5. 设 R 是环，若 $\forall a \in R$ 都有 $a^2 = a$，则称 R 为布尔环. 证明

(1) R 是可交换的；

(2) $\forall a \in R$ 有 $a + a = 0$；

(3) 如果 $|R| > 2$，则 R 不是整环.

(2) $(a+a)^2 = a+a \Rightarrow a^2+a^2+a^2+a^2 = a+a+a+a = a+a$

$\Rightarrow a+a=0$

(1) $(a+b)^2 = a+b \Rightarrow a^2+ab+ba+b^2 = a+b+ab+ba = a+b$

$\Rightarrow ab+ba=0 \Rightarrow ab+ab = ba+ba$

$\Rightarrow ab = ba$

(3) 设 $a \neq b \neq 0$，$a,b \in Z$

若 $ab=0$，显然 a,b 是零因子，R 不是整环

若 $ab \neq 0$，则 $ab(b-a) = ab^2 - aba = ab - aab = ab - ab = 0$

$b-a \neq 0 \Rightarrow ab$ 和 $b-a$ 是零因子，R 不是整环

7. 设正整数 n 不是素数且 $n > 1$，证明

(1) Z_n 中含有零因子；

(2) $\forall r \in Z_n, r \neq 0$，则 r 不是 Z_n 中零因子当且仅当 $(r,n) = 1$；

(3) 找出 Z_{18} 中的全部零因子.

(1) n 不是素数 $\Rightarrow \exists\ p, q \in N^*$ s.t. $pq = n$

$p \otimes q = q \otimes p = pq \bmod n = 0$ 是零因子

(2) 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，$kr = [r,n]$，$k = \frac{[r,n]}{r} = \frac{n}{(r,n)}$

当 $(r,n)=1$ 时，$k = n \notin Z_n$，从而 r 不是右零因子，也不是左零因子

当 $(r,n) > 1$ 时，$0 < k < n$，$k \in Z_n$，从而 r 是零因子

(3) 2, 3, 4, 6, 8, 9, 10, 12, 14, 15, 16

20. 设 R 是环，$A,B \subseteq R$. 令

$$A+B=\{a+b \mid a\in A \wedge b\in B\}.$$

(1) 证明当 A,B 是理想时，$A+B$ 也是理想；

(2) 举例说明当 A,B 是子环时，$A+B$ 未必是子环.

(1) $\forall x,y\in A+B$, $\exists a_1,a_2\in A$, $b_1,b_2\in B$ s.t.

$x=a_1+b_1$, $y=a_2+b_2$

$x-y=a_1+b_1-a_2-b_2=(a_1-a_2)+(b_1-b_2)\in A+B$

$\forall r\in R$, $x\in A+B$, $\exists a\in A$, $b\in B$, s.t. $x=a+b$

$rx=r(a+b)=ra+rb$

A,B 是理想 $\Rightarrow$ $ra\in A$, $rb\in B$

$rx=ra+rb\in A+B$, $r(A+B)\subseteq A+B$

同理 $(A+B)r\subseteq A+B$ $\Rightarrow$ $A+B$ 是理想

(2) $\mathbb{Z}[i]=\{a+bi \mid a,b\in\mathbb{Z}\}$ 和 $\mathbb{R}$ 都是复数域 $\mathbb{C}$ 的子环.

$\mathbb{R}+\mathbb{Z}[i]$ 对乘法不封闭

23. 设 A 是偶数环，$D=\{4x \mid x\in Z\}$. 证明 D 是 A 的一个理想，求 A/D.

$0\in D\Rightarrow$ D 非空

$\forall x\in D$, $\exists m\in\mathbb{Z}$ s.t. $x=4m=2(2m)\in A\Rightarrow D\subseteq A$

$\forall x,y\in D$, $\exists m,n\in\mathbb{Z}$ s.t. $x=4m$, $y=4n\Rightarrow x-y=4(m-n)\in D$

$\forall a\in A$, $d\in D$, $\exists m,n\in\mathbb{Z}$ s.t. $a=2m$, $d=4n$

$\Rightarrow ad=da=8mn=4(2mn)\in D$

$\Rightarrow D$ 是 A 的一个理想

$A/D=\langle\{\bar{0},\bar{2}\},+,\cdot\rangle$

27. 设 R 是交换环，$x_1, x_2, \cdots, x_m \in R$. 令

$$S = \{r_1x_1 + r_2x_2 + \cdots + r_mx_m \mid r_i \in R, i = 1, 2, \cdots, m\}.$$

证明 S 是 R 的理想.

$0 \in S$，S 非空

$\forall\ r_1x_1 + r_2x_2 + \cdots + r_mx_m,\ r_1'x_1 + r_2'x_2 + \cdots + r_m'x_m \in S$

$(r_1x_1 + r_2x_2 + \cdots + r_mx_m) - (r_1'x_1 + r_2'x_2 + \cdots + r_m'x_m)$

$= (r_1 - r_1')x_1 + (r_2 - r_2')x_2 + \cdots + (r_m - r_m')x_m \in S$

$\forall\ a \in R,\ r_1x_1 + r_2x_2 + \cdots + r_mx_m \in S,$

$(r_1x_1 + r_2x_2 + \cdots + r_mx_m)a = (ar_1)x_1 + (ar_2)x_2 + \cdots + (ar_m)x_m \in S$

$\Rightarrow$ S 是 R 的理想

31. 设 R 是环，A, B 是 R 的两个理想，且 $B \subseteq A$. 证明 A/B 是 R/B 的理想，且

$$R/B \big/ (A/B) \cong R/A.$$

$A/B \subseteq R/B$

$B \in A/B \Rightarrow A/B$ 非空

$\forall\ \bar{x}, \bar{y} \in A/B$，有 $x, y \in A$，$x - y \in A$，$\bar{x} - \bar{y} = \overline{x-y} \in A/B$

$\forall\ \bar{x} \in A/B$，$\bar{y} \in R/B$，有 $x \in A$，$y \in R$，$xy \in A$，$yx \in A$

$\Rightarrow \bar{x} \cdot \bar{y} = \overline{xy} \in A/B$，$\bar{y} \cdot \bar{x} = \overline{yx} \in A/B$

于是 A/B 是 R/B 的理想

设 $\varphi: R/B \to R/A$. $\forall\ x + B \in R/B$，令 $\varphi(x+B) = x + A$

$x + B = y + B \Leftrightarrow -x + y \in B \Rightarrow -x + y \in A \Rightarrow x + A = y + A$

$\Rightarrow \varphi(x+B) = \varphi(y+B)$

$\forall\ x + A \in R/A$，$\exists\ x + B \in R/B$ s.t. $\varphi(x+B) = x + A \Rightarrow$ 满射

$\Rightarrow \varphi$ 为满同态

$\varphi(x+B) = x + A = A \Leftrightarrow x \in A$，$\ker\varphi = \{x + B \mid x \in A\} = A/B$

$\Rightarrow R/B/(A/B) \cong R/A$

34. 设 G 为 Abel 群，在 End$G$ 上定义两个运算. $\forall f,g \in \mathrm{End}G$,

$$(f+g)(x) = f(x)+g(x),\quad \forall x \in G,$$

$$f \circ g(x) = f(g(x)),\quad \forall x \in G.$$

证明 $\langle \mathrm{End}G, +, \circ\rangle$ 是一个环. 称为 G 的自同态环. 设 $G = \langle a \rangle$ 是 n 阶循环群，求 G 的自同态环.

$\forall f,g \in \mathrm{End}\,G$ ，$f+g$ 和 $f\circ g$ 仍是函数.

$\forall x,y \in G$ ，$(f+g)(x+y) = (f+g)(x) + (f+g)(y)$

$(f\circ g)(x+y) = (f\circ g)(x) + (f\circ g)(y)$

$+, \circ$ 是 End$G$ 上的二元运算

$+$ 可交换，可结合，φ_0 是单位元，有逆元

$\circ$ 可结合，于是 $\langle \mathrm{End}G, +, \circ\rangle$ 是半群

$\forall f,g,h \in \mathrm{End}G,\ x \in G$

$(f\circ(g+h))(x) = (f\circ g)(x) + (f\circ h)(x)$

$((g+h)\circ f)(x) = (g\circ f)(x) + (h\circ f)(x)$

$\circ$ 对 $+$ 可分配 $\Rightarrow \langle \mathrm{End}G, +, \circ\rangle$ 是环

$\varphi: G \to G,\ \varphi(a) = ia,\ \varphi(ka) = k\varphi(a) = kia$

$\varphi_i = \varphi_j \Leftrightarrow i \equiv j \pmod n$

End$G = \{\varphi_i\}$

$\langle \{\varphi_i \mid i = 0,1,\cdots,n-1\}, +, \circ\rangle$