(Sketches of) Solutions to sample final questions

1. First we list the cyclic subgroups. Since there are 12 elements, we would have at most 12 cyclic subgroups.

$\langle(0,0)\rangle$, $\langle(1,0)\rangle$, $\langle(0,1)\rangle$, $\langle(0,2)\rangle$, $\langle(0,3)\rangle$, $\langle(1,1)\rangle$, $\langle(1,2)\rangle$, $\langle(1,3)\rangle$

$\langle(1,4)\rangle = \{(1,4),(0,2),(1,0),(0,4),(1,2),(0,0)\}$

Same as $\langle(1,2)\rangle$.

$\langle(5,0)\rangle$ same as $\langle(1,0)\rangle$

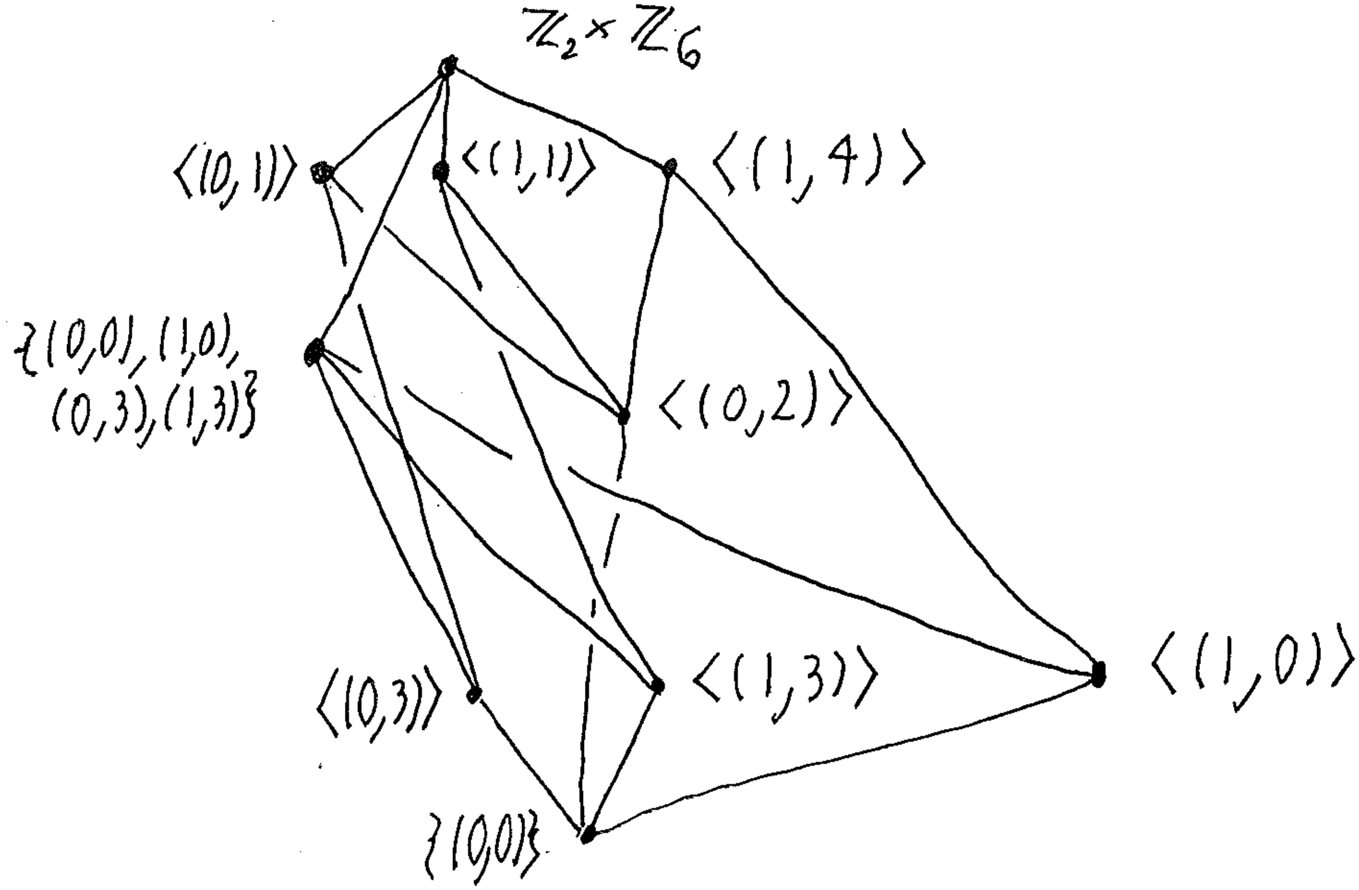
$\langle(0,4)\rangle$ same as $\langle(0,2)\rangle$

$\langle(1,1)\rangle$ same as $\langle(1,5)\rangle$

(In any group G, $\langle g\rangle = \langle g^{-1}\rangle$.)

We also have to consider the non-cyclic subgroups. For example, the full group $\mathbb{Z}_2\times\mathbb{Z}_6$. The orders of the possible subgroups are $1,2,3,4,6,12$ by Lagrange. We know abelian groups of order $1,2,3,6$ are all cyclic. So we only have to look for subgroups isomorphic to $\mathbb{Z}_2\times\mathbb{Z}_2$. The only such group is $\{(0,0),(1,0),(0,3),(1,3)\}$.

Diagram:



2\. (a) The order of a is the same as the order of the cyclic subgroup generated by a, and by Lagrange's theorem, the order of that subgroup divides the order of G.

(b) This is false. For example, there is no element in $\mathbb{Z}_2 \times \mathbb{Z}_2$ of order 4.

(c) The order of $U(\mathbb{Z}_p)$ is $p-1$ (because p is prime. The order of a in $U(\mathbb{Z}_p)$ divides $p-1$, so $a^{p-1} \equiv 1 \bmod p$.

3. If the group of order 6 is cyclic, then there is an element of order 2. Otherwise, all elements have order 1, 2, 3. Only 1 element has order 1. If g has order 3, then g^{-1} has order 3. Thus there are an even number of elements of order 3 and 1 element of order 1, so the leftover element(s) must have order 2.

4. The only element of Q_8 of order 2 is -1. On the other hand, D_4 has 5 elements of order 2: r^2, rs, r^2s, r^3s, s.

5. a. c is the identity.

b. a is the inverse of d because $ad = da = c$.

c. $a^2 = b$, $a^3 = b \cdot a = d$, $a^4 = a \cdot d = c$, so a has order 4.

6. a. The function $f(x) = x$.

b. Let $g(x) = \begin{cases} 2 & \text{if } x = 1 \\ 3 & \text{if } x = 2 \\ 1 & \text{if } x = 3 \\ x & \text{if } x \neq 1, 2, 3. \end{cases}$

This has order 3.

c. Let $f(x) = x + 1$.

d. No. $g(f(3)) = g(4) = 4$

$f(g(3)) = f(1) = 2$.

So the functions $g \circ f$ and $f \circ g$ are not equal, so the group is not abelian.

7. (a) None exists. $U(\mathbb{Z}_8)$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. All four elements would have to map to an element of order 1 or 2. So all four elements would have to map to 0 or 4 in $\mathbb{Z}_8$. Can't be injective.

7. b. This is impossible (none exists).
A subgroup of an abelian group is abelian.

c. $(\mathbb{R}, +)$. It's uncountable so it's not cyclic.

d. None exists. If $\mathbb{R}/H$ is isomorphic to $\mathbb{Z}_2$, say

$$H \to 0$$
$$x + H \to 1$$

is the isomorphism $\mathbb{R}/H \to \mathbb{Z}_2$.
But then the coset $\frac{x}{2} + H$ satisfies $(\frac{x}{2} + H) + (\frac{x}{2} + H) = x + H$.
This is a contradiction.

e. $H = \{ e, (12), (34), (12)(34) \}$
To check that it's not normal, for example $(23) H (23)^{-1} \neq H$.

8. a. True.

$(h,k) \mapsto (k,h)$ is an isomorphism.

b. True. Take $H = \langle g \rangle$, the cyclic subgroup generated by g.

c. True. Take any nonidentity element $g \in G$. Then g has order p, p^2, or p^3.

If g has order p, done.

If g has order p^2, then g^p has order p.

If g has order p^3, then $g^{(p^2)}$ has order p.

d. False. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ has order 4^3 but it has no element of order 4.