1. (1) $\forall A\in SO(3)$，A 正交相似于 $\begin{pmatrix}\cos\theta & -\sin\theta & 0\\ \sin\theta & \cos\theta & 0\\ 0 & 0 & 1\end{pmatrix}$ 即关于过渡正交阵的直角坐标系，A 相当于旋转.

$$\{b_1,b_2,b_3\}\xrightarrow{\{b_1,b_2,b_3\}}\{b_1',b_2',b_3\}$$ 设 $A=(\alpha_1,\alpha_2,\alpha_3)$

任一直角坐标系(右手系)即 $\{\alpha_1,\alpha_2,\alpha_3\}$ 均可由初始坐标系 $\{e_1,e_2,e_3\}$ 通过三次旋转得到：

首先，令 α_1,α_2 的平面交 $\{e_1,e_2\}$ 平面上单位向量为 γ_0

则 $\gamma_0\perp\alpha_3$，$\gamma_0\perp e_3$，实际上 $\gamma_0=e_3\times\alpha_3$ (外积)

$$\{e_1,e_2,e_3\}\xrightarrow{R_{e_3}(\gamma)}\{\gamma_0,e_2',e_3\}\xrightarrow{R_{\gamma_0}(\beta)}\{\gamma_0,e_2'',\alpha_3\}\xrightarrow{R_{\alpha_3}(\alpha)}\{\alpha_1,\alpha_2,\alpha_3\}$$

γ 是 e_1 和 γ_0 的夹角，β 是 e_3 和 α_3 的夹角

α 是 γ_0 和 α_1 夹角.

注意 $R_{\gamma_0}(\beta)=R_{e_3}(\gamma)R_{e_1}(\beta)R_{e_3}^{-1}(\gamma)$

$$R_{\alpha_3}(\alpha)=R_{e_3}(\gamma)R_{e_1}(\beta)R_{e_3}(\alpha)R_{e_1}(\beta)^{-1}R_{e_3}(\gamma)^{-1}$$

$$\Rightarrow\{e_1,e_2,e_3\}\xrightarrow{R_{e_3}(\gamma)R_{e_1}(\beta)R_{e_3}(\alpha)}\{\alpha_1,\alpha_2,\alpha_3\}$$

即 $A=R_{e_3}(\gamma)R_{e_1}(\beta)R_{e_3}(\alpha)$.

2. (1) 由Euler定理 $\forall a\in\mathbb{Z}$, $\bar{a}\in\mathbb{Z}_p$, $(\bar{a})^{p-1}=1$

$U_p=\mathbb{Z}_p^*$ 设 $\bar{a}\in U_p$ 阶数最大 $o(\bar{a})=m$, 若 $m=p-1$ 则 U_p 是循环群. 否则, 存在 $\bar{b}\in U_p$ $o(\bar{b})=k$, k必须是m的因子, 因为 $o(\bar{a}\bar{b})=[m,k]$ 且 m最大 这样 $m\mid p-1$ 且 $x^m=\bar{1}$ 在 U_p 中有 $p-1$ 个根. x^m-1 在 $\mathbb{Z}_p$ 中有 $p-1$ 个根, 这不可能 (通过带余除法, 归纳可得)

注: G 一个有限群 $|G|=n$. $m\mid n$, 可能 $x^m=e$ 在G中有超过m个解(根) 例如 四元群 $\{e,a,b,ab \mid a^2=b^2=(ab)^2=e\}$.

(2) 因为 $|U_{p^r}|=p^{r-1}(p-1)$ 需在 U_{p^r} 中找一个阶为 p^{r-1} 的元素 $\bar{a}$ 和阶为 $p-1$ 的元素 $\bar{b}$

$\bar{a}=\overline{p+1}$, $\bar{a}^{p^{r-1}}=(\overline{p+1})^{p^{r-1}}=\sum_{k=0}^{p^{r-1}}\binom{p^{r-1}}{k}(\bar{p})^{p^{r-1}-k}$

检查 $\bar{a}^p\equiv 1 \pmod{p^2}$, $\bar{a}^{p^2}\equiv 1\pmod{p^3}$, $\cdots$, $(\bar{a})^{p^{r-1}}\equiv 1 \pmod{p^r}$

即 $\bar{a}^{p^{r-1}}=\bar{1}$ (在 $U_{p^r}\subset\mathbb{Z}_{p^r}$ 中) 且 $o(\bar{a})=p^{r-1}$.

在 U_p 中取一生成元 $\bar{b}$, 则 $b^{p-1}\equiv 1 \pmod{p}$ 设 b 在 U_{p^r} 中阶为 l, $\bar{b}^l\equiv 1 \pmod{p^r}$ 即有 $p-1\mid l$ 令 $l=(p-1)m$ b^m 在 U_{p^r} 中阶为 $p-1$. 则 $U_{p^r}=\langle\bar{a}\cdot\bar{b}\rangle$ (因为 p 奇素数, $p-1$ 和 p^{r-1} 互素).

由 扫描全能王 扫描创建

(3) $H=\{\bar{a}\in U_{2^r} \mid a\equiv 1 \pmod 4\}=\{\overline{4k+1} \mid 0\leq 4k+1<2^r\}$

$=\{\overline{4k+1} \mid 0\leq k<2^{r-2}\}$ 则 $|H|=2^{r-2}$

注 $|U_{2^r}|=2^{r-1}$

设 $a\in\mathbb{N}$ $a\equiv(2^2+1)\pmod{2^3}$ 则 $a^2\equiv 2^3+1\pmod{2^4}$

$a^{2^2}\equiv 2^4+1\pmod{2^5}, \cdots, a^{2^{r-2}}\equiv 2^r+1\pmod{2^{r+1}}$.

$\Rightarrow o(a)=2^{r-2}$. 即 $H=\langle a\rangle$

(4) 任意 $\bar{a}\in U_{2^r}$, $(a,2^r)=1$, 则 $a\equiv 1\pmod 4$ 或

$a\equiv -1\pmod 4$. 定义 $u:\{\pm1\}\times H\longrightarrow U_{2^r}$

$u(\pm1,\bar{a})=\pm\bar{a}$.

这是一个群同态且满射，两边阶数相同，因而同构.

(5) 中国剩余定理展示 $\mathbb{Z}_n \xrightarrow{\psi} \mathbb{Z}_{p_1^{r_1}}\times\cdots\mathbb{Z}_{p_k^{r_k}}$ 是一个同构.

限制到 U_n 上，检查定义合理，是满射.

(6) 由(5)显然.

D_{2n}的正规子群

$$D_{2n}=\langle a,b \mid a^n=1,\ b^2=1,\ bab=a^{-1}\rangle$$
$$=\{a^i \mid i\in\mathbb{Z}_n\}\cup\{a^ib \mid i\in\mathbb{Z}_n\}$$

设 $H\lhd D_{2n}$　若 $\forall a^ib\notin H$，则H是$\{a^i \mid i\in\mathbb{Z}_n\}$的子群. $H=\langle a^k\rangle$　$ba^kb=a^{-k}\in H$. 则~~$\{a^i,a^{-i}\}$ $\forall i\in\mathbb{Z}_n$ 是D_{2n}的正规子群. 若$|H|>2$. 则$|H|=2$或n. $m|n$~~. $k|n$. 它是正规的.

若 $\exists a^ib\in H\lhd D_{2n}$, $\Rightarrow a^{-j}(a^ib)a^j\in H$. 即 $a^{-2j+i}b\in H$ $\forall j$　若 $2\nmid n$, $(2,n)=1$　$\bar{2}$在$\mathbb{Z}_n$中可逆, 存在$\bar{t}$　$\bar{2}\cdot\bar{t}=\bar{1}$　令 $j=t(k-i)$ $\forall k$, 则 $a^kb\in H$ $\forall k\in\mathbb{Z}$.

$\Rightarrow b, a\in H$　$H=D_{2n}$.

若 $2|n$, 上述讨论已知 $a^{2j-i}b\in H$.

i为奇数, 则 $a^{2s+1}b\in H$ $\forall s\in\mathbb{Z}_n$　$H=\langle a^2, ab\rangle$

i为偶数, 则 $a^{2s}b\in H$ $\forall s\in\mathbb{Z}_n$, $H=\langle a^2, b\rangle$