MATH 7752 Homework 3

James Harbour

February 11, 2022

Problem 1

Let R be a commutative domain, and let M be a free R-module with basis $X = \{e_1, \dots, e_k\}$, with $k \geq 2$. Prove that the element $e_1 \otimes e_2 + e_2 \otimes e_1$ cannot be written as simple tensor $m \otimes n$, for some $m, n \in M$.

Proof. Suppose, for the sake of contradiction, that there exist $m, n \in M$ such that $m \otimes n = e_1 \otimes e_2 + e_2 \otimes e_1$. Write $m = \sum_{i=1}^n r_i e_i$ and $n = \sum_{j=1}^n s_j e_j$ for some $r_i, s_j \in R$. Then

$$e_1 \otimes e_2 + e_2 \otimes e_1 = \left(\sum_{i=1}^n r_i e_i\right) \otimes \left(\sum_{j=1}^n s_j e_j\right) = \sum_{i,j} r_i s_j e_i \otimes e_j$$

As $M \otimes M$ is free with basis $\{e_i \otimes e_j\}_{i,j=1}^n$, it follows that $r_1 s_2 = 1$, $r_2 s_1 = 1$, and $r_i s_j = 0$ for all $(i,j) \neq (1,2), (2,1)$. However, then $r_1 s_1 = 0$ whence $r_1 = 0$ or $s_1 = 0$, contradicting $r_1, s_1 \in R^\times$.

$\square$

Problem 2

Let R be a commutative ring (with 1) and $n, m \in \mathbb{N}$. Prove that there is an isomorphism of R-**algebras** $R^n \otimes R^m \simeq R^{nm}$. (Here by R^n we mean the direct sum $\underbrace{R \oplus \cdots \oplus R}_{n}$.)

Proof. As R-modules, we have the following isomorphisms:

$$R^n \otimes R^m \cong (R^n \otimes R)^m \cong ((R \otimes R)^n)^m \cong (R \otimes R)^{nm} \cong R^{nm}$$

$$(r_1, \dots, r_n) \otimes (r_1', \dots, r_m') \mapsto (r_i r_j')_{(i,j) \in [n] \times [m]}$$

where we identify R^{nm} with $M_{n \times m}(R)$. Let $\varphi : R^n \otimes R^m \to R^{nm}$ denote this R-module isomorphism. We show that this is in fact an R-algebra isomorphism. It suffices to show that φ is multiplicative on simple tensors, whence by linearity it would be multiplicative on all of $R^n \otimes R^m$.

Let $r \otimes r' = (r_1, \dots, r_n) \otimes (r_1', \dots, r_m'), s \otimes s' = (s_1, \dots, s_n) \otimes (s_1', \dots, s_m') \in R^n \otimes R^m$. Then

$$\varphi((r \otimes r') \cdot (s \otimes s')) = \varphi(rr' \otimes ss') = (r_i r_i' s_j s_j')_{(i,j)) \in [n] \times [m]} = (r_i r_i')_{(i,j)) \in [n] \times [m]} \cdot (s_i s_i')_{(i,j)) \in [n] \times [m]} = \varphi(r \otimes r')\varphi(s \otimes s')$$

so φ is an R-algebra isomorphism. $\square$

Problem 3

(a) Let V be a finite-dimensional $\mathbb{C}$-vector space. Then V can be considered as a vector over $\mathbb{R}$ (by restriction of scalars), and it holds $\dim_{\mathbb{R}} V = 2\dim_{\mathbb{C}} V$. Prove that $V \otimes_{\mathbb{C}} V$ is not isomorphic to $V \otimes_{\mathbb{R}} V$ as $\mathbb{R}$-vector spaces, and compute their dimensions over $\mathbb{R}$.

Proof. Let $k = \dim_{\mathbb{C}} V$. Then $\dim_{\mathbb{R}} V = 2k$. As a $\mathbb{C}$-vector space, $\dim_{\mathbb{C}} V \otimes_{\mathbb{C}} V = (\dim_{\mathbb{C}} V)^2 = k^2$, whence by restricton of scalars $\dim_{\mathbb{R}} V \otimes_{\mathbb{C}} V = 2\dim_{\mathbb{C}} V \otimes_{\mathbb{C}} V = 2k^2$.

On the other hand $\dim_{\mathbb{R}} V \otimes_{\mathbb{R}} V = (\dim_{\mathbb{R}} V)^2 = (2k)^2 = 4k^2$. Hence

$$\dim_{\mathbb{R}} V \otimes_{\mathbb{C}} V = 2k^2 \neq 4k^2 = \dim_{\mathbb{R}} V \otimes_{\mathbb{R}} V$$

so $V \otimes_{\mathbb{C}} V$ and $V \otimes_{\mathbb{R}} V$ are not isomorphic as $\mathbb{R}$-vector spaces. $\square$

(b) Let R be an integral domain (commutative), and let F be its fraction field. Prove that there is an isomorphism of F-modules, $F \otimes_R F \simeq F \otimes_F F \simeq F$, where the F-module structure on $F \otimes_R F$ is given by **extension of scalars** (i.e. tensor product of Type I).

Proof. We have shown previously that $F \otimes_F F \cong F$ as F-modules, so it suffices to show that $F \otimes_R F \cong F$ as F-modules. Consider the map $\Phi : F \times F \to F$ given by $\Phi(\frac{a}{r}, \frac{b}{s}) = \frac{ab}{rs}$. As, Φ is simply multiplication, it is R-bilinear. Hence, there exists an R-module homomorphism $\varphi : F \otimes_R F \to F$ such that $\varphi(\frac{a}{r} \otimes \frac{b}{s}) = \frac{ab}{rs}$. Moreover, this map is clearly an F-module homomorphism as

$$\frac{p}{q} \cdot \varphi(\frac{a}{r} \otimes \frac{b}{s}) = \frac{pab}{qrs} = \varphi(\frac{p}{q} \cdot (\frac{a}{b} \otimes \frac{r}{s})).$$

On the other hand, consider the map $\psi : F \to F \otimes_R F$ given by $\psi(\frac{a}{r}) = 1 \otimes \frac{a}{r}$. This map is clearly an F-module homomorphism by linearity. Moreover, as scalars can move, ψ and φ are mutual inverses. $\square$

Problem 4

The purpose of this problem is to classify all 2-dimensional $\mathbb{R}$-algebras (where $\mathbb{R}$ are the real numbers). That means, to classify (up to algebra isomorphism) those $\mathbb{R}$-algebras that are 2-dimensional $\mathbb{R}$ vector spaces.
Let A be a 2-dimensional $\mathbb{R}$-algebra (with 1).

(a) Let $u \in A$ be any element that is $\mathbb{R}$-linearly independent from 1. Prove that

(i) u generates A as an $\mathbb{R}$-algebra. That is, the minimal $\mathbb{R}$-subalgebra of A containing u and 1 is A itself.

(ii) The element u satisfies a quadratic equation $au^2 + bu + c = 0$, for some $a, b, c \in \mathbb{R}$ with $a \neq 0$. Conclude that A is necessarily commutative.

Proof. Noting that the subalgebra generated by u contains $\operatorname{span}_{\mathbb{R}}(\{1, u\})$ which has dimension 2 as an $\mathbb{R}$-vector space, it follows that the subalgebra generated by u is in fact A.

Since the subalgebra generated by u is A, it follows that there exist $a, b \in \mathbb{R}$ such that $u^2 = au + b1$, whence $u^2 - au - b = 0$. This implies the algebra A is commutative as multiplication is hence defined by the relations $u \cdot 1 = u = 1 \cdot u$ and $1 = 1 \cdot 1$, which are all commutative. $\square$

(b) Show that there exists some $v \in A$ which is $\mathbb{R}$-linearly independent from 1 and is such that $v^2 = -1$, or $v^2 = 1$, or $v^2 = 0$.

Proof. By part (a), there exists $a, b, c \in \mathbb{R}$ with $a \neq 0$ such that $au^2 + bu + c = 0$, i.e. $u^2 = \frac{-bu-c}{a}$. Let $v = xu + y \in A$ be arbitrary, with $x, y \in \mathbb{R}$ to be chosen later. A priori, we require $x \neq 0$ as we want v to be linearly independent from 1.

1. Case: $b = 0$. Take $y = 0$
   - $c = 0$. Then take any $x \in \mathbb{R}$, whence $v^2 = 0$.
   - $c \neq 0$. Then tale $x = \sqrt{|\frac{a}{c}|}$, so that $v^2 = \pm 1$.
2. Case: $b \neq 0$.
   - $c = 0$. Choose $x = \frac{2ay}{b}$, $y = 1$, then $v^2 = 1$.
   - $c \neq 0$. Choose $y = \frac{1}{\sqrt{\frac{4ac}{b^2}+1}}$, $x = \frac{2a}{b\sqrt{\frac{4ac}{b^2}+1}}$, then $v^2 = \pm 1$.

□

(c) Deduce from part (b) that A is isomorphic as an $\mathbb{R}$-algebra to one of the following: $\mathbb{R}[x]/(x^2+1)$, or $\mathbb{R}[x]/(x^2-1)$, or $\mathbb{R}[x]/(x^2)$.

Proof. Let v be as in part (b). As $\mathbb{R}[x]$ is the free $\mathbb{R}$ algebra generated by x, there exists a unique $\mathbb{R}$-algebra homomorphism $\varphi : \mathbb{R}[x] \to A$ such that $\varphi(x) = v$.

If $v^2 = -1$, then $(x^2+1) \subseteq \ker(\varphi)$. As $\mathbb{R}[x]$ is a PID and x^2+1 is irreducible in $\mathbb{R}[x]$, it follows that $\ker(\varphi) = (x^2+1)$ whence $A \cong \mathbb{R}[x]/(x^2+1)$.

Suppose $v^2 = 1$. Note that $x \pm 1 \notin \ker(\varphi)$ as v is linearly independent from 1. Hence $\ker(\varphi) = (x^2-1)$ whence $A \cong \mathbb{R}[x]/(x^2-1)$.

Lastly, if $v^2 = 0$, as $v \neq 0$, $x \notin \ker(\varphi)$ so $\ker(\varphi) = (x^2)$ whence $A \cong \mathbb{R}[x]/(x^2)$. □

(d) Prove that the algebras $\mathbb{R}[x]/(x^2+1)$, $\mathbb{R}[x]/(x^2-1)$, and $\mathbb{R}[x]/(x^2)$ are pairwise non-isomorphic. **Hint:** This can be shown with almost no computation.

Proof. Note first that, as x^2+1 is irreducible, (x^2+1) is maximal whence $\mathbb{R}[x]/(x^2+1)$ is a field and thus has no zero divisors, whereas $\mathbb{R}[x]/(x^2-1)$, and $\mathbb{R}[x]/(x^2)$ have zero divisors.

Observe that, in $\mathbb{R}[x]/(x^2)$, $x^2 \equiv 0$, whence $\mathbb{R}[x]/(x^2)$ has a nonzero square root of zero.

On the other hand, in $\mathbb{R}[x]/(x^2-1)$,

$$0 \equiv (ax+b)^2 \equiv a^2x^2 + 2abx + b^2 \equiv 2abx + a^2 + b^2$$

whence $a, b = 0$, so $ax + b = 0$. Thus $\mathbb{R}[x]/(x^2-1)$ has no nonzero square roots of zero. □

Problem 5

The purpose of this problem is to prove the following theorem: Let D be a finite dimensional division algebra over $\mathbb{R}$. Then D is isomorphic to $\mathbb{R}, \mathbb{C}$ or $\mathbb{H}$ (the quaternions). One way to proceed is to use the following steps:

(a) Let $\alpha \in D$ be an element $\mathbb{R}$-linearly independent from 1. Show that α satisfies a quadratic irreducible polynomial $p_\alpha(x) = x^2 + ax + b \in \mathbb{R}[x]$.

Proof. Since D is finite-dimensional over $\mathbb{R}$, there exists an $n \in \mathbb{N}$ such that the set $\{1, \alpha, \ldots, \alpha^n\}$ is $\mathbb{R}$-linearly dependent. Hence α is algebraic over $\mathbb{R}$, so the set $I_\alpha = \{f(x) \in \mathbb{R}[x] : f(\alpha) = 0\}$.
As I_α is an ideal and $\mathbb{R}[x]$ is a PID, there exists a (without loss of generality) monic polynomial $p_\alpha(x) \in \mathbb{R}[x]$ such that $I_\alpha = (p_\alpha)$. As α is algebraic, $p_\alpha \neq 0$. Moreover, p_α is nonconstant by $p_\alpha(\alpha) = 0$. Hence, p_α is not a unit in $\mathbb{R}[x]$. If $f \in I_\alpha = (p_\alpha)$ is irreducible, then in writing $f = gp_\alpha$ for some $g \in \mathbb{R}[x]$, irreducibility implies that $(f) = (p_\alpha) = I_\alpha$. Moreover, this implies that $\deg(f) = \deg(p_\alpha)$, so p_α being monic implies that p_α is the unique irreducible monic element of I_α.
As $\alpha \notin \mathbb{R} \cdot 1$, $\deg(p_\alpha) \geq 2$. By the Fundamental Theorem of Algebra, it follows then that p_α must be quadratic, so there exist $a, b \in \mathbb{R}[x]$ such that $p_\alpha(x) = x^2 + ax + b$.

$\square$

(b) Let $V = \{\alpha \in D : \alpha^2 \in \mathbb{R}_{\leq 0}\}$. Show that V is an $\mathbb{R}$-linear subspace of D. **Hint:** Show there is an $\mathbb{R}$-linear map $f : D \to \mathbb{R}$ with kernel V.

Proof. For $\alpha \in D$, define an $\mathbb{R}$-endomorphism T_α of D via left multiplication by α. This furnished a linear map $D \to \mathrm{End}_{\mathbb{R}}(D)$. We claim that V is the kernel of the composition of the $\mathbb{R}$-linear maps

$$D \to \mathrm{End}_{\mathbb{R}}(D) \xrightarrow{\mathrm{Tr}} \mathbb{R}.$$

Fix $\alpha \in D$ such that $\alpha \notin \mathbb{R} \cdot 1$. Then by part (a) there exist $a, b \in \mathbb{R}$ such that α satisfies a quadratic irreducible polynomial $p_\alpha(x) = x^2 + ax + b$. Observe that, for $v \in D$,

$$p_\alpha(T_\alpha)(v) = T_\alpha^2(v) + aT_\alpha(v) + b(v) = \alpha^2 v + a\alpha v + bv = (\alpha^2 + a\alpha + b\alpha)(v) = 0$$

so $p_\alpha(T_\alpha) = 0 \in \mathrm{End}_{\mathbb{R}}(D)$. Irreducibility of p_α then implies that p_α is the minimal polynomial for the operator $T\alpha$. Let $\chi_\alpha(x)$ be the characteristic polynomial for T_α. Then $p_\alpha(x) | \chi_\alpha(x)$ and there exists a $k \in \mathbb{N}$ such that $\chi_\alpha(x) | (p_\alpha(x))^k$. As χ_α is monic and p_α is irreducible, there exists an $l \in \mathbb{N}$ such that $\chi_\alpha(x) = (p_\alpha(x))^l$. By multinomial expansion,

$$\chi_\alpha(x) = (p_\alpha(x))^l = \sum_{\substack{n_1+n_2+n_3=l \\ n_1,n_2,n_3 \geq 0}} \binom{l}{n_1,\ n_2,\ n_3} x^{2n_1+n_2} a^{n_2} b^{n_3}$$

This polynomial has x^{2l-1} coefficient

$$\binom{l}{l-1,\ 1,\ 0} a = l \cdot a$$

However, the x^{2l-1} coefficient of χ_α is also $\pm\mathrm{Tr}(T_\alpha)$, so $\pm\mathrm{Tr}(T_\alpha) = l \cdot a$. Moreover, as $p_\alpha(x)$ is irreducible, $a^2 - 4b < 0 \implies b > \frac{a^2}{4} \geq 0$. Hence, if α is such that $\mathrm{Tr}(\alpha) = 0$, then $a = 0$ whence $0 = p_\alpha(\alpha) = \alpha^2 + b \implies \alpha^2 = -b \leq 0$, i.e. $\alpha \in V$. Conversely, suppose that $\alpha \in D \setminus \{0\}$ is such that $\alpha^2 < 0$. Then α is linearly independent from 1, so there exist $a, b \in \mathbb{R}$. such that $\alpha^2 + a\alpha + b = 0$. Note that, as $\alpha^2 \in \mathbb{R}$, linear independence of α from 1 implies that $a = 0$ and $\alpha^2 + b = 0$. Then, $\mathrm{Tr}(T_\alpha) = 0$, as desired. $\square$

(c) Define $B : V \times V \to \mathbb{R}$, $B(\alpha, \beta) := -\dfrac{\alpha\beta + \beta\alpha}{2}$. Show that B defines an inner product on V (i.e. B is a symmetric, positive definite bilinear form on V).

Proof. Observe that, for $\alpha, \beta \in V$, $\alpha^2, \beta^2, (\alpha+\beta)^2 \in \mathbb{R}$, whence $\alpha\beta + \beta\alpha = (\alpha+\beta)^2 - \alpha^2 - \beta^2 \in \mathbb{R}$, so B is in fact real-valued.

Fix $\alpha, \alpha', \beta, \beta' \in V$ and $\lambda \in \mathbb{R}$. Then

$$B(\alpha, \beta) = -\frac{\alpha\beta + \beta\alpha}{2} = -\frac{\beta\alpha + \alpha\beta}{2} = B(\beta, \alpha)$$

$$B(\alpha + \lambda\alpha', \beta) = -\frac{(\alpha + \lambda\alpha')\beta + \beta(\alpha + \lambda\alpha')}{2} = -\frac{\alpha\beta + \beta\alpha}{2} - \lambda\frac{\alpha'\beta + \beta\alpha'}{2} = B(\alpha, \beta) + \lambda B(\alpha', \beta).$$

$$B(\alpha, \beta + \lambda\beta') = -\frac{\alpha(\beta + \lambda\beta') + (\beta + \lambda\beta')\alpha}{2} = -\frac{\alpha\beta + \beta\alpha}{2} - \lambda\frac{\alpha\beta' + \beta'\alpha}{2} = B(\alpha, \beta) + \lambda B(\alpha, \beta'),$$

so B is a symmetric bilinear form. Moreover, as $\alpha \in V \setminus \{0\}$ implies that $\alpha^2 \in \mathbb{R}_{<0}$, we have then that

$$B(\alpha, \alpha) = -\frac{\alpha\alpha + \alpha\alpha}{2} = -\alpha^2 > 0$$

so B is also positive-definite. □

(d) Let W be a linear subspace of V that generates D as an $\mathbb{R}$-algebra. Let $n = \dim_{\mathbb{R}} W$. Choose an orthonormal basis of W, i.e. a basis $\{e_i\}$ of W such that $B(e_i, e_i) = 1$ for all i and $B(e_i, e_j) = 0$ for all $i \neq j$ (such a basis always exists). Using this orthonormal basis show that if $n \geq 2$, then D has a subalgebra isomorphic to $\mathbb{H}$.

Proof. We must first show that such a subspace W of V with the prescribed property actually exists. Let $\psi : D \to \mathbb{R}$ denote the linear map constructed in part (b), i.e. $\psi(\alpha) = \mathrm{Tr}(T_\alpha)$ where T_α is the left multiplication by α operator. We claim that $\operatorname{im}\psi \neq 0$, whence $\operatorname{im}\psi = \mathbb{R}$. To show this, consider $\lambda \in R \setminus \{0\}$. With respect to any $\mathbb{R}$-basis of D, the matrix of T_λ is diagonal with nonzero entries λ along the diagonal, so $\mathrm{Tr}(T_\lambda) = \lambda \dim_{\mathbb{R}} D \in \mathbb{R} \setminus \{0\}$, as desired.

By rank-nullity theorem,

$$\dim D = \dim \ker \psi + \dim \operatorname{im} \psi = \dim V + \dim \mathbb{R} = \dim V + 1$$

so $\dim V = \dim D - 1$. The remaining direct summand of D is spanned by 1 and is thus $\mathbb{R}$, so as the subalgebra generated by V contains 1 and V, it must be all of D.

Now suppose that W is a linear subspace of V that generates D as an $\mathbb{R}$-algebra. Let $n = \dim_{\mathbb{R}} W$. Choose an orthonormal basis $\{e_i\}_{i=1}^n$ of W with respect to B. Then, for $i \in \{1, \dots, n\}$,

$$1 = B(e_i, e_i) = -\frac{e_i^2 + e_i^2}{2} = -e_i^2 \implies e_i^2 = -1.$$

Also, for $i, j \in \{1, \dots, n\}$,

$$0 = B(e_i, e_j) = -\frac{e_ie_j + e_je_i}{2} \implies e_ie_j = -e_je_i.$$

Let A be the subalgebra of D generated by $\{1, e_1, e_2\}$. We will show that $A \cong \mathbb{H}$ as $\mathbb{R}$-algebras. □

(e) Bonus: Suppose $n \geq 2$. Prove that $A = H$. **Hint:** One way to proceed is to show that if $n > 2$, then the multiplication in D cannot be associative.