Chapter 8

Dave

April 14, 2015

1 The Idea of a Module

1. (a) Let ψ be the map defining M as an R-module. Then for $r \in R$, $\psi(r)$ is a homomorphism on M so $r0 = 0$. And ψ is a homomorphism from R to $\text{End}(M)$, so $\psi(0) = 0$.

   (b) As in part a, this is a consequence of the homomorphism property of ψ and $\psi(r)$ for all r.

   (c) As in part a, this is a consequence of the homomorphism property of ψ and $\psi(r)$ for all r.

2. Let W be a linear subspace of V that is closed under T, that means that for all $w \in W$, $T(w) \in W$, and for all $k \in K, kw \in W$, so combining these facts and iterating we get that for all $p = \sum_i k_i x^i \in K[x], p(T)(w) \in W$, so W is a $K[x]$ submodule of V. So those conditions are sufficient to define a $K[x]$ submodule, and it is readily apparent that they are necessary. For any $w \in W$, if $T(w) = 0$, then $p(T)(w) = \sum_i a_i 0^i = 0$ for all $p \in K[x]$, so the colonel of T is a submodule. And if $v \in T(V)$, then $v \in V \to T(v) \in T(V) \to p(T)(v) \in V \forall p$, so $T(V)$ is a submodule.

3. Let $p \in R$, then $p \sum_i r_i x_i = \sum pr_i x_i \in IM$ since I is a left ideal so $pr_i \in I \forall i$.

4. Let $n \in N, r \in \text{ann}(N), p \in R$, then $prn = p0 = 0$ and $rpn = rm$ for some $m \in N$ since N is a submodule, so $rm = 0$ since r annihilates N, so $\text{ann}(N)$ is an ideal of R.

5. (a) Let $r \in R, x \in \cap_\alpha M_\alpha$, then $x \in M_\alpha \forall \alpha \to rx \in M_\alpha \forall \alpha$ since each M_α is a submodule. So $rx \in \cap_\alpha M_\alpha$ so $\cap_\alpha M_\alpha$ is a submodule.

   (b) Let $x \in \cup_n M_n$ then $x \in M_k$ for some k and all $m \geq k$ so $rx \in M_m$ for all such m for all $r \in R$ since each M_m is a submodule so $rx \in \cup_n M_n$ so $\cup_n M_n$ is a submodule.

   (c) $r(a + b) = ra + rb \in A + B$ since A and B are submodules.

6. (a) Let $p \in R$, then $p \sum_i r_i s_i = \sum pr_i s_i \in RS$ since R is a left ideal of itself so $pr_i \in R \forall i$.

(b) It's pretty clear that $\langle S\rangle + RS$ contains S and it's a submodule since for any $p \in R$, $s + rt \in \langle S\rangle + RS$, we have $p(s + rt) = ps + prt \in RS$.

(c) Any submodule containing S must contain $\langle S\rangle$, since it has to be a group, and it must contain RS, since it's a submodule, and so it must contain $\langle S\rangle + RS$ since it's a group. Since we already established that $\langle S\rangle + RS$ is a submodule, this means it's minimal.

(d) If $1 \in R$, then $1S = S$, so $S \subset RS$. And if $s, t \in S$, then $s + t = 1s + 1t \in RS$, and $-s = -1s \in RS$, so $\langle S\rangle \subset RS$, so $\langle S\rangle + RS = RS$.

7. Let x_1 and x_2 be linear independent vectors in a basis of V over K. Then $f : \sum_i a_i x_i \to a_1 x_2 + a_2 x_1 + \sum_{i>2} a_i x_i$ is a nonzero endomorphism on V, but $x_1 - f(x_2) = 0$, so x_1 and x_2 are not linear independent over $\mathrm{End}_K(V)$.

8. The elements of this group are n-tuples of n-dimensional vectors, e.g. if $V = \mathbb{Z}$ and $n = 2$ then a representative element would be $([1, 2], [3, 4])$ and so you can arrange those vectors into the columns of a matrix and represent an endomorphism as a matrix multiplication to see that the group is isomorphic to the group of $n \times n$ matrices, which is generated by multiplying the identity matrix (which would be represented in V^n by the vectors of the elementary basis of V) by all the matrices in $\mathrm{Mat}_n(K)$.

9. Let $x \in V$ then for some i, $T^i = \sum_{j<i} a_j T^j$, for otherwise all the powers of $T(x)$ would be linear independent and hence form an infinite-dimensional basis for V which we said it didn't have. So the polynomial $p(x) = x^i - \sum_{j<i} a_j x^j$ is nonzero and has the feature $p(T)(x) = 0$, so $\{x\}$ is not linear independent so V is not free.

10. Suppose that conditions a and b hold, then by condition a, any $m \in M$ is equal to $\sum_i a_i x_i$, and by b, $f : (a_1, a_2, \ldots a_n) \to \sum_i a_i x_i$ is an isomorphism from R^n to M, so $M = \oplus_i R x_i$. And if it were not the case that $r \to r x_i$ were injective, then there would exist $r, p \in R$ such that $r x_i = p x_i$, so supposing without loss of generality that $i = 1$, we'd have $f(p, a_2, a_3, \ldots a_n) = p x_1 + \sum_{i>1} a_i x_i = r x_1 + \sum_{i>1} a_i x_i = f(r, a_2, a_3, \ldots a_n)$, so f would not be a bijection so not an isomorphism.

    Suppose on the other hand that c holds, then each $m \in M$ is equal to $\sum_i a_i m_i$, and each a_i is uniquely determined by the injectivity of $r \to r x_i$, so the same f is again an isomorphism.

11. ψ is a homomorphism of abelian groups $\leftrightarrow \psi(a + a') = \psi(a) + \psi(a') \forall a, a' \in A \leftrightarrow \psi(a + a + a + \ldots + a) = \psi(a) + \psi(a) + \ldots + \psi(a) \leftrightarrow \psi(na) = n\psi(a) \forall n \in \mathbb{Z} \leftrightarrow \psi$ is a $\mathbb{Z}$-module homomorphism from A to B.

12. Let $rx = (rx_1, rx_2 \ldots)$ for $r \in R, x \in R^\infty$, and let $x + y = (x_1 + y_1, x_2 + y_2, \ldots)$. Then for $x_i, y_i, r, s \in R$, $(rsx_1, rsx_2, \ldots) = r(sx_1, sx_2, \ldots)$;

$(r+s)(x_1, x_2, \ldots) = ((r+s)x_1, (r+s)x_2, \ldots) = (rx_1+sx_1, rs_2+sx_2, \ldots) = (rx_1, rx_2, \ldots)+(sx_1, sx_2, \ldots) = r(x_1, x_2, \ldots) + s(x_1, x_2, \ldots)$;

and $r((x_1, x_2, \ldots)+(y_1, y_2, \ldots)) = r(x_1+y_1, x_2+y_2, \ldots) = (r(x_1+y_1), r(x_2+y_2), \ldots) = (r(x_1, x_2, \ldots)+r(y_1, y_2, \ldots))$, so R^∞ is an R-module. It's free because it has the basis $\{(1, 0, 0, \ldots), (0, 1, 0, 0, \ldots), (0, 0, 1, 0, \ldots), \ldots\}$, which is countably infinite.

2 Homomorphisms and Quotient Modules

1. (a) Let $x \in \ker f, r \in R$, then $\psi(rx) = r\psi(x) = r0 = 0$, and if $y \in f(M)$ with $y = f(x)$ then $ry = rf(x) = f(rx) \in f(M)$ since M is a submodule, so the image and colonel of ψ are submodules.

   (b) Let $a \in M, r \in R, f, g \in \mathrm{Hom}_R(M, N)$, then we showed a long time ago that fg is a homomorphism of abelian groups, and furthermore $fg(ra) = f(g(ra)) = f(rg(a)) = rfg(a)$.

2. (a) For $\psi, \phi \in \mathrm{Hom}_R(M, N), m, n \in M, -\psi(m) = \psi(-m) \in \mathrm{Hom}_R(M, N)$, $(\psi + \phi)(m + n) = (\psi + \phi)(m) + (\psi + \phi)(n) = \psi(m) + \phi(m) + \psi(n) + \phi(n) = (\psi + \phi)(m) + (\psi + \phi)(n)$, and $\psi(x) = 0 \in \mathrm{Hom}_R(M, N)$, so $\mathrm{Hom}_R(M, N)$ is a group.

   (b) Composition is associative and distributive over addition, so it's a valid ring product.

3. Let $m + IM \in M/IM, r + I \in R/I$, then $(r + I)(m + IM) = rm + IM$ defines a module action on M/IM, since it's distributive and associative (and well-defined).

4. For $r \in R, n \in N$, $r\psi^{-1}(n) = \psi^{-1}(rn) \in \psi^{-1}(N)$ since R is a submodule, so ψ carries submodules to submodules and so is a bijection between them, being already a bijection of abelian groups.

5. Let $f(m + N) = \psi(m) + \bar{N}, r \in R$, then f is a group isomorphism and $f(rm + N) = \psi(rm) + \bar{N} = r\psi(m) + \bar{N} = r\psi(m + N)$, so f is a module isomorphism.

6. Let $\tilde{\psi}(m + N) = \psi(m)$, then $\tilde{\psi}(rm + N) = \psi(rm) = r\psi(m) = r\tilde{\psi}(m + N)$, so $\tilde{\psi}$ is a module homomorphism.

7. $\psi(A) \subset \psi(A+N)$ since $0 \in N$, and for $a \in A, n \in N$, $\psi(a+n) = \psi(a)+\psi(n) = \psi(a)+0 = \psi(a) \in \psi(A)$, so $\psi(A+N) \subset \psi(A) \to \psi(A+N) = \psi(A) \to A+N \subset \psi^{-1}(\psi(A))$. And $x \in \psi^{-1}(\psi(A)) \to \psi(x) \in \psi(A) \to \psi(x) = \psi(a) = \psi(a) + 0$ for some $a \in A$, so $x = a + n$ for some $n \in N$. So $\psi^{-1}(\psi(A)) = A + N$, and $a \to \psi(a)$ is a map from A to $\psi(A)$ with colonel $A \cap N$, and $a + n \to \psi(A)$ is a map from $A + N$ to $\psi(A)$ with colonel N.

8. There exists a finite set $S = \{x_1, x_2, \dots x_n\}$ such that $RS = M$, so let $F = \oplus_i Rx_i$, then F is a free R-module, and the map $(r_1x_1, r_2x_2, \dots r_nx_n) \to \sum_i r_ix_i$ is a surjective homomorphism from F to M, and whatever its colonel K is, it's a submodule of F such that $M \cong F/K$.

3 Multilinear Maps and Determinants

1. Let f and g be multilinear maps, then $(f+g)((x_1, x_2, \dots, x, \dots, x_n)+(x_1, x_2, \dots, y, \dots, x_n)) = f((x_1, x_2, \dots, x+y, \dots, x_n))+g((x_1, x_2, \dots, x+y, \dots, x_n)) = f((x_1, x_2, \dots, x, \dots, x_n))+f((x_1, x_2, \dots, y, \dots, x_n))+g((x_1, x_2, \dots, x, \dots, x_n))+g((x_1, x_2, \dots, y, \dots, x_n)) = (f+g)((x_1, x_2, \dots, x, \dots, x_n))+(f+g)((x_1, x_2, \dots, y, \dots, x_n))$, so $f+g$ is multilinear, and $-f$ and 0 are also multilinear, so the multilinear maps are a group, and they're abelian because R is.

2. The definition of multilinearity is independent of the ordering of the groups M_i, so permuting them doesn't change the multilinearity of a function. The action of a permutation on a symmetric multilinear function results in just that same function, so the result is multilinear and symmetric. The action of a permutation on a skew-symmetric multilinear function f returns $\pm f$, both of which are skew-symmetric. Finally, if $x_i = x_j$ for some i, j, then $x_{\sigma(i)} = x_{\sigma(j)}$ for any σ, so if f is alternating then σf is alternating.

3. (a) Subsets of R^n can contain at most n linear independent vectors, so if $S \subset (R^n)^k = \{s_1, s_2, \dots s_k\}$ where $k > n$, then some s_i is a linear combination of the other s_j. Supposing without loss of generality that s_1 is this vector, by Lemma 8.3.10 $f(S) = f(\sum_{j>1} a_j s_j, s_2, \dots s_n) = f(a_2 s_2, s_2, \dots s_n) = a_2 f(s_2, s_2, \dots s_n) = a_2 0 = 0$ for any multilinear alternating map f.

   (b) Formula 8.3.1 for the determinant gives a multilinear nonzero alternating function when $k = n$, and when $k < n$ the same formula applied to k is still alternating and multilinear.

   (c) If they were isomorphic, then a multilinear function on one would be multilinear on the other, but only the ones where $k \leq n$ have multilinear functions.

4. -108, by my calculations.

5. If the kth column and lth column of A are the same, then $\det A_{ij}$ is 0 except when $j = k$ or $j = l$, because otherwise A_{ij} contains both columns k and l and therefore has determinant 0. And the permutation that gets A_{ik} from A_{ij} is the cyclic permutation on columns a_m for $k \leq m \leq l$ (assuming WLG that $l > m$), which has sign $(-1)^{l-k+1}$, so $(-1)^{i+k} \det A_{ik} + (-1)^{i+l} \det A_{il} = (-1)^{l+i+1} \det A_{il} + (-1)^{l+i} \det A_{il} = 0$, and since those are the only nonzero terms in the cofactor expansion, it follows that the cofactor expansion is 0 if two columns of A are the same, so it's alternating.

For multilinearity, let $A_1 = (a_1, a_2, \dots a_k, \dots, a_n), A_2 = (a_1, a_2, \dots a'_k, \dots a_n), A_3 = (a_1, a_2, \dots a_k + a'_k, \dots a_n)$, then $\text{cofactor}(A_3) = \sum_{j \neq k} (-1)^{i+j} a_{ij} \det A_{3_{ij}} + (-1)^{i+k} \det A_{3_{ik}} (a_k + a'_k)$, so for the terms with $j \neq k$, $\det A_{3_{ij}} = \det A_{1_{ij}} + \det A_{2_{ij}}$ since the determinant is multilinear, while $\det A_{3_{ik}} = \det A_{1_{ik}} = \det A_{2_{ik}}$ since the only column that differs among them has been deleted. Taking these facts together, it follows that $\text{cofactor}(A_3) = \text{cofactor}(A_1) + \text{cofactor}(A_2)$, so the cofactor expansion is multilinear.

It is readily calculable that the cofactor expansion of the identity is one, so it is equal to the determinant by the above facts.

6. The determinant is invariant under transpose, so take the transpose of both sides of that equation and apply Exercise 5.

7. $\det(A)^{-1} \det(\tilde{A}_j) = \det(A^{-1} \tilde{A}_j)$, and $A^{-1} \tilde{A}_j$ is the identity matrix except in the jth column, where it is $A^{-1} b$. Taking a cofactor expansion on the jth column of $A^{-1} \tilde{A}_j$, we get $\det(A^{-1} \tilde{A}_j) = (A^{-1} b)_j$.

4 Finitely Generated Modules over a PID, Part 1

Summary: Every matrix A over a PID is row-and-column equivalent to a diagonal matrix where each entry divides the following entries and then some zeroes, so $A = PAQ$ for invertible P and Q, which means that any submodule of a free R-module has a basis $\{d_i v_i\}$, where d_i divides d_j for $i < j$ and the v_i are linear independent over R.

1. (a) Let $V = (v_1, \dots v_n)$, then the kth row of VA is $\sum_i A_{ik} v_i$, and so the kth row of $(VA)B$ is $\sum_i B_{ik} (\sum_j A_{jk} v_j)$, which if you distribute and calculate the coefficients of each v_i you'll find that comes out to $\sum_i (\sum_j A_{ij} B_{jk}) v_i$, whereas $(AB)_{ij} = \sum_l A_{il} B_{lj}$, so the kth row of $V(AB)$ is $\sum_i (\sum_j A_{ij} B_{jk}) v_i$, which is the same.

   (b) Let $B = [v_1, \dots v_n] A_j$, then the jth row of $B = \sum_i A_{ij} v_i$, a linear combination of the linearly independent v_i, so if the jth row of B is 0 then the jth column of A must be 0, and so if B is 0 then A is 0.

2. A submodule of a free R-module of rank 1 is isomorphic to an ideal of R, so it is generated by a single element since R is a PID. So if F is a free R-module of rank n, it has a basis $\{f_1, f_2, \dots f_n\}$, so let $F' = \text{span}(\{f_1, f_2, \dots f_{n-1}\})$. For a submodule N of F, the submodule $N' = N \cap F'$ is generated by at most $n-1$ elements since F' is and that's the induction hypothesis, whereas $N \setminus N'$ is generated by at most 1 element and that's the base case. And so any element $x \in N$ is equal to $x' + \pi_n(x)$, where $\pi_n(x)$ is the coefficient of f_n in the expansion of x and $x' \in N'$, since $x - \pi_n(x) \in N'$, so N is generated by no more than n elements.

3. These are known and attested properties of the Euclidean function, so I'll only be proving them for the new length thing.

   (a) Each irreducible appearing in the factorization of a and each irreducible appearing in the factorization of b appear in the factorization of ab, so $|ab| \geq \max(|a|, |b|)$.

   (b) a is an associate of $b \leftrightarrow a = ub$ for a unit $u \rightarrow$ the prime factorization of a is a unit u_a times a product of irreducibles $\prod_i p_i$ and the prime factorization of b is uu_a times $\prod_i p_i$. Since the product of units uu_a is a unit, $|a| = |b|$ in this case.

   (c) If a does not divide b then at least one of a's divisors p_i does not divide b so p_i cannot be a factor of any common divisor d of a and b so $|d| < |a|$ and by the transitive property of $<$ it follows that $|d| < |b|$.

4. The zero matrix $0 \in R$. If A is row and column finite, so is $-A$ since $-0 = 0$. And $A+B$ has at most as many nonzero entries in each row and column as the sum of how many A has in that row/column and how many B has in that row/column, which will be finite if $A, B \in R$. So R is a group. The diagonal matrix whose diagonal entries are 1 is a member of R, and it is a multiplicative identity. It's not commutative because matrix multiplication isn't commutative. And given $(A, B) \in R \oplus R$, let C be the matrix whose $2i-1$ column is column i of A and $2i$ column is column i of B for $i \in \mathbb{N}$, then the map $(A, B) \rightarrow C$ is an isomorphism $R \oplus R \rightarrow R$ since for $D \in R$ the ith column of DA is DA_i where A_i is the ith column of A, while the jth column of C is DC_j, so the isomorphism respects the ring product in R.

5. $\psi(\sum_i x_i v_i) = \sum_i x_i \psi(v_i) = \sum_i x_i (\sum_j A_{jk} w_k) = [w_1, \ldots w_m] A \begin{pmatrix} x_1 \\ x_2 \\ \ldots \\ x_n \end{pmatrix}$.

6. The columns of $[w_1, \ldots w_m]A$ span range(ψ), and $A = P^{-1}A'Q^{-1}$, so $[w_1, \ldots w_m]A = [w_1, \ldots w_m]P^{-1}A'Q^{-1}$. Let $[w'_1, \ldots w'_n] = [w_1, \ldots w_m]P^{-1}$, then $[w'_1, \ldots w'_n]$ is a basis of W since P^{-1} is invertible, and $[w'_1, \ldots w'_n]A' = [d_1 w'_1, d_2 w'_2, \ldots d_s w'_s, 0, 0, \ldots 0]$, which is a basis for range(ψ) since it has the same span as $[w_1, \ldots w_m]A$ since Q is invertible.

7. I ran the numbers and what came out of it was $P = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & -4 \\ 1 & 0 & 2 \end{pmatrix}$, $A' = \text{diag}(2, -2, -1)$, $Q = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 3 \\ 0 & 0 & 1 & 0 \\ 5 & 3 & 8 & 2 \end{pmatrix}$, and the basis of $\mathbb{Z}^3$ that we want is the columns of P^{-1}, $\begin{pmatrix} 2 & 0 & -1 \\ -6 & 1 & 5 \\ -1 & 0 & 1 \end{pmatrix}$.

8. $\ker A = \ker P^{-1}A'Q^{-1} = \ker A'Q^{-1}$ since P is invertible, so $A'x = 0 \leftrightarrow x_j = 0$ for $1 \leq j \leq s$ since A' is diagonal with s nonzero entries on its diagonal, so we're looking for the vectors x such that $Q^{-1}x = \begin{pmatrix} 0 \\ 0 \\ \dots \\ 0 \\ y_{s+1} \\ y_{s+2} \\ \dots \\ y_n \end{pmatrix}$, which are of course $x = Q \begin{pmatrix} 0 \\ 0 \\ \dots \\ 0 \\ y_{s+1} \\ y_{s+2} \\ \dots \\ y_n \end{pmatrix}$ for all y_i, aka the span of the last $n - s$ columns of Q.

9. I screwed up the arithmetic on this one, but the point is you just find the Smith normal form of A and the span of the last 2 columns of Q is your null space.

10. $[w'_1, \dots w'_s] = [w_1, \dots w_s]D \leftrightarrow [w'_1, \dots w'_s]D^{-1} = [w_1, \dots w_s]$, so the w are a linear combination of the w' as long as D is invertible, so the w' generate the w and hence N.

5 Finitely Generated Modules over a PID, Part 2

Summary: Any finitely generated module $M = \text{span}\{x_1, \dots x_n\}$ over a principal ideal domain R is the sum of cyclic submodules $(\oplus_i R/(d_i)) \oplus R^k$, where the d_i are the diagonal entries from the Smith normal form of $\sum_i r_i f_i \to \sum_i r_i x_i$ where the f_i are the basis of any free R-module of rank n. That's the "invariant factor decomposition". There's also the "primary decomposition", where any finitely generated torsion module with period $m = \prod_i p_i^{m_i}$ is equal to $\oplus_i M[p_i]$, where $M[p_i]$ is the set of elements x with $p_i^k x = 0$ for some k. You can apply the primary decomposition to the summands of the invariant factor decomposition to get the "elementary divisor decomposition".

1. Let $a \in \text{ann}(M), r \in R, m \in M$, then $(ra)m = r(am) = r0 = 0$, so $\text{ann}(M)$ is a ideal of R. $\text{ann}(S) \subset \text{ann}(RS)$ since $1 \in R$, and $\text{ann}(RS) \subset \text{ann}(S)$ since $\text{ann}(RS) = R\text{ann}(S)$ and $\text{ann}(S)$ is an ideal.

2. $M/M_{\text{tor}} = \{a + M_{\text{tor}} : a \in M\}$ so $\exists a, r \in R : ra + M_{\text{tor}} = 0 + M_{\text{tor}} \leftrightarrow ra \in M_{\text{tor}} \leftrightarrow \exists r' \in R : r'ra = 0 \leftrightarrow (r'r)a = 0 \leftrightarrow a \in M_{\text{tor}}$, so M/M_{tor} is torsion free.

3. $B \cap M_{\text{tor}} = \{0\}$ since if $\{b_1, \dots b_n\}$ is a basis for B then any $b \in B$ is equal to $\sum_i r_i b_i$ for $r_i \in R$, and if $rb = 0$ for some $r \in R$ then $r \sum_i r_i b_i = 0 \to \sum_i r r_i b_i = 0 \to r r_i = 0$ for all i since the b_i are linear independent. So B is torsion free and since $M = A + B$ we must have $M_{\text{tor}} \subset A$, and since A is a torsion group it follows that $A = M_{\text{tor}}$.

4. RB is an R-module with a basis B so it's free, and for $a + RB \in M/RB$, if there doesn't exist an $r \in R$ such that $ra + RB = 0 + RB$, then a is linearly independent of the vectors in the basis B, but B is maximal so no such a can exist. So M/RB is a torsion module.

5. If $x \in J$ then $rx \neq 0$ for any $r \in R$ besides 0, since $J \subset R$ and R is an integral domain, so J is torsion free. If $a, b \in J$, then $0 = ab - ba \in RJ$, so any two elements of J are linear independent over R. Because of this linear dependence between distinct elements of J, a linear independent subset of J can contain at most one element, and if this single-element set were a basis of J then J would be a principal ideal, which it's defined not to be, so J is not free.

6. Let $m/n + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$, then $n(m/n) + \mathbb{Z} = m + \mathbb{Z} = 0 + \mathbb{Z}$, so $\mathbb{Q}/\mathbb{Z}$ is a torsion $\mathbb{Z}$-module. Any generating set of $\mathbb{Q}/\mathbb{Z}$ must contain at least $1/p$ for all primes p, since no sum or product of elements without denominator p results in a fraction with denominator p (by the primality of p and the definitions of addition and multiplication in $\mathbb{Q}$). So $\mathbb{Q}/\mathbb{Z}$ is not finitely generated, since there are infinite primes. For any $n \neq 0 \in \mathbb{Z}$, $\frac{1}{2n} + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$, and $n(\frac{1}{2n} + \mathbb{Z}) = \frac{1}{2} + \mathbb{Z} \neq 0 + \mathbb{Z}$, so $\text{ann}(\mathbb{Q}/\mathbb{Z}) = \{0\}$.

7. (a) Suppose p^k divides a, then $a = p^k q$ for some $q \in R$. Then let $f(p^{k-1}x + (a)) = qp^{k-1}x + (a)$, so f is a surjective homomorphism from $p^{k-1}M$ to $qp^{k-1}M$ with colonel p^kM. By the homomorphism theorem, then, $\frac{p^{k-1}M}{p^kM} \cong qp^{k-1}M$. And then $x \to qp^{k-1}x + (a)$ is a surjective homomorphism from R to $qp^{k-1}(R/(a))$ with colonel (p), so $qp^{k-1}M \cong R/(p)$, so by the transitive property of congruence it follows that $\frac{p^{k-1}M}{p^kM} \cong R/(p)$.

   If p^k does not divide a, then $p^k s + at = 1$ for some $s, t \in R$, so for any $p^{k-1}x + (a) \in M, p^{k-1}x + (a) = p^{k-1}(p^k s + at)x + (a) = p^k p^{k-1}sx + (a) \in p^kM$, so $p^{k-1}M \subset p^kM \to \frac{p^{k-1}M}{p^kM} = \{0\}$.

   (b) $\frac{p^{k-1}M}{p^kM} = \frac{p^{k-1}(\oplus_i A_i)}{p^k(\oplus_i A_i)} = \frac{\oplus_i p^{k-1}A_i}{\oplus_i p^k A_i} = \oplus_i(\frac{p^{k-1}A_i}{p^kA_i})$ by Lemma 8.5.1, so since $A_i = R/(a_i)$ the direct summands here are $R/(p)$ when p^k divides a_i and 0 otherwise by part a. Since $X \oplus 0 \cong X$ for any set X, it follows that $\frac{p^{k-1}M}{p^kM} \cong (R/(p))^{m_k(p)}$. Since the set $\frac{p^{k-1}M}{p^kM}$ has no reference to or dependence on the a_i, only on M, it follows that the numbers $m_k(p)$ depend only on M and not on the choice of direct summands A_i.

   (c) If the largest $m_k(p) = 1$, then $s = 1$ and a_1 is the product of $\{p^k : k \text{ is the highest value with } m_k(p) = 1\}$, so s and the a_i are uniquely determined. So suppose that all maximal $m_k(p)$ less than n uniquely identify their s and $\{a_i\}$ up to units. Then let $a_n = \prod\{p^k : k \text{ is the highest value with } m_k(p) = 1\}$ and subtract 1 from all our $m_k(p)$ values and call them $m'_k(p)$, then the highest

$m'_k(p)$ is $n-1$ and any product of $p^k : m'_k(p) \neq 0$ divides a_n, so the induction hypothesis uniquely determines s and the rest of the a_i.

8. M is annihilated by $\prod_i p_i^{m_i}$, so $p_i^{m_i}M$ is annihilated by $\prod_{j\neq i} p_j^{m_j}$, which is not divisible by p_i, so $(p_i^{m_i}M)[p_i] = \{0\}$, so no element of M is annihilated by a higher power of p_i than m_i, so for all $x \in M[p_i], p_i^{m_i}x = 0$.

6 Rational Canonical Form

1. If $h(x) = \sum_i a_i x^i$, then let $g(x,y) = \sum_i a_i \frac{x^i - y^i}{x-y}$, then it is obvious that $(x-y)g(x,y) = h(x) - h(y)$, and it only remains to show that $\frac{x^i-y^i}{x-y} \in K[x]$ for all i. So let $q_0(x) = 1, q_n(x) = \sum_{k=0}^n x^k y^{n-k}$, then $(x-y)q_n(x) = \sum_{k=0}^n x^{k+1}y^{n-k} - \sum_{k=0}^n x^k y^{n-k+1}$ and all the terms in that difference cancel besides $x^{n+1} - y^{n+1}$ so $q_n(x) \in K[x]$ is $\frac{x^{n+1}-y^{n+1}}{x-y}$.

2. Let $v \in V$ have the property $Wv = 0$, where W is the matrix whose ith column is w_i. Let F be the matrix where the ith column is f_i, then $W = F(xE_n - A) \to F(xE_n - A)v = 0$, but $xE_n - A$'s columns are linearly independent since they have polynomials on the diagonal and nowhere else, and the columns of F are linearly independent since the f_i constitute a basis. So $v = 0$, so $\ker W = \{0\}$, so the columns of W, i.e. the w_i, are linearly independent.

3. (a) $V \cong F/\ker\Phi = \oplus_i \frac{K[x]f_i}{K[x]g_i}$, where f_i are the vectors in a basis for F and g_i are the vectors in a basis of $\ker\Phi$. The first $n-s$ summands are $\frac{K[x]y_i}{K[x]y_i} = 0$, so $V = \oplus_{i=n-s}^n \frac{K[x]z_i}{K[x]a_i(x)z_i}$, and $\frac{K[x]z_i}{K[x]a_i(x)z_i} \cong K[x]/(a_i(x))$ by the discussion on page 387, and $K[x]/(a_i(x)) = K[x]/\text{ann}(v_i) \cong K[x]v_i = V_i$. So $V = \oplus_i V_i$.

   (b) The vectors $w_i = T^i(v_j)$ are linear independent because the annihilator of V_j has degree δ_j, and they span V_j since there are δ_j of them. $T(w_i) = w_{i+1}$ for $0 < i < \delta_j - 1$, and $T(w_{j-1}) = T^{\delta_j}(v_j) = a_j(T)(v_j) - \sum_{i=0}^{\delta_j-1} \alpha_i T^i(v_j)$ where α_i are the coefficients of a_j. Since $a_j(T)(v_j) = 0$, the result is simply $-\sum_{i=0}^{\delta_j-1} \alpha_i T^i(v_j)$, so the matrix of $T_{|V_j}$ with respect to this basis is the companion cube of a_j.

4. I got the rotational canonical form to be diag(1, 1, 1, $x-2$), and I was too lazy to do the basis thing. Have your computer do it.

5. $\chi_{SAS^{-1}} = \det(xE - SAS^{-1}) = \det(S(xS^{-1}E - A)S^{-1}) = \det(S)\det(xSES^{-1} - A)\det(S^{-1}) = \det(xE - A)$, so χ_A is a similarity invariant of matrices. So the characteristic polynomial of a linear transformation T is the same without regard to underlying basis, so χ_T is well-defined and a similarity invariant for linear transformations.

6. Taking a cofactor expansion on the first row of an $n \times n$ matrix $xE - A$, the only term that has powers that go as high as $n-1$ is $a_{11} \det A_{11}$, since the matrices A_{1j} for $j \neq 1$ all delete two of the monomials in x, so (inductively) the coefficient of x^{n-1} in the characteristic polynomial of A is the same as the coefficient of x^{n-1} in $\prod_i (x - a_{ii})$, which is $-\sum_i a_{ii}$, so the trace is a similarity invariant.

7. λ is a root of $\chi_A \leftrightarrow \det(\lambda E - A) = 0 \leftrightarrow \exists v \in R^n : (\lambda E - A)v = 0 \leftrightarrow \lambda E v = Av \leftrightarrow Av = \lambda v$.

   v is an eigenvector of $T \leftrightarrow Tv = \lambda v \in Kv$ for some $\lambda \in K$.

8. $\bar{T}(v + v' + V_0) = T(v + v') + V_0 = T(v) + T(v') + V_0 = \bar{T}(v + V_0) + \bar{T}(v' + V_0)$, so $\bar{T}$ is a linear operator on V/V_0. $V \cong V/V_0 \oplus V_0$, so $(v_1, \ldots v_n)$ is a basis of V. Since V_0 is invariant under T, $T(v_i) \in \text{span}(v_1, \ldots v_k)$ for $1 \leq i \leq k$, so the first k columns of the matrix of T with respect to $(v_1, \ldots v_n)$ terminate in $n-k$ zeros, and the particular linear combination of the first k vectors that gives $T(v_i)$ is given by multiplication by A_1, so the first block column of our matrix has the indicated form. Similarly the jth column of A_2 gives the projection of $T(v_j)$ onto the span of the last $n-k$ vectors for $k < j < n$, except we don't have that this space is invariant so $T(v_j)$ could have arbitrary components in the first k vectors as well, which is where B comes in.

9. If v is an eigenvector of T then $K[x]v$ is a T-invariant subspace of V. If $n = 1$, all matrices are upper triangular, so the matrix of T is upper triangular with respect to any basis. So if all linear transformations with splitting characteristic polynomials on R^k are upper-triangularizable for $k < n$, and we want to upper-triangularize a transformation T on R^n where χ_T splits, then we let λ be some root of χ_T, so that λ is an eigenvalue of T with eigenvector v, and let $V_0 = K[x]v$, then applying the previous exercise, we get a basis with respect to which the matrix of T has the form $\begin{pmatrix} \lambda & B \\ 0 & A_2 \end{pmatrix}$, and so by the induction hypothesis the restriction of T to the last $n-1$ vectors in that basis is upper-triangularizable, so T is upper-triangularizable.

10. The determinant of an upper-triangular matrix is the product of its diagonal entries, so $\chi_A = \prod_i (x - \lambda_i)$.

11. Let $v = \sum_{l=1}^{k} a_l v_l$, then $(T - \lambda_k)v = Tv - \lambda_k v = \sum_{l=1}^{k} a_l T(v_l) - \sum_{l=1}^{k} a_l \lambda_k v_l$. Since $T(v_k) = \lambda_k v_k$, this difference reduces to $\sum_{l=1}^{k-1} a_l T(v_l) - \sum_{l=1}^{k-1} a_l \lambda_k v_l \in V_{k-1}$ because A' is upper triangular so $T(v_j)_k = 0$ for $j < k$, and the v_i are linear independent so no sum of them that doesn't involve v_k adds up to something that does. So the foregoing covers both the base case and the induction step for the claim $\prod_{i=k}^{n} (T - \lambda_i)$ maps V into V_{k-1} for all $1 \leq k \leq n$, i.e. the whole claim. In particular, $\prod_{i=1}^{n} (T - \lambda_i)$ maps V into $\{0\}$, but $\prod_{i=1}^{n} (T - \lambda_i) = \chi_T$, so it follows that $\chi_T(T) = 0$.

7 Jordan Canonical Form

1. I got $J_3(5) \oplus J_1(2)$ and $S = \begin{pmatrix} 1 & -1/10 & 51/100 & 0 \\ -3 & 3/10 & -53/100 & -1 \\ 0 & 0 & 1 & 0 \\ 10 & 0 & 0 & 4 \end{pmatrix}$.

2. Ditto.

3. Let D be a diagonal matrix, then $A \sim D \leftrightarrow = SAS^{-1}$ for some $S \leftrightarrow$ the columns of S form a basis with respect to which A is diagonal $\leftrightarrow As_i = D_{ii}s_i$ for s_i a column of $S \leftrightarrow s_i$ is an eigenvector of A with eigenvalue D_{ii}.

4. a $\leftrightarrow$ b by the uniqueness of the Jordan canonical form since diagonal matrices are in Jordan canonical form and A is similar to its Jordan canonical form. b $\leftrightarrow$ c because if A has a root λ of dimension $d > 1$ then the Jordan block corresponding to that eigenvalue would be $J_d(\lambda)$ which is not diagonal, whereas $J_1(\lambda)$ is diagonal. c $\leftrightarrow$ d because the minimal polynomial is the product of the elementary divisors.

5. Let J be the Jordan form of A, then $A = SJS^{-1}$ for some matrix S, and $J = D + M$ where D is the diagonal matrix of eigenvalues of A and M is 0 except at entries M_{i+1i}, i.e. the diagonal below the main diagonal, which is 0 or 1. Any matrix with the form of M is nilpotent because the first row of all such M is 0 and if the first j rows of M are 0 then the first $j+1$ rows of M^2 are 0, since row $j+1$ of M^2 can only be equal to row j * 1 or row j times 0, both of which are 0. If M is nilpotent, then SMS^{-1} is nilpotent, since $(SMS^{-1})^2 = SMS^{-1}SMS^{-1} = SM^2S^{-1}$ and so forth. So $A = SJS^{-1} = S(D+M)S^{-1} = SDS^{-1} + SMS^{-1} = A_0 + N$ where A_0 is diagonalizable and N is nilpotent. For the commutativity relation $A_0N = NA_0$, it suffices to show when A is a Jordan block, so that $A_0 = \lambda E$ so $A_0N = \lambda EN = N\lambda E = NA_0$, since the general case involves only several distinct Jordan-block products.

6. (a) If λ is an eigenvalue of N then there exists a vector v such that $Nv = \lambda v \leftrightarrow N^kv = \lambda^k v$ for all $k \in \mathbb{N}$, but there exists an $m \in \mathbb{N}$ such that $N^m = 0$, so $N^m v = 0v = \lambda^k v$ so $\lambda = 0$, so all the eigenvalues of N are 0 so all the roots of the characteristic polynomial of N are 0 so the polynomial is x^n.

   (b) As shown above, all the eigenvalues of N are 0, so all the Jordan blocks of the Jordan form of N are $J_m(0)$.

   (c) Trace is a similarity invariant, N is similar to its Jordan form, and the diagonal of the Jordan form of N is all zeros, so the trace of N is 0.

   (d) The Jordan form of N as described in b is in rational canonical form, so by uniqueness of the rational canonical form it follows that the Jordan canonical form is the rational canonical form.

7. They are all similar to the matrix M whose elements are all zero besides M_{ij} where $j = i + 1$ and those M_{ij} can be 0 or can be 1; all choices of 1s and 0s for this sub-diagonal correspond to possible nilpotent matrices.

8. (a) The characteristic polynomial of S is $1-x^n = (x-1)(x-\xi)(x-\xi^2)\cdots(x-\xi^{n-1})$, so since the characteristic polynomial is a similarity invariant $S \sim D$.

   (b) Yes.

9. (a) The vector of ten ones is an eigenvector of A with eigenvalue 10, and since the trace of A is 10 and none of the eigenvalues of A can be negative since all its entries are positive, it follows that the Jordan form of A is the zero matrix but for one diagonal entry which is 10. Nine linear independent eigenvectors of eigenvalue 0 are given by the vectors with a 1 in position 1, zeros in eight of the nine remaining positions, and a -1 in the last remaining position.

   (b) $A^2 = 0$ if the characteristic of K is 2 or 5, so A is nilpotent. The rational canonical form of A has one 1 in the diagonal below the main diagonal and zeros elsewhere. A basis with respect to which A has this form is $[1, 0, 0, \ldots 0]$, $[1, 1, 1, \ldots 1]$, $[1, 1, 0, 0, \ldots 0]$, $[1, 0, 1, 0, 0, \ldots 0]$, and six other vectors with a 1 in the first position and one other position and 0s elsewhere in $\mathbb{Z}_2$. In $\mathbb{Z}_5$, the Jordan form is the same and the basis is the same except in the last eight vectors replace the 1 that's not in the first position with a 4.

10. (a) This is equal to the matrix from number 9 plus $3E$, so it has the same eigenvectors as that matrix with eigenvalues equal to $\lambda + 3$, where λ is the eigenvalue found in 9. So the basis with respect to which it's in canonical form is the same, and the eigenvalues are $\lambda + 3$.

    (b) Under the same basis as in 9b, we get the Jordan canonical form, but the eigenvalues on the diagonal are now 1 mod 2 and 3 mod 5.