Introduction to Modern Algebra

Part IV. Rings and Fields

IV.18. Rings and Fields

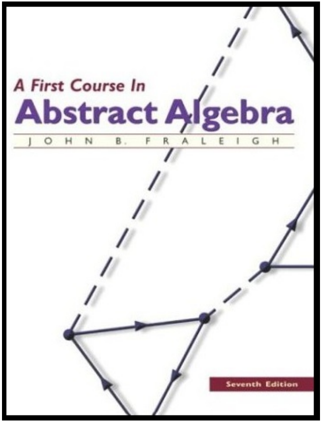

Table of contents

Theorem 18.8

Theorem 18.8. If R is a ring with additive identity 0, then for all $a, b \in R$ we have

1. $0a = a0 = 0$,
2. $a(-b) = (-a)b = -(ab)$, and
3. $(-a)(-b) = ab$.

Proof. First, let $a \in R$. Then $a0 + a0 = a(0+)$, by R_3, $= a0 = 0 + 0a$ since 0 is the additive identity. Using left cancellation in $\langle R, + \rangle$, $a0 = 0$. Using R_3 and left cancellation $0a + 0a = (0 + 0)a = 0a = 0 + 0a$ and so $0a = 0$. So (1) holds.

Theorem 18.8

Theorem 18.8. If R is a ring with additive identity 0, then for all $a, b \in R$ we have

1. $0a = a0 = 0$,
2. $a(-b) = (-a)b = -(ab)$, and
3. $(-a)(-b) = ab$.

Proof. First, let $a \in R$. Then $a0 + a0 = a(0+)$, by R_3, $= a0 = 0 + 0a$ since 0 is the additive identity. Using left cancellation in $\langle R, + \rangle$, $a0 = 0$. Using R_3 and left cancellation $0a + 0a = (0+0)a = 0a = 0 + 0a$ and so $0a = 0$. So (1) holds.

Theorem 18.8 (continued)

Theorem. 18.8. If R is a ring with additive identity 0, then for all $a, b \in R$ we have

1. $0a = a0 = 0$,
2. $a(-b) = (-a)b = -(ab)$, and
3. $(-a)(-b) = ab$.

Proof (continued). Second, let $a, b \in R$. By R_3 $a(-b) + ab = a(-b + b) = a0 = 0$ by (1). So ab is the additive inverse of $a(-b)$: $a(-b) = -(ab)$. Similarly, $(-a)b + ab = (-a + a)b = 0b = 0$ and $(-a)b = -(ab)$. So (2) holds.

Third let $a, b \in R$. Then by (2) $(-a)(-b) = -(a(-b)) = -(-(ab))$. That is, $(-a)(-b)$ is the additive inverse of $-(ab)$. But ab is also an additive inverse of $-(ab)$ and since additive inverse are unique in $\langle R, +\rangle$ (Theorem 4.17), then $(-a)(-b) = ab$. So (3) holds. □

Theorem 18.8 (continued)

Theorem. 18.8. If R is a ring with additive identity 0, then for all $a, b \in R$ we have

1. $0a = a0 = 0$,
2. $a(-b) = (-a)b = -(ab)$, and
3. $(-a)(-b) = ab$.

Proof (continued). Second, let $a, b \in R$. By R_3 $a(-b) + ab = a(-b + b) = a0 = 0$ by (1). So ab is the additive inverse of $a(-b)$: $a(-b) = -(ab)$. Similarly, $(-a)b + ab = (-a + a)b = 0b = 0$ and $(-a)b = -(ab)$. So (2) holds.

Third let $a, b \in R$. Then by (2) $(-a)(-b) = -(a(-b)) = -(-(ab))$. That is, $(-a)(-b)$ is the additive inverse of $-(ab)$. But ab is also an additive inverse of $-(ab)$ and since additive inverse are unique in $\langle R, + \rangle$ (Theorem 4.17), then $(-a)(-b) = ab$. So (3) holds. $\square$

Example

Example. Find the units of $\mathbb{Z}_8$.

Solution. The units are: 1 since $1 \cdot 1 = 1$, 3 since $3 \cdot 3 = 9 \equiv 1 \pmod 8$, 5 since $5 \cdot 5 = 25 \equiv 1 \pmod 8$, and 7 since $7 \times 7 = 49 \equiv 1 \pmod 8$. $\square$

Example

Example. Find the units of $\mathbb{Z}_8$.

Solution. The units are: 1 since $1 \cdot 1 = 1$, 3 since $3 \cdot 3 = 9 \equiv 1 \pmod{8}$, 5 since $5 \cdot 5 = 25 \equiv 1 \pmod{8}$, and 7 since $7 \times 7 = 49 \equiv 1 \pmod{8}$. $\square$