Problem Set 1
Algebra III

Bennett Rennier
bennett@brennier.com

Ex 1. Let R be a ring and n a natural number.

a) Show that $Z(\mathrm{M}_n(R)) = Z(R)$.

b) Show that the ring $\mathrm{M}_n(R)$ is simple if R is a skew field.

c) Show that $\mathrm{M}_n(R)$ is isomorphic to its opposite ring $\mathrm{M}_n(R)^o$ if R is commutative.

Proof.

a) Let $A = \sum_{i,j} a_{ij}e_{ij}$ be in the center of $\mathrm{M}_n(R)$. Then

$$\sum_j a_{\ell j}e_{\ell j} = \sum_{i,j} a_{ij}\delta_{\ell i}e_{\ell j} = \sum_{i,j} a_{ij}e_{\ell\ell}e_{ij} = e_{\ell\ell}A = Ae_{\ell\ell} = \sum_{i,j} a_{ij}e_{ij}e_{\ell\ell} = \sum_{i,j} a_{ij}\delta_{j\ell}e_{i\ell} = \sum_i a_{i\ell}e_{i\ell}.$$

Since the first term only has entries on the ℓth row and the last term only has entries on the ℓth row, we see that this means that $a_{i\ell} = a_{\ell i} = 0$ for $i \neq \ell$. As ℓ was arbitrary, we get that $a_{ij} = 0$ for all $i \neq j$, i.e. A is a diagonal matrix. This means A is of the form $\sum_i a_i e_{ii}$. Furthermore, we see that

$$a_k e_{jk} = \sum_i a_i\delta_{ki}e_{ji} = \sum_i a_i e_{jk}e_{ii} = e_{jk}A = Ae_{jk} = \sum_i a_i e_{ii}e_{jk} = \sum_i a_i\delta_{ij}e_{ik} = a_j e_{jk}$$

proving that all the diagonal entries of A must be the same constant, i.e. $A = \lambda \operatorname{Id}_n$ for some $\lambda \in R$. If $\lambda \notin Z(R)$, then there's some ρ such that $\lambda\rho \neq \rho\lambda$. This means that

$$(\lambda \operatorname{Id}_n)(\rho \operatorname{Id}_n) = \lambda\rho \operatorname{Id}_n \neq \rho\lambda \operatorname{Id}_n = (\lambda \operatorname{Id}_n)(\rho \operatorname{Id}_n).$$

which is a contradiction to $A \in Z(\mathrm{M}_n(R))$. Thus, it must be that $A = \lambda \operatorname{Id}_n$ for some $\lambda \in Z(R)$. Conversely, if $A = \lambda \operatorname{Id}_n \in Z(R)$, then for all matrices $B \in \mathrm{M}_n(R)$ we get that

$$BA = B\lambda \operatorname{Id}_n = \sum_{i,j} b_{ij}\lambda e_{ij} = \sum_{i,j} \lambda b_{ij}e_{ij} = \lambda \operatorname{Id}_n B = AB.$$

This proves that $Z(\mathrm{M}_n(R)) = \{\lambda \operatorname{Id}_n : \lambda \in Z(R)\}$ which we can identify simply as $Z(R)$.

b) Let I be a nonzero ideal of $\mathrm{M}_n(R)$ and let $A = \sum_{i,j} a_{ij}e_{ij}$ be a nonzero element of I, where $a_{\ell k} \neq 0$. Then we have that

$$e_{\ell\ell}Ae_{kk} = \sum_{i,j} a_{ij}e_{\ell\ell}e_{ij}e_{kk} = \sum_{i,j} a_{ij}\delta_{\ell i}e_{\ell j}e_{kk} = \sum_{i,j} a_{ij}\delta_{\ell i}\delta_{jk}e_{\ell k} = a_{\ell k}e_{\ell k}$$

is in I. From here we see that for any $1 \leq s, t \leq n$

$$e_{s\ell}(a_{\ell k}e_{\ell k})e_{kt} = a_{\ell k}\delta_{\ell\ell}e_{sk}e_{kt} = a_{\ell k}\delta_{\ell\ell}\delta_{kk}e_{st} = a_{\ell k}e_{st}$$

is also in I. Since R is a skew field, there is a $b \in R$ such that $ba_{\ell k} = 1$. Using this, we get that $(b\,\mathrm{Id}_n)(a_{\ell k}e_{st}) = (ba_{\ell k})e_{st} = e_{st}$ is in I. Since every matrix in $\mathrm{M}_n(R)$ is generated by elementary matrices and I contains all the elementary matrices, we have that $I = R$, proving that $\mathrm{M}_n(R)$ is simple.

c) If $A = \sum_{i,j} a_{ij}e_{ij}$, then define $A^T = \sum_{i,j} a_{ji}e_{ij}$. I claim that the map $\varphi : M_n(R) \to M_n(R)^o$ where $\varphi(A) = A^T$ is an isomorphism. We see pretty easily from the definition of A^T that this map is injective and surjective. To prove that φ is multiplicative, let $B = \sum_{ij} b_{ij}e_{ij}$ and check that

$$\varphi(AB) = (AB)^T = \left(\left(\sum_{i,j} a_{ij}e_{ij}\right)\left(\sum_{i,j} b_{ij}e_{ij}\right)\right)^T = \left(\sum_{i,j}\sum_{k} a_{ik}b_{kj}e_{ij}\right)^T = \sum_{i,j}\sum_{k} a_{jk}b_{ki}e_{ij}$$
$$= \sum_{i,j}\sum_{k} b_{ki}a_{jk}e_{ij} = \left(\sum_{i,j} b_{ji}e_{ij}\right)\left(\sum_{i,j} a_{ji}e_{ij}\right) = B^T A^T = \varphi(A) \cdot_{opp} \varphi(B).$$

To prove that φ is linear, we see that

$$\varphi(\alpha A + B) = (\alpha A + B)^T = \left(\sum_{i,j}(\alpha a_{ij} + b_{ij})e_{ij}\right)^T = \sum_{i,j}(\alpha a_{ji} + b_{ji})e_{ij}$$
$$= \alpha A^T + B^T = \alpha\varphi(A) + \varphi(B).$$

This proves that φ is an isomorphism. □

Ex 2. Let V be a k-vector space, $R = \mathrm{End}_k(V)$ and f an element of R.

a) Show that the following statements are equivalent:

(i) f has a right inverse in R.

(ii) f is not a right zero divisor in R.

(iii) f is surjective.

If V is infinite-dimensional, given an example of such an f which is *not* in R^*.

b) Show that the following statements are equivalent:

(i) f has a left inverse in R.

(ii) f is not a left zero divisor in R.

(iii) f is injective.

If V is infinite-dimensional, given an example of such an f which is *not* in R^*.

c) Show that R is *not* simple if V is infinite-dimensional.

Proof.

a) i $\implies$ ii) Suppose f has a right inverse g, that is $f \circ g = \mathrm{Id}_V$. If $h \circ f = 0$ for some $h \in R$, then

$$h = h \circ \mathrm{Id}_V = h \circ f \circ g = 0 \circ g = 0$$

which proves that f is not a right zero divisor.

ii $\implies$ iii) Suppose contrapositively that f is not surjective. Let $\{e_i\}_{i \in I}$ be a basis of $f(V)$ (possibly an infinite basis). Since f is not surjective, this is not a basis of V itself. Extend this basis with the elements $\{d_j\}_{j \in J}$ to form a basis of V. Let g be the linear map such that $g(e_i) = 0$ and $g(d_j) = d_j$. We see then that $g \neq 0$ and $g \circ f = 0$. This means f is a right zero divisor. By the contrapostive, if f is not a right zero divisor, then f is surjective.

iii $\implies$ i) Let $\{e_i\}_{i \in I}$ be a basis of V. Since f is surjective, there exists a $v_i \in V$ such that $f(v_i) = e_i$. We define $g(e_i) = v_i$, which uniquely defines g as we know what it does on basis elements. This means that $(f \circ g)(e_i) = f(g(e_i)) = f(v_i) = e_i$. Since $f \circ g$ is the identity on the basis elements, it must be that $f \circ g = \mathrm{Id}_V$. This proves f has a right inverse.

Let V be a vector space with countably infinite basis $\{e_i\}_{i \geq 0}$. Let $f : V \to V$ be the linear map

$$f(e_i) = \begin{cases} 0 & \text{if } i = 0 \\ e_{i-1} & \text{if } i > 0 \end{cases}.$$

We see then that f is surjective (as $f(e_{i+1}) = e_i$ for $i \geq 0$). However, since $f(e_0) = 0 = f(0)$, we also see that f is not injective. By part (b) this means f does not have a left inverse, proving f is not invertible.

b) i $\implies$ ii) Suppose f has a left inverse g, that is $g \circ f = \mathrm{Id}_V$. If $f \circ h = 0$ for some $h \in R$, then

$$h = \mathrm{Id}_V \circ h = g \circ f \circ h = g \circ 0 = 0$$

which proves that f is not a left zero divisor.

ii $\implies$ iii) Suppose contrapositively that f is not injective. Let $\{e_i\}_{i \in I}$ be a basis of $\ker(V)$ (possibly an infinite basis). Since f is not injective, this basis has at least one non-zero vector in it. Extend this basis with the elements $\{d_j\}_{j \in J}$ to form a basis of V. Let g be the linear map such that $g(e_i) = e_i$ and $g(d_j) = 0$. We see then that $g \neq 0$ and $f \circ g = 0$. This means f is a left zero divisor. By the contrapositive, if f is not a left zero divisor, then f is injective.

iii $\implies$ i) Let $\{e_i\}_{i \in I}$ be a basis of V. Since f is injective, $\{f(e_i)\}_{i \in I}$ is linearly independent. Extend this linearly independent set into a basis of V with the elements $\{d_j\}_{j \in J}$. Let g be the linear map such that $g(f(e_i)) = e_i$ and $g(d_j) = d_j$. Thus we have that $(g \circ f)(e_i) = g(f(e_i)) = e_i$. Since $g \circ f$ is the identity on all the basis elements, it must be that $g \circ f = \mathrm{Id}_v$, proving that f has a left inverse.

Let V be a vector space with countably infinite basis $\{e_i\}_{i \geq 0}$. Let $f : V \to V$ be the linear map where $f(e_i) = e_{i+1}$. We see then that f is injective as it's injective on the basis elements. Since f is injective, the elements $\{f_{e_i}\}_{i \geq 0}$ are linearly independent and form a basis of $\mathrm{im}(f)$. However, $\{f(e_i)\}_{i \geq 0} = \{e_i\}_{i \geq 1}$. As e_0 is linearly independent from this set, it cannot be in the image of f. Thus, f is not surjective and by part (a), f does not have a right inverse; that is $f \notin R^*$.

c) Let $R = \mathrm{End}_k(V)$ where V is an infinite-dimensional k-vector space. Let $I = \{f \in R : \mathrm{rank}(f) < \infty\}$. I claim that this is an ideal of R. We see that if $f, g \in I$, then the image

of $f+g$ is contained in $\text{im}(f)+\text{im}(g)$. Since both of these are finite dimensional, we have that $\text{rank}(f+g)<\infty$, so $f+g\in I$. Additionally, if $f\in I$ and $g\in R$, then the image of $f\circ g$ is contained in the image of f, which is finite-dimensional, so $f\circ g\in I$. Lastly, since the image of $g\circ f$ is simply $g(\text{im}(f))$, we see that it's also finite-dimensional as it's the image of a finite-dimensional subspace. Thus, $g\circ f\in I$. This proves that I is an ideal. We note that $I\neq R$ as $\text{Id}_V\notin I$ and $I\neq\{0\}$ as for any $v\in V$ we have that $p_v\in I$ where p_v is the projection map onto v. □

Ex 3.

a) If R is a 3-dimensional k-algebra which is not commutative, show that $Z(R)=k$.

b) Construct an example of a non-commutative 3-dimensional k-algebra R.

Proof.

a) Let R be a 3-dimensional k-algebra. Suppose that $Z(R)$ contained an element not in k, call this element e_2. This means we can extend to a basis $\{e_1,e_2,e_3\}$ of R where we identify ke_1 as simply k and $\langle e_1,e_2\rangle\subseteq Z(R)$. However, since both e_1 and e_2 are in the center, we have that $e_1e_3=e_3e_1$ and that $e_2e_3=e_3e_2$. This proves that $e_3\in Z(R)$ as well as it commutes with all basis elements. Thus $\langle e_1,e_2,e_3\rangle=R\subseteq Z(R)$; proving that $R=Z(R)$. By the contrapositive, if R is non-commutative 3-dimensional k-algebra, then $Z(R)=k$.

b) Take for example the set of upper triangular 2×2 matrices over some field k, that is matrices of the form

$$\begin{bmatrix}a & b\\ 0 & c\end{bmatrix}$$

where $a,b,c\in k$. We can clearly see that this is three-dimensional; it can be generated by $\{e_{11},e_{12},e_{22}\}$ where e_{ij} is an elementary matrix. We also see that

$$\begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix}\begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix}=\begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix},\qquad \begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix}=\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}$$

which proves that this k-algebra is non-commutative. □

Ex 4. Give an example (including arguments) of a group G such that the center $Z(k[G])$ of the group algebra $k[G]$ is strictly bigger than the subalgebra $k[Z(G)]$.

Proof. For this we'll obviously need a non-abelian group to begin with, so let $G=D_3$ (the Dihedral group of order 6). We note that with the representation $D_3=\langle r,s\mid r^3=s^2=1,sr=r^{-1}s\rangle$ the conjugacy classes of D_3 are simply $\{e\}$, $\{r,r^2\}$, and $\{s,sr,sr^2\}$. I claim that the element $r+r^2\in k[D_3]$ is in the center of the algebra but is not in the subalgebra $k[Z(D_3)]$. It is easy to see that the latter is true as the center of D_3 is trivial, meaning $k[Z(D_3)]$ is actually just the field k in $k[D_3]$ (or technically what we've identified as k in the algebra). To prove that $r+r^2$ is in the center, we need only to show that it commutes with all the basis elements. Furthermore, since every element of D_3 can be written in the form s^ir^j where $i\in\{0,1\}$ and $j\in\{0,1,2\}$, we only need to show that $r+r^2$ commutes with s and r. We can prove this directly as

$$(r+r^2)\cdot r=rr+r^2r=rr+rr^2=r\cdot(r+r^2)$$

and that

$$(r+r^2)\cdot s=rs+r^2s=sr^{-1}+sr^{-2}=sr^2+sr^1=sr+sr^2=s\cdot(r+r^2).$$

This proves what was claimed. Thus, $r + r^2$ is an element of the center of $k[D_3]$ that is not in the subalgebra $k[Z(D_3)]$. □

Ex 5. Let a, b be elements $a, b, a', b' \in k^*$ and (a, b) the corresponding quaternion algebra over k.

a) Prove that (a, b) is central k-algebra.

b) Prove that (a, b) is a simple k-algebra.

Proof.

a) Let $x = k_1 + k_2e_2 + k_3e_3 + k_4e_4$ be an arbitary element in the center of (a, b). That would mean that

$$\begin{aligned} 0 = e_2x - xe_2 &= e_2(k_1 + k_2e_2 + k_3e_3 + k_4e_4) - (k_1 + k_2e_2 + k_3e_3 + k_4e_4)e_2 \\ &= e_2(k_3e_3 + k_4e_4) - (k_3e_3 + k_4e_4)e_2 = (ak_4e_3 + k_3e_4) - (-ak_4e_3 - k_4e_3) = 2ak_4e_3 + 2k_3e_4. \end{aligned}$$

As $\text{char}(k) \neq 2$, we can divide by 2 and get that

$$ak_4e_3 + k_3e_4 = 0.$$

As our basis elements are invertible and thus have no zero divisors, this proves that $k_3 = k_4 = 0$. Using a similar trick, we get that

$$0 = e_3x - xe_3 = e_3(k_1 + k_2e_2) - (k_1 + k_2e_2)e_3 = (k_1e_3 - k_2e_4) - (k_1e_3 + k_2e_4) = -2k_2e_4.$$

Again, since $\text{char}(k) \neq 2$, we have that $k_2 = 0$. This proves that $x \in k$ and thus that (a, b) is a central k-algebra.

b) Let I be some non-zero ideal of (a, b) and let $x = k_1 + k_2e_2 + k_3e_3 + k_4e_4$ be some non-zero element of I. By similar calculations as in part (a), we know that

$$e_2x - xe_2 = 2ak_4e_3 + 2k_3e_4$$

and that

$$\begin{aligned} e_2x + xe_2 &= e_2(k_1 + k_2e_2 + k_3e_3 + k_4e_4) + (k_1 + k_2e_2 + k_3e_3 + k_4e_4)e_2 \\ &= (k_1 + k_2e_2 - k_3e_3 - k_4e_4)e_2 + (k_1 + k_2e_2 + k_3e_3 + k_4e_4)e_2 \\ &= (k_1 + k_2e_2)2e_2 = 2ak_2 + 2k_1e_2. \end{aligned}$$

Both of these calculations are in I and since at least one $k_j \neq 0$, we know that at least one of them is non-zero. We note that if $2ak_4e_3 + 2k_3e_4$ is the non-zero element, then we have that

$$e_3(2ak_4e_3 + 2k_3e_4) = 2abk_4 - 2bk_3e_2$$

is in I. Thus, we can assume without loss of generality that x is of the form $k_1 + k_2e_2$. By a similar trick, we see that either

$$e_3x + xe_3 = e_3(k_1 + k_2e_2) + (k_1 + k_2e_2)e_3 = (k_1e_3 - k_2e_4) + (k_1e_3 + k_2e_4) = 2k_1e_3$$

or

$$e_3x - xe_3 = e_3(k_1 + k_2e_2) - (k_1 + k_2e_2)e_3 = (k_1e_3 - k_2e_4) - (k_1e_3 + k_2e_4) = -2k_2e_4$$

is a non-zero element of I. If it's the former, then $e_3(2k_1e_3) = 2k_1b \in I$ and if it's the latter, then $e_4(-2k_2e_4) = 2abk_2 \in I$. Either way, I contains a non-zero element of k. As all non-zero elements of k are invertible, this means that $1 \in I$, proving that I is the whole algebra. Thus, (a, b) is a simple k-algebra. □

Ex 6. For elements $a, b, a', b' \in k^*$, prove that

a) (a, b) and (b, a) are isomorphic k-algebras.

b) (a, b) and (a', b') are isomorphic k-algebras if the quotients a'/a and b'/b are squares in k.

c) Now classify, up to isomorphism, all quaternion algebras over field $k = \mathbb{R}$ of real numbers.

Proof. We recall that the algebra (a, b) can be uniquely determined by the equations $e_2^2 = a$, $e_3^2 = b$, and $e_2e_3 = -e_3e_2 = e_4$.

a) Let φ be the linear map on (a, b) such that

$$\varphi(e_i) = \begin{cases} e_1 & \text{if } i = 1 \\ -e_3 & \text{if } i = 2 \\ -e_2 & \text{if } i = 3 \\ -e_4 & \text{if } i = 4. \end{cases}$$

We then see that

$$\begin{aligned} \varphi(e_2)\varphi(e_2) &= (-e_3)(-e_3) = e_3e_3 = b \\ \varphi(e_3)\varphi(e_3) &= (-e_2)(-e_2) = e_2e_2 = a \\ \varphi(e_2)\varphi(e_3) &= (-e_3)(-e_2) = e_3e_2 = -e_4 = \varphi(e_4) \\ \varphi(e_3)\varphi(e_2) &= (-e_2)(-e_3) = e_2e_3 = e_4 = -\varphi(e_4). \end{aligned}$$

This means that φ is a linear map where $\varphi(e_2)\varphi(e_2) = b$, $\varphi(e_3)\varphi(e_3) = a$, and $\varphi(e_2)\varphi(e_3) = -\varphi(e_3)\varphi(e_2) = \varphi(e_4)$. We see that these equations uniquely defined the image of φ to be the algebra (b, a). Thus, φ is an isomorphism from (a, b) to (b, a).

b) Suppose $a'/a = \alpha^2$ and $b'/b = \beta^2$. Let φ be the linear map on (a, b) such that

$$\varphi(e_i) = \begin{cases} e_1 & \text{if } i = 1 \\ \alpha e_2 & \text{if } i = 2 \\ \beta e_3 & \text{if } i = 3 \\ \alpha\beta e_4 & \text{if } i = 4. \end{cases}$$

We then see that

$$\begin{aligned} \varphi(e_2)\varphi(e_2) &= (\alpha e_2)(\alpha e_2) = \alpha^2 e_2e_2 = \alpha^2 a = a' \\ \varphi(e_3)\varphi(e_3) &= (\beta e_3)(\beta e_3) = \beta^2 e_3e_3 = \beta^2 b = b' \\ \varphi(e_2)\varphi(e_3) &= (\alpha e_2)(\beta e_3) = \alpha\beta e_2e_3 = \alpha\beta e_4 = \varphi(e_4) \\ \varphi(e_3)\varphi(e_2) &= (\beta e_3)(\alpha e_2) = \beta\alpha e_3e_2 = -\alpha\beta e_4 = -\varphi(e_4). \end{aligned}$$

This means that φ is a linear map where $\varphi(e_2)\varphi(e_2) = a'$, $\varphi(e_3)\varphi(e_3) = b'$, and $\varphi(e_2)\varphi(e_3) = -\varphi(e_3)\varphi(e_2) = \varphi(e_4)$. We see that these equations uniquely defined the image of φ to be the algebra (a', b'). Thus, φ is an isomorphism from (a, b) to (a', b').

c) Let (a, b) be a quaternion algebra over $\mathbb{R}$. If we let $\operatorname{sign}(x) = x/|x|$ from $\mathbb{R}$ to $\{-1, 1\}$, then $a/\operatorname{sign}(a)$ and $b/\operatorname{sign}(b)$ are both positive and thus both squares. By part (b), this proves that $(a, b) \simeq (\operatorname{sign}(a), \operatorname{sign}(b))$. Thus all quaternion algebras over $\mathbb{R}$ are isomorphic to either

$(1,1)$, $(-1,1)$, $(1,-1)$, or $(-1,-1)$. By part (a), $(-1,1) \simeq (1,-1)$. Now let φ be a linear map on $(1,-1)$ such that

$$\varphi(e_i) = \begin{cases} e_1 & \text{if } i = 1 \\ e_2 & \text{if } i = 2 \\ e_4 & \text{if } i = 3 \\ e_3 & \text{if } i = 4. \end{cases}$$

We then see that

$$\begin{aligned}
&\varphi(e_2)\varphi(e_2) = e_2e_2 = a = 1 \\
&\varphi(e_3)\varphi(e_3) = e_4e_4 = -ab = -(1)(-1) = 1 \\
&\varphi(e_2)\varphi(e_3) = e_2e_4 = e_2(e_2e_3) = (e_2e_2)e_3 = ae_3 = e_3 = \varphi(e_4) \\
&\varphi(e_3)\varphi(e_2) = e_4e_2 = (e_2e_3)e_2 = (-e_3e_2)e_2 = -e_3(e_2e_2) = -e_3a = -e_3 = -\varphi(e_4).
\end{aligned}$$

This means that φ is a linear map where $\varphi(e_2)\varphi(e_2) = 1$, $\varphi(e_3)\varphi(e_3) = 1$, and $\varphi(e_2)\varphi(e_3) = -\varphi(e_3)\varphi(e_2) = \varphi(e_4)$. We see that these equations uniquely defined the image of φ to be the algebra $(1,1)$. Thus, φ gives us an isomorphism between $(1,-1)$ and $(1,1)$.

Finally, we note that the quaternion norm on $(-1,-1)$ is $N(x) = x_1^2 + x_2^2 + x_3^2 + x_4^2$, which is anisotropic over $\mathbb{R}$. This proves that $(-1,-1)$ has no zero divisors, making $(-1,-1)$ into a division ring. On the other hand the quaternion norm on $(1,1)$ is $N(x) = x_1^2 - x_2^2 - x_3^2 + x_4^2$, which is definitely not anisotropic. This means $(1,1)$ is not a division ring, proving that $(-1,-1)$ can't be isomorphic to $(1,1)$. Thus, all quaternion algebras over the field $\mathbb{R}$ are isomorphic to one of the distinct algebras $(-1,-1)$ or $(1,1)$. $\square$