Let $Q$ be the group of rational numbers under addition and let $Q^*$ be the group of nonzero rational numbers under multiplication. In $Q$, list the elements in $<\frac{1}{2}>$. In $Q^*$, list the elements in $<\frac{1}{2}>$. 

$<\frac{1}{2}> = \{\ldots, -3\frac{1}{2}, -2\frac{1}{2}, -1\frac{1}{2}, 0, 1\frac{1}{2}, 2\frac{1}{2}, 3\frac{1}{2}, \ldots\}$ in $Q$

$<\frac{1}{2}> = \{\ldots, (\frac{1}{2})^{-3}, (\frac{1}{2})^{-2}, (\frac{1}{2})^{-1}, (\frac{1}{2})^0, (\frac{1}{2})^1, (\frac{1}{2})^2, (\frac{1}{2})^3, \ldots\}$ in $Q^*$

Prove that in any group, an element and its inverse have the same order.

Assume that $G$ is a group and $a \in G$. Then we separate the discussion by two parts case, 1: finite group and case 2: infinite group. Let’s see case 1 first. $a$ has finite order (say) $n$. It means that $a^n = e$

$$a^n = e = (a^n \cdot a^{-n}) = a^n (a^{-1})^n$$

It gives us that $a^{-1}$ have at most order $n$. If we let $a^{-1}$ have $k$ order such that $k < n$, then
\[ e = e^k = (a^k * a^{-k}) = a^k(a^{-1})^k = a^k \]

But we know that \( k \) cannot be the order of \( a \). Hence \( |a^{-1}| = n \).

Next, see infinite order case. Let \( a \) has infinite order and \( a^{-1} \) dose not, then we can say that \( |a^{-1}| = n \). Moveover finite inverse of \( a^{-1} \) that is \( (a^{-1})^{-1} \) has same number of order. But this cannot happen. Thus \( a^{-1} \) has infinite order.

Page67:6

Let \( x \) belong to a group. If \( x^2 \neq e \) and \( x^6 = e \), prove that \( x^4 \neq e \) and \( x^5 \neq e \).

What can we say about the order of \( x \)?

Obviously, \( x \neq e \) because \( x^n = e \) for all \( x \in \mathbb{Z} \). Then we can determine that \( x^6 = e = x^4 \cdot x^2 = x^2 \) if \( x^4 = 2 \). Also \( x^6 = x^5 \cdot x = x = e \) if \( x^5 = e \). Those cases are not true so that \( x^4 \neq e \) and \( x^5 \neq e \). Further we can say \( x^3 = e \) and \( x^6 = e \). That’s, \( x \) has order of 3 either 6.

Page67:10

Prove that an Abelian group with two elements of order 2 must have a subgroup of order 4.

Let \( G \) be an Abelian group with distinct elements \( a, b \) such that \( a^2 = b^2 = e \). Then the set of \( H = \{e, a, b, ab\} \) has order 4 and it is the subgroup of \( G \) by Finite subgroup test.

Page67:12

Suppose that \( H \) is a proper subgroup of \( \mathbb{Z} \) under addition and \( H \) contains 18, 30, and 40. Determine \( H \).

As it stated, \( H \) is closed under addition, \( H \) must be linear combination of 18, 30, and 40. We know that \( gcd(18, 30, 40) = 2 \) so that \( 2 = 18r + 30s + 40t \) for some integers \( r, s, \) and \( t \). This means that \( 2 \in H \) but \( H \neq \mathbb{Z} \). That’s \( H = 2\mathbb{Z} \).

Page67:15

Let \( G \) be a group. Show that \( Z(G) = \cap_{a \in G} C(a) \).

Suppose \( x \in Z(G) \). Then \( x \) commutes with every \( a \in G \) and \( x \in C(a) \) for all \( a \in G \). This means that \( x \in \cap_{a \in G} C(a) \) and \( Z(G) \subseteq \cap_{a \in G} C(a) \).

Conversely, suppose \( x \in \cap_{a \in G} C(a) \), this implies that \( x \in C(a) = \{y \in G : ay = ya\} \) for all \( a \in G \) and \( x \) commutes with all \( a \in G \), i.e., \( x \in Z(g) \).

Page67:18

If \( a \) and \( b \) are distinct group elements, prove that either \( a^2 \neq b^2 \), or \( a^3 \neq b^3 \).

This problem requires us to prove that one \( a^2 \neq b^2 \) and if not, prove an-
other $a^3 \neq b^3$. We just need to prove one of the statements at least. (NOT mutually exclusive) Let’s see the $a^2 \neq b^2$. When it is true, then nothing to prove. But assume that $a^2 = b^2$ with distinct elements $a \neq b$. It goes like this. $a \neq b \rightarrow a^2 a \neq a^2 b \rightarrow a^3 \neq a^2 b$ since $a^2 = b^2$, $a^3 \neq b^2 b \rightarrow a^3 \neq b^3$.

2 Isomorphisms

Page132:2
Find Aut($\mathbb{Z}$)

Let $a \in$ Aut($\mathbb{Z}$). Then, we can find two Automorphism; identity Automorphism and Automorphism with $a(n) = -n$. Note that $\mathbb{Z}$ is a cyclic group since every nonzero integer can be written as a finite sum $1 + 1 + \cdots$ or $(-1) + (-1) + \cdots (-1)$ and any Automorphism (which including Isomorphisms) has a mapping from generators to generators. $\mathbb{Z}$ is cyclic with 1, -1 two generators. Thus, $a(1) = \pm 1$. If $n \in \mathbb{Z}$, then $n = 1 \cdot n$ and $a(n) = a(1 \cdot n) = n \cdot a(1)$. We let $a(1) = 1$ then, it represents that identity Automorphism and $a(1) = -1$ for all $n \in \mathbb{Z}$ such that $a(a(n)) = -(-n) = n$ which is inverse of $a$ as well as a one to one correspondence. Also we know that it preserve the operation $a(n + m) = -(n + m) = -n - m = a(n) + a(m)$ Automorphism such that $a(n) = -n$.

Page132:5
Show that $U(8)$ is isomorphic to $U(12)$.
We define isomorphism $\phi : U(8) \rightarrow U(12)$ as follows:

$$\phi(1) = 1, \phi(3) = 5, \phi(5) = 7, \phi(7) = 11.$$ 

The mapping $\phi$ is apparently one-to-one and onto, and the multiplication tables of $U(8)$ and $U(12)$ are described as belows That shows the $\phi$ preserves

<table>
<thead>
<tr>
<th>U(8)</th>
<th>1</th>
<th>3</th>
<th>5</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>7</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>1</td>
<td>7</td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>7</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>5</td>
<td>3</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>U(12)</th>
<th>1</th>
<th>5</th>
<th>7</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>5</td>
<td>7</td>
<td>11</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>1</td>
<td>11</td>
<td>7</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>11</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>7</td>
<td>5</td>
<td>1</td>
</tr>
</tbody>
</table>
3 Cosets and Lagrange’s Theorem

Page148:2
Let $H = \{(1), (12)(34), (13)(24), (14)(23)\}$. Find the left cosets of $H$ in $S_4$.

$|S_4| = 24$ and $|H| = 4$ then $|S_4|/|H| = 24/4 = 6$ by Lagrange’s Theorem.

Page148:8
Suppose that $a$ has order 15. Find all of the left cosets of $<a^5>$ in $<a>$.

The cosets should be $<a^5>$, $a <a^5>$, $a^2 <a^5>$, $a^3 <a^5>$, $a^4 <a^5>$.

Page148:14
Suppose that $K$ is a proper subgroup of $H$ and $H$ is a proper subgroup of $G$. If $|K| = 42$ and $|G| = 420$, what are the possible orders of $H$?

By Lagrange’s theorem, we know that only 2, 5 can be numbers satisfying that $|H| = 2 \cdot 42$, $5 \cdot 42$.

4 External direct products

Page165:2
Show that $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ has seven subgroups of order 2.

Every element of $G$ has order a divisor of 2 but the identity of $G$. Thus, we need to count the number of subgroups. So, there are $|G| − 1 = 8 − 1 = 7$.

Page165:4
Show that $G \oplus H$ is Abelian if and only if $G$ and $H$ are Abelian.

($\rightarrow$)
Let $a, c \in G$ and $b, d \in H$ then

$$(a, b)(c, d) = (c, d)(a, b)$$
$$(ac, bd) = (ca, db)$$

This implies that $ac = ca$, $bd = db$. Thus, $H$ and $G$ are commutative.

($\leftarrow$)
Assume that $G$ and $H$ are Abelian then we just follow the above argument in reverse.
Prove or disprove that $\mathbb{Z} \oplus \mathbb{Z}$ is a cyclic group.

Let $(a, b) \in \mathbb{Z} \oplus \mathbb{Z}$ for $a, b \in \mathbb{Z}$. If we let $a, b \neq 1$ and be a generator $< (a, b) >$ then, $(a + 1, b)$ or $(a, b + 1)$ which belong to $\mathbb{Z} \oplus \mathbb{Z}$ but cannot be generated by $< (a, b) >$. So, $\mathbb{Z} \oplus \mathbb{Z}$ is not cyclic.

Is $\mathbb{Z}_3 \oplus \mathbb{Z}_9$ isomorphic to $\mathbb{Z}_{27}$? Why?

$\mathbb{Z}_{27}$ contains an element of order 27 but $\mathbb{Z}_3 \oplus \mathbb{Z}_9$ have orders divisors of 9. Therefore it is not isomorphic.

5 Normal subgroups and Factor groups

Factor groups, set $G/H = \{aH|a \in G\}$ is a group.
requirement: group G, Normal subgroup H of G and group operation $(aH)(bH) = ab(H)$.

Let $G=\text{GL}(2,\mathbb{R})$ and let $\mathbb{K}$ be a subgroup of $\mathbb{R}^*$. Prove that $H=\{A \in G|\det A \in K\}$ is a normal subgroup of $G$.

Let G be a group and $h \in H$
Need to show $\{ghg^{-1} \in H\}$ for all $g \in G$.This means the normality of $H$ of $G$. (Normal subgroup test).
For all $x \in G$ and any $h \in H$ such that $\det (h) \in K$, $\det (ghg^{-1}) = \det (g) \det (h) \det (g^{-1}) = \det (g) \det (g^{-1}) \det (h) = \det (h) \in K$. In other words, $gHg^{-1} \subseteq H$

Prove that a factor group of a cyclic group is cyclic.

Let $G/H$ and $< g >= G$ be the factor group and cyclic group. Then $G/H = \{g^kH|k \in \mathbb{Z}\}$. Since $< g >$ is cyclic and properties of normality, it can be expressed that $G/H = \{(gH)^k|k\mathbb{Z}\}$ This implies that $< gH >$ is also cyclic.

Prove that a factor group of an Abelian group is Abelian.

Let $G$ be a Abelian group and normal group $H$. Assume that $G/H$ is the
factor group and select $a$ and $b$ such that $a, b \in G/H$. To verify the Abelian, a operation is applied thus, $(aH)(bH) = abH$ by the property of the factor group. Proceed that $abH = baH$ since $G$ is Abelian and $baH = (bH)(aH)$ for all $a, b$. Therefore, this is Abelian.

Page 191: 18
What is the order of the factor group $\mathbb{Z}_{60}/ <15>$?

The order of $\mathbb{Z}_{60}$ is 60 and $<15>$ is 4 then the factor group of order is $\frac{60}{4} = 15$

Page 191: 21
Prove that an Abelian group of order 33 is cyclic.

Let’s say $p$ divides the order of an Abelian group $G$ then $G$ has an element of order $p$. There will be 2 element say $(a, b)$ such that $a^3 = e$ and $b^11 = e$ because $33 = 3 \times 11$. Now we know that $(ab)^3 = a^3b^3 \neq e$ and $(ab)^{11} = a^{11}b^11 = a^2 \neq e$ in Abelian group so that 2 orders exist. Thus, $<ab>$ generates the cyclic group $G$.

Page 191: 69
Let $G$ be a group. If $H = \{g^2 | g \in G\}$ is a subgroup of $G$, prove that it is a normal subgroup of $G$.

Say $g_1 \in G$ and $h \in H$ such that $h = g^2$. Need to show $g_1Hg_1^{-1} \in G$. Rewrite $g_1hg_1^{-1} = g_1g^2g_1^{-1} = (g_1gg_1^{-1})(g_1gg_1^{-1}) = (g_1gg_1^{-1})^2 \in H$ since $g_1gg_1^{-1} \in G$.

6 Group homomorphisms

Page 210: 06
Let $G$ be the group of all polynomials with real coefficients under addition. For each $f$ in $G$, let $f_f$ denote the antiderivative of $f$ that passes through the point $(0, 0)$. Show that the mapping $f \rightarrow f_f$ from $G$ to $G$ is a homomorphism. What is the kernel of this mapping? Is this mapping a homomorphism if $f_f$ denotes the antiderivative of $f$ that passes through $(0, 1)$?

Consider the fact that $f_f$ passes through $(0, 0)$. It represents that antiderivative of a constant term is zero and $\int f_1 + f_2 = \int f_1 + \int f_2$ for $f_1$ and $f_2 \in G$ under addition, (homomorphism). Zero is identity of $G$ under addition and homomorphism transfers identity of $G$ to $\bar{G}$. As stated,know that the constant term and identity of $f_f$ both are zero. So, kernel of the group $\bar{G}$ is 0. But if $f_f$ passes through $(0, 1)$ then it is not homomorphism and this can be verified.
by identity of \( G \).

**Page210:07**

If \( \phi \) is a homomorphism from \( G \) to \( H \) and \( \sigma \) is a homomorphism from \( H \) to \( K \), show that \( \sigma \phi \) is a homomorphism from \( G \) to \( K \).

Let’s say \( p, q \in G \) then we see that \( \sigma(\phi(pq)) = \sigma(\phi(p)\phi(q)) \) since \( \phi \) is homomorphism. Similarly, \( \sigma(\phi(pq)) = \sigma(\phi(p)\phi(q)) = \sigma(\phi(p))\sigma(\phi(q)) \). This \( \phi \sigma \) is also a homomorphism.

**Page210:46**

Suppose that \( Z_{10} \) and \( Z_{15} \) are both homomorphic images of a finite group \( G \). What can be said about \( |G| \)?

Know that \( |G| \) is divisible by 10 and 15 then we can say that 30 is least common multiple of this.

### 7 Introduction to rings

**Page240:17**

Show that a ring that is cyclic under addition is commutative.

**Goal:** \( ab = ba \) note: multiplication denoted by \( ab \) for \( a, b \in R \)

According to the problem, let’s suppose that \( R \) is a cyclic ring under addition. There is a generator \( k \in \mathbb{Z} \) such that any \( a \in R \) and we can write the \( a \) as \( a = \pm(k + k + \cdot \cdot \cdot k) \) for some number(say \( m \) terms) of \( k \)’s, \( a = \pm m \cdot k \)

Suppose \( a, b \in R \) such that \( a = \pm m \cdot k \) and \( b = \pm n \cdot k \).

\[
ab = (\pm m \cdot k)b = \pm \left( \frac{k + k + \cdot \cdot \cdot k}{m \text{ terms}} \right)b = \pm \left( (kb) + (kb) + \cdot \cdot \cdot + (kb) \right) = \pm m \cdot (kb).
\]

and

\[
k b = k(\pm n \cdot k) = \pm k \left( \frac{k + k + \cdot \cdot \cdot k}{n \text{ terms}} \right) = \pm \left( k^2 + k^2 + \cdot \cdot \cdot + k^2 \right) = \pm n \cdot k^2.
\]

we got

\[
ab = \pm m \cdot (kb) = \pm m \cdot (\pm nk^2) = \pm (mn) \cdot k^2,
\]

\[
ba = (\pm n \cdot k)a = \pm n \cdot (ka) = \pm b \cdot (k(\pm m \cdot k)) = \pm n \cdot (m \cdot k^2) = \pm (mn) \cdot k^2.
\]

\( m, n \in \mathbb{Z}, \ mn = nm \), which proves \( ab = ba \)
Show that a unit of a ring divides every element of the ring.

Let $a$ be a unit with $a^{-1}$ and $r \in R$. Then $r = a \cdot a^{-1} \cdot r$ which implies that $a$ divides $r$.

Let $n$ be an integer greater than 1. In a ring in which $x^n = x$ for all $x$, show that $ab = 0$ implies $ba = 0$.

Prove that the mapping $x \to x^6$ from $C^* \to C^*$ is a homomorphism. What is the kernel?

Suppose that $R$ is a ring with unity 1 and $a$ is an element of $R$ such that $a^2 = 1$. Let $S = \{ara | r \in R\}$. Prove that $S$ is a subring of $R$. Does $S$ contain 1?

Let $R$ be a ring. Prove that $a^2 - b^2 = (a + b)(a - b)$ for all $a, b$ in $R$ if and only if $R$ is commutative.

$(\rightarrow)$
\[ a^2 - b^2 = (a + b)(a - b) \]
\[ a^2 - b^2 = (a + b)a - (a + b)b \quad \text{by definition of ring} \]
\[ a^2 - b^2 = a^2 + ba - ab - b^2 \]
\[ a^2 - b^2 - a^2 + b^2 = ba - ab \]
\[ 0 = ba - ab \]
\[ ab = ba \quad \text{Thus, } R \text{ is commutative.} \]

\((\Leftarrow)\) Assume that \( R \) is commutative then

\[ ab = ba \]
\[ a^2 + ab - b^2 = a^2 + ba - b^2 \quad \text{add } a^2, \ b^2 \text{ to both sides} \]
\[ a^2 - b^2 = a^2 - ab + ba - b^2 \quad R \text{ is the ring as we know.} \]
\[ a^2 - b^2 = a(a - b) + b(a - b) \]
\[ a^2 - b^2 = (a + b)(a - b) \]

8 Integral domains

Example8
\( Z \oplus Z \) is not an integral domain.

There are zero divisors. see \((1, 0) \cdot (0, 1) = (0, 0)\).

Page254:05
Show that every nonzero element of \( Z_n \) is a unit or a zero-divisor.

Suppose that \( x \in Z_n \) is not a zero-divisor. Then power\( (x^k \) just say k) of \( x \) is not a zero-divisor, too. if not there is a \( y \in Z_n \) such that \( x^k \cdot y = x \cdot x^{k-1}y = 0 \). \( x \) is turned out to be a zero-divisor.

Invertibility of elements is only that is left to prove. Let’s consider the set of \( \{x^k | k \in Z\} \). Since \( Z_n \) is finite, we think of \( x^k \) and \( x^j \) as \( x^k = x^j \)

\[ x^k = x^j = 0 \]
\[ x^j - x^k = x^k(x^{j-k} - 1) = 0 \]

And we know \( x^k \) is not a zero-divisor, \( x^{j-k} = 1 \) and the equation implies that \( x \cdot x^{j-k-1} = 1 \). Thus, \( x \) has the inverse \( (x^{j-k-1}) \) of \( x \).
Give an example of a commutative ring without zero-divisors that is not an integral domain.

Even integers do.

Let \( a \) belong to a ring \( R \) with unity and suppose that \( a^n = 0 \) for some positive integer \( n \). Prove that \( 1 - a \) has a multiplicative inverse in \( R \).

\[(1 - a)(1 + a + a^2 + \cdots + a^{n-1}) = 1 - a^n = 0\]

Show that the nilpotent elements of a commutative ring form a subring

goal: let \( S \) be the nilpotent elements of a commutative ring \( R \) then, show the \( S \) is under subtraction and multiplication.

Let \( a, b \in S \) and \( a^m = 0, b^n = 0 \) for certain integers (say \( m, n \))

First, we will deal with subtraction

\[(a - b)^{m+n} = \sum_{i=0}^{m+n} M = \binom{m+n}{i} (-1)^i a^{m+n-i} b^i, \quad a^{m+n-i} b^i = 0 \]

for \( 0 \leq i \leq m + n \)

Thus, \( (a - b)^{m+n} = 0 \) that means \( a - b \in S \).

Second, multiplication.

\( (ab)^m = a^m b^m = 0 \cdot b^m = 0 \) that means \( ab \in S \).

Find a zero-divisor in \( \mathbb{Z}_5[i] = \{ a + bi | a, b \in \mathbb{Z}_5 \} \).

\((2 + i)(2 - i) = 4 + 1 = 0\), where \( 2 + i \) and \( 2 - i \) are zero divisors.

Suppose that \( a \) and \( b \) belong to an integral domain.

a. If \( a^5 = b^5 \) and \( a^3 = b^3 \), prove that \( a = b \).

b. If \( a^m = b^m \) and \( a^n = b^n \), where \( m \) and \( n \) are positive integers that are relatively prime, prove that \( a = b \).

a. Say \( b = 0 \), then \( a^3 = 0 \) since no zero divisors. Again, \( a^3 = 0 \) implies that \( a = 0 \) and \( a^2 = 0 \). It turned out that \( a = 0 \) in either case. Thus, \( a = b \)
If $b \neq 0$, $a^3 = b^3 \Rightarrow a^6 = b^6 \Rightarrow aa^5 = b^6 \Rightarrow ab^5 = b^6 \Rightarrow a = b$

a. If $b = 0$, then $a = 0$

b. If $b \neq 0$, Since $m$ and $n$ are relatively prime, there are integers $q$ and $r$ such that $mq + nr = 1$.

$a^m = b^m \rightarrow a^{mq} = b^{mq}$

$a^n = b^n \rightarrow a^{nr} = b^{nr}$

$a^{mq}a^{nr} = b^{mq}b^{nr}$

$a^{mq+nr} = b^{mq+nr}$

$a = b$