这就证明了 $\ker\varphi + S \subseteq \varphi^{-1}(\varphi(S))$。从而有 $\varphi^{-1}(\varphi(S)) = \ker\varphi + S$。 □

18.33

证明： 不妨记 $F_1 = \langle A_1, +_1, *_1\rangle$，$F_2 = \langle A_2, +_2, *_2\rangle$。

由教材定理 18.6 知，$\ker\varphi$ 是 F_1 是理想。由教材例 18.11 知，F_1 中的理想只有 $\{0\}$ 和 F_1。由于 $\varphi(F_1) \neq \{0\}$，所以存在 $x \in F_1$，使得 $\varphi(x) \neq 0$，$x \notin \ker\varphi$。从而 $\ker\varphi \neq F_1$。因此，必有 $\ker\varphi = \{0\}$。

注意到，φ 也是群 $\langle A_1, +_1\rangle$ 到群 $\langle A_2, +_2\rangle$ 的同态。由 $\ker\varphi = \{0\}$ 和教材定理 17.33 知，φ 是从 $\langle A_1, +_1\rangle$ 到 $\langle A_2, +_2\rangle$ 的单同态。这就是说，φ 是从 A_1 到 A_2 的单射，从而也是 F_1 到 F_2 的单同态。 □

18.34

证明： 显然，对任何 $f, g \in \operatorname{End} G$，$f + g$ 和 $f \circ g$ 仍是函数。对任意 $x, y \in G$，

$$\begin{aligned}
(f+g)(x+y) &= f(x+y) + g(x+y) && \text{(定义)}\\
&= f(x) + f(y) + g(x) + g(y) && (f, g \text{ 是同态})\\
&= f(x) + g(x) + f(y) + g(y) && (G \text{ 是 Abel 群})\\
&= (f+g)(x) + (f+g)(y) && \text{(定义)}\\
(f\circ g)(x+y) &= f(g(x+y)) && \text{(定义)}\\
&= f(g(x) + g(y)) && (g \text{ 是同态})\\
&= f(g(x)) + f(g(y)) && (f \text{ 是同态})\\
&= (f\circ g)(x) + (f\circ g)(y) && \text{(定义)}
\end{aligned}$$

这就证明了 $f + g$ 和 $f \circ g$ 都是 G 的自同态。从而 $+$ 和 $\circ$ 都是 $\operatorname{End} G$ 上的二元运算。

$+$ 运算显然满足交换律、结合律，且零同态 φ_0 是加法单位元。令 $\varphi : G \to G$，$\forall x \in G$，$\varphi(x) = -x$。由习题 17.61 结论知，φ 是自同构。对任意 $f \in \operatorname{End} G$，显然有 $\varphi \circ f \in \operatorname{End} G$ 和 $f + \varphi \circ f = \varphi_0$。从而 $\operatorname{End} G$ 中每个元素均有加法逆元。因此，$\langle \operatorname{End} G, +\rangle$ 是 Abel 群。

由教材定理 2.5 知，$\circ$ 运算是可结合的。从而 $\langle \operatorname{End} G, \circ\rangle$ 是半群。

对任意 $f, g, h \in \operatorname{End} G$，$x \in G$，

$$\begin{aligned}
(f\circ(g+h))(x) &= f((g+h)(x)) && (\circ \text{ 运算定义})\\
&= f(g(x) + h(x)) && (+ \text{ 运算定义})\\
&= f(g(x)) + f(h(x)) && (f \text{ 是同态})\\
&= (f\circ g)(x) + (f\circ h)(x) && (\circ \text{ 运算定义})\\
((g+h)\circ f)(x) &= (g+h)(f(x)) && (\circ \text{ 运算定义})\\
&= g(f(x)) + h(f(x)) && (+ \text{ 运算定义})\\
&= (g\circ f)(x) + (h\circ f)(x) && (\circ \text{ 运算定义})
\end{aligned}$$

从而 $\circ$ 运算对 $+$ 运算是可分配的。

这就证明了 $\langle \operatorname{End} G, +, \circ\rangle$ 是环。 □

对循环群上的任何自同态 $\varphi : G \to G$，若 $\varphi(a) = ia$，则必有 $\varphi(ka) = k\varphi(a) = kia$，$k, i \in \mathbb{Z}$。从而循环群上的自同态具有 $\varphi_i(ka) = kia$, $\forall ka \in G$ 的形式。显然，

$$\varphi_i = \varphi_j \iff i \equiv j \pmod{n},$$