ALGEBRA I: SOLUTIONS

Problem 1. Let V be a finite dimensional vector space and let $A : V \to V$ be a linear map. Show that $\dim \operatorname{Ker}(A^2) \le 2 \dim \operatorname{Ker}(A)$.

Solution. We have an exact sequence

$$0 \to \operatorname{Ker}(A) \to \operatorname{Ker}(A^2) \xrightarrow{A} \operatorname{Ker}(A),$$

where the first map is the inclusion. This yields the stated inequality.

Problem 2. Let A and B be 3×3 complex matrices, and suppose that 1 is the only eigenvalue of A. For a non-negative integer n, let $f(n) = \operatorname{Tr}(BA^n)$. Show that f is a polynomial function of n.

Solution. Making a change of basis, we can assume that A is in Jordan normal form. There are three possibilities (up to a permutation of basis vectors):

$$\begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 1 & \\ & 1 & \\ & & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 1 & \\ & 1 & 1 \\ & & 1 \end{pmatrix}.$$

All omitted entries are 0. A simple computation shows that

$$\begin{pmatrix} 1 & 1 & \\ & 1 & \\ & & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & n & \\ & 1 & \\ & & 1 \end{pmatrix}.$$

A slightly more involved computation shows

$$\begin{pmatrix} 1 & 1 & \\ & 1 & 1 \\ & & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & n & (n^2-n)/2 \\ & 1 & n \\ & & 1 \end{pmatrix}.$$

(One can easily prove this formula by induction on n.) Thus in all cases we see that the entires of A^n are polynomial functions of n. Since $\operatorname{Tr}(BA^n)$ is a linear combination of the entries of A^n, the result follows.

Problem 3. Let R be a unique factorization domain (UFD) and let u and v be two nonzero elements of R.

(1) Prove or disprove: The ideal $uR \cap vR$ is necessarily principal.

(2) Prove or disprove: The ideal $uR + vR$ is necessarily principal.

Solution. (1) An element belongs to $uR \cap vR$ if and only if it is a multiply of both u and v. Since R is a UFD, this is equivalent to being a multiple of the lcm of u and v. Thus this ideal is principal and generated by the lcm.

(2) This ideal need not be principal in general. Indeed, let $R = \mathbb{C}[x, y]$ be the two-variable polynomial ring (which is a UDF) and take $u = x$ adn $v = y$. then $uR + vR$ is the maximal

Date: Aug 2022.

ideal (x, y), which is not principal (a generator would have to divide the gcd of x and y, which is 1).

Problem 4. Let S be a principal ideal domain (PID) and let a, b and c be nonzero elements of S. Show that $aS \cap (bS + cS) = (aS \cap bS) + (aS \cap cS)$.

Solution. We recall the following standard facts:

- S is a UFD (since every PID is a UFD)
- the ideal $bS + cS$ is principal and generated by the gcd of b and c
- the ideal $bS \cap cS$ is principal and generated by the lcm of b and c.

Thus we must prove

$$\mathrm{lcm}(a, \gcd(b, c)) = \gcd(\mathrm{lcm}(a, b), \mathrm{lcm}(a, c))$$

To prove this, it suffices to fix a prime element π and check that the maximal power of π dividing each side is the same. Let ℓ, m, and n be the powers of π in a, b, and c. The power of π in a gcd is the minimum of the powers in the input, while for lcm we take the maximum. It thus suffices to prove

$$\max(\ell, \min(m, n)) = \min(\max(\ell, m), \max(\ell, n)).$$

This can be seen directly.

Problem 5. Let M and N be finitely generated $\mathbb{Z}$ modules and let $h : M \to N$ be a $\mathbb{Z}$-linear homorphism. For a prime number p, let

$$h_p : M \otimes_{\mathbb{Z}} \mathbb{F}_p \to N \otimes_{\mathbb{Z}} \mathbb{F}_p$$

be the map $h \otimes \mathrm{Id}$. We consider h_p as a map of $\mathbb{F}_p$-vector spaces. Show that there is an integer d (depending on M, N and f) such that $\dim \mathrm{Ker}\, h_p = d$ for all sufficiently large p.

Solution. Let K and C be the kernel and cokernel of h; we thus have a 4-term exact sequence

$$0 \to K \to M \xrightarrow{h} N \xrightarrow{\pi} C \to 0.$$

Here π is defined to be the quotient map. All four of these terms are finitely generated abelian groups, and thus their torsion subgroups are finite. There is thus some number n such that the p-torsion of each group vanishes when $p > n$. We claim that the sequence

$$0 \to K/pK \to M/pM \to N/pN$$

is exact for $p > n$. Fix $p > n$ in what follows.

We first show that $K/pK \to M/pM$ is injective. Thus suppose $\overline{x} \in K/pK$ maps to 0 in M/pM. Letting $x \in K$ be a lift of $\overline{x}$, we have $x \in pM$, and so $x = py$ for some $y \in M$. Since $x \in K$, we have $h(x) = 0$, and so $ph(y) = 0$. Since the p-torsion of N vanishes, we thus have $h(y) = 0$, and so $y \in \ker(h) = K$. This shows that $x \in pK$, and so $\overline{x} = 0$, as required.

We now show that the image of K/pK is the kernel of $M/pM \to N/pN$. It is clear that K/pK is contained in the kernel. Now suppose that $\overline{x} \in M/pM$ belongs to the kernel, and let $x \in M$ be a lift of $\overline{x}$. Let $y = h(x)$. Since y maps to 0 in N/pN, we see that $y \in pN$. Write $y = pz$ with $z \in N$. Since $y \in \mathrm{im}(h)$, we have $\pi(y) = 0$, and so $p\pi(z) = 0$. Since the p-torsion in C vanishes, we have $\pi(z) = 0$, and so $z \in \mathrm{im}(h)$. Write $z = h(w)$ with $w \in M$. Thus

$$h(x) = y = pz = ph(w) = h(pw)$$

and so $x' = x - pw$ belongs to K. Since x' maps to $\overline{x}$ in M/pM, we see that $\overline{x}$ belongs to the image of K/pK, as required.

Now, note that $M/pM = M \otimes \mathbb{F}_p$, and similarly for N/pN. We have thus shown that $\ker(h_p) = K/pK$ for $p > n$. By the structure theorem, we have $K = \mathbb{Z}^d \oplus T$ where T is a finite abelian group. For $p > n$, T has vanishing p-primary piece, and so $T/pT = 0$, and so $K/pK = \mathbb{F}_p^d$. Thus $\dim(\ker(h_p)) = d$ for $p > n$, as required.