抽象代数 II　　讲义①　　授课时间：2019年9月5日

第一节　群，环，域知识回顾

$\boxed{\S 1.1}$　等价关系，商集与自然映射

(equivalence relations, quotient sets and natural maps)

设 S 为非空集合．我们称笛卡尔积 $\underbrace{S\times S\times\cdots\times S}_{n}$ 的任一子集 R 为 S 上的一个 <u>n元关系</u>．如果 $(x_1,\cdots,x_n)\in R$，则称 $x_1,\cdots,x_n$ 满足关系 R．特别地，对于 $n=2$，如果 $(x_1,x_2)\in R$，则记为 $\underline{x_1Rx_2}$

定义1.（等价关系）集合 S 上二元关系 R 称为 <u>等价关系</u> 如果以下三条性质成立：

1) 反身性：$\forall a\in S$，aRa
2) 对称性：$\forall a,b\in S$，$aRb\Rightarrow bRa$
3) 传递性：$\forall a,b,c\in S$，$aRb,\ bRc\Rightarrow aRc$

（常用 $\sim$ 来记等价关系）

设 $\{S_\lambda\}_{\lambda\in I}$ 为 S 的一个子集族．若 $\bigcup\limits_{\lambda\in I}S_\lambda=S$ 且 $S_\lambda\cap S_\mu=\emptyset$ $(\lambda\neq\mu)$

则称 $\{S_\lambda\}_{\lambda\in I}$ 为 S 的一个 <u>划分</u>．我们有如下对应：

$$\{S\text{上的所有划分}\}\xleftrightarrow{1-1}\{S\text{上的所有等价关系}\}$$

从 S 上的一个划分 $\{S_\lambda\}_{\lambda\in I}$，可以定义等价关系：对 $a,b\in S$

$$a\sim b\ \underset{\text{(定义为)}}{\triangleq}\ a,b\in S_\lambda \text{ for some } \lambda\in I$$

可以验证上定义的关系为 <u>等价关系</u>．从 S 上的一个等价关系 $\sim$，可以定义等价类：$\bar{a}=\{b\in S\mid a\sim b\}$．可以验证任意两个等价类 $\bar{a},\bar{b}$，要么 $\bar{a}=\bar{b}$，要么 $\bar{a}\cap\bar{b}=\emptyset$．则 S 关于 $\sim$ 的互不相同等价类构成 S 的一个划分．等价类全体称为 S 关于等价关系 $\sim$ 的 <u>商集</u>，记为 $S/\sim$．

从集合 S 到商集 $S/\sim$ 可定义映射：$\pi: S \to S/\sim$
$$a \mapsto \bar{a}$$
该映射称为 S 关于 $\sim$ 的<u>自然映射</u>. 该映射为满射，且 $\pi(a)=\pi(b) \Leftrightarrow a\sim b$.

等价关系的例子：

1) 整数集合 $\mathbb{Z}$ 上的同余关系（数论）

给定 $m\in\mathbb{Z}\setminus\{0\}$，称 $a,b\in\mathbb{Z}$ 关于 m <u>同余</u> 如果 $m \mid a-b$

该关系为等价关系，称为 $\mathbb{Z}$ 上关于 m 的同余关系，记为 $\equiv_m$. 对 $a\in\mathbb{Z}$，等价类 $\bar{a}=\{b\in\mathbb{Z} \mid b\equiv_m a\}$ 称为一个剩余类. 则 $\mathbb{Z}$ 关于 $\equiv_m$ 的商集为

$$\mathbb{Z}/_{\equiv_m} = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}$$

通常剩余类全体记为 $\mathbb{Z}/m\mathbb{Z}$. 自然映射：$\pi: \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ 即为 $\pi(a)=\bar{r}$，其中 $a=q\cdot m+r$；$0\le r\le m-1$.

2) 映射的<u>"自然"分解</u>

设 $f: A\to B$ 为 A 到 B 的映射. 定义等价关系：

$$a \sim_f b \triangleq f(a)=f(b)$$

则可验证 $\sim_f$ 确实为 A 上等价关系 且 $a\in A$ 的等价类为

$$\bar{a}=\{b\in A \mid f(b)=f(a)\}.$$

映射 f 可分解为 $f=\bar{f}\circ\pi$，其中 $\bar{f}(\bar{a})=f(a)$

$$\begin{tikzcd} A \arrow[r, "\pi"] \arrow[rr, bend right, "f"'] & A/_{\sim_f} \arrow[r, "\bar{f}"] & B \end{tikzcd}$$

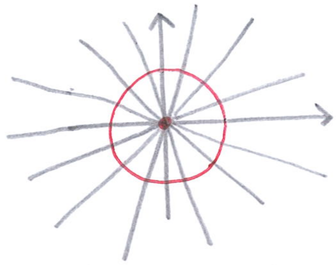
则 $\bar{f}$ 为单射.

3) 射影空间 (几何)

设 $\mathbb{R}^{d+1}$ 为 $\mathbb{R}$ 上 $(d+1)$ 维向量空间，设 $\vec{a}=(a_0,a_1,\cdots,a_d)$，
$\vec{b}=(b_0,b_1,\cdots,b_d)$. 定义等价关系:

$$\vec{a}\sim\vec{b} \ \triangleq\ \exists\,\lambda\in\mathbb{R}\setminus\{0\} \text{ 使得 } a_i=\lambda b_i \quad (i=0,1,\cdots,d)$$

商集 $\mathbb{R}^{d+1}/\sim$ 称为 $\mathbb{R}$ 上 d 维射影空间. 注意，零向量对应等价类为 $\{\vec{0}\}$. 当 $d=2$ 时，一维射影空间可看成"单位圆加原点":



$\boxed{\S 1.2}$ 偏序关系与佐恩引理 (partially ordered set and Zorn Lemma)

定义 2.（偏序关系）集合 S 上二元关系，记为 $\leq$，称为偏序关系 如果以下三条性质成立:

1) 反身性: $\forall a\in S$, $a\leq a$
2) 反对称性: $\forall a,b\in S$, $a\leq b$ 且 $b\leq a \Rightarrow a=b$
3) 传递性: $\forall a,b,c\in S$, $a\leq b$ 且 $b\leq c \Rightarrow a\leq c$

有序对 $(S,\leq)$ 称为一个偏序结构. 如果 S 上偏序关系 $\leq$ 满足: $\forall a,b\in S$，恒有 $a\leq b$ 或 $b\leq a$（即元素之间都可比较），则称 $\leq$ 为全序关系. 如果 S 的子集 A 关于 $\leq$ 构成一个全序集合，则称 A 为 S 的一个链 (chair).

定义2（极小，极大，上界，下界，最大，最小） 设 $(S,\le)$ 为偏序结构

① $a\in S$ 称为极小元素 如果不存在 $x\in S$ 使得 $x\le a$ 且 $x\ne a$（简记为 $x<a$）；a 称为极大元素 如果不存在 $x\in S$ 使得 $a\le x$ 且 $a\ne x$（简记为 $a<x$）

② 设 A 为 S 的子集，$a\in S$ 称为 A 的上界 如果 $\forall x\in A$ 都有 $x\le a$。$a\in S$ 称为 A 的下界 如果 $\forall x\in A$ 都有 $a\le x$。如果 $a\in S$ 为 A 的上界且 $a\in A$ 则称 a 为 A 的最大元素，如果 a 为 A 的下界且 $a\in A$ 则称 a 为 A 的最小元素。

注 1. 偏序结构 $(S,\le)$ 的极大，极小元素可能不存在，如 $(\mathbb{R},\le)$ 也可能存在但不唯一，如所有12的真因子关于整除关系构成的偏序结构：$(\{1,2,3,4,6\},\ |\ )$，4与6皆为极大元素 1为 S 的最小元素

2. 最大，最小元素当存在时必是唯一的，对同一个集合 S 上的两个不同的偏序关系 $\le_1$ 与 $\le_2$，关于 $\le_1$ 的最小元素可能成为 $\le_1$ 的最大元素；如 $S=\mathbb{N}$，关于普通大小关系，0为最小元素，但是关于整除关系，0为最大元素

3. (习题) 有限偏序结构 $(S,\le)$ 中极大元素与极小元素必存在。

偏序结构的例子：

1) 自然数集合 $\mathbb{N}$ 上的整除关系

对 $a,b\in\mathbb{N}$，定义 $a\le b \triangleq a\,|\,b$

$(\mathbb{N},\le)$ 不是全序关系，如 4，6 关于整除关系不能比较

0是最大元素，1是最小元素

2) 集合的所有子集全体关于包含关系

记 2^A 为集合 A 的所有子集构成的集合，称为 A 的幂集.

对 $A_1, A_2 \in 2^A$，$\quad A_1 \leq A_2 \triangleq A_1 \subseteq A_2$

则 $(2^A, \leq)$ 为偏序结构. ϕ 为 2^A 关于 $\leq$ 的最小元素. A 为最大元素. 但是 $(2^A, \leq)$ 不是全序结构 除非 $A=\phi$ 或 A 只含有一个元素.

3). 集合划分的加细 (组合)

设 A 为含有 n 个元素的集合. $\pi(A)$ 为 A 的所有划分构成的集合. 两个划分 $\pi_1 = \bigcup\limits_{\lambda\in I} A_\lambda$，$\pi_2 = \bigcup\limits_{\mu\in J} A_\mu$. 定义

$$\pi_1 \leq \pi_2 \quad \triangleq \quad \forall \lambda\in I,\ \text{存在}\ \mu\in J\ \text{使得}\ A_\lambda \subseteq A_J$$

则 $(\pi(A), \leq)$ 构成偏序结构. 例如: $A=\{a_1, a_2, a_3\}$

$\pi_1 = \{a_1\} \cup \{a_2\} \cup \{a_3\}$，$\pi_2 = \{a_1, a_2\} \cup \{a_3\}$

$\pi_3 = \{a_1, a_3\} \cup \{a_2\}$，$\pi_4 = \{a_1, a_2, a_3\}$

则有 $\quad \pi_1 \leq \pi_2 \leq \pi_4$，但是 π_2 与 π_3 不可比较

当 $\pi_1 \leq \pi_2$，我们称 π_1 为 π_2 的加细.

佐恩引理 若非空偏序集 S 的每个链(全序子集)都有上界，则 S 必有极大元素.

应用例子: 1) 域上任意线性空间必存在一组基 (……)

2) 任一非平凡含幺环都存在极大理想

3) 任意域的代数闭包的存在性与同构意义下的唯一性.

§1.3 群 (group)

设A为非空集合. 我们称笛卡尔积 $\underbrace{A\times A\times\cdots\times A}_{n}$ 到 A的任一映射 f 为 A上的一个 n元代数运算. 设 Ω 为 A上若干n元代数运算构成的集合, 则称 (A,Ω) 为 A上关于运算集 Ω 构成的代数结构(代数系统).

定义 (群) 设 $*$ 为集合G上一个二元代数运算. 称 $(G,*)$ 为群 如以下条件满足:

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

2) 单位元: $\exists e\in G$ 使得 $\forall a\in G$, $a*e=e*a=a$.

3) 逆元: $\forall a\in G, \exists b\in G$ 使得 $a*b=b*a=e$

b称为a的逆元, 记为 a^{-1}

集合G元素个数 $|G|$ 称为G的阶数(order). 若 $|G|<+\infty$, 则称G为有限群. 若 $|G|$ 为无穷, 则称G为无限群. 如果 $\forall a,b\in G$, $a*b=b*a$ 则称G为阿贝尔群 (交换群). 对 $a\in G$, 记 $a^n=\underbrace{a*a*\cdots*a}_{n}$ 若 $a^n=e$, 则称n为a的阶数. G的子集H称为G的子群若满足: $\forall a,b\in H$, $a^{-1}b\in H$.

性质: 设 $\{H_\lambda\}_{\lambda\in I}$ 为G的一族子群. 则 $\bigcap_{\lambda\in I}H_\lambda$ 仍为G的子群.

注 两子群 H_1,H_2 的并不一定为G的子群.

设S为G的子集, 称包含S的所有子群的交为由S生成的子群, 记为 $\langle S\rangle$. 实际上 $\langle S\rangle=\{a_1a_2\cdots a_n \mid a_i\in S\cup S^{-1}\}$, 其中 $S^{-1}=\{a^{-1}\mid a\in S\}$. G的子群H称为循环子群若存在 $h\in H$ 使得 $H=\langle h\rangle$. 若G本身由一个元素生成, 则称G为循环群.

群的例子：

① 集合的全变换群

设 A 为非空集合. $S(A)=\{\phi: A\to A \mid \phi$ 为双射$\}$ 关于映射的复合构成一个群，称为 A 的全变换群. 当 $|A|=n$ 时，$S(A)$ 的阶数为 $n!$，称为 n 元对称群，记为 S_n. S_n 中元素称为 n 元置换. S_n 的任一子群称为 A 的一个置换群. $\forall\ \sigma\in S_n$，可以表示为

$$\sigma=\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_n \end{pmatrix} \qquad \begin{array}{l} \alpha_i\in\{1,2,\cdots,n\} \\ \alpha_i\neq\alpha_j\quad (i\neq j) \end{array}$$

定理（置换的基本性质）

1) 任何一个置换 $\sigma\in S_n$ 可以写成若干对换：$\begin{array}{l}\sigma(\alpha_1)=\alpha_2 \\ \sigma(\alpha_2)=\alpha_1\end{array}$；$\begin{array}{l}\sigma(\alpha_i)=\alpha_i \\ (i\neq 1,2)\end{array}$ 的乘积，且表示中对换个数的奇偶性不变.
设 m 为 σ 写成对换的个数. 称 $(-1)^m$ 为 σ 的签名（Signature），记为 $\mathrm{sign}(\sigma)$. 若 $\mathrm{sign}(\sigma)=1$，则称 σ 为偶置换，若 $\mathrm{sign}(\sigma)=-1$，则称 σ 为奇置换.

2) 所有 S_n 的偶置换全体关于置换乘积构成 S_n 的子群，称为 S_n 的交错子群，记为 A_n，且有 $|A_n|=\frac{1}{2}n!$

3) 任一置换可以分解为若干互不相交轮换 $(\alpha_1\alpha_2\cdots\alpha_m)$ 的乘积.
例如 $\sigma=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 3 & 2 & 1 & 4 \end{pmatrix}=(16425)(13)$

② 由数构成的群

$(\mathbb{Z},+)$ 加法群. $(\mathbb{Q},+)$，$(\mathbb{R},+)$，$(\mathbb{C},+)$

设 $\mathbb{Q}_>=\{a\in\mathbb{Q}\mid a>0\}$. $\mathbb{Q}_>$ 对乘法构成群.

3) 矩阵构成的群

设 $M_n(\mathbb{R})$ 为所有 $n\times n$ 矩阵全体，$GL_n(\mathbb{R}) \subseteq M_n(\mathbb{R})$ 为所有可逆矩阵全体，则 $(M_n(\mathbb{R}), +)$ 构成群且为交换的. $(GL_n(\mathbb{R}), \cdot)$ 关于矩阵乘法构成群，称为一般线性群.

定义（同态，同构） 设 $\phi: G_1 \to G_2$ 为群 $(G_1, *_1)$ 到 $(G_2, *_2)$ 的映射，若满足条件：$\forall a, b \in G_1$，$\phi(a *_1 b) = \phi(a) *_2 \phi(b)$. 则称 ϕ 为 G_1 到 G_2 的同态. 若 ϕ 为双射，则称为 G_1 到 G_2 同构

注 $\phi(e_1) = e_2$，其中 e_1, e_2 分别为 G_1, G_2 的单位元

证明 $\phi(e_1) = \phi(e_1 *_1 e_2) = \phi(e_1) *_2 \phi(e_1) = \phi(e_1)^2$

因为 $\phi(e_1)$ 可逆，则有 $\phi(e_1) *_2 \phi(e_1) = e_2 = \phi(e_1)$

$\phi(a^{-1}) = \phi(a)^{-1}$，即群同态将单位元映为单位元，逆元映为逆元

习题：$(Q, +)$ 与 $(Q_>, \cdot)$ 不同构.

定理（凯莱） 任何一个群都同构于某个集合的变换群（全变换群的子群）

定理（拉格朗日） 设 G 为有限群，H 为 G 的子群，则 $|H|$ 是 $|G|$ 的因子.

注 阶数为 10 的有限群不可能有 7 阶子群. 素数阶有限群只有平凡子群.

设 H 为 G 的子群. 对 $a \in G$，集合 $aH = \{a*h \mid h \in H\}$ 与集合 $Ha = \{h*a \mid h \in H\}$ 分别称为 H 的左陪集与右陪集. 一般而言 $aH \neq Ha$.

定义（正规子群） 设 H 为 G 的子群. 若对 $\forall g\in G$ 都有 $gH=Hg$，则称 H 为 G 的一个正规子群 (normal subgroup)，记为 $H\trianglelefteq G$

注 1) 正规子群的另一个等价刻画为：任意两个左(右)陪集之积还是左(右)陪集。

2) 在交换群中，每个子群都是正规的。

3) 若 H 为 G 的正规子群. 则 H 的所有左陪集全体关于如下运算： $g_1H * g_2H = (g_1 * g_2)H$

形成一个群，称为 G 关于 H 的商群，记为 G/H.

设 $\phi: G\to \bar{G}$ 为同态，称 $\mathrm{Ker}(\phi)=\{g\in G \mid \phi(g)=\bar{e}\}$ 为同态 ϕ 的核，可以证明 $\mathrm{Ker}(\phi)$ 为 G 的正规子群. 另一方面，任给 G 的正规子群 $H\trianglelefteq G$，映射 $\pi: G\to G/H$ 为群同态且为满同态. $\mathrm{Ker}(\pi)=H$. 所以正规子群全体与 G 到另一个群(不一定为 G 本身)的同态全体具有对应关系.

定理（群同态基本定理） 设 $\phi: G\to \bar{G}$ 为满群同态，则 $G/\mathrm{ker}(\phi)$ 与 $\bar{G}$ 同构.

群同态定理：① 设 $H\trianglelefteq G$. 令 $\pi: G\to G/H$ 为自然同态 则 π 建立了 G 中所有包含 H 的子群（正规子群）与 G/H 中子群（正规子群）的 1-1 对应. 如果 $N\trianglelefteq G$ 且 $N\supseteq H$，则有 $G/N \cong (G/H)/(N/H)$.

② 设 $H\leq G$，$N\trianglelefteq G$，则有 $HN/N \cong H/H\cap N$.

例子 1) 设 S_n 为 n元对称群，映射 $\phi: S_n \to \{\pm 1\}$

$\sigma \mapsto \text{sign}(\sigma)$

为 S_n 到群 $(\{\pm 1\}, \cdot)$ 的同态

且 $\ker(\phi) = A_n$，即 A_n 为 S_n 的正规子群

2) 设 $GL_n(\mathbb{R})$ 为 n阶一般线性群，映射

$$\phi: GL_n(\mathbb{R}) \to \mathbb{R}$$
$$A \mapsto |A| \quad (\text{取行列式})$$

由于 $|A \cdot B| = |A| \cdot |B|$，$\phi$为同态，则 $\ker(\phi)$ 为 $GL_n(\mathbb{R})$ 行列式等于1的矩阵全体，记为 $SL_n(\mathbb{R})$，称为特殊线性群。

则有 $SL_n(\mathbb{R}) \trianglelefteq GL_n(\mathbb{R})$.

注 对于任一群 G，$\{e\} \trianglelefteq G$ 构成 G 的正规子群，称为 G 的平凡正规子群

定义（单群） 如果群 G 没有非平凡的正规子群，那么 G 称为一个单群.

注 1) 素数阶的群一定是单群

2) 交错群 A_n $(n \geq 5)$ 为单群

3) 如果 G为交换群且 $G \neq \{e\}$，则

G为单群 $\Leftrightarrow$ G为素数阶的循环群.