Exercise Sheet 9, Advanced Algebra, Summer Semester 2017. Some hints for solutions

(Ehud Meir and Christoph Schweigert)

---

1. The set X is non-empty because $\phi \in X$. If $\{Y_i\}_{i\in I}$ is a chain in X, then we show that $Y := \cup_{i\in I} Y_i$ is an element of X: we use the fact that a linear relation between elements of Y will involve only finitely many elements. By Zorn Lemma we now have a maximal element B in X. If B is not a basis of M, then there exists $m \notin R\cdot B$. The set $B\cup\{m\}$ is then not in X and therefore linearly dependent. We get a linear relation of the form $am + r_1 b1 + \ldots r_n b_n = 0$. If $a = 0$ we get a linear dependence in B, which is impossible. Otherwise by inverting a we get m as a linear combination of elements in B, which is also a contradiction. Therefore B is a basis of M.

2. We are considering here the categories of left R and left A-modules. $F(M)$ is an A-module by the action

$$(a_{ij})_{i,j}\cdot \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} a_{11}m_1 + \cdots a_{1n}m_n \\ a_{21}m_1 + \cdots a_{2n}m_n \\ \vdots \\ a_{n1}m_1 + \cdots a_{nn}m_n \end{pmatrix}.$$

$G(N)$ is an R-module by the action $(r\cdot f)(v) = f(v\cdot r)$ for $v \in R^n$. We use here the right action of R on R^n given by

$$\begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix}\cdot r = \begin{pmatrix} r_1 r \\ \vdots r_n r \end{pmatrix}.$$

The map $r\cdot f$ is again an A-module map because R^n is an $A-R$-bimodule: it holds that $(av)r = a(vr)$ for $a \in A$ and $r \in R$. We had to use the action of R from the right in order to assure that $(r_1 r_2)f = r_1(r_2 f)$. (otherwise we need to invert the order of the multiplication).

The difficult part is to show part (c): that F and G are quasi-inverse to one another. We will use here the standard matrix and vector notations: e_i is the i-th vector in the standard basis of R^n, and e_{ij} is the $n\times n$ matrix which is zero everywhere, except in the (i,j)-entry, where it has the value 1. We begin with showing that $GF \cong Id_{\mathcal{C}}$. We have $GF(M) = Hom_A(R^n, M^n)$. It holds that $f(e_1) = f(e_{11}e_1) = e_{11}f(e_1)$. Thus, if $f(e_1) = \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix}$ we get that $m_2 = m_3 = \ldots m_n = 0$. We define $\Phi : GF(M) \to M$ by $\Phi(f) = m_1$. A direct verification shows that this is indeed a well defined map of R-modules. Since $f(e_1)$ determines f it is clear that Φ is injective (we use here the fact that e_1 is a generator for R^n as an A-module). On the other hand, if $m \in M$, we define

$$f_m(\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}) = \begin{pmatrix} a_1 m \\ \vdots \\ a_n m \end{pmatrix}.$$

A direct verification shows that this map is indeed an A-module homomorphism, and that $\Phi(f_m) = m$. This shows us that Φ is an isomorphism indeed. Notice that the choice of the vector e_1 was arbitrary here. We could have chosen any other non-zero vector in R^n as well. This would make, however, the description of f_m more complicated.

We next show that $GF \cong Id_{\mathfrak{D}}$. So let N be an A-module. We have $GF(N) = (Hom_A(R^n, N))^{\oplus n}$. We define $\Psi : GF(N) \to N$ by

$$\Psi(\begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix}) = f_1(e_1) + f_2(e_2) + \ldots f_n(e_n).$$

A very careful verification shows us that this is indeed a homomorphism of A-modules. The homomorphism Ψ is injective. This follows from the fact that if $\sum_i f_i(e_i) = 1$ then we can multiply this equation with e_{ii} to get $f_i(e_i) = 0$ for every i. Since e_i is a generator of R^n we get that $f_i = 0$ for every i. The homomorphism Ψ is also surjective. Indeed, if v is an element of N, define $f_i : R^n \to N$ by

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \mapsto \sum_j a_j e_{ji} v.$$

As before, a very careful verification shows that f_i are indeed A-module homomorphisms. We then have that $\Psi(\begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix} = \sum_i f_i(e_i) = \sum_i e_{ii} v = v$. This shows us that Ψ is an isomorphism and we are done.

3. If M_i is an A_i module for every i, then $\prod_i M_i = \oplus_i M_i$ is an $R = \prod_i A_i$-module with the action

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \cdot \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} a_1 m_1 \\ \vdots \\ a_n m_n \end{pmatrix}.$$

Let now M be an R-module. Write $M_i = e_i M$ where $e_i \in R$ is the element which is 1 in the i-th entry and zero in all the rest. We use again the fact that $e_i e_j = \delta_{ij} e_i$ and that $\sum_i e_i = 1$ in order to prove that M_i is an A_i-module, and that M is the direct sum of M_i. For $m_i \in M_i$ and $a_j \in A_j$ with $i \neq j$ we have that $a_j \cdot m_i = a_j e_j e_i m_i = 0$ (we consider here a_j as an element of R by the obvious inclusion). This implies that the only non-trivial action we get is of A_i on M_i, and we thus get

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \sum_i a_i m_i = \begin{pmatrix} a_1 m_1 \\ \vdots \\ a_n m_n \end{pmatrix}$$

as desired.

The idea behind this exercise, and the previous ones, was to explain how modules over semisimple rings look like. Indeed, by Wedderburn Theorem we know that a semisimple ring R can be written as

$$R \cong \prod_i M_{n_i}(D_i)$$

where the D_i are division rings. Exercise 3 enables us to reduce the study to modules over $M_n(D)$ where D is a division ring. Exercise 2 reduces to the study of modules over D. Exercise 1 says that all modules over D are free.

4. (a) The first part follows from Exercise 5 in Exercise Sheet 1. We see that the vector $(1,1,1)$ spans a one dimensional sub-representation U upon which $G = S_3$ acts trivially. Using the standard Hermitian product, which in this case is G-invariant, we see that the subspace

$$W := \{ \begin{pmatrix} a \\ b \\ c \end{pmatrix} | a + b + c = 0 \}$$

is also a subrepresentation and a direct sum complement of U. It remains to prove that W is an irreducible representation. The only possible proper subrepresentations of W will be of dimension 1. Assume that the nonzero vector $w = \begin{pmatrix} a \\ b \\ c \end{pmatrix}$ spans such a subrepresentation, which we shall denote by W'. Then the elements $w_2 = (Id - (1,2))w = \begin{pmatrix} a-b \\ b-a \\ 0 \end{pmatrix}$ and $w_3 = (Id - (2,3))w = \begin{pmatrix} 0 \\ b-c \\ c-b \end{pmatrix}$ are also in W'.

If $a \neq b$ then by the fact that the space is one dimensional we get that $c = 0$ (by considering a linear relation on w and w_2). By considering now a linear relation between w_2 and w_3 we get that $b = 0$. But this already implies that $a = 0$ as well, which is a contradiction.

We thus get that the only option for (a,b,c) is one in which $a = b$. Similarly, we can deduce that $b = c$. But since $a+b+c = 0$, we get that w is the zero vector, which is again a contradiction. This shows that W is indeed irreducible.

(b) As for any other symmetric group, we also have the one-dimensional sign representation. The representation is given explicitly in the following way:

$$\sigma \cdot x = (-1)^{sign(\sigma)} x$$

for $\sigma \in G$ and $x \in \mathbb{C}$. It can easily be seen that this representation is not isomorphic with the trivial representation.

(c) We have found 3 irreducible representations, of dimensions 1,1 and 2. The sum of their squares is $1^2 + 1^2 + 2^2 = 6$, which is exactly the order of $G = S_3$. This shows that these are all the irreducible representations of G.

5. (a) The relation $xy = -yx$ enables us to write every product of elements x, y as $\pm x^i y^j$ for some i, j. The first two relations enable us to reduce to the case where $i, j \in \{0,1\}$. this already shows that $\{1, x, y, xy\}$ spans D. We still need to show that these elements are linearly independent. One possible way to show this is by considering the ring homomorphism $D \to M_2(K(\sqrt{a}))$ given by $x \mapsto \begin{pmatrix} \sqrt{a} & 0 \\ 0 & -\sqrt{a} \end{pmatrix}$ and $y \mapsto \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}$ (we can show that the relations between x and y hold in $M_2(K(\sqrt{a}))$. Another option is to write explicitly the product between the four basis elements, and show that we indeed get an associative algebra.

(b) we prove here that if $d^2 \in K$ and $d \notin K$ then $d_1 = 0$ (this was the way it was suppose to be formulated in the exercise sheet, sorry for this mistake!). We calculate:

$$d^2 = d_1^2 + d_2^2 a + d_3^2 b - d_4^2 ab + 2d_1 d_2 x + 2d_1 d_3 y + 2d_1 d_4 xy.$$

All the other elements in the sum vanish due to the relation $xy = -yx$ (which also implies that $x(xy) - (xy)x$ and so on). this implies that $d^2 \in K$ if and only if $d_1d_2 = d_1d_3 = d_1d_4 = 0$. So either $d_1 = 0$ or $d_2 = d_3 = d_4 = 0$. In the second case $d \in K$.

(c) We have a Galois extension $K(\sqrt{a})/K$. We denote by σ the Galois automorphism, which sends $\sqrt{a}$ to $-\sqrt{a}$. We then have that $t^2 - s^2a = (t+s\sqrt{a})\sigma(t+s\sqrt{a})$. Therefore, since σ is multiplicative, we get

$$(t_1^2 - s_1^2a)(t_2^2 - s_2^2a) = (t_1+s_1\sqrt{a})\sigma(t_1+s_1\sqrt{a})(t_2+s_2\sqrt{a})\sigma(t_2+s_2\sqrt{a})$$

$$= (t_1+s_1\sqrt{a})(t_2+s_2\sqrt{a})\sigma((t_1+s_1\sqrt{a})(t_2+s_2\sqrt{a})) = r\sigma(r)$$

where $r = (t_1+s_1\sqrt{a})(t_2+s_2\sqrt{a})$ and therefore has the aforementioned form. This can also be proved directly, without using the Galois action. The inverse of $r^2 - s^2a$ is $(\frac{r}{r^2-s^2a})^2 - (\frac{s}{r^2-s^2a})^2a$.

(d) We would like to show that every element $d = d_1 + d_2x + d_3y + d_4xy$ of $D - K$ is invertible. For this, it will be enough to prove that the minimal polynomial of $d_2x + d_3y + d_4xy$ is irreducible (this will imply that also the minimal polynomial of d is irreducible, and therefore that d must be invertible). Since $d - d_1$ is not in K, but $(d-d_1)^2$ is in K, we see that the minimal polynomial is $t^2 - (d_2^2a + d_3^2b - d_4^2ab)$. This polynomial is irreducible if and only if the equation $d_2^2a + d_3^2b - d_4^2ab = l^2$ does not have a solution in K. We rewrite this equation as $l^2 - d_2^2a = b(d_3^2 - d_4^2a)$. If $d_3^2 - d_4^2a = 0$ we get that $l = d_2 = d_3 = d_4 = 0$ (since $\sqrt{a} \notin K$) and this contradicts our assumption. We rewrite this equation as as $(l^2 - d_2^2a)(d_3^2 - d_4^2a)^{-1} = b$. By the previous part of the exercise, the left hand side can be re-written as $c_1^2 - c_2^2a$ for some $c_1, c_2 \in K$, and we get the equation $c_1^2 - c_2^2a = b$. We thus see that this equation has no non-trivial solution if and only if D is a division algebra.