5-10-2018

Review Session for the Final

Example. (a) Solve the equation $27x = 10 \pmod{42}$, or prove that it has no solution.

If $27x = 10 \pmod{42}$, then for some $y \in \mathbb{Z}$,

$$27x + 42y = 10.$$

Now $3 \mid 27x + 42y$, but $3 \nmid 10$.
This contradiction shows that there are no solutions. □

(b) Solve the equation $27x = 6 \pmod{42}$, or prove that it has no solution.

$27x = 6 \pmod{42}$ means that $27x$ and 6 differ by a multiple of 42:

$$27x + 42y = 6, \quad \text{or} \quad 9x + 14y = 2.$$

The last equation is equivalent to $9x = 2 \pmod{14}$. I can solve this congruence by finding the reciprocal of 9 mod 14 using the Extended Euclidean algorithm:

14	-	3
9	1	2
5	1	1
4	1	1
1	4	0

Thus,

$$(2)(14) + (-3)(9) = 1, \quad \text{so} \quad (11)(9) = 1 \pmod{14}.$$

Multiply $9x = 2 \pmod{14}$ by 11:

$$x = 22 = 8 \pmod{14}.$$

My original congruence was an equation mod 42, so I find all the numbers in the range $0, 1, \ldots, 41$ which satisfy $x = 8 \pmod{14}$. They are 8, 22, and 36. These are solutions to the original equation. □

(c) Solve the equation $25x = 6 \pmod{42}$, or prove that it has no solution.

Use the Extended Euclidean algorithm:

42	-	5
25	1	3
17	1	2
8	2	1
1	8	0

The table shows that

$$(3)(42) + (-5)(25) = 1, \quad \text{or} \quad (37)(25) = 1 \pmod{42}.$$

Multiply $25x = 6 \pmod{42}$ by 37:

$$x = 222 = 12 \pmod{42}. \quad \square$$

Example. Consider the following subset of the ring $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$:

$$R = \{(a, b, c) \mid a = b + c\}.$$

Is R a subring of $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$? Is it an ideal?

$(0, 0, 0) \in R$, since $0 = 0 + 0$.
If $(a, b, c) \in R$, then $a = b + c$. Hence, $-a = (-b) + (-c)$, so

$$-(a, b, c) = (-a, -b, -c) \in R.$$

Suppose $(a, b, c), (d, e, f) \in R$. Then

$$a = b + c \quad \text{and} \quad d = e + f, \quad \text{so} \quad a + d = (b + e) + (c + f).$$

Hence,

$$(a, b, c) + (d, e, f) = (a + d, b + e, c + f) \in R.$$

However, $(3, 1, 2) \in R$ (since $3 = 1 + 2$) and $(4, 1, 3) \in R$ (since $4 = 1 + 3$), but

$$(3, 1, 2)(4, 1, 3) = (12, 1, 6) \notin R.$$

(This is true since $12 \neq 1 + 6$.) Therefore, R is not closed under products, and hence R is not a subring. Therefore, it's also not an ideal. □

Example. Let R be a commutative ring and let $u, x \in R$. Suppose u is a unit and $x^2 = 0$. Prove that $u + x$ is a unit.

I have to guess a multiplicative inverse of $u + x$. To do this, I'll do the following formal computation using geometric series.

$$\frac{1}{u + x} = \frac{1}{u} \frac{1}{1 + u^{-1}x} = u^{-1} \left(1 - u^{-1}x + u^{-2}x^2 - u^{-3}x^3 + \cdots\right) = u^{-1}(1 - u^{-1}x) = u^{-1} - u^{-2}x.$$

The next to the last step used $x^2 = 0$. So I will guess that $(u + x)^{-1} = u^{-1} - u^{-2}x$, and I'll check by computation that this works:

$$(u + x)(u^{-1} - u^{-2}x) = 1 + u^{-1}x - u^{-1}x - u^{-2}x^2 = 1,$$

$$(u^{-1} - u^{-2}x)(u + x) = 1 - u^{-1}x + u^{-1}x - u^{-2}x^2 = 1.$$

In both equations, I used $x^2 = 0$ again.
Thus, $u + x$ is a unit, and its inverse is $u^{-1} - u^{-2}x$. □

Example. Consider the following subset of the group $\mathbb{Z} \times \mathbb{Z}$:

$$H = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid 9x = 5y\}.$$

Prove that $\dfrac{\mathbb{Z} \times \mathbb{Z}}{H} \approx \mathbb{Z}$.

Define $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ by

$$\phi(x, y) = 9x - 5y.$$

I have

$$\phi\left[(a,b)+(c,d)\right]=\phi(a+c,b+d)=9(a+c)-5(b+d)=(9a-5b)+(9c-5d)=\phi(a,b)+\phi(c,d).$$

Therefore, ϕ is a group homomorphism.
Let $(x,y)\in H$, so $9x=5y$. Then

$$\phi(x,y)=9x-5y=0.$$

Hence, $(x,y)\in\ker\phi$.
Let $(x,y)\in\ker\phi$. Then $\phi(x,y)=0$, so $9x-5y=0$, and $9x=5y$. Therefore, $(x,y)\in H$.
Therefore, $H=\ker\phi$.
Next, I'll show that ϕ is surjective. Let $z\in\mathbb{Z}$. I must find (x,y) such that $\phi(x,y)=z$.
Note that

$$\phi(-z,-2z)=9(-z)-5(-2z)=z.$$

Therefore, ϕ is surjective.
By the First Isomorphism Theorem,

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

Example. Prove or disprove: $(8,3)$ is a zero divisor in $\mathbb{Z}_{12}\times\mathbb{Z}$.

$$(8,3)\cdot(3,0)=(0,0).$$

Hence, $(8,3)$ is a zero divisor in $\mathbb{Z}_{12}\times\mathbb{Z}$. $\square$

Example. Consider the quotient ring $\dfrac{\mathbb{Z}_7[x]}{\langle x^2+5\rangle}$.

(a) Is x^2+5 irreducible over $\mathbb{Z}_7$?

x	0	1	2	3	4	5	6
x^2+5	5	6	2	0	0	2	6

The table shows that $x=3$ and $x=4$ are roots. Therefore,

$$x^2+5=(x-3)(x-4)=(x+4)(x+3).\quad\square$$

(b) Find a pair of zero divisors in $\dfrac{\mathbb{Z}_7[x]}{\langle x^2+5\rangle}$.

$$\left[(x+4)+\langle x^2+5\rangle\right]\left[(x+3)+\langle x^2+5\rangle\right]=x^2+5+\langle x^2+5\rangle=\langle x^2+5\rangle.$$

$\langle x^2+5\rangle$ is the zero element in the quotient ring. $(x+4)+\langle x^2+5\rangle$ and $(x+3)+\langle x^2+5\rangle$ are nonzero, because $x+4$ and $x+3$ aren't divisible by x^2+5. Therefore, $(x+4)+\langle x^2+5\rangle$ and $(x+3)+\langle x^2+5\rangle$ are zero divisors. $\square$

(c) Write the product

$$\left[(5x+2)+\langle x^2+5\rangle\right]\left[(2x^3+1)+\langle x^2+5\rangle\right]$$

in the form $(ax+b)+\langle x^2+5\rangle$, where $a,b\in\mathbb{Z}_7$.

$$\left[(5x+2)+\langle x^2+5\rangle\right]\left[(2x^3+1)+\langle x^2+5\rangle\right]=(5x+2)(2x^3+1)+\langle x^2+5\rangle=(3x^4+4x^3+5x+2)+\langle x^2+5\rangle.$$

Next, divide $3x^4 + 4x^3 + 5x + 2$ by $x^2 + 5$:

$$3x^4 + 4x^3 + 5x + 2 = (x^2 + 5)(3x^2 + 4x + 6) + 6x.$$

Thus,

$$3x^4 + 4x^3 + 5x + 2 = 6x \pmod{x^2 + 5}.$$

Hence,

$$\left[(5x + 2) + \langle x^2 + 5\rangle\right]\left[(2x^3 + 1) + \langle x^2 + 5\rangle\right] = 6x + \langle x^2 + 5\rangle. \quad \square$$

(d) How many elements are there in the quotient ring $\dfrac{\mathbb{Z}_7[x]}{\langle x^2 + 5\rangle}$?

Any coset $p(x) + \langle x^2 + 5\rangle$ can be written in the form $(ax + b) + \langle x^2 + 5\rangle$, $a, b \in \mathbb{Z}_7$, by using the Division Algorithm as in part (c). Since there are 7 choices for each of a and b, there are 49 possible cosets. $\square$

(e) Find $\left[(x^2 + x) + \langle x^2 + 5\rangle\right]^{-1}$ in $\dfrac{\mathbb{Z}_7[x]}{\langle x^2 + 5\rangle}$.

Use the Extended Euclidean algorithm:

$x^2 + x$	-	$x + 6$
$x^2 + 5$	1	$x + 5$
$x + 2$	$x + 5$	1
2	$4(x + 2)$	0

The table shows that

$$2 = (x + 6)(x^2 + 5) - (x + 5)(x^2 + x), \quad \text{or} \quad 2 = (x + 6)(x^2 + 5) + (6x + 2)(x^2 + x).$$

Therefore,

$$2 = (6x + 2)(x^2 + x) \pmod{x^2 + 5}.$$

I want the product to be 1, not 2 (since I want a reciprocal), so multiply both sides by 4:

$$1 = (24x + 8)(x^2 + x) \pmod{x^2 + 5}, \quad 1 = (3x + 1)(x^2 + x) \pmod{x^2 + 5}.$$

Thus,

$$\left[(x^2 + x) + \langle x^2 + 5\rangle\right]^{-1} = (3x + 1) + \langle x^2 + 5\rangle. \quad \square$$

Example. (a) Find an element of order 12 in $\mathbb{Z}_4 \times \mathbb{Z}_6$.

$1 \in \mathbb{Z}_4$ has order 4 and $2 \in \mathbb{Z}_6$ has order 3, so $(1, 2)$ has order $[4, 3] = 12$. $\square$

(b) List the elements of order 4 in $\mathbb{Z}_4 \times \mathbb{Z}_6$.

Elements of $\mathbb{Z}_4$ have order 1, 2, or 4. Elements of $\mathbb{Z}_6$ have order 1, 2, 3, or 6.
If $[m, n] = 4$ and $m = 1$, 2, or 4 and $n = 1$, 2, 3, or 6, then $m = 4$ and $n = 1$ or 2.
1 and 3 have order 4 in $\mathbb{Z}_4$.
0 has order 1 and 3 has order 2 in $\mathbb{Z}_6$.
So the elements of order 4 in $\mathbb{Z}_4 \times \mathbb{Z}_6$ are:

$$(1, 0), \quad (1, 3), \quad (3, 0), \quad (3, 3). \quad \square$$

A different question is: List the **subgroups** of order 4 in $\mathbb{Z}_4 \times \mathbb{Z}_6$. Can you do it?

Example. Write the product $(4\ 3\ 6)(1\ 5\ 3)(2\ 4)$ as a product of disjoint cycles. Is this permutation even or odd?

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 2 & 5 & 6 \\ 5 & 4 & 1 & 2 & 3 & 6 \\ 5 & 3 & 1 & 2 & 6 & 4 \end{pmatrix}$$

$$(4\ 3\ 6)(1\ 5\ 3)(2\ 4) = (1\ 5\ 6\ 4\ 2\ 3).$$

Since

$$(1\ 5\ 6\ 4\ 2\ 3) = (1\ 3)(1\ 2)(1\ 4)(1\ 6)(1\ 5),$$

the permutation is odd. □

Example. Let $\phi : G \to H$ be a group homomorphism. Prove that $\operatorname{im}\phi$ is a subgroup of H.

Since $1 = \phi(1)$, $1 \in \operatorname{im}\phi$: $\operatorname{im}\phi$ contains the identity.
Let $\phi(g) \in \operatorname{im}\phi$, where $g \in G$. Then

$$\phi(g)^{-1} = \phi(g^{-1}) \in \operatorname{im}\phi.$$

Thus, $\operatorname{im}\phi$ is closed under taking inverses.
Let $\phi(a), \phi(b) \in \operatorname{im}\phi$, where $a, b \in G$. Then

$$\phi(a)\phi(b) = \phi(ab) \in \operatorname{im}\phi.$$

Therefore, $\operatorname{im}\phi$ is closed under products. Hence, $\operatorname{im}\phi$ is a subgroup of H. □

Example. $\mathbb{R}^2$ is a group under componentwise addition and $\mathbb{R}$ is a group under addition. Let

$$H = \left\{ x \cdot (\sqrt{7}, -e) \;\middle|\; x \in \mathbb{R} \right\}.$$

Prove that $\dfrac{\mathbb{R}^2}{H} \approx \mathbb{R}$.

Define $f : \mathbb{R}^2 \to \mathbb{R}$ by

$$f(x, y) = ex + \sqrt{7}y.$$

Note that

$$f\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = \begin{bmatrix} e & \sqrt{7} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}.$$

Since f can be expressed as multiplication by a constant matrix, it's a linear transformation, and hence a group map.
Let $x \cdot (\sqrt{7}, -e) \in H$. Then

$$f[x \cdot (\sqrt{7}, -e)] = f(\sqrt{7}x, -ex) = e(\sqrt{7}x) + \sqrt{7}(-ex) = 0.$$

Therefore, $x \cdot (\sqrt{7}, -e) \in \ker f$, and hence $H \subset \ker f$.

Let $(x, y) \in \ker f$. Then

$$\begin{aligned} f(x, y) &= 0 \\ ex + \sqrt{7}y &= 0 \\ \sqrt{7}y &= -ex \\ y &= -\frac{e}{\sqrt{7}}x \end{aligned}$$

Hence,

$$(x, y) = \left(x, -\frac{e}{\sqrt{7}}x\right) = \frac{1}{\sqrt{7}}x \cdot (\sqrt{7}, -e) \in H.$$

Therefore, $\ker f \subset H$. Hence, $\ker f = H$.
Let $z \in \mathbb{R}$. Note that

$$f\left(\frac{1}{e}z, 0\right) = e \cdot \frac{1}{e}z + \sqrt{7} \cdot 0 = z.$$

Hence, $\operatorname{im} f = \mathbb{R}$.
Thus,

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