Exercise 1

Chapter 12 | Page 250

Contemporary Abstract Algebra

ISBN: 9781133599708

Table of contents

Explanation Verified

Step 1

1 of 3

Example for finite noncommutative ring is

$$\mathrm{M}_2(\mathbb{Z}_p)=\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a,b,c,d \in \mathbb{Z}_p\}$$

, for any prime p.

Indeed, $\mathrm{M}_2(\mathbb{Z}_p)$ is commutative group under addition of 2×2 matrices, and we know how to multiply two matrices. Distributivity is also easily verified formally. Since matrix mupltiplication is not commutative, this ring is not commutative.

Step 2

2 of 3

Example for infinite noncommutative ring without unity is

$$\mathrm{M}_2(2\mathbb{Z})=\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a,b,c,d \in 2\mathbb{Z}\}$$

.

The same explanation as above provides for this example.

Result

3 of 3

We find two rings of 2×2 matrices.

Exercise 41 Exercise 2

Exercise 2

Chapter 12 | Page 250

Contemporary Abstract Algebra

ISBN: 9781133599708

Table of contents

Explanation

Verified

Step 1

1 of 3

The unit is element 6. Remember that it is the element which is multiplicative identity in ring.

Step 2

2 of 3

These computations explain the conclusion:

- $0 \cdot 6 = 6 \cdot 0 = 0$
- $2 \cdot 6 = 6 \cdot 2 = 12 = 2$
- $4 \cdot 6 = 6 \cdot 4 = 24 = 4$
- $6 \cdot 6 = 6 \cdot 6 = 36 = 6$

Result

3 of 3

Try out different possibilities, there are not many of them.

Exercise 1 Exercise 3

Exercise 3

Chapter 12 | Page 250

Contemporary Abstract Algebra

ISBN: 9781133599708

Table of contents

Explanation Verified

Step 1

1 of 2

For some prime p, we have that $H = \langle \frac{1}{p} \rangle$ is a subgroup of additive group $(\mathbb{Q}, +)$, but it is not closed for multiplication ($\frac{1}{p} \cdot \frac{1}{p} = \frac{1}{p^2} \notin H$), hence it is not a subring of ring $(\mathbb{Q}, +, \cdot)$.

Result

2 of 2

$\boxed{\text{See work.}}$

Exercise 2 Exercise 4

Exercise 4

Chapter 12 | Page 250

Contemporary Abstract Algebra

ISBN: 9781133599708

Table of contents

Explanation Verified

Step 1

1 of 3

In ring $\mathbb{Z}_8$ we note that for $a = 2$ and $b = 4$, the equation $ax = b$ has two solutions: $x = 2$ and $x = 6$.

Step 2

2 of 3

In groups, since there are always inverses, this equation has exactly one solution, which is $x = a^{-1}b$.

Result

3 of 3

$\boxed{\text{See work.}}$

Exercise 3 Exercise 5

Exercise 5

Chapter 12 | Page 250

Contemporary Abstract Algebra

ISBN: 9781133599708

Table of contents

Explanation Verified

Step 1

1 of 3

Theorem 12.2 states that unity in ring is unique, and that multiplicative inverses are unique (provided that they exist).

Assume there are two unuties, e and f. Then we obtain using definitons:

$$e = [f \text{ is unity }] = ef = [e \text{ is unity }] = f$$

Step 2

2 of 3

Now assume that b and c are multiplicative inverses of a. We obtain:

$$b = be = b(ac) = (ab)c = ec = c$$

Result

3 of 3

$$\boxed{\text{See work.}}$$

Exercise 4

Exercise 6

Exercise 6

Chapter 12 | Page 250

Contemporary Abstract Algebra

ISBN: 9781133599708

Table of contents

Explanation Verified

Step 1

1 of 5

The appropriate n for all parts of Exercise is $n = 10$. It is not prime.

Step 2

2 of 5

$\boxed{\text{Part a)}}$

For $a = 6$ we have $6^2 = 36 = 6 \pmod{10}$, and obviously $6 \neq 0$ and $6 \neq 1$.7

Step 3

3 of 5

$\boxed{\text{Part b)}}$

For $a = 2, b = 5$ we have $2 \cdot 5 = 10 = 0 \pmod{10}$, but obviously $2 \neq 0$ and $5 \neq 0$.

Step 4

4 of 5

$\boxed{\text{Part c)}}$

For $a = 2, b = 1, c = 6$ we have $2 \cdot 1 = 2 \cdot 6$, but obviously $b \neq c$ and $a \neq 0$.

Result

5 of 5

$\boxed{\text{See work.}}$

Exercise 5 Exercise 7

Exercise 7

Chapter 12 | Page 251

Contemporary Abstract Algebra

ISBN: 9781133599708

Table of contents

Explanation Verified

Step 1

1 of 3

$\mathbb{Z}_p$ is ring with unity 1 and with $\textbf{multiplicaive inverses}$, which is consequence of $U(p) = \mathbb{Z}_p \setminus \{0\}$, and $\textbf{Theorem 0.2}$.

Step 2

2 of 3

In rings with multiplicative inverses all statements from previous Exercise are valid. For example, if $a^2 = a$ and $a \neq 0$, we can multiply with a^{-1} to obtain $a = 1$.

Result

3 of 3

$\boxed{\text{See work.}}$

Exercise 6 Exercise 8

Exercise 8

Chapter 12 | Page 251

Contemporary Abstract Algebra

ISBN: 9781133599708

Table of contents

Explanation Verified

Step 1

1 of 2

If we plug in ba instead of b and ab instead of c we get the correct equality

$$a(ba) = (ab)a.$$

Now property of this ring implies that $ab = ba$, i.e. R is commutative.

Result

2 of 2

$\boxed{\text{See work.}}$

Exercise 7 Exercise 9

Exercise 9

Chapter 12 | Page 251

Contemporary Abstract Algebra

ISBN: 9781133599708

Table of contents

Explanation Verified

Step 1

1 of 3

Let $\{S_i \mid i \in I\}$ be a collection of subrings of ring R, indexed by some set I.

We use $\textbf{Subring Test}$ to prove that $S = \bigcap_{i \in I} S_i$ is subring of R as well. Note that $0 \in S$, since it must be contained in all subrings S_i.

Step 2

2 of 3

First, for any two $x, y \in S$ we have $x, y \in S_i$, for all $i \in I$, from definition of intersection of sets. Then, since S_i is a subring, we have $x - y \in S_i$ and $xy \in S_i$.

But from here we again from definition of intersection conclude that $x - y, xy \in S$. This completes the $\textbf{Subring Test}$ for set S.

Result

3 of 3

$\boxed{\text{See work.}}$

Exercise 8

Exercise 10

Exercise 10

Chapter 12 | Page 251

Contemporary Abstract Algebra

ISBN: 9781133599708

Table of contents

Explanation Verified

Step 1

1 of 7

Example 8 is obvious, since $0 - 0 = 0$ and $0 \cdot 0 = 0$, and R is ring by definition.

Step 2

2 of 7

Example 9 is easily verified: for example $4 - 2 = 2$ and $4 \cdot 2 = 8 = 2$.

Step 3

3 of 7

Example 10 is verified as follows: we already know that $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$, and product of two elements an, bn is abn^2, which is in $n\mathbb{Z}$ again.

Step 4

4 of 7

Example 11 is verified as follows: difference of two Gaussian integers is obviously Gaussian, and their product is

$$(a + bi)(c + di) = ac - bd + (ad + bc)i$$

is Gaussian as well.

Step 5

5 of 7

Example 12 is verified as follows: value of difference of two functions from S is $0 - 0 = 0$, as it should be, and value of product is $0 \cdot 0 = 0$, as it should be.

Step 6

6 of 7

Example 13 is obvious.

Result

7 of 7

$\boxed{\text{See work.}}$

Exercise 9 Exercise 11

Exercise 11

Chapter 12 | Page 251

Contemporary Abstract Algebra

ISBN: 9781133599708

Table of contents

Explanation Verified

Step 1

1 of 4

Rule 3 of $\textbf{Theorem 12.1}$ says that $(-a)(-b) = ab$. From rule 2 we can conlude the following:

$$(-a)(-b) = -((-a)b) = -(-(ab)) = ab$$

Step 2

2 of 4

Rule 4 is something like distributivity, and follows from it, and rule 2:

$$a(b-c) = a(b+(-c)) = ab + a(-c) = ab - ac$$

Analogously for $(b-c)a = ba - ca$.

Step 3

3 of 4

Rule 5 follows from rule 2:

$$(-1)a = -(1 \cdot a) = -a$$

Rule six is direct consequence of rule 5, for $a = -1$.

Result

4 of 4

$$\boxed{\text{See work.}}$$

Exercise 10
Exercise 12

Exercise 12

Chapter 12 | Page 251

Contemporary Abstract Algebra

ISBN: 9781133599708

Table of contents

Explanation Verified

Step 1

1 of 2

b divides c is equivalent to $c = xb$, for some $x \in R$. We can write this equation as

$$c = xb = x(a^{-1}a)b = xa^{-1}(ab)$$

which exactly is equivalent to ab divides c.

Result

2 of 2

$$\boxed{\text{See work.}}$$

Exercise 11 Exercise 13

Exercise 13

Chapter 12 | Page 251

Contemporary Abstract Algebra

ISBN: 9781133599708

Table of contents

Explanation

Verified

Step 1

1 of 3

We have proved a long time ago that every subgrop of cyclic group is again cyclic, i.e. $\langle n\rangle = n\mathbb{Z}$ are the only subgroups of $\mathbb{Z}$. Hence they are the only candidates for subrings.

Step 2

2 of 3

But in Example 10 we saw that $n\mathbb{Z}$ is really a subring of $\mathbb{Z}$.

Result

3 of 3

$\boxed{\text{See work.}}$

Exercise 12 Exercise 14

Exercise 14

Chapter 12 | Page 251

Contemporary Abstract Algebra

ISBN: 9781133599708

Table of contents

Explanation Verified

Step 1

1 of 3

We compute:

$$m \cdot (ab) = \underbrace{ab + ab + \cdots + ab}_{m \text{ times}} = a(\underbrace{b + b + \cdots + b}_{m \text{ times}}) = a(m \cdot b)$$

Step 2

2 of 3

Analogously $m \cdot (ab) = (m \cdot a)b$.

Result

3 of 3

$$\boxed{\text{See work.}}$$

Exercise 13 Exercise 15

Exercise 15

Chapter 12 | Page 251

Contemporary Abstract Algebra
ISBN: 9781133599708

Table of contents

Explanation Verified

Step 1

1 of 2

We use previous Exercise to compute:

$$(m \cdot a)(n \cdot b) = m \cdot (a(n \cdot b)) = m \cdot (n \cdot (ab)) = (mn) \cdot (ab)$$

Result

2 of 2

$$\boxed{\text{See work.}}$$

Exercise 14 Exercise 16

Exercise 16

Chapter 12 | Page 251

Contemporary Abstract Algebra

ISBN: 9781133599708

Table of contents

Explanation Verified

Step 1

1 of 2

We use property 5 of $\textbf{Theorem 12.1}$ and Exercise 14 to compute:

$$n \cdot (-a) = n \cdot ((-1)a) = (n \cdot (-1))a = (-1 \cdot n)a = (-1) \cdot (n \cdot a) = -(n \cdot a)$$

Result

2 of 2

$\boxed{\text{See work.}}$

Exercise 15 Exercise 17

Exercise 17

Chapter 12 | Page 251

Contemporary Abstract Algebra

ISBN: 9781133599708

Table of contents

Explanation Verified

Step 1

1 of 2

Let $R = \langle a \rangle$. Then for any two elements $m \cdot a, n \cdot b$ we compute using Exercise 15:

$$(m \cdot a)(n \cdot b) = (mn) \cdot (aa) = (nm) \cdot (aa) = (n \cdot a)(m \cdot a)$$

Result

2 of 2

$\boxed{\text{See work.}}$

Exercise 16 Exercise 18

Exercise 18

Chapter 12 | Page 251

Contemporary Abstract Algebra
ISBN: 9781133599708

Table of contents

Explanation Verified

Step 1

Firstly, $0 \in S$, from property 1 of $\mathbf{Theorem\ 12.1}$.

Now we use $\mathbf{Subring\ Test}$ to prove that S is subring of R. Properties from the definition of a ring and $\mathbf{Theorem\ 12.1}$ will be used in computations implicitly.

Take any two $x, y \in S$, i.e. $ax = ay = 0$. Then we first compute:

$$a(x-y) = ax - ay = 0 - 0 = 0$$

which proves that $x - y \in S$.

Next, we look at xy. We have:

$$a(xy) = (ax)y = 0y = 0$$

which proves $xy \in S$ and completes the proof.

Result

HINT: use $\mathbf{Subring\ Test}$ and $\mathbf{Theorem\ 12.1}$.

Exercise 17 Exercise 19

Exercise 19

Chapter 12 | Page 251

Contemporary Abstract Algebra

ISBN: 9781133599708

Table of contents

Explanation Verified

Step 1

1 of 3

We denote the given set with $Z(R) = \{x \in R \,|\, ax = xa,\ \forall a \in R\}$, as in groups. First we observe that $0 \in Z(R)$, since $0a = a0 = 0$.

Now we use $\textbf{Subring Test}$ to prove that S is subring of R.

Step 2

2 of 3

Take any two $x, y \in Z(R)$, i.e. $ax = xa$ and $ay = ya$. Then we first compute:

$$a(x-y) = ax - ay = xa - ya = (x-y)a$$

which proves that $x - y \in Z(R)$.

Next, we look at xy. We have:

$$a(xy) = (ax)y = (xa)y = x(ay) = (xy)a$$

which proves $xy \in Z(R)$ and completes the proof.

Result

3 of 3

$\boxed{\text{See work.}}$

Exercise 18 Exercise 20

Exercise 20

Chapter 12 | Page 251

Contemporary Abstract Algebra
ISBN: 9781133599708

Table of contents

Explanation Verified

Step 1

1 of 3

Since $M_2(\mathbb{Z})$ is a subring of ring $M_2(\mathbb{R})$, the multiplicative inverse of element

$$X = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

is

$$X^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

Step 2

2 of 3

This is element of $M_2(\mathbb{Z})$ if and only if $\det(X) = ad - bc$ divides a, b, c and d.

Result

3 of 3

$$\boxed{\text{See work.}}$$

Exercise 19 Exercise 21

Exercise 21

Chapter 12 | Page 251

Contemporary Abstract Algebra

ISBN: 9781133599708

Table of contents

Explanation Verified

Step 1

1 of 3

If each of $R_1, R_2, \ldots, R_n$ has a unity, say $1_j \in R_j$, then element $1 = (1_1, 1_2, \ldots, 1_n)$ is a unity in $R_1 \oplus R_2 \oplus \cdots \oplus R_n$, since the operation is performed componentwise.

Step 2

2 of 3

Conversely, if $1 = (1_1, 1_2, \ldots, 1_n)$ is a unity in $R_1 \oplus R_2 \oplus \cdots \oplus R_n$, we again conclude that 1_j is unity in ring R_j, because the operation is performed componentwise.

Result

3 of 3

$\boxed{\text{See work.}}$

Exercise 20 Exercise 22

Exercise 22

Chapter 12 | Page 251

Contemporary Abstract Algebra

ISBN: 9781133599708

Table of contents

Explanation Verified

Step 1 1 of 3

Multiplication in R is associative, hence it is associative in $U(R)$ as well.

Step 2 2 of 3

The unity of the ring is its own inverse, so it is in $U(R)$.

Every element in $U(R)$ has a multiplicative inverse, by definition of unit of a ring.

This shows that $U(R)$ satisfies three conditions neccesary for set to be a group.

Result 3 of 3

$\boxed{\text{See work.}}$

Exercise 21 Exercise 23

Exercise 23

Chapter 12 | Page 251

Contemporary Abstract Algebra

ISBN: 9781133599708

Table of contents

Explanation Verified

Step 1

Rememeber that $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ is the set of Gaussian integers, which forms a subring of $\mathbb{C}$.

We need to find all units of this ring.

Step 2

Let $x = a + bi \in U(\mathbb{Z}[i])$, which means there is $y = c + di \in \mathbb{Z}[i]$ such that $xy = yx = 1$.

From this equality we obtain $|xy| = |x| \cdot |y| = 1$ and then conclude that $|x| = 1$, since both $|x|$ and $|y|$ are natural numbers.

Step 3

But now we have $1 = |x|^2 = a^2 + b^2$, which means there are only four possibilities:

- $a = 0, b = -1 \implies x = -i$
- $a = 0, b = 1 \implies x = i$
- $a = -1, b = 0 \implies x = -1$
- $a = 1, b = 0 \implies x = 1$

For all of these numbers it is trivially verified that $x \in U(\mathbb{Z}[i])$.

Hence we have $U(\mathbb{Z}[i]) = \{-i, i, -1, 1\}$.

Result

$\boxed{\text{See work.}}$

Exercise 22 Exercise 24

Exercise 24

Chapter 12 | Page 251

Contemporary Abstract Algebra
ISBN: 9781133599708

Table of contents

Explanation Verified

Step 1

1 of 3

First take any element $x = (x_1, x_2, \ldots, x_n) \in U(R_1 \oplus R_2 \oplus \cdots \oplus R_n)$. This means there is element $y = (y_1, y_2, \ldots, y_n) \in R_1 \oplus R_2 \oplus \cdots \oplus R_n$ such that $xy = yx = 1$.

But this exactly means $x_j y_j = 1_j$, for all $j = 1, 2, \ldots, n$, where 1_j is unity in ring R_j (see solution to Exercise 22). Now we conclude that $x_j \in U(R_j)$, which implies that $U(R_1 \oplus R_2 \oplus \cdots \oplus R_n) \subseteq U(R_1) \oplus U(R_2) \oplus \cdots \oplus U(R_n)$.

Step 2

2 of 3

Opposite inclusion is rather obvious and unworthy of words.

Result

3 of 3

$\boxed{\text{See work.}}$

‹ Exercise 23 Exercise 25 ›

Exercise 25

Chapter 12 | Page 251

Contemporary Abstract Algebra

ISBN: 9781133599708

Table of contents

Explanation Verified

Step 1

1 of 3

Remember that $\mathbb{Z}[x]$ is a ring of all polynomials with integer coefficients. Let $p(x) = a_n x^n + \cdots + a_1 x + a_0 \in U(\mathbb{Z}[x])$, which means there is $q(x) \in \mathbb{Z}[x]$ such that $(pq)(x) = (qp)(x) = 1$, for all $x \in \mathbb{Z}$.

Step 2

2 of 3

By plugging in $x = 0$ we have $a_0 \cdot q(0) = 1$, which implies that $a_0 = \pm 1$, since $a_0, q(0) \in \mathbb{Z}$.

Now we can conclude that $p(x) = \pm 1$ are the only polynomials in $U(\mathbb{Z}[x])$, since if there is some $a_j \neq 0$ for $j > 0$, the part x^j could not become 0.

Result

3 of 3

$\boxed{\text{See work.}}$

‹ Exercise 24 Exercise 26 ›

Exercise 26

Chapter 12 | Page 251

Contemporary Abstract Algebra

ISBN: 9781133599708

Table of contents

Explanation Verified

Step 1

1 of 2

By analogous reasoning as in previous Exercise, we obtain the solution $U(\mathbb{R}[x]) = \mathbb{R}^*$.

Result

2 of 2

$\boxed{\text{See work.}}$

Exercise 25

Exercise 27

Exercise 27

Chapter 12 | Page 251

Contemporary Abstract Algebra

ISBN: 9781133599708

Table of contents

Explanation Verified

Step 1

1 of 3

Let a be unit, a^{-1} its inverse, and c any element from ring R.

By definition, c is said do be divisivle by a if there is element $b \in R$ such that $c = ab$.

Step 2

2 of 3

We compute:

$$c = ec = (aa^{-1})c = a(a^{-1}c)$$

which implies that $a \mid c$ with $b = a^{-1}c$.

Result

3 of 3

$\boxed{\text{See work.}}$

Exercise 26 Exercise 28

Exercise 28

Chapter 12 | Page 251

Contemporary Abstract Algebra
ISBN: 9781133599708
Table of contents

Explanation Verified

Step 1

1 of 2

In $\mathbb{Z}_6$ we have $4 \mid 2$, since $2 = 4 \cdot 2 \pmod 6$.

In $\mathbb{Z}_8$ we have $3 \mid 7$, since $7 = 3 \cdot 5 \pmod 8$.

In $\mathbb{Z}_{15}$ we have $9 \mid 12$, since $12 = 9 \cdot 3 \pmod{15}$.

Result

2 of 2

$$\boxed{\text{See work.}}$$

Exercise 27 Exercise 29

Exercise 29

Chapter 12 | Page 252

Contemporary Abstract Algebra

ISBN: 9781133599708

Table of contents

Explanation Verified

Step 1

Let $ax = 1$ (since a is unit). Ring R is commutative, which implies that $a^2x^2 = (ax)^2 = 1^2 = 1$.

Now we will prove that $a + b$ is unit of R.

Step 2

Compute the product $(a+b)(a-b)$ using the fact that R is commutative and $b^2 = 0$:

$$(a+b)(a-b) = a^2 - ab + ba - b^2 = a^2 - \cancel{ab} + \cancel{ab} - b^2 = a^2 - b^2 = a^2 - 0 = a^2$$

This implies that

$$(a+b)((a-b)x^2) = 1$$

which proves that $a + b \in U(R)$.

Result

$$\boxed{\text{See work.}}$$

Exercise 28 Exercise 30

Exercise 30

Chapter 12 | Page 252

Contemporary Abstract Algebra

ISBN: 9781133599708

Table of contents

Explanation Verified

Step 1

1 of 3

If $m \leq n$, we have immediately $a = a^n = a^m a^{m-n} = 0a^{m-n} = 0$.

Step 2

2 of 3

Otherwise, we can write $n = qm + r$, with $q > 0$. Then we have:

$$a = a^n = a^{qm+r} = a^{qm}a^r = (a^m)^q a^r = 0^q a^r = 0a^r = 0$$

Result

3 of 3

$\boxed{\text{See work.}}$

Exercise 29
Exercise 31

Exercise 31

Chapter 12 | Page 252

Contemporary Abstract Algebra

ISBN: 9781133599708

Table of contents

Explanation

Verified

Step 1

1 of 3

We can take matrices

$$a = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$$

and

$$b = \begin{bmatrix} -1 & -1 \\ 1 & 1 \end{bmatrix}$$

from ring $M_2(\mathbb{R})$.

Step 2

2 of 3

Then we have $ab = 0$, but

$$ba = \begin{bmatrix} -1 & -1 \\ 1 & 1 \end{bmatrix}$$

Result

3 of 3

$$\boxed{\text{See work.}}$$

Exercise 30
Exercise 32

Exercise 32

Chapter 12 | Page 252

Contemporary Abstract Algebra

ISBN: 9781133599708

Table of contents

Explanation Verified

Step 1

1 of 3

We compute:

$$ba = (ba)^n = b(ab)^{n-1}a$$

Step 2

2 of 3

This implies that if $ab = 0$, we have $ab = b0a = 0$ as well.

Result

3 of 3

$$\boxed{\text{See work.}}$$

Exercise 31 Exercise 33

Exercise 33

Chapter 12 | Page 252

Contemporary Abstract Algebra

ISBN: 9781133599708

Table of contents

Explanation Verified

Step 1

1 of 3

We plug in $2x$ instead of x in equality $x^3 = x$ to obtain

$$(2x)^3 = 8x^3 = 2x$$

Step 2

2 of 3

But now if we substitute back $x^3 = x$, we get

$$8x^3 = 8x = 2x$$

from where $\colorbox{#965501}{6x = 0}$ follows.

Result

3 of 3

Plug in $2x$ instead of x in equality $x^3 = x$.

Exercise 32
Exercise 34

Exercise 34

Chapter 12 | Page 252

Contemporary Abstract Algebra

ISBN: 9781133599708

Table of contents

Explanation Verified

Step 1

1 of 3

We use **First Principle of Mathematical Induction**.

Basis is the assumption $a^4 = a^2$.

Step 2

2 of 3

From assumption $a^{2n} = a^2$, we obtain:

$$a^{2(n+1)} = \underbrace{a^2n}_{=a^2}a^2 = a^2a^2 = a^4 = a^2$$

which completes the step of induction.

Result

3 of 3

Use **First Principle of Mathematical Induction**.

Exercise 33 Exercise 35

Exercise 35

Chapter 12 | Page 252

Contemporary Abstract Algebra

ISBN: 9781133599708

Table of contents

Explanation Verified

Step 1

1 of 4

In $\mathbb{Z}_6$ we can take $n = 3$, since:

- $1^3 = 1 = 1 \text{ (mod } 6)$
- $2^3 = 8 = 2 \text{ (mod } 6)$
- $3^3 = 27 = 3 \text{ (mod } 6)$
- $4^3 = 64 = 4 \text{ (mod } 6)$
- $5^3 = 125 = 5 \text{ (mod } 6)$

Step 2

2 of 4

In $\mathbb{Z}_{10}$ we can take $n = 5$, since:

- $1^5 = 1 = 1 \text{ (mod } 10)$
- $2^5 = 32 = 2 \text{ (mod } 10)$
- $3^5 = 243 = 3 \text{ (mod } 10)$
- $4^5 = 1024 = 4 \text{ (mod } 10)$
- $5^5 = 3125 = 5 \text{ (mod } 10)$
- $6^5 = 7776 = 6 \text{ (mod } 10)$
- $7^5 = 16807 = 7 \text{ (mod } 10)$
- $8^5 = 32768 = 8 \text{ (mod } 10)$
- $9^5 = 59049 = 9 \text{ (mod } 10)$

Step 3

3 of 4

If $m = p^2t$, then for element $pt \in \mathbb{Z}_m$ we have $(pt)^n = 0$, which means there can not be n such that $(pt)^n = pt$.

Result

4 of 4

$\boxed{\text{See work.}}$

Exercise 34 Exercise 36

Exercise 36

Chapter 12 | Page 252

Contemporary Abstract Algebra

ISBN: 9781133599708

Table of contents

Explanation Verified

Step 1

1 of 3

Inclusion $k\mathbb{Z} \subseteq m\mathbb{Z} \cap n\mathbb{Z}$ is trivial, since every multiple of k is obviously multiple of both m and n.

Step 2

2 of 3

On the other hand, let $x = am = bn$, i.e. $x \in m\mathbb{Z} \cap n\mathbb{Z}$ is a common multiple of both m and n. We need to prove that x is multiple of k as well.

Say $x = qk + r$, where $r < k$. Since x, k are both multiples of m, n, then so is $r = x - qk$. But this is contradiction, since k is the $\textbf{least}$ natural number with this property.

Result

3 of 3

$\boxed{\textbf{See work.}}$

Exercise 35 Exercise 37

Exercise 37

Chapter 12 | Page 252

Contemporary Abstract Algebra
ISBN: 9781133599708

Table of contents

Explanation Verified

Step 1

1 of 3

Group $\mathbb{Z}_n$ is cyclic, so its subgroup is cyclic as well.

Step 2

2 of 3

We know that any cyclic group is closed under multiplication, which implies that any subgroup of $\mathbb{Z}_n$ is also a subring.

Result

3 of 3

$$\boxed{\text{See work.}}$$

Exercise 36 Exercise 38

Exercise 38

Chapter 12 | Page 252

Contemporary Abstract Algebra

ISBN: 9781133599708

Table of contents

Explanation Verified

Step 1

1 of 2

Just take a look at previous Exercise.

Result

2 of 2

Look at previous Exercise.

Exercise 37 Exercise 39

Exercise 39

Chapter 12 | Page 252

Contemporary Abstract Algebra

ISBN: 9781133599708

Table of contents

Explanation Verified

Step 1

1 of 3

We first have to prove that S is an additive subgroup of R. Take $r_1, r_2 \in R$ and compute:

$$ar_1a - ar_2a = a(r_1 - r_2)a \in S$$

which shows that S passes **One-Step Subgroup Test**.

Step 2

2 of 3

Furthermore, we need to prove that S is closed under multiplication. Again take $r_1, r_2 \in R$ and compute:

$$(ar_1a)(ar_2a) = ar_1\underbrace{a^2}_{=1}r_2a = ar_11r_2a = ar_1r_2a \in S$$

which proves that S is closed under multiplication, and that it is a subring of R.

Since $a1a = a^2 = 1$, we have $1 \in S$.

Result

3 of 3

$\boxed{\text{See work.}}$

Exercise 38
Exercise 40

Exercise 40

Chapter 12 | Page 252

Contemporary Abstract Algebra

ISBN: 9781133599708

Explanation Verified

Step 1

1 of 2

This computation proves that R is not closed under multiplication, which means it is not a subring of $M_2(\mathbb{Z})$:

$$\begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 1 & 3 \\ 3 & 2 \end{bmatrix} = \begin{bmatrix} 7 & 7 \\ 5 & 8 \end{bmatrix} \notin R$$

Result

2 of 2

$\boxed{\text{See work.}}$

Exercise 39

Exercise 41

Exercise 41

Chapter 12 | Page 252

Contemporary Abstract Algebra
ISBN: 9781133599708
Table of contents

Explanation Verified

Step 1

1 of 2

R is obviously subgroup of $M_2(\mathbb{Z})$. Following computation shows that it is closed under multiplication as well, which implies that it is a subgring:

$$\begin{bmatrix} a_1 & a_1-b_1 \\ a_1-b_1 & b_1 \end{bmatrix}\begin{bmatrix} a_2 & a_2-b_2 \\ a_2-b_2 & b_2 \end{bmatrix}=\begin{bmatrix} 2a_1a_2-a_1b_2-a_2b_1+b_1b_2 & a_1a_2-b_1b_2 \\ a_1a_2-b_1b_2 & 2b_1b_2+a_1a_2-a_1b_2-a_2b_1 \end{bmatrix}\in R,$$

because

$$(2a_1a_2-a_1b_2-a_2b_1+b_1b_2)-(2b_1b_2+a_1a_2-a_1b_2-a_2b_1)=a_1a_2-b_1b_2.$$

Result

2 of 2

$\boxed{\text{See work.}}$

< Exercise 40 Exercise 42 >

Exercise 42

Chapter 12 | Page 252

Contemporary Abstract Algebra

ISBN: 9781133599708

Table of contents

Explanation

Verified

Step 1

1 of 2

R is obviously subgroup of $M_2(\mathbb{Z})$. This computation shows that it is closed under multiplication as well, which implies that it is subgring:

$$\begin{bmatrix} a_1 & a_1 \\ b_1 & b_1 \end{bmatrix} \begin{bmatrix} a_2 & a_2 \\ b_2 & b_2 \end{bmatrix} = \begin{bmatrix} a_1a_2 + a_1b_2 & a_1a_2 + a_1b_2 \\ b_1a_2 + b_1b_2 & b_1a_2 + b_1b_2 \end{bmatrix} \in R$$

Result

2 of 2

$\boxed{\text{See work.}}$

Exercise 41
Exercise 43

Exercise 43

Chapter 12 | Page 252

Contemporary Abstract Algebra
ISBN: 9781133599708

Table of contents

Explanation Verified

Step 1

1 of 3

We have that $(1,2,3) \in S$, but $(1,2,3)^2 = (1,4,9) \notin S$, since $1+4 \neq 9$.

Step 2

2 of 3

This proves that S is not closed under multiplication, i.e. it is not a subring of R.

Result

3 of 3

$\boxed{\text{See work.}}$

Exercise 42 Exercise 44

Exercise 44

Chapter 12 | Page 252

Contemporary Abstract Algebra

ISBN: 9781133599708

Table of contents

Explanation Verified

Step 1

1 of 2

We plug in $-a$ in equlity $a^n = a$ and use the fact that n is even to obtain:

$$-a = (-a)^n = a^n = a$$

Result

2 of 2

$$\boxed{\text{See work.}}$$

Exercise 43 Exercise 45

Exercise 45

Chapter 12 | Page 253

Contemporary Abstract Algebra

ISBN: 9781133599708

Table of contents

Explanation

Verified

Step 1

1 of 3

We first have to prove that S is a subgroup of R. Take any two $m, n \in \mathbb{Z}$ and compute:

$$n \cdot 1 - m \cdot 1 = (n - m) \cdot 1 \in S$$

Step 2

2 of 3

Furthermore, from Exercise 15 we have that

$$(m \cdot 1)(n \cdot 1) = (mn) \cdot (11) = (mn) \cdot 1$$

whixh implies that S is closed under multiplication.

Result

3 of 3

$$\boxed{\text{See work.}}$$

Exercise 44

Exercise 46

Exercise 46

Chapter 12 | Page 253

Contemporary Abstract Algebra

ISBN: 9781133599708

Table of contents

Explanation Verified

Step 1

1 of 2

Set $2\mathbb{Z} \cup 3\mathbb{Z}$ is not even a subgroup of $\mathbb{Z}$, since $3 - 2 = 1 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$.

Result

2 of 2

$\boxed{\text{See work.}}$

Exercise 45
Exercise 47

Exercise 47

Chapter 12 | Page 253

Contemporary Abstract Algebra

ISBN: 9781133599708

Table of contents

Explanation Verified

Step 1

1 of 3

The smallest **subgroup** of $\mathbb{Q}$ which contains $\frac{1}{2}$ is cyclic group $\langle\frac{1}{2}\rangle = \{\frac{m}{2} \mid m \in \mathbb{Z}\}$.

Step 2

2 of 3

But any subring containg $\frac{1}{2}$ must also contain elements $\frac{1}{2^n}$, for $n \in \mathbb{N}$.

Thus the smallest subring of $\mathbb{Q}$ containing $\frac{1}{2}$ is set $\{\frac{m}{2^n} \mid m \in \mathbb{Z}, n \in \mathbb{N}\}$.

Result

3 of 3

$\boxed{\text{See work.}}$

‹ Exercise 46 Exercise 48 ›

Exercise 48

Chapter 12 | Page 253

Contemporary Abstract Algebra

ISBN: 9781133599708

Table of contents

Explanation Verified

Step 1

1 of 2

Analogously as in previous Exercise, we conlude that it is set $\{m \cdot \frac{2^n}{3^n} \,|\, m \in \mathbb{Z}, n \in \mathbb{N}\}$.

Result

2 of 2

See work.

Exercise 47 Exercise 49

Exercise 49

Chapter 12 | Page 253

Contemporary Abstract Algebra

ISBN: 9781133599708

Table of contents

Explanation Verified

Step 1

1 of 3

If R is commutative, we can compute:

$$(a-b)(a+b)=a^2+ab-ba-b^2=a^2+ab-ba-b^2=a^2-b^2$$

Step 2

2 of 3

Conversely, using the same computation we obtain:

$$a^2-b^2=(a-b)(a+b)=a^2+ab-ba-b^2.$$

Now cancelling out a^2-b^2 yields $ab=ba$.

Result

3 of 3

$$\boxed{\text{See work.}}$$

Exercise 48 Exercise 50

Exercise 50

Chapter 12 | Page 253

Contemporary Abstract Algebra

ISBN: 9781133599708

Table of contents

Explanation Verified

Step 1

1 of 3

First by plugging in $2a$ instead of a in equality $a^2 = a$ yields:

$$2a = (2a)^2 = 4a^2 = 4a$$

which implies $2a = 0$, for all $a \in R$.

Step 2

2 of 3

Now we will show that $ab = ba$, for all $a, b \in R$, using this computation:

$$a^2 - b^2 = (a - b) = (a - b)^2 = a^2 - ab - ba + b^2$$

from where we obtain

$$ab + ba = 2b = 0.$$

Now we have $ab = -ba$, but then we use result from Exercise 44 to obtain $ab = ba$.

Result

3 of 3

$\boxed{\text{See work.}}$

Exercise 49 Exercise 51

Exercise 51

Chapter 12 | Page 253

Contemporary Abstract Algebra
ISBN: 9781133599708

Table of contents

Explanation Verified

Step 1

1 of 3

Example of Boolean ring with four elements is ring $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Step 2

2 of 3

Example of infinite Boolean ring is ring $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \ldots$.

Result

3 of 3

$\boxed{\text{See work.}}$

Exercise 50 Exercise 52

Exercise 52

Chapter 12 | Page 253

Contemporary Abstract Algebra

ISBN: 9781133599708

Table of contents

Explanation

Verified

Step 1

1 of 4

No to both. Consider first equation $2x+1=4$ in $\mathbb{Z}_6$. It obviously has no solutions.

Step 2

2 of 4

Now consider equation $3x+3=3$ in $\mathbb{Z}_6$. It has 3 solutions, $x=0,2,4$.

Step 3

3 of 4

If a is unit, then there is always a unique solution, namely $x=a^{-1}(c-b)$.

Result

4 of 4

$\boxed{\text{See work.}}$

Exercise 51
Exercise 1