KERALA SCHOOL OF MATHEMATICS
ALGEBRA II 2021 MAY–AUG, FINAL EXAM

Instructions: Answer all questions. To get full credit, you must justify your answers.

(1) Let A be a commutative ring with identity containing a field k as a subring. Suppose that A is finite dimensional as a k-vector space (under the induced structure). For each of the following statements, determine whether it is true or false, and give your reasons (either a proof, or a counter example):
   (a) A is Artinian (as a ring).
   (b) A is Noetherian (as a ring).
   (c) If A is an integral domain, then it is a field.
   (d) The nil-radical and Jacobson radical of A are the same.

SOLUTION: All the statements are true.

Suppose that d is the dimension of A as a vector space over k. Any chain of k-vector subspaces of A (with strict inclusions) can have at most $d+1$ elements. This is because if $V \subsetneq W$ are subspaces then $\dim V \lneq \dim W$. In particular, the ascending chain condition and descending chain condition hold for subspaces of A. Since the ideals of A are subspaces, these conditions hold for them. This proves that A is Noetherian and Artinian.

Now suppose that A is an integral domain and let $0 \neq x$ be an element of A. Consider $1, x, x^2, \ldots$. These cannot be linearly independent (over k), since the size of any linearly independent set is at most d. Choose ℓ least such that $1, x, \ldots, x^\ell$ are linearly dependent, and let $\sum_{0\leqslant i\leqslant \ell} \lambda_i x^i = 0$ be a non-trivial dependence relation (with $\lambda_i \in k$), which we rewrite as $x(\sum_{1\leqslant i\leqslant \ell} \lambda_i x^{i-1}) = \lambda_0$. It is enough to prove $\lambda_0 \neq 0$, for then λ_0 will be a unit in k and thus x will be a unit in A. Suppose, by way of contradiction, that $\lambda_0 = 0$. Then, since A is an integral domain, $\sum_{1\leqslant i\leqslant \ell} \lambda_i x^{i-1} = 0$ is a non-trivial linear dependence relation among $1, x, \ldots, x^{\ell-1}$, contradicting the minimality of ℓ.

Let $\mathfrak{p}$ be a prime ideal in A. Then $\mathfrak{p} \cap k = 0$ and $A/\mathfrak{p}$ contains k as a subring and has finite dimension as a vector space over k. Since $A/\mathfrak{p}$ is also an integral domain, it now follows from the previous part that it is a field. Thus every prime ideal of A is maximal, and the nilradical of A and the Jacobson radical of A coincide. (The nilradical is the intersection of all prime ideals and the Jacobson radical the intersection of all maximal ideals.) $\square$

(2) Consider left ideals in the ring $M_4(\mathbb{Z}/3\mathbb{Z})$ of 4×4 matrices with entries in the field $\mathbb{Z}/3\mathbb{Z}$ of three elements.

- What are their possible cardinalities?
- How many are there of each cardinality?

SOLUTION: Let k be the field $\mathbb{Z}/3\mathbb{Z}$. We identify $M_4(\mathbb{Z}/3\mathbb{Z})$ with the ring $A := \operatorname{End}_k(V)$ of k-linear endomorphisms of a 4-dimensional vector space V over k. As was shown in a tutorial exercise, the left ideals of $M_4(\mathbb{Z}/3\mathbb{Z})$ are in bijection with subspaces of V: for a subspace W, the corresponding left ideal ℓ_W comprises the endomorphisms vanishing on W.

The dimension as a k-vector space of ℓ_W is $\dim V(\dim V - \dim W) = 4(4 - \dim W)$. Thus the cardinality of ℓ_W is $3^{4(4-\dim W)}$. Since W can have dimension 0, 1, 2, 3, or 4, the possible cardinalities of left ideals in A are 3^{16}, 3^{12}, 3^8, 3^4, and 3^0.

To count the number of left ideals of a given cardinality $3^{4(4-d)}$, we need only count the number of subspaces of dimension d in V. Recall that we learnt how to solve such counting problems in class. Fix a d, $0 \leqslant d \leqslant 4$. The group $G := GL_4(k)$ acts transitively on the set of all d-dimensional subspaces of V. So this set can be identified with the left cosets G/H, where H is the stabiliser of any fixed d-dimensional subspace.

Recall that $|GL_d(k)| = (|k|^d - 1) \cdot (|k|^d - |k|) \cdot \cdots \cdot (|k|^d - |k|^{d-1})$. A little thought (e.g., by letting H be the stabiliser of the subspace spanned by the span of the standard basis vectors $e_1, \ldots, e_d$) shows that $|H|$ equals $|GL_d(k)| \cdot |GL_{4-d}(k)| \cdot |k|^{d(4-d)}$ so that

$$\left|\frac{G}{H}\right| = \frac{|G|}{|H|} = \frac{|GL_4(k)|}{|GL_d(k)| \cdot |GL_{4-d}(k)| \cdot |k|^{d(4-d)}}$$

Substituting values 0 through 4 into d in the above, we see that the number of left ideals of cardinality $3^{d(4-d)}$ is, respectively, 1, 40, 130, 40, 1 for d equal to 0, 1, 2, 3, 4. $\square$

(3) State whether the following assertion is true or false. Justify your answer with a proof or counter example as the case may be.

> Let p be a prime, G a finite group, P a Sylow p-subgroup of G, and H a subgroup of G that contains the normaliser $N_G(P)$ of P. Then $N_G(H) = H$.

SOLUTION: The statement is true. Here is a proof. It is enough to show that $H \supseteq N_G(H)$, the other containment being trivially true (for any subgroup H of any group G). Let $x \in N_G(H)$. Then $xPx^{-1} \subseteq xHx^{-1} = H$. Thus xPx^{-1} is a Sylow p-subgroup of H (note that xPx^{-1} is a Sylow p-subgroup of G and being contained in H is a Sylow p-subgroup of H too). By Sylow's second theorem (applied in the group H), there exists h in H such that $xPx^{-1} = hPh^{-1}$ (since P and xPx^{-1} are both Sylow p-subgroups of H). This means $x^{-1}h \in N_G(P) \subseteq H$, and so $x \in H$. $\square$

(4) In how many ways can the edges of a regular tetrahedron be coloured with two colours?

SOLUTION: The answer can be obtained as an application of the Orbit Counting Lemma (OCL), by counting the number of orbits for the action of the symmetry group of the regular tetrahedron on the set of colourings of the edges (of the labelled tetrahedron). Alternatively, a brute force approach is also possible.

The group of symmetries of the regular tetrahedron can be identified with the alternating group A_4. The number of colourings of the six edges with two colours is $2^6 = 6^4$. The number of colourings left fixed respectively by the elements identity, a product of two disjoint transpositions, and a three cycle is 2^6, 2^4, and 2^2. Thus the number of A_4 orbits on the set of colourings of the edges is, by the OCL:

$$\frac{1}{12}\left(2^6 + 3 \times 2^4 + 8 \times 2^2\right) = 12 \qquad \square$$

(5) Determine the numbers in the class equation of the Dihedral group D_{12} (of order 24).

SOLUTION: Let X be a regular dodecagon. Let r denote the rotation (say, counter clockwise) by an angle of $\pi/6$ of X about its centre. Let s denote the reflection in a line through a pair of opposite vertices of X. The group D_{12} of symmetries of X is generated by r snd s. The relations between r and s are all consequences of the following basic relations: $r^{12} = 1$, $s^2 = 1$, $srs^{-1} = r^{-1} = r^{11}$.

Using these, we can see that D_{12} comprises 24 elements: twelve rotations r^j, $0 \leqslant j < 12$, and twelve reflections sr^j, with $0 \leqslant j < 12$. The conjugacy classes in D_{12} are: $\{1\}$, $\{r^6\}$, $\{r, r^{11}\}$, $\{r^2, r^{10}\}$, $\{r^3, r^9\}$, $\{r^4, r^8\}$, $\{r^5, r^7\}$, $\{s, sr^2, sr^4, sr^6, sr^8, sr^{10}\}$, and $\{sr, sr^3, sr^5, sr^7, sr^9, sr^{11}\}$. Thus the class equation is $1+1+2+2+2+2+6+6 = 24$. $\square$

(6) Let M be a finitely generated abelian group.

(a) Let S and T be maximal linearly independent subsets of M. Must S and T have the same cardinality?

SOLUTION: Yes: both S and T have cardinality equal to the rank of M.

PROOF: M being a Noetherian $\mathbb{Z}$-module, all its submodules are finitely generated. In particular, the torsion TM is finitely generated and there exists a positive integer d that kills TM.

Lemma 1. *Elements $m_1, \ldots, m_n$ of M are linearly independent if and only if their images $\overline{m}_1, \ldots, \overline{m}_n$ in M/TM are linearly independent.*

PROOF: If $a_1m_1 + \cdots + a_nm_n \in TM$ (with a_i in $\mathbb{Z}$), then $da_1m_1 + \cdots + da_nm_n = 0$. $\square$

Thanks to the lemma, we may assume that M is free and so isomorphic to $\mathbb{Z}^r$ for some non-negative integer r. Now, thanks to the following lemma, whose proof we leave as an exercise, it follows that a set of elements of $\mathbb{Z}^r$ is maximally linearly independent if and only if the elements form a basis for $\mathbb{Q}^r$. Thus the cardinality of any such set must be r.

Lemma 2. *Elements $m_1, \ldots, m_r$ of $\mathbb{Z}^r$ are linearly independent if and only if they are linearly independent (over $\mathbb{Q}$) in $\mathbb{Q}^r$.* $\square$

(b) Let φ be an abelian group endomorphism of M. For each of the following statements, determine whether it is true or false. Justify your answer.

(i) If φ is surjective, then it is an isomorphism.

SOLUTION: Yes.[1]

PROOF: If M is torsion then it is finite (since M is finitely generated by hypothesis), and then of course the statement is true. Let us now prove the statement when M is free. In this case we have $M \simeq M \oplus \ker \varphi$ (since any surjective homomorphism to a free module splits). Thus $\ker \varphi$ is also free, and by equating ranks on both sides we conclude that $\ker \varphi = 0$.

We can use the snake lemma to derive the result in the general case by combining the results in the two special cases above. Note that φ maps the torsion TM to itself and that the induced map $\overline{\varphi} : M/TM \to M/TM$ is surjective. Since M/TM is free, we conclude, from the second special case above, that $\overline{\varphi}$ is an isomorphism, and so $\ker \overline{\varphi} = 0$.

Let us now apply the snake lemma. Suppose that the rows in its diagram are both $0 \to TM \to M \to M/TM \to 0$ and the vertical maps are (those induced by) φ. The cokernel of $\varphi : TM \to TM$ is caught between $\ker \overline{\varphi}$ and the cokernel of φ in the exact sequence of the conclusion of the snake lemma, and hence vanishes. It follows (by the first special case above) that the $\varphi : TM \to TM$ is an isomorphism. Finally, $\ker \varphi$ being caught between the kernel of $\varphi : TM \to TM$ and $\ker \overline{\varphi}$ is also forced to vanish. □

(ii) If φ is injective, then it is an isomorphism.

SOLUTION: False. Multiplication by 2 on $\mathbb{Z}$ is injective but not surjective.□

[1]The statement holds in general for any Noetherian module, as we show now. Consider the ascending chain $\ker \varphi \subseteq \ker \varphi^2 \subseteq \ldots \subseteq \ker \varphi^i \subseteq \ldots$. Let $i \gg 0$ such that $\ker \varphi^i = \ker \varphi^{2i}$. Since φ is surjective, so is φ^i. We claim that φ^i is injective (it suffices to prove this, since then φ is forced to be injective as well). Suppose $\varphi^i(m) = 0$. Since φ^i is surjective, there exists m' such that $m = \varphi^i(m')$. But then $\varphi^{2i}(m') = \varphi^i(m) = 0$, which means m' belongs to $\ker \varphi^{2i}$. But $\ker \varphi^{2i} = \ker \varphi^i$ (by choice of i), so $m = \varphi^i(m') = 0$. □

(7) Let M, M', and N be finitely generated abelian groups. Assume that $M \oplus N \simeq M' \oplus N$. Is it true that $M \simeq M'$? Justify your answer.

SOLUTION: By one of the versions of the structure theorem for finitely generated abelian groups, N is a finite product of cyclic groups with the finite factors being of prime power orders. Thus we are immediately reduced to the case when N equals $\mathbb{Z}$ or $\mathbb{Z}/p^r\mathbb{Z}$ for some prime power $p^r > 1$.

To show that $M \simeq M'$, it is enough to show that $TM \simeq TM'$ and $\operatorname{rank} M = \operatorname{rank} M'$ (because $M \simeq TM \oplus \mathbb{Z}^{\operatorname{rank} M}$ and similarly for M'). We are given that $M \oplus N \simeq M' \oplus N$, which is equivalent (for the same reason as above) to saying that $T(M \oplus N) \simeq T(M' \oplus N)$ and that $\operatorname{rank}(M \oplus N) = \operatorname{rank}(M' \oplus N)$. But $T(M \oplus N) = TM \oplus TN$ and $\operatorname{rank}(M \oplus N) = \operatorname{rank} M + \operatorname{rank} N$ and similarly with M' in place of M. Thus we readily obtain that $\operatorname{rank} M = \operatorname{rank} M'$, and it is enough to show that $TM \simeq TM'$.

By the primary decomposition theorem, $TM = \oplus_{\ell \text{ prime}} \ell(M)$, where ℓ varies over all the primes, and $\ell(M)$ denotes the ℓ-primary component of M. Similarly for M'. Thus it is enough to show that $\ell(M) = \ell(M')$ for every prime ℓ.

Suppose that $N = \mathbb{Z}$. Then $T(M \oplus N) = TM \oplus TN = TM$ and similarly $T(M' \oplus N) = TM'$. So we immediately have $TM \simeq TM'$.

Now suppose that $N = \mathbb{Z}/p^r\mathbb{Z}$. We have $\ell(M \oplus N) = \ell(M)$ for $\ell \neq p$ and $p(M \oplus N) = p(M) \oplus N$ and similarly for M'. Thus we immediately conclude that $\ell(M) = \ell(M')$ for $\ell \neq p$.

The only case that remains is when $\ell = p$. The structure theorem for finite p-primary abelian groups (finitely generated modules over $\mathbb{Z}/p^k\mathbb{Z}$ for some $k \geqslant 1$) says that isomorphism classes of these are in one-to-one correspondence with multisets of non-negative integers; furthermore, denoting by $\lambda(\cdot)$ the multiset function on such modules, the multiset $\lambda(A \oplus B)$ corresponding to the direct sum $A \oplus B$ of two such modules A and B is the multiset-union of the multisets $\lambda(A)$ and $\lambda(B)$. From $p(M) \oplus N \simeq p(M') \oplus N$ we are thus lead to an equality of multisets $\lambda(p(M)) \cup \{r\} = \lambda(p(M')) \cup \{r\}$, from which it is immediate that $\lambda(p(M)) = \lambda(p(M'))$ and so $p(M) \simeq p(M')$. $\square$

(8) Determine the following:

(a) The number of abelian group homomorphisms from $\mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ to $\mathbb{Z}/3\mathbb{Z}$.

(b) The number of such homomorphisms that are surjective.

(c) The number of such surjective homomorphisms that are split. (A surjective homomorphism $\varphi : M \to N$ of abelian groups is <u>split</u> if there exists a group homomorphism $\psi : N \to M$ such that $\varphi \circ \psi$ is the identity map on N.)

SOLUTION: The homomorphisms from a direct sum are in bijection with the direct product of homomorphisms from each factor (by the universal property of direct sum). A homomorphism from a cyclic group is determined by the image of any fixed generator. The image under a homomorphism of any generator of either $\mathbb{Z}/9\mathbb{Z}$ or $\mathbb{Z}/3\mathbb{Z}$ can be any element of $\mathbb{Z}/3\mathbb{Z}$. Thus the answer to part (a) is $3 \times 3 = 9$.

Since $\mathbb{Z}/3\mathbb{Z}$ is a simple group, any non-zero homomorphism to it is onto. Thus, out of the 9 homomorphisms in part (a), the only one that is not onto is the zero homomorphism. The answer to part (b) is therefore $9 - 1 = 8$.

To answer part (c), we claim that a homomorphism φ as in part (a) is (surjective and) split if and only if its restriction $\varphi|$ to the second factor $\mathbb{Z}/3\mathbb{Z}$ is an isomorphism. Assuming the claim, we see that the number of such homomorphisms is $3 \times 2 = 6$ (the image of the generator of the first factor $\mathbb{Z}/9\mathbb{Z}$ can be arbitrary, and the image of the generator of the second factor $\mathbb{Z}/3\mathbb{Z}$ must be non-zero).

It remains only to prove the claim. Suppose that $\varphi|$ is an isomorphism. Then φ is split: a splitting homomorphism is obtained by the product of the zero homomorphism from $\mathbb{Z}/3\mathbb{Z}$ to the first factor $\mathbb{Z}/9\mathbb{Z}$ and the inverse of $\varphi|$ from $\mathbb{Z}/3\mathbb{Z}$ to the second factor $\mathbb{Z}/3\mathbb{Z}$. For the converse, suppose now that φ is split. Note that any splitting homomorphism—call it ψ—is zero when further composed with the projection on to the first factor (since the only homomorphism from $\mathbb{Z}/3\mathbb{Z}$ to $\mathbb{Z}/9\mathbb{Z}$ is the trivial one). Thus $\varphi| \circ \psi$ is the identity map on $\mathbb{Z}/3\mathbb{Z}$, and $\varphi|$ is a bijection. $\square$