Math 345
4-24-2018

Review Session for Test 3

Example. How many cosets does $\langle(4,6)\rangle$ have in the group $\mathbb{Z}_{12} \times \mathbb{Z}_{12}$?

The order of $(4,6)$ in $\mathbb{Z}_{12} \times \mathbb{Z}_{12}$ is 6. Thus, $|\langle(4,6)\rangle| = 6$. Since $|\mathbb{Z}_{12} \times \mathbb{Z}_{12}| = 144$, there are $\dfrac{144}{6} = 24$ cosets. □

Example. (a) How many cosets does the subgroup $\langle 3\rangle$ have in the group $\mathbb{Z}_{720}$?

$$\langle 3\rangle = \{0, 3, 6, 9, \ldots, 717\}.$$

Since $\dfrac{720}{3} = 240$, this subgroup has 240 elements. By Lagrange's theorem, the subgroup has $\dfrac{720}{240} = 3$ cosets. □

(b) How many cosets does the subgroup $\langle 110\rangle$ have in the group $\mathbb{Z}_{160}$?

This time, I'll use a formula to figure out the order of $\langle 110\rangle$. 110 has order $\dfrac{160}{(110, 160)} = \dfrac{160}{10} = 16$ in $\mathbb{Z}_{160}$. This means that $\langle 110\rangle$ has order 16. Hence, $\langle 110\rangle$ has $\dfrac{160}{16} = 10$ cosets. □

Example. (a) Let G and H be groups. Let

$$G \times \{1\} = \{(g, 1) \mid g \in G\}.$$

Prove that $G \times \{1\}$ is a normal subgroup of $G \times H$.

$G \times \{1\}$ is the subset of $G \times H$ consisting of elements which have the identity (of H) as their second component.

First, I'll show that it's a subgroup.

$G \times \{1\}$ is closed under multiplication: If $(g_1, 1), (g_2, 1) \in G \times \{1\}$, then

$$(g_1, 1)(g_2, 1) = (g_1 g_2, 1) \in G \times \{1\}.$$

The identity element of $G \times H$ is $(1, 1)$, and $(1, 1)$ is an element of $G \times \{1\}$.

Finally, if $(g, 1) \in G \times \{1\}$, its inverse is

$$(g, 1)^{-1} = (g^{-1}, 1) \in G \times \{1\}.$$

Therefore, $G \times \{1\}$ is a subgroup of $G \times H$.

To show that it's a normal subgroup, take $(x, 1) \in G \times \{1\}$ and $(g, h) \in G \times H$. Then

$$(g, h)(x, 1)(g, h)^{-1} = (g, h)(x, 1)((g^{-1}, h^{-1}) = (g \cdot x \cdot g^{-1}, h \cdot 1 \cdot h^{-1}) = (g \cdot x \cdot g^{-1}, 1) \in G \times \{1\}.$$

This proves that $G \times \{1\}$ is a normal subgroup of $G \times H$. □

(b) Prove that $\dfrac{G \times H}{G \times \{1\}} \approx H$.

Define $\phi : G \times H \to H$ by

$$\phi(g, h) = h.$$

I have

$$\phi[(g_1,h_1)(g_2,h_2)] = \phi(g_1g_2, h_1h_2) = h_1h_2 \quad \text{and} \quad \phi(g_1,h_1)\phi(g_2,h_2)] = h_1h_2.$$

Hence, ϕ is a group map.
If $(g,1) \in G \times \{1\}$, then

$$\phi(g,1) = 1.$$

Hence, $G \times \{1\} \subset \ker\phi$.
If $(g,h) \in \ker\phi$, then

$$\begin{aligned} \phi(g,h) &= 1 \\ h &= 1 \\ (g,h) &= (g,1) \end{aligned}$$

Thus, $(g,h) = (g,1) \in G \times \{1\}$, so $\ker\phi \subset G \times \{1\}$.
Therefore, $G \times \{1\} = \ker\phi$.
Let $h \in H$. Then

$$\phi(1,h) = h.$$

This shows that $\operatorname{im}\phi = H$.
By the First Isomorphism Theorem,

$$\frac{G}{G \times \{1\}} = \frac{G}{\ker\phi} \approx \operatorname{im}\phi = H. \quad \square$$

Note: In this part I showed that $G \times \{1\} = \ker\phi$. Since kernels of group maps are normal subgroups, this gives another proof of (a).

Example. (a) List the cosets of $\langle 6\rangle$ in $\mathbb{Z}_{12}$. For each coset, list the elements of the coset.

Since $\langle 6\rangle = \{0,6\}$ has two elements, there are $\dfrac{12}{2} = 6$ cosets. They are

$$\{0,6\}, \quad 1+\{0,6\} = \{1,7\}, \quad 2+\{0,6\} = \{2,8\}, \quad 3+\{0,6\} = \{3,9\}, \quad 4+\{0,6\} = \{4,10\},$$

$$5+\{0,6\} = \{5,11\}. \quad \square$$

(b) Construct an addition table for the quotient group $\dfrac{\mathbb{Z}_{12}}{\langle 6\rangle}$.

$+$	$\{0,6\}$	$\{1,7\}$	$\{2,8\}$	$\{3,9\}$	$\{4,10\}$	$\{5,11\}$
$\{0,6\}$	$\{0,6\}$	$\{1,7\}$	$\{2,8\}$	$\{3,9\}$	$\{4,10\}$	$\{5,11\}$
$\{1,7\}$	$\{1,7\}$	$\{2,8\}$	$\{3,9\}$	$\{4,10\}$	$\{5,11\}$	$\{0,6\}$
$\{2,8\}$	$\{2,8\}$	$\{3,9\}$	$\{4,10\}$	$\{5,11\}$	$\{0,6\}$	$\{1,7\}$
$\{3,9\}$	$\{3,9\}$	$\{4,10\}$	$\{5,11\}$	$\{0,6\}$	$\{1,7\}$	$\{2,8\}$
$\{4,10\}$	$\{4,10\}$	$\{5,11\}$	$\{0,6\}$	$\{1,7\}$	$\{2,8\}$	$\{3,9\}$
$\{5,11\}$	$\{5,11\}$	$\{0,6\}$	$\{1,7\}$	$\{2,8\}$	$\{3,9\}$	$\{4,10\}$

For example, to do $\{3,9\} + \{2,8\}$, I take representatives $3 \in \{3,9\}$ and $2 \in \{2,8\}$. I add the representatives: $3 + 2 = 5$. (If the sum is 12 or greater, I have to reduce mod 12.) Then 5 is in $\{5,11\}$, so $\{3,9\} + \{2,8\} = \{5,11\}$. $\square$

(c) What is the order of $\{4,10\}$ in the quotient group $\dfrac{\mathbb{Z}_{12}}{\langle 6\rangle}$?

The identity element in the quotient group is the original subgroup $\{0, 6\}$. What is the smallest multiple of $\{4, 10\}$ which gives $\{0, 6\}$?

$$\{4, 10\} + \{4, 10\} = \{2, 8\}, \quad \{4, 10\} + \{4, 10\} + \{4, 10\} = \{0, 6\}.$$

The smallest multiple is 3, so $\{4, 10\}$ has order 3. □

Example. (a) List the elements of the cosets of $\langle 33 \rangle$ in U_{34}.

$$U_{34} = \{1, 3, 5, 7, 9, 11, 13, 15, 19, 21, 23, 25, 27, 29, 31, 33\}.$$

The cosets are

$$\begin{aligned} \langle 33 \rangle &= \{1, 33\} \\ 3 \cdot \langle 33 \rangle &= \{3, 31\} \\ 5 \cdot \langle 33 \rangle &= \{5, 29\} \\ 7 \cdot \langle 33 \rangle &= \{7, 27\} \\ 9 \cdot \langle 33 \rangle &= \{9, 25\} \\ 11 \cdot \langle 33 \rangle &= \{11, 23\} \\ 13 \cdot \langle 33 \rangle &= \{13, 21\} \\ 15 \cdot \langle 33 \rangle &= \{15, 19\} \quad \square \end{aligned}$$

(b) Find the prinary decomposition for the quotient group $\dfrac{U_{34}}{\langle 33 \rangle}$.

The quotient group is an abelian group of order 8. Therefore, it could be $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, or $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. I'll try to figure out the orders of the cosets — they could have order 1, 2, 4, or 8.

I have

$$\{3, 31\}^2 = \{9, 25\}, \quad \{9, 25\}^2 = \{13, 21\}, \quad \{13, 21\}^2 = \{1, 33\}.$$

It follows that $\{3, 31\}$ has order 8. Therefore, it generates the quotient group, and the quotient group is cyclic of order 8. In other words,

$$\frac{U_{34}}{\langle 33 \rangle} \approx \mathbb{Z}_8. \quad \square$$

Example. Let H be the subgroup of $\mathbb{R}^3$ defined by

$$H = \{(a, 2a, a) \mid a \in \mathbb{R}\}.$$

Use the First Isomorphism Theorem to prove that

$$\frac{\mathbb{R}^3}{H} \approx \mathbb{R}^2.$$

Define $f : \mathbb{R} \times \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$ by

$$f(x, y, z) = (2x - y, y - 2z).$$

Note that

$$f\left(\begin{bmatrix} x \\ y \\ z \end{bmatrix}\right) = \begin{bmatrix} 2 & -1 & 0 \\ 0 & 1 & -2 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix}.$$

Since f can be defined by matrix multiplication, it's a linear transformation, so it's a group map.

Let $(a, 2a, a) \in H$. Then

$$f(a, 2a, a) = (2a - 2a, 2a - 2a) = (0, 0).$$

Therefore, $H \subset \ker f$.
Let $(x, y, z) \in \ker f$. Then

$$f(x, y, z) = (0, 0)$$
$$(2x - y, y - 2z) = (0, 0)$$

This gives $2x - y = 0$ and $y - 2z = 0$.
The first equation gives $y = 2x$. Plugging this into the second equation gives $2x - 2z = 0$, so $z = x$. Therefore,

$$(x, y, z) = (x, 2x, x) \in H.$$

Thus, $\ker f \subset H$. Hence, $\ker f = H$.
Let $(p, q) \in \mathbb{R}^2$. Then

$$f\left(\frac{1}{2}p, 0, -\frac{1}{2}q\right) = \left(2 \cdot \frac{1}{2}p - 0, 0 - 2 \cdot \left(-\frac{1}{2}q\right)\right) = (p, q).$$

This proves that $\operatorname{im} f = \mathbb{R}^2$.
Thus,

$$\frac{\mathbb{R}^3}{H} = \frac{\mathbb{R}^3}{\ker f} \approx \operatorname{im} f = \mathbb{R}^2. \quad \square$$

Example. Give examples *other than the multiplicative identity* of units in $\mathbb{Z}$, in $\mathbb{Z}_6$, and in $M(2, \mathbb{R})$.

-1 is a unit in $\mathbb{Z}$, since $(-1)(-1) = 1$.
5 is a unit in $\mathbb{Z}_6$, since $5 \cdot 5 = 1$ in $\mathbb{Z}_6$.
The matrix

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

is a unit in $M(2, \mathbb{R})$. In fact,

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \quad \square$$

Example. The ring $\mathbb{Z}_2[i]$ consists of elements of the form $a + bi$, where $a, b \in \mathbb{Z}_2$. Addition and multiplication are defined by

$$(a + bi) + (c + di) = (a + c) + (b + d)i,$$

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

The terms $a + c$, $b + d$, $ac - bd$, and $ad + bc$ are all evaluated in $\mathbb{Z}_2$.

(a) What is i^2?

$$(0 + 1 \cdot i)(0 + 1 \cdot i) = (0 + 1) + (0 + 0)i = 1. \quad \square$$

(b) How many elements are there in $\mathbb{Z}_2[i]$?

In $a + bi$ there are two choices for each of a and b, so there are four elements. $\square$

(c) Construct addition and multiplication tables for $\mathbb{Z}_2[i]$.

$+$	0	1	i	$1+i$
0	0	1	i	$1+i$
1	1	0	$1+i$	i
i	i	$1+i$	0	1
$1+i$	$1+i$	i	1	0

$*$	0	1	i	$1+i$
0	0	0	0	0
1	0	1	i	$1+i$
i	0	i	1	$1+i$
$1+i$	0	$1+i$	$1+i$	0	□

(d) Is $\mathbb{Z}_2[i]$ an integral domain? Why or why not?

$\mathbb{Z}_2[i]$ is a commutative ring with 1. However, $(1+i)(1+i) = 0$, so $1+i$ is a zero divisor. Therefore, $\mathbb{Z}_2[i]$ is not an integral domain. □

Example. (a) Is $(2,3)$ a zero divisor in $\mathbb{Z}_4 \times \mathbb{Z}_9$?

Since $(2,3)(2,3) = (0,0)$, $(2,3)$ is a zero divisor in $\mathbb{Z}_4 \times \mathbb{Z}_9$. □

(b) Show that $(3,8)$ is a unit in $\mathbb{Z}_4 \times \mathbb{Z}_9$.

$$(3,8)(3,8) = (1,1),$$

$(3,8)$ is a unit in $\mathbb{Z}_4 \times \mathbb{Z}_9$. □

Example. Give an example of a noncommutative ring. Show using specific elements that the ring is not commutative.

Consider $M(2,\mathbb{R})$, the ring of 2×2 matrices with real entries.

$$\begin{bmatrix} 1 & 2 \\ -2 & 1 \end{bmatrix}\begin{bmatrix} 3 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 5 & 2 \\ -5 & 1 \end{bmatrix} \quad \text{but} \quad \begin{bmatrix} 3 & 0 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ -2 & 1 \end{bmatrix} = \begin{bmatrix} 3 & 6 \\ -1 & 3 \end{bmatrix},$$

$M(2,\mathbb{R})$ is not commutative. □

Example. Is $M(2,\mathbb{R})$ a division ring? Why or why not?

$M(2,\mathbb{R})$ has a multiplicative identity, namely

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

However, it's not a division ring, since not every nonzero element is invertible. For example,

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

is a nonzero matrix which is not invertible. □

Example. $M(2,\mathbb{R})$ is the ring of 2×2 matrices with real entries. Let

$$S = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \;\middle|\; a, b, d \in \mathbb{R} \right\}.$$

Prove that S is a subring, but that S is not an ideal.

Obviously,

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in S.$$

Also,

$$-\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} = \begin{bmatrix} -a & -b \\ 0 & -d \end{bmatrix} \in S.$$

S is closed under addition:

$$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} + \begin{bmatrix} x & y \\ 0 & z \end{bmatrix} = \begin{bmatrix} a+x & b+y \\ 0 & d+z \end{bmatrix} \in S.$$

S is closed under multiplication:

$$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \begin{bmatrix} x & y \\ 0 & z \end{bmatrix} = \begin{bmatrix} ax & ay+bz \\ 0 & dz \end{bmatrix} \in S.$$

Therefore, S is a subring.
However, take

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in S \quad \text{and} \quad \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \in M(2,\mathbb{R}).$$

Then

$$\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 1 & 2 \end{bmatrix} \notin S.$$

Therefore, S is not an ideal. □

Example. If R is a commutative ring, an element $r \in R$ is **nilpotent** if $r^n = 0$ for some positive integer n.

(a) Show that if R is a commutative ring with nonzero nilpotent elements, then R cannot be an integral domain.

Let $r \in R$ be a nonzero nilpotent element. Then $r^n = 0$ for some positive integer n. Let m be the *smallest* positive integer with this property, so $r^m = 0$ but no smaller power of r is 0. Note that $m > 1$, since $r \neq 0$.

Write

$$0 = r^m = r \cdot r^{m-1}.$$

r and r^{m-1} are nonzero, by the choice of m. Therefore, r and r^{m-1} are zero divisors, and R can't be an integral domain. □

(b) Prove that if R is a commutative ring, the set of nilpotent elements forms an ideal of R.

Let N be the set of nilpotent elements in R.
Since $0^1 = 0$, $0 \in N$.

Suppose $r \in N$, so $r^n = 0$ for some positive integer n. Then

$$(-r)^n = \pm r^n = \pm 0 = 0.$$

Hence, $-r \in N$.
Suppose $r, s \in N$. Say $r^m = 0$ and $s^n = 0$ for positive integers m and n. By the Binomial Theorem,

$$(r+s)^{m+n} = \sum_{k=0}^{m+n} \binom{m+n}{k} r^k s^{m+n-k}.$$

Consider a term $r^k s^{m+n-k}$. If $k \geq m$, then $r^k = 0$ and the term is 0. If $k < m$, then $m + n - k > n$, and $s^{m+n-k} = 0$, and again the term is 0. So all the terms are 0, and

$$(r+s)^{m+n} = 0.$$

Therefore, $r + s \in N$.
Let $s \in N$ and let $r \in R$. Say $s^n = 0$ for $n \in \mathbb{Z}^+$. Then

$$(rs)^n = r^n \cdot s^n = r^n \cdot 0 = 0.$$

Therefore, $rs \in N$.
Hence, N is an ideal. □

(c) Give an example of a nonzero nilpotent element in $\mathbb{Z}_{12}$. Give an example of a nonzero nilpotent element in $M(2, \mathbb{R})$.

In $\mathbb{Z}_{12}$, $6^2 = 0$, so 6 is nilpotent.
In $M(2, \mathbb{R})$,

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

Hence, $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ is nilpotent. □

Example. Define $f : \mathbb{R}^2 \to M(2, \mathbb{R})$ by

$$f(x, y) = \begin{bmatrix} x & 0 \\ 0 & xy \end{bmatrix}.$$

Check each axiom for a ring map. If the axiom holds, prove it. If the axiom doesn't hold, give a specific counterexample.

The multiplicative identity of $\mathbb{R}^2$ is $(1, 1)$, and

$$f(1, 1) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

The identity axiom holds.
The addition axiom does not hold.

$$f[(1,2) + (3,4)] = f(4,6) = \begin{bmatrix} 4 & 0 \\ 0 & 24 \end{bmatrix}, \quad \text{but} \quad f(1,2) + f(3,4) = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} + \begin{bmatrix} 3 & 0 \\ 0 & 12 \end{bmatrix} = \begin{bmatrix} 4 & 0 \\ 0 & 14 \end{bmatrix}.$$

The multiplication axiom holds:

$$f[(a,b) \cdot (c,d)] = f(ac, bd) = \begin{bmatrix} ac & 0 \\ 0 & abcd \end{bmatrix} \quad \text{and} \quad f(a,b) \cdot f(c,d) = \begin{bmatrix} a & 0 \\ 0 & ab \end{bmatrix} \cdot \begin{bmatrix} c & 0 \\ 0 & cd \end{bmatrix} = \begin{bmatrix} ac & 0 \\ 0 & abcd \end{bmatrix}. \quad \square$$
