目录

1 分析学复习题

1 有度量空间 $(X_1,d_1),\cdots,(X_n,d_n)$, 在 $X=\prod_{i=1}^{n}X_i$ 上定义度量 $\rho_1,\rho_2:\forall x=(x_1,\cdots,x_n),y=(y_1,\cdots,y_n)\in X$,

$$\rho_1(x,y)=\sqrt{\sum_{i=1}^{n}d_i(x_i,y_i)^2},\rho_2(x,y)=\sum_{i=1}^{n}d_i(x_i,y_i)$$

证明 ρ_1,ρ_2 诱导的度量拓扑相同.

证明. 仅需证明度量等价, 注意到

$$\rho_1(x,y)=\frac{1}{\sqrt{n}}\sqrt{\left(\sum_{i=1}^{n}d_i(x_i,y_i)^2\right)\left(\sum_{i=1}^{n}1^2\right)}\geq\frac{1}{\sqrt{n}}\sum_{i=1}^{n}d_i(x_i,y_i)=\frac{\rho_2(x,y)}{\sqrt{n}}$$

以及由 $d_i(x_i,y_i)\leq\rho_2(x,y)$ 知 $\rho_1(x,y)\leq\sqrt{n}\rho_2(x,y)$, 故得证. □

2 度量空间 $(X,\rho),x\in X,\varnothing\neq A\subset X$, 证明 $(1)f=\rho(\cdot,A)$ 一致连续.$(2)\overline{A}=\{x\in X|\rho(x,A)=0\}$.

证明. (1) 由 inf 性质知 $\forall x_1,x_2\in X\forall a\in A,\rho(x_1,A)\leq\rho(x_1,a)\leq\rho(x_1,x_2)+\rho(x_2,a)$, 从而 $\rho(x_1,A)-\rho(x_2,a)\leq\rho(x_1,x_2)$, 两端取 $\inf\limits_{a\in A}$ 即得 $\rho(x_1,A)-\rho(x_2,A)\leq\rho(x_1,x_2)$. 由 x_1,x_2 任意知 $|f(x_1)-f(x_2)|\leq\rho(x_1,x_2)$, 故 f Lipschitz 连续, 从而一致连续.

(2)$\forall x\in\overline{A}\forall\varepsilon>0\exists y\in A,\rho(x,y)<\varepsilon$, 故取 inf 即可. 另一方面, 可以取收敛列来写 (取 $\varepsilon=1/n$ 可取到 $a_n\in A$ 趋于 $a\in\overline{A}$), 也可以注意到 $A\subset\{x\in X|\rho(x,A)=0\}=f^{-1}(0)$, 而后者是闭集, 故 $\overline{A}\subset\{x\in X|\rho(x,A)=0\}$. □

3 度量空间 (X,ρ) 完备 $\Longleftrightarrow$ 任意 X 中点列 $\{x_n\}_{n=1}^{\infty}$, 若有 $\forall n\geq1,\rho(x_n,x_{n+1})\leq2^{-n}$ 则点列收敛.

证明. $\Longrightarrow$: 注意到 $\rho(x_m,x_n)\leq2^{1-m}(m\leq n)$ 故 $\{x_n\}_{n=1}^{\infty}$ 是 Cauchy 列, 由完备知收敛.

$\Longleftarrow$: 任取 X 中 Cauchy 列 $\{y_n\}_{n=1}^{\infty}$, 对于 $\forall k\in\mathbb{N}$ 取 $\varepsilon_k=2^{-k}\exists N_k>N_{k-1}\forall m,n\geq N_k,\rho(y_m,y_n)<2^{-k}$, 从而可取子列 $\{y_{N_i}\}_{i=1}^{\infty}$, 由题设知收敛, 而 Cauchy 列有收敛子列即自身收敛, 故得证. □

4 完备度量空间 (X,ρ) 上有 $T:X\to X,\exists N\in\mathbb{N}^*\exists\alpha\in(0,1),\rho(T^Nx,T^Ny)\le\alpha\rho(x,y)\forall x,y\in X$, 其中 $T^N=\underbrace{T\circ T\circ\cdots\circ T}_{N次}$, 证明 T 有唯一不动点.

证明. 由不动点定理知 T^N 有唯一不动点 x_0, 而 $T^NTx_0=T^{N+1}x_0=TT^Nx_0=Tx_0$, 故 Tx_0 也为 T^N 不动点,$Tx_0=x_0$, 故 x_0 是 T 不动点. 若 T 有其他不动点 x' 则 T^N 也有不动点 x', 与唯一矛盾, 从而 T 有唯一不动点. □

5 度量空间 (X,ρ) 内有开集 U 和非空紧集 $A\subset U$, 证明 $\exists\delta>0\forall x\in A,B(x,\delta)\subset U$.

证明. 由 U 开知 $\forall x\in A\exists\delta_x>0,B(x,\delta_x)\subset U$, 从而 $\left\{B\left(x,\frac{\delta_x}{2}\right)\right\}_{x\in A}$ 是 A 的开覆盖, 其中有有限子覆盖 $\left\{B\left(x_i,\frac{\delta_i}{2}\right)\right\}_{i=1}^n$, 取 $\delta=\min\limits_{1\le i\le n}\frac{\delta_i}{2}$, 从而 $\forall x\in A\forall y\in B(x,\delta)\exists x_i,\rho(y,x_i)\le\rho(y,x)+\rho(x,x_i)<\delta+\frac{\delta_i}{2}\le\delta_i$, 故 $y\in B(x_i,\delta_i)\subset U$. □

6 实线性赋范空间 X 上有线性泛函 $f:X\to\mathbb{R}$, 证明 f 连续 $\iff N(f)=\{x\in X|f(x)=0\}$ 是闭集.

证明. $\Longrightarrow$: 由于 $\{0\}$ 是闭集且 f 连续, 故 $N(f)=f^{-1}(\{0\})$ 是闭集.

$\Longleftarrow$: 若 f 不连续, 则由线性泛函连续的等价条件知,$\forall M>0\exists x\in X,|f(x)|>M\|x\|$, 从而可取点列 $x_n\in X-\{0\},|f(x_n)|>n\|x_n\|$, 取点列 $y_n=\frac{x_n}{f(x_n)}-\frac{x_1}{f(x_1)},f(y_n)\equiv0$, 从而 $y_n\in N(f)$. 但 $\left\|y_n+\frac{x_1}{f(x_1)}\right\|=\frac{\|x_n\|}{|f(x_n)|}<\frac{1}{n}\to0(n\to\infty),y_n\to-\frac{x_1}{f(x_1)}\notin N(f)$. 这与 $N(f)$ 闭矛盾, 因此 f 连续. □

7 域 $\mathbb{K}$ 上线性赋范空间 $(X,\|\cdot\|)$ 中有有限维真线性子空间 $M\subsetneq X$. 证明 $\exists y\in X,\|y\|=1$ 且 $\forall x\in M,\|y-x\|\ge1$.

证明. 任取 $y_0\in X$, 令 $d=d(y_0,M)$, 由 inf 性质可取 $\forall n\ge1\exists x_n\in M,d\le\|y_0-x_n\|\le d+\frac{1}{n},\|x_n\|\le\|x_n-y_0\|+\|y_0\|\le\|y_0\|+d+1$, 故 $\{x_n\}$ 是 M 中有界序列, 由 M 有限维知 $\overline{B_M}(0,\|y_0\|+d+1)$ 是紧集, 从而其中点列 $\{x_n\}$ 有收敛子列 $\{x_{n_k}\}$ 收敛于 x_0, 从而 $d\le\|y_0-x_0\|=\lim\limits_{k\to\infty}\|y_0-x_{n_k}\|\le d,\|y_0-x_0\|=d$, 故可取 $y=\frac{y_0-x_0}{\|y_0-x_0\|},\|y\|=1$, 从而 $\forall x\in M,\|y-x\|=\left\|\frac{y_0-x_0}{d}-x\right\|=\frac{\|y_0-(x_0+dx)\|}{d}\ge\frac{d}{d}=1$, 从而得证. □

8 在 $X=C^1([0,1],\mathbb{R})$ 上定义范数 $\|f\|_{C^1}=\max\{\|f\|_\infty,\|f'\|_\infty\}$, 证明 $(X,\|\cdot\|_{C^1})$ 构成实 Banach 空间.

证明. 取 X 中的 Cauchy 列 $\{f_n\}_{n=1}^\infty$, 即 $\forall\varepsilon>0\exists N\in\mathbb{N}\forall m,n\ge N,\|f_m-f_n\|_{C^1}<\varepsilon$, 而由 $\|f\|_\infty\le\|f\|_{C^1},\|f'\|_\infty\le\|f\|_{C^1}$ 知,f_n,f_n' 在 $(C[0,1],\|\cdot\|_\infty)$ 中是 Cauchy 列, 而 $[0,1]$ 紧从而该空间完备, Cauchy 列收敛, 而函数列在范数 $\|\cdot\|_\infty$ 下收敛等价于一致收敛. 记 $f_n\to f,f_n'\to g$, 则有

$$f(x)=\lim_{n\to\infty}f_n(x)=\lim_{n\to\infty}\left(f_n'(0)+\int_0^x f_n'(t)\mathrm{d}t\right)=g(0)+\int_0^x\lim_{n\to\infty}f_n'(t)\mathrm{d}t=g(0)+\int_0^x g(t)\mathrm{d}t$$

从而 $f'=g,\|f_n-f\|_{C^1}=\max\{\|f_n-f\|_\infty,\|f_n'-g\|_\infty\}\to0,\{f_n\}_{n=1}^\infty$ 收敛, 故 X 是 Banach 空间. □

9 域 $\mathbb{K}$ 上线性赋范空间 $(X,\|\cdot\|)$ 中有以 θ 为内点的真凸子集 E, 其产生 Minkowski 泛函 P.
证明 $(1)E^\circ=\{x\in X|P(x)<1\}.(2)\overline{E^\circ}=\overline{E}$.

证明. $(1)\subset$: $\forall x\in E^\circ\exists\delta>0,B(x,\delta)\subset E$, 故由 $\left\|\left(1+\frac{\delta}{2\|x\|}\right)x-x\right\|=\frac{\delta}{2}<\delta$ 知 $\left(1+\frac{\delta}{2\|x\|}\right)x\in B(x,\delta)\subset E$, 从而 $P(x)\le\left(1+\frac{\delta}{2\|x\|}\right)^{-1}<1$. $\supset$: 若 $P(x)<1$ 则有 $\lambda\in[P(x),1),x/\lambda\in E$. 由 0 是 E 内点知 $\exists\delta>0,B(0,\delta)\subset E$, 故 $\forall y\in B(0,\delta),\lambda\cdot(x/\lambda)+(1-\lambda)y=x+(1-\lambda)y\in E$, 即 $B(x,(1-\lambda)\delta)\subset E,x\in E^\circ$.

(2) 由 $E^\circ\subset E$ 知 $\overline{E^\circ}\subset\overline{E}$, 仅需证 $E\subset\overline{E^\circ}$. 由 0 是内点知 $\exists\delta>0,B(0,\delta)\subset E$, 故 $\forall x\in E\forall y\in B(0,\delta)\forall\lambda\in[0,1),\lambda x+(1-\lambda)y\in E$, 故 $B(\lambda x,(1-\lambda)\delta)\subset E,\lambda x\in E^\circ,x=\lim\limits_{\lambda\to1^-}\lambda x\in\overline{E^\circ}$. □

10 $\mathbb{R}^n$ 内 Lebesgue 可测子集 $\Omega, m(\Omega)<\infty, 1\le p_1<p_2<\infty$, 证明 $L^{p_2}(\Omega)\subset L^{p_1}(\Omega)$ 且

$$\|f\|_{p_1}\le [m(\Omega)]^{\frac{1}{p_1}-\frac{1}{p_2}}\|f\|_{p_2}, \forall f\in L^{p_2}(\Omega).$$

证明. 由 Hölder 不等式知

$$\begin{aligned}\forall f\in L^{p_2}(\Omega), \|f\|_{p_1}=\|f\cdot 1\|_{p_1}&\le \|f\|_{p_2}\|1\|_r \qquad \text{其中}\frac{1}{r}=\frac{1}{p_1}-\frac{1}{p_2}\\ &=\|f\|_{p_2}\left(\int_\Omega 1^r \mathrm{d}m\right)^{1/r}=\|f\|_{p_2} m(\Omega)^{\frac{1}{p_1}-\frac{1}{p_2}}\end{aligned}$$

从而不等式得证, 且右端有限, 故左端有限, 即 $f\in L^{p_1}(\Omega), L^{p_2}(\Omega)\subset L^{p_1}(\Omega)$. □

11 域 $\mathbb{K}$ 上的 Hilbert 空间 H 中有可数规范正交集合 $\{e_n\}_{n=1}^\infty$, 证明 Bessel 不等式 $\sum\limits_{n=1}^\infty |\langle x,e_n\rangle|^2\le \|x\|^2, \forall x\in H$.

证明. 从 $\{e_n\}_{n=1}^\infty$ 中取有限集 $\{e_i\}_{i\in I}$, 则有

$$\begin{aligned}0\le\left\|x-\sum_{i\in I}\langle x,e_i\rangle e_i\right\|^2&=\left\langle x-\sum_{i\in I}\langle x,e_i\rangle e_i, x-\sum_{i\in I}\langle x,e_i\rangle e_i\right\rangle=\|x\|^2-2\sum_{i\in I}|\langle x,e_i\rangle|^2+\sum_{i,j\in I}\langle x,e_i\rangle\langle e_j,x\rangle\langle e_i,e_j\rangle\\ &=\|x\|^2-2\sum_{i\in I}|\langle x,e_i\rangle|^2+\sum_{i\in I}|\langle x,e_i\rangle|^2=\|x\|^2-\sum_{i\in I}|\langle x,e_i\rangle|^2\end{aligned}$$

从而 $\|x\|^2\ge\sum\limits_{i\in I}|\langle x,e_i\rangle|^2$, 因此 $\sum\limits_{n=1}^\infty|\langle x,e_n\rangle|^2$ 收敛且仍有 $\sum\limits_{n=1}^\infty|\langle x,e_n\rangle|^2\le\|x\|^2$. □

12 非零实线性赋范空间 X 中有点列 $\{x_n\}_{n=1}^\infty, x_0\in X-\{\theta\}$.(1) 证明 $\exists f\in X^*, f(x_0)=\|x_0\|, \|f\|=1$.(2) 若 $\{x_n\}_{n=1}^\infty$ 在 X^* 中弱收敛, 证明其弱极限唯一.

证明. (1) 取 X 的线性子空间 $X_0=\mathrm{span}(x_0)$, 定义线性泛函 $f_0: X_0\to\mathbb{R}, \lambda x_0\mapsto\lambda\|x_0\|$, 则 $f_0(x_0)=\|x_0\|, \|f_0\|=\sup\limits_{\lambda\ne0}\dfrac{|\lambda\|x_0\||}{\|\lambda x_0\|}=1$, 从而由 Hahn-Banach 定理知 $\exists f\in X^*, f|_{X_0}=f_0, f(x_0)=f_0(x_0)=\|x_0\|, \|f\|=\|f_0\|=1$.

(2) 若 $x_n\overset{w}{\to}y_1$ 且 $x_n\overset{w}{\to}y_2$, 则 $\forall f\in X^*, f(y_1)=\lim\limits_{n\to\infty}f(x_n)=f(y_2), f(y_1-y_2)=0$. 若 $y_1-y_2\ne0$, 则 $\exists f\in X^*, f(y_1-y_2)=\|y_1-y_2\|=0$, 矛盾, 故 $y_1=y_2$. □

13 Hilbert 空间 H 中有非零闭线性子空间 $Y, P: H\to Y$ 是正交投影算子. 证明 $(1)Y^{\perp\perp}=Y$.$(2)\|P\|=1$.

证明. (1) 一方面 $y\in Y, y\perp Y^\perp$, 故 $y\in Y^{\perp\perp}, Y\subset Y^{\perp\perp}$. 另一方面考虑 Y 上的正交分解 $X=Y\oplus Y^\perp$, 则 $\forall x\in Y^{\perp\perp}, x=Px+Qx, Px\in Y\subset Y^{\perp\perp}, Qx\in Y^\perp$. 而 $Qx=x-Px\in Y^{\perp\perp}$, 从而 $Qx=0, x=Px\in Y, Y^{\perp\perp}\subset Y$.

(2) 由 $\forall y\in Y-\{\theta\}, Py=y$ 知 $\|P\|\ge\dfrac{\|Py\|}{\|y\|}=1$, 另一方面 $\|P\|=\sup\limits_{x\ne0}\dfrac{\|Px\|}{\|x\|}=\sup\limits_{x\ne0}\dfrac{\|Px\|}{\sqrt{\|Px\|^2+\|x-Px\|^2}}\le1$, 从而 $\|P\|=1$. □

14 X, Y 分别是域 $\mathbb{K}$ 上的 Banach 空间和线性赋范空间,$T\in\mathcal{L}(X,Y)$. 若 $\exists M>0\forall x\in X, \|Tx\|\ge M\|x\|$. 证明 $R(T)=\{Tx|x\in X\}$ 是 Y 的闭线性子空间.

证明. 取 $\forall x\in\ker T, 0=\|Tx\|\ge M\|x\|$ 知 $x=0, T$ 是单射, 故 $T: X\to R(T)$ 是双射, 其有逆映射 $T^{-1}: R(T)\to X$, 其是线性映射, 且 $\forall y\in R(T)\exists! x\in X, Tx=y, \left\|T^{-1}\right\|=\sup\limits_{y\in R(T)-\{0\}}\dfrac{\|T^{-1}y\|}{\|y\|}=\sup\limits_{y\in R(T)-\{0\}}\dfrac{\|x\|}{\|Tx\|}\le M$, 故 T^{-1} 是连续线性映射, 从而 $R(T)=T(X)=(T^{-1})^{-1}(X)$ 是闭集, 显然 $R(T)$ 是线性子空间, 故得证. □

15 用闭图像定理证明 Banach 逆算子定理.

闭图像定理: 对于 Banach 空间 X, Y 之间的线性映射 $T \in \mathcal{L}(X, Y)$, T 连续 $\iff$ T 是闭线性算子, 即 $G(T) = \{(x, Tx) \in X \times Y | x \in X\}$ 是 $X \times Y$ 中闭集.

Banach 逆算子定理: Banach 空间 X, Y 之间的双射连续线性映射 $T : X \to Y$ 的逆映射 $T^{-1} : Y \to X$ 是连续线性映射.

证明. 考虑双射连续线性映射 $T : X \to Y$, 其逆映射 T^{-1} 同样是线性映射, 由闭图像定理知 T^{-1} 连续 $\iff$ $G(T^{-1}) = \left\{(y, T^{-1}y) \in Y \times X | y \in Y\right\}$ 是闭集. 考虑 $G(T^{-1})$ 中收敛列 $\left\{(y_n, T^{-1}y_n)\right\}_{n=1}^{\infty}, (y_n, T^{-1}y_n) \to (y_0, x_0) \in Y \times X$, 即 $y_n \to y_0, T^{-1}y_n \to x_0$, 由 T 连续知 $Tx_0 = T\left(\lim\limits_{n\to\infty} T^{-1}y_n\right) = \lim\limits_{n\to\infty} TT^{-1}y_n = y_0$, 故 $(y_0, x_0) = (y_0, T^{-1}y_0) \in G(T^{-1})$, 即 $G(T^{-1})$ 闭, 得证. □

真题 2 线性赋范空间 X 中有紧集 A 与闭集 B, 证明 $A + B$ 是闭集.

真题 5 Ω 是 $\mathbb{R}^n$ 中 Lebesgue 可测集.(1) 任取 $1 \le p < q < \infty$, 证明 $L^{\infty}(\Omega) \cap L^p(\Omega) \subset L^q(\Omega)$.
(2) 若 $\dfrac{1}{p} + \dfrac{1}{q} = \dfrac{1}{r}, p, q, r \in [1, \infty)$, 证明 Hölder 不等式 $\|fg\|_r \le \|f\|_p \|g\|_q$.
(3) 若 $f \in \bigcap\limits_{1 \le p < \infty} L^p(\Omega)$ 且 $\exists C > 0 \forall p \in [1, \infty), \|f\| \le C$, 证明 $f \in L^{\infty}(\Omega)$.

2 群

2.1 群作用与 Sylow 定理

类数公式 群 G 作用在集合 S 上有 $|S| = |Z| + \sum_{a\in A}[G : G_a]$, 其中 $Z = \{x \in S|\forall g \in G, g \cdot x = x\}$ 是稳定点集合,G_a 是 a 的稳定子,A 是轨道非平凡元素. 考虑群 G 共轭作用于自身, 则有类公式 $|G| = |C(G)| + \sum_{a\in A}[G : C_G(a)]$.

关于 p-群的引理 若 G 是 p-群, 则由 $p|[G : G_a]||G|$ 知 $|Z| \equiv |S| \bmod p$, 对于共轭作用即 $|C(G)| \equiv 0 \bmod p$. 而 $e \in C(G), |C(G)| \geq 1$, 故 $|C(G)| \geq p$, 即 p-群中心非平凡.

若有限 G 有 p-子群 H, 则考虑 H 在左陪集 $G/_lH = \{gH|g \in G\}$ 上的左平移作用, 其稳定点

$$Z = \left\{gH|\forall h \in H, g^{-1}hg \in H\right\} = \{gH|g \in N_G(H)\} = N_G(H)/H$$

故 $[N_G(H) : H] = |Z| \equiv |G/_lH| = [G : H] \bmod p$. 从而若 $p|[G : H]$ 则 $p|[N_G(H) : H] \geq 1, N_G(H) \gneq H$.

Cauchy 定理 G 是有限群,$|G|$ 有素因子 p, 则 G 中总有 p 阶元.

证明 *(James McKay).* 考虑 $S = \{(a_1, \cdots, a_p)|a_i \in G, a_1 \cdots a_p = e\}$, 由 a_p 由前元素唯一决定, 故 $|S| = |G|^{p-1} \equiv 0 \bmod p$. 令 $\mathbb{Z}/p$ 循环作用于 S 上, 即 $m \cdot (a_1, \cdots, a_p) = (a_{m+1}, \cdots, a_p, a_1, \cdots, a_m) \in S$(容易验证 $ab = e$ 则 $ba = e$), 显然该作用的稳定点 $Z = \{(a, \cdots, a)|a \in G\}$, 且有 $|Z| \equiv |S| \equiv 0 \bmod p$, 而 $e \in Z, |Z| \geq 1$, 故有 $a \neq e, a^p = e$. □

Sylow 第一定理 G 为有限群, 则对 $|G|$ 的任意素因子 p, G 总含 Sylow p-子群.G 中的 Sylow p-子群 P 即 $P < G$ 为 p-群且 p 与 $[G : P]$ 互素, 即 G 中的极大 p-子群. 换言之,$|G| = p^r m, |P| = p^r, \gcd(p, m) = 1$.

定理的等价 (由 p-群性质) 描述为:G 为 $p^n m$ 阶群 (p 为素数且与 m 互素), 则对 $k \in [n]$ 总有 p^k 阶子群, 且该子群是某个 p^{k+1} 阶子群的正规子群.

证明. 首先由 Cauchy 定理,G 中总含 p 阶子群. 下对 k 归纳证明: 若 H 是 G 的 p^k 阶子群 ($k < n$), 则 $0 \equiv [G : H] \equiv [N_G(H) : H] \bmod p$, 后项非 0 故 $N_G(H) \neq H$, 且 $N_G(H)/H$ 也含 p 阶子群, 记为 H_1/H, 从而 $H \rhd H_1, |H_1| = |H|\,|H_1/H| = p^{k+1}$. □

Sylow 第二定理 P 是有限群 G 中的 Sylow p-子群,$H < G$ 是 p-子群, 则 H 在 P 的某个共轭中, 即 $H < gPg^{-1}$. 特别的,G 的 Sylow p-子群间互相共轭.

证明. 令 H 左乘作用于 $G/_LP$ 上, 作用不动点集的势 $|Z| \equiv [G : P] \not\equiv 0 \bmod p$, 故有作用不动点 $aP, a^{-1}ha \in P(\forall h \in H), H < aPa^{-1}$. □

Sylow 第三定理 G 为有限群,$|G| = p^n m$, 其中 p 为素数且与 m 互素, 则 G 中的 Sylow p-子群数量 $N_p|m$ 且 $N_p \equiv 1 \bmod p$.

证明. G 在 $\mathcal{P}(G)$ 上的共轭作用中, 任意 Sylow p-子群 P 所在的轨道即 G 中所有 Sylow p-子群构成的集合, 而 P 的稳定子为 $N_G(P)$. 故由轨道-稳定子定理知 G 中 Sylow p-子群的数量为 $N_p = [G : N_G(P)]|[G : P] = m$. 而 $m = [G : P] \equiv [N_G(P) : P] \bmod p$, 因此 $mN_p \equiv m \bmod p$, 故由 $m \perp p$ 得 $N_p \equiv 1 \bmod p$. □

2.2 可解群

G 为可解群: 存在有限长可解列 $G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{e\}$,G_i/G_{i+1} 为非平凡交换群, 其等价于存在循环列, 即 $G_i/G_{i+1} \cong \mathbb{Z}/p$. 从而所有 p-群均可解.

- 四面体群 $D_4 = \langle a, b|a^4 = b^2 = a^3bab = e\rangle$ 可解: 注意到 Klein 群 $K_4 \cong \mathbb{Z}/2 \oplus \mathbb{Z}/2 \cong \left\{e, a^2, b, a^2b\right\} \rhd D_4$, 从而有可解列 $D_4 \rhd K \rhd \{e\}$.
- 对称群 S_3 可解:$S_3 \rhd A_3 = \{(1), (123), (132)\} \rhd \{(1)\}$.

- 对称群 S_4 可解:$S_4 \rhd A_4 \rhd \{(1), (12)(34), (13)(24), (14)(23)\} \cong K_4 \rhd \{e\}$.[1]

3 环

3.1 素元与不可约元

- 素理想 $P \lneq R : ab \in P \implies a \in P \vee b \in P$(对理想也成立), 等价于 R/P 是整环.
- 极大理想 $M \lneq R$: 不存在含 M 的真理想, 等价于 R/M 是域.
- 极大理想都是素理想, PID 中极大理想 = 非零素理想.[2]
- $a|b \iff (a) \supset (b)$.
- p 是素元即 $p|ab \implies p|a \vee p|b$, 等价于 (p) 为素理想.
- m 为不可约元即 $m = ab \implies a = 1 \vee b = 1$, 等价于 (m) 为主理想中极大理想.
- 不可约元都是素元, UFD 中素元也是不可约元.

3.2 UFD, PID 和 Euclid 环

UFD 的等价条件 R 是 UFD $\iff$ R 中主理想满足升链条件, 且不可约元均为素元.

PID 是 UFD

3.3 中国剩余定理 (CRT)

4 模

4.1 图追踪法

4.2 有限生成交换群的结构

4.3 Jordan 标准型的存在性

5 域

5.1 尺规作图

5.2 有限域的结构与构造

[1] 由于 S_n 中轮换 $\sigma = (a_1, \cdots, a_k)$ 的共轭 $\tau\sigma\tau^{-1} = (a_1\tau^{-1}, \cdots, a_k\tau^{-1})$, 从而 S_n 中置换共轭等价于置换的类 type 相同. 而 S_4 中所有类为 $[2, 2]$ 的置换生成的群即为 K_4.

[2] (a) 是非零素理想, 若有 $(a) \subset (b)$ 则有 $a = bc.b \in (a)$ 则 $(b) = (a)$;$c \in (a)$ 则 $c = da, a = bda, bd = 1 \in (b) = R$.