Representation Theory
Homework 4

Ari Feiglin

1 Problem

(1) Show that R has the structure of an R^{op} module given by multiplication on the right.

(2) Show that $R \to \mathrm{end}_{R^{\mathsf{op}}}(R)$ given by $r \mapsto [x \mapsto rx]$ is a ring isomorphism.

(3) Show that there is an isomorphism $\mathrm{end}_R(R) \cong R^{\mathsf{op}}$ ($\mathrm{end}_R(R)$ is the ring of R-morphisms of R, considered as an R-module).

(4) Let D be a division ring and M a finitely-generated D-module. Show that if $M \cong D^n$ then $\mathrm{end}_D(M) \cong M_n(D^{\mathsf{op}})$.

(5) Let $R' = M_n(D)$ where D is a division ring. Show that R' is semisimple and all of its simple modules are isomorphic to D^n.

(1) This is simple, we just need to show that $(a^{\mathsf{op}}, b) \mapsto ba$ is biadditive and satisfies $(a \cdot^{\mathsf{op}} a', b) = (a, (a', b))$. Biadditivity is clear. And we note $(a \cdot^{\mathsf{op}} a', b) = (a'a, b) = ba'a = (a, (a', b))$ as required.

(2) We claim that for $r \in R$, $x \mapsto rx$ is an R^{op}-morphism. It is clearly additive, and $a^{\mathsf{op}}x \mapsto r(a^{\mathsf{op}}x) = r(xa) = rxa$ which is equal to a^{op} times the image of x. So the morphism is well-defined. Let us denote by $f_r\colon x \mapsto rx$. Now $r \mapsto f_r$ is a ring morphism: $f_{r+s}\colon x \mapsto rx + sx$ so $f_{r+s} = f_r + f_s$ as required and $f_{rs}\colon x \mapsto rsx$ and so $f_{rs} = f_r \circ f_s$. It is also clearly injective since if $x \mapsto rx$ is the identity then $1 \mapsto r1 = r$ but as it is the identity $1 \mapsto 1$ so $r = 1$.

Now let $f \in \mathrm{hom}_{R^{\mathsf{op}}}(R, R)$ be a module morphism. Then we claim $f = f_{f1}$. Indeed, $f(r) = f(r^{\mathsf{op}}1) = r^{\mathsf{op}}f(1) = f(1)r$, i.e. $r \mapsto f(1)r$ so f is indeed equal to $f_{f(1)}$.

(3) Map $f \in \mathrm{end}_R(R)$ to $f(1)$. This is a ring morphism: $f + g \mapsto (f+g)(1) = f1 + g1$ and $f \circ g \mapsto f(g(1)) = f(g(1) \cdot 1) = g(1)f(1) = f(1) \cdot^{\mathsf{op}} g(1)$. It is injective since every endomorphism f is determined by its image on 1: $f(r) = rf(1)$. And it is surjective: let $x \in R^{\mathsf{op}}$, then define $f(r) = rx$. This is an R-endomorphism: it is clearly additive, and $f(rs) = rsx = rf(s)$. And clearly $f \mapsto x$.

(4) We need to show that $\mathrm{end}_D(D^n) \cong M_n(D^{\mathsf{op}})$. We want to map $f \in \mathrm{end}_D(D^n)$ to a matrix $[f_{ij}] \in M_n(D^{\mathsf{op}})$ such that for all $\bar{d} \in D^n$:

$$f\bar{d} = [f_{ij}]\bar{d}$$

This implies that $\pi_i \circ f\bar{d} = \pi_i([f_{ij}]\bar{d})$ where $\pi\colon D^n \to D$ is the ith projection morphism. So

$$\pi_i \circ f\bar{d} = \sum_{j=1}^{n} f_{ij} \cdot^{\mathsf{op}} d_j = \sum_{j=1}^{n} d_j f_{ij}$$

Now let $\bar{d} = e_\ell$ be a standard basis vector (equal to $\iota_\ell 1$ where $\iota_\ell\colon D \to D^n$ is the inclusion morphism), then

$$\pi_i \circ fe_\ell = \sum_{j=1}^{n} \delta_{j\ell} f_{ij} = f_{i\ell}$$

So we define $f_{ij} = \pi_i \circ fe_j = \pi_i \circ f \circ \iota_j 1$. And indeed for $\bar{d} \in D^n$ we have

$$\pi_i[f]\bar{d} = \sum_{j=1}^{n} f_{ij} \cdot^{\mathsf{op}} d_j = \pi_i \sum_{j=1}^{n} (f\iota_j 1) \cdot^{\mathsf{op}} d_j = \pi_i \sum_{j=1}^{n} d_j f\iota_j 1$$

Since f, ι_i are D-morphisms, we get

$$= \pi_i \sum_{j=1}^{n} f\iota_j(d_j) = \pi_i f \sum_{j=1}^{n} \iota_j(d_j)$$

Clearly $\sum_j \iota_j(d_j) = \bar{d}$ and so this is equal to

$$= \pi_i f\bar{d}$$

Thus we get $[f]\bar{d} = f\bar{d}$ as required. Notice that this $[f]$ is unique (since we showed that existence implies a specific matrix).

Now, we claim that this is a ring isomorphism. It is clearly additive: $(f+g)_{ij} = \pi_i(f+g)\iota_j 1 = \pi_i f\iota_j 1 + \pi_i g\iota_j 1 = f_{ij} + g_{ij}$. And it is multiplicative: $(f \circ g)_{ij} = \pi_i fg\iota_j 1$, while $[f_{ij}][g_{ij}]$ at the ijth index is equal to

$$\sum_{\ell=1}^{n} f_{i\ell} \cdot^{\mathsf{op}} g_{\ell j} = \sum_{\ell=1}^{n} (\pi_\ell g\iota_j 1)(\pi_i f\iota_\ell 1)$$

Now since π_i, f, ι_i are D-morphisms, we get that this is equal to

$$= \sum_{\ell=1}^{n} \pi_i f\iota_\ell(\pi_\ell g\iota_j 1) = \pi_i f \sum_{\ell=1}^{n} \iota_\ell(\pi_\ell g\iota_j 1) = \pi_i f \sum_{\ell=1}^{n} (\iota_\ell \pi_\ell)(g\iota_j 1)$$

Now notice that for $a \in D^n$, we have

$$\sum_{\ell=1}^{n} \iota_\ell \pi_\ell(a) = a$$

Indeed, $\iota_\ell \pi_\ell(a)$ maps to the vector with zeroes except for at the ℓth index, when it is equal to a_ℓ. So we have that

$$= \pi_i fg\iota_j 1$$

as required.

Now we must show that it is a bijection. It is indeed injective: as we showed $f\bar{d} = [f]\bar{d}$. Thus if $[f] = I$ then $f\bar{d} = \bar{d}$ for all $\bar{d} \in D^n$, so $f = \mathrm{id}$. And it is surjective: given $[f_{ij}] \in M_n(D^{\mathsf{op}})$, define $f \in \mathrm{end}_D(D^n)$ by $f\bar{d} = [f_{ij}]\bar{d}$. This is clearly a D-morphism: $f(a\bar{d}) = [f](a\bar{d}) = a[f]\bar{d} = af\bar{d}$ and $f(\bar{d}+\bar{c}) = [f](\bar{d}+\bar{c}) = [f]\bar{d}+[f]\bar{c} = f\bar{d}+f\bar{c}$. And since the image of f is the unique matrix satisfying $f\bar{d} = [f]\bar{d}$, $[f]$ is this matrix.

(5) Let us define $M_\ell = \{[m_{ij}] \in M_n(D) \mid m_{ij} = 0 \text{ if } j \neq \ell\}$. This is indeed a submodule of R': for $M \in R'$ and $m \in M_\ell$, $[Mm]_{ij} = \sum_{t=1}^{n} M_{it} m_{tj}$ which is zero when $j \neq \ell$. Clearly we have that

$$M_n(D) = \bigoplus_{\ell=1}^{n} M_\ell$$

Now, we claim that M_ℓ are simple and isomorphic to D^n. Clearly the map $M_\ell \to D^n$ given by $m \mapsto (m_{1\ell}, \ldots, m_{n\ell})$ is a bijection. It is also an R'-morphism: for $M \in M_\ell$, $[Mm]_{i\ell} = \sum_{t=1}^{n} M_{it} m_{t\ell}$ which is equal to $M(m_{1\ell}, \ldots, m_{n\ell})$. Thus $M_\ell \cong D^n$ as required.

Now we claim that M_ℓ is simple. Indeed, we claim that for $0 \neq m \in M_\ell$, $R'm = M_\ell$. This would mean that there are no nontrivial proper submodules of M_ℓ. Let $E_{ij} \in M_n(D)$ be the matrix of zeroes except in the ijth index, which is equal to 1. A simple calculation shows

$$E_{ij}E_{\ell t} = \begin{cases} E_{it} & j = \ell \\ 0 & \text{else} \end{cases}$$

Let $0 \neq m \in M_\ell$, so $m = \sum_{i=1}^n m_i E_{i\ell}$, and let $1 \leq k \leq n$. Then notice that $E_{kj}m = \sum_{i=1}^n m_i E_{kj} E_{i\ell} = m_j E_{k\ell}$, so $m_j E_{k\ell} \in R'm$. Now let j such that $m_j \neq 0$ (since $m \neq 0$), and since D is a division ring, this means that $m_j^{-1} I \in R'$ so $E_{k\ell} \in R'm$. This is true for all k, and so $E_{1\ell}, \ldots, E_{n\ell} \in R'm$. These generate M_ℓ, and so $R'm = M_\ell$ (explicitly, let $m' = \sum_i m_i' E_{i\ell} \in M_\ell$ then $m' = \sum_i (m_i' I) E_{i\ell} \in R'E_{1\ell} + \cdots + R'E_{n\ell} \subseteq R'm$; so $M_\ell \subseteq R'm$).

So we have found simple modules $M_1, \ldots, M_n$ such that $M_i \cong D^n$ and $R' = M_1 \oplus \cdots \oplus M_n$. If M is another simple R' module, then M is isomorphic to some M_i and thus D^n. Indeed, let $0 \neq m \in M$ and define $f(r) = rm$; this is a nonzero R-morphism $R \to M$. Thus it defines morphisms $f_i = f \circ \iota_i \colon M_i \to M$ between simple modules. Since f is nonzero, not all f_i are zero. By Schur this means that at least one f_i is an isomorphism, i.e. $M \cong M_i$ as required.

2 Problem

Let $\mathbb{Z}, \mathbb{Q}$ be viewed as $\mathbb{Z}$-modules. For p prime, let $\mathbb{Z} \subseteq \mathbb{Z}[1/p] \subseteq \mathbb{Q}$ be the submodule

$$\mathbb{Z}[1/p] = \left\{ \frac{a}{p^k} \;\middle|\; a \in \mathbb{Z}, k \geq 0 \right\}$$

(1) Find all the $\mathbb{Z}$-submodules of $\mathbb{Z}$ and $\mathbb{Z}[1/p]/\mathbb{Z}$. Show that the former is Noetherian but not Artinian, and the latter is Artinian but not Noetherian.

(2) Is $\mathbb{Q}/\mathbb{Z}$ Artinian?

(3) Describe all simple $\mathbb{Z}$-modules, and show that $\mathbb{Q}$ has neither a simple $\mathbb{Z}$ submodule nor a simple quotient $\mathbb{Z}$-module.

(1) If A is a $\mathbb{Z}$-module (i.e. an Abelian group), a $\mathbb{Z}$-submodule of A is simply a subgroup of A. In $\mathbb{Z}$'s case, all of its submodules (equivalently, subgroups, or equivalently ideals) are of the form $n\mathbb{Z}$. Thus $\mathbb{Z}$ is Noetherian: it has no infinite increasing submodules: if $n_1\mathbb{Z} \subset n_2\mathbb{Z} \subset \cdots$ then n_2 divides n_1 and so on, implying that n_1 has infinite distinct divisors, a contradiction. But $\mathbb{Z}$ is not Artinian: $2n\mathbb{Z} \subset n\mathbb{Z}$ (proper subset), and as such $\left\{2^k\mathbb{Z}\right\}_{k \geq 0}$ forms an infinite strictly decreasing sequence of submodules.

Recall the correspondence theorem: there is a one-to-one correspondence between subgroups of G/N and subgroups of G containing N. So let us study the subgroups of $\mathbb{Z}[1/p]$. Notice that

$$\mathbb{Z}[1/p] = \bigcup_{k \geq 0} \left\langle \frac{1}{p^k} \right\rangle \subseteq \mathbb{Q}$$

Where $\left\langle 1/p^k \right\rangle$ is the cyclic subgroup generated by $1/p^k$, i.e. $1/p^k\mathbb{Z}$. and $\left\langle 1/p^k \right\rangle \subseteq \left\langle 1/p^{k+1} \right\rangle$ forms an increasing sequence of cyclic subgroups of $\mathbb{Q}$. So let $A \leq \mathbb{Z}[1/p]$ be a subgroup; if it is contained in some $\left\langle 1/p^k \right\rangle$ then it is cyclic, and thus of the form $A = \left\langle a/p^k \right\rangle = a/p^k\mathbb{Z}$. Since we are concerned with subgroups containing $\mathbb{Z}$, we want to know when $a/p^k\mathbb{Z}$ contains $\mathbb{Z}$, equivalently 1. This occurs iff $1 \in a/p^k\mathbb{Z}$ i.e. iff $p^k \in a\mathbb{Z}$ iff a divides p^k, i.e. $a = p^\ell$ for $0 \leq \ell \leq k$. This means that

$$A = \frac{p^\ell}{p^k}\mathbb{Z} = p^{\ell - k}\mathbb{Z}$$

Thus subgroups of $\mathbb{Z}[1/p]$ containing A and contained in some $1/p^k\mathbb{Z}$ are precisely those of the form $1/p^k\mathbb{Z}$. Now notice that $(1/p^k\mathbb{Z})/\mathbb{Z} \cong \mathbb{Z}/p^k\mathbb{Z}$, given by $n + p^k\mathbb{Z} \mapsto n/p^k + \mathbb{Z}$. Note then that this gives us an infinite strictly increasing sequence of $\mathbb{Z}$-submodules:

$$\frac{\mathbb{Z}}{\mathbb{Z}} \subseteq \frac{1/p\mathbb{Z}}{\mathbb{Z}} \subseteq \frac{1/p^2\mathbb{Z}}{\mathbb{Z}} \subseteq \cdots$$

So $\mathbb{Z}[1/p]/\mathbb{Z}$ is not Noetherian.

Otherwise, if $A \cap \langle 1/p^k \rangle \neq \emptyset$ for all $k \geq 0$ then there exists an $n_k > 0$ for all $k \geq 0$ such that $n_k/p^k \in A$ and $\gcd(p, n_k) = 1$. Since we are interested in when $\mathbb{Z} \subseteq A$, we can assume $n_0 = 1$. Now we claim that $A = \mathbb{Z}[1/p]$. To do we will show that $1/p^k \in A$ for every $k \geq 0$. Now, notice that since $\gcd(p, n_k) = 1$ and thus $\gcd(p^k, n_k) = 1$, there exist $c_0, c_1 \in \mathbb{Z}$ such that $c_0 p^k + c_1 n_k = 1$. This means that $c_0 + c_1 n_k/p^k = 1/p^k$. Now $n_k/p^k \in A$ by assumption and $c_0 \in \mathbb{Z} \subseteq A$, so this means $1/p^k \in A$. Thus $A = \mathbb{Z}[1/p]$.

To conclude, this means all proper subgroups of $\mathbb{Z}[1/p]/\mathbb{Z}$ are of the form

$$\frac{1/p^k\mathbb{Z}}{\mathbb{Z}}$$

As already said, this means $\mathbb{Z}[1/p]/\mathbb{Z}$ is not Noetherian. But it is Artinian: we know that in general $(1/p^k\mathbb{Z})/\mathbb{Z} \subset (1/p^{k+1}\mathbb{Z})/\mathbb{Z}$. So if we take some subgroup $(1/p^k\mathbb{Z})/\mathbb{Z}$, the only subgroups which are subgroups of it are $(1/p^i\mathbb{Z})/\mathbb{Z}$ for $i \leq k$. So any descending chain must be finite.

(2) $\mathbb{Q}/\mathbb{Z}$ is not Artinian. Let $\{p_i\}_{i=1}^{\infty}$ enumerate the prime numbers, and define the groups

$$A_k = \left\{ \frac{a}{b} \;\middle|\; \gcd(a, b) = \gcd(b, p_i) = 1 \text{ for } i < k \right\}$$

These are obviously subgroups of $\mathbb{Q}$, $a/b + c/d = (ad + bc)/ad$ and $\gcd(ad, p_i) = 1$. And they form a strictly decreasing sequence of subgroups of $\mathbb{Q}$: $1/p_k \in A_k - A_{k-1}$. Furthermore, $\mathbb{Z} \subseteq A_k$ clearly. Thus their quotients $\mathbb{Q}/\mathbb{Z} = A_0/\mathbb{Z} \supset A_1/\mathbb{Z} \supset A_2/\mathbb{Z} \supset \cdots$ forms an infinite strictly decreasing sequence of submodules.

(3) A simple R-module is isomorphic to R/I where I is a maximal ideal of R (this is a one-to-one correspondence). In the case of $\mathbb{Z}$, maximal ideals of $\mathbb{Z}$ are of the form $p\mathbb{Z}$ for p prime, and so simple $\mathbb{Z}$-modules are of the form $\mathbb{Z}/p\mathbb{Z}$.

Since $\mathbb{Q}$ is torsion-free, all of its non-trivial subgroups are torsion-free and as such cannot be isomorphic to $\mathbb{Z}/p\mathbb{Z}$, and so cannot be simple.

Now, suppose $\mathbb{Q}/A \cong \mathbb{Z}/p\mathbb{Z}$ for some subgroup $A \subseteq \mathbb{Q}$ This means that A is the kernel of some surjection $f\colon \mathbb{Q} \to \mathbb{Z}/p\mathbb{Z}$. Now notice that $f(n) = nf(1)$, and $nf(1) = f(n) = f(m \cdot n/m) = mf(n/m)$. In particular $f(1) = pf(1/p)$, and since $p \equiv 0 \pmod p$, we have that $f(1) = 0$. And so for m not divisible by p, $f(n/m) = 0$. So f is determined by $f(1/p)$, and since f is surjective, wlog $f(1/p) = 1$. But then f cannot be a homomorphism: let $q \neq p$ be another prime, then

$$f\left(\frac{1}{pq} + \frac{1}{p}\right) = f\left(\frac{1+q}{pq}\right)$$

Since $\gcd(pq, 1+q) = 1$ but $\gcd(p, pq) = p \neq 1$, we have that this is equal to 0. On the other hand

$$f\left(\frac{1}{pq}\right) + f\left(\frac{1}{p}\right) = 0 + 1 = 1$$

So f is not a homomorphism, a contradiction.

3 Problem

(1) Let M be an R-module of finite length. Show that M is both Artinian and Noetherian.

(2) Let M be Artinian and Noetherian, show that M has finite length.

(1) If M has finite length, it has a composition series $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$, i.e. M_{k+1}/M_k are simple. We induct on n to show that M is both Artinian and Noetherian. If $n = 1$, then

$M/0 \cong M$ is simple, and as such it is trivially Artinian and Noetherian. Suppose $0 = M_0 \subset \cdots \subset M_n \subset M_{n+1} = M$ is a composition series. Then by induction M_n is Artinian and Noetherian, and since M/M_n is simple, it too is Artinian and Noetherian. So M has a submodule which is Artinian and Noetherian and for which its quotient is Artinian and Noetherian, therefore M is Artinian and Noetherian.

(2) We will show that M has a simple submodule. Suppose not; then we will define an infinite strictly descending sequence of nontrivial submodules. Let $M_0 = M$, and given $0 \neq M_k \subset M$ by assumption M has no simple submodules and so M_k must not be simple and as such has a nontrivial proper submodule $0 \neq M_{k+1} \subset M_k$. But this contradicts M being Artinian.

Now suppose M does not have a composition series. Let $M_1 \subset M$ be a simple submodule, since M does not have a composition series it is not simple so $M_1 \neq M$. Since $0 = M_0 \subset M_1 \subset M$ cannot be a composition series, M/M_1 cannot be simple. Now, since M is Artinian M/M_1 is also Artinian and thus has a simple submodule. Since submodules of M/M_1 are of the form M_2/M_1 for $M_1 \subseteq M_2 \subseteq M$, we have a submodule M_2 such that M_2/M_1 is simple. Since M/M_1 is not simple, $M_2 \neq M$ and so we have $0 = M_0 \subset M_1 \subset M_2 \subset M$. Continuing this inductively, we get an infinite strictly increasing sequence of submodules, contradicting M being Noetherian.

4 Problem

Prove the Jordan-Hoelder theorem for modules of finite length: any two composition series of a module with finite length are equivalent.

Let $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$ be a composition series of M. We will show by induction on n that all composition series of M are equivalent to this one. For $n = 1$, we have $0 \subset M$ is a composition series, so M is simple. As such this is the only composition series, and our claim follows.

For our induction step, suppose we have another composition series $0 = N_0 \subset N_1 \subset \cdots \subset N_k = M$; let $N = N_1$. Now let i be the smallest index for which $N \subseteq M_i$ (since $N \neq 0$, $i > 0$). Then composing the inclusion with the canonical projection $N \to M_i \to M_i/M_{i-1}$ gives a nonzero morphism (since if it were zero, then $N \subseteq M_{i-1}$, contradicting i being minimal) between two simple modules. By Schur, this is an isomorphism.

Now let $X = M/N$, and let $X_j = (M_j + N)/N$. So $0 = X_0 \subseteq X_1 \subseteq \cdots \subseteq X_n = X$. Now notice that

$$X_j = X_{j+1} \iff M_j + N = M_{j+1} + N$$

For $j \geq i$, this is iff $M_j = M_{j+1}$ (since $N \subseteq M_i \subseteq M_j$), so $X_j \neq X_{j+1}$. For $j + 1 < i$, we note that this is equivalent to $M_{j+1} \subseteq M_j + N$. Now since N is not a subset of M_{j+1}, we have that $N \cap M_{j+1} \subset N$, and since N is simple, $N \cap M_{j+1} = 0$. So let $0 \neq m \in M_{j+1}$, so there exists $m' \in M_j \subseteq M_{j+1}$ such that $m \in m' + N$, i.e. $m - m' \in N$. But then $m - m' \in N \cap M_{j+1}$, so $m = m'$. So $M_{j+1} \subseteq M_j$, a contradiction.

Notice that $M_i = M_{i-1} + N$. Indeed, $M_{i-1}, N \subseteq M_i$ so $M_{i-1} + N \subseteq M_i$. Since M_i/M_{i-1} is simple, and $(M_{i-1} + N)/M_{i-1}$ is a submodule, it is either equal to 0 or $M_/M_{i-1}$. That is, $M_{i-1} + N = M_{i-1}$ or $M_{i-1} + N = M_i$. The former cannot be true, since it implies $N \subseteq M_{i-1}$. Thus $M_{i-1} + N = M_i$ and thus $X_{i-1} = X_i$.

So we have a composition series

$$0 = X_0 \subset X_1 \subset \cdots \subset X_{i-1} \subset X_{i+1} \subset \cdots \subset X_n = X = M/N$$

of M/N, of length $n - 1$. Let $Y_j = X_j$ for $j < i$ and $Y_j = X_{j+1}$ for $j \geq i$. Now, notice that

$$0 = N_1/N \subset N_2/N \subset \cdots \subset N_k/N = M/N$$

is another composition series of M/N of length $k - 1$. By induction these composition series are equivalent, so $n = k$ and there exists a permutation σ such that $Y_{k+1}/Y_k \cong (N_{\sigma(k)+1}/N)/(N_{\sigma(k)}/N) \cong N_{\sigma(k)+1}/N_{\sigma(k)}$.

For $k = i-1$ we have $Y_{k+1}/Y_k = Y_i/Y_{i-1} = X_{i+1}/X_{i-1} \cong M_{i+1}/M_i$. For $k < i-1$ we have $Y_{k+1}/Y_k = X_{k+1}/X_k \cong M_{k+1}/M_k$ (since it is equal to $((M_{k+1}+N)/N)/((M_k+N)/N) \cong M_{k+1}/M_k$). For $k \geq i$ we have $Y_{k+1}/Y_k = X_{k+2}/X_{k+1} \cong M_{k+2}/M_{k+1}$. We are thus only missing M_i/M_{i-1}.

The only quotient not counted yet by the permutation is $N_1/0 = N$ itself. So we must have that $M_i/M_{i-1} \cong N$. And indeed, we already showed this. So this concludes the proof.

5 Problem

(1) Observe that $Q_8 \subseteq \mathbb{H}^\times$ (where Q_8 is the quaternion group). Show that $\mathbb{H}$ is a representation of Q_8 by $x.h = hx^{-1}$.

(2) Let V be the 2-dimensional complex representation from the previous problem set. View it as a 4-dimensional real representation. Show that it is isomorphic to the representation of Q_8 on $\mathbb{H}$.

(3) Show that the action of $\mathbb{H}$ on itself by left multiplication is a Q_8-equivariant map. Deduce that there is a homomorphism of algebras $\mathbb{H} \to \hom_{Q_8}(V, V)$.

(4) Show that a nonzero homomorphism of algebras, where the domain is a division algebra, is an injection.

(5) Show that the homomorphism given is an isomorphism.

(1) We already showed that $Q_8 \subseteq \mathbb{H}^\times$ previously. We now claim that $x.h$ is a representation. Indeed x maps to a linear endomorphism: $x.(h_1 + h_2) = (h_1 + h_2)x^{-1} = h_1x^{-1} + h_2x^{-1} = x.h_1 + x.h_2$ and $x.(ch) = chx^{-1} = c(x.h)$. And $(xy).h = h(xy)^{-1} = hy^{-1}x^{-1} = x.(y.h)$ as required.

(2) We recall that the previous representation was given by

$$\rho(i) = \begin{pmatrix} i & \\ & -i \end{pmatrix}, \qquad \rho(j) = \begin{pmatrix} & 1 \\ -1 & \end{pmatrix}$$

To view this as a 4-dimensional real representation, let $\bar{x} = (a, b, c, d) \in \mathbb{R}^4$, then

$$\rho(i)\bar{x} \to \begin{pmatrix} i & \\ & -i \end{pmatrix} \begin{pmatrix} a+ib \\ c+id \end{pmatrix} = \begin{pmatrix} -b+ia \\ d-ic \end{pmatrix} \to (-b, a, d, -c)$$

and

$$\rho(j)\bar{x} \to \begin{pmatrix} & 1 \\ -1 & \end{pmatrix} \begin{pmatrix} a+ib \\ c+id \end{pmatrix} = \begin{pmatrix} c+id \\ -a-ib \end{pmatrix} \to (c, d, -a, -b)$$

We now claim that this representation is isomorphic to Q_8 on $\mathbb{H}$. So we need a vector-space isomorphism $f\colon \mathbb{R}^4 \to \mathbb{H}$ such that $f(\rho(i)\bar{x}) = i.f(\bar{x}) = -f(\bar{x})i$ and $f(\rho(j)\bar{x}) = j.f(\bar{x}) = -f(\bar{x})j$. (This is sufficient since i, j generate Q_8.) Since $\rho(g)$ and f are linear, it is sufficient to show this for $\bar{x}$ basis vectors. Now, notice that

$$\rho(i)e_1 = e_2, \quad \rho(i)e_2 = -e_1, \quad \rho(i)e_3 = -e_4, \quad \rho(i)e_4 = e_3$$

and

$$\rho(j)e_1 = -e_3, \quad \rho(j)e_2 = -e_4, \quad \rho(j)e_3 = e_1, \quad \rho(j)e_4 = e_2$$

So we need

$$f(e_2) = -f(e_1)i, \quad f(e_1) = f(e_2)i, \quad f(e_4) = f(e_3)i, \quad f(e_3) = -f(e_4)i$$

and

$$f(e_3) = f(e_1)j, \quad f(e_4) = f(e_2)j, \quad f(e_1) = -f(e_3)j, \quad f(e_2) = -f(e_4)j$$

We can reduce this to just four conditions, equivalent to these eight:

$$f(e_1) = f(e_2)i, \quad f(e_3) = -f(e_4)i, \quad f(e_1) = -f(e_3)j, \quad f(e_2) = -f(e_4)j$$

Let $f(e_1) = 1$, then we see that $f(e_2) = -i$, $f(e_3) = j$, $f(e_4) = -k$ satisfy these equations. Since $1, i, j, k$ form a basis for $\mathbb{H}$ this is an isomorphism. That is,

$$f(a, b, c, d) = a - ib + cj - kd$$

gives an isomorphism.

(3) Let $h \in \mathbb{H}$ and define $f_h\colon \mathbb{H} \to \mathbb{H}$ by $f_h(x) = hx$. We claim that this is equivariant. Indeed: $f_h(x.y) = f_h(yx^{-1}) = hyx^{-1}$ and $x.f_h(y) = f_h(y)x^{-1} = hyx^{-1}$. So $f_h \in \mathrm{end}_{Q_8}(\mathbb{H})$.

Now, we claim that $\mathbb{H} \to \mathrm{end}_{Q_8}(\mathbb{H}), h \mapsto f_h$ is a homomorphism of algebras. So we need to show

(i) Additivity: $f_{h+g} = f_h + f_g$. Indeed, $f_{h+g}(x) = (h+g)x = hx + gx = f_h x + f_g x$.

(ii) Multiplicity: $f_{hg} = f_g \circ f_h$. Indeed, $f_{hg}(x) = hgx = f_h(f_g(x))$.

(iii) Scalar multiplicity: for $c \in \mathbb{R}$, $f_{ch} = cf_h$. Indeed, $f_{ch}(x) = chx = c_h(x)$.

Since $\mathbb{H} \cong V$ as Q_8 representations, this defines an algebra morphism $\mathbb{H} \to \mathrm{end}_{Q_8}(V)$.

(4) Suppose $f\colon D \to A$ is an algebra of $\mathbb{F}$-algebras, and D is a division algebra. In particular, $f\colon D \to A$ is a ring morphism, so $\ker f \subseteq D$ is an ideal. Now suppose $d \in \ker f$ is nonzero, then $d^{-1} \in D$ since D is a division ring. Then $d^{-1}d \in \ker f$ as an ideal, so $1 \in \ker f$. Since $\ker f$ is an ideal, this implies $\ker f = D$, so f is the zero morphism, a contradiction.

(5) Our morphism $\mathbb{H} \to \mathrm{end}_{Q_8}(\mathbb{H})$ is nonzero (since $1 \mapsto \mathrm{id}$), and as such it is injective. Now let $f \in \mathrm{end}_{Q_8}(\mathbb{H})$. We claim that $f = f_{f(1)}$. Indeed, notice that for $q \in Q_8$ we have $f(q) = f(q^{-1}.1) = q^{-1}.f(1) = f(1)q$. In particular for $a, b, c, d \in \mathbb{R}$:

$$f(a + ib + jc + kd) = f(1)a + f(i)b = f(j)c + f(k)d = f(1)\big(a + ib + jc + kd\big)$$

That is, $f(x) = f(1)x$, so $f = f_{f(1)}$ as claimed.

Thus our morphism $\mathbb{H} \to \mathrm{end}_{Q_8}(\mathbb{H})$ is a surjection, and thus an isomorphism. Since $\mathbb{H} \cong V$, this extends to an isomorphism $\mathbb{H} \cong \mathrm{end}_{Q_8}(V)$.