Sample questions

1. Suppose that G is a *simple* group (which means: the only *normal* subgroups of G are the trivial subgroups $\{e\}$ and G). Suppose that $\phi : G \to H$ is a homomorphism. Show that ϕ is injective or trivial (meaning: $\phi(g) = e$ for all $g \in G$).

   Let K be the kernel of ϕ. Then K is a normal subgroup of G. But if G is simple, then K is either $\{e\}$ (in which case ϕ is injective) or K is G (in which case ϕ is trivial).

2. Let G be a group of order n and H a group of order m, and let $\phi : G \to H$ is a homomorphism.

   (a) Show that $\phi(G)$ is a subgroup of H.

   The identity in H is in $\phi(G)$ because it equals $\phi(e)$. If we take two elements of $\phi(G)$, say $\phi(g_1)$ and $\phi(g_2)$, then the product is again in $\phi(G)$ because the product $\phi(g_1)\phi(g_2)$ equals $\phi(g_1 g_2)$, and $g_1 g_2 \in G$. Similarly, $\phi(G)$ is also closed under taking inverses.

   (b) Show that the order of $\phi(G)$ divides m.

   If $|H| = m$ then any subgroup of H has order dividing m. Part (a) showed that $\phi(G)$ is a subgroup of H.

   (c) Show that the order of $\phi(G)$ divides n as well.

   By the first isomorphism theorem, $\phi(G)$ is isomorphic to G/K where K is the kernel of ϕ. Thus the number of elements of $\phi(G)$ is $|G/K| = |G|/|K| = n/|K|$ which divides n.

3. List (up to isomorphism) all *abelian groups* of order ≤ 10. Don't list the same one twice.

   $\mathbf{Z}_1, \mathbf{Z}_2, \mathbf{Z}_3, \mathbf{Z}_4, \mathbf{Z}_2 \times \mathbf{Z}_2, \mathbf{Z}_5, \mathbf{Z}_6, \mathbf{Z}_7, \mathbf{Z}_8, \mathbf{Z}_4 \times \mathbf{Z}_2, \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2,$
   $\mathbf{Z}_9, \mathbf{Z}_3 \times \mathbf{Z}_3, \mathbf{Z}_{10}.$

4. Compute the elementary divisors and the invariant factors of $\mathbf{Z}_{10} \oplus \mathbf{Z}_{15} \oplus \mathbf{Z}_{20} \oplus \mathbf{Z}_{25}$.

   First, split up as much as possible using the rule $\mathbf{Z}_{nm} \cong \mathbf{Z}_n \times \mathbf{Z}_m$ whenever $\gcd(n, m) = 1$. Note that this allows us to split up $\mathbf{Z}_N$ as a product of smaller groups whenever N is not a prime-power.
   Then we get $\mathbf{Z}_2 \oplus \mathbf{Z}_5 \;\oplus\; \mathbf{Z}_3 \oplus \mathbf{Z}_5 \;\oplus\; \mathbf{Z}_4 \oplus \mathbf{Z}_5 \;\oplus\; \mathbf{Z}_{25}$
   so the elementary divisors are $2, 5,\ 3, 5,\ 4, 5,\ 25$ and if we sort them by prime-power we get $2, 4,\ \ 3,\ \ 5, 5, 5, 25$.

Next, to get the invariant factors, you need to combine the highest p-powers, then combine the next highest p-powers, etc. The highest 2-power is 4, the highest 3-power is 3, and the highest 5-power is 25. Combine them (multiply) to get 300. The next highest 2-power is 2, the next highest 3-power is 1 (there is no 3-power left), and the next highest 5-power is 5. Combine them, and you get 10. After that, what remains are two more 5's. Result:

invariant factors: 300, 10, 5, 5

5. Compute the elementary divisors and the invariant factors of $\mathbf{Z}_4 \oplus \mathbf{Z}_6 \oplus \mathbf{Z}_8 \oplus \mathbf{Z}_{12}$.

   Elementary divisors: 4, 2,3, 8, 3,4. Collected by prime-power:
   Elementary divisors: 2,4,4,8, 3,3.

   Invariant factors: 24, 12, 4, 2.

6. For each of the following, indicate if it is a group or not. If it is a group, then no further explanation is needed. If it is not a group, then indicate the group axiom(s) that fail. Recall that the 4 axioms are:

   #1 = "Closure under the group operation" (applying the group operation to two elements in that set gives again an element of that set)
   #2 = Associativity
   #3 = "There is an identity"
   #4 = "Every element has an inverse"

   (a) The set $\{\ldots, -4, -2, 0, 2, 4, \ldots\}$ of all even integers with operation $+$

   Group.

   (b) The set $\{1, 2, 4, \frac{1}{2}, \frac{1}{4}\}$ with operation $\cdot$

   Fails #1

   (c) The set $\{1, i, -1, -i\}$ with operation $\cdot$

   Group.

   (d) $\{\overline{0}, \overline{2}, \overline{4}\}, +$ where $\{\overline{0}, \overline{2}, \overline{4}\} \subset \mathbb{Z}_6$ which means work modulo 6.

   Group.

   (e) $\{\overline{0}, \overline{2}, \overline{4}\}, \cdot$ where $\{\overline{0}, \overline{2}, \overline{4}\} \subset \mathbb{Z}_6$.

   Fails #3 because $\overline{0}$ has no multiplicative inverse.

   (f) $\{\overline{1}, \overline{3}, \overline{9}\}, \cdot$ where $\{\overline{1}, \overline{3}, \overline{9}\} \subset \mathbb{Z}_{13}$ which means work modulo 13.

That's a group: $<\overline{3}>$.

7. True or false? For parts (d) and (e) give some explanation.

   (a) Is a UFD always a PID? False.

   (b) Is a PID always a UFD? True.

   (c) Is a Euclidean Domain always a PID? True.

   (d) If $u \in \mathbb{C}$ is the solution of some non-zero polynomial $f(x) \in \mathbb{Q}[x]$, must u then also be a solution of some *irreducible* non-zero polynomial in $\mathbb{Q}[x]$? Yes (the minpoly of u).

   (e) If $[K : \mathbb{Q}] = 5$ and $u \in K$ and $u \notin \mathbb{Q}$ must then the degree of the minimal polynomial of u over $\mathbb{Q}$ always be 5? Yes, because $5 = [K : \mathbb{Q}] = [K : \mathbb{Q}(u)]\cdot[\mathbb{Q}(u) : \mathbb{Q}]$ so the number $d := [\mathbb{Q}(u) : \mathbb{Q}]$ (this is always the degree of the minpoly of u over $\mathbb{Q}$) divides 5, so d is 1 or 5, but it is not 1 since $u \notin \mathbb{Q}$ so $d = 5$.