证明： 若不然，则存在 $c \in \langle a\rangle \cap \langle b\rangle$，$c \neq e$。考虑 $\langle c\rangle$。由于 $c \neq e$ 且 $c, e \in \langle c\rangle$，故 $|\langle c\rangle| > 1$。又由于 $c \in \langle a\rangle$，且 $\langle a\rangle$ 是群，故由 $\langle c\rangle$ 的定义知：$\langle c\rangle \leqslant \langle a\rangle$。从而由 $|\langle a\rangle| = |a| = p$ 是素数和 Lagrange 定理可知，$|\langle c\rangle| = |\langle a\rangle|$。结合 $\langle c\rangle \subseteq \langle a\rangle$ 就有，$a \in \langle c\rangle = \langle a\rangle$。这就是说，存在是 $k \in \mathbb{Z}$，使得 $c^k = a$。从而由 $\langle b\rangle$ 是群和 $c \in \langle b\rangle$ 可知，$a = c^k \in \langle b\rangle$。这与题设 $a \notin \langle b\rangle$ 矛盾。 □

17.21

证明： $H_1H_2 \subseteq G$ 是显然的。

设 $G = \langle a\rangle$。由教材定理 17.13(3) 可知，$H_1 = \langle a^s\rangle, H_2 = \langle a^r\rangle$。由于 $(r, s) = 1$。故存在 $m, n \in \mathbb{Z}$，使得 $mr+ns = 1$。对任意 $x \in G$，设 $x = a^t$，则有 $x = a^{tmr+tns} = a^{s(tm)}a^{r(tn)} \in H_1H_2$。从而有 $G \subseteq H_1H_2$。

综合即有：$G = H_1H_2$。 □

17.22

证明： 记 $H = H_1 \cap H_2$。由定义有，$a^d \in H$。对由教材例 17.12(1) 知，$H \leqslant G$。从而有 $\langle a^d\rangle \subseteq H$。

下面证明 $H \subseteq \langle a^d\rangle$。分两种情况讨论：

情况一：若 G 是无限群，则对任意 $a^t \in H$，由于 $H = H_1 \cap H_2$，故 $a^t \in H_1$，$a^t \in H_2$，由定义知，存在 $k_1, k_2 \in \mathbb{Z}$，使得 $a^{k_1r} = a^{k_2s} = a^t$。由于 G 是无限阶的，所以必有 $k_1r = t$ 和 $k_2s = t$ (否则，不妨设 $k_1r \neq t$，则由消去律知 $a^{k_1r-t} = 0$ 和 $k_1r - t \neq 0$，从而 $|G| = |a| \mid k_1r - t$，这与 G 是无限阶群矛盾)，从而有 $r \mid t$，$s \mid t$，由最小公倍数的性质知 $d = [r, s] \mid t$，从而有 $a^t \in \langle a^d\rangle$。由 a^t 的任意性知，$H \subseteq \langle a^d\rangle$。

情况二：若 G 是 n 阶有限群，则由教材例 17.12 和子群定义知，$H \leqslant H_1$ 且 $H \leqslant H_2$。从而由 Lagrange 定理知和教材例 17.16 知，$|H| \mid |H_1| = \dfrac{n}{(n, r)}$，$|H| \mid |H_2| = \dfrac{n}{(n, s)}$。从而 $(n, r) \mid n|H|$，$(n, s) \mid n|H|$，$[(n, r), (n, s)] \mid n|H|$，也即 $|H| \mid \dfrac{n}{[(n, r), (n, s)]}$。另一方面，由教材例 17.16 知，$|\langle a^d\rangle| = |\langle a^d\rangle| = \dfrac{n}{(n, d)} = \dfrac{n}{(n, [r, s])}$。

下面只需证明 $(n, [r, s]) = [(n, r), (n, s)]$，就可得到 $|H| \mid |\langle a^d\rangle|$，进而由 $\langle a^d\rangle \subseteq H$ 可得 $|\langle a^d\rangle| \leq |H|$，综合得 $|\langle a^d\rangle| = |H|$。再由 $H \subseteq G$ 是有限群和教材定理 5.5 推论就有 $\langle a^d\rangle = H$。

在证明 $(n, [r, s]) = [(n, r), (n, s)]$ 之前，注意到如下事实：

引理 17.2 对任意 $x, y, z \in \mathbb{R}$，有 $\min(x, \max(y, z)) = \max(\min(x, y), \min(x, z))$。

证明： 分两种情况考虑。

若 $x \leq \max(y, z)$，则 $\min(x, \max(y, z)) = x$，而对 y, z 中较大者(不妨设为 y)，则有 $\min(x, y) = x$，而 $\min(x, z) \leq x$。从而 $\max(\min(x, y), \min(x, z)) = x$。等式成立。

若 $x > \max(y, z)$，则必有 $x > y$，$x > z$，从而 $\min(x, y) = y$，$\min(x, z) = z$，$\max(\min(x, y), \min(x, z)) = \max(y, z)$。而由于 $x > \max(y, z)$，所以 $\min(x, \max(y, z)) = \max(y, z)$。等式也成立。 □

下面证明 $(n, [r, s]) = [(n, r), (n, s)]$。

设 n, r, s 的素因子分解式分别为 $n = \prod p_i^{a_i}$，$r = \prod p_i^{b_i}$，$s = \prod p_i^{c_i}$。则：

$$
\begin{aligned}
(n, [r, s]) &= \prod p_i^{\min(n, \max(r, s))} && \text{(gcd, lcm 性质)} \\
&= \prod p_i^{\max(\min(n, r), \min(n, s))} && \text{(引理 17.2)} \\
&= [(n, r), (n, s)] && \text{(gcd, lcm 性质)}
\end{aligned}
$$

□

17.23