Solutions to Exam 2 practice problems

1. $f: \mathbb{Z} \to \mathbb{Z}_6$ given by $f(x) = [x]_6$

a. homomorphism (of rings!): <u>check</u>

$$f(x+y) = [x+y]_6 = [x]_6 + [y]_6 = f(x)+f(y) \checkmark$$
$$f(xy) = [xy]_6 = [x]_6[y]_6 = f(x)f(y) \checkmark$$
$$f(1) = [1]_6 = \text{identity in } \mathbb{Z}_6.$$

b. f is onto: need every $\alpha \in \mathbb{Z}_6$ is $= f(x)$ for some x. But $\alpha = [x]_6$ for some x, so $f(x) = [x]_6 = \alpha$.

c. f is not injective: need $x, y \in \mathbb{Z}$ with $x \neq y$ but $f(x) = f(y)$. I.e., want $[x]_6 = [y]_6$. But just pick (e.g.) $x=1$, $y=7$, then $x \neq y$ but $f(x) = f(1) = [1]_6 = [7]_6 = f(7) = f(y)$ (since $6 \mid 7-1$).

2. $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$ are not isomorphic.

$\mathbb{Z}_4$ has 2 units ($1, 3$), but $\mathbb{Z}_2 \times \mathbb{Z}_2$ only has one $(1,1)$, since $(\mathbb{Z}_2 \times \mathbb{Z}_2)^* = \mathbb{Z}_2^* \times \mathbb{Z}_2^* = \{1\} \times \{1\}$. But an isomorphism gives a one-to-one correspondence between units; so there <u>can't</u> be an isomorphism

<u>OR</u> If $\varphi: \mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ were an isomorphism, then
$$\underset{\varphi([2]_4)}{\overset{\|}{\varphi(2 \cdot [1]_4)}} = 2\varphi([1]_4) = 2([1]_2, [1]_2) = ([0]_2, [0]_2)$$
But we <u>also</u> have $\varphi([0]_4) = ([0]_2, [0]_2)$; since $[0]_4 \neq [2]_4$, φ <u>can't</u> be 1-to-1. So no such isomorphism φ can exist.

3. $D: \mathbb{R}[x] \to \mathbb{R}[x]$, $D(p(x)) = p'(x)$, is <u>not</u> a homomorphism of rings.

<u>Check</u>: $D(x^2) = 2x$, but $D(x) \cdot D(x) = 1 \cdot 1 = 1$; so

$D(x \cdot x) = D(x^2) = 2x \neq 1 = D(x) \cdot D(x)$, so D does not behave well with respect to multiplication in $\mathbb{R}[x]$. So D is <u>not</u> a homomorphism.

<u>or</u>

$D(1) = 0 \neq 1$, so it doesn't send $1_{\mathbb{R}[x]}$ to $1_{\mathbb{R}[x]}$.

So it isn't a homomorphism.

4. $R' \subseteq R$ subring, $S' \subseteq S$ subring, then $R' \times S' \subseteq R \times S$ is a subring.

<u>Check</u>: $(r,s), (r',s') \in R' \times S'$, then

$(r,s) + (r',s') = (r+r', s+s') \in R' \times S'$, since $r+r' \in R'$, $s+s' \in S'$, and

$(r,s)(r',s') = (rr', ss') \in R' \times S'$, since $rr' \in R'$ and $ss' \in S'$.

$-(r,s) = (-r,-s) \in R' \times S'$, since $-r \in R'$, $-s \in S'$.

R' and S' have identities $1_{R'}, 1_{S'}$, so

$(1_{R'}, 1_{S'})(r,s) = (r,s)(1_{R'}, 1_{S'}) = (r,s)$, since $1_{R'} r = r 1_{R'} = r$ all $r \in R'$, $1_{S'} s = s 1_{S'} = s$ all $s \in S'$.

So (R', S') is a subring.

5. $\mathbb{Z}_6 \times \mathbb{Z}_5 \cong \mathbb{Z}_{10} \times \mathbb{Z}_3$

Since $(6,5) = 1$ we have $\mathbb{Z}_6 \times \mathbb{Z}_5 \cong \mathbb{Z}_{6 \cdot 5} = \mathbb{Z}_{30}$. But $(3,10) = 1$, so $\mathbb{Z}_{10} \times \mathbb{Z}_3 \cong \mathbb{Z}_{10 \cdot 3} = \mathbb{Z}_{30}$. So

$\mathbb{Z}_6 \times \mathbb{Z}_5 \cong \mathbb{Z}_{30} \cong \mathbb{Z}_{10} \times \mathbb{Z}_3$. So $\mathbb{Z}_6 \times \mathbb{Z}_5 \cong \mathbb{Z}_{10} \times \mathbb{Z}_3$.

6. $R \neq \{0\} \neq S$, then $R \times S$ has a non-trivial idempotent.

Since $1_R \cdot 1_R = 1_R$ and $0_S \cdot 0_S = 0_S$, we have
$(1_R, 0_S)\cdot(1_R, 0_S) = (1_R 1_R, 0_S 0_S) = (1_R, 0_S)$, so $(1_R, 0_S)$ is an idempotent. But

$(1_R, 0_S) \neq (0_R, 0_S) = 0_{R\times S}$, since $1_R \neq 0_R$, and
$(1_R, 0_S) \neq (1_R, 1_S) = 1_{R\times S}$, since $0_S \neq 1_S$. So
$(1_R, 0_S)$ is a non-trivial idempotent in $R\times S$.

7. Solve $x \equiv 3\ (5)$, $x \equiv 1\ (6)$, $x \equiv 2\ (11)$

First solve $3 + 5l = x = 1 + 6k$ so $2 = 6k - 5l$

$6 = 5\cdot 1 + 1$ so $1 = 6 - 5\cdot 1$ so $2 = 6\cdot 2 - 5\cdot 2$, so set

$l = 2$, $k = 2$, so $x = 3 + 5l = 13$. Then replace first two equations with $x \equiv 13 \pmod{5\cdot 6}$, i.e. $x \equiv 13\ (30)$. Then solve

$13 + 30l = x = 2 + 11k$ so $11 = 11k - 30l$

Hm! well, just take $k = 1$, $l = 0$!

So $x = 13 + 30l = 13$. So the general solution is

$x = 13 + (11\cdot 30)n = 13 + 330n$.

[Your problem on the exam will be a little bit more involved!]

8. $f: \mathbb{Z}_8 \to \mathbb{Z}_{12}$ given by $f([x]_8) = [3x]_{12}$.

(a) f is a function: $[x]_8 = [y]_8$, then $y - x = 8k$ some k,
so $3y - 3x = 3(y-x) = 3(8k) = 24k = 12(2k)$, so
$[3x]_{12} = [3y]_{12}$. So value of $f([x]_8)$ doesn't depend

a representative of $[x]_8$.

homomorphism of groups: $f([x]_8+[y]_8) = f([x+y]_8)$

$= [3(x+y)]_{12} = [3x+3y]_{12} = [3x]_{12}+[3y]_{12} = f([x]_8)+f([y]_8)$

(b) Not injective: $f([0]_8) = [3\cdot 0]_{12} = [0]_{12}$, but so is $f([4]_8) = [3\cdot 4]_{12} = [12]_{12} = [0]_{12}$. ~~But~~ $[0]_8 \neq [4]_8$. So f sends two different elements to the same place, so f isn't 1-to-1.

Not surjective; Short way: you can't have a function from 8 things onto 12 things.

OR $f(x) = [3x]_{12} = [1]_{12}$ is impossible, since we would need $3x-1=12k$ for some k, so $1 = 3x-12k = 3(x-4k)$, but 1 isn't a multiple of 3 !

OR By listing them all (all $f([x]_8)$, $x=0,\dots,7$), f only takes the values $[0]_{12}, [3]_{12}, [6]_{12}$, and $[9]_{12}$. So f misses 8 values.

(c) homomorphism of rings? No: $f([1]_8) = [3\cdot 1]_{12} = [3]_{12} \neq [1]_{12}$, so f doesn't send 1 to 1.

OR $f(1_R\cdot 1_R) = f([1]_8) = [3]_{12}$, but $f(1_R)\cdot f(1_R) = [3]_{12}\cdot[3]_{12} = [9]_{12} \neq [3]_{12}$, so f does not behave well under multiplication.

$= a^{mn} b^{mn} = (a^n)^m (b^m)^n = e^m e^n = e^{m+n} = e$

(b) $H = \{ a \in G : a^k = e \text{ some } k \in \mathbb{N} \}$ is a subgroup:

if $a, b \in H$ then $a^n = e$, $b^m = e$ some $n, m \in \mathbb{N}$, so by (a), $(ab)^{mn} = e$ so $(ab)^k = e$ some $k \in \mathbb{N}$, so $ab \in G$.

if $a \in H$ then $a^n = e$ some $n \in \mathbb{N}$, so
$(a^n)^{-1} = e^{-1} = e = a^{n(-1)} = a^{-n} = a^{(-1)n} = (a^{-1})^n$, so $(a^{-1})^n = e$ some $n \in \mathbb{N}$, so $a^{-1} \in H$.
Finally, $e^1 = e$ so $e \in H$. So H is a subgroup.

10. G group, $H, K \leq G$ subgroups, then $H \cap K$ is a subgroup.

<u>Need</u> If $h_1, h_2 \in H \cap K$, then $h_1 h_2 \in H \cap K$.

But $h_1 \in H \cap K \Rightarrow h_1 \in H$ and $h_1 \in K$
$h_2 \in H \cap K \Rightarrow h_2 \in H$ and $h_2 \in K$
so $h_1, h_2 \in H$, $h_1, h_2 \in K$ so $h_1 h_2 \in H$ (b/c H is a subgroup), $h_1 h_2 \in K$ (b/c K is a subgroup)

so $h_1 h_2 \in H$ and $h_1 h_2 \in K$, so $h_1 h_2 \in H \cap K$.

If $h \in H \cap K$ then $h^{-1} \in H \cap K$.

But $h \in H \cap K \Rightarrow h \in H$, $h \in K$ so $h^{-1} \in H$ (b/c H is a subgroup), $h^{-1} \in K$ (b/c K is a subgroup)
so $h^{-1} \in H$ and $h^{-1} \in K$, so $h^{-1} \in H \cap K$. //

Finally $1_G \in H$ (b/c H is a subgroup) and $1_G \in K$ (b/c K is a subgroup) so $1_G \in H \cap K$.

So, $H \cap K$ is a subgroup.