证明: 由于 $|R|>2$，任取两个互异的非零元 $a,b\in R-\{0\}$，$a\neq b$，有

$$
\begin{aligned}
& ab+ab=0 && \text{(第 (2) 小题结论)}\\
\iff\ & a^2b+ab^2=0 && (a^2=a, b^2=b)\\
\iff\ & a(ab+b^2)=0 && \text{(分配律)}\\
\iff\ & a(a+b)b=0 && \text{(分配律)}
\end{aligned}
$$

由于 $a+b=a-b\neq 0$，所以：若 $a(a+b)=0$，则 a 为左零因子，$a+b$ 为右零因子。若 $a(a+b)\neq 0$，则 $a(a+b)$ 为左零因子，b 为右零因子。从而 R 中总有零因子，因而不是整环。 □

18.6

(1) 由教材定理 15.6 即可得证。

(2) 由教材定理 15.6 即可得证。

(3) 不一定。取 $R_1=R_2=\langle\mathbb{Z}_2,\oplus,\otimes\rangle$，其中 $\oplus$ 和 $\otimes$ 分别是模 2 加法和模 2 乘法。易于验证，它们是整环。但它们的积代数 $\langle\mathbb{Z}_2\times\mathbb{Z}_2,\overline{\oplus},\overline{\otimes}\rangle$ 不是整环，因为 $\langle 0,1\rangle,\langle 1,0\rangle\in\mathbb{Z}_2\times\mathbb{Z}_2$ 是非零元，但 $\langle 0,1\rangle\overline{\otimes}\langle 1,0\rangle=\langle 0,0\rangle$。

18.7

(1) 由于 n 不是素数，所以存在正整数 $1<p,q<n$，使得 $pq=n$。从而 $p\otimes q=q\otimes p=pq \bmod n=0$，是零因子。

(2)

证明: 令 k 为最小的使 $k\otimes r=0$ 的正整数，其中 $\otimes$ 为模 n 乘法。显然，$kr=[r,n]$，其中 $[r,n]$ 是 r 和 n 的最小公倍数。从而 $k=\dfrac{[r,n]}{r}=\dfrac{rn}{r\cdot(r,n)}=\dfrac{n}{(r,n)}$。

当 $(r,n)=1$ 时，$k=n\notin\mathbb{Z}_n$，从而 r 不是右零因子，由乘法交换律知，r 也不是左零因子，从而不是零因子。当 $(r,n)>1$ 时，$0<k<n$，$k\in\mathbb{Z}_n$，从而 r 是零因子。 □

(3) $2,3,4,6,8,9,10,12,14,15,16$。

18.8

证明: 对任何 $b\in R$，若有 $ab=0$，则有 $b=1b=(a^{-1}a)b=a^{-1}(ab)=a^{-1}0=0$，从而 a 不是左零因子。同理可证 a 不是右零因子。从而 a 不是零因子。 □

18.9 先证明第 11 小题结论：

引理 18.1 有限整环必是域。[1]

证明: 设 $\langle R,+,\cdot\rangle$ 是有限整环。令 $R^*=R-\{0\}$。

对任意 $a,b\in R^*$，由 R^* 定义有 $a\neq 0$，$b\neq 0$。因为 R 是整环，所以 $ab\neq 0$，从而有 $ab\in R^*$。这就是说，$\cdot$ 是 R^* 上的二元运算，从而 $\langle R^*,\cdot\rangle$ 是有限的代数系统。

由于 $\cdot$ 在 R 上是交换的、结合的，所以 $\cdot$ 在 R^* 也是交换的、结合的。

由于 $1\in R$ 且 $1\neq 0$，所以 $1\in R^*$。

对任何 $a\in R^*$，取 $\varphi_a:R^*\to R^*$，$\forall x\in R^*$，$\varphi_a(x)=ax$。由于 $\cdot$ 在 R 中适合消去律，因此对任何 $x,y\in R^*$，$\varphi_a(x)=\varphi_a(y)\Leftrightarrow x=y$，从而 φ_a 是单射。这就是说，φ_a 是从 R^* 到 $\varphi_a(R^*)$ 的双射。换言之，R^* 与 $\varphi_a(R^*)$ 等势。

由教材定理 5.5 推论 1 知，$\varphi_a(R^*)\not\subset R^*$，但由 $\cdot$ 对 R^* 的封闭性显然有 $\varphi_a(R^*)\subseteq R^*$。从而就有 $\varphi_a(R^*)=R^*$。

因此，对任意 $a\in R^*$ 都有 $1\in R^*=aR^*$，即存在 $b\in R^*$，使得 $1=ba=ab\in aR^*$，从而 a

[1] 这里按通常的定义，将“含幺”理解成“$1\in R$ 且 $1\neq 0$”。否则 1 阶的代数系统也是有限整环(但按教材定义，它不是域)，定理不成立。