 是环同态，则 $R/\ker f\sim \text{im } f$。

第一同构定理：设 R 是环，I 是 R 的理想，则在典范同态 $f:R\to R/I, a\to a+I$ 下，1°R 的包含 I 的子环与 R/I 的子环在 f 下一一对应，这种对应保持包含关系（称为是格对应）；2°R 的包含 I 的理想与 R/I 的理想在 f 下一一对应；3°若 J 是 R 的理想，且 $I\subset J$，则 $R/J\sim(R/I)/(J/I)$。

第二同构定理：设 R 是环，I 是 R 的理想，$S\leqslant R$ 是 R 的非零子环，则：1°$S+I\leqslant R$，$S\cap I$ 是 S 的理想，I 是 S+I 的理想；2°$(S+I)/I\sim S/S\cap I$。

设 R_1,R_2 是环，在它们的笛卡尔积上定义运算如下：对于$(a_1,b_1),(a_2,b_2)\in R_1\times R_2$，定义$(a_1,b_1)(a_2,b_2)=(a_1a_2,b_1b_2)$，$(a_1,a_2)+(b_1,b_2)=(a_1+a_2,b_1+b_2)$，则 $R_1\times R_2$ 在此运算下构成一个环，称为 R_1 与 R_2 的（外）直和，记为 $R_1\oplus R_2$。R_1 和 R_2 称为 $R_1\oplus R_2$ 的直和因子。(e_1,e_2)是 $R_1\oplus R_2$ 中的单位元，$(a,b)\in R_1\oplus R_2$ 可逆当且仅当 $a\in R_1, b\in R_2$ 均可逆。

设 R 是环，I_1,I_2 是 R 的理想，$R=I_1+I_2$。则下述四条等价：1°$f:I_1+I_2\to R,(a,b)\to a+b$ 是同构；2°R 的任一元素表示为 I_1 与 I_2 的元素的和表示法唯一；3°R 的 0 元表示为 I_1 与 I_2 的元素的和表示法唯一；4°$I_1\cap I_2=\{0\}$。R 称为理想 I_1,I_2 的（内）直和，也记为 $R=I_1\oplus I_2$，I_1 和 I_2 称为 R 的直和因子。

1.3 体、域的基本概念

设 D 是一个非零环，如果 D 中每个非零元素可逆，则称 D 是一个体（可除环）。交换的体称为域。一个域（或体）的子环是域则称之为子域（子体）。

对于环 R，我们通常用 R*表示 R 中的非零元组成的集合，而用 R^X 表示 R 中可逆元组成的子集合。若环 D 是体，等价于 $D^*=D^X$。
交换环 D 是域的充分必要条件是 D 只有{0}、D 两个理想。（利用逆的性质）
例：代数数域 Q[α]，α是不可约 n 次有理系数多项式的根，Q[α]≌Q[x]/(f(x))。

p-进数域：考虑 $a=\frac{z_1}{z_2}\in Q$，我们有 $a=p^e\frac{z_3}{z_4}$ with $(z_3z_4,p)=1$。我们定义 a 的 p-进绝对值为 $|a|_p=p^{-e}$，规定 $|0|_p=0$。满足以下性质：1° $|a|_p\geqslant 0$；2° $|ab|_p=|a|_p|b|_p$；3°（强三角不等式）$|a+b|_p\leqslant\max\{|a|_p,|b|_p\}$。一个由有理数组成的无穷序列$\{a_1,a_2,\cdots\}$称为 p-进 Cauchy 序列，如果对 $|a_m-a_n|_p$ 满足 Cauchy 性质。以 S 记 Q 中所有 Cauchy 序列组成的集合，定义 S 中二元关系~为$(a_1,a_2,\ldots)\sim(b_1,b_2,\ldots)$，if $|a_n-b_n|_p\to 0$ with $n\to+\infty$。容易证明~是一个等价关系。在商集 S/~上平凡地定义"+","·"运算，即 $\overline{(a_1,a_2,\cdots)}+\overline{(b_1,b_2,\cdots)}=\overline{(a_1+b_1,a_2+b_2,\cdots)}$，$\overline{(a_1,a_2,\cdots)}\cdot\overline{(b_1,b_2,\cdots)}=\overline{(a_1b_1,a_2b_2,\cdots)}$，容易验证该运算是良定义的，且利用 Q 是域容易证明 S/~也是域，称为 p-进数域，记为 Q_p。令 $T=\{(a_tp^t,a_tp^t+a_{t+1}p^{t+!},\cdots)\mid t\in Z,0\leqslant a_i\leqslant p-1\}$。容易证明 $T\to S/\sim,t\mapsto\overline{t}$ 是一个双射。从而可记 $Q_p=\{\sum_{i=t}^{+\infty}a_ip^i\mid t\in Z,0\leq a_i\leq p-1\}$，其中任意两个元素的四则运算的结果的 p^i 系数都可以在有限步骤内确定。对于 $a=\sum_{i=t}^{+\infty}a_ip^i\in Q_p$，规定 $|a|_p=p^{-t}$。p-进绝对值可以被 p-进赋值等价刻画，定义 $v_p(a)=t$，$v_p(0)=\infty$。对应满足性质：1° $v_p(a)\in Z\cup\{\infty\}$；2° $v_p(ab)=v_p(a)v_p(b)$；3° $v_p(a+b)\geqslant\min\{v_p(a),v_p(b)\}$。容易验证 $R=\{a\in Q_p\mid|a|_p\leqslant 1\}=\{a\in Q_p\mid v_p(a)\geqslant 0\}$构成环，称为 p-进整数环，记为 Z_p。R 有理想 $I=\{a\in Q_p\mid|a|_p<1\}=\{a\in Q_p\mid v_p(a)>0\}$，称为 Q_p 的赋值理想。K=R/I 称为 Q_p 的剩余域，是 p 元有限域。

四元数体：形如 a+bI+cJ+dK，a,b,c,d∈R（实数域）。在环 $M_2(C)$中理解为：$1=\begin{pmatrix}1&0\\0&1\end{pmatrix}$，$I=\begin{pmatrix}i&0\\0&i\end{pmatrix}$，$J=\begin{pmatrix}0&1\\-1&0\end{pmatrix}$，$K=\begin{pmatrix}0&i\\i&0\end{pmatrix}$，$I^2=J^2=K^2=-1$，IJ=K=-JI，JK=I=-KJ，KI=J=-KI。

给定两个域 F,F_1，环同态 $f:F\to F_1$ 称为一个从域 F 到域 F_1 的同态（显然该同态一定是单的，这是也称 f 是一个从 F 到 F_1 的嵌入）如果同态 f 是满射，则称 f 是一个从 F 到 F_1 的同构；如果存在 F 到 F_1 的同构映射，则称 F 与 F_1 是同构的，记为 $F\sim F_1$。
没有更小子域的域称为素域。
设 F 是域，使得 n·1=0 的最小正整数 n 称为 F 的特征，如果不存在这样的正整数，称 F 的特征为 0。F 的特征记为 char(F)。
设 F 是域，如果 char(F)>0，则 char(F)必为素数。
设 F 是域，如果 char(F)=0，则 F 包含的最小子域与 Q 同构，如果 char(F)=p>0，则 F 包含的最小子域与 GF(p)=Z/pZ 同构。

第 2 章 群

2.1 几种特殊类型的群

无限循环群同构于整数加法群 Z，有限循环群同构于某个商群 Z/mZ。
循环群 G 的子群是循环群。若 G 是无限循环群，则 G 的子群与非负整数一一对应，每个 s 对应于子群$<a^s>$；若 G 是 m 阶有限循环群，则 G 的子群与 m 的正因子一一对应，d 对应于 G 的子群$<a^{m/d}>$。
G 是 Abel 群，a,b∈G，o(a)=m，o(b)=n 且(m,n)=1。则 o(ab)=mn。
设 G_1,G_2 分别是 m,n 阶循环群，则 $G_1 \oplus G_2$ 是 mn 阶循环群。
有限 Abel 群 G 存在一个元素 g，它的阶数是群 G 的方次数，即 o(g)=exp(G)。
设 G 是有限 Abel 群，则 G 是循环群的充要条件是对于任一正整数 m，方程 $x^m=e$ 在 G 中至多有 m 个解。
如果 G 的正规子群只有{e}和 G 自身，则称 G 是一个单群。
Abel 群是单群当且仅当它是素数阶循环群。
任一偶置换都可以写成 3 轮换的乘积。
n≥5 时，A_n 是单群。
设 G 是群，a,b∈G。规定$[a,b]=aba^{-1}b^{-1}$，并称之为元素 a 和 b 的换位子。由 G 中所有元素对的换位子生成的子群为 G 的换位子群，或导群，记为 G'。显然，G 为交换群的充要条件是 G'={e}，从而 G'可看成是 G 的非交换性的一种度量。
G'是 G 的正规子群，G/G'是交换群。若 H 是正规子群，则 G/H 是交换群的充要条件是 G'≤H。
称 G 的子群 H 是特征子群，如果对于 f∈Aut(G)，都有 f(H)=H。并记为 H◁◁G。事实上，G'◁◁G。

设 A,B,C 是群，则：1° A◁◁B，则 A◁B；2° A◁◁B，B◁◁C，则 A◁◁C；3° A◁◁B，B◁C，则 A◁C。

定义 G 的 n 阶导群 $G^{(n)}=(G^{(n-1)})'$，则 $G^{(n)}$◁◁G。
给定群 G，如果存在一个正整数 n 使得 $G^{(n)}=\{e\}$，则称 G 是一个可解群。

给定群 G，则 G 是一个可解群的充要条件是存在 G 的子群列 $G=G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_s=\{e\}$

使得 G_i/G_{i+1} 都是交换群。
可解群示例：$S_4>A_4>K_4>\{e\}$，$S_3>A_3>\{e\}$。
设$(i_1,i_2,\cdots,i_t)$是对称群 S_n 中的一个轮换，$\sigma\in S_n$，则$\sigma(i_1,i_2,\cdots i_t)\sigma^{-1}=(\sigma(i_1),\sigma(i_2),\cdots,\sigma(i_t))$。
设对于 g∈G，I_g:G→G，a→gag^{-1}(g 引起的共轭变换)。则 I_g 在映射的乘法下构成群，称为内自同构群 $I_{nn}(G)$，这是 Aut(G)的正规子群。I_e 是单位元，$I_gI_h=I_{gh}$，$I_{g^{-1}}=(I_g)^{-1}$，$fI_gf^{-1}=I_{f(g)}$。外自同构群定义为 $Aut(G)/I_{nn}(G)$。
重要结论：$G/Z(G)\sim I_{nn}(G)$；N 是 G 的正规子群，N 可解，G/N 可解，则 G 可解。
设 H≤G，$C_G(H)=\{x\in G|xa=ax,\forall a\in H\}$，$N_G(H)=\{x\in G|xHx^{-1}=H\}$，它们分别称为 H 在 G 中的中心化子和正规化子。称 $Z(G)=C_G(G)$为 G 的中心。容易验证，$C_G(H)$和 $N_G(H)$均为 G 的子群，且 H 和 $C_G(H)$是 $N_G(H)$的正规子群，Z(G)是 G 的特征子群。
常见结论：$Z(S_3)=\{e\}$，$Z(S_4)=\{e\}$。
设 G 是一个群，定义 $Z_0(G)=\{e\}$，$Z_1(G)=Z(G)$，$Z_2(G)/Z_1(G)=Z(G/Z_1(G))$，…，$Z_{k+1}(G)/Z_k(G=Z(G/Z_k(G))$。如果存在 k 使得 $Z_k(G)=G$，则称 G 是一个幂零群，最小的 k 称为幂零群的类。对 k 类幂零群 G，其正规子群组成的子群链$\{e\}=Z_0(G)\triangleleft Z_1(G)\triangleleft\cdots\triangleleft Z_k(G)=G$称为 G 的上中心链。幂零群是交换群，幂零群和可解群都是交换群的推广。（交

换⇒幂零⇒可解）
定义阶数为素数 p 的方幂的群为 p 群。
对群 G 中元素 a,b 如果存在元素 c 使得 $cac^{-1}=b$，则称 a 与 b 共轭，或 a 在 c 的共轭作用下变为 b。共轭是一种等价关系，a 所在的共轭类中元素的个数为$[G:C_G(a)]$。p 群是幂零群，p^2 阶群是交换群。

类方程：$|G|=|Z(G)|+\sum_{i=1}^{n}|\overline{a_i}|=|Z(G)|+\sum_{i=1}^{n}|G:C_G(a_i)|$。（本质是等价类无交并）

2.2 群在集合上的作用和 Sylow 定理

设 G 是一个群，M 是一个集合，映射 f:G×M→M，(g,m)→f(g,m)/g(m)如果满足：1° e(m)=m；2° $g_1(g_2(m))=(g_1g_2)(m)$，则称为 f 是群 G 在集合 M 上的一个作用。群 G 在集合 S 上的作用，实际上是指 G 到 M 的全变换群 S(M)的同态映射。
对给定的作用 f:G×S→S，S 中元素的下述关系是等价关系：s_1~s_2 if there exists g belonging to G and $g(s_1)=s_2$。S 在这个等价关系之下的等价类称为轨道。元素 s∈S 所在的轨道记为 Orb(s)。我们有 $S=\bigcup_{Orb(s)}Orb(s)$。定义 Stab(s)={g∈G|g(s)=s}，称之为元素 s 的稳定子群或稳定化子。
设群 G 在集合 S 上有一个作用，则：1° 若 $gs_1=s_2$，则 $Stab(s_2)=gStab(s_1)g^{-1}$；2° 如果集合 S 有限，则|Orb(s)|=|G:Stab(s)|。
设群 G 在有限集合 S 上有一个作用，$s_1,s_2,\cdots,s_m$ 是全体轨道代表元，则有推论

$$S=\sum_{i=1}^{m}|Orb(s_i)|=\sum_{i=1}^{m}|G:Stab(s_i)|。$$

设$|G|=p^an$，p 是素数，则 G 必有 p^a 阶子群。且 G 的 p^a 解子群个数 $N(p^a)$满足关系 $N(p^a)\equiv1(\mathrm{mod}\ p)$。
如果 $o(G)=p^an$ 且(p,n)=1，则 G 的 p^a 阶子群称为 G 的 Sylow p-子群。
第一 Sylow 定理：若 p|o(G)，p 是素数，则 G 必有 Sylow p-子群，且 G 的 Sylow p-子群个数 $N_p\equiv1(\mathrm{mod}\ p)$。
Cauchy 定理：设 G 是一个有限群，素数 p|o(G)，则 G 必有 p 阶元，且 G 的 p 阶元的个数 n_p 满足关系 $n_p\equiv-1(\mathrm{mod}\ p)$。
第二 Sylow 定理：设 G 是一个有限群，素数 p|o(G)，则 1° 若 S_p 是 G 的一个 Sylow p-子群，P 是 G 的一个 p-子群，则必有一个元素 x∈G 使得 $P\leqslant xS_px^{-1}$；2° G 的所有 Sylow p-子群两两共轭，因此$|G:N_G(S_p)|$(每一个陪集对应一个共轭元，从而相等)$=N_p\equiv1(\mathrm{mod}\ p)$。【从而设$|G|=p^an$ 且(p,n)=1，那么有 $N_p|n$】
设 G 是一个有限群，素数 p|o(G)，S_p 是 G 的一个 Sylow p-子群，$N_G(S_p)\leqslant H\leqslant G$，那么 $N_G(H)=H$。
设 G 是一个有限幂零群，素数 $p_1,p_2,\cdots,p_n$ 为|G|的所有素因子，则 $G=S_{p1}\oplus S_{p2}\cdots\oplus S_{pn}$。【有限幂零群的 Sylow p-子群一定是正规子群；有限幂零群的子群是其正规化子的正规真子群】

设 G 是一个有限 Abel 群，$o(G)=p_1^{e1}p_2^{e2}\cdots p_n^{en}$，则 $G\sim\bigoplus_{i=1}^{t}\bigoplus_{j=1}^{k_i}Z/p_i^{l_{ij}}Z$，且 $\sum_{j=1}^{k_i}l_{ij}=e^i$。

设 G 是一个有限 Abel 群，o(G)=n，则 $G\sim\bigoplus_{i=1}^{k}Z_{d_i}$，其中 d_i 满足 $d_1|d_2|\cdots|d_n$ 且 $d_1d_2\cdots$

$d_n=n$。这些 d_i 称为 G 的不变因子。

设 G 是一个初等交换 p 群，则 $G \sim \overset{n}{\underset{i=1}{\oplus}} Z/pZ$ 。

2.3 合成群列

设 G 是一个群，一个子群降链 $G=G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_r=e$ 称为群 G 的次正规群列，其中每个子群称为群G的次正规子群。如果上述次正规群列中 G_{i-1}/G_i 是非平凡单群，则称该群列为 G 的一个合成群列，r 个商群 G_{i-1}/G_i 称为该群列的合成因子。

Schreier 定理：设 G 是一个有限群，它的任意一个无重复项的次正规群列可以加细成为合成群列。

Jordan-Holder 定理：设 G 是一个有限群，它的所有合成群列的长度都相等，且他们的合成因子在不记顺序的意义下对应同构。

第 3 章 环

3.1 环的若干基本知识

设 I,J 是环 R 的两个理想，则 I+J,I∩J 也是环 R 的理想。

当 I+J=R（$\Leftrightarrow 1\in I+J$）时，称理想 I 与 J 互素。当 I=(a),J=(b)是交换环 R 的主理想时，I 与 J 互素表示存在 u,v 使得 ua+vb=1，这与 Z、F[x]情形下两个元素互素的定义一致。

设 I,J 是环 R 的两个理想，称由集合{ab|a∈I,b∈J}生成的理想为理想 I 与 J 的积，记为 IJ。$IJ=\{\Sigma a_ib_j|a_i\in I,b_j\in J\}$；一般情况下，IJ≠JI；$IJ\subset I\cap J$，当 I 与 J 互素且 IJ=JI 等号成立；分配律成立，I(J+K)=IJ+IK，(I+J)K=IK+JK。

设 I_1,I_2,J 是环 R 的理想，且 I_1,I_2 都与 J 互素，则 I_1I_2 与 J 互素。从而设 $I_1,\cdots I_n,J$ 是环 R 的理想，且 $I_1,\cdots,I_n$ 都与 J 互素，则 $I_1\cdots I_n$ 与 J 互素。

中国剩余定理：设 $I_1,\cdots,I_n$ 是环 R 中两两互素的理想，则 $R/(I_1\cap\cdots\cap I_n)\sim R/I_1\oplus\cdots\oplus R/I_n$。

设 P 是环 R 的真理想。如果对于任意 a,b∈R，ab∈P 蕴含 a∈P 或 b∈P，则称 P 为 R 的一个素理想；如果对于 R 的理想 I，$I\supset P$ 蕴含 I=R，则称 P 为 R 的一个极大理想。

设 R 是交换环，则 1° P 是 R 的素理想当且仅当 R/P 是整环；2° P 是 R 的极大理想当且仅当 R/P 是域。对于交换环 R，其极大理想一定是素理想。

设 R 是整环，$R\times R^*=\{(a,b)|a,b\in R,b\neq 0\}$。在 $R\times R^*$上定义一个关系~：(a,b)~(a',b')当且仅当 ab'=a'b。容易验证这是一个等价关系，把(a,b)所在的等价类记为 a/b，定义 a/b+c/d=(ad+bc)/bd,a/b·c/d=ac/bd。从而 $R\times R^*/\sim$在此二元运算下构成域，并且 $R<R\times R^*$。该域$(R\times R^*)$称为整环 R 的分式域。

设 R 是交换环，S 是 R 的包含 1 的乘法封闭子集。这是在集合 $R\times S=\{(a,b)|a\in R,b\in S,b\neq 0\}$上定义一个关系~：(a,b)~(a',b')当且仅当存在 s∈S 使得 sab'=sa'b。从而 $R\times S/\sim$在类似运算下构成分式化环，记为 $S^{-1}R$。此时 $R\to S^{-1}R$，$a\to a/1$ 是嵌入（单同态）的充要条件是 S 中不包含 R 的零因子。

在 Z 中，取 P=(p)，p 是素数，S=Z\P，则 $Q\supset S^{-1}Z=\{b/a|a,b\in Z,p\nmid a\}=Z_{(p)}$。从而 $S^{-1}Z$ 只有一个非零素理想 $pZ_{(p)}=\{bp/a|a,b\in Z,p$ 不整除 $a\}$（只有一个非零素理想的环称作局部环）。

3.2 整环内的因子分解理论

在整环 R 中，如果 a,b,c∈R 满足 a=bc，则称 a 是 b 的倍式，b 是 a 的因子。这时称 b 整除 a，记作 b|a。如果 R 的非零元 a,b 满足 a|b,b|a，则称 a 与 b 相伴，记作 a~b。
在整环 R 中，0≠a=bc，则 a 与 b 相伴的充分必要条件是 c 为可逆元。
在整环 R 中，如果 b|a_i，则称 b 是 a_i 的公因子；如果 d 是 a_i 的公因子，且 a_i 的任一公因子都能整除 d，则称 d 为 a_i 的最大公因子，记为 d=(a_i)。如果 a_i|b，则称 b 是 a_i 的公倍式；如果 c 是 a_i 的公倍式，且 a_i 的任一公倍式都被 c 整除，则称 c 是 a_i 的最小公倍式，记作 c=[a_i]。最大公因子和最小公倍式非零时，它们在相伴意义下唯一。
在整环 R 中，如果 0≠a∈R 不是可逆元，且 a=bc 蕴含 b 或 c 二者之一是可逆元，则称 a 为 R 的不可约元；如果 0≠p∈R 不是可逆元，且 p|bc 蕴含 p|b 或 p|c，则称 p 为 R 的素元。
在整环 R 中，p 是素元的充要条件是(p)是非零素理想；素元一定是不可约元，但不可约元未必是素元。例：在 R=Z[$\sqrt{-5}$]={a+b$\sqrt{-5}$ |a,b∈Z}中，3,2±$\sqrt{-5}$ 都是不可约元，但不是素元；9 和 3×(2+$\sqrt{-5}$)没有最大公因子。
如果整环 R 中不存在无限多个元素 $a_1,a_2,\cdots$使得 a_{i+1} 是 a_i 的真因子（即 a_{i+1}|a_i 但 $a_i \nmid a_{i+1}$），则称 R 满足因子链条件。如果整环 R 满足因子链条件，则 R 的每一个不可逆元可以分解为有限个不可约元的乘积。
整环 R 称为唯一分解整环，如果：1° R 的每一个不可逆元 a 可以分解为有限个不可约元的乘积 a=$p_1p_2\cdots p_m$；2° 如果 a=$p_1p_2\cdots p_m$=$q_1q_2\cdots q_n$ 是 a 的两种不可约分解，则必有 m=n，且适当调整次序后有 p_i~q_i。
整环 R 是唯一分解整环的充要条件是 R 满足因子链条件且 R 中的不可约元都是素元。
一个环称为 Noether 环，如果不存在 R 无限个理想的真升链 $I_1\subset I_2\subset I_3\cdots$。显然，Noether 整环一定满足因子链条件。
如果整环 R 的每一个理想都是由一个元素生成的，则称 R 是主理想整区（PID）。PID 是 Noether 环，且 PID 中的非零素理想是极大理想。这种环称为 1 维的。
PID 中 a 不可约当且仅当(a)是极大理想。
PID 是唯一分解整环。
整环 R 中，如果有一个从 R\{0}到非负整数 N 的映射 f，使得对任意 a,b∈R，b≠0 都存在 a=bq+r，r=0 或 f(r)<f(b)，则称 R 是一个欧几里得环。欧氏环是 PID。
假设 R 是一个环，同域上的多项式类似，我们可以定义环 R 上的多项式环如下：R[x]={$a_0+a_1x+\cdots+a_nx^n$|$a_0,a_1,\cdots a_n$∈R,n∈N}。R[x]中元素的加法、乘法和域上的多项式类似。
设 R 是唯一分解整环，f(x)∈R[x]。f(x)的各项系数的最大公因式称为 f(x)的容度，记为 c(f(x))。若 c(f(x))=1，则称 f(x)是 R[x]中的本原多项式。
Gauss 引理：设 R 是唯一分解整环，则本原多项式的乘积也是本原多项式。
设 R 是唯一分解整环，则 c(fg)=c(f)c(g)。
设 R 是唯一分解整环，K 是 R 的分式域，f(x)∈R[x]，deg f≥1，如果 f(x)在 R[x]中不可约，则 f(x)在 K[x]中也不可约。
唯一分解整环上的多项式环仍是唯一分解整环；唯一分解整环上的多元多项式环

仍是唯一分解整环。
域一定是唯一分解整环，因为它没有不可约元。

第 4 章 域

设域 E 是域 F 的一个扩域，F≤E，S 是 E 的一个子集，E 中包含 F 和 S 的最小子域，称为域 F 添加 S 的扩域或域 F 上由 S 生成的域，记为 F(S)。这时称 S 为 F(S)在 F 上的一个生成元系。当一个子域 K 包括 F 可以是 F 添加有限集 S 的扩域时，则称 K 是 F 上的有限生成域，否则称为无限生成的。如果 $S=\{a_1,a_2,\cdots,a_n\}$，则 F(S)可记为 $F(a_1,a_2,\cdots,a_n)$。特别地，F(a)称为 F 的单扩张。
$F(a)=f(a)/g(a),f(x),g(x)\in F[x]$；$F(a_1,a_2,\cdots,a_n)=F(a_1,\cdots,a_n)=f(a_1,\cdots,a_n)/g(a_1,\cdots,a_n),f(x),g(x)\in F[x]$；F(S)(T)=F(T)(S)=F(S∪T)。
假设域 E、F 是 K 的子域，K 中包含 F 和 E 的最小子域称为域 F 和 E 的合成，记为 FE。容易看出 FE=EF=E(F)。
假设 K/F 是域扩张，$t_1,t_2,\cdots,t_n\in K$。如果存在 F 上的非零多项式 $f(x_1,x_2,\cdots,x_n)$使得 $f(t_1,t_2,\cdots,t_n)=0$，则称 $t_1,\cdots,t_n$ 在 F 上代数相关，否则称它们代数无关。一个元素 t 在 F 上代数相关（无关）时，称 t 是 F 上的代数元（超越元）。如果域扩张 K/F 中 K 的所有元素均为 F 上的代数元，则称 K 是 F 的代数扩张，否则称为超越扩张。
设 F 是域，K=F(a)，如果 a 是 F 上的超越元，则 F(a)同构于 F 上的一元有理分式域 F(x)。
设 K/F 是添加代数元的单扩张，即 K=F(a)，a 是 F 上的代数元。集合 I={g(x)∈F[x]|g(a)=0}称为 a 的零化理想，它是首一生成元 f(x)称为 a 的最小多项式，记为 $I_{rr}(a,F)$。这时称 deg f(x)为 a 的次数。
设 K/F 是添加代数元的单扩张，即 K=F(a)，a 是 F 上的代数元。则 a 的最小多项式 f(x)是不可约多项式，且 K~F[x]/(f(x))。
商环 F[x]/(f(x))是域的充分必要条件是 f(x)是 F 上的不可约多项式。这时 F[x]/(f(x))是 F 的单扩张 F[a]。且 a 是 deg f(x)次的代数元。
设 K/F 是域扩张，$\dim_F K$ 称为扩张 K/F 的次数，记为[K:F]。当[K:F]有限时，称 K/F 是有限扩张，否则称为无限扩张。单扩张 F(a)/F 是有限扩张当且仅当 a 是 F 上的代数元，这时 a 的次数等于扩张次数[F(a):F]。
设 K/E 和 E/F 是域扩张，则 K/F 是有限扩张当且仅当 K/E 和 E/F 是有限扩张，此时[K:F]=[K:E][E:F]。【基的组合乘法是新基，域扩张是按倍数扩大】
K/F 是有限扩张当且仅当它是有限生成的代数扩张。
添加代数元的单扩张是代数扩张。
在扩张 K/F 中，K 中全体代数元组成一个 F 的扩域，称之为 F 在 K 中的代数闭包。当一个域没有真代数扩张时，则称之为代数封闭域。假设扩张 K/F 是代数扩张，且 K 是代数封闭域，则称 K 是 F 的代数闭包。
一个域 K 是代数必域的充分必要条件是它上面的任意非常数多项式 f(x)∈K[x]均可分解为一次因式的乘积。

4.2 分裂域与正规扩张

假设 F 是一个域，f(x)∈F[x]是一个 n 次多项式。如果 K 是 F 的一个扩张，使得 f(x)在 K 上可以分解为一次因式的乘积，且 $K=F[a_1,a_2,\cdots,a_n]$，这里 $a_1,a_2,\cdots,a_n$ 是 f(x)的全部根。则称 K 是 f(x)在 F 上的分裂域。
假设 F 是一个域，f(x)∈F[x]是一个 n 次多项式，则 f(x)在 F 上的分裂域存在，且在 F-同构的意义下唯一。

假设 g:F→F'是域同构，f(x)是 F 上的一个不可约多项式，则 $f^g(x)$是 F'上的不可约多项式。又设 a 和 a'分别是 f(x)和 $f^g(x)$的零点，则 g':F[a]→F[a']，m(a)→m(a')是域同构。由于 $g'|_F=g$，我们称 g'是 g 的延长。恒等同构的延长称为 F-同构。
假设 g:F→F'是域同构，f(x)∈F[x]，F 是一个域，E 是 f(x)在 F 上的一个分裂域，E'是 $f^g(x)$在 F'上的一个分裂域，则存在同构映射 g':E→E'，它是 g 的一个延长 $g'|_F=g$。
假设 F 是一个域，f(x)∈F[x]是一个非常数多项式，f(x)在 F 上的某个分裂域在域 L 中，则 f(x)在 F 上的在 L 中的分裂域在相等意义下唯一。并且此分裂域在 L 的任一 F-同构下映射到自身。
假设 F 是一个域，f(x)∈F[x]是一个非常数多项式，E 是 f(x)在 F 上的一个分裂域。则对于 F[x]中的任意一个不可约多项式 g(x)，如果在 E 中有根，则它在 E 中分裂。
设 E/F 是代数扩张，如果对于 F[x]的任意一个不可约多项式 g(x)，在 E 中有根，必有它在 E 中分裂，则称 E/F 是正规扩张。
有限扩张 E/F 是正规扩张，当且仅当 E 是 F[x]中某多项式在 F 上的分裂域。
E/F 是有限正规扩张，L/E 是任意域扩张，则 L 的任意 F-自同构把 E 映到自身。
设 K/F 是有限扩张，E 是 K 的扩张，使得 1° E/F 正规；2° K 和 E 之间没有其他的 F 的正规扩张；则称 E 是扩张 K/F 的正规闭包。正规闭包在 F-同构意义下唯一。
含有有限个元素的域称为有限域。如果 K 是有限域，则它的素域一定是 GF(p)，这里 p 是素数，而且 K/GF(p)一定是有限扩张。设[K:GF(P)]=n，即 K 是 GF(p)上的线性空间，故$|K|=p^n$。
对于任意的素数方幂 p^n，存在 p^n 个元素的域，并且这种域在同构意义下唯一。

【$x^{p^n}-x$ 的分裂域】我们把它称为 p^n 元域，记为 $GF(p^n)$。$GF(p^n)^X$ 是 p^n-1 阶的循环群。【$x^d=1$ 至多有 d 个解】
假设 $GF(p^n)^X=<a>$，则必有 $GF(p^n)=GF(p)[a]$。可见 a 满足的极小多项式 f(x)是 n 次的。从而对任意正整数 n，GF(p)上存在 n 次不可约多项式。
映射 $f_p:GF(p^n)\to GF(p^n)$，$a\to a^p$ 是 $GF(p^n)$的 GF(p)-同构，称为 Frobenius 自同构。事实上，$Aut(GF(p^n))=<f_p>$是 n 阶循环群。

4.3 可分扩张

设 F 是一个域，f(x)∈F[x]，a 是 f(x)的 k≥1 重根。用 f'(x)表示 f(x)的导数，则 1° 当 char(F)不整除 k 时，a 是 f'(x)的 k-1 重根；2° 当 char(F)|k 时，a 至少是 f'(x)的 k 重根。
设 F 是一个域，不可约多项式 f(x)∈F[x]有重根 ⇔ (f(x),f'(x))≠1 ⇔ f'(x)=0。
设 F 是一个域，不可约多项式 f(x)∈F[x]。如果 f(x)在它的分裂域中无重根，则称 f(x)是可分多项式，否则称 f(x)是不可分多项式。
特征 0 域和有限域上的不可约多项式都是可分多项式。
特征 0 域和有限域上的代数扩张一定是可分扩张。

设 f(x)是特征为 p 的域 F 上不可分多项式，则 $f(x)=g(x^{p^i})$，这里 g(y)是 F 上的可分多项式。
设 char(F)=p，则 x^p-a 要么不可约（从而不可分），要么完全分裂 $x^p-a=(x-b)^p$。
假设 K/F 是一个代数扩张，a∈K。如果 Irr(a,F)是 F 上的可分多项式，称 a 是 F 上的可分元，否则称 a 是不可分元。如果 K 中所有元都是可分元，则称它是 F 的可分扩张，否则称 K 是 F 的不可分扩张，特别地，当 K\F 中所有元都是 F 上的不可分元，则称 K 是 F 的纯不可分扩张。

假设 K=F[a,b]是 F 的一个代数扩张，且 b 是 F 上的可分元，则 K=F[c]是单扩张。
有限可分扩张是单扩张。
设 g:K→L 是域嵌入，a 是 K 上不可约多项式 f(x)的根，L 包括 $f^g(x)$的分裂域，则 g 可延拓为 K(a)到 L 的嵌入。这种延拓与 $f^g(x)$的零点一一对应，从而在 g 上的延拓数≤[K[a]:K]，等号成立当且仅当 a 是 K 上的可分元。
设 K/F 是有限域扩张，$K=F(a_1,a_2,\cdots,a_t)$，$g_i(x)=Irr(a_i,F)$，E 是多项式 $g(x)=\Pi g_i(x)$在 F 上的分裂域，则 K 到 E 的 F-嵌入个数≤[K:F]，等号成立当且仅当 K/F 是可分扩张。
设 $K=F(a_1,a_2,\cdots,a_t)$，则 K/F 是可分扩张当且仅当 $a_1,a_2,\cdots,a_t$ 是 F 上的可分元。
设 K/F 是有限扩张，则 K 中全部 F 上的可分元构成 K/F 的一个中间域，称为 F 在 K 中的可分闭包。
设 E/F 是一个有限正规扩张（多项式的分裂域），则 E 是 F 的可分扩张当且仅当 E 到自身的 F-同构个数是[E:F]。

4.4 Galois 理论简介

设 K/F 是一个域扩张，K 的全体 F-自同构构成的群称为扩张 K/F 的 Galois 群，记为 Gal(K/F)。
设 G 是域 K 的一个自同构群（指由部分自同构组成的群），元素 a∈K 如果满足 f(a)=a，∀f∈G，则称 a 是 G 的一个不动元。K 中全体不动元的集合称为 G 的不动域，记为 Inv(G)。
给定域 K 的两个自同构群 G_1,G_2，若 $G_1\subset G_2$，则 $Inv(G_1)\supset Inv(G_2)$。
给定域 K 的两个子域 F_1,F_2，若 $F_1\subset F_2$，则 $Gal(K/F_1)\supset Gal(K/F_2)$。
若域扩张 E/F 的 Galois 群 Gal(E/F)的不动域恰好为 F，即 Inv(Gal(E/F))=F，则称 E/F 是一个 Galois 扩张。
关于有限域扩张 E/F，下列三条等价：
1° E/F 是一个 Galois 扩张；
2° E/F 是可分正规扩张；
3° |Gal(E/F)|=[E:F]。
Artin 引理：设 H 是 E 的一个有限自同构群，L=Inv(H)，则[E:L]≤|H|。
Galois 基本定理：设 E/F 是有限 Galois 扩张，G=Gal(E/F)，用 $I_H=\{H|\{e\}\leqslant H\leqslant G\}$表示 G 的全体子群集合，用 $I_L=\{L\}F\leqslant L\leqslant E\}$表示 E/F 的全体中间子域的集合，则
1° L→Gal(E/L)，H→Inv(H)是互逆双射；
2° 反包含关系，$H_1\subset H_2\Leftrightarrow Inv(H_1)\supset Inv(H_2)$；
3° [E:L]=|Gal(E/L)|，[L:F]=|Gal(E/F):Gal(E/L)|；
4° 若 H 与 L 对应，则共轭子群$\sigma H\sigma^{-1}$与子域σ(L)对应；
5° H 是 G 的正规子群当且仅当 L=Inv(H)是 F 上的正规扩张，且 r:G→Gal(L/F)，σ→$\sigma|_L$是群的满同态，其核为 H，从而 Gal(L/F)~G/H。
Galois 定理：设 F 是特征 0 域，f(x)∈F[x]，E 是 f(x)在 F 上的分裂域，则 f(x)=0 存在根式解的充分必要条件是 Gal(E/F)为可解群。

第 5 章 模与格简介

5.1 模的基本概念

设 R 是一个环，M 是一个交换群，定义一个左乘运算：R×M→M，(a,x)→ax，如果满足 a(x+y)=ax+ay，(a+b)x=ax+bx，(ab)x=a(bx)，1x=x，则称 M 是一个环 R 上的一个（左）模，或（左）R 模。
设 M 是一个 R 模，N⊂M 是 M 的加法子群，且 R 在 M 上的作用限制在 N 上使得

N 构成一个 R 模，则称 N 是 M 的一个子模。
设 $M_1,M_2\subset M$ 是 R 模 M 的两个子模，它们的交与和定义为加法子群的交与和。
设 M 是一个 R 模，$S\subset M$，则称 M 的所有包含 S 的子模的交为由 S 生成的子模，记为 R·S 或 RS。S 称为子模 RS 的生成元集。如果 S 是有限集，则称 RS 有限生成的；由一个元素 x 生成的子模可简记为 Rx，称为循环模。
设 N 是 R 模 M 的一个子模，规定 R 在商群(M/N,+)上的作用为 $R\times M/N\to M/N$，$(a,x+N)\to ax+N$，则 M/N 构成了一个 R 模，称为 M 关于子模 N 的商模。
环 R 模 M 到环 R 模 T 的映射 $f:M\to T$，如果满足 $f(x+y)=f(x)+f(y),x,y\in M$，$f(ax)=f(a)f(x)$，$a\in R,x\in M$，则称 f 是 R 模 M 到 R 模 T 的一个同态，模同态 f 如果又是单射（满射）则称 f 是单（满）同态，既单又满的同态称为同构。如果存在模 M 到模 T 的同构映射，则称 M 与 T 是同构的，记为 M~T。
若 $f:M\to T$ 是 R-模同态，用 Im f 或 f(M)表示 f 的像，而称 $\ker f=\{x\in M|f(x)=0\}$为 f 的核。
同态基本定理：M/Ker f~Im f。
第一同构定理：设 R 是环，N 是 R-模 M 的理想，则在典范同态 $f:M\to M/N$，$a\to a+N$ 下，1° M 包含 N 的子模与 M/N 的子模在 f 下一一对应，这种对应保持包含关系；2° 若 L 是 M 的子模，且 $N\subset L$，则 M/L~(M/N)/(L/N)。
第二同构定理：设 M 是 R 模，L,N 是 M 的子模，则有模同构：$f:(L+N)/N\to L/(L\cap N)$，$l+n\to l+(L\cap N)$。
设 M_1,M_2 是 R-模，在它们的笛卡尔积上定义运算如下：对于加法群的直和 $M_1\oplus M_2$，按分量定义 R 左乘作用 a(x,y)=(ax,ay)，则 $M_1\oplus M_2$ 在此运算下构成一个 R-模，称为 M_1 与 M_2 的直和，仍记为 $M_1\oplus M_2$。M_1 和 M_2 称为 $M_1\oplus M_2$ 的直和因子。
设 M 是 R-模，M_1,M_2 是 M 的子模，$M=M_1+M_2$。下述 4 条等价：1° 映射 $f:M_1\oplus M_2\to M$，$(x,y)\to x+y$ 是同构；2° M 的任一元素表示为 M_1 与 M_2 的元素的和表示法唯一；3° M 的 0 元表示为 M_1 与 M_2 的元素的和表示法唯一；4° $M_1\cap M_2=\{0\}$。

5.1* 主理想整区上的有限生成模

本节中均假定环 R 是主理想整区，我们重点研究有限生成的 R-模。
设 R 为主理想整区，$x\in M$ 是 R-模 M 中的一个元素，称 $\text{ann}(x)=\{a\in R|ax=0\}$是元素 x 的零化子；$\text{ann}(x)\neq\{0\}$时称 x 为扭元；当 $\text{ann}(x)=\{0\}$时称 x 为自由元。
ann(x)是 R 的理想，故零化子也叫作零化理想。由于 Rx~R/ann(x)，从而 $Rx\sim R\Leftrightarrow x$ 是自由的。
设 M 是 R-模。如果 M 中每个元素均是扭元素，则称 M 是扭模；如果 M 中每个元素均是自由模，则称 M 是无扭模。
设 R 为主理想整区，有限生成 R-模 M 如果可以写成 $M=Re_1\oplus Re_2\oplus\cdots\oplus Re_n$，且 $\text{ann}\{e_i\}=\{0\}$，则称 R 是一个秩为 n 的自由模。秩是由有限生成自由模唯一决定的。
设 R 是主理想整区，M 是秩为 n 的自由模，则 M 的任一子模也是自由 R-模，且秩≤n。（自由模一定是无扭模）
主理想整区上的有限生成模的子模也是有限生成的。
主理想整区上的有限生成的无扭模一定是自由模。
设 M 是有限生成 R-模，Tor(M)表示 M 的扭元集，$\text{Tor}(M)\leq M$，则 M/Tor(M)无扭。
考虑映射 $f:M\to M/\text{Tor}(M)$，$M/\text{Tor}(M)=\langle e_1',\cdots,e_s'\rangle$，考虑原像集 $N=Re_1\oplus\cdots\oplus Re_s$，则 $M=\text{Tor}(M)\oplus N$。（扭元+自由元直和）
设 A,B 是主理想整区 R 上的两个 $m\times n$ 矩阵，如果存在 m 阶可逆矩阵 P，n 阶可

逆矩阵 Q 使得 B=PAQ，则称 A,B 在 R 上等价。
设 A 为主理想整区 R 上的一个 m×n 矩阵，则 A 等价于下列矩阵 B=diag{$d_1,\cdots,d_r$, 0,⋯,0}，其中 $d_1|d_2|\cdots|d_r$ 不为零，除相差 R 中可逆元外，$d_1,\cdots,d_r$ 由 A 唯一确定，它们称做 A 的不变因子。
设 M 是主理想整区上 m 秩自由模，N 是它的一个子模，则存在 M 的一组基 $e_1,\cdots,e_m$，及满足 $d_1|d_2|\cdots|d_r$ 的 r 个非零数使得 $d_1e_1,\cdots,d_re_r$ 是 N 的一组基。
有限生成模的基本结构定理：设 M 是主理想整区上的有限生成模，则 M 可以写生循环模的直和 $Rz_1\oplus Rz_2\oplus\cdots\oplus Rz_s$，这里 $ann(z_1)\supset ann(z_2)\supset\cdots\supset ann(z_s)$。若令 $ann(z_i)=(d_i)$，则 d_i 满足 $d_1|d_2|\cdots|d_r$，$d_{r+1}=\cdots=d_s=0$。