MATH STUDIES ALGEBRA SPRING 2018: HOMEWORK 2

JC

This homework is due by class time on Monday 5 February. 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 R be a ring with 1, and consider a sequence of R-modules $(M_i)_{i\in I}$ for some interval I in $\mathbb{Z}$, together with morphisms $\phi_i : M_i \to M_{i+1}$ defined when $i, i+1 \in I$. Such a sequence is said to be *exact at* i if $i-1, i, i+1 \in I$ and the image of ϕ_{i-1} is equal to the kernel of ϕ_i, and to be *exact* if it is exact at each relevant i.

Note: usually we describe exact sequences informally, by writing things like

$$A \xrightarrow{\alpha} B \xrightarrow{\beta} C$$

Also we typically don't name the arrows when it is clear what they must be. In particular the zero module 0 is both initial and terminal, so we just write $0 \to M$ or $N \to 0$.

Prove that:

(a) The sequence

$$0 \longrightarrow B \xrightarrow{\alpha} C$$

is exact iff α is injective.

The image of $0 \to B$ is always zero. The sequence is exact iff the kernel of $B \to C$ is zero iff $B \to C$ is injective.

(b) The sequence

$$A \xrightarrow{\alpha} B \longrightarrow 0$$

is exact iff α is surjective.

The kernel of $B \to 0$ is always B. The sequence is exact iff the image of $A \to B$ is B iff $A \to B$ is surjective.

(c) The sequence

$$0 \longrightarrow A \xrightarrow{\alpha} B \longrightarrow 0$$

is exact iff α is an isomorphism.

Combine the previous two parts.

(d) If the sequence

$$0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$$

is exact, then $C \simeq B/\alpha[A]$.

By the previous parts, α is injective and β is surjective. By the first IM theorem applied to β, $C \simeq B/\ker(\beta)$, and by exactness at B we have $\ker(\beta) = \mathrm{im}(\alpha) = \alpha[A]$. Note that $\alpha[A]$ is just an isomorphic copy of A, so the exact sequence gives a kind of abstract representation of a quotient construction.

(2) Let H be a non-trivial torsion-free abelian group, and assume that H has the following property: for all nonzero elements $a, b \in H$ there exist nonzero integers m, n such that $ma = nb$ (groups with this property are sometimes said to have "rank one").

For any nonzero $a \in H$ and any prime number p, define $n_p(a)$ as follows: $n_p(a)$ is the largest integer $k \geq 0$ such that there exists b with $p^k b = a$ (b will necessarily be unique as H is torsion-free), or $n_p(a) = \infty$ if such b exists for all k.

Let $a, b \in H$ be nonzero. Prove that $n_p(a) = \infty$ if and only if $n_p(b) = \infty$, and also that $\{p : n_p(a) \neq n_p(b)\}$ is finite.

Hint: facts about gcd's may be helpful.

To simplify matters, we start by proving that V is isomorphic to a subgroup of $(\mathbb{Q}, +)$. This is similar to an exercise on HW1. Fix $a \neq 0$. Then for every $b \in H$ (including zero if you think about it) there exist m and n such that $n \neq 0$ and $ma = nb$. We claim that the ratio m/n is independent of the choice of m, n. To see this suppose that $m_1 a = n_1 b$ and $m_2 a = n_2 b$, then $(m_1 n_2 - m_2 n_1)a = n_1 n_2 b - n_1 n_2 b = 0$, so as H is t-f and a is nonzero $m_1 n_2 - m_2 n_1$. It is now routine to check that the map which takes $b \in H$ to m/n where $ma = nb$ is an injective HM from H to $(\mathbb{Q}, +)$. For the rest of the problem we assume that $H \leq \mathbb{Q}$, so that $n_p(a)$ is literally the sup of the k's such that $a/p^k \in H$ (with right convention about ∞)

Now let $a \in H$, and consider the special case where $b = Ma$ for some nonzero integer M. Suppose first that p is a prime which does not divide M, and let $k \geq 0$. By elementary number theory $gcd(p^k, M) = 1$ and there exist integers X and Y such that $Xp^k + YM = 1$. Then $b/p^k = M(a/p^k)$, and $a/p^k = Xa + Yb/p^k$, so that $a/p^k \in H \iff b/p^k \in H$. It follows that $n_p(a) = n_p(b)$.

Now suppose that p is a prime which divides M, say $M = p^j M_0$ where p does not divide M_0. Now as before $b/p^k = M(a/p^k)$, so that if $n_p(a) = \infty$ then $n_p(b) = \infty$. For all $k \geq 0$ we may find X and Y such that $Xp^k + YM_0 = 1$. It follows that $a/p^k = Xa + Yb/p^{k+j}$, so that if $n_p(b) = \infty$ then $n_p(a) = \infty$.

Since M has only a finite number of prime divisors, we have established the special case. The general case follows easily from the special case since any two elements of H have a common integer multiple.

(3) Recall that a subset $A \subseteq \mathbb{R}$ is *open* if for all $a \in A$ there is $\epsilon > 0$ such that $(a - \epsilon, a + \epsilon) \subseteq A$, and *closed* if its complement is open. It is a standard fact that a subset C of $\mathbb{R}$ is closed if and only if every convergent sequence (x_n) with $x_n \in C$ converges to a point of C. It is also standard that if B is

a subset of $\mathbb{R}$ and C is the set of limits of convergent sequences of elements of B, then C is closed and is the least closed set containing B: in this case we write $C = \bar{B}$ and call C the *closure* of B.

(a) Give an example of a non-closed subgroup of $(\mathbb{R}, +)$.
$\mathbb{Q}$.

(b) Prove that the closure of a subgroup of $(\mathbb{R}, +)$ is also a subgroup.
Easy, because $(x, y) \mapsto x - y$ is a continuous function. So if H is a subgroup and $x, y \in \bar{H}$ we fix $x_n \in H$ such that $x_n \to x$, and $y_n \in H$ such that $y_n \to y$; $x_n - y_n \in H$ because it's a subgroup and $x_n - y_n \to x - y$ by continuity.

(c) Prove that a non-trivial closed subgroup of $(\mathbb{R}, +)$ must either be an infinite cyclic group or be $\mathbb{R}$ itself.
Let H be a non-trivial closed subgroup. Note that $a \in H \iff -a \in H$, so H has positive elements. If $a \in H$ is nonzero then easily every real number is within $|a|$ of some integer multiple of a (which is also an element of H).
Let b equal the inf of $\{a \in H : a > 0\}$, and distinguish two cases:
   (i) $b = 0$. Then for every real c there are elements of H arbitrarily close to c, so we can choose $c_n \in H$ such that $c_n \to c$. As H is closed, $c \in H$. So $H = \mathbb{R}$.
   (ii) $b > 0$. There are elements of H arbitrarily close to b, so arguing as above $b \in H$. We claim that H is the infinite cyclic group generated by b. To see this let $c \in H$, and let n be the unique integer such that $nb \leq c < (n+1)b$. Then $0 \leq c - nb < b$ and $c \in H$, so $c = 0$.

(d) (Challenging, not for credit) Describe with proof the closed subgroups of $(\mathbb{R}^2, +)$
If L is a line through the origin then L is a closed subgroup isomorphic to $\mathbb{R}$. Now consider $L \cap H$, this is a closed subgroup of L which we can analyse as above: $L \cap H$ is either trivial, infinite cyclic, or L itself. If $L \cap H$ is trivial for all L then H is trivial.
Suppose that $L \cap H = L$ for some L, that is $L \subseteq H$. Let M be the line through the origin orthogonal to L, then every element of H can be written uniquely as $l + m$ where $l \in L$ and $m \in M \cap H$. Now the three possibilities for $M \cap H$ give us three possibilities for H; $H = L$, $H = \mathbb{R}^2$ and $H = \{l + nv : l \in L, n \in \mathbb{Z}\}$ where v is nonzerto and orthogonal to L.
So we reduced to the case where H is non-trivial and $L \cap H$ is either trivial or infinite cyclic for every L. We claim that in this case there is $d > 0$ such that every nonzero $v \in H$ is at distance at least d from 0. Otherwise we choose a sequence of nonzero $v_i = r_i(\cos(\theta_i), \sin(\theta_i)) \in H$ such that $r_i > 0$, $\theta_i \in [0, 2\pi]$, $r_i \to 0$. By an easy compactness argument we may thin out the sequence so that $\theta_i \to \theta$ for some θ. Now for any nonzero r we may choose integers n_i such that $n_i r_i \to r$, so that $n_i v_i \to r(\cos(\theta), \sin(\theta))$: so H contains a line through the origin contradicting our case assumption.
Now we know that for each $v \in H$, there is no other $w \in H$ within distance d (otherwise $w - v$ is too close to 0). So H is a *discrete*

subgroup. If H is contained in a line we know that H is an infinite cyclic subgroup of that line, so we may assume that H contains two linearly independent elements a and b say. If $\Lambda = \langle a, b\rangle$ then $\Lambda \leq H$ and it is easy to see that H/Λ is finite (because we can view the torus $\mathbb{R}^2/\Lambda$ as a compact space or as a probability space). If H/Λ has order n then easily $nH \subseteq \Lambda$, that is $H \leq \Lambda/n = \langle a/n, b/n\rangle$. So H is a free abelian group of rank 2, generated by two elements c and d which are linearly indepedendent.

(4) Let R be a commutative ring with 1, let M be an R-module, and recall from class the definition of the functor $Hom(M, -)$.

Give a proof or a counterexample for each of the following statements:

(a) If $\alpha : N_1 \to N_2$ is injective, then $Hom(M, \alpha) : Hom(M, N_1) \to Hom(M, N_2)$ is injective.

This is true. Suppose that $\phi, \psi \in Hom(M, N_1)$ with $\phi \neq \psi$. Fix m such that $\phi(m) \neq \psi(m)$. As α is injective, $\alpha\phi(m) \neq \alpha\psi(m)$, so $\alpha\phi \neq \alpha\psi$,

(b) If $\alpha : N_1 \to N_2$ is surjective, then $Hom(M, \alpha) : Hom(M, N_1) \to Hom(M, N_2)$ is surjective.

This is false in general. The assertion that $Hom(M, \alpha)$ is surjective amounts to saying that every morphism from M to N_2 factors through α. But let $R = \mathbb{Z}$, $M = N_2 = \mathbb{Z}/2\mathbb{Z}$, $N_1 = \mathbb{Z}$ and α the quotient map. Then α is surjective but the identity map from M to N_2 can't be factored through α, because the only morphism from M to N_1 is the zero map.

(c) If $\alpha : N_1 \to N_2$ is an isomorphism, then $Hom(M, \alpha) : Hom(M, N_1) \to Hom(M, N_2)$ is an isomorphism.

This is true. If $\beta : N_1 \to N_1$ is α^{-1}, then since $Hom(M,)$ is a functor it is easy to see that $Hom(M, \beta) = Hom(M, \alpha)^{-1}$.

(5) A function from $\mathbb{R}$ to the set of real $N \times N$ matrices is differentiable if each of the N^2 functions corresponding to the entries is differentiable, and the derivative is the matrix made up of the derivatives of the entries. Let A be a real $N \times N$ matrix. Prove that the matrix exponential function $\exp(At)$ is a differentiable function of t, and find its derivative.

Hint 1: since $AtAh = AhAt$ you can simplify the expression $\frac{\exp(At+Ah)-\exp(At)}{h}$ in a helpful way.

Hint 2: You may find it useful to bound the entries in $\sum_{i=2}^{\infty} \frac{(Ah)^i}{i!}$.

Taking the hint, we use the fact that $\exp(At + Ah) = \exp(At)\exp(Ah)$ to write $\frac{\exp(At+Ah)-\exp(At)}{h} = \exp(At)\frac{\exp(Ah)-I}{h}$.

Now $\exp(Ah) = I + hA + \sum_{i=2}^{\infty} h^i \frac{A^i}{i!}$.

We already saw that there is a constant $M > 0$ such that the absolute values of the entries in A^i is bounded by M^i. So the absolute values of the entries in the partial sum $\sum_{i=2}^{n} h^i \frac{A^i}{i!}$ are bounded by $\sum_{i=2}^{n} \frac{(|h|M)^i}{i!}$, and in the limit the absolute values of the entries in $\sum_{i=2}^{\infty} \frac{(Ah)^i}{i!}$ are bounded by $\sum_{i=2}^{n} \frac{(|h|M)^i}{i!} = \exp(|h|M) - 1 - |h|M$. It is now easy to see that $\frac{\sum_{i=2}^{\infty} \frac{(Ah)^i}{i!}}{h} \to 0$ as $h \to 0$, so $\exp(At)$ is differentiable with derivative $\exp(At)A$.

A little thought (rearrange partial sums) shows that $\exp(At)A = A\exp(At)$.