University of Cergy-Pontoise **2010-2011**
L1-MI 2nd semester

Test nº 1 - Answers and Solutions

Question about course 1. $(R,+,\times)$ is a ring if it satisfies each of the following point

i) R is a nonempty set

ii) $+$ and $\times$ are binary operation on R

$$\forall (a,b)\in R^2,\ \begin{cases} a+b\in R \\ a\times b\in R \end{cases}$$

iii) $(R,+)$ is an abelian group, that is it satisfies each of the following point

$\forall (a,b,c)\in R^3,\ (a+b)+c=a+(b+c)$

$\exists 0\in R/\ \forall a\in R,\ a+0=0+a=a$

$\forall a\in R,\ \exists a'\in R/\ a+a'=a'+a=0$

$\forall (a,b)\in R^2,\ a+b=b+a$

iv) the binary operation $\times$ is associative

$\forall (a,b,c)\in R^3,\ (a\times b)\times c=a\times(b\times c)$

v) the binary operation $\times$ is distributive over the binary operation $+$

$$\forall (a,b,c)\in R^3,\ \begin{cases} a\times(b+c)=a\times b+a\times c \\ (b+c)\times a=b\times a+c\times a \end{cases}$$

Exercise 2. At first, $n=0$ gives

$$6^{2n+1}+2^{3n+1}=6^1+2^1=8=1+7\equiv 1\quad [7]$$

So the claim is true for $n=0$. Now assume the claim is true for a given integer $n\in\mathbb{N}$. We have

$$6^{2(n+1)+1}+2^{3(n+1)+1}=6^{2n+2+1}+2^{3n+3+1}=6^2\times 6^{2n+1}+2^3\times 2^{3n+1}=36\times 6^{2n+1}+8\times 2^{3n+1}$$

Using the division algorithm we get

$$\begin{cases} 36 &=& 5\times 7+1 &\equiv& 1 & [7] \\ 8 &=& 1\times 7+1 &\equiv& 1 & [7] \end{cases}$$

Then

$$\begin{aligned} 6^{2(n+1)+1}+2^{3(n+1)+1}=36\times 6^{2n+1}+8\times 2^{3n+1} &\equiv 1\times 6^{2n+1}+1\times 2^{3n+1} \quad [7] \\ &\equiv 6^{2n+1}+2^{3n+1} \quad [7] \end{aligned}$$

Consequently the claim is also true for $n+1$ since it is true for n by inductive assumption. The conclusion follows by induction.

Problem 3. 1. Obviously, if $a=b=0$ then $a+b\sqrt{2}=0$. Conversely, assume $a+b\sqrt{2}=0$. If $b\neq 0$ then we get $\sqrt{2}=\frac{-a}{b}$ which is a contradiction with $\sqrt{2}\notin\mathbb{Q}$. Consequently $b=0$ and $a=-b\sqrt{2}=0$.

2. A is a nonempty subset of $\mathbb{R}$ and $(\mathbb{R},+,\times)$ is a commutative unital ring (and even more a field). Moreover for every $x=a+b\sqrt{2}\in A$ and $y=c+d\sqrt{2}\in A$ we have

$$\left\{\begin{array}{rcccl} x-y & = & (a+b\sqrt{2})-(c+d\sqrt{2}) & = & (a-c)+(b-d)\sqrt{2}\in A \\ x\times y & = & (a+b\sqrt{2})\times(c+d\sqrt{2}) & = & (ac+2bd)+(ad+bc)\sqrt{2}\in A \end{array}\right.$$

The first point shows that $(A,+)$ is a subgroup of $(\mathbb{R},+)$ and the second point shows that $\times$ is a binary operation on A. Consequently $(A,+,\times)$ is a subring of $(\mathbb{R},+,\times)$ and in particular $(A,+,\times)$ is a commutative ring. Furthermore $1=1+0\sqrt{2}\in A$ is the multiplicative identity, so $(A,+,\times)$ is unital.

Now we need to find a nonzero element in A which has no multiplicative inverse in A. For instance, assume $\sqrt{2}=0+1\sqrt{2}\in A$ has a multiplicative inverse denoted by $a+b\sqrt{2}$, that is

$$\sqrt{2}\times(a+b\sqrt{2})=2b+a\sqrt{2}=1$$

In particular we get $(2b-1)+a\sqrt{2}=0$ and the first point of this problem implies $2b-1=0$ and $a=0$. But $2b-1=0$ is a contradiction with $b\in\mathbb{Z}$ (2 has no multiplicative inverse in $\mathbb{Z}$). It follows that $\sqrt{2}\neq 0$ has no multiplicative inverse in A and then $(A,+,\times)$ is not a field.

3. (a) Let $x=a+b\sqrt{2}\in A$ and $y=c+d\sqrt{2}$. Then

$$N(x)=x\times\varphi(x)=(a+b\sqrt{2})\times(a-b\sqrt{2})=a^2-ab\sqrt{2}+ab\sqrt{2}+2b^2=a^2-2b^2\in\mathbb{Z}$$

$$\begin{array}{rrcl} \text{and} & N(xy) & = & N\left((a+b\sqrt{2})(c+d\sqrt{2})\right) \\ & & = & N\left((ac+2bd)+(ad+bc)\sqrt{2}\right) \\ & & = & (ac+2bd)^2-2(ad+bc)^2 \\ & & = & a^2c^2+4abcd+4b^2d^2-2a^2d^2-4abcd-2b^2c^2 \\ & & = & a^2c^2-2b^2c^2-2a^2d^2+4b^2d^2 \\ & & = & (a^2-2b^2)(c^2-2d^2) \\ & & = & N(x)N(y) \end{array}$$

(b) Assume $x\in A$ has a multiplicative inverse in A denoted by x^{-1}. Using the previous results we get

$$N(x)N(x^{-1})=N(xx^{-1})=N(1)=1$$

In particular, $N(x)\in\mathbb{Z}$ has a multiplicative inverse $N(x^{-1})\in\mathbb{Z}$. That implies either $N(x)=1$ or $N(x)=-1$ (only these two integers have multiplicative inverse in $\mathbb{Z}$).

Conversely, if $N(x)=x\times\varphi(x)$ is equal to 1 or -1 then x has a multiplicative inverse in A which is respectively $\varphi(x)$ or $-\varphi(x)$.

Problem 4. Consider the following map for a given number $\lambda\in\mathbb{R}^*$

$$\begin{array}{rccc} f_\lambda: & \mathbb{R}^2 & \longrightarrow & \mathbb{R}^2 \\ & (x,y) & \longmapsto & \left(\lambda x,\dfrac{y}{\lambda}\right) \end{array}$$

1. $(\mathbb{R}^2,+)$ is an abelian group. Let (x,y) and (x',y') be two points in $\mathbb{R}^2$. Then

$$\begin{array}{rcl} f_\lambda\left((x,y)+(x',y')\right) & = & f_\lambda\left((x+x',y+y')\right) \\ & = & \left(\lambda(x+x'),\dfrac{y+y'}{\lambda}\right) \\ & = & \left(\lambda x,\dfrac{y}{\lambda}\right)+\left(\lambda x',\dfrac{y'}{\lambda}\right) \\ & = & f_\lambda\left((x,y)\right)+f_\lambda\left((x',y')\right) \end{array}$$

So f_λ is a group endomorphism from $(\mathbb{R}^2, +)$ to itself.

2. (a) Let (x, y) be a point in $\mathbb{R}^2$. Then

$$f_\lambda \circ f_\mu(x, y) = f_\lambda\left(f_\mu(x, y)\right) = f_\lambda\left(\mu x, \frac{y}{\mu}\right) = \left(\lambda\mu x, \frac{y}{\lambda\mu}\right) = f_{\lambda\mu}(x, y)$$

Consequently, $f_\lambda \circ f_\mu = f_{\lambda\mu}$.

(b) Since the product of two numbers in $\mathbb{R}^*$ stays in $\mathbb{R}^*$, we have

$$\begin{array}{rcl} \circ : \mathcal{F} \times \mathcal{F} & \longrightarrow & \mathcal{F} \\ (f_\lambda, f_\mu) & \longmapsto & f_\lambda \circ f_\mu = f_{\lambda\mu} \in \mathcal{F} \end{array}$$

In other words, $\circ$ is a binary operation on $\mathcal{F}$.

(c) The associativity of $(\mathcal{F}, \circ)$ comes from that one of $(\mathbb{R}^*, \times)$

$$\forall (\lambda, \mu, \nu) \in (\mathbb{R}^*)^3,\ (f_\lambda \circ f_\mu) \circ f_\nu = f_{\lambda\mu} \circ f_\nu = f_{(\lambda\mu)\nu} = f_{\lambda(\mu\nu)} = f_\lambda \circ f_{\mu\nu} = f_\lambda \circ (f_\mu \circ f_\nu)$$

$f_1 : (x, y) \mapsto (x, y)$ is obviously the identity element of $(\mathcal{F}, \circ)$. Moreover for every $\lambda \in \mathbb{R}^*$ we have

$$f_\lambda \circ f_{1/\lambda} = f_{\lambda/\lambda} = f_1 \quad \text{and} \quad f_{1/\lambda} \circ f_\lambda = f_{\lambda/\lambda} = f_1$$

In particular, every $f_\lambda \in \mathcal{F}$ has an inverse element (which is $f_{1/\lambda} \in \mathcal{F}$). Finally $(\mathcal{F}, \circ)$ is a group.

3. (a) Let λ and μ be two numbers in $\mathbb{R}^*$. We have

$$h(\lambda\mu) = f_{\lambda\mu} = f_\lambda \circ f_\mu = h(\lambda) \circ h(\mu)$$

Then h is a group homomorphism from $(\mathbb{R}^*, \times)$ to $(\mathcal{F}, \circ)$. Moreover h is a surjective map by definition of $\mathcal{F}$ and an injective map since

$$\forall (\lambda, \mu) \in (\mathbb{R}^*)^2,\ h(\lambda) = h(\mu) \Rightarrow f_\lambda = f_\mu \Rightarrow f_\lambda(1, 0) = f_\mu(1, 0) \Rightarrow (\lambda, 0) = (\mu, 0) \Rightarrow \lambda = \mu$$

Finally, h is a bijective map and hence a group isomorphism from $(\mathbb{R}^*, \times)$ to $(\mathcal{F}, \circ)$.

(b) Since $(\mathbb{R}^*, \times)$ is an abelian group, we have

$$\forall (\lambda, \mu) \in (\mathbb{R}^*),\ f_\lambda \circ f_\mu = h(\lambda) \circ h(\mu) = h(\lambda\mu) = h(\mu\lambda) = h(\mu) \circ h(\lambda) = f_\mu \circ f_\lambda$$

Then the binary operation $\circ$ is commutative on $\mathcal{F}$ or equivalently, $(\mathcal{F}, \circ)$ is an abelian group.