Abstract Algebra by Pinter, Chapter 17

Amir Taaki

Chapter 17 on Rings

Contents

A. Examples of Rings

Prove that the following are commutative rings with unity.

Indicate the zero element, the unity and the negative for an a.

Ring axioms:

1. $a \oplus b = b \oplus a$
2. $(a \otimes b) \otimes c = a \otimes (b \otimes c)$
3. $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$

Commutative:

1. $a \otimes b = b \otimes a$

With unity:

1. $\exists 1' \in A : a \otimes 1' = a$

Q1

$$a \oplus b = a + b - 1 \qquad a \otimes b = ab - (a + b) + 2$$

Axiom 1 is self evident.

Using sage, we prove axioms 2 and 3.

```
sage: a = var('a')
sage: b = var('b')
sage: c = var('c')
sage: ab = a*b - (a + b) + 2
sage: ab_c = ab*c - (ab + c) + 2
sage: bc = b*c - (b + c) + 2
sage: a_bc = a*bc - (a + bc) + 2
sage: ab_c.full_simplify()
-(a - 1)*b + ((a - 1)*b - a + 1)*c + a
sage: a_bc.full_simplify()
-(a - 1)*b + ((a - 1)*b - a + 1)*c + a
```

```
sage: def mul(a, b):
....:     return a*b - (a + b) + 2
....:
sage: def add(a, b):
....:     return a + b - 1
....:
sage: mul(a, add(b, c)).full_simplify()
(a - 1)*b + (a - 1)*c - 2*a + 3
sage: add(mul(a, b), mul(a, c)).full_simplify()
(a - 1)*b + (a - 1)*c - 2*a + 3
```

To calculate zero and unity:

$$a \oplus 0' = a$$
$$a + b - 1 = a$$
$$b = 1 = 0'$$

$$a \otimes 1' = a$$
$$ab - (a + b) + 2 = a$$
$$b = 2 = 1'$$

Lastly for the negative:

$$a \oplus b = 0'$$
$$a + b - 1 = 1$$
$$b = -a$$

Q2

$$a \oplus b = a + b + 1 \qquad a \otimes b = ab + a + b$$

```
sage: def add(a, b):
....:     return a + b + 1
....:
sage: def mul(a, b):
....:     return a*b + a + b
```

Axiom 1: $a \oplus b = b \oplus a$

Self-evident

Axiom 2: $(a \otimes b) \otimes c = a \otimes (b \otimes c)$

```
sage: bool(mul(mul(a, b), c) == mul(a, mul(b, c)))
True
```

Axiom 3: $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$

```
sage: bool(mul(a, add(b, c)) == add(mul(a, b), mul(a, c)))
True
```

Commutative: $a \otimes b = b \otimes a$

Self-evident

Zero:

```
sage: solve(add(a, b) - a, b)
[b == -1]
sage: add(a, -1)
a
```

Unity:

```
sage: solve(mul(a, b) - a, b)
[b == 0]
sage: mul(a, 0)
a
```

Negative a:

```
sage: solve(add(a, b) + 1, b)
[b == -a - 2]
sage: add(a, -a -2)
-1
```

Q3

$$(a, b) \oplus (c, d) = (a + c, b + d)$$

$$(a, b) \otimes (c, d) = (ac - bd, ad + bc)$$

```
sage: c = var('c')
sage: d = var('d')
sage: e = var('e')
sage: f = var('f')
sage: def add(ab, cd):
....:     a, b = ab
....:     c, d = cd
....:     return (a + c, b + d)
....:
sage: def mul(ab, cd):
....:     a, b = ab
....:     c, d = cd
....:     return (a*c - b*d, a*d + b*c)
....:
```

Axiom 1: $a \oplus b = b \oplus a$

```
sage: bool(add((a, b), (c, d)) == add((c, d), (a, b)))
True
```

Axiom 2: $(a \otimes b) \otimes c = a \otimes (b \otimes c)$

```
sage: bool(mul(mul((a, b), (c, d)), (e, f)) == mul((a, b), mul((c, d), (e, f))))
True
```

Axiom 3: $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$

```
sage: bool(mul((a, b), add((c, d), (e, f))) == add(mul((a, b), (c, d)), mul((a, b), (e, f))))
True
```

Commutative: $a \otimes b = b \otimes a$

Self-evident

Zero:

```
sage: ab_plus_cd = add((a, b), (c, d))
sage: solve(ab_plus_cd[0] - a, c)
[c == 0]
sage: solve(ab_plus_cd[1] - b, d)
[d == 0]
sage: add((a, b), (0, 0))
(a, b)
```

Unity:

```
sage: ab_mul_cd = mul((a, b), (c, d))
sage: solve([ab_mul_cd[0] - a, ab_mul_cd[1] - b], c, d)
[[c == 1, d == 0]]
sage: mul((a, b), (1, 0))
(a, b)
```

Negative a:

Since $0' = (0, 0)$ then the negative for (a, b) is simply $(-a, -b)$.

Q4

$$A = \{x + y\sqrt{2} : x, y \in \mathbb{Z}\}$$

Since normal algebraic operations are defined on A, then 1, 2 and 3 pass. It is also commutative.

Zero: 0

Unity: 1

Negative: $-x - y\sqrt{2}$

Q5

Prove the ring in part 1 is an integral domain.

We show that it has the cancellation property.

Assume $a \otimes b = a \otimes c$.

$$ab - (a + b) + 2 = ac - (a + c) + 2$$
$$ab - b = ac - c$$

Therefore $b = c$, and the ring has the cancellation property.

Q6

Prove the ring in part 2 is a field.

A field is a commutative ring with unity in which every nonzero element is invertible.

$$0' = -1$$
$$1' = 0$$

Thus

$$a \otimes b = 1'$$
$$ab + a + b = 0$$

We solve for b as follows

```
sage: def mul(a, b):
....:         return a*b + a + b
....:
sage: solve(mul(a, b), b)
[b == -a/(a + 1)]
```

(Excluding the $0'$ element which is equal to -1)

Q7

Find the inverse for the ring in part 3.

```
sage: def mul(ab, cd):
....:     a, b = ab
....:     c, d = cd
....:     return (a*c - b*d, a*d + b*c)
....:
sage: ab_mul_cd = mul((a, b), (c, d))
sage: solve([ab_mul_cd[0] - 1, ab_mul_cd[1]], c, d)
[[c == a/(a^2 + b^2), d == -b/(a^2 + b^2)]]
```

B. Ring of Real Functions

Q1

Let $a, b \in \mathcal{F}(\mathbb{R})$

Ring axioms:

1. $ab = ba$
2. $(ab)c = a(bc)$
3. $a(b + c) = ab + ac$

Commutative:

1. ab = ba

Zero: $f(x) = 0$

Unity: $f(x) = 1$

Negative: $-f(x)$

Q2

Divisors of zero, are any two functions which when $f(x) \neq 0$ then $g(x) = 0$ but in general $f(x) \neq 0$ and $g(x) \neq 0$.

See more here

Q3

Any functions which are one to one and have an inverse. That is $f(x) = x^3$ but not $f(x) = x^2$.

Q4

A field must have every element invertible. So the ring is not a field.

Ring has divisors of zero, so it does not have the cancellation property $\implies$ ring is not an integral domain.

C. Ring of 2×2 Matrices

Q1

```
sage: a = var('a')
sage: b = var('b')
sage: c = var('c')
```

```
sage: d = var('d')
sage: r = var('r')
sage: s = var('s')
sage: t = var('t')
sage: u = var('u')
sage: w = var('w')
sage: x = var('x')
sage: y = var('y')
sage: z = var('z')
sage:
sage: def add(abcd, rstu):
....:     a, b, c, d = abcd
....:     r, s, t, u = rstu
....:     return (a + r, b + s, c + t, d + u)
....:
sage: def mul(abcd, rstu):
....:     a, b, c, d = abcd
....:     r, s, t, u = rstu
....:     return (a*r + b*t, a*s + b*u, c*r + d*t, c*s + d*u)
```

Axiom 1:

Self evident.

Axiom 2:

```
sage: bool(mul((a,b,c,d), mul((r,s,t,u), (w,x,y,z))) == mul(mul((a,b,c,d), (r,s,t,u)), (w,x,y,z
....: )))
True
```

Axiom 3:

```
sage: bool(mul((a,b,c,d), add((r,s,t,u), (w,x,y,z))) == add(mul((a,b,c,d), (r,s,t,u)), mul((a,b
....: ,c,d), (w,x,y,z))))
True
```

Q2

```
sage: bool(mul((a,b,c,d), (r,s,t,u)) == mul((r,s,t,u), (a,b,c,d)))
False
```

Unity: $(a, b, c, d)(r, s, t, u) = (a, b, c, d)$

```
sage: solve([x_mul_y[0] - a, x_mul_y[1] - b, x_mul_y[2] - c, x_mul_y[3] - d], r,s,t,u)
[[r == 1, s == 0, t == 0, u == 1]]
```

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Q3

Matrices don't have the cancellation property.

For example $ar_1 + bt_1 = ar_2 + bt_2$ does not imply that $r_1 = r_2$ and $t_1 = t_2$.

Thus is not an integral domain.

Not all matrices are invertible, for example when $det(A) = 0$. See more info here. Hence they $\mathcal{M}_2(\mathbb{R})$ is not a field either.

D. Rings of Subsets of a Set

$$A + B = (A - B) \cup (B - A)$$
$$AB = A \cap B$$

Q1

Ring axioms:

1.

$$\begin{aligned} A + B &= (A - B) \cup (B - A) \\ &= B + A \end{aligned}$$

2.

$$(AB)C = (A \cap B) \cap C = A \cap (B \cap C) = A(BC)$$

3.

$$\begin{aligned} A(B + C) &= A \cap [(B - C) \cup (C - B)] \\ &= [A \cap (B - C)] \cup [A \cap (C - B)] \\ &= (AB - AC) \cup (AC - AB) \\ AB + AC &= (AB - AC) \cup (AC - AB) \end{aligned}$$

Commutativity:

$$AB = A \cap B = BA$$

Unity:

$$AB = A \implies B = D$$

Zero:

$$A + B = A \implies B = \emptyset$$

Q2

All elements of P_D with non-overlapping regions are divisors of zero.

$$X \in P_D, X^2 = \emptyset$$

Q3

$$\begin{gathered} 1' = D \\ AB = D \implies A \cap B = D \end{gathered}$$

Thus $A = D$ and $B = D$

Q4

There exist non-zero non-invertible elements in P_D, hence it is *not* a field.

$AB = AC$ does not imply $B = C$, hence cancellation property does not hold, and P_D is not an integral domain.

Q5

$$\begin{aligned} e &= \emptyset \\ a &= \{a\} \\ b &= \{b\} \\ c &= \{c\} \\ ab &= \{a, b\} \\ ac &= \{a, c\} \\ bc &= \{b, c\} \\ abc &= \{a, b, c\} \end{aligned}$$

⊕	e	a	b	c	ab	ac	bc	abc
e	e	a	b	c	ab	ac	bc	abc
a	a	e	ab	ac	b	c	abc	bc
b	b	ab	e	bc	a	abc	c	ac
c	c	ac	bc	e	abc	a	b	ab
ab	ab	b	a	abc	e	bc	ac	c
ac	ac	c	abc	a	bc	e	ab	b
bc	bc	abc	c	b	ac	ab	e	a
abc	abc	bc	ac	ab	c	b	a	e

⊗	e	a	b	c	ab	ac	bc	abc
e	e	a	b	c	ab	ac	bc	abc
a	a	a	ab	ac	ab	ac	abc	abc
b	b	ab	b	bc	ab	abc	bc	abc
c	c	ac	bc	e	abc	a	b	abc
ab	ab	ab	ab	abc	ab	abc	abc	abc
ac	ac	ac	abc	ac	abc	ac	abc	abc
bc	bc	abc	bc	bc	abc	abc	bc	abc
abc	abc	abc	abc	abc	abc	abc	abc	abc

E. Ring of Quaternions

Q1

Unity:

```
sage: a = var('a')
sage: b = var('b')
sage: c = var('c')
sage: d = var('d')
sage: matrix([[a + b*I, c + d*I], [-c + d*I, a - b*I]])
[ a + I*b  c + I*d]
[-c + I*d  a - I*b]
sage: alpha = matrix([[a + b*I, c + d*I], [-c + d*I, a - b*I]])
sage: matrix([[1, 0], [0, 1]]) * alpha
[ a + I*b  c + I*d]
[-c + I*d  a - I*b]
```

Distributive law:

```
sage: bb = var('e f g h')
sage: cc = var('i j k l')
sage: def make_matrix(xx):
....:     return matrix([[xx[0] + I*xx[1], xx[2] + xx[3]*I], [-xx[2] + xx[3]*I, xx[0] - xx[1]*I]])
....:
sage: bool(alpha*(make_matrix(bb) + make_matrix(cc)) == (alpha*make_matrix(bb) + alpha*make_matrix(cc))
True
```

Non-commutative:

```
sage: bool(alpha*make_matrix(bb) == make_matrix(bb)*alpha)
False
```

Q2

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

$$\mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

$$\mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

$$\begin{aligned} \alpha &= a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \\ &= \begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix} \end{aligned}$$

Q3

For the formula $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -\mathbf{1}$

```
sage: ii = matrix([[I, 0], [0, -I]])
sage: ii*ii
[-1  0]
[ 0 -1]
sage: -ii*ii
[1 0]
[0 1]
sage: jj = matrix([[0, 1], [-1, 0]])
sage: jj*jj
[-1  0]
[ 0 -1]
sage: kk = matrix([[0, I], [I, 0]])
sage: kk*kk
[-1  0]
[ 0 -1]
sage: bool(ii**2 == jj**2)
True
sage: bool(ii**2 == kk**2)
True
```

$\mathbf{ij} = -\mathbf{ji} = \mathbf{k}$

```
sage: bool(ii*jj == -jj*ii)
True
sage: bool(ii*jj == kk)
True
```

$\mathbf{jk} = -\mathbf{kj} = \mathbf{i}$

```
sage: bool(jj*kk == -kk*jj)
True
sage: bool(jj*kk == ii)
True
```

$\mathbf{ki} = -\mathbf{ik} = \mathbf{j}$

```
sage: bool(kk*ii == -ii*kk)
True
sage: bool(kk*ii == jj)
True
```

Q4

$$\bar{\alpha} = \begin{pmatrix} a-bi & -c-di \\ c-di & a+bi \end{pmatrix}$$

$$||\alpha|| = a^2 + b^2 + c^2 + d^2 = t$$

Show that

$$\bar{\alpha}\alpha = \alpha\bar{\alpha} = \begin{pmatrix} t & 0 \\ 0 & t \end{pmatrix}$$

```
sage: alpha
[ a + I*b  c + I*d]
[-c + I*d  a - I*b]
sage: alpha_bar = matrix([[a - b*I, -c - d*I], [c - d*I, a + b*I]])
sage: bool(alpha_bar*alpha == alpha*alpha_bar)
True
sage: alpha_bar*alpha
[(a + I*b)*(a - I*b) + (c + I*d)*(c - I*d)                                          0]
[                                         0 (a + I*b)*(a - I*b) + (c + I*d)*(c - I*d)]
```

Note that $(a+ib)(a-ib) = a^2 + b^2$ and the same for c and d.

Earlier we found the identity is

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Thus the multiplicative inverse (both on the left and right) such that $\alpha\beta = \beta\alpha = \mathbf{1}$ is given by $(1/t)\bar{\alpha}$.

Q5

From part 4 we show there is a multiplicative inverse. Thus by the definition, $\mathcal{L}$ is a skew field.

F. Ring of Endomorphisms

Q1

Let $f, g, h \in End(G)$

1. $f + g = g + f$
2. $(f \cdot g) \cdot h = f \cdot (g \cdot h)$
3. $f \cdot (g + h) = f \cdot g + f \cdot h$

Q2

For a homomorphism $f(0) = 0$

Applying the rule $f(a+b) = f(a) + f(b)$

$$e = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 1 & 2 & 3 \end{pmatrix}$$

$$a = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 2 & 0 & 2 \end{pmatrix}$$

$$b = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 3 & 2 & 1 \end{pmatrix}$$

$$c = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

+	e	a	b	c
e	a	b	c	e
a	b	c	e	a
b	c	e	a	b
c	e	a	b	c

×	e	a	b	c
e	e	a	b	c
a	a	c	a	c
b	b	a	e	c
c	c	c	c	c

G. Direct Product of Rings

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$$
$$(x_1, y_1) \cdot (x_2, y_2) = (x_1x_2, y_1y_2)$$

Q1

1.

$$\begin{aligned}(x_1, y_1) + (x_2, y_2) &= (x_1 + x_2, y_1 + y_2) \\ &= (x_2 + x_1, y_2 + y_1) \\ &= (x_2, y_2) + (x_1, y_1)\end{aligned}$$

2.

$$\begin{aligned}(x_1, y_1) \cdot [(x_2, y_2) \cdot (x_3, y_3)] &= (x_1x_2x_3, y_1y_2y_3) \\ &= [(x_1, y_1) \cdot (x_2, y_2)] \cdot (x_3, y_3)\end{aligned}$$

3.

$$\begin{aligned}(x_1, y_1) \cdot [(x_2, y_2) + (x_3, y_3)] &= (x_1, y_1) \cdot (x_2 + x_3, y_2 + y_3) \\ &= (x_1 \cdot (x_2 + x_3), y_1 \cdot (y_2 + y_3)) \\ &= (x_1x_2 + x_1x_3, y_1y_2 + y_1y_3) \\ &= (x_1, y_1) \cdot (x_2, y_2) + (x_1, y_1) \cdot (x_3, y_3)\end{aligned}$$

Q2

$$\begin{aligned}(x_1, y_1) \cdot (x_2, y_2) &= (x_1x_2, y_1y_2) \\ &= (x_2x_1, y_2y_1) \\ &= (x_2, y_2) \cdot (x_1, y_1)\end{aligned}$$

$$\begin{aligned}(1, 1) \cdot (x_1, y_1) &= (1x, 1y) \\ &= (x, y)\end{aligned}$$

Q3

Divisors of 0 are x_1, x_2 and y_1, y_2 such that $x_1x_2 = 0'_x$ and $y_1y_2 = 0'_y$ where for any $x \in A$ and $y \in B$ $x + 0'_x = x$ and $y + 0'_y = y$.

$(x, 0)$ and $(0, y)$ are zero divisors of $A \times B$.

Q4

(a, b) is an invertible elemtn of $A \times B$ iff there is an ordered pair (c, d) in $A \times B$ satisfying $(a, b) \cdot (c, d) = (1, 1)$.

Q5

Because $A \times B$ has zero divisors, it is not an integral domain, thus also not a field since every field is an integral domain.

H. Elementary Properties of Rings

Q1

In any ring, $a(b - c) = ab - ac$ and $(b - c)a = ba - ca$.

$$
\begin{aligned}
a(b-c) &= a(b+(-c)) \\
&= ab + a(-c) \\
&= ab - ac
\end{aligned}
$$

$$
(b-c)a = ba - ca
$$

Q2

In any ring, if $ab = -ba$, then $(a + b)^2 = (a - b)^2 = a^2 + b^2.

$$
\begin{aligned}
(a+b)^2 &= (a+b)a + (a+b)b \\
&= a^2 + ba + ab + b^2 \\
&= a^2 + ba + (-ba) + b^2 \\
&= a^2 + b^2
\end{aligned}
$$

$$
\begin{aligned}
(a-b)^2 &= (a-b)a - (a-b)b \\
&= a^2 - ba - ab - (-b^2)
\end{aligned}
$$

Now to solve this we prove that $(-x)(-y) = xy$. We make use of 3 facts of rings:

1. $a0 = 0 = 0a$
2. $x + (-x) = 0$
3. $a(x+y) = ax + ay$

$$
\begin{aligned}
(-x)(-y) &= (-x)(-y) + x(-y+y) \\
&= (-x)(-y) + x(-y) + xy \\
&= (-x+x)(-y) + xy \\
&= 0 + xy \\
&= xy
\end{aligned}
$$

$$
\begin{aligned}
(a-b)^2 &= a^2 - ba - ab - (-b^2) \\
&= a^2 - ba - ab + b^2 \\
&= a^2 + ab - ab + b^2 \\
&= a^2 + b^2
\end{aligned}
$$

Q3

In any integral domain, if $a^2 = b^2$, then $a = \pm b$.

An integral domain is a commutative ring with unity having the cancellation property.

The cancellation property says:

If $ab = ac$ or $ba = ca$, then $b = c$ if $a \neq 0$.

$$
\begin{aligned}
a^2 - b^2 &= 0 \\
&= (a+b)a - (a+b)b \qquad \text{[Note: integral domain is commutative]} \\
&= (a+b)(a-b)
\end{aligned}
$$

Integral domains have no divisors of zero, so $(a+b)(a-b) = 0$ implies that either $a + b = 0$ or $a - b = 0$. In either case, adding or subtracting b from both sides yields $a = \pm b$.

Q4

*In any integral domain, only 1 and -1 are their own multiplicative inverses.$

Note that $x = x^{-1}$ iff $x^2 = 1$

Taking the converse, only $(-1)^2$ and 1^2 are equal to 1.

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

Q5

Show that the commutative law for addition need not be assumed in defining a ring with unity: it may be proved from the other axioms.

$$\begin{aligned}(a+b)(1+1) = (a+b)1 + (a+b)1 &= a(1+1) + b(1+1) \\ a+b+a+b &= a+a+b+b \\ (-a)+a+b+a+b &= (-a)+a+a+b+b \\ b+a+b &= a+b+b \\ b+a+b+(-b) &= a+b+b+(-b) \\ b+a &= a+b\end{aligned}$$

Q6

Let A be any ring. Prove that if the additive group of A is cyclic, then A is a commutative ring.

Let c be the additive generator of A. Then any element of A can be expressed as repeated addition of c for n times. Then adding two elements of A where $a = nc$ and $b = mc$, then $ab = (m+n)c = ba$.

Q7

Prove if any integral domain if $a^n = 0$ for some integer n, then $a = 0$.

$$a^n = a^{n-1}a = a \cdots a = 0$$

But integral domains have no zero divisors. Thus $a = 0$.

I. Properties of Invertible Elements

Prove parts 1-5 are true in a nontrivial ring with unity.

Q1

If a is invertible and $ab = ac$ then $b = c$.

Pre-multiply by a^{-1} on both sides and by $a^{-1}a = 1$, then $b = c$.

Q2

An element a can have no more than one multiplicative inverse.

This would imply $ab = ac$ where $b \neq c \neq 0$, which is a contradiction.

Q3

If $a^2 = 0$ then $a + 1$ and $a - 1$ are invertible.

$$\begin{aligned} a^2 &= 0 \\ a^2 - 1 &= -1 \\ (a+1)(a-1) &= -1 \\ -1(a+1)(a-1) &= 1 \end{aligned}$$

Thus the inverse $(a+1)^{-1} = -(a-1)$ and $(a-1)^{-1} = -(a+1)$.

Q4

If a and b are invertible, their product ab is invertible.

$$\begin{aligned} ab(ab)^{-1} &= abb^{-1}a^{-1} \\ &= aa^{-1} \\ &= 1 \end{aligned}$$

Q5

The set S of all the invertible elements in a ring is a multiplicative group.

By above, any $a, b \in S$ where a and b are invertible, then their product ab is also invertible and hence $ab \in S$.

Q6

By part 5, the set of all the nonzero elements in a field is a multiplicative group. Now use Lagrange's theorem to prove that in a finite field with m elements, $x^{m-1} = 1$ for every $x \neq 0$.

By Lagrange's theorem, the order of any element in the group must divide the group's order. Therefore let $\mathrm{ord}(x) = n$, then $m - 1 = qn$ where $|S| = m$. Note we are not counting the zero element as part of the multiplicative group.

$$x^(m-1) = x^{qn} = (x^n)^q = 1$$

Q7

*If $ax = 1$, x is a right inverse of a; if $ya = 1$, y is a left inverse of a. Prove if a has a right inverse x and a left inverse y, then a is invertible, and its inverse is equal to x and to y.

$$\begin{aligned} yaxa &= y(ax)a = 1 \\ &= (ya)(xa) && = xa \end{aligned}$$

Thus $ax = xa = 1$, and by similar argument $ay = ya = 1$.

Q8

Prove that in a commutative ring, if ab is invertible, then a and b are both invertible.

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

Thus a and b are both invertible.

J. Properties of Divisors of Zero

Q1

If $a \neq \pm 1$ and $a^2 = 1$, then $a + 1$ and $a - 1$ are divisors of zero.

$$a^2 - 1 = 0 = (a + 1)(a - 1)$$

Q2

If ab is a divisor of zero, then a or b is a divisor of zero.

$$a \neq 0, abx = 0 = a(bx) = 0$$

Likewise for b.

Q3

In a commutative ring with unity, a divisor or zero cannot be invertible.

$$x \neq 0, a^{-1}ax = a^{-1}(ax) = a^{-1}0 = 0 = (a^{-1}a)x = 1x = x$$

Proof by contradiction.

Q4

Suppose $ab \neq 0$ in a commutative ring. If either a or b is a divisor or zero, so is ab.

$$(ax)b = 0b = 0 = abx$$

Same for b.

Q5

Suppose a is neither 0 nor a divisor or zero. If $ab = ac$ then $b = c$.

$$ab - ac = a(b - c) = 0$$

Since $a \neq 0$ and is not a divisor of zero, then $b - c = 0$.

Hence $b - c = 0$ or $b = c$.

Q6

$A \times B$ always has divisors of zero.

$(x, 0)$ and $(0, y)$ are zero divisors of $A \times B$.

K. Boolean Rings

A ring A is a boolean ring if $a^2 = a$ for every $a \in A$. Prove that parts 1 and 2 are true in any boolean ring A.

Q1

For every $a \in A$, $a = -a$.

$$\begin{aligned}
(a+a)^2 &= (a+a) \\
&= a(a+a) + a(a+a) = a^2 + a^2 + a^2 + a^2 = a + a + a + a \\
a + a + a + a &= a + a \\
a + a + a + a + (-a) + (-a) &= a + a + (-a) + (-a) \\
a + a &= 0 \\
a + a + (-a) &= -a \\
a &= -a
\end{aligned}$$

Q2

$$\begin{aligned}
(a+b) &= (a+b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b \\
ab + ba &= 0 \\
ab &= ba
\end{aligned}$$

Q3

$$x(x-1) = x^2 - x = x - x = 0$$

Thus for every $x \notin \{0,1\}$, x is a divisor of zero.

Q4

$$aa^{-1} = 1 = a(aa^{-1})a^{-1} = a^2a^{-1}a^{-1} = (aa^{-1})a^{-1} = a^{-1}$$

Q5

$$a \vee b = a + b + ab$$

$$a \vee bc = a + bc + abc$$

$$(a \vee b)(a \vee c) = (a + b + ab)(a + c + ac) = a^2 + ac + a^2c + ba + bc + bac + a^2b + abc + a^2bc$$

Using the fact $a^2 = a$, $a = -a$ and that A is commutative, we get

$$(a \vee b)(a \vee c) = a + bc + abc = a \vee bc$$

$$a \vee (1 + a) = a + 1 + a + a + a^2 = 1$$

$$a \vee a = a + a + a^2 = a$$

$$a(a \vee b) = a^2 + ab + a^2b = a$$

I. The Binomial Formula

Prove

$$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$$

Expansion for $a^{n-k}b^k$ is

$$\binom{n}{k}$$

Thus

$$\binom{n-1}{k} + \binom{n-1}{k-1} = \binom{n}{k}$$

Hence formula is true by induction.

M. Nilpotent and Unipotent Elements

An element a of a ring is *nilpotent* if $a^n = 0$ for some positive integer n.

Q1

In a ring with unity, prove that if a is nilpotent, then $a+1$ and $a-1$ are both invertible.

$$\begin{aligned}
1 - a^n &= (1-a)(1 + a + a^2 + \cdots + a^{n-1}) \\
&= (1-a)(-1\dot{-}1)(1 + a + a^2 + \cdots + a^{n-1}) \\
&= (a-1)(a^{n-1} + \cdots + a^2 + a + 1) \\
&= (1+a)(1 - a + a^2 - a^3 + \cdots \pm a^{n-1}) \\
&= (a+1)(1 - a + a^2 - a^3 + \cdots \pm a^{n-1}) \\
&= 1
\end{aligned}$$

Because $a^n = 0$

Q2

In a commutative ring, prove that any product xa of a nilpotent element a by any element x is nilpotent.

$$(xa)^n = x^n a^n = x^n 0 = 0$$

Q3

In a commutative ring, prove the sum of two nilpotent elements is nilpotent.

$(a+b)^{m+n}$ is nilpotent, because every element of the expansion is zero. When the power of a is less than m, then the power of b is greater than n and vice versa.

Q4

In a commutative ring, prove that the product of two unipotent elements a and b is unipotent.

$$(1-a)^n = 0 \quad \text{and} \quad (1-b)^m = 0$$
$$(1-ab)^{m+n} = [(1-a) + a(1-b)]^{m+n}$$

From part 3 above.

Q5

In a ring with unity, prove that every unipotent element is invertible.

From part 1 we see

$$1 - a^n = (1-a)(1 + a + \cdots + a^{n-1}) = 1$$

But a is unipotent hence $(1-a)^n = 0$,

$$1 - (1-a)^n = (1 - (1-a))(\cdots) = a(\cdots) = 1$$

Hence a is invertible.