Modern Algebra

Chapter III. Rings

III.1. Rings and Homomorphisms—Proofs of Theorems

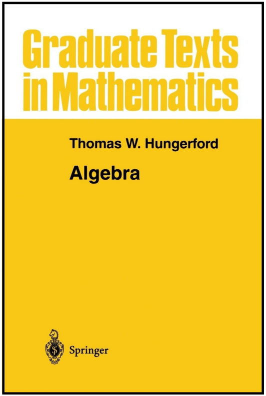

Table of contents

Theorem III.1.2

Theorem III.1.2. Let R be a ring. Then

(i) $0a = a0 = 0$ for all $a \in R$.

(ii) $(-a)b = a(-b) = -(ab)$ for all $a, b \in R$.

(iii) $(-a)(-b) = ab$ for all $a, b \in R$.

(iv) $(na)b = a(nb) = n(ab)$ for all $n \in \mathbb{Z}$ and for all $a, b \in R$.

(v) For all $a_i, b_j \in R$, $\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{j=1}^{m} b_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j$.

Proof. (i) We have that

$$\begin{aligned} 0a &= (0+0)a \text{ since 0 is the additive identity} \\ &= 0a + 0a \text{ by right distribution,} \end{aligned}$$

and so $(0a) - 0a = (0a + 0a) - 0a$ or $0 = 0a$. Similarly $a0 = 0$.

(ii) We have that

$$\begin{aligned} ab + (-a)b &= (a + (-a))b \text{ by right distribution} \\ &= 0b = 0 \text{ by (i).} \end{aligned}$$

Since additive inverses are unique in a group, $(-a)b = -(ab)$. Similarly $a(-b) = -(ab)$.

Theorem III.1.2

Theorem III.1.2. Let R be a ring. Then

(i) $0a = a0 = 0$ for all $a \in R$.

(ii) $(-a)b = a(-b) = -(ab)$ for all $a, b \in R$.

(iii) $(-a)(-b) = ab$ for all $a, b \in R$.

(iv) $(na)b = a(nb) = n(ab)$ for all $n \in \mathbb{Z}$ and for all $a, b \in R$.

(v) For all $a_i, b_j \in R$, $\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{j=1}^{m} b_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j$.

Proof. (i) We have that

$$\begin{aligned} 0a &= (0+0)a \text{ since } 0 \text{ is the additive identity} \\ &= 0a + 0a \text{ by right distribution,} \end{aligned}$$

and so $(0a) - 0a = (0a + 0a) - 0a$ or $0 = 0a$. Similarly $a0 = 0$.

(ii) We have that

$$\begin{aligned} ab + (-a)b &= (a + (-a))b \text{ by right distribution} \\ &= 0b = 0 \text{ by (i).} \end{aligned}$$

Since additive inverses are unique in a group, $(-a)b = -(ab)$. Similarly $a(-b) = -(ab)$.

Theorem III.1.2 (continued)

Theorem III.1.2. Let R be a ring. Then

(iii) $(-a)(-b) = ab$ for all $a, b \in R$.

(iv) $(na)b = a(nb) = n(ab)$ for all $n \in \mathbb{Z}$ and for all $z, b \in R$.

(v) For all $a_i, b_j \in R$, $\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{j=1}^{m} b_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j$.

Proof. (iii) By (ii),
$(-a)(-b) = -(a)(-b) = -(-(a)(b)) = -(-(ab)) = ab$ since the additive inverses are unique in a group.

(iv) For $n \in \mathbb{Z}$, $n > 0$, we have

$$\begin{aligned} (na)b &= (a + a + \cdots + a)b \text{ (n-times)} \\ &= ab + ab + \cdots + ab \text{ (n-times); by right distribution and induction} \\ &= n(ab). \end{aligned}$$

Similarly, $a(nb) = n(ab)$. For $n < 0$, the result follows similarly but with the use of additive inverses.

(v) This follows by induction and left and right distribution. □

Theorem III.1.2 (continued)

Theorem III.1.2. Let R be a ring. Then

(iii) $(-a)(-b) = ab$ for all $a, b \in R$.

(iv) $(na)b = a(nb) = n(ab)$ for all $n \in \mathbb{Z}$ and for all $z, b \in R$.

(v) For all $a_i, b_j \in R$, $\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{j=1}^{m} b_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j$.

Proof. (iii) By (ii),
$(-a)(-b) = -(a)(-b) = -(-(a)(b)) = -(-(ab)) = ab$ since the additive inverses are unique in a group.

(iv) For $n \in \mathbb{Z}$, $n > 0$, we have

$$\begin{aligned}(na)b &= (a + a + \cdots + a)b \ (n\text{-times}) \\ &= ab + ab + \cdots + ab \ (n\text{-times}); \text{ by right distribution and induction} \\ &= n(ab).\end{aligned}$$

Similarly, $a(nb) = n(ab)$. For $n < 0$, the result follows similarly but with the use of additive inverses.

(v) This follows by induction and left and right distribution. □

Lemma III.1.A

Lemma III.1.A. A ring has no zero divisors if and only if left or right cancellation hold in R (that is, for all $a, b, c \in R$ with $a \neq 0$, if either $ab = ac$ or $ba = ca$ then $b = c$).

Proof. Suppose R has no zero divisors. If $ab = ac$ then $ab - ac = 0$ and $a(b - c) = 0$.

Lemma III.1.A

Lemma III.1.A. A ring has no zero divisors if and only if left or right cancellation hold in R (that is, for all $a, b, c \in R$ with $a \neq 0$, if either $ab = ac$ or $ba = ca$ then $b = c$).

Proof. Suppose R has no zero divisors. If $ab = ac$ then $ab - ac = 0$ and $a(b - c) = 0$. Since $a \neq 0$ then it must be that $b - c = 0$ since R has no zero divisors. Hence $b = c$. Similarly, if $ba = ca$ and $a \neq 0$ then $b = c$.

Lemma III.1.A

Lemma III.1.A. A ring has no zero divisors if and only if left or right cancellation hold in R (that is, for all $a, b, c \in R$ with $a \neq 0$, if either $ab = ac$ or $ba = ca$ then $b = c$).

Proof. Suppose R has no zero divisors. If $ab = ac$ then $ab - ac = 0$ and $a(b - c) = 0$. Since $a \neq 0$ then it must be that $b - c = 0$ since R has no zero divisors. Hence $b = c$. Similarly, if $ba = ca$ and $a \neq 0$ then $b = c$.

Suppose left cancellation holds in R. If $ab = 0$ where $a \neq 0$ then $ab = a0$ by Theorem III.1.2(i) and by left cancellation $b = 0$. So a is not a left divisor of 0.

Lemma III.1.A

Lemma III.1.A. A ring has no zero divisors if and only if left or right cancellation hold in R (that is, for all $a, b, c \in R$ with $a \neq 0$, if either $ab = ac$ or $ba = ca$ then $b = c$).

Proof. Suppose R has no zero divisors. If $ab = ac$ then $ab - ac = 0$ and $a(b - c) = 0$. Since $a \neq 0$ then it must be that $b - c = 0$ since R has no zero divisors. Hence $b = c$. Similarly, if $ba = ca$ and $a \neq 0$ then $b = c$.

Suppose left cancellation holds in R. If $ab = 0$ where $a \neq 0$ then $ab = a0$ by Theorem III.1.2(i) and by left cancellation $b = 0$. So a is not a left divisor of 0. Similarly, if right cancellation holds then there are no right divisors of 0. □

Lemma III.1.A

Lemma III.1.A. A ring has no zero divisors if and only if left or right cancellation hold in R (that is, for all $a, b, c \in R$ with $a \neq 0$, if either $ab = ac$ or $ba = ca$ then $b = c$).

Proof. Suppose R has no zero divisors. If $ab = ac$ then $ab - ac = 0$ and $a(b - c) = 0$. Since $a \neq 0$ then it must be that $b - c = 0$ since R has no zero divisors. Hence $b = c$. Similarly, if $ba = ca$ and $a \neq 0$ then $b = c$.

Suppose left cancellation holds in R. If $ab = 0$ where $a \neq 0$ then $ab = a0$ by Theorem III.1.2(i) and by left cancellation $b = 0$. So a is not a left divisor of 0. Similarly, if right cancellation holds then there are no right divisors of 0. □

Theorem III.1.6. Binomial Theorem

Theorem III.1.6. Binomial Theorem.

Let R be a ring with identity, $n \in \mathbb{N}$, and $a, b, a_1, a_2, \ldots, a_s \in R$.

(i) If $ab = ba$ then $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$.

(ii) If $a_i a_j = a_j a_i$ for all i and j, then

$$(a_1 + a_2 + \cdots + a_s)^n = \sum \frac{n!}{i_1! i_2! \cdots i_s!} a_1^{i_1} a_2^{i_2} \cdots a_s^{i_s}$$

where the sum if over all s-tuples $(i_1, i_2, \ldots, i_n)$ where $i_1 + i_2 \cdots + i_s = n$.

Proof. (i) The result holds for $n = 1$. Suppose it holds for n and consider:

$$\begin{aligned}(a+b)^{n+1} &= (a+b)\left(\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}\right) \\ &= \sum_{k=0}^{n} \binom{n}{k} (a^{k+1} b^{n-k} + a^k b^{n-k+1}) \text{ since } ab = ba\end{aligned}$$

Theorem III.1.6. Binomial Theorem

Theorem III.1.6. Binomial Theorem.

Let R be a ring with identity, $n \in \mathbb{N}$, and $a, b, a_1, a_2, \ldots, a_s \in R$.

(i) If $ab = ba$ then $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$.

(ii) If $a_i a_j = a_j a_i$ for all i and j, then

$$(a_1 + a_2 + \cdots + a_s)^n = \sum \frac{n!}{i_1! i_2! \cdots i_s!} a_1^{i_1} a_2^{i_2} \cdots a_s^{i_s}$$

where the sum if over all s-tuples $(i_1, i_2, \ldots, i_n)$ where $i_1 + i_2 \cdots + i_s = n$.

Proof. (i) The result holds for $n = 1$. Suppose it holds for n and consider:

$$\begin{aligned} (a+b)^{n+1} &= (a+b)\left(\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}\right) \\ &= \sum_{k=0}^{n} \binom{n}{k} (a^{k+1} b^{n-k} + a^k b^{n-k+1}) \text{ since } ab = ba \end{aligned}$$

Theorem III.1.6. Binomial Theorem (continued 1)

Proof (continued).

$$\begin{aligned}
(a+b)^{n+1} &= \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^{k} b^{n-k+1} \\
&= \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \binom{n}{(k-1)+1} a^{k} b^{n-(k-1)} \\
&= \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n-1} \binom{n}{k+1} a^{k+1} b^{n-k} + b^{n+1} \\
&\qquad \text{(replacing } k \text{ with } k+1\text{)} \\
&= a^{n+1} + \sum_{k=0}^{n-1} \left(\binom{n}{k} + \binom{n}{k+1} \right) a^{k+1} b^{n-k} + b^{n+1}
\end{aligned}$$

Theorem III.1.6. Binomial Theorem (continued 1)

Proof (continued).

$$\begin{aligned}
(a+b)^{n+1} &= \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k+1} \\
&= \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \binom{n}{(k-1)+1} a^k b^{n-(k-1)} \\
&= \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n-1} \binom{n}{k+1} a^{k+1} b^{n-k} + b^{n+1} \\
&\qquad \text{(replacing } k \text{ with } k+1\text{)} \\
&= a^{n+1} + \sum_{k=0}^{n-1} \left(\binom{n}{k} + \binom{n}{k+1} \right) a^{k+1} b^{n-k} + b^{n+1}
\end{aligned}$$

Theorem III.1.6. Binomial Theorem (continued 2)

Proof (continued).

$$\begin{aligned}(a+b)^{n+1} &= a^{n+1} + \sum_{k=0}^{n-1} \binom{n+1}{k+1} a^{k+1} b^{n-k} + b^{n+1} \\ &\quad \text{since } \binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1} \text{ by Exercise III.1.10(c)} \\ &= a^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} a^k b^{n+1-k} + b^{n+1} \\ &\quad \text{(replacing } k \text{ with } k-1\text{)} \\ &= \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k},\end{aligned}$$

so the result holds for $n+1$ and by mathematical induction, holds for all $n \in \mathbb{N}$.

Theorem III.1.6. Binomial Theorem (continued 2)

Proof (continued).

$$
\begin{aligned}
(a+b)^{n+1} &= a^{n+1} + \sum_{k=0}^{n-1} \binom{n+1}{k+1} a^{k+1} b^{n-k} + b^{n+1} \\
&\qquad \text{since } \binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1} \text{ by Exercise III.1.10(c)} \\
&= a^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} a^{k} b^{n+1-k} + b^{n+1} \\
&\qquad \text{(replacing } k \text{ with } k-1\text{)} \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} a^{k} b^{n+1-k},
\end{aligned}
$$

so the result holds for $n+1$ and by mathematical induction, holds for all $n \in \mathbb{N}$.

Theorem III.1.6. Binomial Theorem (continued 3)

Theorem III.1.6. Binomial Theorem.
Let R be a ring with identity, $n \in \mathbb{N}$, and $a, b, a_1, a_2, \ldots, a_s \in R$.

(ii) If $a_i a_j = a_j a_i$ for all i and j, then

$$(a_1 + a_2 + \cdots + a_s)^n = \sum \frac{n!}{i_1! i_2! \cdots i_s!} a_1^{i_1} a_2^{i_2} \cdots a_s^{i_s}$$

where the sum if over all s-tuples $(i_1, i_2, \ldots, i_n)$ where $i_1 + i_2 \cdots + i_s = n$.

Proof. (ii) When $s = 2$, this is part (i). Suppose the result holds for s and consider

$$\begin{aligned} (a_1 + \cdots + a_s + a_{s+1})^n &= ((a_1 + \cdots + a_s) + a_{s+1})^n \\ &= \sum_{k=0}^{n} \binom{n}{k} (a_1 + \cdots + a_s)^k a_{s+1}^{n-k} \text{ by (i)} \end{aligned}$$

Theorem III.1.6. Binomial Theorem (continued 3)

Theorem III.1.6. Binomial Theorem.
Let R be a ring with identity, $n \in \mathbb{N}$, and $a, b, a_1, a_2, \ldots, a_s \in R$.

(ii) If $a_i a_j = a_j a_i$ for all i and j, then

$$(a_1 + a_2 + \cdots + a_s)^n = \sum \frac{n!}{i_1! i_2! \cdots i_s!} a_1^{i_1} a_2^{i_2} \cdots a_s^{i_s}$$

where the sum if over all s-tuples $(i_1, i_2, \ldots, i_n)$ where $i_1 + i_2 \cdots + i_s = n$.

Proof. (ii) When $s = 2$, this is part (i). Suppose the result holds for s and consider

$$\begin{aligned} (a_1 + \cdots + a_s + a_{s+1})^n &= ((a_1 + \cdots + a_s) + a_{s+1})^n \\ &= \sum_{k=0}^{n} \binom{n}{k} (a_1 + \cdots + a_s)^k a_{s+1}^{n-k} \text{ by (i)} \end{aligned}$$

Theorem III.1.6. Binomial Theorem (continued 4)

Proof (continued).

$$= \sum_{k+j=n;j,k\in\mathbb{N}} \frac{n!}{k!j!}(a_1 + a_2 + \cdots a_s)^k a_{s+1}^j \text{ (replacing } n-k \text{ with } j)$$

$$= \sum_{k+j=n} \frac{n!}{k!j!}\left(\sum \frac{k!}{(i_1)!\cdots(i_s)!} a_1^{i_1} a_2^{i_2} \cdots a_s^{i_s}\right) a_{s+1}^j$$

where $i_1 + i_2 + \cdots + i_s = k$, by the induction hypothesis

$$= \sum_{k+j=n} \left(\sum \left(\frac{n!}{(i_1)!\cdots(i_s)!} a_1^{i_1} a_2^{i_2} \cdots a_s^{i_s}\right) \frac{1}{j!} a_{s+1}^j\right)$$

where the second sum is over $i_1 + i_2 + \cdots + i_n = k$

$$= \sum \frac{n!}{(i_1)!\cdots(i_s)!(i_{s+1})!} a_1^{i_1} a_2^{i_2} \cdots a_s^{i_s} a_{s+1}^{i_{s+1}}$$

where the sum is over $i_1 + i_2 + \cdots i_s + i_{s+1} = n$.

So the result holds for all $s \in \mathbb{N}$, by induction. □

Theorem III.1.9

Theorem III.1.9. Let R be a ring with identity 1_R and characteristic $n > 0$.

(i) If $\varphi : \mathbb{Z} \to R$ is the map given by $m \mapsto m1_R$, then φ is a homomorphism of rings, with kernel $\langle n \rangle = \{kn \mid k \in \mathbb{Z}\} = n\mathbb{Z}$.

(ii) n is the least positive integer such that $n1_R = 0$.

(iii) If R has no zero divisors (in particular, if R is an integral domain) then n is prime.

Proof. **(i)** Let $\ell, m \in \mathbb{Z}$ where f is the mapping such that $f(m) = m1_R$. Then

$$f(\ell + m) = (\ell + m)1_R = \underbrace{1_R + 1_R + \cdots + 1_R}_{\ell+m \text{ times}}$$

$$= \underbrace{1_R + 1_R + \cdots + 1_R}_{\ell \text{ times}} + \underbrace{1_R + 1_R + \cdots + 1_R}_{m \text{ times}} = f(\ell) + f(m),$$

Theorem III.1.9

Theorem III.1.9. Let R be a ring with identity 1_R and characteristic $n > 0$.

(i) If $\varphi : \mathbb{Z} \to R$ is the map given by $m \mapsto m1_R$, then φ is a homomorphism of rings, with kernel $\langle n \rangle = \{kn \mid k \in \mathbb{Z}\} = n\mathbb{Z}$.

(ii) n is the least positive integer such that $n1_R = 0$.

(iii) If R has no zero divisors (in particular, if R is an integral domain) then n is prime.

Proof. (i) Let $\ell, m \in \mathbb{Z}$ where f is the mapping such that $f(m) = m1_R$. Then

$$f(\ell + m) = (\ell + m)1_R = \underbrace{1_R + 1_R + \cdots + 1_R}_{\ell+m \text{ times}}$$

$$= \underbrace{1_R + 1_R + \cdots + 1_R}_{\ell \text{ times}} + \underbrace{1_R + 1_R + \cdots + 1_R}_{m \text{ times}} = f(\ell) + f(m),$$

Theorem III.1.9 (continued 1)

$$f(\ell m) = (\ell m)1_R = \underbrace{1_R + 1_R + \cdots + 1_R}_{\ell m \text{ times}} = \underbrace{1_R \cdot 1_R + 1_R \cdot 1_R + \cdots + 1_R \cdot 1_R}_{\ell m \text{ times}}$$

$$= (\underbrace{1_R + 1_R + \cdots + 1_R}_{\ell \text{ times}})(\underbrace{1_R + 1_R + \cdots + 1_R}_{m \text{ times}}) = (\ell 1_R)(m1_R) = f(\ell)f(m).$$

So f is a ring homomorphism.

Suppose $f(k) = 0$. Then for $k > 0$,

$$f(k) = k\,1_R = \underbrace{1_R + 1_R + \cdots + 1_R}_{k \text{ times}} = 0,$$

and since R is hypothesized to be of characteristic n, then k must be a multiple of n (since n is the smallest positive integer such that $n\,1_R = 0$).

Theorem III.1.9 (continued 1)

$$f(\ell m) = (\ell m)1_R = \underbrace{1_R + 1_R + \cdots + 1_R}_{\ell m \text{ times}} = \underbrace{1_R \cdot 1_R + 1_R \cdot 1_R + \cdots + 1_R \cdot 1_R}_{\ell m \text{ times}}$$

$$= (\underbrace{1_R + 1_R + \cdots + 1_R}_{\ell \text{ times}})(\underbrace{1_R + 1_R + \cdots + 1_R}_{m \text{ times}}) = (\ell 1_R)(m 1_R) = f(\ell)f(m).$$

So f is a ring homomorphism.
Suppose $f(k) = 0$. Then for $k > 0$,

$$f(k) = k\,1_R = \underbrace{1_R + 1_R + \cdots + 1_R}_{k \text{ times}} = 0,$$

and since R is hypothesized to be of characteristic n, then k must be a multiple of n (since n is the smallest positive integer such that $n\,1_R = 0$). So $kn \in \mathrm{Ker}(f)$ for all $k \in \mathbb{N}$. Similarly $-kn \in \mathrm{Ker}(f)$ for all $k \in \mathbb{N}$ and by definition, $0 \in \mathrm{Ker}(f)$. Hence $\mathrm{Ker}(f) = n\mathbb{Z}$.

Theorem III.1.9 (continued 1)

$$f(\ell m) = (\ell m)1_R = \underbrace{1_R + 1_R + \cdots + 1_R}_{\ell m \text{ times}} = \underbrace{1_R \cdot 1_R + 1_R \cdot 1_R + \cdots + 1_R \cdot 1_R}_{\ell m \text{ times}}$$

$$= (\underbrace{1_R + 1_R + \cdots + 1_R}_{\ell \text{ times}})(\underbrace{1_R + 1_R + \cdots + 1_R}_{m \text{ times}}) = (\ell 1_R)(m 1_R) = f(\ell)f(m).$$

So f is a ring homomorphism.
Suppose $f(k) = 0$. Then for $k > 0$,

$$f(k) = k\,1_R = \underbrace{1_R + 1_R + \cdots + 1_R}_{k \text{ times}} = 0,$$

and since R is hypothesized to be of characteristic n, then k must be a multiple of n (since n is the smallest positive integer such that $n\,1_R = 0$). So $kn \in \text{Ker}(f)$ for all $k \in \mathbb{N}$. Similarly $-kn \in \text{Ker}(f)$ for all $k \in \mathbb{N}$ and by definition, $0 \in \text{Ker}(f)$. Hence $\text{Ker}(f) = n\mathbb{Z}$.

Theorem III.1.9 (continued 2)

Theorem III.1.9. Let R be a ring with identity 1_R and characteristic $n > 0$.

(ii) n is the least positive integer such that $n1_R = 0$.

Proof. (ii) If n is the least positive integer such that $n1_R = 0$, then the characteristic of R must be greater than or equal to n.

Theorem III.1.9 (continued 2)

Theorem III.1.9. Let R be a ring with identity 1_R and characteristic $n > 0$.

(ii) n is the least positive integer such that $n1_R = 0$.

Proof. (ii) If n is the least positive integer such that $n\,1_R = 0$, then the characteristic of R must be greater than or equal to n. But also, for all $a \in R$ we have

$$na = n(1_R a) = \underbrace{1_R a + 1_R a + \cdots + 1_R a}_{n \text{ times}}$$

$$= (\underbrace{1_R + 1_R + \cdots + 1_R}_{n \text{ times}})a = (n\,1_R)a = 0a = 0$$

by Theorem III.1.2(i). Hence, the characteristic of R is n.

Theorem III.1.9 (continued 2)

Theorem III.1.9. Let R be a ring with identity 1_R and characteristic $n > 0$.

(ii) n is the least positive integer such that $n1_R = 0$.

Proof. **(ii)** If n is the least positive integer such that $n\,1_R = 0$, then the characteristic of R must be greater than or equal to n. But also, for all $a \in R$ we have

$$na = n(1_R a) = \underbrace{1_R a + 1_R a + \cdots + 1_R a}_{n \text{ times}}$$

$$= (\underbrace{1_R + 1_R + \cdots + 1_R}_{n \text{ times}})a = (n\,1_R)a = 0a = 0$$

by Theorem III.1.2(i). Hence, the characteristic of R is n.

Theorem III.1.9 (continued 3)

Theorem III.1.9. Let R be a ring with identity 1_R and characteristic $n > 0$.

(iii) If R has no zero divisors (in particular, if R is an integral domain) then n is prime.

Proof. **(iii)** Suppose R has characteristic n and R has no zero divisors. ASSUME n is composite, say $n = kr$ with $1 < k < n$ and $1 < r < n$.

Theorem III.1.9 (continued 3)

Theorem III.1.9. Let R be a ring with identity 1_R and characteristic $n > 0$.

(iii) If R has no zero divisors (in particular, if R is an integral domain) then n is prime.

Proof. **(iii)** Suppose R has characteristic n and R has no zero divisors. ASSUME n is composite, say $n = kr$ with $1 < k < n$ and $1 < r < n$. Then $0 = n1_R = (k\,r)1_R 1_R = (k\,1_R)(r\,1_r)$ by part (i). Since R has no divisors of zero, then either $k\,1_R = 0$ or $r\,1_R = 0$.

Theorem III.1.9 (continued 3)

Theorem III.1.9. Let R be a ring with identity 1_R and characteristic $n > 0$.

(iii) If R has no zero divisors (in particular, if R is an integral domain) then n is prime.

Proof. (iii) Suppose R has characteristic n and R has no zero divisors. ASSUME n is composite, say $n = kr$ with $1 < k < n$ and $1 < r < n$. Then $0 = n\,1_R = (k\,r)1_R 1_R = (k\,1_R)(r\,1_r)$ by part (i). Since R has no divisors of zero, then either $k\,1_R = 0$ or $r\,1_R = 0$. But then, by part (ii), the characteristic of R is then either $\leq k$ or $\leq r$, a CONTRADICTION. So the assumption that n is composite is false and n must be prime. □

Theorem III.1.9 (continued 3)

Theorem III.1.9. Let R be a ring with identity 1_R and characteristic $n > 0$.

(iii) If R has no zero divisors (in particular, if R is an integral domain) then n is prime.

Proof. (iii) Suppose R has characteristic n and R has no zero divisors. ASSUME n is composite, say $n = kr$ with $1 < k < n$ and $1 < r < n$. Then $0 = n\,1_R = (k\,r)1_R 1_R = (k\,1_R)(r\,1_r)$ by part (i). Since R has no divisors of zero, then either $k\,1_R = 0$ or $r\,1_R = 0$. But then, by part (ii), the characteristic of R is then either $\leq k$ or $\leq r$, a CONTRADICTION. So the assumption that n is composite is false and n must be prime. □

Theorem III.1.10

Theorem III.1.10. Every ring R may be embedded in a ring S with identity (that is, there is a one to one homomorphism mapping R into S).The ring S (which is not unique) may be chosen to be either of characteristic zero or of the same characteristic as R.

Proof. Let S be the additive abelian group $R \oplus \mathbb{Z}$ and define multiplication in S by $(r_1, k_1)(r_2, k_2) = (r_1 r_2 + k_2 r_1 + k_1 r_2, k_1 k_2)$. It is straightforward to verify that S is a ring.

Theorem III.1.10

Theorem III.1.10. Every ring R may be embedded in a ring S with identity (that is, there is a one to one homomorphism mapping R into S).The ring S (which is not unique) may be chosen to be either of characteristic zero or of the same characteristic as R.

Proof. Let S be the additive abelian group $R \oplus \mathbb{Z}$ and define multiplication in S by $(r_1, k_1)(r_2, k_2) = (r_1 r_2 + k_2 r_1 + k_1 r_2, k_1 k_2)$. It is straightforward to verify that S is a ring. Now $(r_1, k_1)(0, 1) = (r_1(0) + 1r_1 + k_1(0), k_1(1)) = (r_1, k_1)$, so $(0, 1)$ is the multiplicative identity in S. From Theorem III.1.9(ii), by considering $(0, 1)$ we see that S is of characteristic 0. Define $g : R \to S$ as $g(r) = (r, 0)$.

Theorem III.1.10

Theorem III.1.10. Every ring R may be embedded in a ring S with identity (that is, there is a one to one homomorphism mapping R into S).The ring S (which is not unique) may be chosen to be either of characteristic zero or of the same characteristic as R.

Proof. Let S be the additive abelian group $R \oplus \mathbb{Z}$ and define multiplication in S by $(r_1, k_1)(r_2, k_2) = (r_1 r_2 + k_2 r_1 + k_1 r_2, k_1 k_2)$. It is straightforward to verify that S is a ring. Now $(r_1, k_1)(0, 1) = (r_1(0) + 1r_1 + k_1(0), k_1(1)) = (r_1, k_1)$, so $(0, 1)$ is the multiplicative identity in S. From Theorem III.1.9(ii), by considering $(0, 1)$ we see that S is of characteristic 0. Define $g : R \to S$ as $g(r) = (r, 0)$. Then $g(r_1 + r_2) = (r_1 + r_2, 0) = (r_1, 0) + (r_2, 0) = g(r_1) + g(r_2)$ and $g(r_1 r_2) = (r_1 r_2, 0) = (r_1, 0)(r_2, 0) = g(r_1)g(r_2)$ hence g is a homomorphism. "Clearly" g is one to one. So R is embedded in S where S has characteristic 0.

Theorem III.1.10

Theorem III.1.10. Every ring R may be embedded in a ring S with identity (that is, there is a one to one homomorphism mapping R into S).The ring S (which is not unique) may be chosen to be either of characteristic zero or of the same characteristic as R.

Proof. Let S be the additive abelian group $R \oplus \mathbb{Z}$ and define multiplication in S by $(r_1, k_1)(r_2, k_2) = (r_1 r_2 + k_2 r_1 + k_1 r_2, k_1 k_2)$. It is straightforward to verify that S is a ring. Now $(r_1, k_1)(0, 1) = (r_1(0) + 1r_1 + k_1(0), k_1(1)) = (r_1, k_1)$, so $(0, 1)$ is the multiplicative identity in S. From Theorem III.1.9(ii), by considering $(0, 1)$ we see that S is of characteristic 0. Define $g : R \to S$ as $g(r) = (r, 0)$. Then $g(r_1 + r_2) = (r_1 + r_2, 0) = (r_1, 0) + (r_2, 0) = g(r_1) + g(r_2)$ and $g(r_1 r_2) = (r_1 r_2, 0) = (r_1, 0)(r_2, 0) = g(r_1)g(r_2)$ hence g is a homomorphism. "Clearly" g is one to one. So R is embedded in S where S has characteristic 0.

Theorem III.1.10 (continued)

Theorem III.1.10. Every ring R may be embedded in a ring S with identity (that is, there is a one to one homomorphism mapping R into S).The ring S (which is not unique) may be chosen to be either of characteristic zero or of the same characteristic as R.

Proof. If the characteristic of R is $n > 0$, define $S = R \oplus \mathbb{Z}_n$ and define multiplication by $(r_1, \overline{k}_1)(r_2, \overline{k}_2) = (r_1 r_2 + k_2 r_2 r_1 + k_1 r_2, \overline{k}_1 \overline{k}_2)$ where $\overline{k}_i$ is the equivalence class on $\mathbb{Z}$ containing k_i with $0 \le k_i < n$. It is straightforward to verify that S is a ring.

Theorem III.1.10 (continued)

Theorem III.1.10. Every ring R may be embedded in a ring S with identity (that is, there is a one to one homomorphism mapping R into S).The ring S (which is not unique) may be chosen to be either of characteristic zero or of the same characteristic as R.

Proof. If the characteristic of R is $n > 0$, define $S = R \oplus \mathbb{Z}_n$ and define multiplication by $(r_1, \overline{k}_1)(r_2, \overline{k}_2) = (r_1 r_2 + k_2 r_2 r_1 + k_1 r_2, \overline{k}_1 \overline{k}_2)$ where $\overline{k}_i$ is the equivalence class on $\mathbb{Z}$ containing k_i with $0 \leq k_i < n$. It is straightforward to verify that S is a ring. As above, $(0, \overline{1})$ is the multiplicative identity and S is of characteristic n. As above, $g : R \to S$ defined as $g(r) = (r, \overline{0})$ is a one to one homomorphism and so R is embedded in S where S has characteristic n. □

Theorem III.1.10 (continued)

Theorem III.1.10. Every ring R may be embedded in a ring S with identity (that is, there is a one to one homomorphism mapping R into S).The ring S (which is not unique) may be chosen to be either of characteristic zero or of the same characteristic as R.

Proof. If the characteristic of R is $n > 0$, define $S = R \oplus \mathbb{Z}_n$ and define multiplication by $(r_1, \overline{k}_1)(r_2, \overline{k}_2) = (r_1 r_2 + k_2 r_2 r_1 + k_1 r_2, \overline{k}_1 \overline{k}_2)$ where $\overline{k}_i$ is the equivalence class on $\mathbb{Z}$ containing k_i with $0 \leq k_i < n$. It is straightforward to verify that S is a ring. As above, $(0, \overline{1})$ is the multiplicative identity and S is of characteristic n. As above, $g : R \to S$ defined as $g(r) = (r, \overline{0})$ is a one to one homomorphism and so R is embedded in S where S has characteristic n. □