(2)

证明： 由第 (1) 小题已知 $\varphi^{-1}(H)$ 为群。对任意 $g \in G_1, h \in \varphi^{-1}(H)$，$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g^{-1}) \in H$，所以有 $ghg^{-1} \in \varphi^{-1}(H)$。由教材定理 17.32 知，$\varphi^{-1}(H) \trianglelefteq G_1$。 □

17.52

证明： 必要性。设 φ 是同态，则有 $b^{km} = \varphi(a^m) = \varphi(e_1) = e_2$。由教材定理 17.8(1) 知，$n \mid mk$。

充分性。首先证明，当 $n \mid mk$ 时，φ 是函数。

$$
\begin{aligned}
& forall s, t \in \mathbb{Z}, \\
& a^s = a^t \\
\iff & a^{s-t} = e_1 && \text{(消去律)} \\
\iff & m \mid s-t && \text{(教材定理 17.8(1))} \\
\implies & mk \mid ks-kt && \text{(两边乘 } k\text{)} \\
\implies & n \mid ks-kt && (n \mid mk) \\
\iff & b^{ks-kt} = e_2 && \text{(教材定理 17.8(1))} \\
\iff & b^{ks} = b^{kt} && \text{(两边乘 } b^{kt}\text{)} \\
\iff & \varphi(a^s) = \varphi(a^t) && (\varphi \text{ 定义})
\end{aligned}
$$

这就证明了 φ 是函数。而对任意 $a^s, a^t \in G_1$，$\varphi(a^s a^t) = \varphi(a^{s+t}) = b^{k(s+t)} = b^{ks}b^{kt} = \varphi(a^s)\varphi(a^t)$，所以 φ 是同态。 □

17.53 先证一个引理。

引理 17.4 设 φ 是群 G_1 到 G_2 的同态映射，H 是 G_1 的子群。则有

$$|\varphi(H)| \,\big|\, (|G_2|, |H|).$$

证明： 由教材定理 17.35(1) 知，$\varphi(H) \leqslant G_2$。从而由 Lagrange 定理知，$|\varphi(H)| \,\big|\, G_2$。

考虑 $\varphi \restriction H : H \to \varphi(H)$，显然，$\varphi \restriction H$ 也是同态，且为满同态。由群同态基本定理知，$H/\ker(\varphi \restriction H) \cong \varphi(H)$。从而 $|\varphi(H)| = |H/(\ker \varphi \restriction H)| = [H : \ker \varphi] \,\big|\, |H|$。所以有 $|\varphi(H)| \,\big|\, (|H|, |G_2|)$。 □

再证原题。

证明： 由题设和引理 17.4 知，$|\varphi(H)| \,\big|\, (|H|, |G_2|) = 1$，即有 $\varphi(H) = \{e_2\}$。由同态核的定义即有 $H \subseteq \ker \varphi$。 □

17.54

证明： 作自然映射 $\varphi : G \to G/N$，$\forall g \in G$，$\varphi(g) = Ng$。

由引理 17.4 知，$|\varphi(H)| \,\big|\, (|H|, |G/N|) = (|H|, [G : N]) = 1$，$\varphi(H) = \{N\}$。这就是说，$\forall h \in H$，$\varphi(h) = hN = N$，即有 $h \in N, \forall h \in H$。

这就证明了 $H \subseteq N$。 □

17.55 先证一个引理。

引理 17.5 设 φ 是群 G_1 到 G_2 的同态映射，H 是 G_1 的子群，且 $\ker \varphi \subseteq H$。则对任意 $a \in G_1$ 有

$$a \in H \Leftrightarrow \varphi(a) \in \varphi(H).$$

证明： 由定义立即有 $a \in H \Rightarrow \varphi(a) \in \varphi(H)$。

下面证明 $\varphi(a) \in \varphi(H) \Rightarrow a \in H$。

$\varphi(a) \in \varphi(H)$