Solution to Exam 2 practice problems

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

a. Homomorphism (of rings!): check
\[
\begin{align*}
    f(x+y) &= [x+y]_6 = [x]_6 + [y]_6 = f(x) + f(y) \checkmark \\
    f(xy) &= [xy]_6 = [x]_6 [y]_6 = f(x)f(y) \checkmark \\
    f(1) &= [1]_6 = \text{identity in } \mathbb{Z}_6.
\end{align*}
\]

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 \( x = 1, y = 7 \), 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
\[
(\mathbb{Z}_2 \times \mathbb{Z}_2)^* = \mathbb{Z}_2^* \times \mathbb{Z}_2^* = \{1, 3\} \times \{1, 3\}.
\]

But an isomorphism gives a one-to-one correspondence between units; so there can't be an isomorphism.

\( \Box \) If \( \phi : \mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2 \) were an isomorphism, then
\[
\begin{align*}
\phi ([x]_4) &= \phi ([2]_4) = 2 \phi ([1]_4) = 2 (1, 3) = (2, 6) = (2, 0) \\
\phi ([y]_4) &= \phi ([3]_4) = \phi ([1]_4) = \phi ([2]_4),
\end{align*}
\]

since \( 2 \cdot 3 \neq 2 \cdot 1 \), \( \phi \) can't be 1-1. So no such isomorphism \( \phi \) can exist.
3. \( D: \mathbb{R}[x] \to \mathbb{R}[x], \quad D(p(x)) = p'(x), \) is not a homomorphism of rings.

Check: \( D(x^2) = 2x, \) but \( D(x)D(x) = 1 \cdot 1 = 1; \) so
\[
D(x \cdot x) = D(x^2) = 2x \neq 1 = D(x)D(x),
\]
so \( D \) does not behave well with respect to multiplication in \( \mathbb{R}[x]. \) So \( D \) is not a homomorphism.

\( \text{As } D(1) = 0 \neq 1, \) so it doesn't send \( 1_{\mathbb{R}[x]} \) to \( 1_{\mathbb{R}[x]}. \)
So it isn't a homomorphism.

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

Check: \( (r,s), (r',s') \in R' \times S', \) then
\[
(r,s) + (r',s') = (r+r', s+s') \in R' \times S', \text{ since } r+r' \in R' \text{ and } s+s' \in S'.
\]
\[
(r,s)(r',s') = (rr', ss') \in R' \times S', \text{ since } rr' \in R' \text{ and } ss' \in S'.
\]
\(- (r,s) = (-r, -s) \in R' \times S', \text{ since } -r \in R', \ -s \in S'.
\]
\( R' \text{ and } S' \) have identites: \( 7e, 7'i, \) so \( 7e \cdot 7e = 7ei = 7 \) all \( r \in R', \)
\[
(7e, 7'i)(r,s) = (7es, 7sis) = (r,s), \text{ since } 7s = 5, 7i = 5 \text{ all } s \in S'.
\]
So \( (R', S') \) is a subring.

5. \( \mathbb{R}_6 \times \mathbb{R}_5 \cong \mathbb{R}_{10} \times \mathbb{R}_3 \)

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

6. If \( R \neq \{0\} \pm \{S \}, \text{ then } R \times S \text{ has a non-trivial idempotent.}

Since \( 7r \cdot 7r = 7r \) and \( 0_5 \cdot 0_5 = 0_5 \), we have
\[
(7r, 0_5) \cdot (7r, 0_5) = (7r, 0_5) \circ (7r, 0_5) = (7r, 0_5)
\]
as an idempotent. But
\[
(7r, 0_5) \neq (0_5, 0_5) = 0_5 \times 0_5, \quad \text{since } 7r \neq 0r, \quad \text{and}

(7r, 0_5) \neq (7r, 7s) = 7r \times 7s, \quad \text{since } 0_5 \neq 1, \quad \text{So}

(7r, 0_5) \text{ 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 \( 3 + 5l = x = 1 + 6l \) so \( 2 = 6k - 5l = 6 \cdot 2 - 5 \cdot 2 \), so set
\[
l = 2, \; k = 2, \quad \text{so} \quad x = 3 + 5l = 13.
\]
Then replace first two equations with \( x \equiv 13 \pmod{5 \cdot 6}, \) i.e. \( x \equiv 13(3) \).
Then solve
\[
13 + 30l = x = 2 + 11k \quad \text{so} \quad 11 = 11k - 30l
\]
then! 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. \( f: \mathbb{Z}_8 \rightarrow \mathbb{Z}_{12} \) given by \( f([x]_8) = [3x]_{12} \).

(a) \( f \) is a function: \( [x]_8 = [y]_8 \), then \( y - x = 8k \) some \( k \),
\[
3y - 3x = 3(y - x) = 3(8k) = 24k = 12(2k), \quad \text{so}
\]
\( [3x]_{12} = [3y]_{12} \). So value of \( f([x]_8) \) doesn't depend
an representative of \([x_{7p}]\).

- Homomorphism of graphs: \(f([x_{7p} + y_{7p}]) = f(x_{7p}) = [3x + 3y]_{12} = [3x]_{12} + [3y]_{12} = f([x_{7p}]) + f([y_{7p}])\)

(b) Not injective: \(f([0]_{7}) = [3\cdot 0]_{12} = [0]_{12}\), but \(0\) is
\(f([4]_{7}) = [3\cdot 4]_{12} = [12]_{12} = [0]_{12}\). But \([0]_{12} \neq [4]_{12}\). So
\(f\) sends two different elements to the same place, so \(f\)
isn't 1-1.

Not surjective: Short way: you can't have a function from 7 things onto 12 things.

\(\Rightarrow \ f([x]_{7}) = [3x]_{12} = [0]_{12}\) 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 ! (call \(f([x]_{7})), x = 0, \ldots, 6)\)

\(\Rightarrow \) By listing them all, \(f\) only takes the values \([3]_{12}, [3]_{12}, [0]_{12}\),
and \([9]_{12}\). So \(f\) misses 8 values.

(c) Homomorphism of rings? No: \(f([7]_{7}) = [3\cdot 7]_{12} = [21]_{12} \neq [7]_{12}\), so
\(f\) doesn't send 1 to 7.

\(\Rightarrow \ f([x]_{7} + [7]_{7}) = f([x]_{7}) = [3x]_{12}, \) but
\(f([7]_{7}) \cdot f([x]_{7}) = [3]_{12} \cdot [3x]_{12} = [9x]_{12} \neq [3]_{12}, \) so \(f\) does not
believe in under multiplication.
= a^m b^n = (a^n)(b^m)^n = e^m e^n = e^{m+n} = e

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

- If $a,b \in H$ then $a^k = e$, $b^k = e$ some $k \in \mathbb{N}$, so by (a) $(ab)^k = e$ some $k \in \mathbb{N}$, so $ab \in H$.

- If $a \in H$ then $a^k = e$ some $k \in \mathbb{N}$, so $\left(a^{-1}\right)^k = e = a^{k \cdot (-1)} = a^{-k} = a^{-(k-1)} = a^{-(k-2)} \cdots a^{-(k-n)} = e$, so $\left(a^{-1}\right)^n = e$ some $n \in \mathbb{N}$, so $a^{-1} \in H$.

Finally, $e^k = e \in H$ too. So $H$ is a subgroup.

10. For a group, $H \subseteq G$, subgroups, then $HK$ is a subgroup.

Need

If $h_1, h_2 \in HK$, then $h_2 \in HK$.

But $h_1 \in HK \Rightarrow h_1H \cap HK \neq \emptyset$, $h_2 \in HK \Rightarrow h_2H \cap HK \neq \emptyset$, $h_1H \cap h_2H \neq \emptyset$, $h_1h_2 \in H$ (since $HK$ is a subgroup) $h_1H \cap h_2H$ $h_1h_2 \in HK$, so $h_2 \in HK$.

If $h_1H \cap h_2H$, then $h_1 \in H$.

But $h_1H \cap h_2H \neq \emptyset$, $h_1h_2 \in H$ (since $HK$ is a subgroup)$h_1 \in HK \cap h_2H$, so $h_2 \in HK$.

Finally, $h_1H \cap h_2H$ $h_1 \in HK \cap h_2H$, $h_1h_2 \in HK$, so $h_2 \in HK$.

So, $HK$ is a subgroup.