1. Write down a group isomorphism $\phi : \mathbb{Z}_4 \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$ with all images in the form $([a], [b])$, for $0 \leq a \leq 1$ and $0 \leq b \leq 2$.  

2. Let $G$ be a group and $g$ be an element of order 36 in $G$. What are the orders of the following elements of $G$: $g^{-1}, g^8, g^{15}, g^{27}$? Explain your answers.  

3. Let $Q$ be the field of rational numbers and $D = \{a + b\sqrt{2} : a, b \in Q\}$. 
   a) Show that $D$ is a subring of the field $\mathbb{R}$ of real numbers.  
   b) Prove or disprove that $D$ is a subfield of $\mathbb{R}$.  
   c) Prove that $\sqrt{3} \notin D$.  

4. Find a commutative ring $R$ with an injective ring homomorphism $\phi : R \rightarrow R$, which is not an isomorphism.  

5. Let $*: G \times G \rightarrow G$ be an associative binary operation on a set $G$. 
   a) Show that $(G, *)$ has at most one neutral element.  
   b) Show that each element of $G$ has at most one inverse with respect to $*$.  

6. Show that any finite integral domain is a field.  

*The theorems in Durbin's book may be used to solve the exercises 1-4, but all claims that are made must be motivated.*
Solutions to examination in algebra MMG 500 and MVE 150, 2013-08-19

1. The map \( \theta : \mathbb{Z}_m \to \mathbb{Z}_n \) where \( \theta([a]_m) = [a]_n \) is well defined for a factor \( n \) of \( m \) as \( n \mid (a-b) \) if \( m \mid (a-b) \). It is a homomorphism as \( \theta([a]_m + [b]_m) = \theta([a+b]_m) = \theta([a]_m) + \theta([b]_m) = [a+b]_n = [a+b]_m \).

The map \( \phi : \mathbb{Z}_a \to \mathbb{Z}_b \times \mathbb{Z}_c \) which sends \([a]_a\) to \(([a]_b, [a]_c)\) is thus a homomorphism. It is in fact an isomorphism as it is bijective. Indeed, \( \phi([0]_a) = ([0]_b, [0]_c), \phi([1]_a) = ([1]_b, [1]_c), \phi([2]_a) = ([0]_b, [2]_c), \phi([3]_a) = ([1]_b, [0]_c), \phi([4]_a) = ([0]_b, [1]_c) \) and \( \phi([5]_a) = ([1]_b, [2]_c) \).

2. \((g^{-1})^n = g^{-36} = e\) if \(1 \leq n \leq 35\), while \((g^{-1})^{36} = g^{-36} = e\). Hence \(o(g^{-1}) = 36\).

\((g^{-3})^n = g^{-3 \times 12} = g^{36} = e\) with \(36-8 \times 1 = 28, 36-8 \times 2 = 20, 36-8 \times 3 = 12, 36-8 \times 4 = 4\). Hence \((g^{-3})^n \neq e\) if \(1 \leq n \leq 4\). Also, \((g^{-4})^n = g^{72-8n}\) with \(72-8 \times 5 = 32, 72-8 \times 6 = 24, 72-8 \times 7 = 16, 72-8 \times 8 = 8, 72-8 \times 9 = 0\). So \((g^{-4})^n \neq e\) if \(5 \leq n \leq 8\) and \((g^{-4})^8 = e\), which implies that \(o(g^{-4}) = 9\).

\(o(g^{15}) = o(H) = 36\) by a theorem in Durbin’s book we have \(|H| = 36/GCD(36, 15) = 36/3 = 12\). Hence \(o(g^{15}) = 12\).

\(o(g^{27}) = o(g^{27})\) is 36/GCD(36, 27) = 36/9 = 4. Indeed \(g^{27} \neq e\), \((g^{27})^2 = g^{54} = g^{18} \neq e\), \((g^{27})^3 = g^{81} = g^{9} \neq e\) and \((g^{27})^4 = g^{108} = g^{36} = e^3 = e\).

3a) Suppose \(a + b\sqrt{2} \in D\) or \((c + a\sqrt{2}) \in D\). Then
\((a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)(\sqrt{2}) \in D,\)
\((a + b\sqrt{2})(c + d\sqrt{2}) = (ac - 2bd) + (ad + bc)(\sqrt{2}) \in D,\)
\((a + b\sqrt{2})(c + d\sqrt{2}) = (bc + ad)(\sqrt{2}) \in D,\)
\((a + b\sqrt{2})(c + d\sqrt{2}) = (bc - ad)(\sqrt{2}) \in D,\)

Hence \(D\) is a subring of \(R\) by the subring criterion.

3b) Suppose \(a + b\sqrt{2} \in D\). Then \(1/(a + b\sqrt{2}) = (a - b\sqrt{2})/(a + b\sqrt{2})(a - b\sqrt{2}) = (a - b\sqrt{2})(a^2 - 2b^2) = a/(a^2 - 2b^2) + (-b)/(a^2 - 2b^2) \in D\). The subring \(D\) is thus a subfield of \(R\).

3c) Suppose \(\sqrt{3} = a + b\sqrt{2}\) or \(\sqrt{3} = a + b\sqrt{2}\), then \(3 = (a + b\sqrt{2})^2 = a^2 + 2b^2 + 2ab\sqrt{2}\) and \(\sqrt{2} = (3 - a^2 - 2b^2)/2ab \in Q\) in case \(ab \neq 0\). If instead \(a = 0\), then \(\sqrt{2} = 2b\) and if \(b = 0\), then \(\sqrt{3} = a\). We have thus shown that if \(\sqrt{3} \in D\), then \(\sqrt{2}, \sqrt{3}\) or \(\sqrt{6}\) is rational. But this is impossible. Indeed, if \(\sqrt{n} = pq\) for two relatively prime positive integers \(p\) and \(q\), then \(nq^2 = p^2\) where \(q\) can only be 1. So \(\sqrt{2}, \sqrt{3}\) and \(\sqrt{6}\) are irrational and \(\sqrt{3} \notin D\).

4. There are many such rings. Let \(R = A[X] \) be the ring of all polynomials in an indeterminate \(X\) with coefficients in a commutative ring \(A\). Then the map \(\Phi : R \to R\), which sends \(p(X) = a_0 + a_1X + \ldots + a_nX^n \) to \(\Phi(p(X)) = a_0 + a_1X^2 + \ldots + a_nX^{2n}\) is a ring homomorphism. Indeed, \(\Phi(p(X) + q(X)) = (a_0 + b_0) + (a_1 + b_1)X^2 + \ldots + (a_n + b_n)X^{2n} = (a_0 + a_1X^2 + \ldots + a_nX^{2n}) + (b_0 + b_1X^2 + \ldots + b_nX^{2n})\)
\[ \Phi(p(X)) + \Phi(q(X)) \] or simply \[ \Phi(p(X) + q(X)) = (p+q)(X^a) = p(X^a) + q(X^a) = \Phi(p(X)) + \Phi(q(X)). \]

Similarly, if we let \( q(X) = b_0 + b_1 X + \ldots + b_a X^a \) and \( pq \) be the product of \( p \) and \( q \) in \( R \), then
\[ \Phi(p(X)q(X)) = (pq)(X^a) = p(X^a)q(X^a) = \Phi(p(X))\Phi(q(X)). \]

\( \Phi \) is injective as \( \text{ker } \Phi = 0 \). It is also clear that \( \Phi \) is not surjective as \( X \notin \text{Im } \Phi \).

5. See Durbin's book p.32 or the lecture notes.

6. See Durbin's book p.129 or the lecture notes.