Solutions of exercise sheet 6

The content of the marked exercises **(*)** should be known for the exam.

1. Consider the set

$$\mathbb{H} = \left\{ \begin{pmatrix} \alpha & -\bar{\beta} \\ \beta & \bar{\alpha} \end{pmatrix} : \alpha, \beta \in \mathbb{C} \right\} \subset M_2(\mathbb{C}).$$

Prove:

1. $\mathbb{H}$ is a subring of $M_2(\mathbb{C})$, the ring of matrices with entrywise sum and row-times-column multiplication;
2. $\mathbb{H}$ is a division ring (it is called the ring of Hamilton quaternions);
3. $\mathbb{H}$ is non-commutative;
4. $\mathbb{H}$ is a $\mathbb{R}$-vector space of dimension 4, and there exists an $\mathbb{R}$-basis $(\mathbb{1}, \mathbb{i}, \mathbb{j}, \mathbb{k})$ for $\mathbb{H}$ such that $\mathbb{i}^2 = \mathbb{j}^2 = \mathbb{k}^2 = -\mathbb{1}$, $\mathbb{i}\mathbb{j} = \mathbb{k} = -\mathbb{j}\mathbb{i}$, $\mathbb{j}\mathbb{k} = \mathbb{i} = -\mathbb{k}\mathbb{j}$ and $\mathbb{k}\mathbb{i} = \mathbb{j} = -\mathbb{i}\mathbb{k}$.

Solution:

1. To prove that $\mathbb{H}$ is a subring of $M_2(\mathbb{C})$, we have to check that it is a subgroup with respect to addiction and a submonoid with respect to multiplication (that is, it contains 1 and is stable under multiplication), since the distributive property is inherited from the superset $M_2(\mathbb{C})$.

   First, notice that chosing $\alpha = \beta = 0$ one obtains the zero matrix, which is the neutral element of the entrywise addition, and chosing $\alpha = 1$ and $\beta = 0$ one obtains the identity matrix, which is the neutral element of the row-times-column multiplication. Hence $0_{M_2(\mathbb{C})}, 1_{M_2(\mathbb{C})} \in \mathbb{H}$.

   Now, for all $\alpha_i, \beta_i \in \mathbb{C}$, $i = 1, 2$, we have (using the facts that complex conjugation respects sum and multiplication and that $\bar{\bar{z}} = z$ for every $z \in \mathbb{C}$):

   $$\begin{pmatrix} \alpha_1 & -\bar{\beta_1} \\ \beta_1 & \bar{\alpha_1} \end{pmatrix} - \begin{pmatrix} \alpha_2 & -\bar{\beta_2} \\ \beta_2 & \bar{\alpha_2} \end{pmatrix} = \begin{pmatrix} \alpha_1 - \alpha_2 & -\overline{(\beta_1 - \beta_2)} \\ \beta_1 - \beta_2 & \overline{(\alpha_1 - \alpha_2)} \end{pmatrix} \in M_2(\mathbb{C}), \text{ and}$$

   $$\begin{pmatrix} \alpha_1 & -\bar{\beta_1} \\ \beta_1 & \bar{\alpha_1} \end{pmatrix} \cdot \begin{pmatrix} \alpha_2 & -\bar{\beta_2} \\ \beta_2 & \bar{\alpha_2} \end{pmatrix} = \begin{pmatrix} \alpha_1\alpha_2 - \bar{\beta_1}\beta_2 & -\overline{(\bar{\alpha_1}\beta_2 + \beta_1\alpha_2)} \\ \bar{\alpha_1}\beta_2 + \beta_1\alpha_2 & \overline{\alpha_1\alpha_2 - \bar{\beta_1}\beta_2} \end{pmatrix} \in M_2(\mathbb{C}).$$

   This proves that $\mathbb{H}$ is a subring of $M_2(\mathbb{C})$, as desired.

2. Let $\mathbb{a} \in \mathbb{H}$. We know from linear algebra that $\mathbb{a}$ has an inverse in $M_2(\mathbb{C})$ if and only if $\det(\mathbb{a}) \neq 0$. Supposing that $\mathbb{a} = \begin{pmatrix} \alpha & -\bar{\beta} \\ \beta & \bar{\alpha} \end{pmatrix}$, we have that $\det(\mathbb{a}) = \alpha\bar{\alpha} + \beta\bar{\beta} = |\alpha|^2 + |\beta|^2 \in \mathbb{R}_{\geq 0}$, which is zero only when $\alpha = \beta = 0$, as the absolute value of any non-zero complex numbers is always positive. Hence if $\mathbb{a} \in \mathbb{H} \setminus \{0\}$, then $\mathbb{a}$ has an inverse matrix in $M_2(\mathbb{C})$,

$$\mathbb{a}^{-1} = \begin{pmatrix} \alpha & -\bar{\beta} \\ \beta & \bar{\alpha} \end{pmatrix}^{-1} = \frac{1}{|a|^2 + |b|^2} \begin{pmatrix} \bar{\alpha} & \bar{\beta} \\ -\beta & \alpha \end{pmatrix} = \begin{pmatrix} \alpha_0 & -\bar{\beta_0} \\ \beta_0 & \bar{\alpha_0} \end{pmatrix} \in \mathbb{H},$$

where one puts $\alpha_0 = \bar{\alpha}(|a|^2 + |b|^2)^{-1}$ and $\beta_0 = -\beta(|a|^2 + |b|^2)^{-1}$. In conclusion, every non-zero matrix in $\mathbb{H}$ has an inverse in $\mathbb{H}$, so that $\mathbb{H}$ is a division ring.

3. From the multiplication formula above it is already clear that interchanging the indexes 1 and 2 we can get a different result. For example, take two matrices $\mathbb{a}_1$ and $\mathbb{a}_2$ corresponding to chosing $\alpha_1 = \beta_1 = \alpha_2 = i$, and $\beta_2 = 1$. Then the upper-left entry of $\mathbb{a}_1 \cdot \mathbb{a}_2$ is $\alpha_1\alpha_2 - \bar{\beta_1}\beta_2 = -1 + i$, while the upper-left entry of $\mathbb{a}_2 \cdot \mathbb{a}_1$ is $\alpha_1\alpha_2 - \beta_1\bar{\beta_2} = -1 - i$, so that $\mathbb{a}_1 \cdot \mathbb{a}_2 \neq \mathbb{a}_2 \cdot \mathbb{a}_1$. Hence $\mathbb{H}$ is not a commutative ring.

4. $\mathbb{H}$ is an $\mathbb{R}$ vector space of dimension 4 because every element $\mathbb{a} \in \mathbb{H}$ is determined by two complex numbers, and a complex numbers are determined by two real numbers. This can be formalized by considering the map

$$\begin{aligned} \phi : \mathbb{R}^4 &\to \mathbb{H} \\ (a, b, c, d) &\mapsto \begin{pmatrix} a + ib & c + id \\ -c + id & a - ib \end{pmatrix} \end{aligned}$$

It is immediately checked that this map respects sum and multiplication by scalars in $\mathbb{R}$, so that it is an $\mathbb{R}$-linear map. Moreover, it is clear that the only quadruple mapped to the zero matrix is $(0, 0, 0, 0)$, so that the kernel is trivial and ϕ is injective. Surjectivity is also evident, so that ϕ is an isomorphism of $\mathbb{R}$-vector space and $\dim_{\mathbb{R}}(\mathbb{H}) = 4$.

Mapping the canonical basis $(\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \mathbf{e}_4)$ of $\mathbb{R}^4$ (where $\mathbf{e}_i$ is the quadruple with 1 in the i-th position and 0 elsewhere) via ϕ, on gets a basis for $\mathbb{H}$. This basis is

$$\mathcal{B} = \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \right).$$

Then one has

$$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}^2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}^2 = -\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

$$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \text{ and}$$

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}.$$

See next page!

This means that rewriting the basis above as $\mathcal{B} = (\mathbb{1}, \mathbb{i}, \mathbb{j}, \mathbb{k})$, one has the properties $\mathbb{i}^2 = \mathbb{j}^2 = \mathbb{k}^2 = -\mathbb{1}$, $\mathbb{i}\mathbb{j} = \mathbb{k}$, $\mathbb{j}\mathbb{k} = \mathbb{i}$ and $\mathbb{k}\mathbb{i} = \mathbb{j}$. Then the multiplication in the reversed order automatically satisfy the required condition. Indeed all the three matrices $\mathbb{i}, \mathbb{j}, \mathbb{k}$ satisfy the equality $\mathbb{x}^2 = -\mathbb{1}$ in $\mathbb{H}$, which is equivalent (assuming invertibility of $\mathbb{x}$) to $\mathbb{x}^{-1} = -\mathbb{x}$. Then the equality $\mathbb{i}\mathbb{j} = \mathbb{k}$ gives $\mathbb{j}^{-1}\mathbb{i}^{-1} = \mathbb{k}^{-1}$, i.e. $\mathbb{j}\mathbb{i} = -\mathbb{k}$, and similarly can be done for the other equalities.

2. Let X be a set, A a commutative ring and $C(X, A) = \{f : X \to A\}$ be the ring of functions $X \to A$, with pointwise sum and multiplication. Given a subset $Y \subseteq X$, define

$$I_Y = \{f \in C(X, A) : f|_Y = 0\}.$$

Prove that I_Y is an ideal, and prove that it is principal by finding a generator.

Solution:

Notice that if $X = \varnothing$, then $C(X, A)$ only contains the empty map, so that it is the zero ring (as it has only one element), and I_Y is the zero ideal, which is principal (generated by 0). Hence we will exclude the case in which $X = \varnothing$.

As seen in class, the restriction map $\varrho : C(X, A) \to C(Y, A)$ sending $f \mapsto f|Y$ is a ring homomorphism. Then $\ker(\varrho) = I_Y$ by definition, so that I_Y is an ideal in $C(X, A)$.

A generator of I_Y as a principal ideal needs to be a map $f : X \to A$ which vanishes on Y and can reach any combination of values in $X \setminus Y$ if multiplied by some other function on X. This is actually equivalent to asking f to be such that for some function $g : X \to A$ one has $f \cdot g = 1$ on $X \setminus Y$ (since multiplying $f \cdot g$ with all the function one then gets every possible combination of values on $X \setminus Y$), in particular, the function

$$f(x) = \begin{cases} 1 & \text{if } x \in X \setminus Y \\ 0 & \text{if } x \in Y \end{cases}$$

does the job (with $g = 1$). Then $I_Y = (f)$, so that I_Y is principal.

3. We say that a ring A is simple if $A \neq 0$ and the only ideals of A are 0 and A. Prove: $M_n(\mathbb{R})$ is a simple ring for every $n \in \mathbb{Z}_{>0}$.

Solution:

Of course $M_n(\mathbb{R}) \neq 0$. Now suppose that I is an ideal of $M_n(\mathbb{R})$ and that $I \neq 0$. We want to prove that $I = M_n(\mathbb{R})$. This is equivalent to proving that I contains the identity matrix. Since $I \neq 0$, there exists a matrix $C \in I$ which is not zero in every entry, and $(C) \subseteq I$. The idea is to build the identity matrix starting from C using operations under which ideals are stable, that is, internal sum and multiplication with elements of $M_n(\mathbb{R})$ (on both sides).

It is very useful to be able to move elements of a matrix using multiplication, so that we can move a non-zero entry of C. In order to do this, for each pair of indexes

Please turn over!

$1 \leq \lambda, \mu \leq n$ consider the matrix $S_{\lambda,\mu}$ which has value 1 in the entry of position (λ, μ) (row, column), and zero everywhere else. To describe it easily, we use Kronecher's delta function on pairs of indexes between 1 and n, defined as

$$\delta_\alpha^\beta = \begin{cases} 1 & \text{if } \alpha = \beta \\ 0 & \text{else.} \end{cases}$$

Then the matrix $S_{\lambda,\mu}$ can be written as $S_{\lambda,\mu} = (\delta_i^\lambda \delta_j^\mu)_{i,j}$, where the row and column indexes range in $1 \leq i, j \leq n$. Then we can multiply $S_{\lambda,\mu}$ with a matrix $B = (b_{ij})_{i,j}$ obtaining the following:

$$S_{\lambda,\mu} \cdot B = \left(\sum_{k=1}^{n} \delta_i^\lambda \delta_k^\mu b_{kj} \right)_{i,j} = \left(\delta_i^\lambda b_{\mu j} \right)_{i,j}$$

$$B \cdot S_{\lambda,\mu} = \left(\sum_{k=1}^{n} b_{ik} \delta_k^\lambda \delta_j^\mu \right)_{i,j} = \left(b_{i\lambda} \delta_j^\mu \right)_{i,j}.$$

Putting the two formulas together (paying attention to the indexes) we get

$$S_{\lambda_1,\mu_1} \cdot B \cdot S_{\lambda_2,\mu_2} = \left(\delta_i^{\lambda_1} b_{\mu_1 \lambda_2} \delta_j^{\mu_2} \right)_{i,j}$$

and this is the matrix which in the position (λ_1, μ_2) has entry $b_{\mu_1 \lambda_2}$ and has entry zero everywhere else. Now let $C = (c_{i,j})_{i,j} \in I$ be a non-zero matrix, and let (u, v) indexes such that $c_{u,v} \in \mathbb{R}^\times$. Then applying the formula above, one has

$$I \ni \sum_{k=1}^{n} S_{k,u} \cdot B \cdot S_{v,k} = c_{u,v} \cdot \mathbb{1}_m$$

Multiplying this matrix by the scalar matrix with $c_{u,v}^{-1}$ in the diagonal and 0 elsewhere we get that $\mathbb{1}_m \in I$, so that $I = \mathbb{R}$.

4. Let $A \neq 0$ be a ring. We say that $e \in A$ is *idempotent* if $e^2 = e$. We say that an idempotent element $e \in A$ is non-trivial if $e \notin \{0, 1\}$.

1. Prove: if $e \in A$ is idempotent, then $1 - e$ is also idempotent.
2. Suppose that $e \neq 1$ is idempotent in A. Prove: e is not a unit of A.
3. Prove that if $e \in A$ is idempotent, then $B = eAe = \{eae : a \in A\}$, endowed with sum and multiplications from A, is a ring with $0_B = 0_A$ and $1_B = e$.
4. Find a non-trivial idempotent element of $A = \mathbb{Z}/10\mathbb{Z}$.

Solution:

1. Using distributivity and the fact that $e = e^2$, we have $(1 - e)^2 = 1 - e - e + e^2 = 1 - e - e + e = 1 - e$, so that $1 - e$ is idempotent.

See next page!

2. We have that $e(1-e) = e - e^2 = e - e = 0$. If e has an inverse of d, then $0 = d \cdot 0 = de(1-e) = 1 \cdot (1-e) = 1 - e$, so that $e = 1$, contradiction.
3. For every $a_1, a_2 \in A$ we have $ea_1e + ea_2e = e(a_1 + a_2)e \in eAe$ and $ea_1e \cdot ea_2e = e(a_1ea_2)e$, so that B is closed under sum and multiplication in A. Since $B \subseteq A$, associativity of sum and product and distributivity are inherited from A. Also, $0_A = e \cdot 0_A \cdot e \in B$, so that it is the neutral element 0_B of the addition in B. Clearly $-eae = e(-a)e \in eAe$, so that B is a subgroup with respect to addition. Then one easily sees that $e = e \cdot 1_A \cdot e \in eAe$ is neutral with respect to the multiplication, so that B is a ring with identity $1_B = e$.
4. We have that $[5]^2 = [25] = [5]$, so that $[5]$ is a non-trivial idempotent element.

5. (*) Consider the set

$$X = \{(f, \varepsilon) | \varepsilon \in \mathbb{R}_{>0}, f :]-\varepsilon, \varepsilon[\to \mathbb{C} \text{ continuous map}\}.$$

Define a relation $\sim$ on X via

$$(f_1, \varepsilon_1) \sim (f_2, \varepsilon_2) \iff (\ \exists \varepsilon \in \mathbb{R}_{>0},\ \varepsilon \leq \min(\varepsilon_1, \varepsilon_2) :\ f_1|_{]-\varepsilon,\varepsilon[} = f_2|_{]-\varepsilon,\varepsilon[}\ ).$$

1. Show that $\sim$ is an equivalence relation. We write $[(f, \varepsilon)]$ for the class of (f, ε), and $A = X/\sim$.
2. Show that the following are well defined maps $A \times A \to A$, i.e. binary operations on A:

$$\begin{aligned}
&[(f_1, \varepsilon_1)] + [(f_2, \varepsilon_2)] = [(f_1|_{]-\varepsilon,\varepsilon[} + f_2|_{]-\varepsilon,\varepsilon[}, \varepsilon)],\\
&[(f_1, \varepsilon_1)] \cdot [(f_2, \varepsilon_2)] = [(f_1|_{]-\varepsilon,\varepsilon[} \cdot f_2|_{]-\varepsilon,\varepsilon[}, \varepsilon)],\\
&\text{where } \varepsilon = \min(\varepsilon_1, \varepsilon_2),
\end{aligned}$$

   and that they define a ring structure on A with $0_A = [(0, 1)]$ and $1_A = [(1, 1)]$.
3. Show that $(f, \varepsilon) \mapsto f(0)$ defines a ring homomorphism $A \to \mathbb{C}$. Deduce that $I = \{[(f, \varepsilon)] | f(0) = 0\}$ is an ideal of A, and that $A/I \cong \mathbb{C}$.
4. Prove: $A^\times = A \setminus I$.

The ring A we defined is called the ring of "germs of continuous functions at 0".

Solution (sketch):

Notation: we denote $J(\varepsilon) =]-\varepsilon, \varepsilon[\subseteq \mathbb{R}$, for every $\varepsilon \in \mathbb{R}_{>0}$.

1.
   - Reflexivity is clear since if we take two equal functions defined on a same interval $J(\varepsilon)$, then we can "restrict" them to $J(\varepsilon)$, obtaining two equal functions.
   - Symmetry is also clear because the equality $f_1|_{]-\varepsilon,\varepsilon[} = f_2|_{]-\varepsilon,\varepsilon[}$ in the definition of $\sim$ is symmetric in f_1 and f_2.

Please turn over!

- Transitivity: Suppose we have $(f_1, \varepsilon_1) \sim (f_2, \varepsilon_2)$ and $(f_1, \varepsilon_2) \sim (f_2, \varepsilon_3)$. By taking the minimal of the two ε that we need to consider in the definition, we have $f_1|_{J(\varepsilon)} = f_2|_{J(\varepsilon)}$ and $f_2|_{J(\varepsilon)} = f_3|_{J(\varepsilon)}$ are two equalities in the set of continuous functions $J(\varepsilon) \to \mathbb{C}$, so that $f_1|_{J(\varepsilon)} = f_3|_{J(\varepsilon)}$, giving $(f_1, \varepsilon_1) \sim (f_3, \varepsilon_3)$.

Hence $\sim$ is a equivalence relation.

2. First, notice that summing and multiplying continuous function we have always a continuous function, so that what we need to prove in order to say that the operations are well-defined is that the definition given do not depend on the choice of representatives in X. Suppose $(f_i, \varepsilon_i) \sim (f'_i, \varepsilon'_i)$, for $i = 1, 2$, and let $\varepsilon = \min(\varepsilon_1, \varepsilon_2)$ and $\varepsilon' = \min(\varepsilon'_1, \varepsilon'_2)$, and $\delta = \min(\varepsilon, \varepsilon')$. We want to prove that $(f_1|_{J(\varepsilon)} + f_2|_{J(\varepsilon)}, \varepsilon) \sim (f_1|_{J(\varepsilon)} + f_2|_{J(\varepsilon)}, \varepsilon)$, and the same for the multiplication. This is easily done by restricting both sides to $J(\delta)$, and using compatibility of restriction with ring operations. Then it is immediate to check that $[(0, 1)]$ and $[(1, 1)]$ are respectively zero and unity of A just using the given definitions of sum and multiplication. Associativity of the two operations and distributivity are induced by the corresponding properties on the rings of continuous functions from $J(\varepsilon)$ to $\mathbb{C}$ for every $\varepsilon > 0$ (which is a subring of $C(J(\varepsilon), \mathbb{C})$, using the notation of Exercise 2).

3. Since 0 is contained in all symmetric interval $J(\delta)$ to which one may restricts functions, the value in 0 of two equivalent germs is the same, so that $f(0) \in \mathbb{C}$ is well-defined for every $[(f, \varepsilon)] \in A$. It is then immediate to check that the resulting map $A \to \mathbb{C}$ respects group operations and maps $1_A \to 1_{\mathbb{C}}$. This map is surjective, since any complex value $\lambda \in \mathbb{C}$ is obtained evaluating at zero the constant germ $[(\lambda, 1)]$. It is immediate to check that I is the kernel of this ring map, so that it is an ideal of A, and $A/I \cong \mathbb{C}$ by the First Isomorphism Theorem for rings.

4. If $[(f, \varepsilon)]$ is a unit, then it is easy to see that $f(0) \neq 0$. Conversely, assume that $[(f, \varepsilon)]$ is a germ with $f(0) \neq 0$. Then continuity gives an open neighborhood $J(\delta) \subseteq \mathbb{R}$ of 0 where the function has value lying in the open subset $\mathbb{C} \setminus \{0_{\mathbb{C}}\}$, and then the germ $[(1/f, \delta)]$ is the inverse of $[(f, \varepsilon)]$. In conclusion, $A^\times = A \setminus I$.