第一次习题课

1(作业题 4): 设 G 是一个半群, 如果:
(1) G 中含有左幺元 e, 即 $\forall x \in G, ex = x$;
(2) G 的每个元素 x 有 (关于 e) 左逆元 x^{-1} 使得 $x^{-1}x = e$.
试证 G 是群.
证明: 我们欲说明 e 是幺元, 那么应该证明 $xe = x(x^{-1}x) = (xx^{-1})x = ex = x, \forall x \in G$, 因此我们只需要证明 $xx^{-1} = e, \forall x \in G$, 而 $xx^{-1} = e(xx^{-1}) = (ex)x^{-1} = (((x^{-1})^{-1}x^{-1})x)x^{-1} = ((x^{-1})^{-1}(x^{-1}x))x^{-1} = ((x^{-1})^{-1}e)x^{-1} = (x^{-1})^{-1}(ex^{-1}) = (x^{-1})^{-1}x^{-1} = e$. 因此 e 是 G 中幺元, 而且同时说明了 G 中任意一个元素有逆元. □

2(作业题 8): 举例:
(1) 举出一个半群的例子, 其中存在元素有左逆元但是没有右逆元;
(2) 举出一个半群的例子, 其中存在元素至少有两个左逆元;
(3) 举出一个半群的例子, 其中存在元素有无数个左逆元.
证明: 大多数时候我们谈论左右逆元, 都是在幺半群的情况下, 因为此时只有唯一一个幺元, 性质相对会好些. 我们分别看一些例子:
(a): 右零半群.
设 S 是一个非空子集, 定义其中乘法: $a \cdot b = b, \forall a, b \in S$, 易证 S 是半群, 而且任一元素都是左幺元, 且任一元素 a 都是元素 b 的相对于左幺元 b 的左逆元. 因此 b 有 $|S|$ 个相对于 b 的左逆元. 同时, 任一元素 b 都是元素 a 的相对于左幺元 b 的左逆元
注意: 右零半群构成一个群 $\Longrightarrow ae = a = e, \forall a \in S \Rightarrow |S| = 1$.
(b): 集合的全变换半群 $\mathcal{T}(X)$(幺半群).
例: $f : \mathbf{N} \to \mathbf{N}, n \longmapsto n + 1$, 没有右逆元因为其不是满射.$f$ 有无限个左逆: $g_a : \mathbf{N} \to \mathbf{N}$,

$$g_a(n) = \begin{cases} n-1 & n \geq 1 \\ a & n = 0 \end{cases} \qquad \forall a \in \mathbf{N}.$$

或者 $f(n) = n^2$.
也可以考虑 R^∞ 上的线性变换: $f : (a_1, a_2, \cdots, a_n, \cdots) = (0, a_1, a_2, \cdots, a_n, \cdots)$. □
Remark:
(a): 固定右零半群里的一个左幺元, 记为 e, 那么 $\forall a \in G, ab = b = e$ 意味着每个元素关于 e 都有唯一的右幺元 e, 但是 S 一般不是群.
(b) 若半群 G 有唯一的右幺元 e 并且每个元素都有关于 e 的左逆元, 那么 G 是一个群. 事实上: $e = (a^{-1})^{-1}a^{-1} = (a^{-1})^{-1}(a^{-1}a)a^{-1} = eaa^{-1}$, 所以 $\forall b \in G, b = be = beaa^{-1} = baa^{-1} \Rightarrow e = aa^{-1}$, 进一步 $ea = (aa^{-1})a = ae = a$. 因此,G 是群.
(c)Kaplansky 定理: 含幺环中一元素若有至少两个右逆元, 则其有无限个右逆元 $(x_0 + (1 - x_0x)x^k)$.
(d) 定义 $f : \mathbf{N} \to \mathbf{N}$:

$$f(n) = \begin{cases} n-1 & n > 1 \\ 0 & 0 \leq n \leq 1 \end{cases}.$$

易验证 f 只有两个右逆元, 因此 $\mathcal{T}(X)^{op}$ 中 f 恰有两个左逆元.

3(作业题 9): 令 S 是一非空集. 定义 S 上的运算:$a \cdot b = a(a \cdot b = b)$. 则 $(S, \cdot)$ 是一个半群, 称其为左 (右) 零半群. 若 S 是一半群, 证明如下三款等价:
(1) S 是一左零半群, 或者 S 是一右零半群;
(2) $ab = cd \Rightarrow a = c$ 或者 $b = d$;

(3) 任意映射 $f: S \to S, f(ab) = f(a)f(b)$.

证明: (1)⇒(3): 显然;
(3)⇒(2): 先证明 $\forall a, b \in S, ab = a$ 或者 b. 若 $ab \neq a$, 做 S 上的变化 $f(x) = a(x = ab), f(x) = ab(x \neq ab) \Rightarrow a = f(ab) = f(a)f(b) = (ab)f(b)$, 若 $f(b) = ab$, 那么 $a = (ab)(ab) = ab$(考虑到独点的映射), 矛盾, 因此 $f(b) =\neq ab$, 即 $ab = a$. 现证明命题, 设 $ab = cd$, 若 $a = b$, 那么 $ab = aa = a = b = cd = c(d)$, 若 $a \neq b$, 那么 $ab = a(b)$, 若 $ab = a$, 做 S 上的变化 $f(x) = c(x = ab), f(x) = d(x \neq ab)$, 则 $c = f(ab) = f(a)f(b) = cd = ab = a$. 若 $ab = b$, 则 $b = d$.
(2)⇒(1): 若 S 不是左零半群, 则 $\exists a_0, b_0 \in S$ 使得 $a_0 b_0 \neq a_0$, 所以 $\forall a \in S$, 有 $(a_0 b_0)a = a_0(b_0 a) \Rightarrow a = b_0 a \Rightarrow ba = (b_0 b)a = b_0(ba) \Rightarrow a = ba, \forall b \in S \backslash \{b_0\}$. 因此 S 是一个右零半群. □

4(作业题 10): 令 G 是一个半群. 则 G 是一个群当且仅当

$$\forall a \in G, \exists! b \in G, (ab)^2 = ab.$$

证明: 第一步: 记上述 b 为 a', 那么有 $(aa'aa')^2 = aa'aa' \Rightarrow a'aa' = a' \Rightarrow (a'a)^2 = a'a$. 若存在另一个 a'' 满足 $(a''a)^2 = a''a$, 即 $a = (a'')'$, 那么 $(aa'')^2 = aa'' \Rightarrow a'' = a'$.
第二步: 任意 $a, b \in G, ((ba')'(ba'))^2 = (((ba')'b)a'))^2 = ((ba')'b)a') \Rightarrow (ba')'b = a$. 即 $xb = a$ 有解, 类似的 $ay = b$ 有解, 故 G 是群. □

5:(一些小维典型群)
(1):SO(2)≅U(1)(课堂上说过);
(2): SU(2) ↠ SO(3).

证明: (1):$\mathrm{SO}(2) = \left\{ \begin{pmatrix} cos\varphi & -sin\varphi \\ sin\varphi & cos\varphi \end{pmatrix} \in M_2(R) | 0 \leq \varphi < 2\pi \right\} \to \mathrm{U}(1)$

. $\begin{pmatrix} cos\varphi & -sin\varphi \\ sin\varphi & cos\varphi \end{pmatrix} \mapsto e^{i\varphi}$.

(2): 旋转群 SO(3). 在 $\mathbb{R}^3$ 上给定标准内积.$\mathbb{R}^3$ 的原点表示成 O,$\mathbb{R}^3$ 上的旋转 (rotation) 是一个光滑映射 $R: \mathbb{R}^3 \to \mathbb{R}^3$, 其保持原点 O、角度、距离和定向. 考虑 $\mathbb{R}^3$ 中任意两点 A, B, 由于 R 保持距离和角度, 则四边形 $OABC$ 和四边形 $R(O)R(A)R(B)R(C)$ 全等, 因此 $O\overrightarrow{R(A)} + O\overrightarrow{R(B)} = O\overrightarrow{R(C)}$, 也就是 $R(C) = R(A + B) = R(A) + R(B)$. 而且我们有 $R(rA) = rR(A)$, 因此 R 是一个线性映射.(如果觉得该描述不够数学, 也可以利用内积得到更严格的数学证明).
因为:

$$cos(\mathbf{a}, \mathbf{b}) = \frac{\mathbf{a} \cdot \mathbf{b}}{\sqrt{\mathbf{a} \cdot \mathbf{a}} \mathbf{b} \cdot \mathbf{b}}$$

一个旋转保持距离和角度当且仅当其保持内积.

为了保持定向, 只需要其保持外积 $\mathbf{a} \cdot \mathbf{b} \times \mathbf{c} = det(\mathbf{a}, \mathbf{b}, \mathbf{c})$,$R$ 对应的矩阵同样记为 R, 则有 $\mathrm{sgn}(\det R \cdot \det(\mathbf{a}, \mathbf{b}, \mathbf{c})) = \mathrm{sgn}(\det(\mathbf{a}, \mathbf{b}, \mathbf{c}))$. 因此 $\det R > 0$.
综上, 一个旋转对应于一个线性变换, 其满足:$R^T R = I_3$, $\det R = 1$, 即 SO(3). 而我们又知道三阶特殊正交矩阵必有一个实特征根, 且可知其是 $1(\lambda_1 \lambda_2 \bar{\lambda_2} = 1)$. 因此存在 e_r 使得 $Re_R = e_R$. 若 R 不是恒等矩阵, 则其属于 1 的特征子空间的维数为一, 其在 R 的作用下是不变的. 我们称改不变子空间为旋转轴 (the axis of rotation),R 可以视作绕着该轴的旋转 (角度记为 ϕ, 旋转 R 记为 $R(e_R, \phi)$). 我们能通过一个坐标变换使得 z 轴变成 e_R, 例如: 记 e_R 在 zy 平面的投影和 z 轴的夹角为 θ,e_R 和 z 轴的夹角为 φ, 则:

$$R(e_R, \phi) = \begin{pmatrix} cos\theta & -sin\theta & 0 \\ sin\theta & cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} cos\varphi & 0 & sin\varphi \\ 0 & 1 & 0 \\ -sin\varphi & 0 & cos\varphi \end{pmatrix} \begin{pmatrix} cos\phi & -sin\phi & 0 \\ sin\phi & 0 & cos\phi \\ 0 & 0 & 1 \end{pmatrix}$$

上述矩阵分别记为 $R_z(\theta), R_y(\varphi), R_z(\phi)$, 因此 $R = R_z(\theta)R_y(\varphi)R_z(\phi)$.

类似的有 $R_x(\alpha) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & cos\alpha & -sin\alpha \\ 0 & sin\alpha & cos\alpha \end{pmatrix}$. 故 SO(3) 可以由初等旋转矩阵 $R_x(\alpha), R_y(\varphi), R_z(\phi)$ 生成.

复旋转. 在 $\mathbb{C}^2$ 给定标准内积. 我们有群同态 det:$U(2) \longrightarrow U(1)$, 显然这是一个满同态, 且其 kernel 是 $SU(2)$. 特别的, 我们有 $U(2) \cong U(1) \times SU(2)$ ($U(1) \cong \begin{pmatrix} e^{i\varphi/2} & 0 \\ 0 & e^{i\varphi/2} \end{pmatrix}$).

$\forall U \in SU(2)$, $U^*U = I_2$, 且 $\det U = 1$, 因此可以得到如下等式

$$\begin{aligned} |a|^2 + |c|^2 = 1, \quad |b|^2 + |d|^2 = 1, \\ \bar{a}b + \bar{(c)}d = 0, \quad ad - bc = 1. \end{aligned}$$

故 $U^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$, 所以 $d = \bar{a}, c = -\bar{b}$. 因此 $SU(2)$ 中的任意一个元素都可以写成如下形式:

$$U(x, y) = \begin{pmatrix} x & y \\ -\bar{y} & \bar{x} \end{pmatrix} \qquad |x|^2 + |y|^2 = 1,$$

特别的我们有流形间的同构 $SU(2) \cong S^3$.

泡利矩阵. 定义如下矩阵:

$$\sigma^1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma^2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma^3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

注意到 $M_0 = \mathbb{R}\sigma^1 + \mathbb{R}\sigma^2 + \mathbb{R}\sigma^3$ 是所有迹零的二阶复 Hermitian 矩阵.$\forall (x_1, x_2, x_3)^T \in \mathbb{R}^3, (x_1, x_2, x_3)^T \leftrightarrow H_x := \sum_{i=1}^3 x_i\sigma^i$, 由于在 M_0 上具有矩阵 A(基: $\sigma^1, \sigma^2, \sigma^3$) 的线性变换对应到 $\mathbb{R}^3$ 同样具有矩阵 A(基: e_1, e_2, e_3) 的线性变换, 因此我们可以简单地将这两个空间等同起来.

令 $g \in SU(2)$, 定义如下映射: $\Phi_g : H_x \mapsto gH_xg^{-1}$,$tr(gH_xg^{-1}) = tr(H_x) = 0$, $(gH_xg^{-1})^* = (g^{-1})^*H_x^*g^* = gH_xg^{-1} \Rightarrow \Phi_g(H_x) = gH_xg^{-1} \in M_0$. 又有 $\Phi_g(H_{\alpha x} + H_{\beta y}) = \alpha\Phi_g(H_x) + \beta\Phi_g(H_y)$, 即 Φ 是 M_0 上的线性算子.

设 $\Phi_g(H_x) = H_y$, 我们说明 Φ 是 $\mathbb{R}^3$ 上的正交变换.$\Phi_g(x) \cdot \Phi_g(x) = y \cdot y = y_1^2 + y_2^2 + y_3^2$ =-det $H_y = -\det\Phi_g(H_x) = -\det gH_xg^{-1} = -\det H_x = x_1^2 + x_2^2 + x_3^2 = x \cdot x$.

容易证明 $\Phi_{gh} = \Phi_g \circ \Phi_h$, 因此 $\Phi : g \mapsto \Phi_g$ 是 SU(2) 到 O(3) 的同态, 其 kernel 满足 $gH = Hg, \forall H \in M_0$, 即 $g\sigma^i = \sigma^i g, 1 \le i \le 3 \Rightarrow g = \pm I_2$.

又因为:

$$\begin{aligned} U(e^{i\gamma/2}, 0)\sigma^1 U(e^{i\gamma/2}, 0)^{-1} = cos\varphi\sigma^1 + sin\varphi\sigma^2, \\ U(e^{i\gamma/2}, 0)\sigma^2 U(e^{i\gamma/2}, 0)^{-1} = -sin\varphi\sigma^1 + cos\varphi\sigma^2, \\ U(e^{i\gamma/2}, 0)\sigma^3 U(e^{i\gamma/2}, 0)^{-1} = \sigma^3. \end{aligned}$$

因此 $\Phi(U(e^{-i\gamma/2}, 0)) = R_z(\gamma)$.

而我们又有 $g = hU(e^{-i\gamma/2}, 0)h^{-1}$,$h$ 是某个酉矩阵. 因此 $\det\Phi_g$ =$\det(\Phi_h\Phi_{U(e^{-i\gamma/2},0)}\Phi_{h^{-1}}) = 1$(此时的 Φ_h 的定义和上面是一样的).

同样可以计算 $\Phi(U(cos\alpha/2, -isin\alpha/2)) = R_x(\alpha), \Phi(U(cos\beta/2, -sin\beta/2)) = R_x(\alpha)$.

综上 $SU(2)/Z_2 \cong SO(3)$. □

第四次习题课

伍文超 MJTDX USTC

1：(1) 证明 $GL_2(2)$ 同构于 S_3.
(2) 证明 $PGL_2(3) \cong S_4$. 从而也有 $PSL_2(3) \cong A_4$ 因为其是 $PGL_2(3)$ 的指数为而的子群.
$GL_n(\mathbb{F}_q)$ 简记为 $GL_n(q)$,q 是素数的幂.
证明: (1): 考虑：

$$GL_2(2) \curvearrowright (\mathbb{Z}_2 \oplus \mathbb{Z}_2)\backslash\{(0,0)^T\} \longrightarrow (\mathbb{Z}_2 \oplus \mathbb{Z}_2)\backslash\{(0,0)^T\}$$

上述作用是合理的, 因为 $GL_2(2)$ 中任意一个元素给出 $S = (\mathbb{Z}_2 \oplus \mathbb{Z}_2)\backslash\{(0,0)^T\}$ 的一个置换 (元素是可逆矩阵). 通过计算可知 $A \in GL_2(2)$ 在 S 上作用平凡当且仅当 $A = I_2$. 因此有单射 $GL_2(2) \hookrightarrow S_3$. 最后由 $|GL_2(2)| = 2 \cdot 3 = 6 = |S_3|$ 可知二者同构.

(2) 类似于 (1), 考虑 $\mathbb{Z}_3 \oplus \mathbb{Z}_3$ 中的四个子集 $V_i = \{a(i,1) \in \mathbb{Z}_3 \oplus \mathbb{Z}_3 | a = 0,1,2\}, i = 0,1,2, V_\infty = \{a(1,0) \in \mathbb{Z}_3 \oplus \mathbb{Z}_3 | a = 0,1,2\}$. 记 $S = \{V_0, V_1, V_2, V_\infty\}$. 同样的 $GL_2(3)$ 中任意一个元素给出 S 的一个置换 (合理的)，而且通过计算可知 $A \in GL_2(3)$ 在 S 上作用平凡当且仅当 A 是标量矩阵 (scalar matrices). 因此有单射 $GL_2(3)/Z(GL_2(3)) = PGL_2(3) \hookrightarrow S_4$. 最后由 $|GL_2(3)| = 24 = |S_4|$ 可知二者同构. □
Remark:(1) 类似的，我们可以取 $\mathbb{F}_q \oplus \mathbb{F}_q$ 中的 $q+1$ 个子集 (一维子空间)$V_i = \{a(i,1) \in \mathbb{F}_q \oplus \mathbb{F}_q | a = 0,1,\cdots,q-1\}, i = 0,2,\cdots,q-1, V_\infty = \{a(1,0) \in \mathbb{F}_q \oplus \mathbb{F}_q | a = 0,1,\cdots,p-1\}$，记 $S = \{V_0, V_1, V_2, \cdots,$
$V_{q-1}, V_\infty\}$. 同样的 $GL_2(q)$ 中任意一个元素给出 S 的一个置换 (合理的), 且只有标量矩阵给出平凡作用，因此我们得到单射 $PGL_2(q) \hookrightarrow S_{q+1}$
(2) 在线性代数中，我们定义射影空间为 $\mathbb{R}^n$ 的所有一维子空间 (直线) 构成的集合.$n = 2$ 时就是射影直线，$n = 3$ 时就是射影平面. 在此处我们可以类似的命名 (1) 中的集合为 $\mathbb{F}_q$ 上的射影直线，不妨记为 $PL(q)$. 根据我们的定义，$PL(q) = \{V_0, V_1, V_2, \cdots, V_{q-1}, V_\infty\} \leftrightsquigarrow \mathbb{F}_q \bigcup \{\infty\}$(将每一个直线视作一个点)，我们将二者视为恒等的. 如果取 $\mathbb{F}_q^3$ 的二维子空间构成的集合则是射影平面 (有限射影平面, 有 $q^2 + q + 1$ 个点和线，每条线上 $q+1$ 个点，每个点关联 $q+1$ 条线.)
(3) 任意 $A = \begin{pmatrix} a & b \\ c & c \end{pmatrix} \in GL_2(q)$, 我们有 $A(k(i,1)^T) = k(ai+b, ci+d)$,$A(k(1,0)^T) = k(a,0)$. 等价的：

$$GL_2(q) \curvearrowright PL(q) \longrightarrow PL(q)$$

$$z \longrightarrow \frac{az+b}{cz+d} = \frac{a+b/z}{c+d/z}$$

2: 旋转群 SO(3) 是单群 (SO(n)?).
证明: 第一次习题课我们证明了 $SU(2)/\{\pm I_2\} \cong SO(3)$, 第四次作业说明了 $SU(2)$ 的包含 $\{\pm I_2\}$ 的正规子群和 $SO(3)$ 的正规子群是一一对应的，因此我们只需要说明 $SU(2)$ 的真包含 $\{\pm I_2\}$ 的正规子群 G 等于 $SU(2)$. 回顾：

$$SU(2) = \left\{ \begin{pmatrix} x & y \\ -\bar{y} & \bar{x} \end{pmatrix} \middle| |x|^2 + |y|^2 = 1, x, y \in \mathbb{C} \right\}$$

从线性代数我们知道任意 $A \in SU(2)$ 酉相似于对角矩阵, 特征多项式有共轭复根或都为 ± 1, 记为 $B_\varphi = \begin{pmatrix} e^{i\varphi} & 0 \\ 0 & e^{-i\varphi} \end{pmatrix}, \varphi \in [0, 2\pi)$. 因此 $SU(2)$ 的每个共轭类都含有对角矩阵, 而由于正规子群是共轭类的无交并, 因此 G 包含一个对角矩阵 ($\neq \pm I_2$), 记为 $B_{\alpha_0}, \alpha_0 \neq 0, \pi$. 自然的 $B_{\alpha_0}^{-1} = B_{2\pi-\alpha_0} \in G$, 故设 $0 < \alpha_0 < \pi$. 考虑 B_{α_0} 和 $\forall A \in G$ 的换位子:

$$\begin{aligned}
[B_{\alpha_0}, A] &= B_{\alpha_0} A B_{\alpha_0}^{-1} A^{-1} \\
&= \begin{pmatrix} e^{i\alpha_0} & 0 \\ 0 & e^{-i\alpha_0} \end{pmatrix} \begin{pmatrix} x & y \\ -\bar{y} & \bar{x} \end{pmatrix} \begin{pmatrix} e^{-i\alpha_0} & 0 \\ 0 & e^{i\alpha_0} \end{pmatrix} \begin{pmatrix} \bar{x} & -y \\ \bar{y} & x \end{pmatrix} \\
&= \begin{pmatrix} |x|^2 + |y|^2 e^{i2\alpha_0} & (e^{i2\alpha_0} - 1)xy \\ (1 - e^{-i2\alpha_0})\bar{x}\bar{y} & |x|^2 + |y|^2 e^{-i2\alpha_0} \end{pmatrix}.
\end{aligned}$$

$tr([B_{\alpha_0}, A]) = 2|x|^2 + |y|^2(e^{i2\alpha_0} + e^{-i2\alpha_0} = 2(1 - |y|^2) + 2|y|^2(-2sin^2\alpha_0 + 1) = 2(1 - 2|y|^2 sin^2\alpha_0)$. 设 $[B_{\alpha_0}, A]$ 和 B_{α_1} 共轭, 故 $e^{i\alpha_1} + e^{-i\alpha_1} = 2cos\alpha_1 = 2 - 4|y|^2 sin^2\alpha_0 \Rightarrow cos\alpha_1 = 1 - 2|y|^2 sin^2\alpha_0 \in [1 - 2sin^2\alpha_0, 1] = [cos2\alpha_0, 1]$, 因为 $0 \leq |y|^2 \leq 1$.

不妨设 $2\alpha_0 \leq 2\pi - 2\alpha_0$(另一边类似) , 则有 α_1 可以取遍 $[0, 2\alpha_0], [2\pi - 2\alpha_0, 2\pi]$. 也就是说 $B_{\alpha_1} \in G, \forall \alpha_1 \in [0, 2\alpha_0]$. 因为对于任意的 $\alpha > 0$, 存在 $n \in \mathbb{Z}_{\geq 0}$ 使得 $0 < \alpha/n \leq 2\alpha_0$, 因此 $B_\alpha \in G, \forall \alpha$, 即 $G = SU(2)$. □

Remark: 一般的,SO(2n+1) 是单群,SO(2n)/$\{\pm I_{2n}\}$ 是单群.

3: 如果域 F 有至少四个元素, 则 $SL_2(F)/\{\pm I_2\}$ 是单群 (一般的, $PSL_n(F_p)$ 呢?).

证明: 我们先给出一些需要用到的子群:

$$U = \left\{ u(x) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \middle| x \in F \right\}$$

$$V = \left\{ v(x) = \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \middle| x \in F \right\}$$

$$D = \left\{ d(x) = \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \middle| x \in F^* \right\}$$

$$B = DU = UD = \left\{ \begin{pmatrix} x & y \\ 0 & x^{-1} \end{pmatrix} \middle| x \in F^*, y \in F \right\}$$

.

取 $w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, 断言 $G = SL_2(F)$ 有双陪集分解 $G = B \bigcup BwB$. 实际上:

(a)$\forall A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$, 若 $c = 0$, 则 $A \in B$; 若 $c \neq 0$, 则 $\begin{pmatrix} x & y \\ 0 & x^{-1} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} f & g \\ 0 & f^{-1} \end{pmatrix} = \begin{pmatrix} -yf & -yg + xf^{-1} \\ -x^{-1}f & -x^{-1}g \end{pmatrix}$, 总是可以取到 x, y, f, g 使得其乘积为 A.

(b)$A \in B \bigcap BwB \Rightarrow -x^{-1}f = 0$, 矛盾.

再考虑 $[G,G]=\{ABA^{-1}B^{-1}\in G|A,B\in G\}$, 容易证明 $[G,G]$ 是 G 的正规子群. $d(a)u(b)d(a)^{-1}u(b)^{-1}=\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix}\begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} 1 & b(a^2-1) \\ 0 & 1 \end{pmatrix}$ 因此只需要 $a^2\neq 1$, 则可以得到 $U\subset[B,B]\subset U$, 故 $U=[B,B]\leq[G,G]$. 进而 $wUw^{-1}=V\leq[G,G]\Rightarrow w=\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\in[G,G]\Rightarrow[G,G]=G$.

设 K 是 G 的正规子群, 则 $B\leq KB$. 若 $B=KB\Rightarrow K\in B\Rightarrow K=CKC^{-1}\subset\bigcap_{A\in G}ABA^{-1}=\{\pm I_2\}$.

若 $B\neq KB$, 则存在 $h\in KB\backslash B$ 且 $h=b_1wb_2\Rightarrow w\in KB\Rightarrow KB=G$. 从而 $w=kb, k\in K, b\in B\Rightarrow V=wUw^{-1}=kbUb^{-1}k^{-1}=kUk^{-1}=kk_1U\subset KU\Rightarrow KU=G$, 故 $G/K=KU/K\cong U/U\bigcap K$ 是交换群, 因此 $G=[G,G]\leq K\Rightarrow K=G$.

□

Remark: 一般的, 若 $n\geq 3$, 则 $PSL_n(q)$ 是单群 (利用 Iwasawa 定理).

第七次习题课

伍文超 MJTDX USTC

1: 证明 $S_n(n \geq 5)$ 没有指数为 i 的子群, 其中 $2 < i < n$. 而且 S_n(任意 n) 的指数为 n 的子群同构于 S_{n-1}(在以前的问题中我们已经知道 $S_n(n \geq 2)$ 指数为 2 的子群只有 A_n).

证明: 设 H 是指数为 $i, 2 \leq i \leq n$ 的子群, 考虑 S_n 在 H 的全体左陪集 S 上的左乘作用给出的群作用, 则我们有群同态 $\varphi : S_n \to Sym(S) \cong S_i$, 并且通过同态第一基本定理 $ker\varphi$ 是 $S_n(n \geq 5)$ 的正规子群, 故 $ker\varphi = 1, A_n$ 或者 S_n. 而 $ker\varphi = 1, A_n, S_n$ 意味着 $i = n, 2, 1$.

若 H 是指数为 n 的子群, 则 H 作用在 S 上有一个固定点 H, 且由于 φ 是同构,H 中的每一个元素给出 $S - \{H\}$ 上不同的变换, 即有嵌入 $H \hookrightarrow S_{n-1}$. 通过比较阶数, 即可知此为同构. □

2: 利用群的表现证明总存在 p^3 阶非阿贝尔群.

(1) 例子: $GL(n, \mathbb{F}_p)$ 的 Sylow p-子群, 例如 $\begin{pmatrix} 1 & \mathbb{F}_p & \mathbb{F}_p \\ 0 & 1 & \mathbb{F}_p \\ 0 & 0 & 1 \end{pmatrix}$

(2) 分析:

(a)若 $p \neq 2$,G 是 p^3 阶群, 则其有非平凡中心 $Z(G)$, 由第四次作业 11 和该题前两问知 $|Z(G)| = p, G/Z(G) \cong \mathbb{Z}_p \times \mathbb{Z}_p$. 令 $G/Z(G) =< a, b | a^p = b^p = 1, ab = ba >$, 取 a 和 b 在 G 中的原像 x, y, 则 $[x, y] := xyx^{-1}y^{-1} \in Z(G)$.

(i) 若 $[x, y] = 1$, 则 $\langle x, y, Z(G)\rangle$ 生成 G, 故 G 是阿贝尔群, 因此 $< [x, y] >= Z(G) = G'$.

(ii) 若 $ord(x) = ord(y) = p$, 则由于 $xy = [x, y]yx = yx[x, y]$,G 中元素都可以写成 $x^i y^j [x, y]^k, 1 \leq i, j, k \leq p$ 的形式, 因此 $G \cong \langle x, y | x^p = y^p = [x, y]^p = 1, [[x, y], x] = [[x, y], y] = 1\rangle \cong \langle x, y, z | z = [x, y], x^p = y^p = z^p = 1, [z, x] = [z, y] = 1\rangle$. 可以看出此类即是我们 (1) 中给出的例子.

(iii.1) 若 G 中存在 $ord(x) = p^2$ 的元素, 令 $X = \langle x\rangle$, 则总存在 $y \in G - X$ 使得 $y^p \in X$. 事实上, 若 $ord(y) = p$, 则显然,$ord(y) = p^2$, 则由于 $x^i y^j, 1 \leq i, j \leq p^2$ 计数 p^4 次, 故存在 $i—_1, i_2, j_1, j_2$ 使得 $x^{i_1} y^{j_1} = x_{i_2} y^{j_2} \Rightarrow x^{i_3} = y^{j_3}$ 这同时意味着 $(i_3, p^2) = (j_3, p^2) = p$, 也就是说 $y^p \in \langle x^p\rangle \leq X$. 由于 G 非交换, 因此 $C_G(X) = X$ 是指数为 p 的子群 (lec11, 例 2.7), 因此其是 G 正规子群. 考虑 y 在 X 上的共轭作用 σ_y, 其显然是一个非平凡的自同构, 因为 $ord(y^{-1}xy) = ord(x) = p^2, y \notin X$(第三次作业). 而由第二次习题课知 $Aut(\mathbb{Z}/p^2\mathbb{Z}) \cong \mathbb{Z}_p \times \mathbb{Z}_{p-1}$ 或者 $\mathbb{Z}_2$.$y^p \in X$ 意味着 σ_y 是 p 阶自同构, 因此 $\sigma_y(x) = x^{kp}, 1 \leq k \leq p-1$, 通过选取适当的 y(因为 y 和 $\langle y\rangle$ 效果一样), 可以使得 $k = 1$, 因此 $y^{-1}xy = x^{p+1} \Rightarrow x^p y = yx^{p(p+1)} = yx^p$, 从而 $Z(G) = \langle x^p\rangle = \langle [x, y]\rangle$. 因此 $x^i y^j$ 形式的不同元素有 p^3 个, 故构成 G.

(iii.2) 若 $ord(y) = p^2$, 则 $y^p = x^{kp}, 1 \leq k \leq p-1$, 令 $z = y^{-1}x^k \notin X$, 则因为 $y^{-1}xy = x^{p+1}, i.e.[x^{-1}, y^{-1}] = x^p$, 有 $z^p = (y^{-1}x^k)^p = x^{k\sum_{i=1}^{p}(p+1)^i} y^{-p} = x^{kp}y^{-p} = 1$, 此处 $\sum_{i=1}^{p}(p+1)^i = (p+1)\frac{(p+1)^p - 1}{p} \equiv p(p+1) \equiv p(mod\ p^2)$(需要 $p \neq 2$). 因此总可以找到 $G - X$ 中的 p 阶元 y_1 满足 $y_1^{-1}xy_1 = x^{p+1}$. 因此 $G \cong \langle x, y | x^{p^2} = y^p = 1, y^{-1}xy = x^{p+1}\rangle$.

(b)若 $p = 2$, 如果其中元素都是二阶元, 则其是阿贝尔群. 故其存在 4 阶元 x, 记 $X = (x)$. 取 $y \in G - X$, 若 $ord(y) = 2$, 则结论和上面分析一样, 即有 $G \cong \langle x, y | x^4 = y^2 = 1, y^{-1}xy = x^3\rangle \cong D_4$. 若 $G - X$ 中元素都是 4 阶元, 此时和前文不同的是, 无法将其转化为 $G - X$ 中的二阶元. 但是同样地, 通过共轭作用,y 定义了一个 X 的非平凡自同构, 因此 $y^{-1}xy = x^3$,$G \cong \langle x, y | x^4 = y^4 = 1, y^{-1}xy = x^3\rangle \cong Q_8$.

Rmk: (1) 因为 $\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & n & \frac{n(n+1)}{2} \\ 0 & 1 & n \\ 0 & 0 & 1 \end{pmatrix}$, 所以 $p \neq 2$ 时, 这些矩阵都是 p 阶元, 但是 p 为 2 时, 就存在 4 阶元, 根据二阶元的数量可知此时其同构于 D_4.

(2) 同样地,$p=2$ 时,$G-X$ 中的 4 阶元无法转化成二阶元,$x^{-1}yx^{-1}y=x^{-2}[x,y]y^2=y^2=x^2,(xy)^2=x^2$, 故 Xy 中无二阶元.

3: 令 $G=\langle x_i,i\in\mathbb{Z}_{>0}|\,x_n^n=x_{n-1},n>1\rangle$, 证明 $(G,\cdot)\cong(\mathbb{Q},+)$.
证明: 考虑群同态 $\varphi:G\to Q$, 其由 $x_n\mapsto\frac{1}{n!},n>0$ 给出, 可知其是满射 (因为 $\{\frac{1}{n!}\}_{n=1}^{\infty}$ 生成 $\mathbb{Q}$), 因此只需要证明 φ 是单同态即可. 由于 $x_n^n=x_{n-1}$, 因此 G 是交换群, 且其中元素 x 都有形式: $\prod_{i=1}^k x_{n_i}^{s_i},0\le s_i<n_i,1\le i\le k,s_i\in\mathbb{Z}$. 因此 $\varphi(x)=\sum_{i=1}^k\frac{s_i}{n_i!}.\varphi(x)=0$ 当且仅当 $\sum_{i=1}^k\frac{s_i}{n_i!}=0$ 当且仅当 $m+\frac{s_k}{n_k}=0,m\in\mathbb{Z}$, 因此 $n_k=1,s_k=0$, 即 $x=1$. □

4: 给定生成元 $X=\{x_0,x_1,\cdots,x_n,\cdots\}$, 令 F 是 X 上的自由阿贝尔群,R 为包含 $\{px_0,x_0-px_1,x_1-px_2,\cdots,x_{n-1}-px_n,\cdots\}$ 的最小正规子群,p 为一素数,$G=F/R$, 记 $a_n=x_n+R$.
(1) 证明:$\forall x\in G,\exists n\ge0$ 使得 $p^nx=0$.
(2) $a_n\ne0,\forall n\ge0$ 且所有的 a_n 是互异的, 从而 G 是一个无限群.
(3) 证明 G 的每个真子群都是有限循环群.
(4) 对于每一个正整数 n,G 有唯一的 p^n 阶子群.
(5) 令 $U_p=\{e^{\frac{2\pi ik}{p^n}}|k\in\mathbb{Z},n\ge0\}\le\mathbb{C}$ 是所有 p^n 次单位根构成的乘法群, 证明 $G\cong U_p$.
我们将上述群 G 记为 $\mathbb{Z}(p^\infty)$.
证明: (1) $p^{n+1}x_n=px_0\in R$, 因此 $p^{n+1}a_n=0,\forall n\ge0$. 由于 $pa_{n+1}=a_n$, 因此 G 是交换群, 其中元素都有 $a=\sum_{i=1}^k m_ia_i$ 的形式. 故 p^{k+1} 零化 a.
(2) 若 $a_0=0$, 则 $x_0\in R$. 而我们知道 $F\cong\otimes_{i\in X}\mathbb{Z}$, 因此 $x_0=\sum_{i=1}^k m_i(x_{i-1}-px_i)+m_0px_0=(m_0p+m_1)x_0+\sum_{i=1}^{k-1}(m_{i+1}-m_ip)x_i+m_kpx_k,m_j\in\mathbb{Z},j\ge0$. 故 $m_0p+m_1=1,m_{i+1}=m_ip1\le i\le k-1,m_kp=0$. 因此 $1=m_0p$, 矛盾. 类似的可以证明 $a_n\ne0$.
若 $a_n=a_m,m\ge n$, 则 $a_n=p^{m-n}a_m\Rightarrow(1-p^{m-n})a_m=0$, 乘以一个合适的 $p^i(\ne0)$ 可以得到 $p^i=0$, 矛盾. 因此 a_n 是互异的. 从而 G 是无限群.
(3) 设 $H\le G$, 若 H 含有无限个 a_n, 则由 $pa_n=a_{n-1}$ 可知 H 含有所有的 a_n,$H=G$. 若其只含有限个 a_n. 若 $a=\sum_{i=1}^k m_ia_i\in H,0\le m_i<p,m_k\ne0$, 则 $p^ka=p^km_ka_k=m_ka_0\in H\Rightarrow a_0\in H\Rightarrow m_ka_1=p^{n-1}a-m_{k-1}a_0\in H\Rightarrow a_1\in H$, 依次即可得 $H=\langle a_0,a_1,\cdots,a_m\rangle=\langle a_m\rangle$, 即 H 是有限循环群.
(4) 从 (3) 即可得知 G 的有限子群都是形如 $\langle a_m\rangle$ 的 p^{m+1} 阶循环群, 因此 p^n 阶子群是唯一的.
(5) 易知 $R_p\cong Z[\frac{1}{p}]/Z\cong G$. 第一个同构是自然的, 第二个同构类似于上面那个问题. □
Rmk: $Q/Z\cong\oplus_p\mathbb{Z}(p^\infty)$,$\mathbb{Q}/\mathbb{Z}_{(p)}\cong Z(p^\infty)$, 此处 $\mathbb{Z}_{(p)}$ 代表 p 进整数环.

5: 令 $A=\begin{pmatrix}0&1\\-1&0\end{pmatrix},B=\begin{pmatrix}1&1\\0&1\end{pmatrix}$, 我们在第三次作业证明了 A,B 是 $SL_2(\mathbb{Z})$ 的一组生成元. 令 $C=AB^{-1}=\begin{pmatrix}0&1\\-1&1\end{pmatrix}$, 则 $SL_2(\mathbb{Z})$ 也可以由 A,C 生成. 因此我们有自然群同态 $f:G:=\langle x,y|x^4=1,x^2=y^3\rangle\to SL_2(\mathbb{Z})(x\mapsto A,y\mapsto C)$ 并且 f 诱导出群同态 $g:H:=\langle x,y|x^2=y^3=1\rangle\to PSL_2(\mathbb{Z})$.
(1) 证明 $\langle x,y|x^4=1,x^2=y^3\rangle\cong\langle a,b|aba=bab,(aba)^4=1\rangle$.
(2) 证明 f 是单射当且仅当 g 是单射, 证明 f 是满射当且仅当 g 是满射.
(3) 尝试证明 f 和 g 都是群同构.
证明: (1) 容易看出 (分析一下 relations 就能看出): 由 $\varphi:x\mapsto aba,y\mapsto ab$,$\phi:a\mapsto y^{-1}x,b\mapsto xy^{-1}$ 定义的映射是群同态, 且二者复合都是恒等群同态, 因此两群同构.
(2)$f:x\mapsto A,y\mapsto C$,$A^4=I_2,A^2=C^3$. 由于 $x^2\in C(G),x^2=-I_2$, 因此 f 诱导出 $\bar{f}=g:G/<x^2>=H\to SL_2(\mathbb{Z})/\{\pm I_2\}\cong PSL_2(\mathbb{Z})$. 因此从这样的映射定义出发知 f 是单

射 (满射) 则显然 g 是单射 (满射),f 不是单射 (注意到 $x^2 \notin ker f$) 则 g 不是单射. 若 g 是满射, 则任意 $A \in SL_2(\mathbb{Z}), \exists X \in H,\ s.t\ g(X) = \bar{A}, \exists Y \in G\ s.t.\ \pi_2(A) = (A) = g(X) = g\pi_1(Y) = \pi_2 f(Y) \Rightarrow A^{-1} f(Y) \in ker\pi_2 = \{\pm I_2\}$, 故 f 是满射.

(3) 我们证明 f 是满射且 g 是因此 f 和 g 都是同构.f 是满射因为 $A, , C$ 生成 $SL_2(\mathbb{Z})$(第三次作业第 4 题, 第二次习题课). 下面说明 g 是单射.

H 中的元素都可以写成如下形式 $w = y^{\epsilon_1} x y^{\epsilon_2} x \cdots y^{\epsilon_{r-1}} x y^{\epsilon_r}, xw, wx, xwx, x, \epsilon_i \in \{\pm 1\}, 1 \le i \le r$. 又有 $x \notin kerg, xwx = xwx^{-1}, xwxx^{-1} = xw$, 所以只需要证明 $\{w, wx\} \bigcap kerg =$.

我们有 $g(y^{-1}x) = g(y^2)g(x) = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}^2 \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix} = \bar{B}, g(yx) = A\bar{C}B.$ $(i.e.[1, 0; -1, 1])$. 令 $D = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, 则 $g(wx) = g(y^{\epsilon_1} x y^{\epsilon_e} x \cdots y^{\epsilon_r} x) = \prod_{i=1}^{r} g(y^{\epsilon_i} x) = A^{t_1} B^{t_2} \cdots A^{t_l} A^{t_l} \neq \bar{1}$, 这是因为 $A^{t_1} B^{t_2} \cdots A^{t_l} A^{t_l}$ 的非对角元素非零.

若 $g(w) = \bar{q}$, 则 $g(wx) = g(w)g(x) = g(x)$, 得到矛盾因为 $A^{t_1} B^{t_2} \cdots A^{t_l} A^{t_l}$ 的元素全正, 因此 $g(wx)$ 对应元素的代表元里的元素全正或者全负.

综上,g 是单射. 因此我们证明了所需结论.

□

6: 设 G 是一个无限阿贝尔群.
(1) 若 G 的每一个真子群是有限群, 则存在素数 p 使得 $G \cong \mathbb{Z}(p^\infty)$.
(2) 若 G 同构于每一个真子群, 则 $G \cong \mathbb{Z}$.
(3) 若 G 同构于每个非平凡商群, 则 $G \cong \mathbb{Z}(p^\infty)$.
(4) 若 G 的每个非平凡商群是有限的, 则 $G \cong \mathbb{Z}$.

证明: (1) p 为任一素数, 定义 G 的 p 准素部分为 $G_p = \{g \in G | p^n g = 0, \exists n \in \mathbb{N}\}$, 易证 G_p 是 G 的子群且 $G = \oplus_p G_p$. 如果有 2 个或以上数量的素数使得 $G_p \neq 0$, 则每个 G_p 都是有限群, 且有无穷个 p 使得 $G_p \neq 0$, 但是此时 G 有无限真子群. 因此只能存在某个素数 p 使得 $G = G_p$. 令 $G[p] = \{g \in G | pg = 0\}$, 则 $G[p] = ker(p : G \to G)$. 显然 pG 和 $G[p]$ 都是 G 的子群. 若 $p[G]$ 有限, 则 $G[p] = G$ 是无限的, 但是这样意味着 G 存在无限真子群 $\oplus \mathbb{Z}_p$. 因此 $G = pG$, 且 $|G[p^n]| = |G[p]|^n$. 而由 Cauchy 定理可知 $|G[p]| = p^k$ 因为其内所有非零元素都是 p 阶的.

引理 (GTM148,10.27): 若 G 和 H 是可除 p 准素群, 则 $G \cong H \Leftrightarrow G[p] \cong H[p]$

因此 $G \cong \oplus_{i=1}^{k} Z(p^\infty)$, 只可能 $k = 1$, 故命题得证.

也可以考虑 G 中含有任意 p^k 阶群因为 $G = pG$, 因此 $G = \text{limit } \mathbb{Z}/p^k\mathbb{Z} \cong Z(p^\infty)$.

(2) 因为 G 同构与每一个真子群, 因此 $G \cong \langle x \rangle \cong \mathbb{Z}, \forall x \in \mathbb{Z}$.

(3) 定义 $tor(G) = \{g \in G | ord(g) < \infty\}$,$tor(G)$ 中的元素称为扭元. 若 $tor(G) = 0$, $\forall x \in G, G/(nx) \cong G$ 但是 $G/(nx)$ 有扭元 x. 因此 $tor(G) \neq 0$. 断言 $tor(G) = G$, 否则 $G/tor(G)$ 是无扭模但是 G 有扭元, 矛盾. 因此 G 中元素都是扭元 $\Rightarrow G = \oplus_p G_p$. 而 G/G_p 中无 p 准素部分, 因此存在唯一的素数使得 $G = G_p$. 类似于 (1), 有 $G \cong G/G[p] \cong pG$(否则利用 Zorn 引理可证明 $G \cong G[p] \cong \oplus_{i \in I} \mathbb{Z}/p\mathbb{Z}$, 不同构于任意非平凡商群), 从而 $G \cong \mathbb{Z}(p^\infty)$.

(4) 任取非零 $x \in G$,$G/(x) = \{a_1(x), \cdots, a_n(x)\}$ 是有限群, 故 $ord(x) = \infty$ 且 G 是有限生成阿贝尔群, 由结构定理可知 $G \cong \oplus_i \mathbb{Z} \oplus \oplus_m \mathbb{Z}_m$, 因此 $G \cong \mathbb{Z}$. □

Rmk: 若不预先假定 G 是阿贝尔群, 则结论不一定成立. 如 $G = SO(3)$, 一个无限单群, 因此无非平凡商群,(3)(4) 不成立. (2) 则是任意情况都成立. 至于 (1), 例如 Tarski monster groups, 即每一个真子群都是有限 p 阶循环群的无限单群.

7 :S_n, A_n 的表示老师已经讲过,也可以参考近世代数 300 题或者 GTM80< *A course in the theory of group* >,p52.

第十次习题课

1:(1) 设 R 是一含幺环,$f: R \to \mathbb{Z}$ 是任意一个幺环同态 $f(1_R) = 1$. 证明作为群, 有同构 $R \cong ker f \oplus \mathbb{Z}$.
(2) $\varphi: R \to ker f \oplus \mathbb{Z}, r \mapsto (r - f(r)1_R, f(r))$ 给出一个群同构. 我们可以给 $ker f \oplus \mathbb{Z}$ 赋予环结构使得 φ 是环同构, 即满足 $\varphi(r_1 r_2) = \varphi(r_1)\varphi(r_2)$, 请给出 $ker f \oplus \mathbb{Z}$ 上的乘法结构满足上述性质. 你发现了什么?
证明: (1): (2) 中给的映射即为我们所求的群同构.

(2): 通过简单的演算不难得知乘法结构可以由 $(r_1, n_1)(r_2, n_2) = (r_1 r_2 + r_1 n_2 + r_2 n_1, n_1 n_2)$ 给出. 这正是我们之前将 R 嵌入到 $R \times \mathbb{Z}$ 中时, 环 $R \times \mathbb{Z}$ 中的乘法.

□

2:$\mathbb{R}$ 上的有限维可除结合代数只有三种 $\mathbb{R}, \mathbb{C}, \mathbb{H}$(同构意义下).
证明: (1):$\mathbb{R}$ 上的二维可除交换代数 (扩域) 只有 $\mathbb{C}$. 设 $\mathbb{K} = span_{\mathbb{R}}\{1, x\}$, 则 $x^2 = ax + b \Rightarrow (x + c)^2 + d = 0$ 且 $d > 0$(若 $d = 0$, 由于 $\mathbb{K}$ 是可除代数因此 $x + c = 0 \Rightarrow x \in \mathbb{R}$; 若 $d < 0$, 因为 $(x + c)^2 = -d$ 的两个根都在 $\mathbb{R}$ 上, 因此 $x \in \mathbb{R}$). 不防令 $y = (x + c)/\sqrt{d}$, 则有 $\mathbb{K} = span_{\mathbb{R}}\{1, y\}$ 且 $y^2 = -1$. 因此 $\mathbb{K} \cong \mathbb{C}$.

(2): $\mathbb{R}$ 上的有限维可除交换代数 $\mathbb{K}$ 只有 $\mathbb{R}, \mathbb{C}$ 两种情形.

(a): 若 $\mathbb{C} \leq \mathbb{K}$, 则 $\mathbb{K}$ 也是 $\mathbb{C}$ 上的有限维可除交换代数. 任取 $a \in \mathbb{K}$, 因为 $\mathbb{K}$ 是有限维空间, 因此 $\{a^i\}_{i=0}^{dim_{\mathbb{R}}}$ 肯定线性相关, 因此存在 $f(x) \in \mathbb{C}[x]$ 使得 $f(a) = 0$. 由代数基本定理可知 $a \in \mathbb{C}$, 也就是说 $\mathbb{C} = \mathbb{K}$.

(b): 和 (a) 类似, 任取 $a \in \mathbb{K}$, 存在 $f(x) \in \mathbb{C}[x]$ 使得 $f(a) = 0$. 因此 a 的最小零化多项式的次数为 1 或者 2. 若其为 1, 则 $a \in \mathbb{R}$, 否则, 类似于 (1) 的证明可知存在 $y \in \mathbb{K}$ 使得 $y^2 = -1$. 因此 $\mathbb{C} \leq \mathbb{K}$.

(3):$\mathbb{R}$ 上的可除代数只有 $\mathbb{R}, \mathbb{C}, \mathbb{H}$. 此处 $\mathbb{H} = span_{\mathbb{R}}\{1, i, j, k\}$ 满足关系 $i^2 = j^2 = k^2 = -1, ij = -ji = k, jk = -kj = i, ki = -ik = j$.

(c): 令 $\mathbb{K}(\neq \mathbb{R})$ 是 $\mathbb{R}$ 上的一个有限维可除代数且 1 是其单位元, 令 $x \in \mathbb{K} - \mathbb{R}, F = span_{\mathbb{R}}\{1, x\}$ 是 $\mathbb{R}$ 的一个二维子空间, F_1 是 $\mathbb{K}$ 中包含 F 的且其内元素可交换的维数极大子空间 (因为 F 本身是交换子空间, 暂时还不知道 F_1 是不是一个子环). 若 $a, b \in F_1$, 那么 $F_1 + \mathbb{R}(ab)$ 是包含 F 的交换子空间, 因此 $ab \in F_1$. 若 $a, b \in F_1$, 则 $ab = ba \Rightarrow ba^{-1} = a^{-1}b \Rightarrow a^{-1} \in F_1$. 因此 F_1 是 F_1 的交换可除子代数, 即一个包含 $\mathbb{R}$ 的域. 故 $F_1 = \mathbb{C}$. 因此我们不妨选定 $\mathbb{K}$ 中一元素使得 $i^2 = -1$ 且将 $span_{\mathbb{R}}\{1, i\}$ 视为 $\mathbb{C}$

(d):i 在 $\mathbb{K}$ 上的右乘作用给出一个 $\mathbb{K}$(作为复线性空间) 上的线性变换, 记改变换为 T, 即 $Tx = xi, \forall x \in \mathbb{K}. T^2 = -id$ 意味着 T 恰有两个特征根 $i, -i$, 记对应的特征子空间为 V_i, V_{-i}. 显然 $\mathbb{K} = V_i \oplus V_{-i}$ 因为这两个子空间交为 0 且 $x = \frac{x - ixi}{2} + \frac{x + ixi}{2}$. 而由 D_i 的定义可知其内任意元素都和 $\mathbb{C}$ 中元素可交换, 因此由 (1) 可知 $V_i = \mathbb{C}$.

(e) 容易验证 $\forall a, b \in V_{-i}, c \in V_i, ab, ba \in V_i, ac, ca \in V_{-i}$. 而我们知道 $\mathbb{K}$ 有限维可除代数, 因此其内任意一个元素 a 的左乘作用给出 $\mathbb{K}$ 上一个线性同构, 取 $a \in V_{-i}$, 则有 $dim_{\mathbb{R}} V_i = dim_{\mathbb{R}} V_{-i}$. 故 $\mathbb{K}$ 是实四维空间.

(f) 由 (c) 可知, 任意 $a \in V_{-i}$, $span_{\mathbb{R}}\{1, a\}$ 同构于 $\mathbb{C}$. 因此 $a^2 \in span_{\mathbb{R}}\{1, a\} \bigcap span_{\mathbb{R}}\{1, i\} = \mathbb{R}$, 且 $a^2 < 0$. 通过适当的变换我们可以选取 $j \in V_{-i}$ 使得 $j^2 = -1$. 定义 $k = ij$, 则有 $k^2 = -1, jk = -kj = i, ki - ik = j$, 且 j, k 是线性无关的 ($ej + fk = 0 \Rightarrow ej^2 + fkj = -e - fi = 0$). 因此 $\mathbb{K} \cong \mathbb{H}$.

□

Remark: 利用同论论的证明可以参考 <Algebraic Topology>,Allen Hatcher,Theorem2B.5. 一个和 S^3 上向量丛有联系解释可以看 Hatcher 的 <Vector bundles and K-theory>,P9,P11 和 Theorem2.16, 说明 S^n 拥有平凡切丛当且仅当 $n = 0, 1, 3, 7$, 对应到实可除代数的维数 1,2,4,8(Cayley octonion,a non-associative algebra).