MATH STUDIES ALGEBRA SPRING 2018: HOMEWORK 1

JC

This homework is due by class time on Monday 29 January. It must be typeset (preferably in LaTeX) and submitted as a PDF file on the Canvas site, with a filename of the form

`andrewID_alg_homeworknumber.pdf`

For each minute that it is late, the grade will be reduced by 10 percent.

(1) Let G be a finite group, let k be a field and let R be the set of all functions from G to k. In a suggestive notation we will write a typical element $f \in R$ in the form $\sum_{i=1}^{n} a_i g_i$, where $g_1, \dots g_n$ enumerates G and $f(g_i) = a_i$.

We define operations $+$ and $\times$ on R as follows:

- $\sum_{i=1}^{n} a_i g_i + \sum_{i=1}^{n} b_i g_i = \sum_{i=1}^{n} c_i g_i$, where $c_i = a_i + b_i$.
- $\sum_{i=1}^{n} a_i g_i \times \sum_{j=1}^{n} b_j g_j = \sum_{k=1}^{n} c_k g_k$, where $c_k = \sum\{a_i b_j : g_i g_j = g_k\}$.

(a) Prove that R forms a ring with 1, given these definitions of $+$ and $\times$.
$(R, +)$ is clearly isomorphic to the product of $|G|$ copies of the abelian group $(k, +)$, so it is an abelian group.
For associativity, let $r_1 = \sum_{i=1}^{n} a_i g_i$, $r_2 = \sum_{j=1}^{n} b_j g_j$, $r_3 = \sum_{k=1}^{n} c_k g_k$. A short calculation shows that $(r_1 r_2) r_3$ and $r_1 (r_2 r_3)$ have the common value $\sum_{l=1}^{n} d_l g_l$ where $d_l = \sum\{a_i b_j c_k : g_i g_j g_k = g_l\}$.
For distributivity, let r_i be as above. Another short calculation shows that $r_1(r_2 + r_3)$ and $r_1 r_2 + r_1 r_3$ have the common value $\sum_{l=1}^{n} d_l g_l$ where $d_l = \sum\{a_i(b_j + c_j) : g_i g_j = g_l\}$. The other distributive law is similar.
Finally we need a 1. The obvious candidate is the element $1_k e_G$, and yet another short calculation shows that it works.

(b) Prove that $(R, \times)$ contains an isomorphic copy of G.
It is easy to see that the map $g \mapsto 1_k g$ sets up an IM between G and $\{1_k g : g \in G\}$.

(c) Prove that R contains an isomorphic copy of k.
It is easy to see that the map $a \mapsto a e_G$ sets up an IM between G and $\{a e_G : a \in k\}$.

(d) Identify (with proof) the class of groups G for which R is commutative.
If G is commutative then a short calculation shows $rs = sr$ for all $r, s \in R$. If R is commutative then the embedded copy of G from a previous part must be commutative.

(2) Let k be a field, G a finite group and V a vector space over k (IE a k-module). Suppose that G acts on V in such a way that the map $v \mapsto g \cdot v$ is linear for each $g \in G$. Let R be the ring constructed from k and G in the preceding question.

(a) Prove that if we define $(\sum_{i=1}^{n} a_i g_i)v = \sum_{i=1}^{n} a_i (g_i \cdot v)$, then V becomes a left R-module.

This is reasonably painful. There are so many 1's and 0's floating around that I broke with my usual practice and flagged them with subscripts.

(i) Since $0_R = \sum_i 0_k g_i$, $0_R v = \sum_i 0_k (g_i \cdot v) = 0_V$ because $0_k w = 0_V$ for all $w \in V$.

(ii) Since $1_R = 1_k e_G$, $1_R v = 1_k (e_G \cdot v) = 1_k v = v$. Here $e_G \cdot v = v$ because we have a group action, and $1v = v$ because V is a k-module.

(iii) Let $r_1 = \sum_{i=1}^n a_i g_i$, $r_2 = \sum_{j=1}^n b_j g_j$, $v \in V$. By definition $(r_1 r_2)v = \sum_{k=1}^n c_k (g_k \cdot v)$, where $c_k = \sum_{g_i g_j = g_k} a_i b_j$.
Now $r_1(r_2 v) = \sum_{i=1}^n a_i (g_i \cdot (\sum_{j=1}^n b_j (g_j \cdot v))$. Since $w \mapsto g_i \cdot w$ is linear, and we are dealing with a group action, $g_i \cdot (\sum_{j=1}^n b_j (g_j \cdot v)) = \sum_{j=1}^n b_j g_i \cdot (g_j \cdot v)) = \sum_{j=1}^n b_j (g_i g_j) \cdot v$. So $r_1(r_2 v) = \sum_{i,j} a_i b_j (g_i g_j) \cdot v$, and we can collect terms to see that $(r_1 r_2)v = r_1(r_2 v)$.

(iv) Let $r_1 = \sum_{i=1}^n a_i g_i$, $r_2 = \sum_{j=1}^n b_j g_j$, $v \in V$. By definition and the assumption that V is a k-module, $(r_1 + r_2)v = \sum_{i=1}^n (a_i + b_i)(g_i \cdot v) = \sum_{i=1}^n a_i (g_i \cdot v) + \sum_{i=1}^n b_i (g_i \cdot v) = r_1 v + r_2 v$.

(v) Let $r = \sum_{i=1}^n a_i g_i$ and $v, w \in W$. Since g_i acts as a linear map, $g_i \cdot (v + w) = g_i \cdot v + g_i \cdot w$, and so easily $r \cdot (v + w) = r \cdot v + r \cdot w$.

(b) Prove that all left R-modules arise in this way.
Let W be a left R-module. Since R contains an isomorphic copy of k given by $a \mapsto a e_G$, it is immediate that we can make W into a k-module by defining $aw = (a e_G)w$. Since R contains an isomorphic copy of G given by $g \mapsto 1_k g$, we can also attempt to define an action of G on W by defining $g \cdot w = (1_k g)w$: this gives an action because $(g_1 g_2) \cdot w = (1_k g_1)(1_k g_2)w = 1_k g_1 g_2 w$, using the module axioms. We must verify that $w \mapsto g \cdot w$ is linear. The module axioms give $g \cdot (v + w) = (1g)(v + w) = (1g)v + (1g)w = g \cdot v + g \cdot w$, and $g \cdot (\lambda v) = (1g)(\lambda 1)v = (\lambda 1)(1g)v = \lambda (g \cdot v)$ using the definition and the fact that $(1g)(\lambda 1) = (\lambda 1)(1g) = \lambda g$ in R.
Now that we made W into a k-module on which G acts by linear maps, we have to check that the original R-module structure agrees with one induced by the k-module structure and the G-action: if $r = \sum_{i=1}^n a_i g_i$ then we rewrite $r \sum_{i=1}^n (a_i e_G)(1 g_i)$, use the module axioms and definitions to get $rv = \sum_i a_i (g_i \cdot v)$, and we are done.

(3) Consider the ring R of $N \times N$ real matrices. We will generalise some familiar ideas from calculus to this setting:

- If $(M_n)_{nin\mathbb{N}}$ is a sequence of elements of R, then (M_n) is *convergent* if and only if for each i and j the sequence formed by the (i,j)-entries in M_n is convergent. In this case the *limit* is the matrix M whose (i,j)-entry is the limit of the sequence formed by the (i,j)-entries in M_n.
- Similarly, an infinite sum $\sum_{n=0}^\infty M_n$ of elements of R is convergent iff the sequence of partial sums $\sum_{n=0}^j M_n$ is convergent, and in this case $\sum_{n=0}^\infty M_n$ is defined as the limit of the sequence of partial sums.

(a) Prove that for any matrix $A \in R$, the power series $\sum_{n=0}^\infty \frac{A^n}{n!}$ converges.

Hint: Let K be the maximum of the absolute values of the entries in A. Find an upper bound for the absolute values of the entries in A^n in terms of K, N and n. Now use the Comparison Test.
We claim that for every n (including zero, where by convention $A^0 = I$) the absolute values of the entries in A^n are bounded by $(KN)^n$. This is clear for $n = 0$, so we proceed ny induction. If $A^n = B$ and $A^{n+1} = C = AB$, then

$$|c_{ik}| = |\sum_j a_{ij}b_{jk}| \leq |\sum_j |a_{ij}| \times |b_{jk}| \leq KN(KN)^n = (KN)^{n+1}.$$

By comparison with the power series for $\exp(KN)$, it is clear that the (i,j)-entries of the terms $\frac{A^n}{n!}$ form an (absolutely) convergent series.

(b) Compute the sum of the series $\sum_{n=0}^{\infty} \frac{A^n}{n!}$ when $N = 2$ and $A = \begin{pmatrix} \lambda & 0 \\ 1 & \lambda \end{pmatrix}$
By an easy induction, $A^n = \begin{pmatrix} \lambda^n & 0 \\ n\lambda^{n-1} & \lambda^n \end{pmatrix}$
Of course $\sum_{n=0}^{\infty} \frac{\lambda^n}{n!} = \exp(\lambda)$, while $\sum_{n=0}^{\infty} n\frac{\lambda^{n-1}}{n!} = \sum_{n=1}^{\infty} \frac{\lambda^{n-1}}{(n-1)!} = \exp(\lambda)$. So $\exp(A) = \begin{pmatrix} \exp(\lambda) & 0 \\ \exp(\lambda) & \exp(\lambda) \end{pmatrix}$

(c) (Challenging, not for credit) We define $\exp(A) = \sum_{n=0}^{\infty} \frac{A^n}{n!}$. Prove that if $AB = BA$ then $\exp(A+B) = \exp(A)\exp(B)$.
Since $AB = BA$, it is easy to verify that we have a "matrix binomial theorem" $(A+B)^n = \sum_{i=0}^{n} \binom{n}{i} A^i B^{n-i}$, so easily $\frac{(A+B)^n}{n!} = \sum_{i+j=n} \frac{A^i B^j}{i!j!}$. Arguing as we did for the matrix power series $\exp(A)$ above, it is not hard to see that the "expanded" series $\sum_n \sum_{i+j=n} \frac{A^i B^j}{i!j!}$ is absolutely convergent (in the sense that the (k,l) entries form an absolutely convergent series for each k and l). By a standard fact about series, it may be rearranged without changing its sum.
It is easy to see that matrix multiplication for $N \times N$ real matrices (considered as a function from $\mathbb{R}^{2N^2}$ to $\mathbb{R}^{N^2}$ is continuous, and so $\exp(A)\exp(B) = \lim_{n\to\infty} \sum_{i=0}^{n} \sum_{j=0}^{n} \frac{A^i B^j}{i!j!}$. Now rearrange the expanded series $\sum_n \sum_{i+j=n} \frac{A^i B^j}{i!j!}$ so that in the rearranged version the first $(n+1)^2$ terms have sum $\sum_{i=0}^{n} \sum_{j=0}^{n} \frac{A^i B^j}{i!j!}$. This does not chnage the sum and shows that $\exp(A)\exp(B) = \exp(A+B)$.

(4) Review the following basic definitions from category theory: *category*, *object*, *morphism*, *initial object*, *terminal object*.

(5) Let $\mathcal{C}$ be a category, let I be some (potentially infinite) set I and let $(a_i)_{i\in I}$ be an I-indexed family of objects of $\mathcal{C}$. A *cone* over this family consists of an object b and an I-indexed family of morphisms $(f_i : b \to a_i)_{i\in I}$ (I usually imagine (a_i) as a horizontal line of objects and b sitting above them all with arrows going down into each a_i)

We will make a new category $\mathcal{D}$ as follows: The objects of $\mathcal{D}$ are cones over (a_i). If B is a cone consisting of an object b and morphisms $(f_i : b \to a_i)_{i\in I}$, and C consists of an object c and morphisms $(g_i : c \to a_i)_{i\in I}$, then

a morphism from B to C in $\mathcal{D}$ is a morphism h from b to c in $\mathcal{C}$ such that $f_i = g_i \circ h$.

(a) Verify that $\mathcal{D}$ is a category.
Very tedious.

(b) A *product* for the sequence $(a_i)_{i\in I}$ is a terminal object in the category $\mathcal{D}$. Prove that if $\mathcal{C}$ is the category of left R-modules over a ring R then every sequence has a product.
Let $(M_i)_{i\in I}$ be left R-modules, let $\prod_i M_i$ be the Cartesian product with pointwise operations, and let $\pi_j : \prod_i M_i \to M_j$ be given by $\pi_j : f \mapsto f(j)$. It is routine to check that $\prod_i M_i$ is an R-module and that the "projections" π_j are linear. If we have a system of linear maps $\rho_i : P \to M_i$ for all i, and we define $\sigma : P \to \prod_i M_i$ by $\sigma : p \mapsto \langle \rho_i(p) : i \in I\rangle$, then it is easy to check that σ is linear and is the unique linear map such that $\pi_j \circ \sigma = \rho_j$ for all j.

(6) Let G be an abelian group. A *torsion element* of G is an element $g \in G$ such that $ng = 0$ for some integer $n > 0$, and G is *torsion-free* if 0 is the only torsion element.

(a) Let G be any abelian group. Prove that the set H of torsion elements forms a subgroup of G, and that the quotient G/H is torsion-free.
Clearly $0 \in H$. If $a, b \in H$ fix $m, n > 0$ such that $ma = nb = 0$. Then $mn(a - b) = 0$. So $H \leq G$.
Now let $a + H$ be a torsion element of G/H. Then $m(a + H) = 0 + H$ for some $m > 0$, that is $ma \in H$. Then for some $n > 0$ we have $n(ma) = (nm)a = 0$, so $a \in H$ hence $a + H = 0 + H$.

(b) Given an example of an infinite abelian group in which every element is a torsion element.
One of many examples is $\mathbb{Q}/\mathbb{Z}$.

(c) Let G be a torsion-free abelian group. Prove that there is a vector space V over the field $\mathbb{Q}$ such that G is a subgroup of $(V, +)$ and every element of V has the form $\frac{1}{n}g$ for some integer $n > 0$ and $g \in G$ (n and g will not be unique here).
Imitate the construction of the rationals as the field of fractions of the integers.
Define a binary relation $\simeq$ on $G \times \mathbb{N}^+$ by $(g, m) \simeq (h, n)$ iff $gn = mh$. It is routine to check it's reflexive and symmetric, we claim it is also transitive. So let $(g_1, m_1) \simeq (g_2, m_2) \simeq (g_3, m_3)$, that is $m_1g_2 = m_2g_1$ and $m_2g_3 = m_3g_2$. Then $m_2(m_1g_3 - m_3g_1) = m_1m_3g_2 - m_1m_3g_2 = 0$, so $m_1g_3 = m_3g_1$ because G is torsion-free.
Let V be the set of equivalence classes, and in a suggestive notation we write g/n for the equivalence class of (g, n). Attempt to define an operation $+$ by $g/m + h/n = (gn + hm)/(mn)$.
Now verify (tedious but easy) that $+$ is well-defined and makes V into an abelian group. Then define $(m/n)(g/t) = (mg)/(nt)$ and verify (tedious but easy) that this is well-defined and makes V into a VS over $\mathbb{Q}$. Finally note that $g/1 = g'/1$ if and only if $g = g'$, also $g/1 + g'/1 = (g + g')/1$, so the elements of form $g/1$ form a subgroup of $(V, +)$ isomorphic to G. To finish identify $g/1$ with g and observe that $1/ng = 1/n(g/1) = g/n$.