这就证明了 φ 是自同态，从而是自同构。

必要性。

若 φ 是自同构，则对任意 $a, b \in G$，

$$
\begin{aligned}
ab &= ((ab)^{-1})^{-1} && (\text{教材定理 17.2(1)})\\
&= \varphi((ab)^{-1}) && (\varphi\text{ 定义})\\
&= \varphi(b^{-1}a^{-1}) && (\text{教材定理 17.2(2)})\\
&= \varphi(b^{-1})\varphi(a^{-1}) && (\varphi\text{ 是同构})\\
&= (b^{-1})^{-1}(a^{-1})^{-1} && (\varphi\text{ 定义})\\
&= ba && (\text{教材定理 17.2(1)})
\end{aligned}
$$

这就证明了 G 是交换群。 □

17.62

(1)

证明： 由于对任意正整数 n, t 都有 $n \mid nt$。由习题 17.52 知，φ 是自同态。 □

(2)

证明： 充分性。若 $(n, t) = 1$，则存在 $p, q \in \mathbb{Z}$，使 $pn + qt = 1$。从而对任意 $a^i \in G$，有 $a^i = a^{i-ipn} == a^{iqt} = \varphi(a^{iq}) \in \varphi(G)$。从而 φ 是满自同态。再由习题 17.60 结论知，φ 是自同构。

必要性。若 φ 是自同构，则必是满射。因而，存在 $q \in \mathbb{Z}$，使得 $\varphi(a^q) = a^{qt} = a$，即，$qt - 1 \mid n$。从而必有 $k \in \mathbb{Z}$，使得 $qt - 1 = kn$，取 $p = -k \in \mathbb{Z}$，就有 $pn + qt = 1$。从而有 $(n, t) = 1$。 □

17.63

证明： 定义 $f : G \to \operatorname{Inn} G$，$\forall g \in G$，$f(g) = \varphi_g$。显然 f 是函数且为满射。下面证明 f 是同态。

对任意 $x, y, a \in G$，

$$
\begin{aligned}
\varphi_{xy}(a) &= xya(xy)^{-1} && (\varphi_{xy}\text{ 定义})\\
&= xyay^{-1}x^{-1} && (\text{教材定理 17.2(2)})\\
&= \varphi_x(yay^{-1}) && (\varphi_x\text{ 定义})\\
&= \varphi_x(\varphi_y(a)) && (\varphi_y\text{ 定义})\\
&= \varphi_x \circ \varphi_y(a) && (\text{教材定理 3.3})
\end{aligned}
$$

这就证明了 f 是同态。

下面证明 $\ker f = C$。

$\forall g \in G$,

$$
\begin{aligned}
& g \in C \\
\iff & \forall a(a \in G \to ga = ag) && (C\text{ 定义})\\
\iff & \forall a(a \in G \to gag^{-1} = a) && (\text{右乘 } g^{-1})\\
\iff & \forall a(a \in G \to \varphi_g(a) = a) && (\varphi\text{ 定义})\\
\iff & \varphi_g = I_G && (I_G\text{ 定义})\\
\iff & g \in \ker f && (\ker f\text{ 定义})
\end{aligned}
$$

这就证明了 $\ker f = C$。由群同态基本定理就有，$G/C \cong \operatorname{Inn} G$。 □