MATHEMATICS
Univ. of Gothenburg and Chalmers University of Technology
Examination in algebra : MMG500 and MVE 150, 2019-08-21.
No aids are allowed. Telephone 031-772 5325.

1. Let R be the quotient ring $\mathbf{Z}_2[x]/(x^2+1)$. Write down the Cayley tables for addition and multiplication on R. 4p
(All cosets should be represented by binary polynomials of minimal degree.)

2. Find the subgroups of $\mathbf{Z}_2 \times \mathbf{Z}_4$. (There are eight.) 4p

3. Let G be the abelian group of all rotations of the unit circle $S^1=\{(\cos\theta, \sin\theta)\in\mathbf{R}^2 : 0\leq\theta<2\pi)\}$. Determine the number of elements of order one million in G. (Hint: Prove first that $G\approx\mathbf{R}/2\pi\mathbf{Z}$.) 4p

4. Let $\varepsilon=\cos(2\pi/3)+i\sin(2\pi/3)=(-1+i\sqrt{3})/2$ and D be the set of all complex numbers of the form $a+b\varepsilon$ with $a,b\in\mathbf{Z}$

a) Show that D is a subring of $\mathbf{C}$. 2p

b) Show that the integral domain D is Euclidean by means of the function $\delta(a+b\varepsilon)=|a+b\varepsilon|^2 = a^2-ab+b^2$ 3p

5. Formulate and prove the fundamental homomorphism theorem for groups. 4p

6. Show that the kernel of a ring homomorphism $\theta: R\to S$ is an ideal of R by verifying <u>all</u> conditions for a subset of R to be an ideal. 4p

The theorems in Durbin's book may be used to solve exercises 1–4, *but all claims that are made must be motivated.*

Solutions to examination in algebra : MMG500 /MVE 150, 2019-08-21.

1.

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\times$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	0	$x+1$
$x+1$	0	$x+1$	$x+1$	0

where all polynomials $p(x)$ should be interpreted as the coset $p(x)+(x^2+1)$ in $\mathbf{Z}_2[x]/(x^2+1)$

2. There are two trivial subgroups $\{([0], [0])\}$ and $\mathbf{Z}_2\times\mathbf{Z}_4$,
three cyclic subgroups of order 2 : $<([0], [2])>$, $<([1], [0])>$, and $<([1], [2])>$.
one non-cyclic subgroup $\mathbf{Z}_2\times<([2])>$ of order 4 given by the elements
$([0], [0])$, $([0], [2])$, $([1], [0])$ and $([1], [2])$.
and two cyclic subgroups of order 4 :
$<([0], [1])> =<([0], [3])>$ and $<([1], [1])> =<([1], [3])>$.

3. If we represent the points on the unit circle by complex number $e^{i\varphi}=\cos\varphi+i\sin\varphi$, $\varphi\in\mathbf{R}/2\pi\mathbf{Z}$, then a rotation on S^1 will send $e^{i\varphi}$ to $e^{i(\varphi+\alpha)}$ for some $\alpha\in\mathbf{R}/2\pi\mathbf{Z}$. The composition $e^{i\varphi}\to e^{i(\varphi+\alpha)}\to e^{i(\varphi+\alpha+\beta)}$ of two such rotations correspond to the sum $\alpha+\beta$ in $\mathbf{R}/2\pi\mathbf{Z}$ such that G is isomorphic to the additive group $A= \mathbf{R}/2\pi\mathbf{Z}$. But any coset $\alpha\in\mathbf{R}/2\pi\mathbf{Z}$ with $n\alpha=0$ in $\mathbf{R}/2\pi\mathbf{Z}$ can be represented by exactly one of the real numbers $\frac{k}{n}2\pi$ for some $k\in\{0,\ldots, n-1\}$ and $\frac{k}{n}2\pi+2\pi\mathbf{Z}$ is of order n in $\mathbf{R}/2\pi\mathbf{Z}$ if and only if $(k, n)=1$. If $n=10^6$, then $(k, n)=1$ if and only $k\equiv1,3,7$ or $9 \pmod{10}$. There are thus 4×10^5 elements of order 10^6 in $\mathbf{R}/2\pi\mathbf{Z}$ and in G.

4a) Let $a+b\varepsilon$ and $c+d\varepsilon$ be elements to D. Then,
$(a+b\varepsilon)+(c+d\varepsilon)=(a+c)+(b+d)\varepsilon\in D$,
$(a+b\varepsilon)-(c+d\varepsilon)=(a-c)+(b-d)\varepsilon\in D$ and
$(a+b\varepsilon)(c+d\varepsilon)=ac+(ad+bc)\varepsilon+bd\varepsilon^2=ac-bd +(ad+bc-bd)\varepsilon\in D$.

Hence R is a subring of $\mathbf{C}$ by the subring criterion.

4b) There are two conditions for a function $\delta: D\backslash\{0\}\to \mathbf{N}$ to be Euclidean. To verify these, let w and $z=a+b\varepsilon\in D\backslash\{0\}$. Then $\delta(z)\geq 1$ as $\delta(z)=a^2-ab+b^2\in\mathbf{Z}$ and $\delta(z)=|z|^2>0$. We have therefore that

(i) $\delta(wz)=|wz|^2=|w|^2|z|^2=\delta(w)\delta(z)\geq\delta(w)$

To prove the second property of Euclidean functions, we use that the fact the elements in D divide the complex plane into equilateral triangles with side 1. We may therefore approximate $w/z\in\mathbf{C}$ by an element $q\in D$ with $|w/z-q|<1$. For $r:=w-qz$ we have hence that

(ii) $\delta(r)=|w-qz|^2=|w/z-q|^2|z|^2<|z|^2=\delta(z)$,

which implies that D is a Euclidean domain.

5. See page 114 in Durbin's book.

6. See page 179 in Durbin's book.