从而 $\mathrm{End}\,G=\{\varphi_i \mid i=0,1,\cdots,n-1\}$。

对任意 $\varphi_i,\varphi_j\in\mathrm{End}\,G$，$a^t\in G$，

$$\begin{aligned}
(\varphi_i+\varphi_j)(ka) &= \varphi_i(ka)+\varphi_j(ka) && (+\text{ 运算定义})\\
&= kia+kja && (\varphi_i,\varphi_j\text{ 定义})\\
&= k(i+j)a && (\text{整数乘法分配律})\\
&= \varphi_{i+j}(ka) && (\varphi_{i+j}\text{ 定义})\\
(\varphi_i\circ\varphi_j)(ka) &= \varphi_i(\varphi_j(ka)) && (\circ\text{ 运算定义})\\
&= kjia && (\varphi_i,\varphi_j\text{ 定义})\\
&= \varphi_{ji}(ka) && (\varphi_{ji}\text{ 定义})
\end{aligned}$$

因此，G 的自同态环为，$\langle\{\varphi_i \mid i=0,1,\cdots,n-1\},+,\circ\rangle$，对所有 $\varphi_i,\varphi_j\in\mathrm{End}\,G$，$\varphi_i+\varphi_j=\varphi_{(i+j \bmod n)}$，$\varphi_i\circ\varphi_j=\varphi_{(ji \bmod n)}$。

18.35

证明: 仿上题的方法可证，对有理数加法群上的任何自同态 $\varphi:\mathbb{Q}\to\mathbb{Q}$，若 $\varphi(1)=a$，则 $\forall x\in\mathbb{Q}$，$\varphi(x)=ax$。从而 $\mathrm{End}\,G=\{\varphi_a \mid a\in\mathbb{Q}\}$，其中 φ_a 定义为 $\forall x\in\mathbb{Q}$，$\varphi_a(x)=ax$。

作 $\sigma:\mathrm{End}\,\mathbb{Q}\to\mathbb{Q}$，$\forall\varphi_a\in\mathrm{End}\,\mathbb{Q}$，令 $\sigma(\varphi_a)=a$。显然，σ 是双射。下面证 σ 是从 $\langle\mathrm{End}\,\mathbb{Q},+,\circ\rangle$ 到 $\langle\mathbb{Q},+,\cdot\rangle$ 的同态。

对任意 $\varphi_a,\varphi_b\in\mathrm{End}\,\mathbb{Q}$，$x\in\mathbb{Q}$，

$$\begin{aligned}
(\varphi_a+\varphi_b)(x) &= \varphi_a(x)+\varphi_b(x) && (+\text{ 运算定义})\\
&= ax+bx && (\varphi_a,\varphi_b\text{ 定义})\\
&= (a+b)x && (\text{分配律})\\
&= \varphi_{a+b}(x) && (\varphi_{a+b}\text{ 定义})\\
(\varphi_a\circ\varphi_b)(x) &= \varphi_a(\varphi_b(x)) && (\circ\text{ 运算定义})\\
&= abx && (\varphi_a,\varphi_b\text{ 定义})\\
&= \varphi_{ab}(x) && (\varphi_{ab}\text{ 定义})
\end{aligned}$$

从而有 $\sigma(\varphi_a+\varphi_b)=\sigma(\varphi_{a+b})=a+b=\sigma(\varphi_a)+\sigma(\varphi_b)$，$\sigma(\varphi_a\circ\varphi_b)=\sigma(\varphi_{ab})=ab=\sigma(\varphi_a)\sigma(\varphi_b)$。

这就证明了 σ 是同态，从而是同构。于是有 $\langle\mathrm{End}\,\mathbb{Q},+,\circ\rangle\cong\langle\mathbb{Q},+,\cdot\rangle$。 □

18.36

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	x	0
$x+1$	0	$x+1$	0	$x+1$

由于 $x,(x+1)\in F_2[x]/(x+x^2)$，$x\neq 0$，$x+1\neq 0$，但 $x\cdot(x+1)=0$，所以 $F[2]/(x+x^2)$ 不是域。

18.37

证明: 对任意次数大于 1 的多项式 $f(x)=a_0+a_1x+\cdots+a_nx^n\in F_2[x]$，若 $f(x)$ 中有偶数个非零系数，不妨设它们是 $a_{i_1}=a_{i_2}=\cdots=a_{i_k}=1$，其中 $i_1<i_2<\cdots<i_k$，k 为偶数。则