**Lemma 12.1.** *Let $a$ $b \in R$, then $(-a) + (-b) = -(a + b)$.*

*Proof.*

$$\begin{aligned}
&(-a) + (-b) + (a + b)\\
=&(-a) + (-b) + a + b\\
=&(-a) + a + (-b) + b\\
=&e\\
=&-(a + b) + (a + b)
\end{aligned}$$

Then by cancellation, $(-a) + (-b) = -(a + b)$. □

**Exercise 12.14.** *Let $a$ $b \in R$ and $m \in \mathbb{Z}$. Prove that $m \cdot (ab) = (m \cdot a)b = a(m \cdot b)$.*

*Proof.* Induction on $m$, and using multiplication left/right distributive over addition. □

**Exercise 12.15.** *Let $a$ $b \in R$ and $m$ $n \in \mathbb{Z}$. Prove that $(m \cdot a)(n \cdot b) = (m \times n) \cdot (ab)$.*

*Proof.* Induction on $m$, and using Exercise 12.14 on $n$. □

**Exercise 12.16.** *Let $a \in R$ and $n \in \mathbb{Z}$. Prove that $n \cdot (-a) = -(n \cdot a)$.*

*Proof.* Induction on $n$.

- Base: $0 \cdot (-a) = 0 = -0 = -(0 \cdot a)$.
- Induction (Positive Direction): We have the following induction hypothesis:

  $$\boxed{(n - 1) \cdot (-a) = -((n - 1) \cdot a)}.$$

  Then

  $$\begin{aligned}
  n \cdot (-a) &= ((n - 1) \cdot (-a)) + (-a)\\
  &= -((n - 1) \cdot a) + (-a)\\
  &= -((n - 1) \cdot a + a) \quad \text{(by Lemma 12.1)}\\
  &= -(n \cdot a)
  \end{aligned}$$

  Same for negative direction.

$\square$

**Exercise 12.17.** *For any ring $R$ where the group $(R, +)$ is cyclic, show that $R$ is commutative.*

*Proof.* Suppose the generator of $(R, +)$ is $r$, then for any $a$ $b$ in $R$, they have form $a = i \cdot r$ and $b = j \cdot r$ where $i$ $j \in \mathbb{N}^+$. Then $ab = (i \cdot r)(j \cdot r) = (i \times j) \cdot rr = (j \times i) \cdot rr = (j \cdot r)(i \cdot r) = ba$. $\square$

**Exercise 12.18.** *Let $r \in R$, and $S = \{ x \in R \mid rx = 0 \}$. Show that $S$ is a subring of $R$.*

*Proof.* By two-steps test:

0. $S$ is not empty since $r0 = 0$.
1. For any $a$ $b \in S$, $r(a - b) = ra - rb = 0 - 0 = 0$.
2. For any $a$ $b \in S$, $rab = 0b = 0$.

$\square$

**Exercise 12.19** (Center of Ring)**.** *Let $R$ be a ring, the center of $R$ is the set $\{ x \in R \mid \forall a \in R, ax = xa \}$. Prove that the center of $R$ is a subgring of $R$.*

*Proof.* By two-steps test:

0. $S$ is non-empty since $x0 = 0x = 0$.
1. For any $a$ $b \in S$, $x(a - b) = xa - xb = ax - bx = (a - b)x$.
2. For any $a$ $b \in S$, $x(ab) = axb = abx = (ab)x$.

$\square$

**Definition 12.1** (Nilpotent)**.** *Let $R$ a ring, and $a \in R$, if there is a positive integer $n$ such that $a^n = 0$, then $a$ is nilpotent.*

**Exercise 12.31.** *Shows that the nilpotent elements of a commutative ring form a subring.*

*Proof.* We denote such set by $S$. By two-sptes test:

0. $S$ is non-empty since $0^1 = 0$.

1. For any $a\ b \in S$, there are $m\ n \in \mathbb{N}^+$ such that $a^m = b^n = 0$. Let $k = \max(m, n)$. We claim $(a+b)^{2k} = 0$. We know each term in $(a+b)^k$ has form $ca^ib^j$ where $c$ is the coefficient which is not important, and $i\ j \in \mathbb{N}$, $i + j = 2k$. In the worst situation, $i = j = k$, at this moment, $a^ib^j = a^kb^k = 0 \times 0$.

2. For any $a\ b \in S$, there are $m\ n \in \mathbb{N}^+$ such that $a^m = b^n = 0$. Let $k = \max(m, n)$, then $(ab)^k = a^kb^k = 0$ (by commutative of ring).

□

**Exercise 12.32.** *Let $R$ a ring, suppose there is an integer $n > 1$ such that for any $x \in R$, $x^n = x$. If $a^m = 0$ for some positive integer $m$ and $a \in R$. Prove that $a = 0$.*

*Proof.* Since $a^m = 0$, there is an smallest integer $k$ such that $a^k = 0$. If $k \leq n$, then $n = k + r$, $a = a^n = a^{k+r} = a^ka^r = 0a^r = 0$. If $k > n$, then $k = n + r$, $0 = a^k = a^{n+r} = a^na^r = aa^r = a^{r+1}$. Since $n > 1$, we know $r + 1 < r + n$, therefore $r + 1 < k$ and $a^{r+1} = 0$, which contradict our assumption of $k$. □

**Exercise 12.50.** *Suppose that there is a positive even integer $n$ such that $a^n = a$ for all $a \in R$. Show that $a = -a$ for all $a \in R$.*

*Proof.* $a = a^n = (-a)^n = -a$, $a^n = (-a)^n$ is valid, since $n$ is even. □

**Exercise 12.55.** *Let $R$ be a ring, prove that $a^2 - b^2 = (a + b)(a - b) \iff R$ is commutative.*

*Proof.* Trivial. □

**Exercise 12.56** (Boolean ring)**.** *A Boolean ring is a ring $R$ such that $a^2 = a$ for any $a \in R$, show that Boolean ring is commutative.*

*Proof.* For any $a \in R$, $(2 \cdot a) + (2 \cdot a) = 2^2 \cdot a = 2^2 \cdot a^2 = (2 \cdot a)^2 = 2 \cdot a$, then $2 \cdot a = 0$ and $a = -a$. Then we know $(a + b)(a - b) = (a + b)(a + b) = a + b = a^2 + b^2 = a^2 - b^2$, by Exercise 12.55, $R$ is commutative. □

**Exercise 12.61.** *Let $R$ be a commutative ring with more than one element, if for any non-zero element $a$, $aR = R$, then $R$ has a unity and every non-zero element are unit.*

*Proof.* For any non-zero element $a$, the mapping $f(b) = ab : R \to R$ is onto since $f(R) = aR = R$. There is an element $1 \in R$ such that $f(1) = a1 = a$ since $f$ is onto, then for any element $c \in R$, there is $b \in R$ such that $f(b) = ab = c$, then $c1 = ab1 = a1b = ab = c$, therefore 1 is unity. There is an element $a^{-1} \in R$ such that $f(a^{-1}) = aa^{-1} = 1$ since $f$ is onto, therefore $a$ is unit. □