CHAPTER

TEN

GROUPS AND RINGS

10.1 (a), (b), (c), (e) Yes. (d) No.

10.2 (a)

$$a \bigstar (b \bigstar c) = a \bigstar b = a$$
$$(a \bigstar b) \bigstar c = a \bigstar c = a$$

(b) Only if A has only one element.

10.3 $(a \bigstar b) \bigstar (a \bigstar c) = (a \bigstar a) \bigstar (b \bigstar c) = a \bigstar (b \bigstar c)$

10.4 (a)

	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

(b) Closure is obvious. Associativity can be seen from

$$\begin{aligned}(a \odot b) \odot c &= r_1 \odot c \text{ where } r_1 = \text{reminder of } ab/n,\\ &= r_2 \text{ where } r_2 = \text{remainder of } r_1c/n\\ &= \text{remainder of } abc/n\\ &= a \odot (b \odot c) \text{ since this is also the remainder of } abc/n.\end{aligned}$$

10.5 $(x \square y) \square z = (x * a * y) * a * z = x * a * (y * a * z)$
$x \square (y * z) = x * a * (y * a * z)$

10.6 (a)

$$(a * a) * a = a * (a * a)$$

Thus, $a * a = a$

(b)

$$\begin{aligned}(a * b * a) * a &= a * b * (a * a) = a * b * a\\ &= (a * a) * b * a = a * (a * b * a)\end{aligned}$$

Thus, $a * b * a = a$

(c) $(a * b * c) * (a * c) = a * b * (c * a * c) = a * b * c$

$= (a * c * a) * b * c = (a * c) * (a * b * c)$

Thus, $a * b * c = a * c$.

10.7 $(a * b) * c = a * (b * c) = a * (c * b)$

$= (a * c) * b = (c * a) * b$

$= c * (a * b)$

10.8 (a) $a * (a * a) = a * b$

$(a * a) * a = b * a$

(b) If $b * b = a$, then $a * (b * b) = a * a = b$.

Suppose $a * b = a$, $(a * b) * b = a * b = a$.

Suppose $a * b = b$, $(a * b) * b = b * b = a$.

Thus, $b * b \neq a$, and we must have $b * b = b$.

10.9 $(a * b) * (a * b) = a * (b * a) * b$

$= (a * a) * (b * b)$

$= a * b$

10.10 Use induction on $|A|$. The result is trivially true for $|A| = 1$. Assume $|A| = n$ and the result holds for all smaller semigroups. Let $a \in A$ and consider a, a^2, $a^3, \ldots, a^{n+1}$. These are not all distinct, so $a^i = a^j$, for some $i < j$. Then $a^{i+1} = a^{j+1}$ for all l and the sequence a^i, $a^{i+1}, \ldots, a^{j-1}$ repeats. Hence $(\{a^i, \ldots, a^{j-1}\}, *\}$ is a semigroup. If $j - i < |A|$, then by induction there is an $a^k \in \{a^i, \ldots, a^{j-1}\} \subseteq A$ satisfying the result. If $j - i = n$, then $(A, *)$ is isomorphic to the integers modulo n under addition and a^{j-i} is the identity element.

10.11 For a, there exist u_1 and v_1 such that $a * u_1 = v_1 * a = a$. It follows that $v_1 * a * u_1 = a$. For any x, $x = a * u_1 = v_1 * a * u_1 = v_1 * x$.

Thus, v_1 is a left identity.

For any x, $x = v_1 * a = v_1 * a * u_1 = x * u_1$.

Thus, u_1 is a right identity.

It follows that $v_1 = u_1$ and is the identity.

10.12 (a) $a * b = a * c$

$$\hat{a} * a * b = \hat{a} * a * c$$
$$e * b = e * c$$
$$b = c$$

(b) $\hat{x} * x * (\hat{x} * x) = \hat{x} * x * e$

Also, $(\hat{x} * x) * \hat{x} * x = e * \hat{x} * x = \hat{x} * x$

Thus, $\hat{x} * x * e = \hat{x} * x$

According to (a), $x * e = x$

Thus, e is also a right identity.

10.13 (a) $a \bigstar (a \bigstar b) = [(a \bigstar b) \bigstar a] \bigstar (a \bigstar b) = a \bigstar b.$

(b) $a \bigstar a = [(a \bigstar b) \bigstar a] \bigstar a$ (by (i))[†]

$= [a \bigstar (a \bigstar b)] \bigstar (a \bigstar b)$ (by (ii))

$= (a \bigstar b) \bigstar (a \bigstar b)$ (by part (a))

(c) $a \bigstar a = (a \bigstar b) \bigstar (a \bigstar b)$ (by part (b))

$= [(a \bigstar b) \bigstar b] \bigstar [(a \bigstar b) \bigstar b]$ (by part (b))

$= [(b \bigstar a) \bigstar a] \bigstar [(b \bigstar a) \bigstar a]$ (by (ii))

$= b \bigstar b$ (by (i))

(d) $(a \bigstar a) \bigstar a = a$ (by (i))

$a \bigstar (a \bigstar a) = a \bigstar a = e$ (by part (a))

(e) If $a \bigstar b = b \bigstar a$

$a = (a \bigstar b) \bigstar a$ (by (i))

$= (b \bigstar a) \bigstar a$

$= (a \bigstar b) \bigstar b$ (by (ii))

$= (b \bigstar a) \bigstar b$

$= b$ (by (i))

If $a = b$ then obviously,

$a \bigstar b = b \bigstar a$

(f) $a \bigstar a = (a \bigstar a) \bigstar a = a$

$a \bigstar b = (a \bigstar b) \bigstar b = (b \bigstar a) \bigstar a = b \bigstar a$

10.14 (a) $((a \bigstar a) \bigstar (a \bigstar b)) \bigstar ((a \bigstar b) \bigstar c) = a \bigstar b$

$((a \bigstar a) \bigstar (a \bigstar b)) \bigstar ((a \bigstar b) \bigstar c) = a \bigstar ((a \bigstar b) \bigstar c)$

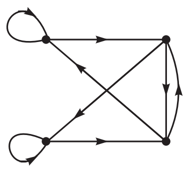
Thus, $a \bigstar b = a \bigstar ((a \bigstar b) \bigstar c)$

The other equality can be proved in a similar fashion.

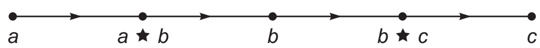
(b) Since $(a \bigstar ((d \bigstar (b \bigstar c)) \bigstar d)) \bigstar ((b \bigstar c) \bigstar d) = b \bigstar c$

$(b \bigstar c) \bigstar (c \bigstar d) = ((a \bigstar (d \bigstar (b \bigstar c)) \bigstar d)) \bigstar ((b \bigstar c) \bigstar d)) \bigstar (c \bigstar d) = c$

(c)



(d) Consider the path



We must have $(a \bigstar b) \bigstar (b \bigstar c) = c$

[†](i) and (ii) refer to the two given conditions.

(e) We show first there is an edge (c, b) in E if and only if $c = a \star b$ for some a. If (c, b) is in E, $b = c \star d$ for some d, hence $(c \star c) \star b = (c \star c) \star (c \star d) = c$. Conversely, if $a \star b = c$, then there is an edge from c to $(a \star b) \star (b \star b)$ which is b.
Now, for any two vertices, there is a path

$$a \longrightarrow a \star b \longrightarrow b$$

To show that this path is unique, we note that if we have a path then $a = d_1 \star c$ and $b = c \star d_2$ for some d_1 and d_2.

$$a \longrightarrow c \longrightarrow b$$

Thus, $a \star b = (d_1 \star c) \star (c \star d_2) = c$.

(f) For any c in $L(b)$ there is a unique d in $R(a)$ such that there is a path

$$a \longrightarrow d \longrightarrow c \longrightarrow b$$

Therefore, there is a one to one correspondence between the elements in $R(a)$ and $L(b)$.

(g) The sets $R(b_1), R(b_2),\ldots, R(b_m)$ are mutually disjoint and their union contains all the elements in A.

10.15 $b \star d = b \star (c \star c^{-1}) \star (a^{-1} \star a) \star d$
$= (b \star c) \star (a \star c)^{-1} \star (a \star d)$
$= (b_1 \star c_1) \star (a_1 \star c_1)^{-1} \star (a_1 \star d_1)$
$= (b_1 \star c_1) \star (c_1^{-1} \star a_1^{-1}) \star (a_1 \star d_1)$
$= b_1 \star d_1$

10.16 (a) Let a be the non-identity element of the group. Then $a^2 \neq a$, so $a^2 = e$, the identity, and G is cyclic of order 2. The function f: $\{a, e\} \to \{0, 1\}$ for which $f(a) = 1, f(e) = 0$ is an isomorphism.

(b) Similar to the argument in (a), any non-identity element a must generate the whole group, and the function $f(a) = 1, f(a^2) = 2, f(e) = 0$ is the isomorphism. ($a^2 \neq a$. $a^2 \neq e$. Since if $a^2 = e$, $ab = b$ implies $a = e$.)

(c) There are 2, the cyclic group of order 4 and the group all of whose non-indentity elements have order 2.

10.17 It is clearly closed.
$((a_1, b_1) \square (a_2, b_2)) \square (a_3, b_3)$
$= (a_1 \star a_2, b_1 * b_2) \square (a_3, b_3) = ((a_1 \star a_2) \star a_3, (b_1 * b_2) * b_3)$
$= (a_1 \star (a_2 \star a_3), b_1 * (b_2 * b_3)) = (a_1, b_1) \square ((a_2, b_2) \square (a_3, b))$
So, it is associative.

If a_A and e_B are identities of A and B, then (e_A, e_B) is the identity of $A \times B$ and the inverse of (a, b) is (a^{-1}, b^{-1}).

10.18 (a) $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = e$

(b) By induction: $((a_1 \ldots a_{r-1})a_r)^{-1} = a_r^{-1}(a_1 \ldots a_{r-1})^{-1}$

$$= a_r^{-1}\, a_{r-1}^{-1} \ldots a_1^{-1}$$

(c) Follows from (b) setting $a_1, \ldots, a_i$ to a and $a_{i+1}, \ldots, a_r$ to b, with $r = i + j$.

10.19 Clearly, $x^{-1} = x$. Commutativity follows from

$$(x * y)^{-1} = y^{-1} * x^{-1} = y * x$$
$$(x * y)^{-1} = x * y$$

10.20 (i) H is non-empty. For $a \in H$, $a \bigstar a^{-1} = e$ is in H.

(ii) For $a \in H$, $e \bigstar a^{-1} = a^{-1}$ is in H.

(iii) $\bigstar$ is closed. Since for $a, b \in H$, $a \bigstar (b^{-1})^{-1} = a \bigstar b$ is in H.

10.21 Let a be a generator of the group G and let a^i be the smallest power, $i > 0$, of a such that a^i is in the subgroup H. If a^i does not generate H, let a^j be an element of H which is not a power of a^i. The *g. c. d.* of i and j is not i since if $j = hi$, then $a^j = (a^i)^h$. Hence $d = (j, i) < i$. But $d = mj + ni$ for some integers m and n. Thus $a^d = (a^j)^m\,(a^i)^n \in H$ but $d < i$ contradicting our assumption that i was minimal.

10.22 $\{a, a^2, \ldots a^m\}$ is a subgroup of the group. Thus, according to Theorem 11.3 m divides the order of the group.

10.23 There exists a_1 that is in H_1 but not in H_2. There exists a_2 that is in H_2 but not in H_1. We claim that $a_1 a_2$ is not in H_1. Suppose $a_1 a_2$ is in H_1. Because a_1^{-1} is in H_1, a_2 will be in H_1, which is a contradiction. Similarly, $a_1 a_2$ is not in H_2.

10.24 (i) Closure: If $x \in N$ and $y \in N$, then $xy \in N$ since $xyHy^{-1}x^{-1} = xHx^{-1} = H$.

(ii) Identity: $eHe^{-1} = H$.

(iii) Inverse: If $xHx^{-1} = H$, $H = x^{-1}Hx$.

10.25 If x is the inverse of y, then y is the inverse of x. Since e is the inverse of e, there exists an element a, $a \neq e$, such that a is the inverse of itself. (Because we can pair off the elements x and x^{-1}, and the number of elements is even.)

10.26 Consider the set $C = \{a \bigstar b^{-1} \mid b \in B\}$. Since $|C| = |B|$, there is an element that is in both B and C. That is, $b_1 = a \bigstar b_2^{-1}$, or $a = b_1 \bigstar b_2$.

10.27 Suppose that $HK = KH$, that is, for $h \in H$ and $k \in K$ there exist $h_1 \in H$ and $k_1 \in K$ such that $hk = k_1 h_1$. To show that HK is closed, we note that $h(kh')\, k' = h(h_1 k_1)k'$ which is in HK. To show that if x is in HK then so is x^{-1}, we note $(hk)^{-1} = k^{-1}\, h^{-1} \cdot k^{-1}\, h^{-1}$ is in KH which is equal to HK.

Suppose that HK is a subgroup. For any $h \in H$ and $k \in H$, $h^{-1}k^{-1}$ is in HK. Thus, $kh = (h^{-1}\, k^{-1})^{-1}$ is in HK. We have $KH \subseteq HK$. Also, if x is in HK, $x^{-1} = hk$ is also in HK. $x = k^{-1}\, h^{-1}$ is in KH. Therefore, we have $HK \subseteq KH$.

10.28 If $(A, \bigstar)$ is abelian, then $(a \bigstar b) \bigstar (a \bigstar b) = (a \bigstar a) \bigstar (b \bigstar b)$

If $(a \bigstar b)^2 = a^2 \bigstar b^2 = a \bigstar a$, then

$$a \bigstar b \bigstar a \bigstar b = a \bigstar a \bigstar b \bigstar b$$

$$a^{-1} \bigstar (a \bigstar b \bigstar a \bigstar b) \bigstar b^{-1} = a^1 \bigstar (a \bigstar a\, (a \bigstar a \bigstar b \bigstar b) \cdot b^{-1}$$

$$b \bigstar a = a \bigstar b$$

10.29 $a^3 \bigstar b^3 = (a \bigstar b)^3$ implies that

$$a^2 \bigstar b^2 = b \bigstar a \bigstar b \bigstar a \qquad (1)$$

$a^4 \bigstar b^4 = (a \bigstar b)^4$ implies that

$$a^4 \bigstar b^3 = b \bigstar a \bigstar b \bigstar a \bigstar b \bigstar a \qquad (2)$$

Combining (1) and (2), we obtain

$$a^3 \bigstar b^3 = a^2 \bigstar b^2 \bigstar b \bigstar a$$

which implies that $a \bigstar b^3 = b^3 \bigstar a$ (3)

$a^5 \bigstar b^5 = (a \bigstar b)^5$ implies that

$$a^4 \bigstar b^4 = b \bigstar a \bigstar b \bigstar a \bigstar b \bigstar a \bigstar b \bigstar a \qquad (4)$$

Combining (2) and (4), we obtain

$$a^4 \bigstar b^4 = a^3 \bigstar b^3 \bigstar b \bigstar a$$

$$a \bigstar b^4 = b^4 \bigstar a \qquad (5)$$

Combining (3) and (5), we obtain

$$b^3 \bigstar a \bigstar b = b^4 \bigstar a$$

which implies that $a \bigstar b = b \bigstar a$

10.30 G is partitioned into H and $a \bigstar H$. G is also partitioned into H and $H \bigstar a$. Thus, we must have $a \bigstar H = H \bigstar a$.

10.31 Suppose H is normal. Then $a \bigstar H = H \bigstar a$.

If $x \in a \bigstar H \bigstar a^{-1}$, then $x = a \bigstar h \bigstar a^{-1}$

$$= h_1 \bigstar a \bigstar a^{-1} = h_1 \in H$$

Conversely, if $a \bigstar H \bigstar a^{-1} \subseteq H$ for all a, then

$$a \bigstar h \bigstar a^{-1} = h_1 \in H.$$

Hence, $a \star h = h_1 \star a$ and $a \star H \subseteq H \star a$

Also, for $h \in H$, $a^{-1} \star h \star a = h_1 \in H$,

so $h \star a = a \star h_1$ and $H \star a \subseteq a \star H$.

10.32 H is closed since $a, b \in H$ and $c \in G$ implies that $(a \star b) \star c = a \star c \star b = c \star (a \star b)$. Clearly, $e \in H$. If $a \in H$, then $(a^{-1} \star b)^{-1} = b^{-1} \star a = a \star b^{-1} = (b \star a^{-1})^{-1}$, so $a^{-1} \star b = b \star a^{-1}$.

10.33 (a) Since $e \in H$ and $e \in K$, $H \cap K \neq \emptyset$. For $a, b \in H \cap K$, $a \star b^{-1} \in H \cap K$ since both H and K contain inverse and are closed.

(b) Consider the coset $a \star (H \cap K) = \{a \star x | x \in H \cap K\}$. For $a \star x \in a \star (H \cap K)$, $a \star x \in a \star H$ so $a \star x \in H \star a$. Similarly, $a \star x \in K \star a$. Since $a \star x = y \star a$ for a unique y, we have $y \in H$ and $y \in K$. Thus, $a \star x \in (H \cap K) \star a$. The same reasoning shows that if $x \star a \in (H \cap K) \star a$ then $x \star a \in a \star (H \cap K)$.

10.34 Suppose (1), (2), and (3) hold. Then

$$\begin{aligned} f((a_1, b_1) \square (a_2, b_2)) &= f(a_1 \star a_2, b_1 \star b_2) \\ &= a_1 \star a_2 \star b_1 \star b_2 \end{aligned}$$

Since H and K are both normal, $a_2 \star b_1 \star a_2^{-1} \star b_1^{-1} \in H \cap K$ ($a_2 \star b_1 \star a_2^{-1} \in K$, $b_1 \star a_2^{-1} \star b_1^{-1} \in H$). Since $H \cap K = \{e\}$, $(a_2 \star b_1)^{-1} = a_2^{-1} \star b_1^{-1} = b_1^{-1} \star a_2^{-1}$. It follows that for any two elements $a \in H$, $b \in K$, $a \star b = b \star a$. Thus

$$\begin{aligned} a_1 \star a_2 \star b_1 \star b_2 &= a_1 \star b_1 \star a_2 \star b_2 \\ &= f(a_1, b_1) \star f(a_2, b_2) \end{aligned}$$

and f is a homomorphism.

$$f(a, b) = e \leftrightarrow a \star b = e \leftrightarrow a = b^{-1} \Rightarrow a \in H \cap K.$$

Since $H \cap K = \{e\}$, $f(a, b) = e \Rightarrow a = b = e$ and f is one-to-one.
Since $G = \{h \star k | h \in H, k \in K\}$, for any $g \in G$, $g = h \star k = f(h, k)$ so f in onto.

Suppose f is an isomorphism. Then for any $g \in G$, $g = f(h, k) = h \star k$ so (2) is satisfied. If $a \in H \cap K$, then $a^{-1} \in H \cap K$ and $(a, a^{-1}) \in H \times K$. $f(a, a^{-1}) = e$ so $(a, a^{-1}) = (e, e)$ since f is one-to-one. Hence, $a = e$ and $H \cap K = \{e\}$. Finally, if $h \in H$, $k \in K$ then $f((h, k)\ (h, k)) = (h \star h) \star (k \star k) = f(h, k) \star f(h, k) = h \star k \star h \star k$, so $h \star k = k \star h$. Thus, for any $g = h \star k \in G$

$$\begin{aligned} g \star H = h \star k \star H &= \{h \star k \star a | a \in H\} = \{h \star a \star k | a \in H\} \\ &= \{a \star k | a \in H\} \\ &= \{a \star h \star k | a \in H\} \\ &= H \star h \star k \end{aligned}$$

so H, and similarly K, are normal.

10.35 If $a \bigstar b \bigstar a^{-1} \bigstar b^{-1} \in H$ for all $a, b \in G$, then $(a \bigstar H) \bigstar (b \bigstar H) = a \bigstar b \bigstar H$, while $b^{-1} \bigstar a^{-1} \bigstar b \bigstar a \in H$. Hence, $a \bigstar b \bigstar b^{-1} \bigstar a^{-1} \bigstar b \bigstar a \bigstar H = a \bigstar b \bigstar H$ and $b \bigstar a \bigstar H = a \bigstar b \bigstar H$. Thus G/H is abelian.

If G/H is abelian, then $b^{-1} \bigstar a^{-1} \bigstar H = a^{-1} \bigstar b^{-1} \bigstar H$ and $b^{-1} \bigstar a^{-1} \bigstar h = a^{-1} \bigstar b^{-1}$ for some $h \in H$. $h = a \bigstar b \bigstar a^{-1} \bigstar b^{-1}$ and for all $a, b \in G$, $a \bigstar b \bigstar a^{-1} \bigstar b^{-1} \in H$.

10.36 (a) $(a \bigstar b) \bigstar c = a \bigstar (b \bigstar c)$

$$f((a \bigstar b) \bigstar c) = f(a \bigstar b) * f(c) = (f(a) * f(b)) * f(c)$$
$$f(a \bigstar (b \bigstar c)) = f(a) * f(b \bigstar c) = f(a) * (f(b) * f(c))$$

Note that given x, y, z in B, there exist a, b, c in A such that

$$f(a) = x, f(b) = y, f(c) = z$$

(b) $a \bigstar e = a \quad \Rightarrow \quad f(a) * f(e) = f(a)$

$e \bigstar a = a \quad \Rightarrow \quad f(e) * f(a) = f(a)$

(c) $a \bigstar b = e \quad \Rightarrow \quad f(a) * f(b) = f(e)$

10.37 $g(a \bigstar b) = f_1(a \bigstar b) * f_2(a \bigstar b)$
$= f_1(a) * f_1(b) * f_2(a) * f_2(b)$
$= f_1(a) * f_2(a) * f_1(b) * f_2(b)$
$= g(a) * g(b)$

Hence, g is a homomorphism from $(A, \bigstar)$ to $B, *)$.

10.38 (1) $f(e) = g(e) =$ identity of $(H, *)$
Thus, $e \in C$.

(2) If $f(a) = g(a) = a'$
then $f(a^{-1}) = g(a^{-1}) = (a')^{-1}$

(3) If $f(a) = g(a)$ and $f(b) = g(b)$,
then $f(a \bigstar b) = f(a) * f(b) = * g(a) * g(b) = g(a \bigstar b)$

Hence, $(C, \bigstar)$ is a subgroup of $(G, \bigstar)$.

10.39 $\frac{1}{2}(4^6 + 4^3) = 160$

10.40 $\frac{1}{4}(3^8 + 3^2 + 3^4 + 3^2) = 1665$

10.41 (a) $\frac{1}{4}(2^4 + 2 + 4 + 2) = 6$

(b) $\frac{1}{4}(2^{16} + 2^4 + 2^8 + 2^4) = 16{,}456$

10.42 (a) $p < \dfrac{1}{2} \Rightarrow \dfrac{p}{1-p} < 1$

Thus, for $t_1 < t_2$, $\left(\dfrac{p}{1-p}\right)^{t_1} > \left(\dfrac{p}{1-p}\right)^{t_2}$

or $(1-p)^n \left(\dfrac{p}{1-p}\right)^{t_1} > (1-p)^n \left(\dfrac{p}{1-p}\right)^{t_2}$

(b) Similar to (a)

10.43 (a)

00000	11111
00001	11110
00010	11101
00100	11011
01000	10111
10000	01111
00011	11100
00101	11010
01001	10110
10001	01110
00110	11001
01010	10101
10010	01101
01100	10011
10100	01011
11000	00111

(b) To show that $(G, \oplus)$ is a group, we note that (i) associativity is obvious, (ii) 0000000 is the identity, and (iii) every word is its own inverse. Closure follows from the observation that

(1) 1101000 $\oplus$ a cyclic shift of 1101000 = a cyclic shift of 0010111

(2) 1101000 $\oplus$ 1111111 = 0010111.

10.44 We show first $e_1 = e_1 * e_2$

$$\begin{aligned} &= e_1 * (e_2 \bigstar e_1) \\ &= (e_1 * e_2) \bigstar (e_1 * e_1) \\ &= e_1 \bigstar (e_1 * e_1) \\ &= e_1 * e_1 \end{aligned}$$

Now $x = x \bigstar e_1 = x \bigstar (e_1 * e_1) = (x \bigstar e_1) * (x \bigstar e_1)$

$= x * x$

That $x = x \bigstar x$ can be proved in a similar fashion.

10.45 $a * (b \bigstar c) = a * b$

$$(a * b) \bigstar (a * c) = a * b$$

10.46 (a) $(a + a) \cdot (a + a) = a \cdot a + a \cdot a + a \cdot a + a \cdot a = a + a + a + a = a + a$
Thus, $a + a = 0$

(b) $(a + b) \cdot (a + b) = a \cdot a + a \cdot b + b \cdot a + b \cdot b = a + a \cdot b + b \cdot a + b = a + b$
Thus, $a \cdot b + b \cdot a = 0$. Since $a \cdot b + a \cdot b = 0$, we have $a \cdot b = b \cdot a$.

10.47 Let $x_1, x_2, \ldots, x_n$ denote the elements in the integral domain. Let $a \neq 0$ be one of the elements in the integral domain. We note that $x_1 \cdot a, x_2 \cdot a, \ldots, x_n \cdot a$ are all distinct. (If not, we have $x_i \cdot a - x_j \cdot a = 0$ implying that $(x_i - x_j) \cdot a = 0$ or $x_i = x_j$.) Thus, every element y in the integral domain can be written as $x_i \cdot a$ for some x_i. In particular, we have $a = x_j \cdot a$ for some x_j. Thus, $a = x_j \cdot a = a \cdot x_j$. We claim that x_j is a multiplicative identity, since for any element y in the integral domain, $y \cdot x_j = (x_i \cdot a) \cdot x_j = x_i \cdot (a \cdot x_j) = x_i \cdot a = y$.

Now, for any $a \neq 0$, there exists an x_k such that $x_k \cdot a = x_i$. Thus, x_k is the multiplicative inverse of a.

10.48 (a)

0	2	3	4
1	2	3	0
2	3	0	1
3	0	1	2

(b)

0	1	2	0	1	2
1	2	0	2	0	1
2	0	1	1	2	0

10.49 (a) Since the ideal H will be the additive identity (0) in the homomorphic image, according to the definition of a prime ideal, in the homomorphic image, the product of two cosets is equal to H only if one of them is H.

(b) Suppose H is a maximal ideal. Let b be any element in A but not in H. The set of all elements $c + b \cdot x$ for any c in H and any x in A can be shown to be an ideal. Since this ideal contains b which is not in H, and since H is a maximal ideal, it must be the whole ring A. In particular, 1 (the multiplicative identity) is in the ideal. That is, for some a, $1 = c + b \cdot a$. Note that 1 will be in the coset which is the multiplicative identity of the homomorphic image. Thus, the coset containing a is the multiplicative inverse of the coset containing b in the homomorphic image. The converse can be proved in a similar manner.

10.50 (a)

$\triangle$	0	1	x	$1+x$
0	0	1	x	$1+x$
1	1	0	$1+x$	x
x	x	$1+x$	0	1
$1+x$	$1+x$	x	1	0

$\triangle$	0	1	x	$1+x$
0	0	0	0	0
1	0	1	x	$1+x$
x	0	x	$1+x$	1
$1+x$	0	$1+x$	1	x

(b)

$\triangle$	0	1	2	x	$1+x$	$2+x$	$2x$	$1+2x$	$2+2x$
0	0	1	2	x	$1+x$	$2+x$	$2x$	$1+2x$	$2+2x$
1	1	2	0	$1+x$	$2+x$	x	$1+2x$	$2+2x$	$2x$
2	2	0	1	$2+x$	x	$1+x$	$2+2x$	$2x$	$1+2x$
x	x	$1+x$	$2+x$	$2x$	$1+2x$	$2+2x$	0	1	2
$1+x$	$1+x$	$2+x$	x	$1+2x$	$2+2x$	$2x$	1	2	0
$2+x$	$2+x$	x	$1+x$	$2+2x$	$2x$	$1+2x$	2	0	1
$2x$	$2x$	$1+2x$	$2+2x$	0	1	2	x	$1+x$	$2+x$
$1+2x$	$1+2x$	$2+2x$	$2x$	1	2	0	$1+x$	$2+x$	x
$2+2x$	$2+2x$	$2x$	$1+2x$	2	0	1	$2+x$	x	$1+x$

$\triangle$	0	1	2	x	$1+x$	$2+x$	$2x$	$1+2x$	$2+2x$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$1+x$	$2+x$	$2x$	$1+x$	$2+2x$
2	0	2	1	$2x$	$2+2x$	$1+2x$	x	$2+x$	$1+x$
x	0	x	$2x$	$1+x$	$1+2x$	1	$2+2x$	2	$2+x$
$1+x$	0	$1+x$	$2+2x$	$1+2x$	2	x	$2+x$	$2x$	1
$2+x$	0	$2+x$	$1+2x$	1	x	$2+2x$	2	$1+x$	$2x$
$2x$	0	$2x$	x	$2+2x$	$2+x$	2	$1+x$	1	$1+2x$
$1+2x$	0	$1+2x$	$2+x$	2	$2x$	$1+x$	1	$2+2x$	x
$2+2x$	0	$2+2x$	$1+x$	$2+x$	1	$2x$	$1+2x$	x	2

10.51 (a) $(a + bx) \mathbin{\triangleplus} (c + dx) = (a + c) + (b + d)x$

$(a + bx) \mathbin{\trianglecdot} (c + dx) = (ac - bd) + (ad + bc)x$

(b) $(R_2[x], \triangleplus, \trianglecdot)$ is isomorphic to the field of complex numbers.