# 421 HW 13 Group

## Put names here

**NOTE**: Unless stated otherwise, $G$ is a (multiplicative) group with identity element $e$.

**Problem** (8.2.20)**.**

(a) Let $N$ and $K$ be subgroups of a group $G$. If $N$ is normal in $G$, prove that $NK = \{nk \mid n \in N, k \in K\}$ is a subgroup of $G$. [Compare Exercise 26(b) of Section 7.3.]

(b) If both $N$ and $K$ are normal subgroups of $G$, prove that $NK$ is normal.

**Solution.**

(a)

normality: $\forall n \in N, g \in G \quad gng^{-1} \in N$

To prove: $e_G \in NK$

Since $N$ and $K$ are subgroups of $G$, $e_G \in N$, and $e_G \in K$.

Since $e_G \in N$ and $e_G \in K$, $e_Ge_G \in NK$.

$e_G \in NK$

To prove: $NK$ is closed under inverses

Let $nk \in NK$, where $n \in N$ and $k \in K$.

$N$ and $K$ are both groups, so $n^{-1} \in N$ and $k^{-1} \in K$.

Since $n^{-1} \in N$, $N$ is a normal subgroup of $G$, and $k^{-1} \in G$, $k^{-1}n^{-1}k \in N$.

Since $k^{-1}n^{-1}k \in N$ and $k^{-1} \in K$, $k^{-1}n^{-1}kk^{-1} \in NK$.

Equivalently, $k^{-1}n^{-1} = (nk)^{-1} \in NK$.

$NK$ is closed under inverses.

To prove: $NK$ is closed under multiplication

Let $nk, mj \in NK$, for some $n, m \in N$ and $k, j \in K$.

Since $N$ is normal, $m \in N$, and $k \in K$, $kmk^{-1} \in K$.

$n \in N \quad kmk^{-1} \in N$ $\qquad\qquad$ $k, j \in K$

$\Downarrow$ $\qquad\qquad$ $\Downarrow$

$nkmk^{-1} \in N$ $\qquad\qquad$ $kj \in K$

$$nkmk^{-1}kj \in NK$$

$$nkmj \in NK$$

$$(nk)(mj) \in NK$$

$NK$ is closed under multiplication.

(b)

Let $nk \in NK$, for some $n \in N$ and $k \in K$.

Let $g$ be an arbitrary element of $G$.

Since $N$ and $K$ are normal, $gng^{-1} \in N$ and $gkg^{-1} \in K$.

By the definition of $NK$, $gng^{-1}gkg^{-1} \in NK$.

By inverses, $gnkg^{-1} \in NK$.
$NK$ is normal.

**Problem** (8.3.9)**.** Let $G = \mathbb{Z}_6 \times \mathbb{Z}_2$ and let $N$ be the cyclic subgroup $\langle (1,1) \rangle$. Describe the quotient group $G/N$. [That is, what well-known group $G/N$ isomorphic to?] Justify.

**Solution.** $|G/N| = [G : N] = \frac{|G|}{|N|} = \frac{12}{6} = 2$.
All groups of order 2 are isomorphic to $\mathbb{Z}_2$.
$G/N$ is isomorphic to $\mathbb{Z}_2$.

**Problem** (8.3.25)**.**
(a) Find the order of $\frac{8}{9}$, $\frac{14}{5}$, and $\frac{48}{28}$ in the additive group $\mathbb{Q}/\mathbb{Z}$.
(b) Prove that every element of $\mathbb{Q}/\mathbb{Z}$ has finite order.
(c) Prove that $\mathbb{Q}/\mathbb{Z}$ contains elements of every possible finite order.

**Solution.**
The identity element is $\mathbb{Z}$.
(a)
$|\frac{8}{9}| = 9$, $|\frac{14}{5} = 5$, $|\frac{48}{28}| = |\frac{12}{7}| = 7$.
(b)
Let $\frac{a}{b}$ be an arbitrary element of $\mathbb{Q}/\mathbb{Z}$, for some $a \in \mathbb{Z}$ and $b \in \mathbb{Z}^+$.
$b\frac{a}{b} = a \in \mathbb{Z}$, so $|\frac{a}{b}| \mid b$.
$|\frac{a}{b}| \mid b$, and $b > 0$, so $|\frac{a}{b}| \leq b$
The order of this element is less than a finite integer, and so must be finite.
Since this element was arbitrary, the order of any element is finite.
(c)
Let $b \in \mathbb{Z}^+$.
Consider the element $\frac{1}{b}$.
$b\frac{1}{b} = 1 \in \mathbb{Z}$, so the order of $\frac{1}{b}$ must divide $b$.
For every positive integer $a$ such that $a < b$, $0 < a\frac{1}{b} < 1$.
This means that $a\frac{1}{b}$ is not an integer, so $\frac{1}{b}$ cannot be of order less than $b$.
The only integer which divides $b$ and is not less than $b$ is $b$.
$\frac{1}{b}$ must be of order $b$.
Since $b$ was an arbitrary element of $\mathbb{Z}^+$, for every finite order, there exists an element with that order.

**Problem** (8.4.18)**.** Find all homomorphic images of $D_4$. In other words, if $f : D_4 \to H$ is a surjective homomorphism, then what are all the possibilities for $H$, up to isomorphism? [Hint: First Isomorphism Theorem.]

**Solution.** The First Isomorphism Theorem says that $D_4/\ker f \cong H$.
Since $D_4/\ker f \cong H$, $|D_4/\ker f| = |H|$
Theorem 8.13 says that, since $D_4$ is finite, $|D_4/\ker f| = |D_4|/|\ker f|$.
Since $|H| = |D_4|/|\ker f|$, $|H||\ker f| = |D_4$, so $|H| \mid |D_4|$.
Since $|D_4| = 8$, $H$ can be of order 8, 4, 2, or 1.

Case $|H| = 8$: $H$ and $D_4$ have the same number of elements, so any surjective homomorphism $f$ is also an injection. Since $f$ is a surjection, an injection, and a homomorphism, it is a bijective homomorphism, and therefore an isomorphism. In this case, $H \cong D_4$.

Case $|H| = 4, |\ker f| = 2$: There are two possibilities ($\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$). Setting the kernel of $f$ to $\{r_0, r_2\}$ makes $D_4/\ker f$ isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

By theorem 8.16, the kernel of any $f$ must be a normal subgroup of $D_4$. If the kernel of $f$ contains $r_1$ or $r_3$, it can't even be a group since a group must contain both identity and inverses, and there's just not enough space in a group of order 2. If the kernel of $f$ contains $d$, $h$, $v$, or $t$, then (by checking each case), it isn't a normal subgroup. This excludes $\mathbb{Z}_4$ as a possibility.

Case $|H| = 2$: There is only one possibility, $\mathbb{Z}_2$.

Case $|H| = 1$: The only possibility is $\{e\}$.

**Problem** (8.4.26)**.** Prove that $(\mathbb{Z}\times\mathbb{Z})/\langle(2,2)\rangle \cong \mathbb{Z}\times\mathbb{Z}_2$. [Hint: Show that $f : \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}\times\mathbb{Z}_2$, given by $f((a,b)) = (a-b, [b]_2)$, is a surjective homomorphism.]

**Solution.**

Let $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}_2$ be defined as $f((a,b)) = (a-b, [b]_2)$.

To prove: $f$ is surjective

Let $(c,d)$ be an arbitrary element of $\mathbb{Z} \times \mathbb{Z}_2$.

Let $b$ be 0 if $d = [0]$, or 1 if $d = [1]$.

Let $a$ be $c + d$.

$(a,b)$ is an element of $\mathbb{Z} \times \mathbb{Z}$, and $f((a,b)) = (c,d)$.

Since $(c,d)$ was arbitrary, every element in $\mathbb{Z} \times \mathbb{Z}_2$ has a preimage.

$f$ is surjective.

To prove: $f$ is a homomorphism.

Let $(a,b)$ and $(c,d)$ be arbitrary elements of $\mathbb{Z} \times \mathbb{Z}$.

To check homomorphism of addition:

$$\begin{array}{c|c} f((a,b)) + f((c,d)) & f((a,b) + (c,d)) \\ (a, [b]_2) + (c, [d]_2) & f((a+c, b+d)) \\ (a+c, [b]_2 + [d]_2) & (a+c, [b+d]_2) \end{array}$$

To check whether $[b]_2 + [d]_2 = [b+d]_2$, see 4 cases:

| $b$ | $d$ | $[b+d]_2$ | $[b]_2 + [d]_2$ |
|---|---|---|---|
| even | even | 0 | 0 |
| even | odd | 1 | 1 |
| odd | even | 1 | 1 |
| odd | odd | 0 | 0 |

It is always that $[b]_2 + [d]_2 = [b+d]_2$.

Thus, $(a+c, [b]_2 + [d]_2) = (a+c, [b+d]_2)$,

and $f((a,b) + (c,d)) = f((a,b)) + f((c,d))$.

$f$ is homomorphic under addition.

It is now established that $f$ is a surjective homomorphism.

The kernel of $f$ is all $(a,b)$ for which $a - b = 0$ and $[b]_2 = 0$ - that is, $a = b$ and $b$ is even.

This is the subgroup of $\mathbb{Z} \times \mathbb{Z}$ which is generated by $(2,2)$.

The first isomorphism states that, given groups $G$ and $H$, and a surjective homomorphism $f : G \to H$, $G/\ker f \cong H$.

By the first isomorphism, with $G = \mathbb{Z} \times \mathbb{Z}$ and $H = \mathbb{Z} \times \mathbb{Z}_2$, $\mathbb{Z} \times \mathbb{Z}/\langle(2, 2)\rangle \cong \mathbb{Z} \times \mathbb{Z}_2$.

**Problem** (3.3.16)**.** Let $T$, $R$, and $F$ be the four-element rings whose tables are given in Example 5 of Section 3.1 and in Exercises 2 and 3 of Section 3.1. Show that no two of these rings are isomorphic.

For convenience, here are their operation tables:

$T = \{z, r, s, t\}$

| $+$ | $z$ | $r$ | $s$ | $t$ |
|---|---|---|---|---|
| $z$ | $z$ | $r$ | $s$ | $t$ |
| $r$ | $r$ | $z$ | $t$ | $s$ |
| $s$ | $s$ | $t$ | $z$ | $r$ |
| $t$ | $t$ | $s$ | $r$ | $z$ |

| $\cdot$ | $z$ | $r$ | $s$ | $t$ |
|---|---|---|---|---|
| $z$ | $z$ | $z$ | $z$ | $z$ |
| $r$ | $z$ | $z$ | $r$ | $r$ |
| $s$ | $z$ | $z$ | $s$ | $s$ |
| $t$ | $z$ | $z$ | $t$ | $t$ |

$R = \{0, e, b, c\}$

| $+$ | $0$ | $e$ | $b$ | $c$ |
|---|---|---|---|---|
| $0$ | $0$ | $e$ | $b$ | $c$ |
| $e$ | $e$ | $0$ | $c$ | $b$ |
| $b$ | $b$ | $c$ | $0$ | $e$ |
| $c$ | $c$ | $b$ | $e$ | $0$ |

| $\cdot$ | $0$ | $e$ | $b$ | $c$ |
|---|---|---|---|---|
| $0$ | $0$ | $0$ | $0$ | $0$ |
| $e$ | $0$ | $e$ | $b$ | $c$ |
| $b$ | $0$ | $b$ | $b$ | $0$ |
| $c$ | $0$ | $c$ | $0$ | $c$ |

$F = \{0, e, a, b\}$

| $+$ | $0$ | $e$ | $a$ | $b$ |
|---|---|---|---|---|
| $0$ | $0$ | $e$ | $a$ | $b$ |
| $e$ | $e$ | $0$ | $b$ | $a$ |
| $a$ | $a$ | $b$ | $0$ | $e$ |
| $b$ | $b$ | $a$ | $e$ | $0$ |

| $\cdot$ | $0$ | $e$ | $a$ | $b$ |
|---|---|---|---|---|
| $0$ | $0$ | $0$ | $0$ | $0$ |
| $e$ | $0$ | $e$ | $a$ | $b$ |
| $a$ | $0$ | $a$ | $b$ | $e$ |
| $b$ | $0$ | $b$ | $e$ | $a$ |

**Solution.** They are all isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ under addition, so that cannot be used as a basis for finding differences.

$(T, \cdot)$ has an element of order 2 (specifically, $r$), but $R$ and $F$ do not. $T$ cannot be isomorphic to $R$ or $F$.

In $R$, there exist two nonzero elements which multiply to be the additive identity. This does not happen in $F$, so these cannot be isomorphic.

**Problem** (3.3.34)**.** If $f : R \to S$ is an isomomorphism of rings, which of the following properties are preserved by this isomorphism? Justify your answers.

(a) $a \in R$ is a zero divisor.

(b) $a \in R$ is idempotent. (That is, $a^2 = a$.)

(c) $R$ is an integral domain.

**Solution.**

(a) Yes.

By theorem 3.10.1, $f(0_R) = 0_S$.

Lemma: if $b \in R \neq 0_R$, then $f(b) \neq 0_S$.

Since $f$ is an isomorphism, $f$ is a bijection, $f$ is an injection, and every element of $S$ has at most one preimage.

The preimage of $0_S$ is $0_R$ by theorem 3.10.1, so no element of $R$ but $0_R$ can map to $0_S$.

If $a \in R$ is a zero divisor, then

$$\exists b \in R \quad b \neq 0 \text{ and } (ab = 0_R) \text{ or } ba = 0_R)$$

$$\begin{array}{r|l} \text{case } ab = 0_R & \text{case } ba = 0_R \\ f(a)f(b) = 0_S & f(b)f(a) = 0_S \end{array}$$

In either case, $f(b) \neq 0_S$ by the lemma a few words ago, so $f(a)$ is a zero divisor.

(b) Yes.

$$a^2 = a$$
$$aa = a$$
$$f(a)f(a) = f(a)$$

(c) Yes.

Integral domains

- are commutative
- have multiplicative identity (which is not equal to additive identity)
- $ab = 0 \Rightarrow (a = 0 \text{ or } b = 0)$

For commutativity, let $f(a), f(b)$ be any elements of $S$ (which is possible because $f$ is an isomorphism):

$$ab = ba$$
$$f(a)f(b) = f(b)f(a)$$

For multiplicative identity, $R$ has an element $1_R$ such that $\forall r \in R \quad r1_R = 1_R r = r$. If $f$ is applied, this implies that $S$ has an element $f(1_R)$ such that $\forall f(r) \in S \quad f(r)f(1_R) = f(1_R)f(r) = f(r)$.

Let $f(a), f(b) \in S$ such that $cd = 0$.

$$f(a)f(b) = 0_S$$
$$f(ab) = 0_S$$
$$ab = 0_R$$
$$a = 0_R \text{ or } b = 0_R$$
$$f(a) = 0_S \text{ or } f(b) = 0_S$$

If $R$ has this property, then $S$ has this property.

If $R$ is an integral domain, then $S$ is an integral domain.

**Problem** (3.3.38)**.** Let $F$ be a field and $f : F \to R$ a homomorphism of rings.

(a) If there is a nonzero element $c$ of $F$ such that $f(c) = 0_R$, prove that $f$ is the zero homorphism (that is, $f(x) = 0_R$ for every $x \in F$). [Hint: $c^{-1}$ exists (Why?). If $x \in F$, consider $f(xcc^{-1})$.]

(b) Prove that $f$ is either injective or the zero homomorphism. [Hint: If $f$ is not the zero homomorphism and $f(a) = f(b)$, then $f(a - b) = 0_R$.]

**Solution.**

(a)

Let $c$ be a nonzero element of $F$ (which exists since $F$ is a field).

Since $F$ is a field, $c \in F$, and $c$ is nonzero, $c^{-1}$ exists.

Let $x \in F$. Since $f$ is a homomorphism, $f(xcc^{-1}) = f(x)f(c)f(c^{-1})$.

$$\begin{aligned} f(x) &= f(xcc^{-1}) && = f(x)f(c)f(c^{-1}) \\ &= f(x)0_R f(c^{-1}) \\ &= 0_R \end{aligned}$$

Since $x$ was an arbitrary element of $F$, this must be true for all elements of $F$.

Thus, $f$ is the zero homomorphism.

(b)

Two cases:

Case $f$ is injective: $f$ is injective.

Case $f$ is not injective:

Let $a, b \in F$ such that $f(a) = f(b)$.

Since $f$ is a homomorphism, $f(a - b) = 0_R$.

If $a - b = 0_F$, then $a = b$. This is a contradiction.

If $a - b \neq 0_F$, then, by part (a), $f$ is the zero homomorphism.

Thus, if $f$ is not injective, it is the zero homomorphism.

$f$ is either injective or the zero homomorphism.

**Problem** (3.3.42)**.** If $(m, n) \neq 1$, prove that $\mathbb{Z}_{mn}$ is not isomorphic to $\mathbb{Z}_m \times \mathbb{Z}_n$.

**Solution.**