Abstract Algebra by Pinter, Chapter 19

Amir Taaki

Abstract

Chapter 19 on Quotient Rings

Contents

1 A. Examples of Quotient Rings

1.1 Q1

$$A = \mathbb{Z}_{10}, J = \{0, 5\}$$

$$\begin{aligned} J = J + 0 &= \{0, 5\} \\ J + 1 &= \{1, 6\} \\ J + 2 &= \{2, 7\} \\ J + 3 &= \{3, 8\} \\ J + 4 &= \{4, 9\} \end{aligned}$$

+	J	J + 1	J + 2	J + 3	J + 4
J	J	J + 1	J + 2	J + 3	J + 4
J + 1	J + 1	J + 2	J + 3	J + 4	J
J + 2	J + 2	J + 3	J + 4	J	J + 1
J + 3	J + 3	J + 4	J	J + 1	J + 2
J + 4	J + 4	J	J + 1	J + 2	J + 3

·	J	J + 1	J + 2	J + 3	J + 4
J	J	J	J	J	J
J + 1	J	J + 1	J + 2	J + 3	J + 4
J + 2	J	J + 2	J + 4	J + 1	J + 3
J + 3	J	J + 3	J + 1	J + 4	J + 2
J + 4	J	J + 4	J + 3	J + 2	J + 1

1.2 Q2

$$A = P_3, J = \{\emptyset, \{a\}\}$$

$$\begin{aligned} J = J + 0 &= \{\emptyset, \{a\}\} \\ J + \{b\} &= \{\{b\}, \{a, b\}\} \\ J + \{c\} &= \{\{c\}, \{a, c\}\} \\ J + \{b, c\} &= \{\{b, c\}, \{a, b, c\}\} \end{aligned}$$

+	J	J + {b}	J + {c}	J + {b,c}
J	J	J + {b}	J + {c}	J + {b,c}
J + {b}	J + {b}	J	J + {b,c}	J + {c}
J + {c}	J + {c}	J + {b,c}	J	J + {b}
J + {b,c}	J + {b,c}	J + {c}	J + {b}	J

·	J	J + {b}	J + {c}	J + {b,c}
J	J	J	J	J
J + {b}	J	J + {b}	J	J + {b}
J + {c}	J	J	J + {c}	J + {c}
J + {b,c}	J	J + {b}	J + {c}	J + {b,c}

1.3 Q3

$$A = \mathbb{Z}_2 \times \mathbb{Z}_6, J = \{(0,0),(0,2),(0,4)\}$$

$$\begin{aligned} J &= \{(0,0),(0,2),(0,4)\} \\ J + (0,1) &= \{(0,1),(0,3),(0,5)\} \\ J + (1,0) &= \{(1,0),(1,2),(1,4)\} \\ J + (1,1) &= \{(1,1),(1,3),(1,5)\} \end{aligned}$$

+	J	J + (0,1)	J + (1,0)	J + (1,1)
J	J	J + (0,1)	J + (1,0)	J + (1,1)
J + (0,1)	J + (0,1)	J	J + (1,1)	J + (1,0)
J + (1,0)	J + (1,0)	J + (1,1)	J	J + (0,1)
J + (1,1)	J + (1,1)	J + (1,0)	J + (0,1)	J

·	J	J + (0,1)	J + (1,0)	J + (1,1)
J	J	J	J	J
J + (0,1)	J	J + (0,1)	J	J + (0,1)
J + (1,0)	J	J	J + (1,0)	J + (1,0)
J + (1,1)	J	J + (0,1)	J + (1,0)	J + (1,1)

2 B. Examples of the Use of the FHT

2.1 Q1

$$f(x) = x \bmod 5$$
$$\ker f = \{0,5,10,15\} = \langle 5 \rangle$$
$$\mathbb{Z}_5 \cong \mathbb{Z}_{20}/\langle 5 \rangle$$

$$\begin{aligned} J = J + 0 &= \{0,5,10,15\} \\ J + 1 &= \{1,6,11,16\} \\ J + 2 &= \{2,7,12,17\} \\ J + 3 &= \{3,8,13,18\} \\ J + 4 &= \{4,9,14,19\} \end{aligned}$$

+	J	J + 1	J + 2	J + 3	J + 4
J	J	J + 1	J + 2	J + 3	J + 4
J + 1	J + 1	J + 2	J + 3	J + 4	J
J + 2	J + 2	J + 3	J + 4	J	J + 1
J + 3	J + 3	J + 4	J	J + 1	J + 2
J + 4	J + 4	J	J + 1	J + 2	J + 3

·	J	J + 1	J + 2	J + 3	J + 4
J	J	J	J	J	J
J + 1	J	J + 1	J + 2	J + 3	J + 4
J + 2	J	J + 2	J + 4	J + 1	J + 3
J + 3	J	J + 3	J + 1	J + 4	J + 2
J + 4	J	J + 4	J + 3	J + 2	J + 1

Tables are exact same for mod 5.

2.2 Q2

$$f(x) = x \bmod 3$$
$$\ker f = \{0, 3\} = \langle 3 \rangle$$
$$\mathbb{Z}_3 \cong \mathbb{Z}_6/\langle 3 \rangle$$

$$\begin{aligned} J = J + 0 &= \{0, 3\} \\ J + 1 &= \{1, 4\} \\ J + 2 &= \{2, 5\} \end{aligned}$$

+	J	J + 1	J + 2
J	J	J + 1	J + 2
J + 1	J + 1	J + 2	J
J + 2	J + 2	J	J + 1

·	J	J + 1	J + 2
J	J	J	J
J + 1	J	J + 1	J + 2
J + 2	J	J + 2	J + 1

Tables are exact same for mod 3.

2.3 Q3

$$P_2 = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$$
$$P_3 = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$$

$$\begin{aligned} K = K + \emptyset &= \{\emptyset, \{c\}\} \\ K + \{a\} &= \{\{a\}, \{a, c\}\} \\ K + \{b\} &= \{\{b\}, \{b, c\}\} \\ K + \{a, b\} &= \{\{a, b\}, \{a, b, c\}\} \end{aligned}$$

$$f(X) = X \cap \{a, b\}$$
$$f : P_3 \to P_2$$
$$P_2 \cong P_3/\langle\{\emptyset, \{c\}\}\rangle$$

+	K	K + {a}	K + {b}	K + {a,b}
K	K	K + {a}	K + {b}	K + {a,b}
K + {a}	K + {a}	K	K + {a,b}	K + {b}
K + {b}	K + {b}	K + {a,b}	K	K + {a}
K + {a,b}	K + {a,b}	K + {b}	K + {a}	K

·	K	K + {a}	K + {b}	K + {a,b}
K	K	K	K	K
K + {a}	K	K + {a}	K	K + {a}
K + {b}	K	K	K + {b}	K + {b}
K + {a,b}	K	K + {a}	K + {b}	K + {a,b}

2.4 Q4

$$f : \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2$$
$$f((x, y)) = x$$
$$K = \{(0, 0), (0, 1)\}$$
$$K + (1, 0) = \{(1, 0), (1, 1)\}$$

+	K	K + (1,0)
K	K	K + (1,0)
K + (1,0)	K + (1,0)	K

·	K	K + (1,0)
K	K	K
K + (1,0)	K	K + (1,0)

3 C. Quotient Rings and Homomorphic Images in $\mathcal{F}(\mathbb{R})$

3.1 Q1

$$\phi : \mathcal{F}(\mathbb{R}) \to \mathbb{R} \times \mathbb{R}$$
$$\phi(f) = (f(0), f(1))$$

1. $\phi(f + g) = ((f + g)(0), (f + g)(1)) = (f(0), f(1)) + (g(0), g(1)) = \phi(f) + \phi(g)$
2. $\phi(f \cdot g) = ((f \cdot g)(0), (f \cdot g)(1)) = (f(0), f(1))(g(0), g(1)) = \phi(f)\phi(g)$

Let $f(x) = (a - b)x + b$, then $f \in \mathcal{F}(\mathbb{R})$, $f(0) = b$ and $f(1) = a$. Thus functions of this form can represent any value in $\mathbb{R} \times \mathbb{R}$ and so the homomorphism ϕ is *onto* $\mathbb{R} \times \mathbb{R}$.

$$K = \{f \in \mathcal{F}(\mathbb{R}) : f(0) = 0 \text{ and } f(1) = 0\}$$

3.2 Q2

$$J = \{f \in \mathcal{F}(\mathbb{R}) : f(0) = 0 \text{ and } f(1) = 0\}$$

Thus J is the kernel of the homomorphism ϕ. The kernel is also an ideal of $\mathcal{F}(\mathbb{R})$, so

$$\mathcal{F}(\mathbb{R})/J \cong \mathbb{R} \times \mathbb{R}$$

3.3 Q3

$$\phi : \mathcal{F}(\mathbb{R}) \to \mathcal{F}(\mathbb{Q}, \mathbb{R})$$
$$\phi(f) = f_{\mathbb{Q}} = \text{ the restriction of } f \text{ to } \mathbb{Q}$$

ϕ is onto because $\forall g \in \mathcal{F}(\mathbb{Q}, \mathbb{R}), \exists f \in \mathcal{F}(\mathbb{R}) : g = f_{\mathbb{Q}}$. ϕ is a homomorphism since $\phi(f \cdot g) = \phi(f) \cdot \phi(g)$ and $\phi(f + g) = \phi(f) + \phi(g)$.

$$K = \{f \in \mathcal{F}(\mathbb{R}) : f(x) = 0\}$$

3.4 Q4

J is also the kernel of $\mathcal{F}(\mathbb{R})$, which means it is also an ideal. Thus

$$\mathcal{F}(\mathbb{R})/J \cong \mathcal{F}(\mathbb{Q})$$

4 D. Elementary Applications of the Fundamental Homomorphism Theorem

4.1 Q1

Note that ring is commutative then

$$(x+y)^2 = x(x+y) + y(x+y) = x^2 + xy + yx + y^2 = x^2 + 2xy + y^2 = x^2 + y^2$$

So $h(x) = x^2$ is a homomorphism since $h(x+y) = x^2 + y^2 = h(x) + h(y)$ and $h(xy) = x^2y^2 = h(x)h(y)$

$$J = \{x \in A : x^2 = 0\}$$
$$B = \{x^2 : x \in A\}$$

h is a homomorphism from A to B and the kernel is J

$$A/J \cong B$$

4.2 Q2

$h(x) = 3x$ is a homomorphism because $h(x+y) = 3x + 3y = h(x) + h(y)$ and $h(xy) = h(x)h(y)$ because

$$h(xy) = 3xy = 6xy + 3xy = (3x)(3y) = h(x)h(y)$$

$J = \{x : 3x = 0\}$ is the kernel and thus ideal of h. $B = \{3x : x \in A\}$ is a subring of A by the homomorphism shown above

$$A/J \cong B$$

4.3 Q3

$$\pi_a(xy) = axy = a^2xy = (ax)(ay) = \pi_a(x)\pi_a(y)$$
$$\pi_a(x+y) = a(x+y) = ax + ay = \pi_a(x) + \pi_a(y)$$
$$I_a = \{x \in A : ax = 0\} = \ker \pi_a$$
$$\pi_a(1) = a$$
$$\pi_a(x) = \pi_a(x \cdot 1) = a + \cdots + a \in \langle a \rangle$$
$$\pi_a : A \to \langle a \rangle$$
$$A/I_a \cong \langle a \rangle$$

4.4 Q4

$$\phi(ab) = \pi_{ab} = \pi_a\pi_b = \phi(a)\phi(b)$$
$$\phi(a+b) = \pi_{a+b} = \pi_a + \pi_b = \phi(a) + \phi(b)$$
$$I = \{x \in A : ax = 0, \forall a \in A\}$$
$$\pi_a(x) = ax$$
$$\bar{A} = \{\pi_a : a \in A\}$$
$$\phi(a) = \pi_a$$
$$\ker \phi = \{x \in A : \phi(x) = \pi_0\}$$
$$\forall a \in A \qquad \pi_0(a) = 0$$
$$\therefore \ker \phi = I$$
$$\phi : A \to \bar{A}$$
$$A/I \cong \bar{A}$$

5 E. Properties of Quotient Rings A/J in Relation to Properties of J

5.1 Q1

Every element of A/J has a square root iff for every $x \in A$, there is some $y \in A$ such that $x - y^2 \in J$.

Let $J + x \in A/J$ then

$$J + x = (J + y)(J + y)$$

But J is ideal and so absorbs products in A

$$J + x = J + y^2$$

$$J + x - y^2 = J$$

$$x - y^2 \in J$$

5.2 Q2

Every element of A/J is its own negative iff $x + x \in J$ for every $x \in A$.

$$\forall x \in A, x + x \in J \implies J + x + x = J$$

$$\therefore \forall x \in A \qquad J + x = -(J + x)$$

5.3 Q3

A/J is a boolean ring iff $x^2 - x \in J$ for every $x \in A$.

$$(J + x)^2 - (J + x) = J^2 + Jx + xJ + x^2 - J - x$$

But noting J absorbs products

$$(J + x)^2 - (J + x) = J + x^2 - x$$

But $x^2 - x \in J$ so

$$J + x^2 - x = J$$

so A/J is a boolean ring.

5.4 Q4

If J is the ideal of all the nilpotent elements of commutative ring A, then A/J has no nilpotent elements (except zero).

$$a \in J \implies a^n = 0 \text{ for some } n$$

Let $x \in A : x \notin J \implies x^n \neq 0$

$$(J + x)^n = J + x^n \neq J$$

Thus $\forall x \in A : x \in J$, $J + x$ is not nilpotent.

5.5 Q5

Every element of A/J is nilpotent iff J has the following property: for every $x \in A$, there is a positive integer n such that $x^n \in J$.

$$\forall x \in A, x^n \in J$$

$$(J + x)^n = J + x^n = J$$

Thus every element of A/J is nilpotent.

5.6 Q6

A/J has a unity element iff there exists an element $a \in A$ such that $ax - x \in J$ and $xa - x \in J$ for every $x \in A$.

$$\begin{aligned}(J+a)(J+x) &= J+x \\ &= J+ax \\ (J+x)(J+a) &= J+x \\ &= J+xa\end{aligned}$$

$$J+x = J+ax$$

$$J+ax-x = J$$

So $ax - x \in J$ Likewise

$$J+xa = J+x$$

$$J+xa-x = J$$

$$\implies xa - x \in J$$

6 F. Prime and Maximal Ideals

Let A be a commutative ring with unity, and J an ideal of A. Prove the following:

6.1 Q1

A/J is a commutative ring with unity.

$$(J+x)(J+y) = J+xy$$

But $xy = yx$

$$J+xy = J+yx$$

$$\implies (J+x)(J+y) = (J+y)(J+x)$$

$$(J+1_A)(J+x) = J+x$$

6.2 Q2

J is a prime ideal iff A/J is an integral domain.

Assume J is a prime ideal.

$$ab \in J \implies a \in J \text{ or } b \in J$$

$$J+ab = J+ac \implies J+b = J+c$$

Let $J+ab = J+ac$

$$J+ab-ac = J$$

$$a(b-c) \in J$$

But $a \notin J, b \notin J$ and $c \notin J$

$$\implies b - c \in J$$

$$J+b = J+c$$

Thus

$$J+ab = J+ac \implies J+b = J+c$$

For the converse, assume $a \notin J$, if $a \in J$, then we are done, otherwise

$$J + ab = J + a0 \implies J + b = J + 0$$

$$J + ab = J \implies J + b = J$$
$$a(b - c) \in J \implies b - c \in J$$
$$ab \in J \implies b \in J$$

6.3 Q3

Every maximal ideal of A is a prime ideal.

Let J be a maximal ideal of A.

Then A/J is a field.

Every field is an integral domain, so A/J is an integral domain.

Since A/J is an integral domain, so J is a prime ideal.

6.4 Q4

If A/J is a field, then J is a maximal ideal.

$$\phi(x) = J + x$$
$$j \in J, \phi(j) = J$$

A/J is a field, so ideal is J, which is maximal.

7 G. Further Properties of Quotient Rings in Relation to Their Ideals

7.1 Q1

Prove that A/J is a field iff for every element $a \in A$, where $a \notin J$, there is some $b \in A$ such that $ab - 1 \in J$.

$$(J + a)(J + b) = J + ab = J + 1 \implies ab - 1 \in J$$

7.2 Q2

Prove that every nonzero element of A/J is either invertible or a divisor of zero iff the following property holds, where $a, x \in A$: For every $a \notin J$, there is some $x \notin J$ such that either $ax \in J$ or $ax - 1 \in J$.

$$ax - 1 \in J \implies (J + a)(J + x) = J + 1$$

and thus $J + a$ is invertible.

$$ax \in J \implies (J + a)(J + x) = J$$

and so $J + a$ is a divisor of zero.

7.3 Q3

An ideal J of a ring A is called primary iff for all $a, b \in A$, if $ab \in J$, then either $a \in J$ or $b^n \in J$ for some positive integer n. Prove that every zero divisor in A/J is nilpotent iff J is primary.

Nilpotent means $(J + x)^n = J$, but $(J + x)^n = J + x^n$, that is $x^n \in J$. Every zero divisor in A/J means $(J + a)(J + b) = J + ab = J$ or that $ab \in J$. Thus either $a^1 \in J$ or $b^n \in J$. Thus we can say that $J + b$ is nilpotent since $(J + b)^n = J$.

7.4 Q4

An ideal J of a ring A is called semiprime iff it has the following property: For every $a \in A$, if $a^n \in J$ for some positive integer n, then necessarily $a \in J$. Prove that J is semiprime iff A/J has no nilpotent elements (except zero).

A/J has no nilpotent elements means that $J + x^n \neq J$ for any integer n. Thus for every $a \in A : a \notin J$, then $a^n \notin J$. If A/J has a nilpotent element, then J cannot be semiprime because $a \notin J$ and $a^n \in J$ is a contradiction. This also holds true in reverse since $a^n \in J$ where $a \notin J$ would imply J is not semiprime.

7.5 Q5

Prove that an integral domain can have no nonzero nilpotent elements. Then use part 4, together with Exercise F2, to prove that every prime ideal in a commutative ring is semiprime.

Nilpotent elements are also zero divisors since $a^n = 0 = a \cdot a^{n-1}$. So an integral domain cannot have nilpotent elements.

From F2, we learn that if J is a prime ideal, then A/J is an integral domain (no nilpotent elements). From the last exercise, we see that if A/J has no nilpotent elements, then J is semiprime.

8 H. $\mathbb{Z}_n$ as a Homomorphic Image of $\mathbb{Z}$

8.1 Q1

$$x^2 - 7y^2 - 24 = 0$$
$$\phi : \mathbb{Z} \to \mathbb{Z}_7$$
$$x^2 - 3 = 0$$
$$x^2 = 3$$
$$\forall x \in \mathbb{Z}_7, x^2 \neq 3$$

No solution.

8.2 Q2

$$x^2 + (x+1)^2 + (x+2)^2 = y^2$$
$$3x^2 + 6x + 5 = y^2$$
$$\phi : \mathbb{Z} \to \mathbb{Z}_3$$
$$y^2 = 2$$
$$\forall y \in \mathbb{Z}_3, y^2 \neq 2$$

No solution.

8.3 Q3

$$x^2 + 10y^2 = 10n + a, a \in \{2, 3, 7, 8\}$$
$$\phi : \mathbb{Z} \to \mathbb{Z}_{10}$$
$$x^2 = a$$

$$
\begin{aligned}
0^2 &= 0 \\
1^2 &= 1 \\
2^2 &= 4 \\
3^2 &= 9 \\
4^2 &= 6 \\
5^2 &= 5 \\
6^2 &= 6 \\
7^2 &= 9 \\
8^2 &= 6 \\
9^2 &= 1
\end{aligned}
$$

No solution.

8.4 Q4

$$3, 8, 13, 18, 23, \cdots = \langle 3 \rangle$$
$$x \in \mathbb{Z}_5 : x^2 = 3$$

$$
\begin{aligned}
0^2 &= 0 \\
1^2 &= 1 \\
2^2 &= 4 \\
3^2 &= 4 \\
4^2 &= 1
\end{aligned}
$$

8.5 Q5

$$2, 10, 18, 26, \cdots = \langle 2 \rangle$$
$$x \in \mathbb{Z}_8 : x^3 = 2$$

$$
\begin{aligned}
0^3 &= 0 \\
1^3 &= 1 \\
2^3 &= 0 \\
3^3 &= 1 \\
4^3 &= 0 \\
5^3 &= 5 \\
6^3 &= 0 \\
7^3 &= 7
\end{aligned}
$$

8.6 Q6

$$3, 11, 19, 27, \cdots = \langle 3 \rangle$$
$$x \in \mathbb{Z}_8 : x^2 + y^2 = 3$$

$$
\begin{aligned}
0^2 &= 0 \\
1^2 &= 1 \\
2^2 &= 4 \\
3^2 &= 1 \\
4^2 &= 0 \\
5^2 &= 1 \\
6^2 &= 4 \\
7^2 &= 1
\end{aligned}
$$

For any $a \in \mathbb{Z}_8, a^2 = 1$ or $a^2 = 4$, so $\nexists x, y \in \mathbb{Z}_8 : x^2 + y^2 = 3$

8.7 Q7

$$n(n+1) = 10u + a, a \in \{0, 2, 6\}$$
$$\phi : \mathbb{Z} \to \mathbb{Z}_{10}$$

$$
\begin{aligned}
0 \cdot 1 &= 0 \\
1 \cdot 2 &= 2 \\
2 \cdot 3 &= 6 \\
3 \cdot 4 &= 2 \\
4 \cdot 5 &= 0 \\
5 \cdot 6 &= 0 \\
6 \cdot 7 &= 2 \\
7 \cdot 8 &= 6 \\
8 \cdot 9 &= 2 \\
9 \cdot 0 &= 0
\end{aligned}
$$

Thus $n(n+1) \in \{0, 2, 6\}$

8.8 Q8

$$n(n+1)(n+2) = 10u + a, a \in \{0, 4, 6\}$$
$$\phi : \mathbb{Z} \to \mathbb{Z}_{10}$$

$$
\begin{aligned}
0 \cdot 1 \cdot 2 &= 0 \\
1 \cdot 2 \cdot 3 &= 6 \\
2 \cdot 3 \cdot 4 &= 4 \\
3 \cdot 4 \cdot 5 &= 0 \\
4 \cdot 5 \cdot 6 &= 0 \\
5 \cdot 6 \cdot 7 &= 0 \\
6 \cdot 7 \cdot 8 &= 6 \\
7 \cdot 8 \cdot 9 &= 4 \\
8 \cdot 9 \cdot 0 &= 0 \\
9 \cdot 0 \cdot 1 &= 0
\end{aligned}
$$