D-MATH | Algebra I | HS 14

Prof. Emmanuel Kowalski

Solutions of exercise sheet 7

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

1. (*) Let R be a ring. Similarly as for groups, given two R-linear maps $\alpha : L \to M$ and $\beta : M \to N$ we say that

$$L \xrightarrow{\alpha} M \xrightarrow{\beta} N$$

is an exact sequence of R-modules if $\mathrm{Im}(\alpha) = \ker(\beta)$, and given

$$(**) \qquad \cdots \longrightarrow M_{n-2} \xrightarrow{\alpha_{n-2}} M_{n-1} \xrightarrow{\alpha_{n-1}} M_n \xrightarrow{\alpha_n} M_{n+1} \xrightarrow{\alpha_{n+1}} M_{n+2} \longrightarrow \cdots$$

we say that $(**)$ is an exact sequence if $M_{i-1} \xrightarrow{\alpha_{i-1}} M_i \xrightarrow{\alpha_i} M_{i+1}$ is an exact sequence for every i. We call a short exact sequence of R-modules any exact sequence of R-modules of the form

$$0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0.$$

1. Show that in the exact sequence above N is determined, up to isomorphism, by the map α.
2. Find a short exact sequence as above, with $R = \mathbb{Z}$, $L = \mathbb{Z}$, $M = \mathbb{Z} \oplus \bigoplus_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$, and $\alpha(n) = 2n + 0$.
3. Find a short exact sequence as above, with $R = \mathbb{R}$, $L = M \oplus M$ and $M \neq 0$.

Solution:

1. Since by exactness we have $\mathrm{Im}(\beta) = \ker(N \to 0) = N$ and $\ker(\beta) = \mathrm{Im}(\alpha)$, the First Isomorphism Theorem applied to the map β gives $M/\mathrm{Im}(\alpha) = M/\ker(\beta) \cong \mathrm{Im}(\beta) = N$, so that N is determined, up to isomorphism, by the map α. Notice that $\ker(\alpha) = \mathrm{Im}(0 \to L) = 0$, so that α is injective and $L \cong \mathrm{Im}(\alpha)$. [Calling $\bar\beta$ the isomorphism $M/\mathrm{Im}(\alpha) \to N$ we just used, the First Isomorphism Theorems can be explicited by saying that $\bar\beta(m + \mathrm{Im}(\alpha)) = \beta(m)$, so that $\beta = \bar\beta \circ \pi_{\mathrm{Im}(\alpha)}$, where $\pi_{\mathrm{Im}(\alpha)}$ is the canonical projection $M \to M/\mathrm{Im}(\alpha)$. Then we have an *isomorphism of exact sequences*, in the sense that the two squares in the following diagram commute:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & L & \xrightarrow{\alpha} & M & \xrightarrow{\pi} & M/\mathrm{Im}(\alpha) & \longrightarrow & 0 \\
 & & \Big\downarrow{\scriptstyle \mathrm{id}_L} & & \Big\downarrow{\scriptstyle \mathrm{id}_M} & & \Big\downarrow{\scriptstyle \bar\beta'} & & \\
0 & \longrightarrow & L & \xrightarrow{\alpha} & M & \xrightarrow{\beta} & N & \longrightarrow & 0
\end{array}$$

This means that the isomorphism $\bar\beta'$ is determined by β and viceversa.]

Please turn over!

2. By previous point, we can take $N \cong M/\operatorname{Im}(\alpha)$. We have

$$(*)\ M/\operatorname{Im}(\alpha) \cong \frac{\mathbb{Z} \oplus \bigoplus_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}}{2\mathbb{Z} \oplus 0} \cong \mathbb{Z}/2\mathbb{Z} \oplus \bigoplus_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z} \cong \bigoplus_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z} =: N$$

The second isomorphism is just a translation by one of the index, while the first isomorphism comes from the more general fact that given R-modules A_i, $i \in I$ and submodules $A_i' \leq A_i$, the following is a surjective R-linear map:

$$(**)\ \bigoplus_{i \in I} A_i \to \bigoplus_{i \in I} (A_i/A_i')$$
$$a_{i_1} + \cdots + a_{i_m} \mapsto (a_{i_1} + A_{i_1}) + \cdots + (a_{i_m} + A_{i_m})$$

whose kernel is precisely $\bigoplus_{i \in I} A_i'$.
Composing the resulting isomorphism $(*)$ with the natural projection $M \to M/\operatorname{Im}(\alpha)$ we obtain an R-linear map (notice that every element in a infinite direct sum is always equal to a finite sum of elements in the direct summands):

$$\beta : M = \mathbb{Z} \oplus \bigoplus_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z} \to \bigoplus_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z} = N$$
$$t + a_1 + a_2 + \cdots a_k \mapsto b_1 + b_2 + \cdots + b_{k+1}, \text{ where}$$
$$b_1 = t \text{ and } b_{i-1} = a_i \text{ for } i = 1, \ldots, k+1$$

With this β and N, we have exactness by construction.

3. Since we want to construct an injection of non-zero $\mathbb{R}$-vector spaces $M \oplus M \to M$, we need $0 < 2\dim_{\mathbb{R}}(M) = \dim_{\mathbb{R}}(M \oplus M) \leq \dim_{\mathbb{R}}(M)$, which can only hold when M is infinite dimensional. We then suppose that $M = \bigoplus_{i \in \mathbb{Z}} \mathbb{R} \cdot e_i$, and by taking two copies $(e_i')_{i \in \mathbb{Z}}, (e_i'')_{i \in \mathbb{Z}}$ of the basis $(e_i')_{i \in \mathbb{Z}}$ we can write $M \oplus M = \bigoplus_{i \in \mathbb{Z}} \mathbb{R} \cdot e_i' \oplus \bigoplus_{i \in \mathbb{Z}} \mathbb{R} \cdot e_i''$.
Then we can define many $\mathbb{R}$-linear injective maps $\alpha : M \oplus M \to M$, with a resulting N that can vary. Recall that defining a $\mathbb{R}$-linear map of $\mathbb{R}$-vector space is equivalent to choosing images for a basis of the domain.

   a) Define α by imposing $\alpha(e_i') = e_{3i+1}$ and $\alpha(e_i'') = e_{3i+2}$. Then $\operatorname{Im}(\alpha) = \oplus_{i \in \mathbb{Z} \setminus 3\mathbb{Z}} \mathbb{R} \cdot e_i$, so that by the isomorphism $(**)$ above we have $M/\ker(\alpha) \cong \oplus_{i \in 3\mathbb{Z}} \mathbb{R} \cdot e_i$, which is easily seen to be isomorphic to M by mapping e_{3k} to e_k. Hence one can take $N = M$, and the surjective $\mathbb{R}$-linear map

$$\beta : M \to N$$
$$e_{3k} \mapsto e_k$$
$$e_h \mapsto 0 \text{ if } 3 \nmid h.$$

   Then $\operatorname{Im}(\alpha) = \ker(\beta)$, and we have a short exact sequence

$$0 \to M \oplus M \xrightarrow{\alpha} M \xrightarrow{\beta} M \to 0.$$

See next page!

b) Define α by imposing $\alpha(e_i') = e_{2i}$ and $\alpha(e_i'') = e_{2i+1}$. Then $\mathrm{Im}(\alpha) = M$, meaning that α is an isomorphism, and by Point 1 we get $N = 0$, so that we have a short exact sequence

$$0 \to M \oplus M \xrightarrow{\alpha} M \xrightarrow{\beta} 0 \to 0.$$

c) Let n be a positive integer and take bijections $\gamma : \mathbb{Z} \to \mathbb{Z}_{\leq 0}$ and $\chi : \mathbb{Z} \to \mathbb{Z}_{>n}$ - this can be done by "counting" (with non-positive integers and with integers bigger than n) the elements of $\mathbb{Z}$. Then define α by imposing $\alpha(e_i') = e_{\gamma(i)}$ and $\alpha(e_i'') = e_{\chi(i)}$, so that α is injective and $\mathrm{Im}(\alpha) = \oplus_{i\in\mathbb{Z}_{\leq 0}\cup\mathbb{Z}_{>n}}\mathbb{R}\cdot e_i$ and the isomorphism $(**)$ above gives $M/\mathrm{Im}(\alpha) \cong \bigoplus_{i=1}^n \mathbb{R}\cdot e_i =: \mathbb{R}^n$. So we take $N = \mathbb{R}^n$ and define $\beta : M \to N$ mapping $e_k \mapsto e_k$ if $1 \leq k \leq n$ and $e_h \mapsto 0$ else. Then we have a short exact sequence

$$0 \to M \oplus M \xrightarrow{\alpha} M \xrightarrow{\beta} \mathbb{R}^n \to 0.$$

2. Let R be a ring and M be an R-module. Let $N \leq M$ and $L \leq M$, meaning that N and L are R-submodules of M.

Show that $N \cap L \leq N$, and that $L \leq N + L \leq M$, and prove that there is an isomorphism $N/(N \cap L) \xrightarrow{\sim} (N + L)/L$.

Solution:

This exercise is very similar to Exercise 2 from exercise sheet 4, which we will assume as already proven. All our R-modules are in particular abelian groups, and at level of the underlying abelian groups everything is proven.

To prove that $N \cap L \leq N$ and $L \leq (N + L) \leq M$, first notice that this is true at level of abelian groups (that is, those statement are true giving to "$\leq$" the meaning of "is a subgroup of"), so that we only need to check that they are stable subsets under scalar multiplication.

- $N \cap L \leq N$: If $x \in N \cap L$ and $r \in R$, then we have $r \cdot x \in N$ and $r \cdot x \in L$, since N and L are submodules of M, so that $r \cdot x \in N \cap L$;
- $L \leq N + L$ is trivial being $L \leq M$;
- $N + L \leq M$: every element $x \in N + L$ can be written as $x = n + l$ for some $n \in N$ and $l \in L$, so that $\forall r \in R$ we have $r \cdot x = r \cdot (n + l) = r \cdot n + r \cdot l \in N + L$ by definition, being $r \cdot n \in N$ and $r \cdot l \in L$.

Now, define the map

$$\begin{aligned} N &\to (N + L)/L \\ n &\mapsto n + L. \end{aligned}$$

This map is easily seen to be R-linear, and it is surjective because elements in the codomain are all of the form $(n' + l') + L = n' + L$ for $n' \in N$ and $l' \in L$. Finally, we have that $l + L = 0_{(N+L)/L}$ if and only if $l \in L$, so that the kernel of the map is $N \cap L$. Then the First Isomorphism Theorem for R-modules gives an isomorphism $N/(N \cap L) \xrightarrow{\sim} (N + L)/L$.

3. Let $R \neq 0$ be a commutative ring. We say that $a \in R$ is a zero-divisor if there exists $b \in R$ such that $b \neq 0$ and $ab = 0$. We say that $a \in R$ is regular if a is not a zero-divisor.

1. Prove that invertible elements in R are regular. Is the converse true?
2. Let $R_{\text{reg}} = \{a \in R : a \text{ is regular}\}$. Prove that R_{reg} contains 1_R and that it is stable under multiplication. This is also phrased by saying that the R_{reg} is a multiplicative subset of R.
3. Let now M be an R-module. Define $M_{\text{tor}} = \{m \in M | \exists r \in R_{\text{reg}} : r \cdot m = 0_M\}$. Prove that M_{tor} is a submodule of M. It is called the *torsion submodule* of M.
4. We say that a module N is torsion-free if $N_{\text{tor}} = 0$. Prove: for every R-module M, the module M/M_{tor} is torsion-free.
5. Find the torsion submodule of the $\mathbb{Z}$-module $M = \mathbb{R}/\mathbb{Z}$. What is M/M_{tor}?

Solution:

1. First, observe that $r \in R$ is regular if and only if $ru = 0$ with $u \in R$ implies $u = 0$. Let $r \in R$ be a unit, with inverse s. If $ru = 0$ for some $u \in R$, then $0 = 0 \cdot s = (ru)s = (rs)u = u$, so that $u = 0$. Hence every invertible element in R is regular. The converse is not true in general. For instance, if $R = \mathbb{Z}$, then 2 is regular, but it is not invertible.
2. We have that 1_R is regular, because $1_R \cdot r = 0$ implies $r = 0$. Now suppose that $r, s \in R_{\text{reg}}$. Then rs is also regular, since if $rsu = 0$ for some $u \in R$, then being r regular we get $su = 0$, and being s regular we can conclude $u = 0$.
3. Let $m, n \in M_{\text{tor}}$, with $r \cdot m = s \cdot n = 0_M$ for some $r, s \in R_{\text{reg}}$. Then $rs \cdot (m + n) = (rs) \cdot m + (rs) \cdot n = s \cdot (r \cdot m) + r \cdot (s \cdot n) = 0_M$, and being $rs \in R_{\text{reg}}$ by previous point, we have $m + n \in M_{\text{tor}}$. Now for any $a \in R$ we also have $r \cdot (a \cdot m) = a \cdot (r \cdot m) = 0_M$, so that $a \cdot m \in M_{\text{tor}}$ as well. We can then conclude that M_{tor} is a submodule of M.
4. Suppose that $m + M_{\text{tor}} \in (M/M_{\text{tor}})_{\text{tor}}$. Then there exists $r \in R_{\text{reg}}$ such that $0_{M/M_{\text{tor}}} = r \cdot (m + M_{\text{tor}}) = r \cdot m + M_{\text{tor}}$, which is equivalent to $r \cdot m \in M_{\text{tor}}$. Hence there exists $s \in R_{\text{reg}}$ such that $s \cdot (r \cdot m) = 0_M$. Then $(sr) \cdot m = 0_M$, and since $sr \in R_{\text{reg}}$ by Point 2, we can conclude that $m \in M_{\text{tor}}$, so that $m + M_{\text{tor}} = 0_{M/M_{\text{tor}}}$. Hence M/M_{tor} is torsion-free.
5. For $R = \mathbb{Z}$ and $M = \mathbb{R}/\mathbb{Z}$, we claim that $M_{\text{tor}} = \mathbb{Q}/\mathbb{Z} = \{q + \mathbb{Z} | q \in \mathbb{Q}\} \leq \mathbb{R}/\mathbb{Z}$. To prove the inclusion "$\subseteq$", suppose that $\alpha + \mathbb{Z} \in M_{\text{tor}}$. This means that for some non-zero $n \in \mathbb{Z}$ we have $n\alpha = m \in \mathbb{Z}$, so that $\alpha = m/n$ is rational by definition. Conversely, if $q \in \mathbb{Q}$, there exists a positive integer k such that $kq \in \mathbb{Z}$, so that $k \cdot (q + \mathbb{Z}) = \mathbb{Z}$.

See next page!

Now we have that
$$\frac{M}{M_{\rm tor}} = \frac{\mathbb{R}/\mathbb{Z}}{\mathbb{Q}/\mathbb{Z}} \cong \mathbb{R}/\mathbb{Q},$$
where the last isomorphism is due to the Third Isomorphism Theorem stated below (applied with $R = \mathbb{Z}$, $A = \mathbb{Z}$, $B = \mathbb{Q}$ and $C = \mathbb{R}$).

Third Isomorphism Theorem. Let R be a ring and $A \leq B \leq C$ inclusions of R-modules. Then $B/A \leq C/A$, and there is an isomorphism
$$\frac{C/A}{B/A} \cong C/B.$$

Proof: The inclusion of quotient modules is clear by definition. For the isomorphism, consider the map $C \to \frac{C/A}{B/A}$ sending $c \mapsto (c + A) + (B/A)$. It is easily seen to be a surjective R-linear map, whose kernel is B. Then the isomorphism follows from First Isomorphism Theorem. □

4. (*) Let R be a commutative ring. If M and N are R-modules, we define $\mathrm{Hom}_R(M, N)$ as the set of R-linear maps $M \to N$. It is easily seen to be an R-module by defining
$$(f+g)(m) = f(m)+g(m),\ \ (a\cdot f)(m) := a\cdot(f(m)),\ \ \forall f, g \in \mathrm{Hom}_R(M, N),\ a \in R,\ m \in M.$$

1. Let N be an R-module. For every R-linear map $f : M_1 \to M_2$, define
$$f^* : \mathrm{Hom}_R(M_2, N) \to \mathrm{Hom}_R(M_1, N)$$
$$g \mapsto g \circ f.$$
Prove that f^* is also an R-linear map, and that we have the following properties:
   - $(f_2 \circ f_1)^* = f_1^* \circ f_2^*$, for every couple of R-linear maps $f_1 : M_1 \to M_2$ and $f_2 : M_2 \to M_3$;
   - $\mathrm{id}_M^* = \mathrm{id}_{\mathrm{Hom}_R(M,N)}$ for every R-module M.
2. Define a natural map $\mathrm{Hom}_R(M_1 \oplus M_2, N) \to \mathrm{Hom}_R(M_1, N) \oplus \mathrm{Hom}_R(M_2, N)$ and prove that it is an isomorphism of R-modules.
3. Prove that for any exact sequence of R-modules $A \to B \to C \to 0$, one has that the corresponding
$$0 \to \mathrm{Hom}_R(C, N) \to \mathrm{Hom}_R(B, N) \to \mathrm{Hom}_R(A, N)$$
is also an exact sequence of modules.
4. Let $A = \mathrm{End}_{\mathbb{R}}(M)$, where M is a countably infinite dimensional $\mathbb{R}$-vector space (i.e., M has an $\mathbb{R}$-basis $\mathcal{B} = (e_i)_{i\in\mathbb{Z}_{>0}}$). Prove that A^2 is isomorphic to A as an A-module. [*Hint:* First, prove that $M \cong M \oplus M$ as $\mathbb{R}$-vector spaces.] What happens if M is finite dimensional? (What if M is uncountably infinite dimensional?)

Solution (sketch):

Please turn over!

1. To prove that f^* is R-linear it is enough to check on elements of M_1 the equalities of maps $(g+h)\circ f = (g\circ f)+(h\circ f)$ and $(r\cdot f)\circ g = r\cdot(f\circ g)$, where $g,h \in \mathrm{Hom}_R(M_2,N)$ and $r\in R$.

   The property $(f_2\circ f_1)^* = f_1^*\circ f_2^*$, for linear maps $f_1 : M_1 \to M_2$ and $f_2 : M_2 \to M_3$ is easily checked on elements $g \in \mathrm{Hom}_R(M_2,N)$. Analogously one can check that $\mathrm{id}_M^* = \mathrm{id}_{\mathrm{Hom}_R(M,N)}$.

2. For $i = 1,2$, denote by e_i the canonical inclusion map $M_i \mapsto M_1 \oplus M_2$ and by p_i the canonical projection map $p_i : M_1 \oplus M_2 \to M_1$. In the same way, denote by d_i the canonical inclusion $d_i : \mathrm{Hom}_R(M_i,N) \to \mathrm{Hom}_R(M_1,N)\oplus \mathrm{Hom}_R(M_2,N)$ and by q_i the projection $\mathrm{Hom}_R(M_1,N)\oplus\mathrm{Hom}_R(M_2,N) \to \mathrm{Hom}_R(M_i,N)$.

   Define a map $\psi : \mathrm{Hom}_R(M_1\oplus M_2,N) \to \mathrm{Hom}_R(M_1,N)\oplus\mathrm{Hom}_R(M_2,N)$ sending $g \mapsto e_1^*(g)+e_2^*(g)$. To be precise, we can write $\psi = d_1\circ e_1^* + d_2\circ e_2^*$, and deduce that ψ is R-linear (why?).

   Also, define $\varphi : \mathrm{Hom}_R(M_1,N)\oplus\mathrm{Hom}_R(M_2,N) \to \mathrm{Hom}_R(M_1\oplus M_2,N)$, sending $f = f_1+f_2$, where $f_i \in \mathrm{Hom}_R(M_i,N)$, to $p_1^*(f_1)+p_2^*(f_2)$. Formally, $\varphi = p_1^*\circ q_1 + p_2^*\circ q_2$.

   Now $\psi\circ\varphi = (\sum_{i=1,2} d_i\circ e_i^*)\circ(\sum_{j=1,2} p_j^*\circ q_j)$. Using linearity, we need to consider compositions of the form $e_i^*\circ p_j^* = (p_j\circ e_i)^*$. By Point 1, this can be seen to be the zero map for $i\neq j$, and an identity map for $i=j$. Then $\psi\circ\varphi = d_1\circ q_1 + d_2\circ q_2$, which is the identity of $\mathrm{Hom}_R(M_1,N)\oplus\mathrm{Hom}_R(M_2,N)$ (check!).

   Conversely, $\varphi\circ\psi = (\sum_{j=1,2} p_j^*\circ q_j)\circ(\sum_{i=1,2} d_i\circ e_i^*)$, and considering that $q_j\circ d_i$ is zero if $i\neq j$ and an identity otherwise, using Point 1 we get $\varphi\circ\psi = (e_1\circ p_1 + e_2\circ p_2)^*$, which turns out (how?) to be the identity of $\mathrm{Hom}_R(M_1\oplus M_2,N)$.

   Hence φ and ψ are each others inverses, and we have proven the desired isomorphism.

3. In the given exact sequence, call the maps $f : A \to B$ and $g : B \to C$. We have to prove that g^* is injective, and that $\mathrm{Im}(g^*) = \ker(f^*)$.

   a) g^* is injective: Suppose that $\gamma \in \ker(g^*)$. This means that $\gamma : C \to N$ is an R-linear map such that $\gamma\circ g$ is the zero map $B \to N$. But g is surjective, so that for every $c \in C$ we have that there exists $b \in B$ such that $c = g(b)$, and $\gamma(c) = (\gamma\circ g)(b) = 0(b) = 0$, and $\gamma = 0$. Hence g^* is injective.

   b) $\mathrm{Im}(g^*) \subseteq \ker(f^*)$: Suppose that $\beta \in \mathrm{Im}(g^*)$. This means that $\beta = \gamma\circ g$ for some $\gamma \in \mathrm{Hom}_R(C,N)$. Then $f^*(\beta) = \beta\circ f = \alpha\circ g\circ f = 0$ since $g\circ f = 0$, so that $\beta \in \ker(f^*)$, proving the desired inclusion.

   c) $\mathrm{Im}(g^*) \supseteq \ker(f^*)$: Suppose that $\beta \in \ker(f^*)$, that is, $\beta \in \mathrm{Hom}_R(B,N)$ is such that $\beta\circ f$ is the zero map $A \to N$. We want to define an R-linear map $\gamma : C \to N$ such that $\gamma\circ g = g^*(\gamma) = \beta$. For $c \in C$, by surjectivity of g there exists $b \in B$ such that $g(b) = c$, and we try to define $\gamma(c) = \beta(b)$. This can be seen to be a good definition: if $g(b) = g(b')$, then $g(b-b') = 0$, so that $b-b' \in \ker(g) = \mathrm{Im}(f)$ and $b-b' = f(a)$ for some $a \in A$. Then $\beta(b)-\beta(b') = \beta(b-b') = (\beta\circ f)(a) = 0$ by hypothesis. Hence γ is well defined, and it is easily seen to be a linear map by chosing, for each R-linear combination $c = r_1\cdot c_1 + r_2\cdot c_2$ of elements $c_1,c_2 \in C$ some counterimages b_1 and b_2 via g of c_1 and c_2, and noticing that $g(r_1\cdot b_1 + r_2\cdot b_2) = c$, so that

See next page!

$\gamma(c) = \beta(r_1 \cdot b_1 + r_2 \cdot b_2) = r_1 \cdot \beta(b_1) + r_2 \cdot \beta(b_2) = r_1 \cdot \gamma(c_1) + r_2 \cdot \gamma(c_2)$. Then $g^*(\gamma) = \beta$ follows directly from the definition of γ, proving the desired inclusion.

4. - Suppose that M is a countably infinite dimensional $\mathbb{R}$-vector space, with $M = \bigoplus_{i\in\mathbb{Z}} \mathbb{R} \cdot e_i$. Then part 3.b of Exercise 1 gives an isomorphism $M \oplus M \xrightarrow{\vartheta} M$ and Point 1 can be used to prove that ϑ^* is also an isomorphism, so that

$$A = \operatorname{Hom}_{\mathbb{R}}(M, M) \xrightarrow{\vartheta^*} \operatorname{Hom}_{\mathbb{R}}(M \oplus M, M) \xrightarrow{\psi} (\operatorname{Hom}_{\mathbb{R}}(M, M))^2 = A^2,$$

is a chain of isomorphisms of $\mathbb{R}$-vector spaces, where ψ is the isomorphism from Point 2 (with $M_1 = M_2 = N = M$).
Denoting the isomorphism above as $\xi : A \to A^2$, we want to prove that ξ is also an isomorphism of A-module. To do so, we decompose $\xi = d_1 \circ \xi_1 + d_2 \circ \xi_2$, with $\xi_i : A \to A$, and establish A-linearity by proving that for $f, g \in A$ one has the equality () in the following:

$$d_1 \circ \xi_1(f \circ g) + d_2 \circ \xi_2(f \circ g) = \xi(f \circ g) \overset{(*)}{=} f \circ \xi(g) = d_1 \circ f \circ \xi_1(g) + d_2 \circ f \circ \xi_2(g),$$

where in the last equality we used the A-module structure of A^2 (A acts by composition on the left in both entries of A^2). To check $(*)$ above, we prove that the first and the last compositions are equal, and this is true of course if $d_i \circ \xi_i(f \circ g) = d_i \circ f \circ \xi_i(g)$ for both $i = 1, 2$. Notice that $\xi_i = q_i \circ \xi$, so that using the definition of ξ and ψ, we get:

$$\begin{aligned} d_i \circ \xi_i(f \circ g) &= d_i \circ q_i \circ (d_1 \circ e_1^* + d_2 \circ e_2^*) \circ \vartheta^*(f \circ g) = d_i \circ e_i^* \circ \vartheta^*(f \circ g) = \\ &= d_i \circ f \circ g \circ \vartheta \circ e_i = d_i \circ f \circ e_i^* \circ \vartheta^*(g) = \cdots = \\ &= d_i \circ f \circ \xi_i(g), \end{aligned}$$

and we can conclude the proof.

- If M is zero, then the result is trivially true, being $A = 0$. If $M \neq 0$ is finite dimensional, with $k = \dim_{\mathbb{R}}(M)$, then by basic linear algebra we have an isomorphism of $\mathbb{R}$-vector spaces $A = \operatorname{Hom}_{\mathbb{R}}(M, M) \cong M_{k,k}(\mathbb{R}) \cong \mathbb{R}^{k^2}$, so that $A^2 \cong \mathbb{R}^{2k^2}$ and we cannot have an isomorphism $A \cong A^2$, the dimensions over $\mathbb{R}$ being distinct.
- Finally, if M is an infinite dimensional $\mathbb{R}$-vector space, one can prove that still $M \oplus M \cong M$, and repeat the same argument used for M countably infinite dimensional (where the only information about ϑ that we used is that it is an isomorphism of $\mathbb{R}$-vector spaces). First, recall that any vector space has a basis (this can be proven using Zorn's Lemma). Then let $M = \sum_{i\in I} e_i\mathbb{R}$. We can write $M \oplus M = \sum_{i\in I\cup I'} e_i M$, where we take a set I' disjoint with I with $|I| = |I'|$. Then giving an isomorphism of $\mathbb{R}$-vector spaces $M \oplus M \cong M$ is equivalent to giving a bijection $I \to I \sqcup I'$, which is equivalent to proving that $I = J \cup K$, for some $J, K \subseteq I$ with $I \cap K = \varnothing$ and $|J| = |K| = |I|$. To prove this, it is enough to prove that I is a disjoint union of subsets of countable cardinality [then one can split all those countable subsets N_r into two disjoint

parts J_r, K_r of countable cardinality, and take $J = \cup_r J_r$ and $K = \cup_r K_r$, which can be easily proven to be of the same cardinality of I].
To prove that I is a disjoint union of subsets of countable cardinality, again one can apply Zorn's Lemma: consider the following poset of families of disjoint countable subsets:

$$\mathcal{S} = \{\{S_\alpha\}_{\alpha\in A} | \forall \alpha \neq \beta \in A,\ S_\alpha \subseteq I, |S_\alpha| = |\mathbb{Z}|, S_\alpha \cap S_\beta = \varnothing\},$$

order by inclusion $\subseteq$ (of families of countable subsets). Being I infinite, we have a copy Z of $\mathbb{Z}$ in I, so that $\{Z\} \in \mathcal{S} \neq \varnothing$. Now suppose we are given a chain of elements $(S_K)_K = (\{S_\alpha\}_{\alpha\in K})_K \subseteq \mathcal{S}$. Then it is bounded by $B = \bigcup_K S_K$. Indeed, B is a family of countable subsets of I and if two of those subsets $S_{\alpha_1}, S_{\alpha_2}$ are not disjoint, suppose that they belong respectively to S_{K_1} and S_{K_2} (with $\alpha_i \in K_i$). Since $(S_K)_K$ is a chain we have $S_{K_1}, S_{K_2} \subseteq S_{K_3}$ for some K_3, so that $S_{K_3} \in \mathcal{S}$ contains both S_{α_1} and S_{α_2}, contradiction. Then there is a maximal collection of countable disjoint subsets $\{S_r\}_{r\in T}$, with $S_r \subseteq I$, which means that the subset of the remaining elements $U := I \setminus \bigcup_{r\in T}$ is finite (else, we could add another disjoint countable subset to the maximal collection, contradiction). Then we can choose $r_0 \in T$ and replace S_{r_0} with $S_{r_0} \cup U$ (which is still countable), and obtain a disjoint union of countable subsets of I.