MATHEMATICS Chalmers University of Technology
Examination in algebra MMG 500 and MVE 150, 2013-08-19
No books, written notes or any other aids are allowed.
Telephone : 0703-08 83 04

1.Write down a group isomorphism $\phi : \mathbf{Z}_6 \to \mathbf{Z}_2 \times \mathbf{Z}_3$ with all images in the form $([a]_2, [b]_3)$ for $0\leq a\leq 1$ and $0\leq b\leq 2$. 3p

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. 4p

3. Let $\mathbf{Q}$ be the field of rational numbers and $D = \{a + b\sqrt{2} : a, b \in \mathbf{Q}\}$. 6p

a) Show that D is a subring of the field $\mathbf{R}$ of real numbers.

b) Prove or disprove that D is a subfield of $\mathbf{R}$.

c) Prove that $\sqrt{3} \notin D$.

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

5. Let $* : G \times G \to G$ be an associative binary operation on a set G. 4p

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. 4p

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

The map $\phi : \mathbf{Z}_6 \to \mathbf{Z}_2 \times \mathbf{Z}_3$ which sends $[a]_6$ to $([a]_2,[a]_3)$ is thus a homomorphism. It is in fact an isomorphism as it is bijective. Indeed, $\phi([0]_6) = ([0]_2,[0]_3)$, $\phi([1]_6) = ([1]_2,[1]_3)$, $\phi([2]_6) = ([0]_2,[2]_3)$, $\phi([3]_6) = ([1]_2,[0]_3)$, $\phi([4]_6) = ([0]_2,[1]_3)$ and $\phi([5]_6) = ([1]_2,[2]_3)$.

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

$(g^{-8})^n = g^{-8n} = g^{36-8n}$ with $36-8\times1=28$, $36-8\times2=20$, $36-8\times3=12$, $36-8\times4=4$. Hence $(g^{-8})^n \neq e$ if $1 \leq n \leq 4$. Also, $(g^{-8})^n = g^{72-8n}$ with $72-8\times5=32$, $72-8\times6=24$, $72-8\times7=16$, $72-8\times8=8$, $72-8\times9=0$. So $(g^{-8})^n \neq e$ if $5 \leq n \leq 8$ and $(g^{-8})^9 = e$, which implies that $o(g^{-8})=9$.

$o(g^{15})$ is equal to the order of the cyclic group $H=\langle g^{15}\rangle$. But by a theorem we in Durbin's book we have $|H| = 36/\mathrm{GCD}(36,15) = 36/3 = 12$. Hence $o(g^{15})=12$.

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

3a) Suppose $a + b\sqrt{2}$ and $(c + d\sqrt{2}) \in D$. Then
$(a + b\sqrt{2})+(c + d\sqrt{2})=(a+c)+(b+d)\sqrt{2} \in D$,
$(a + b\sqrt{2})-(c + d\sqrt{2})=(a-c)+(b-d)\sqrt{2} \in D$,
$(a + b\sqrt{2})(c + d\sqrt{2})=(ac+2bd)+(ad+bc)\sqrt{2} \in D$.
Hence D is a subring of $\mathbf{R}$ by the subring criterion.

3b) Suppose $a + b\sqrt{2} \in D\setminus\{0\}$. Then $1/(a + b\sqrt{2})=(a - b\sqrt{2})/(a + b\sqrt{2})(a - b\sqrt{2})=(a - b\sqrt{2})/(a^2-2b^2)= a/(a^2-2b^2)+(-b/(a^2-2b^2))\sqrt{2} \in D$. The subring D is thus a subfield of $\mathbf{R}$.

3c) Suppose $\sqrt{3}= a + b\sqrt{2} \in D$. Then, $3= (a + b\sqrt{2})^2=a^2+2b^2+2ab\sqrt{2}$ and $\sqrt{2}=(3- a^2-2b^2)/2ab \in \mathbf{Q}$ in case $ab\neq0$. If instead $a=0$, then $\sqrt{6}= 2b$ 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 $\sqrt{n}=p/q$ 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 $p(X^2)= a_0+a_1X^2+\ldots+a_nX^{2n}$ is a ring homomorphism. Indeed, if $q(X)=b_0+b_1X+\ldots+b_nX^n$ is another element in R, then

$\Phi(p(X)+ q(X))=(a_0+b_0)+ (a_1+b_1)X^2+\ldots+(a_n+b_n)X^{2n} =(a_0+a_1X^2+\ldots+a_nX^{2n})+ (b_0+b_1X^2+\ldots+b_nX^{2n})=$

$\Phi\,(p(X))+\Phi(q(X))$ or simply $\Phi(p(X)+q(X))=(p+q)(X^2)=p(X^2)+q(X^2)=\Phi(p(X))+\Phi(q(X))$.
Similarily, if we let $q(X)=b_0+b_1X+\ldots+b_mX^m$ and pq be the product of p an q in R, then
$\Phi(p(X)q(X))=(pq)(X^2)=p(X^2)q(X^2)=\Phi(p(X))\Phi(q(X))$.
Φ is injective as ker $\Phi=0$. It is also clear that Φ is not surjective as $X\notin\mathrm{Im}\,\Phi$.

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

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