0.1 自由幺半群与自由群

定义 0.1 (自由幺半群)

设 X 是一个非空集合, 称 X 中任一有限长的序列

$$x_1x_2\cdots x_i,\quad x_1,x_2,\cdots,x_i\in X$$

为一个**字**. 当 $i=0$ 时, 称为**空字**, 记为 $\wedge$. 记所有字的集合为 $\widetilde{X}$. 在 $\widetilde{X}$ 上定义乘法为

$$(x_1x_2\cdots x_i)(y_1y_2\cdots y_j)=x_1x_2\cdots x_iy_1y_2\cdots y_j.$$

显然 $\widetilde{X}$ 对此乘法是以 $\wedge$ 为幺元的幺半群, 称为**由 X 生成的自由幺半群**.

♣

定理 0.1

设集合 X 非空,S 是幺半群,f 是 X 到 S 的映射, 则存在唯一的 $\widetilde{X}$ 到 S 的同态 ϕ, 使

$$\phi(x)=f(x),\quad\forall x\in X.$$

♡

注 由这个定理知任何幺半群均可视为自由半群的同态像.

证明 记 e 为 S 的幺元, 定义 $\widetilde{X}$ 到 S 的映射 ϕ:

$$\phi(\wedge)=e,\quad\phi(x_1x_2\cdots x_i)=f(x_1)f(x_2)\cdots f(x_i),\ \forall x_1x_2\cdots x_i\in\widetilde{X}.$$

则 ϕ 显然为同态且 $\phi(x)=f(x)$, $\forall x\in X$.

若 ψ 为 $\widetilde{X}$ 到 S 的同态且 $\psi(x)=f(x)$, 则对 $\forall x_1x_2\cdots x_i\in\widetilde{X}$, 有

$$\psi(x_1x_2\cdots x_i)=\psi(x_1)\psi(x_2)\cdots\psi(x_i)=f(x_1)f(x_2)\cdots f(x_i)=\phi(x_1x_2\cdots x_i),$$

即 ϕ 唯一.

□

定义 0.2

设非空集合 X, 令非空集合 X' 满足 $X\cap X'=\varnothing$, 并且存在 X 到 X' 上的一一对应 φ, 记 $\varphi(a)=a',\forall a\in X$. 令 $X^*=X\cup X'$, 设 $x\in X^*$, 定义 x',

$$x'=\begin{cases}\varphi^{-1}(x)=a, & x=a'\in X',\\ \varphi(x)=a', & x=a\in X,\end{cases}\tag{1}$$

并且记 X^* 生成的自由幺半群为 $\widetilde{X^*}$. 设 $w_1,w_2\in\widetilde{X^*}$, 若 $\exists g,h\in\widetilde{X^*},x\in X^*$, 使得

$$\begin{cases}w_1=gh,\\ w_2=gxx'h\end{cases}\quad\text{或}\quad\begin{cases}w_1=gxx'h,\\ w_2=gh,\end{cases}$$

则称 w_1 与 w_2 是**相邻的**.

♣

定理 0.2

设非空集合 X, 令非空集合 X' 满足 $X\cap X'=\varnothing$, 并且存在 X 到 X' 上的一一对应 φ, 记 $\varphi(a)=a',\forall a\in X$. 再设 $X^*=X\cup X'$,$\widetilde{X^*}$ 为集合 X^* 生成的自由幺半群. 在 $\widetilde{X^*}$ 中定义关系 $\sim$ 如下: $w_1,w_2\in\widetilde{X^*}$, 称 $w_1\sim w_2$, 如果存在 $\widetilde{X^*}$ 中序列

$$w_1=v_1,v_2,\cdots,v_l=w_2$$

满足 v_i 与 v_{i+1} 相邻. 则 "$\sim$" 是 $\widetilde{X^*}$ 中同余关系, 并且 $\widetilde{X^*}$ 对于 $\sim$ 的商幺半群 $\widetilde{X^*}/\sim=F(X)$ 是群, 称 $F(X)$ 为**由 X 生成的自由群**. 用 $\overline{x}$ 表示 x 在 $F(X)$ 中的同余类, 则 $\overline{\wedge}$ 是 $F(X)$ 的幺元. 并且

$$(\overline{x_1x_2\cdots x_m})^{-1}=\overline{x'_mx'_{m-1}\cdots x'_1},\ \forall\overline{x_1x_2\cdots x_m}\in F(X).$$

特别地,$(\overline{x})^{-1} = \overline{x'}$, $\forall x \in X$. 因此也记 $x' = x^{-1}$,$X' = X^{-1}$.

注 X' 是根据 X 随便取一个形式逆集合, 只是为了满足群中每个元素都有逆元而引入的符号.

证明 首先证 $\sim$ 是等价关系.

$\forall w \in \widetilde{X^*}$, 取 $v_1 = w = w\wedge$, $v_2 = wa_1a_1'\wedge$, $v_3 = w\wedge = w$. 于是 v_1 与 v_2 相邻,v_2 与 v_3 相邻, 故有 $w \sim w$.

又设 $w_1 \sim w_2$, 即有 $w_1 = v_1, v_2, \cdots, v_l = w_2$ 且 v_i 与 v_{i+1} 相邻. 令 $u_i = v_{l-i+1}$, 则 $u_1 = w_2, u_2, \cdots, u_l = w_1$ 且 u_i 与 u_{i+1} 相邻. 于是 $w_2 \sim w_1$.

再设 $w_1 \sim w_2$, $w_2 \sim w_3$, 于是存在以下序列:

$$w_1 = v_1, v_2, \cdots, v_l = w_2, \quad v_i \text{与} v_{i+1} \text{相邻},$$
$$w_2 = u_1, u_2, \cdots, u_m = w_3, \quad u_j \text{与} u_{j+1} \text{相邻},$$

因而序列 $w_1 = v_1, v_2, \cdots, v_l = u_1, u_2, \cdots, u_m = w_3$ 的任意相邻两项是相邻的, 故 $w_1 \sim w_3$.

其次证 $\sim$ 为同余关系. 设 $w_1 \sim w_2$, $u_1 \sim u_2$, 则于是存在以下序列:

$$w_1 = v_1, v_2, \cdots, v_l = w_2, \quad v_i \text{与} v_{i+1} \text{相邻},$$
$$u_1 = u_1, u_2, \cdots, u_m = u_2, \quad u_j \text{与} u_{j+1} \text{相邻}.$$

注意到若 u_1 与 u_2 相邻, 即有 $u_1 = gh$, $u_2 = gxx'h$, 因而对 $\forall v \in \tilde{X}^*$, 有 $u_1v = ghv$, $u_2v = gxx'hv$, 于是 u_1v 与 u_2v 相邻, 同样 vu_1 与 vu_2 相邻. 于是有

$$w_1u_1 = v_1u_1, v_2u_1, \cdots, v_lu_1 = w_2u_1 \quad v_iu_1 \text{与} v_{i+1}u_1 \text{相邻},$$
$$w_2u_1 = v_lu_1, v_lu_2, \cdots, v_lu_m = w_2u_2 \quad v_lu_i \text{与} v_lu_{i+1} \text{相邻}.$$

这说明 $w_1u_1 \sim w_2u_1$,$w_2u_1 \sim w_2u_2$, 故 $w_1u_1 \sim w_2u_2$, 即 $\sim$ 为同余关系.

最后, 由定理**??**知 $F(X) = \widetilde{X^*}/\sim$ 是商幺半群. 再证明商幺半群 $F(X) = \widetilde{X^*}/\sim$ 是群, 只需证明 $F(X)$ 中任一元素可逆. 对 $\forall x \in \widetilde{X^*}$,$\wedge$ 为空字,x' 如式(1), 则有 $\wedge xx' \wedge = xx'$,$\wedge = \wedge\wedge$, 即 xx' 与 $\wedge$ 相邻, 因而

$$\wedge \sim xx', \ \forall x \in \widetilde{X^*}. \tag{2}$$

用 $\overline{x}$ 表示 x 在 $F(X)$ 中的同余类, 则 $\overline{\wedge}$ 是 $F(X)$ 的幺元. 对任意 $\overline{x_1x_2\cdots x_m} \in F(X)$, 有 $x_1x_2\cdots x_m \in \widetilde{X^*}$, 从而 $x_m'x_{m-1}'\cdots x_1' \in \widetilde{X^*}$, 再结合 "$\sim$" 是同余关系和(2)式可得

$$\begin{aligned}(x_1x_2\cdots x_m)(x_m'x_{m-1}'\cdots x_1') &= x_1x_2\cdots x_mx_m'\cdots x_1' \sim x_1x_2\cdots x_{m-1}\wedge x_{m-1}'\cdots x_1' \\ &= x_1x_2\cdots x_{m-1}x_{m-1}'\cdots x_1' \sim \cdots \sim x_1 \wedge x_1' = x_1x_1' \sim \wedge.\end{aligned}$$

于是

$$\begin{aligned}&\left(\overline{x_1x_2\cdots x_m}\right)\left(\overline{x_m'x_{m-1}'\cdots x_1'}\right) = \overline{(x_1x_2\cdots x_m)\left(x_m'x_{m-1}'\cdots x_1'\right)} \\ &= \left\{x \in \widetilde{X^*} \mid x \sim (x_1x_2\cdots x_m)\left(x_m'x_{m-1}'\cdots x_1'\right)\right\} \\ &= \left\{x \in \widetilde{X^*} \mid x \sim \wedge\right\} = \overline{\wedge}.\end{aligned}$$

故 $\overline{x_m'x_{m-1}'\cdots x_1'}$ 就是 $\overline{x_1x_2\cdots x_m}$ 的逆. 这就证明了 $F(X)$ 中元素均可逆, 故为群.

□

命题 0.1

设 $X = \{a\}$, 则 $F(X)$ 为无限循环群.

证明

□

定理 0.3

设非空集合 X, 令非空集合 X' 满足 $X \cap X' = \varnothing$, 并且存在 X 到 X' 上的一一对应 φ, 记 $\varphi(a) = a', \forall a \in X$. 再设 $X^* = X \cup X'$,$\widetilde{X^*}$ 为集合 X^* 生成的自由幺半群. 在 $\widetilde{X^*}$ 中定义关系 $\sim$ 如下: $w_1, w_2 \in \widetilde{X^*}$, 称 $w_1 \sim w_2$, 如果存在 $\widetilde{X^*}$ 中序列

$$w_1 = v_1, v_2, \cdots, v_l = w_2$$

满足 v_i 与 v_{i+1} 相邻. 又 f 是 X 到 G 的映射, 则存在唯一的自由群 $F(X)$ 到群 G 的同态 ψ, 使得

$$\psi(\overline{x}) = f(x)(\forall x \in X),$$

其中 $\overline{x}$ 表示 x 在 $F(X) = \widetilde{X^*}/\sim$ 中的同余类.

证明 首先将 f 扩充为 X^* 到 G 的映射, 仍以 f 表示, 满足 $f(x') = f(x)^{-1}(\forall x' \in X')$.

由定理 0.1知有唯一的幺半群 $\widetilde{X^*}$ 到 G 的同态 ϕ, 使得 $\phi(x) = f(x)(\forall x \in X^*)$. 若 $\widetilde{X^*}$ 中元素 w_1 与 w_2 相邻, 不妨设

$$w_1 = gh,\ w_2 = gxx'h, \quad g, h \in \widetilde{X^*},\ x, x' \in X^*.$$

其中 x' 的定义如式(1), 则有

$$\phi(w_2) = \phi(g)\phi(x)\phi(x')\phi(h) = \phi(g)f(x)f(x)^{-1}\phi(h) = \phi(g)\phi(h) = \phi(w_1),$$

即对 $\forall w_1, w_2 \in \widetilde{X^*}$, 都有

$$w_1 \sim w_2 \Longrightarrow \phi(w_1) = \phi(w_2). \tag{3}$$

定义 $F(X)$ 到 G 的映射 ψ, 满足

$$\psi(\overline{w}) = \phi(w), \forall\, \overline{w} \in F(X).$$

若 $\overline{w_1} = \overline{w_2}$, 则 $w_1 \sim w_2$, 由(3)式知

$$\psi\left(\overline{w_1}\right) = \phi\left(w_1\right) = \phi\left(w_2\right) = \psi\left(\overline{w_2}\right).$$

故 ψ 是良定义的. 对 $\overline{w_1}, \overline{w_2} \in F(x)$, 有

$$\psi\left(\overline{w_1}\overline{w_2}\right) = \psi\left(\overline{w_1 w_2}\right) = \phi\left(w_1 w_2\right) = \phi\left(w_1\right)\phi\left(w_2\right) = \psi\left(\overline{w_1}\right)\psi\left(\overline{w_2}\right).$$

故 ψ 为同态. 显然 $\psi(\overline{x}) = \phi(x) = f(x)(\forall x \in X)$.

最后证明 ψ 的唯一性. 若 ψ' 为 $F(X)$ 到 G 的同态且 $\psi(\overline{x}) = f(x)(\forall x \in X)$, 则对 $\forall x \in X$, 有

$$\psi'\left(\overline{x}\right) = f\left(x\right) = \psi\left(\overline{x}\right).$$

对 $\forall x' \in X'$, 由定理 0.2知 $(\overline{x})^{-1} = \overline{x'}$. 从而

$$\psi'\left(\overline{x'}\right) = \psi'\left((\overline{x})^{-1}\right) = \psi'\left(\overline{x}\right)^{-1} = f\left(x\right)^{-1} = f\left(x'\right) = \psi\left(\overline{x'}\right).$$

因此

$$\psi'\left(\overline{x}\right) = \psi\left(\overline{x}\right), \quad \forall x \in X \cup X' = X^*.$$

对 $\forall \overline{x_1 x_2 \cdots x_m} \in F\left(X\right)$, 则 $x_1, x_2, \cdots, x_m \in X^*$. 于是

$$\begin{aligned}\psi'\left(\overline{x_1 x_2 \cdots x_m}\right) &= \psi'\left(\overline{x_1}\overline{x_2}\cdots\overline{x_m}\right) = \psi'\left(\overline{x_1}\right)\psi'\left(\overline{x_2}\right)\cdots\psi'\left(\overline{x_m}\right) \\ &= \psi\left(\overline{x_1}\right)\psi\left(\overline{x_2}\right)\cdots\psi\left(\overline{x_m}\right) = \psi\left(\overline{x_1}\overline{x_2}\cdots\overline{x_m}\right) = \psi\left(\overline{x_1 x_2 \cdots x_m}\right).\end{aligned}$$

因此 ψ 唯一.

□

推论 0.1

设非空集合 $X = \{a_1, a_2, \cdots, a_n\}$, 则 $\alpha : x \to \overline{x}, \forall x \in X$ 是 X 到 $F(X)$ 中的单射.

注 由这个推论知, 当 X 为非空有限集时,$X \cong \alpha(X) \subseteq F(X)$, 从而 X 可视为 $F(X)$ 的子集, 此时,定理 0.3中 ψ 的条件可改为

$$\psi(x) = f(x), \quad \forall x \in X.$$

证明 在 $\mathbb{Z}^n = \{(m_1, m_2, \cdots, m_n) \mid m_i \in \mathbb{Z}, 1 \leqslant i \leqslant n\}$ 中定义加法运算为

$$(m_1, m_2, \cdots, m_n) + (l_1, l_2, \cdots, l_n) = (m_1 + l_1, m_2 + l_2, \cdots, m_n + l_n),$$

则 $\mathbb{Z}^n$ 是交换群, 而 X 到 $\mathbb{Z}^n$ 中映射

$$f : a_i \to (m_1, m_2, \cdots, m_n), \quad m_j = \delta_{ij} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}, 1 \leqslant i, j \leqslant n$$

是单射. 如图 1所示, 由定理 0.3知有 $F(X)$ 到 $\mathbb{Z}^n$ 的同态 ψ, 使得

$$\psi(\overline{x}) = f(x), \quad \forall x \in X,$$

即有 $\psi\alpha = f$. 若 $\alpha(a_i) = \alpha\left(a_j\right)\left(a_i, a_j \in X\right)$, 即 $\overline{a_i} = \overline{a_j}$, 则两边同时作用 ψ 得

$$f\left(a_i\right) = \psi\left(\overline{a_i}\right) = \psi\left(\overline{a_j}\right) = f\left(a_j\right).$$

因为 f 是单射, 所以 $a_i = a_j$. 故 α 也是单射.

$$\begin{tikzcd} X \arrow[r, "a"] \arrow[d, "f"'] & F(X) \arrow[dl, "\psi"] \\ \mathbb{Z}^n & \end{tikzcd}$$

图 1

□

推论 0.2

设是有限生成群 $G = \langle g_1, g_2, \cdots, g_n \rangle$, 非空集合 $X = \{a_1, a_2, \cdots, a_n\}$,$F(X)$ 是集合 X 的自由群. 定义 X 到 G 的映射 f,

$$f(a_i) = g_i, \quad 1 \leqslant i \leqslant n.$$

由定理 0.3和推论 0.1知, 存在 $F(X)$ 到 G 的满同态 ψ 满足

$$\psi(\overline{a_i}) = \psi(a_i) = f(a_i) = g_i, \quad 1 \leqslant i \leqslant n,$$

则

$$G \cong F(X)/\ker\psi.$$

称 $\ker\psi$ 为 G 的生成元 $g_1, g_2, \cdots, g_n$ 间的**关系集**. 若 $\ker\psi$ 也是由有限个元素 $w_1, w_2, \cdots, w_r$ 生成, 即 $\ker\psi = \langle w_1, w_2, \cdots, w_r \rangle$, 则称 G 是**可有限表现的**, 而且

$$\psi(w_i) = e, \quad 1 \leqslant i \leqslant r.$$

称 $w_1, w_2, \cdots, w_r$ 为 G 的生成元 $g_1, g_2, \cdots, g_n$ 的一组**生成关系**.

♡

证明 由定理**??**知

$$\langle G \rangle = \left\{x_1 x_2 \cdots x_m \mid x_i \in G \cup G^{-1}, 1 \leqslant i \leqslant m, m \in \mathbb{N}\right\}.$$

于是对 $\forall \overline{a_1 a_2 \cdots a_m} \in F(X)(1 \leqslant m \leqslant n)$, 有

$$\psi\left(\overline{a_1 a_2 \cdots a_m}\right) = \psi\left(\overline{a_1 a_2} \cdots \overline{a_m}\right) = \psi\left(\overline{a_1}\right)\psi\left(\overline{a_2}\right) \cdots \psi\left(\overline{a_m}\right) = g_1 g_2 \cdots g_m \in \langle G \rangle.$$

因此 $\psi(F(X)) \subseteq \langle G\rangle$. 对 $\forall x_1x_2\cdots x_m \in \langle G\rangle\,(1\leqslant m\leqslant n)$, 不妨设

$$x_1x_2\cdots x_m = \left(g_{i_1}g_{i_2}\cdots g_{i_k}\right)\left(g_{i_{k+1}}^{-1}g_{i_{k+2}}^{-1}\cdots g_{i_m}^{-1}\right),\quad i_1,i_2,\cdots,i_m\in\{1,2,\cdots,m\}.$$

从而

$$\begin{aligned}
x_1x_2\cdots x_m &= \left(g_{i_1}g_{i_2}\cdots g_{i_k}\right)\left(g_{i_{k+1}}^{-1}g_{i_{k+2}}^{-1}\cdots g_{i_m}^{-1}\right)\\
&= \left(\psi\left(\overline{a_{i_1}}\right)\psi\left(\overline{a_{i_2}}\right)\cdots\psi\left(\overline{a_{i_k}}\right)\right)\left(\psi\left(\overline{a_{i_{k+1}}}\right)^{-1}\psi\left(\overline{a_{i_{k+2}}}\right)^{-1}\cdots\psi\left(\overline{a_{i_m}}\right)^{-1}\right)\\
&= \psi\left(\overline{a_{i_1}a_{i_2}\cdots a_{i_k}}\right)\left(\psi\left(\left(\overline{a_{i_{k+1}}}\right)^{-1}\right)\psi\left(\left(\overline{a_{i_{k+2}}}\right)^{-1}\right)\cdots\psi\left(\left(\overline{a_{i_m}}\right)^{-1}\right)\right)\\
&= \psi\left(\overline{a_{i_1}a_{i_2}\cdots a_{i_k}}\right)\left(\psi\left(\overline{a'_{i_{k+1}}}\right)\psi\left(\overline{a'_{i_{k+2}}}\right)\cdots\psi\left(\overline{a_{i_m}'}\right)\right)\\
&= \psi\left(\overline{a_{i_1}a_{i_2}\cdots a_{i_k}}\right)\psi\left(\overline{a'_{i_{k+1}}a'_{i_{k+2}}\cdots a'_{i_m}}\right)\\
&= \psi\left(\overline{a_{i_1}a_{i_2}\cdots a_{i_k}a'_{i_{k+1}}a'_{i_{k+2}}\cdots a'_{i_m}}\right)\in\psi(F(X)).
\end{aligned}$$

因此 $\psi(F(X)) \supseteq \langle G\rangle$. 故 $\psi(F(X)) = \langle G\rangle$, 即 ψ 是 $F(X)$ 到 G 的满同态. 故由群的同态基本定理知 $G\cong F(X)/\ker\psi$. □

命题 0.2

设 D_n 是保持正 n 边形不动的转动与反射 (也叫对称) 生成的群, 通常称为**二面体群**. 以正 n 边形的中心为原点, 并设 x 轴的正方向通过一个顶点. 设 a 是转动 $\frac{2\pi}{n}$, 而 b 是对 x 轴的反射. 容易看出 D_n 由 a 与 b 生成, 即 $D_n=\langle a,b\rangle$.

令 $X=\{x_1,x_2\}$, 于是由推论 0.2知有 $F(X)$ 到 D_n 的满同态 ψ, 使 $\psi(x_1)=a,\psi(x_2)=b$. 则 $x_1^n,x_2^2,x_1x_2x_1x_2$ 就是 D_n 的生成元 a,b 的一组生成关系.

证明 不难发现 D_n 中只有 n 个不同的转动和 n 个不同的反射对称, 即

$$\mathrm{id},a,\cdots,a^{n-1};\quad b,ab,\cdots,a^{n-1}b.$$

故 $|D_n|=2n$ 且有

$$a^n=\mathrm{id},\quad b^2=\mathrm{id},\quad abab=\mathrm{id}.$$

由上式知

$$\psi\left(x_1^n\right)=a^n=\mathrm{id},\quad \psi\left(x_2^2\right)=b^2=\mathrm{id},\quad \psi\left(x_1x_2x_1x_2\right)=abab=\mathrm{id}.$$

故 $x_1^n,x_2^2,x_1x_2x_1x_2\in\ker\psi$. 由推论 0.1知可将 X 视为 $F(X)$ 的子集, 于是由 $x_1^n,x_2^2,x_1x_2x_1x_2$ 生成的 $F(X)$ 的子群 K 在 $\ker\psi$ 中, 故 $|K|\leqslant|\ker\psi|$.

对 $\forall x\in X^*$, 用 $\widetilde{x}$表示x在$F(X)$ 中的同余类. 对 $\forall \widetilde{x_{k_1}^{\varepsilon_1}x_{k_2}^{\varepsilon_2}\cdots x_{k_m}^{\varepsilon_m}}\in F(X)\,(k_i\in\{1,2\},\varepsilon_i\in\{-1,1\},1\leqslant i\leqslant m)$, 有

$$\begin{aligned}
\left(\widetilde{x_{k_1}^{\varepsilon_1}x_{k_2}^{\varepsilon_2}\cdots x_{k_m}^{\varepsilon_m}}\right)x_1^n\left(\widetilde{x_{k_1}^{\varepsilon_1}x_{k_2}^{\varepsilon_2}\cdots x_{k_m}^{\varepsilon_m}}\right)^{-1} &= \left(\widetilde{x_{k_1}^{\varepsilon_1}x_{k_2}^{\varepsilon_2}\cdots x_{k_m}^{\varepsilon_m}}\right)\widetilde{x_1^n}\left(\widetilde{x_{k_m}^{-\varepsilon_m}x_{k_{m-1}}^{-\varepsilon_{m-1}}\cdots x_{k_1}^{-\varepsilon_1}}\right)\\
&= \widetilde{x_{k_1}^{\varepsilon_1}}\widetilde{x_{k_2}^{\varepsilon_2}}\cdots\widetilde{x_{k_m}^{\varepsilon_m}}\widetilde{x_1^n}\widetilde{x_{k_m}^{-\varepsilon_m}}\widetilde{x_{k_{m-1}}^{-\varepsilon_{m-1}}}\cdots\widetilde{x_{k_1}^{-\varepsilon_1}}\in F(X),\\
\left(\widetilde{x_{k_1}^{\varepsilon_1}x_{k_2}^{\varepsilon_2}\cdots x_{k_m}^{\varepsilon_m}}\right)x_2^2\left(\widetilde{x_{k_1}^{\varepsilon_1}x_{k_2}^{\varepsilon_2}\cdots x_{k_m}^{\varepsilon_m}}\right)^{-1} &= \left(\widetilde{x_{k_1}^{\varepsilon_1}x_{k_2}^{\varepsilon_2}\cdots x_{k_m}^{\varepsilon_m}}\right)\widetilde{x_2^2}\left(\widetilde{x_{k_m}^{-\varepsilon_m}x_{k_{m-1}}^{-\varepsilon_{m-1}}\cdots x_{k_1}^{-\varepsilon_1}}\right)\\
&= \widetilde{x_{k_1}^{\varepsilon_1}}\widetilde{x_{k_2}^{\varepsilon_2}}\cdots\widetilde{x_{k_m}^{\varepsilon_m}}\widetilde{x_2^2}\widetilde{x_{k_m}^{-\varepsilon_m}}\widetilde{x_{k_{m-1}}^{-\varepsilon_{m-1}}}\cdots\widetilde{x_{k_1}^{-\varepsilon_1}}\in F(X),\\
\left(\widetilde{x_{k_1}^{\varepsilon_1}x_{k_2}^{\varepsilon_2}\cdots x_{k_m}^{\varepsilon_m}}\right)\left(x_1x_2x_1x_2\right)\left(\widetilde{x_{k_1}^{\varepsilon_1}x_{k_2}^{\varepsilon_2}\cdots x_{k_m}^{\varepsilon_m}}\right)^{-1} &= \left(\widetilde{x_{k_1}^{\varepsilon_1}x_{k_2}^{\varepsilon_2}\cdots x_{k_m}^{\varepsilon_m}}\right)\left(\widetilde{x_1x_2x_1x_2}\right)\left(\widetilde{x_{k_m}^{-\varepsilon_m}x_{k_{m-1}}^{-\varepsilon_{m-1}}\cdots x_{k_1}^{-\varepsilon_1}}\right)\\
&= \widetilde{x_{k_1}^{\varepsilon_1}}\widetilde{x_{k_2}^{\varepsilon_2}}\cdots\widetilde{x_{k_m}^{\varepsilon_m}}\widetilde{x_1}\widetilde{x_2}\widetilde{x_1}\widetilde{x_2}\widetilde{x_{k_m}^{-\varepsilon_m}}\widetilde{x_{k_{m-1}}^{-\varepsilon_{m-1}}}\cdots\widetilde{x_{k_1}^{-\varepsilon_1}}\in F(X).
\end{aligned}$$

因而 K 是 $F(X)$ 的正规子群.

又 $F(X)/\ker\psi$ 与 D_n 同构, 从而 $[F(X):\ker\psi]=|D_n|=2n$. 因而只需证明 $[F(X):K]\leqslant|D_n|=2n$, 则由推

论??可得

$$[F(X):K]=\frac{|F(X)|}{|K|}\leqslant 2n \Longrightarrow |K|\geqslant \frac{|F(X)|}{2n}=\frac{|F(X)|}{\left[F(X):\ker\psi\right]}=\frac{|F(X)|}{|F(X)|}\cdot|\ker\psi|=|\ker\psi|.$$

因此 $|K|=|\ker\psi|$, 故 $\ker\psi=K$, 即 $x_1^n,x_2^2,x_1x_2x_1x_2$ 就是 D_n 的生成元 a,b 的一组生成关系.

注意到

$$F(X)=\left\{\widetilde{y_1y_2\cdots y_m}\mid y_i\in X^*=\left\{x_1,x_2,x_1^{-1},x_2^{-1}\right\},1\leqslant i\leqslant m,m\in\mathbb{N}\right\},$$

故 $\overline{x_1}=x_1K,\overline{x_2}=x_2K$ 为 $F(X)/K$ 的生成元, 即 $F(X)/K=\langle\overline{x_1},\overline{x_2}\rangle$. 由 $x_1^n,x_2^2,x_1x_2x_1x_2\in K$ 有

$$\overline{x_1^n}=\overline{x_2^2}=\overline{x_1x_2x_1x_2}=\overline{e},$$

故

$$\overline{x_1x_2x_1x_2}=\overline{e}\Longrightarrow\overline{x_1^{-1}}\left(\overline{x_1x_2x_1x_2}\right)\overline{x_2}=\overline{x_1^{-1}}\overline{x_2}\Longleftrightarrow\overline{x_2x_1}=\overline{x_1^{-1}}\overline{x_2}.$$

假设 $\overline{x_2}\overline{x_1^k}=\overline{x_1^{-k}}\overline{x_2}$, 则

$$\overline{x_2}\overline{x_1^{k+1}}=\left(\overline{x_2}\overline{x_1^k}\right)\overline{x_1}=\left(\overline{x_1^{-k}}\overline{x_2}\right)\overline{x_1}=\overline{x_1^{-k}}\left(\overline{x_2x_1}\right)=\overline{x_1^{-k}}\left(\overline{x_1^{-1}}\overline{x_2}\right)=\overline{x_1^{-(k+1)}}\overline{x_2}.$$

故由数学归纳法知

$$\overline{x_2}\overline{x_1^k}=\overline{x_1^{-k}}\overline{x_2},\quad 1\leqslant k\leqslant n.$$

再结合 $\left(\overline{x_2^2}\right)=\overline{x_2}$ 可得

$$\overline{x_1^k}\overline{x_2}=\overline{x_2}\overline{x_1^{-k}},\quad 1\leqslant k\leqslant n. \tag{4}$$

令 $G_1=\{\overline{x_1^k},\overline{x_1^k}\overline{x_2}\mid 1\leqslant k\leqslant n\}$, 则对 $\forall k,l\in\{1,2,\cdots,n\}$, 由 $\overline{x_1^n}=\overline{e}$ 知

$$\overline{x_1^{k+l}}=\begin{cases}\overline{x_1^{k+l-n}}\in G_1, & n<k+l\leqslant 2n,\\ \overline{x_1^{k+l}}\in G_1, & 1\leqslant k+l\leqslant n.\end{cases}$$

于是再利用(4)式可得

(i) $\overline{x_1^k}\cdot\overline{x_1^{-l}}=\overline{x_1^{k-l}}\in G_1$;

(ii) $\left(\overline{x_1^k}\overline{x_2}\right)\cdot\left(\overline{x_1^l}\overline{x_2}\right)^{-1}=\left(\overline{x_1^k}\overline{x_2}\right)\cdot\left(\overline{x_2^{-1}x_1^{-l}}\right)=\left(\overline{x_1^k}\overline{x_2}\right)\cdot\left(\overline{x_2}\overline{x_1^{-l}}\right)=\overline{x_1^{k-l}}\in G_1$;

(iii) $\left(\overline{x_1^l}\overline{x_2}\right)\cdot\overline{x_1^{-k}}\xlongequal{(4)式}\left(\overline{x_2}\overline{x_1^{-l}}\right)\cdot\overline{x_1^{-k}}=\overline{x_2}\overline{x_1^{-k-l}}\xlongequal{(4)式}\overline{x_1^{k+l}}\overline{x_2}\in G_1$;

(iv) $\overline{x_1^k}\cdot\left(\overline{x_1^l}\overline{x_2}\right)^{-1}=\overline{x_1^k}\cdot\left(\overline{x_2^{-1}x_1^{-l}}\right)=\overline{x_1^k}\cdot\left(\overline{x_2}\overline{x_1^{-l}}\right)\xlongequal{(4)式}\overline{x_1^k}\cdot\left(\overline{x_1^l}\overline{x_2}\right)=\overline{x_1^{k+l}}\overline{x_2}\in G_1$.

因而由定理????知 $F(X)/K=\langle\overline{x_1},\overline{x_2}\rangle\subseteq G_1$. 故 $G_1=\{\overline{x_1^k},\overline{x_1^k}\overline{x_2}\mid 1\leqslant k\leqslant n\}$ 为 $F(X)/K$ 的子群, 显然 $|G_1|\leqslant 2n$. 但由 $\overline{x_1},\overline{x_2}\in G_1$ 知 $G_1=F(X)/K$, 因而 $[F(X):K]\leqslant 2n$.

□