VIGRE Algebra QR Review, October 7, 2002

Summary of Session

Hint for the sequence 10, 11, 12, 13, 14, 15, 16, 17, 20, 22, 24, 31, 100, 121, 10000: it's constant. (Really.)

Because of the break next week, our next meeting will be on Monday, October 21: the focus for that meeting will be linear algebra and canonical forms for matrices. The following problems from the list for October 7 were discussed.

1. Let R be the PID $k[x]$, where k is a field and x is an indeterminate. Consider the quotient M of the free R-module R^3 by the submodule N generated by the elements (x^2, x^3, x^4) and $(1, x+1, x^2)$. Express M explicitly as a direct sum of cyclic modules.

Solution. One method is to make the given vectors into the rows or columns of a matrix. (Rows were used during the session, but columns will be used here.) One is killing the column space of the matrix in the appropriate free module. Elementary column operations (permuting the columns, adding or subtracting a multiple of one column from another) do not affect the span of the columns and so do not affect the isomorphism class of the answer. Elementary row operations likewise do not affect the isomorphism class of the answer: they correspond to a change of free basis in the ambient free module. Putting the second vector first, we have the matrix:

$$\begin{bmatrix} 1 & x^2 \\ x+1 & x^3 \\ x^2 & x^4 \end{bmatrix} \to \begin{bmatrix} 1 & 0 \\ x+1 & -x^2 \\ x^2 & 0 \end{bmatrix} \to \begin{bmatrix} 1 & 0 \\ 0 & -x^2 \\ x^2 & 0 \end{bmatrix} \to \begin{bmatrix} 1 & 0 \\ 0 & -x^2 \\ 0 & 0 \end{bmatrix}$$

where at the first step we subtracted x^2 times the first column from the second, and at the second (resp., third) step we subtract $x+1$ (resp., x^2) times the first row from the second (resp., third) row. The column space of the third matrix is the kernel of the map from $R^3 \to R/(x^2) \oplus R$ that sends e_1 to 0, e_2 to the generator of $R/(x^2)$, and e_3 to the generator of R, where $e_1 = (1, 0, 0) \in R^3$, and so forth. Thus, the module under consideration is isomorphic with $R/(x^2) \oplus R$. (It was not asked, but the annihilator of this module is (0), because there is a free component.) Note that matrices can alway be brought to diagonal form by elementary row and column operations over a Euclidean ring such as $k[x]$ or $\mathbb{Z}$.

2. (a) Classify the abelian groups of order 540 up to isomorphism.

(b) Can a subgroup of S_9 act transitively on a set with 25 elements? Can a group of order 75 act doubly transitively on a set with 5 elements?

Solution. Two solutions were presented to (a). I recommend the second method as requiring less thought. Let $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. For both solutions, note that $540 = 2^2 \cdot 3^3 \cdot 5$. The first method used the classification theorem which asserts that every nonzero finite abelian group is uniquely isomorphic with a direct sum $\mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_k}$ with $d_1 > 1$ and $d_i | d_{i+1}$ for $1 \le i < k$. Note that $|G| = d_1 \cdots d_k$ here, and it follows that d_1^k, d_2^{k-1}, etc. all divide

$|G|$. Thus, $k \le 3$. The prime 5 cannot occur except in d_k, and the prime 2 cannot occur before d_{k-1}. Suppose that $k = 3$. The $d_1 = 3$ is forced, d_2 must be 3 or 6, and d_3 must 60 in the first case and 30 in the second case. Next, suppose that $k = 2$. Then d_1 must be 2, 3 or 6 and d_2 must be 270, 180, or 90, resp. Finally, if $k = 1$ then $d_1 = 540$. There are 6 groups: $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{60}$, $\mathbb{Z}_3 \oplus \mathbb{Z}_6 \oplus Z_{30}$, $\mathbb{Z}_2 \oplus \mathbb{Z}_{270}$, $Z_3 \oplus \mathbb{Z}_{180}$, $\mathbb{Z}_6 \oplus \mathbb{Z}_{90}$, and $\mathbb{Z}_{540}$.

The second method uses the fact that a finite abelian group is uniquely, except for the order of the terms, a direct sum of primary cyclic groups (i.e., ones of prime power order). We generalize the problem slightly and classify abelian groups of order p^2q^3r where p, q, and r are distinct primes. Again, the product of the orders of the summands must be $|G|$. We can analyze the contributions for the primes p, q and r separately. For the contribution from p^2 we must have either $\mathbb{Z}_p \oplus \mathbb{Z}_p$ or $\mathbb{Z}_{p^2}$. For the contribution from q^3 we must have either $\mathbb{Z}_q \oplus \mathbb{Z}_q \oplus Z_q$ or $\mathbb{Z}_q \oplus \mathbb{Z}_{q^2}$ or $\mathbb{Z}_{q^3}$. For the contribution from r we can only have $\mathbb{Z}_r$. Again, there are six possibilities, $2 \cdot 3 \cdot 1$: $\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_q \oplus \mathbb{Z}_q \oplus Z_q \oplus \mathbb{Z}_r$, $\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_q \oplus \mathbb{Z}_{q^2} \oplus \mathbb{Z}_r$, $\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_{q^3} \oplus \mathbb{Z}_r$, $\mathbb{Z}_{p^2} \oplus \mathbb{Z}_q \oplus \mathbb{Z}_q \oplus Z_q \oplus \mathbb{Z}_r$, $\mathbb{Z}_{p^2} \oplus \mathbb{Z}_q \oplus \mathbb{Z}_{q^2} \oplus \mathbb{Z}_r$, and $\mathbb{Z}_{p^2} \oplus \mathbb{Z}_{q^3} \oplus \mathbb{Z}_r$. To convert one of these decompositions back to the other form, use the fact that if $a_1, \ldots, a_k$ are integers that are relatively prime in pairs, then $\mathbb{Z}_{a_1 \cdots a_k} \cong \mathbb{Z}_{a_1} \oplus \cdots \oplus \mathbb{Z}_{a_k}$, a form of the Chinese remainder theorem. For each prime combine the cyclic groups involving the largest distinct prime powers into one group: then repeat with the summands that have not been "used." E.g., $\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_{q^3} \oplus \mathbb{Z}_r = \mathbb{Z}_p \oplus \mathbb{Z}_{pq^3r}$, $\mathbb{Z}_{p^2} \oplus \mathbb{Z}_q \oplus \mathbb{Z}_{q^2} \oplus \mathbb{Z}_r \cong \mathbb{Z}_q \oplus \mathbb{Z}_{p^2q^2r}$, and $\mathbb{Z}_{p^2} \oplus \mathbb{Z}_q \oplus \mathbb{Z}_q \oplus Z_q \oplus \mathbb{Z}_r \cong \mathbb{Z}_q \oplus \mathbb{Z}_q \oplus \mathbb{Z}_{p^2qr}$.

Note, quite generally, that in an abelian group of order n where p^k is the highest power of p dividing n, the contribution from p^k is the Sylow p-subgroup, and the possibilities correspond to ways of factoring p^k into powers of p (excluding 1), where the order of the factors does not count. This is the same as the ways to write k as a sum of positive integers, where order does not count. After one determines the possible contributions from the various maximum prime powers occurring in the factorization of n, one combines them in all possible ways.

For part (b) the answer is "no" to both questions. $|S_9| = 9!$ which is divisible by 5 but not by 25. Since the order of an orbit will divide the order of the group, and a subgroup of S_9 has order dividing $9!$, such a subgroup cannot act transitively on a set with 25 elements. For the second part, note that the number of ordered pairs of distinct elements from the 5 element set is $5 \cdot 4 = 20$. Double transitivity means that the group acts transitively on these pairs. Since 20 does not divide 75, there cannot be such an action.

5. Let k be a field, and x a variable over k. (a) Let $p(x)$, $q(x) \in k[x]$ be relatively prime non-zero polynomials. Viewing $\dfrac{k[x]}{(p(x))}$ and $\dfrac{k[x]}{(q(x))}$ as $k[x]$-modules in the natural way, prove that $\mathrm{Hom}_{k[x]}\left(\dfrac{k[x]}{(p(x))}, \dfrac{k[x]}{(q(x))}\right) = 0$.

(b) Let V and W be vector spaces over k. Let $A : V \to V$ and $B : W \to W$ be k-linear endomorphisms. Make V into a $k[x]$-module so that multiplication by x is the same as the action of A, and make W into a $K[x]$-module so that multiplication by x is the same as the action of B. Given a k-linear map $T : V \to W$, give a necessary and sufficient condition on T, A, and B fo T to be a homomorphism of $k[x]$-modules.

(c) Let $A = \begin{pmatrix} 0 & 0 & 3 \\ 1 & 0 & -3 \\ 0 & 1 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$. Use parts (a) and (b) to show that the only 3×3 matrix T such that $TA = BT$ is the zero matrix.

Solution. In general, if $M = Ru$ is a cyclic module generated by u then $f \in \mathrm{Hom}_R(M,\, N)$ is uniquely determined by the element of N to which u maps: if u maps to v then linearity forces ru to map to rv. Thus, if $[1]$ maps to $[h]$ (where $[]$ are being used to indicate classes in the quotients, while $1,\, h \in k[x]$, then $[p] \in K[x]/(p)$ maps to $[ph]$ in $k[x]/(q)$. But $[p] = 0$, and so maps to 0 in $K[x]/(q)$. Thus, $q|(ph)$. Since p and q are relatively prime, it follows that $q|h$. But then $[h] = 0$ in $k[x]/(q)$, and so the image of $[r]$, which is $r[h] = r(0) = 0$ for all $r \in k[x]$.[1]

(b) A necessary condition is that $T(xv) = xT(v)$ for all $v \in V$. This says that $T(A(v)) = B(T(v))$ for all $v \in V$ or simply that $TA = BT$. This condition is sufficient as well: one simply needs to check that multiplication by any polynomial $\sum_i c_i x^i$ commutes with the action of T. From the fact that T is linear, one easily reduces to showing that $T(x^i v) = x^i T(v)$ for all i, and the condition that $TA = BT$ gives this for $i = 1$. Now use induction: at the inductive step, $T(x^{i+1}v) = T(xx^i v) = xT(x^i v)$ (by the case $i = 1$) $= xx^i T(v)$ (by the induction hypothesis) $= x^{i+1}T(v)$, as required.

(c) Consider the $k[x]$-module $k[x]/(f)$ where f is $x^n - a_{n-1}x^{n-1} - \cdots - a_0$. By the division algorithm, every element has a unique representative that is 0 or a polynomial of degree at most $n-1$, and so $1, x, \ldots, x^{n-1}$ is a basis for this module. The matrix of multiplication by x, which is a linear transformation on $k[x]/(f)$, has columns $e_2, \ldots, e_n$. The last column is the transpose of $(a_0 \;\; a_{n-1})$. This matrix is called the *companion matrix*[2] of the polynomial f. It has a string of $n-1$ 1 's just below the main diagonal, all zeros elsewhere in the first $n-1$ columns, and the coefficients of the polynomial, with signs reversed, in the final column. Thus, the module corresponding to the first matrix is $k[x]/p$ where $p = x^3 - x^2 + 3x - 3$, while the module corresponding to the second matrix is $K[x]/(q)$ where $q = x^3$. It is clear that p and q are relatively prime, and so parts (a) and (b) together clear give the required result.

7. (a) Let $I,\, J,\, K$ be ideals of a principal ideal domain R. Prove that $I \cap (J + K) = (I \cap J) + (I \cap K)$. (b) Find ideals $I,\, J,\, ,K$ of $S = \mathbb{C}[x,y]/(x,y)^2$ such that $I \cap (J + K) \neq (I \cap J) + (I \cap K)$. [You may assume that $(x,y)/(x,y)^2$ is a vector space of dimension 2, thought of as a module over $\mathbb{C} \cong \mathbb{C}[x,y]/(x,\, y)$.

Solution. (a) is easy to verify if any of the three ideals is (0). If not, we use the fact that two nonzero ideals will be equal if for every prime p, the highest power of p dividing a generator for one is the same as the highest power of p dividing a generator for the other. Let the highest powers of p dividing generators for I, J, and K be i, j, and k, resp. The highest powers dividing generators for the sum of two ideals will be the min (for

---

[1] Here is a different approach to (a). For any two modules M, N over a commutative ring R, the annihilator of M and the annihilator of N both kill $\mathrm{Hom}_R(M,\, N)$. This shows that $(p,\, q)k[x]$ kills the Hom, and since p and q are relatively prime, they generate all of $k[x]$.

[2] One more fact, not used here: the characteristic polynomial of the companion matrix of f is the polynomial f.

which we use $\wedge$) of the highest powers for the individual ideals, while the highest power for the intersection will be the max (for which we use $\vee$). Therefore, it suffices to show that $i \vee (j \wedge k) = (i \vee j) \wedge (i \vee k)$, which is well known.[3]

For part (b), $\mathbb{C}[x,\, y]/(x, y)^2 = \mathbb{C}[x,\, y]/(x^2,\, xy,\, y^2] \cong \mathbb{C} + \mathbb{C}\overline{x} + \mathbb{C}\overline{y}$, a 3-dimensional $\mathbb{C}$-vector space with $\mathbb{C}$-basis 1, $\overline{x}$, $\overline{y}$. In this ring, $\overline{m} = \mathbb{C}\overline{x} + \mathbb{C}\overline{y} \cong \mathbb{C}^2$ as a $\mathbb{C}$-vector space, and every subspace is an ideal, since multiplication by $\overline{x}$ and $\overline{y}$ will kill it, and it will be closed under scalar multiplication. Choose three vectors in $\overline{m}$ such that any two are linearly independent, e.g., $\overline{x}$, $\overline{y}$, and $\overline{x}+\overline{y}$. The 1-dimensional subspaces I, J, K they span over $\mathbb{C}$ are ideals. Then $J + K = \overline{m}$, and $I \cap (J + K) = I \cap \overline{m} = I$ is 1-dimensional. But $(I \cap J) + (I \cap K) = 0 + 0 = 0$.

[3]Sketch of proof. By symmetry, we may assume $j \leq k$. If $i \geq k$ both sides are i, if $i \leq j$ both sides are j, and if $j \leq i \leq k$ both sides are i.