本部分参考蓝以中《高等代数》，§3.4.

Laplace 展开：推广了按行列展开.

$M_A\begin{pmatrix} i_1 \cdots i_m \\ j_1 \cdots j_m \end{pmatrix}$ 为 A $i_1, \cdots, i_m$ 行，$j_1, \cdots, j_m$ 列构成的子式的行列式

设 A 为 n 阶矩阵，记 $\overline{M_A}\begin{pmatrix} i_1 \cdots i_m \\ j_1 \cdots j_m \end{pmatrix}$

为 A 去掉 $i_1, \cdots, i_m$ 行，$j_1, \cdots, j_m$ 列所剩方阵行列式

若我们考虑固定行指标 $i_1, \cdots, i_m$，

则记 $M_A(j_1 \cdots j_m)$ 为子式，$\overline{M_A}(j_1, \cdots, j_m)$

$$M_A(j_1 \cdots j_m) = M_A\begin{pmatrix} i_1 \cdots i_m \\ j_1 \cdots j_m \end{pmatrix} \qquad \overline{M_A}(j_1, \cdots, j_m) = \overline{M_A}\begin{pmatrix} i_1 \cdots i_m \\ j_1 \cdots j_m \end{pmatrix}$$

令 $W_A(j_1 \cdots j_m) = (-1)^{j_1 + \cdots + j_m} M_A(j_1 \cdots j_m) \cdot \overline{M_A}(j_1 \cdots j_m)$

后面将固定行指标 $i_1, \cdots, i_m$，并省略符号 A，$1 \leq m \leq n-1$.

Lemma 1：若 A 中方阵有 k, l 两列相同，给定自然数列

$$1 \leq j_1 < j_2 < \cdots < j_{m+1} \leq n$$

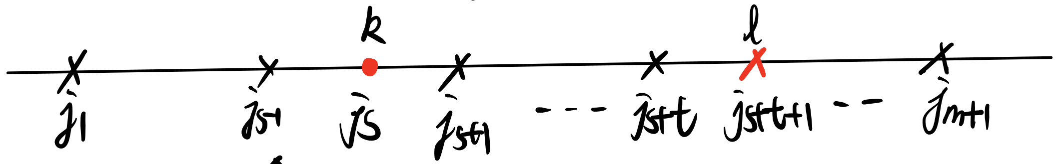
若 $j_s = k$，$j_{s+t+1} = l$. 则有

$$w(j_1 \cdots \hat{j_s} \cdots j_{s+t+1} \cdots j_{m+1}) + w(j_1 \cdots j_s \cdots \hat{j}_{s+t+1} \cdots j_{m+1}) = 0$$

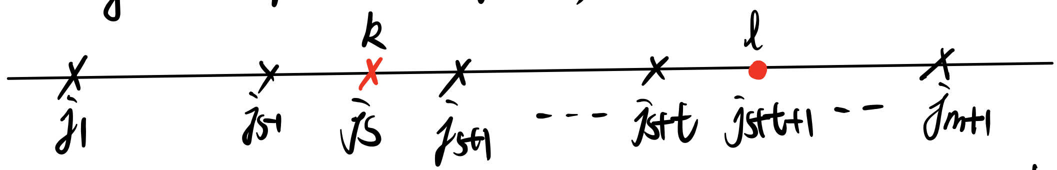
pf: ① 把 $M(j_1, \cdots \hat{j_s} \cdots j_{m+1})$ 中 j_{s+t+1} 列以交换相邻两列的方法向左平移 t 次有 $M(j_1 \cdots \hat{j_s} \cdots j_{m+1})$

$$= (-1)^t M(j_1 \cdots j_s \cdots \hat{j}_{s+t+1} \cdots j_{m+1})$$

② 用如下示意图表示 $\overline{M}(j_1\cdots\hat{j}_s\cdots j_{m+1})$ 中的列，



$\overline{M}(j_1\cdots\hat{j}_{s+t+1}\cdots j_{m+1})$



则只要把 $\overline{M}(j_1\cdots\hat{j}_s\cdots j_{m+1})$ 中标号为 $j_s=k$ 的列向右平移 $l-k-t+1$ 次，则有

$$\overline{M}(j_1\cdots\hat{j}_{s+t+1}\cdots j_{m+1})=(-1)^{l-k+1-t}\overline{M}(j_1\cdots\hat{j}_s\cdots j_{m+1})$$

令 $j=j_1+\cdots+j_{m+1}$.

则 $W(j_1\cdots\hat{j}_s\cdots j_{m+1})$

$$=(-1)^{j-j_s}M(j_1\cdots\hat{j}_s\cdots j_{m+1})\cdot\overline{M}(j_1\cdots\hat{j}_s\cdots j_{m+1})$$

$$=(-1)^{j-k}(-1)^{t}M(j_1\cdots\hat{j}_{s+t+1}\cdots j_{m+1})(-1)^{l-k-t+1}M(j_1\cdots\hat{j}_{s+t+1}\cdots j_{m+1})$$

$$=(-1)^{j+l+1}M(\cdots\hat{j}_{s+t+1}\cdots)\overline{M}(\cdots\hat{j}_{s+t+1}\cdots)$$

$$=(-1)^{j-j_{s+t+1}+1}M(\cdots\hat{j}_{s+t+1}\cdots)\overline{M}(\cdots\hat{j}_{s+t+1}\cdots)$$

$$=-W(j_1\cdots\hat{j}_{s+t+1}\cdots j_{m+1})\qquad\square$$

Thm (Laplace)：给定 $A\in M_n(\mathbb{R})$ $1\leq m\leq n$，固定 $1\leq i_1<i_2<\cdots<i_m\leq n$，

令 $i=i_1+\cdots+i_m$，则有

$$|A| = (-1)^{i}\sum_{1\leq j_1<\cdots<j_m\leq n}(-1)^{j_1+j_2+\cdots+j_m}M(j_1,\cdots,j_m)\overline{M}(j_1,\cdots,j_m)$$

证明：

令 $$f(A)=(-1)^{i}\sum_{1\leq j_1<\cdots<j_m\leq n}(-1)^{j_1+j_2+\cdots+j_m}M_A(j_1,\cdots,j_m)\overline{M}_A(j_1,\cdots,j_m)$$

我们证明 $f(A)$ 为一行列式函数（反对称，n重线性函数，$f(E)=1$）

① f 关于列线性. 设 $A=(\alpha_1,\cdots,\lambda\alpha+\mu\beta,\cdots,\alpha_n)$

$A_1=(\alpha_1,\cdots,\alpha,\cdots,\alpha_n)$

$A_2=(\alpha_1,\cdots,\beta,\cdots,\alpha_n)$

（↑ k 列.）

若 $k\in\{j_1,\cdots,j_m\}$，则

$$M_A(j_1,\cdots,j_m)=\lambda M_{A_1}(j_1,\cdots,j_m)+\mu M_{A_1}(j_1,\cdots,j_m)$$

$$\overline{M}_A(j_1,\cdots,j_m)=\overline{M}_{A_1}(j_1,\cdots,j_m)=\overline{M}_{A_2}(j_1,\cdots,j_m)$$

若 $k\in\{j_1,\cdots,j_m\}^c$

$$M_A(j_1,\cdots,j_m)=M_{A_1}(j_1,\cdots,j_m)=M_{A_2}(j_1,\cdots,j_m)$$

$$\overline{M}_A(j_1,\cdots,j_m)=\lambda\overline{M}_{A_1}(j_1,\cdots,j_m)+\mu\overline{M}_{A_2}(j_1,\cdots,j_m)$$

直接验证两种情况均有

$$M_A\cdot\overline{M}_A=\lambda M_{A_1}\cdot\overline{M}_A+\mu M_{A_2}\cdot\overline{M}_{A_2}$$

$$\Longrightarrow f(A)=\lambda f(A_1)+\mu f(A_2).$$

② $f(A)$ 反对称. 若第 k, l 列相同, $k<l$. 固定某 $j_1 \cdots j_m$

a) 若 $\{k, l\} \subset \{j_1, \cdots, j_m\}$ $\quad M_A(j_1, \cdots, j_m)=0$

b) 若 $\{k, l\} \subset \{j_1, \cdots, j_m\}$ $\quad \overline{M}_A(j_1, \cdots, j_m)=0$.

c) 若 $k \in \{j_1, \cdots, j_m\}$ $\; l \in \{j_1, \cdots, j_m\}^c$.

c-1) 若 $l<j_m$, 考虑

$$1 \le j_1 < \cdots < j_{s-1} < j_s = k < j_{s+1} < \cdots < j_{s+t} < l < j_{s+t+1} < \cdots < j_m \le n$$

c-2) 若 $l<j_m$, 考虑

$$1 \le j_1 < \cdots < j_{s-1} < j_s = k < j_{s+1} < \cdots < j_m < l.$$

由引理有

$$(-1)^{j_1+\cdots+j_m} M_A(j_1, \cdots, j_m) \cdot \overline{M}_A(j_1 \cdots j_m)$$

$$= -(-1)^{j_1+\cdots j_{s-1}+j_{s+1}+\cdots+j_m+l} M_A(\cdots \hat{j_s} \cdots l \cdots) \overline{M}_A(\cdots \hat{j_s} \cdots l \cdots)$$

$\Rightarrow$ 每个含 k 但不含 l 的排列 $\{j_1 \cdots j_m\}$ 恰有一个含 l 但不含 k 的排列与其相消.

$$\Longrightarrow f(A)=0.$$

③ 注意到

$$M_E(j_1, \cdots j_m) = \begin{cases} 1 & j_1=i_1, \cdots, j_m=i_m \\ 0 & \text{otherwise} \end{cases}$$

$$\overline{M}_E(j_1, \cdots j_m) = \begin{cases} 1 & j_1=i_1, \cdots, j_m=i_m \\ 0 & \text{otherwise.} \end{cases}$$

$$\Rightarrow f(E)=1. \qquad \square$$

应用举例：求下述2n阶行列式的值.

$$|A_n| = \begin{vmatrix} a & & & & & & & b \\ & a & & & & & b & \\ & & \ddots & & & \iddots & & \\ & & & a & b & & & \\ & & & b & a & & & \\ & & \iddots & & & \ddots & & \\ & b & & & & & a & \\ b & & & & & & & a \end{vmatrix}$$

解：对第一行，最后一行展开.

$$|A_n| = (-1)^{1+2n} \sum_{1 \le j_1 < j_2 \le 2n} (-1)^{j_1+j_2} M_{A_n}(j_1, j_2) \cdot \bar{M}_{A_n}(j_1, j_2)$$

若 $j_1 \neq 1$，$j_2 \neq 2n \Rightarrow \bar{M}_{A_n} = 0$

$$\Rightarrow |A_n| = \begin{vmatrix} a & b \\ b & a \end{vmatrix} \cdot |A_{n-1}|$$

$$= (a^2-b^2)^2 \cdot |A_{n-1}| = \cdots = (a^2-b^2)^n. \quad \square$$

1、设 A 为一 n 阶方阵, 用 $\mathrm{rank}(A)$ 表示 $\mathrm{rank}(A^\vee)$.

对 rankA 分类讨论.

① 若 $\mathrm{rank}A = n$, $A^\vee = |A| \cdot A^{-1}$

$\mathrm{rank}A^{-1} = \mathrm{rank}(A) = n$.

② 若 $\mathrm{rank}(A) = n-1$, 则 A 存在 n-1阶非零子式

i.e. $\exists\, i, j$ s.t. $A_{ij} \neq 0$

$\Rightarrow \mathrm{rank}(A^\vee) \geq 1$

$A \cdot A^\vee = |A| \cdot E = 0 \Rightarrow$

$\mathrm{rank}(A \cdot A^\vee) \geqslant \mathrm{rank}(A) + \mathrm{rank}(A^\vee) - n$

$\Rightarrow \mathrm{rank}(A^\vee) \leq 1$

$\Rightarrow \mathrm{rank}(A^\vee) = 1$

③ 若 $\mathrm{rank}(A) < n-1$, 则 A 所有 n-1阶子式均为0.

$\Rightarrow \mathrm{rank}(A^\vee) = 0$.

2、证明: 若 A, B, C, D 为 n 阶方阵, $\det(A) \neq 0$, 则

$$\det\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \det(AD - ACA^{-1}B) = \det(A) \cdot \det(D - CA^{-1}B).$$

此外, 验证:

$$\det\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{cases} \det(AD - BC), & 若 AC = CA, \\ \det(DA - CB), & 若 AB = BA. \end{cases}$$

Pf: $\begin{pmatrix} A^{-1} & 0 \\ 0 & E \end{pmatrix}\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} E & A^{-1}B \\ C & D \end{pmatrix}$

$\begin{pmatrix} E & 0 \\ -C & E \end{pmatrix}\begin{pmatrix} E & A^{-1}B \\ C & D \end{pmatrix} = \begin{pmatrix} E & A^{-1}B \\ 0 & D - CA^{-1}B \end{pmatrix}$

$$\Rightarrow \begin{pmatrix} E & 0 \\ -C & E \end{pmatrix}\begin{pmatrix} A^{-1} & 0 \\ 0 & E \end{pmatrix}\cdot\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} E & A^{-1} \\ 0 & D-CA^{-1}B \end{pmatrix}$$

$$\Rightarrow \quad |A^{-1}|\cdot\begin{vmatrix} A & B \\ C & D \end{vmatrix} = |D-CA^{-1}B| \qquad |A^{-1}| = |A|^{-1}$$

$$\Rightarrow \quad \begin{vmatrix} A & B \\ C & D \end{vmatrix} = |A|\cdot|D-CA^{-1}B|$$
$$= |AD-ACA^{-1}B|.$$

验证后面等式显然，代入即可. □

3、 证明集合:

$$M_n^0(\mathbb{R}) = \left\{ A = (a_{ij}) \in M_n(\mathbb{R}) \middle| \sum_j^n a_{ij} = 0, i = 1, 2, \ldots, n \right\}$$

在矩阵通常乘法下运算下构成一个半群. $(M_n^0(\mathbb{R}), \cdot)$ 是幺半群吗?

解：若 $A=(a_{ij})$ $B=(b_{ij})$，$A,B\in M_n^0(\mathbb{R})$

则 $A\cdot B = C_{ij}$，$\sum_j C_{ij} = \sum_j\sum_k a_{ik}\cdot b_{kj} = \sum_k \sum_j a_{ik}\cdot b_{kj} = 0$

$\Rightarrow A\cdot B \in M_n^0(\mathbb{R})$，

又矩阵乘法结合，

$\Rightarrow (M_n^0(\mathbb{R}), \cdot)$ 为一半群.

其不为幺半群，若是，设其幺为 $e=(e_{ij})$

记 e 的第 i 列为 $e^{(i)}$

则 $e\begin{bmatrix} 1 & -1 & & 0 \\ 0 & & & 0 \end{bmatrix} = \begin{bmatrix} 1 & -1 & & 0 \\ 0 & & & 0 \end{bmatrix}$　　则 $e^{(1)} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$

同理 $e\begin{bmatrix} 0 & & & 0 \\ 0 & 1 & -1 & \\ & & \ddots & 0 \end{bmatrix} = \begin{bmatrix} 0 & & & 0 \\ 0 & 1 & -1 & \\ & & \ddots & 0 \end{bmatrix}$

$\Rightarrow e^{(i)} = 0 \quad \forall i$

$\Rightarrow e = E_n$，但 $E_n \notin M_n^0(\mathbb{R})$

$\Rightarrow (M_n^0(\mathbb{R}), \cdot)$ 无单位元.

Rem：若 (S, e_S) 为幺半群，(S', e_S') 为其子集，也构成幺半群，一般不能得到 $e_S = e_S'$.

eg 任一群 $\bar{1}, \bar{3}$，$\bar{1}, \bar{3} \subset \mathbb{Z}/6\mathbb{Z}$

4、设 $p=3$, 写出 $\mathbb{Z}_p$ 的加法与乘法表. 证明:$\mathbb{Z}_p^\times := \mathbb{Z}_p\backslash\{\bar{0}\}$ 关于乘法构成一个群. 另验证否存在一个元素 $a\in\mathbb{Z}_p^\times$ 使得 $\{a^i|i\in\mathbb{Z}\}=\mathbb{Z}_p^\times$. (注: 此题结论对一般素数 p 均成立.)

+	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

×	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{1}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{1}$	$\bar{2}$	$\bar{1}$

由上表 $\bar{1}\cdot\bar{1}=\bar{1}$ $\quad \bar{2}\cdot\bar{2}=\bar{1}$ $\quad \mathbb{Z}_p^\times=\{\bar{1},\bar{2}\}$

$\bar{1}$为单位元, $\bar{2}^{-1}=\bar{2}$

$\{\bar{2},\bar{2}^2\}=\mathbb{Z}_p^\times$.

Rem: $\mathbb{Z}_p^\times=\{\bar{1},\cdots,\overline{p-1}\}$ $\quad \forall\, \bar{a}\in\mathbb{Z}_p^\times$ $\quad (a,p)=1$

$\Rightarrow\ \exists k,l$ s.t. $ak+pl=1$

$\Rightarrow\ \bar{a}\bar{k}+\bar{p}\bar{l}=\bar{1} \Rightarrow \bar{a}\cdot\bar{k}=\bar{1}$.

$\Rightarrow$ $\mathbb{Z}_p^\times$为乘法群.

5、设 G,H 为两个群, 单位元分别为 e_G,e_H, 设 $\phi:G\to H$ 为两个群, 记 $\ker(\phi)=\{g\in G|\phi(g)=e_H\}$. 证明:

i) $\ker(\phi)$ 为 G 的一个子群;

ii) $g\ker(\phi)=\ker(\phi)g$ 对任意 $g\in G$ 成立, 其中 $g\ker(\phi)=\{gg'|g'\in\ker(\phi)\}$, $\ker(\phi)g=\{g'g|g'\in\ker(\phi)\}$;

iii) ϕ 是单射当且仅当 $\ker(\phi)=\{e_G\}$.

Pf: i) $\forall\ g_1,g_2\in\ker\Phi$, $\quad \Phi(g_1g_2^{-1})=\Phi(g_1)\cdot\Phi(g_2^{-1})$

$=\Phi(g_1)\cdot\Phi(g_2)^{-1}=e_H$

$\Rightarrow g_1g_2^{-1}\in\ker\Phi$, $\Rightarrow \ker\Phi$ 为 G 子群.

ii) ① $g\ker(\Phi)\subset\ker(\Phi)g$

$g\ker\varphi=\ker\varphi g$ $\quad \forall\ g\cdot g'\in g\ker\Phi$, $\quad g'\in\ker\Phi$

$\Phi(gg'\cdot g^{-1})=\Phi(g)\cdot\Phi(g')\cdot\Phi(g^{-1})$

~~$\Updownarrow$~~ $\quad =\Phi(g)\cdot\Phi(g^{-1})=e_H$.

$g\cdot g'=g'g$ $\quad \Rightarrow g\cdot g'g^{-1}\in\ker\Phi \Rightarrow g\cdot g'=(g\cdot g'g^{-1})\cdot g\in\ker\Phi\cdot g$.

② 同理考虑 $g^{-1}g'g$，则有 $\ker(\Phi)g \subset g\ker\Phi$.

$\Rightarrow g\cdot\ker(\Phi) = \ker(\Phi)\cdot g$

iii) 若 Φ 单，显然 $\ker(\Phi)=\{e_G\}$，因为 $\Phi(e_G)=e_H$.

若 $\ker\Phi=\{e_G\}$，设 $\Phi(g_1)=\Phi(g_2)$

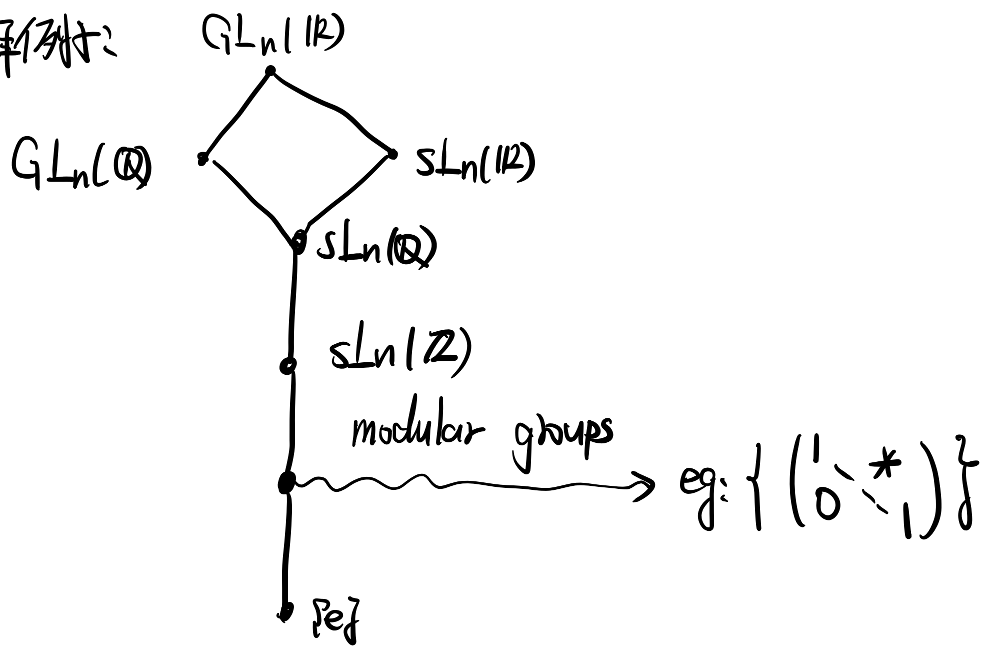
则 $\Phi(g_1g_2^{-1}) = \Phi(g_1)\cdot\Phi(g_2)^{-1}=e_H$

$\Rightarrow g_1g_2^{-1}\in\ker(\Phi)$

$\Rightarrow g_1g_2^{-1}=e_G \Rightarrow g_1=g_2$

$\Rightarrow$ Φ 单射.

子群例子：



Rem：$GL_n(\mathbb{Z})=\{A\in GL_n(\mathbb{R}) \mid A=(a_{ij})\ a_{ij}\in\mathbb{Z}\}$

为一幺半群，但不是群.

6、 证明若 $|G|$ 为偶数, 则必有元素 $g \neq e$ 满足 $a^2 = e$. (提示:$g^2 \neq e$ 则 $(g^{-1})^2 \neq e$.)

证: 若 $a^2=e$ 则 $a^{-1}=a$ (g) $(a^{-1})^2=a^2=e$

$a\neq e$

i.e. $a^2=e \Leftrightarrow (a^{-1})^2=e$

$\Rightarrow a^2\neq e \Leftrightarrow (a^{-1})^2\neq e$.

$a^2\neq e \Rightarrow a^{-1}\neq a$

则 我们 $g^2\neq e$ 的元素可两两配对

$g\neq e$

令 $T=\{a \mid a\in G \mid a^2\neq e\} \Rightarrow |T|$ 为偶数

$e\notin T, \Rightarrow |G|-|T|$ 为偶数, $\Rightarrow \exists g\neq e$ s.t. $g^2=e$.