Exercises 3

Please submit solutions by 3pm on Thursday 1st March to the pigeonholes in 4W (ground floor).

(W) = Warm-up; (H) = Homework; (A)=Additional.

1. (W) Let R, S and T be rings and let $\phi : R \to S$ and $\psi : S \to T$ be ring homomorphisms. Show that the composition $\psi \circ \phi \colon R \to T$ is a ring homomorphism.

2. (W) Let $\phi \colon R \to S$ be a ring homomorphism. Show that ϕ is a ring isomorphism if and only if ϕ is bijective as a map of *sets*. [Hint: one direction is immediate.]

3. (H) *This exercises illustrates that isomorphic rings share the same ring-theoretic properties, i.e., as rings they are indistinguishable.* Let R, S be rings and let $\phi \colon R \to S$ be an isomorphism. Show that

(1) R is a ring with 1 if and only if S is a ring with 1;

(2) R is a commutative ring if and only if S is a commutative ring;

(3) R is an integral domain if and only if S is an integral domain.

4. (H) Let V be a finite dimensional vector space over a field $\Bbbk$. An *endomorphism on* V is a linear map $\alpha \colon V \to V$, and let $\mathrm{End}\,(V)$ denote the set of all endomorphisms on V. For $\alpha, \beta \in \mathrm{End}\,(V)$, define maps $(\alpha + \beta) \colon V \to V$ and $(\alpha \cdot \beta) \colon V \to V$ as follows: for $v \in V$, define

$$(\alpha + \beta)(v) := \alpha(v) + \beta(v) \in V \quad \text{and} \quad (\alpha \cdot \beta)(v) := \alpha(\beta(v)) \in V.$$

(1) Show that both $(\alpha + \beta)$ and $(\alpha \cdot \beta)$ are endomorphisms of V (i.e., show that both are linear maps), and prove that these two operations make $(\mathrm{End}\,(V), +, \cdot)$ into a ring with 1.

(2) Let n denote the dimension of V as a $\Bbbk$-vector space. Show that $\mathrm{End}\,(V)$ is isomorphic to the ring $M_n(\Bbbk)$ of $n \times n$ matrices with entries in $\Bbbk$.

5. (A) Let V be a two dimensional vector space over a field $\Bbbk$ with basis (u, v). Let $\phi \in \mathrm{End}(V)$ be the linear map satisfying $\phi(u) = v$ and $\phi(v) = -u$.

(1) Show that the subset $F = \{a\,\mathrm{id} + b\phi \mid a, b \in \Bbbk\}$ is a subring of $\mathrm{End}(V)$. [Hint: first compute $\phi^2(u)$ and $\phi^2(v)$.]

(2) Show that F is a field if and only if $x^2 + 1$ has no root in $\Bbbk$.

(3) In the case when $\Bbbk = \mathbb{R}$, the field F is an old friend. Which one?

The course website is: `http://people.bath.ac.uk/dmjc20/Alg2B/`

Solutions 3

1. As both ϕ and ψ are homomorphisms, we have

$$\psi(\phi(a+b)) = \psi(\phi(a)+\phi(b)) = \psi(\phi(a)) + \psi(\phi(b))$$

and

$$\psi(\phi(ab)) = \psi(\phi(a)\phi(b)) = \psi(\phi(a))\psi(\phi(b)).$$

Hence $\psi \circ \phi$ is a homomorphism.

2. If ϕ is a ring isomorphism, then we saw in class (see Remark 2.11(1)) that ϕ is bijective as a map of sets. For the converse, suppose that ϕ is bijective as a map of sets. Let $u, v \in S$. As ϕ is bijective there exist $a, b \in R$ such that $\phi(a) = u$ and $\phi(b) = v$ and thus $\phi^{-1}(u) = a$ and $\phi^{-1}(v) = b$. It follows that

$$\phi^{-1}(u+v) = \phi^{-1}(\phi(a)+\phi(b)) = \phi^{-1}(\phi(a+b)) = a+b = \phi^{-1}(u)+\phi^{-1}(v)$$

and

$$\phi^{-1}(uv) = \phi^{-1}(\phi(a)\phi(b)) = \phi^{-1}(\phi(ab)) = ab = \phi^{-1}(u)\phi^{-1}(v).$$

This shows that ϕ^{-1} is an isomorphism.

3. (1) Let R be a ring with 1. We claim that the element $\phi(1) \in S$ is the multiplicative identity in S, making S into a ring with 1. For this, let $s \in S$. Then for $r = \phi^{-1}(s) \in R$, we have that

$$s \cdot \phi(1) = \phi(\phi^{-1}(s)) \cdot \phi(1) = \phi(r) \cdot \phi(1) = \phi(r \cdot 1) = \phi(r) = s,$$

and similarly,

$$\phi(1) \cdot s = \phi(1) \cdot \phi(\phi^{-1}(s)) = \phi(1) \cdot \phi(r) = \phi(1 \cdot r) = \phi(r) = s.$$

This shows that $\phi(1)$ is the multiplicative identity in S, so S is a ring with 1.

To prove the other direction, rather than rewrite all of the above in the other direction, notice that since $\phi^{-1}\colon S \to R$ is a ring isomorphism, the above argument applied to ϕ^{-1} shows that if S is a ring with 1 then $\phi^{-1}(1)$ makes R into a ring with 1.

(2) Let R be commutative, and let $s, s' \in S$. Then for $r = \phi^{-1}(s)$ and $r' = \phi^{-1}(s')$, we have

$$s \cdot s' = \phi(r) \cdot \phi(r') = \phi(r \cdot r') = \phi(r' \cdot r) = \phi(r') \cdot \phi(r) = s' \cdot s,$$

so S is commutative. As in part (1), if we assume that S is commutative, then the argument we've just given applied to the isomorphism $\phi^{-1}\colon S \to R$ shows that R is commutative.

(3) Let R be an integral domain. By parts (1) and (2), we know that S is a commutative ring with 1.

We claim that $0_S \neq 1_S$ in S. Indeed, suppose for a contradiction that $0_S = 1_S$. Then $\phi^{-1}(0_S) = \phi^{-1}(1_S)$ in R, but this is a contradiction because $\phi^{-1}(0_S)$ is the zero element in R (by applying Lemma 2.4(3) to the ring homomorphism ϕ^{-1}) and $\phi^{-1}(1_S)$ is the multiplicative identity 1_R in R by applying part (1) above to ϕ^{-1}; and of course we know $0_R \neq 1_R$ as R is an integral domain.

Finally, let $s, t \in S$ satisfy $st = 0$. Then by applying Lemma 2.4(3) again, we know that

$$0_R = \phi^{-1}(0_S) = \phi^{-1}(st) = \phi^{-1}(s) \cdot \phi^{-1}(t).$$

Since R is an integral domain, we deduce that $\phi^{-1}(s) = 0$ or $\phi^{-1}(t) = 0$. Now apply ϕ to each equation (and use Lemma 2.4(3) again) to see that either $s = \phi(\phi^{-1}(s)) = 0$ or $t = \phi(\phi^{-1}(t)) = 0$ as required, so S is indeed an integral domain.

4. (1) The map $\alpha+\beta$ is linear, because for $v, w \in V$ and $\lambda \in \Bbbk$ we have

$$\begin{aligned}
(\alpha+\beta)(\lambda v+w) &= \alpha(\lambda v+w)+\beta(\lambda v+w) && \text{by definition}\\
&= \lambda\alpha(v)+\alpha(w)+\lambda\beta(v)+\beta(w) && \text{as } \alpha,\beta \text{ are linear}\\
&= \lambda\big(\alpha(v)+\beta(v)\big)+\big(\alpha(w)+\beta(w)\big)\\
&= \lambda(\alpha+\beta)(v)+(\alpha+\beta)(w).
\end{aligned}$$

This means that $(\alpha+\beta) \in \mathrm{End}\,(V)$. Also, the composition of two linear maps is linear, so $(\alpha\cdot\beta) \in \mathrm{End}\,(V)$.

To check that we have a ring, let $\alpha, \beta, \gamma \in \mathrm{End}(V)$. As the addition in V is commutative and associative, we have $\alpha(v)+\beta(v) = \beta(v)+\alpha(v)$ and $(\alpha(v)+\beta(v))+\gamma(v) = \alpha(v)+(\beta(v)+\gamma(v))$, so

$$\alpha+\beta = \beta+\alpha \quad\text{and}\quad (\alpha+\beta)+\gamma = \alpha+(\beta+\gamma).$$

Let $O \in \mathrm{End}(V)$ be the linear map that takes each element in V to $0 \in V$. Clearly $\alpha+O = O+\alpha = \alpha$ and also $\mathrm{id}\cdot\alpha = \alpha\cdot\mathrm{id} = \alpha$. Thus O is the additive identity and id is the multiplicative identity. As composition of maps is an associative operation *by definition*, we have that $\cdot$ is associative. Let $-\alpha$ be the linear map that takes v to $-\alpha(v)$. Then $[\alpha+(-\alpha)](v) = \alpha(v)+(-\alpha(v)) = 0$ and thus $\alpha+(-\alpha) = O$. This shows that every element in $\mathrm{End}(V)$ has an additive inverse. It now only remains to show that the distributive laws hold. But as α is a linear map, we have

$$[\alpha(\beta+\gamma)](v) = \alpha(\beta(v)+\gamma(v)) = \alpha(\beta(v))+\alpha(\gamma(v)) = [\alpha\beta+\alpha\gamma](v)$$

and

$$[(\beta+\gamma)\alpha](v) = [\beta+\gamma](\alpha(v)) = \beta(\alpha(v))+\gamma(\alpha(v)) = [\beta\alpha+\gamma\alpha](v).$$

This shows that $\alpha(\beta+\gamma) = \alpha\beta+\alpha\gamma$ and $(\beta+\gamma)\alpha = \beta\alpha+\beta\gamma$.

(2) To write down a map from $M_n(\Bbbk)$ to $\mathrm{End}\,(V)$, choose a basis $(v_1,\dots,v_n)$ of V and consider the invertible linear map

$$\alpha\colon \Bbbk^n \to V \;:\; \begin{pmatrix} a_1\\ \vdots\\ a_n\end{pmatrix} \mapsto a_1v_1+\cdots+a_nv_n.$$

This map is the bridge between $n\times n$ matrices with entries in $\Bbbk$ and linear maps $V \to V$: on one hand, left multiplication by a square matrix $A \in M_n(\Bbbk)$ defines a linear map $A\colon \Bbbk^n \to \Bbbk^n$; and on the other hand, the composition

$$a_1v_1+\cdots+a_nv_n \xrightarrow{\alpha^{-1}} \begin{pmatrix} a_1\\ \vdots\\ a_n\end{pmatrix} \xrightarrow{\text{left mult by } A} \begin{pmatrix} b_1\\ \vdots\\ b_n\end{pmatrix} \xrightarrow{\alpha} b_1v_1+\cdots+b_nv_n,$$

defines the linear map $f_A\colon V \to V$ given by $f_A(v) = \alpha A\alpha^{-1}(v)$. We claim that the map

$$\phi\colon M_n(\Bbbk) \longrightarrow \mathrm{End}\,(V) \;:\; A \mapsto f_A$$

is a ring isomorphism. To prove the claim, notice that

$$\phi(A+B) = \alpha(A+B)\alpha^{-1} = \alpha A\alpha^{-1}+\alpha B\alpha^{-1} = f_A+f_B = \phi(A)+\phi(B)$$

and

$$\phi(AB) = \alpha AB\alpha^{-1} = (\alpha A\alpha^{-1})(\alpha B\alpha^{-1}) = f_A\circ f_B = \phi(A)\phi(B),$$

so ϕ is a ring homomorphism. Finally, it's bijective as a map of sets with inverse given by the matrix $\phi^{-1}(f)$ corresponding to the map $\alpha^{-1}f\alpha\colon \Bbbk^n \to \Bbbk^n$. Explicitly, $\phi^{-1}(f)$ is the $n\times n$ matrix whose ith column is $(\alpha^{-1}f\alpha)(e_i)$, where e_i denotes the basis vector of $\Bbbk^n$ with 1 in the ith entry and 0 elsewhere. It follows from Question 2 above that ϕ is an isomorphism.

5. (1) First compute $\phi^2(u) = \phi(v) = -u$ and $\phi^2(v) = \phi(-u) = -\phi(u) = -v$. Hence $\phi^2 = -\mathrm{id}$. To verify that F is a subring of $\mathrm{End}\,(V)$, consider $a\,\mathrm{id} + b\phi, c\,\mathrm{id} + d\phi \in F$ and notice that

$$(a\,\mathrm{id} + b\phi) - (c\,\mathrm{id} + d\phi) = (a - c)\,\mathrm{id} + (b - d)\phi$$

lies in F, as does

$$(a\,\mathrm{id} + b\phi)(c\,\mathrm{id} + d\phi) = ac\,\mathrm{id} + bd\phi^2 + (ac + bd)\phi = (ac - bd)\,\mathrm{id} + (ac + bd)\phi.$$

This shows that F is a subring of $\mathrm{End}\,(V)$.

(2) Suppose first that $a^2 + 1 = 0$ for some $a \in \Bbbk$. Then $(a\,\mathrm{id} + \phi) \cdot (a\,\mathrm{id} - \phi) = (a^2 + 1)\,\mathrm{id} = 0$, whereas neither of the factors $a\,\mathrm{id} + \phi$ nor $a\,\mathrm{id} - \phi$ is zero. This can't happen in a field (why?). Conversely suppose that there is no $a \in \Bbbk$ such that $a^2 + 1 = 0$. Take any non-zero element $a\,\mathrm{id} + b\phi$ in F, i.e., at least one of a, b is nonzero. If $a^2 + b^2 \neq 0$ then

$$(a\,\mathrm{id} + b\phi)\left(\frac{a}{a^2 + b^2}\,\mathrm{id} - \frac{b}{a^2 + b^2}\phi\right) = \frac{a^2 + b^2}{a^2 + b^2}\mathrm{id} = \mathrm{id},$$

so $a\,\mathrm{id} + b\phi$ has a multiplicative inverse. It therefore remains to show that $a^2 + b^2 \neq 0$. We know that one of a and b is non-zero, say $b \neq 0$. Then

$$a^2 + b^2 = b^2\left((\frac{a}{b})^2 + 1\right)$$

and if this was zero then dividing by b^2 would give $(\frac{a}{b})^2 + 1 = 0$, thereby contradicting our assumption that $x^2 + 1$ has no root in $\Bbbk$.

(3) Notice that $F = \mathbb{R}\mathrm{id} + \mathbb{R}\phi \cong \mathbb{R} + \mathbb{R}i \cong \mathbb{C}$.