Linear Algebra

June 2001
Final Exam
Ali Nesin

1. *Find all isomorphism types of abelian groups of order* 90 *and* 2001.

Since $90 = 2 \times 3^2 \times 5$, an abelian group G of order 90 is the direct sum of G_2, G_3 and G_5 where $G_p = \{g \in G : o(g) = p^k \text{ for some } k\}$ is the p-primary part of G. Since $|G_2| = 2$, $G_2 \approx \mathbb{Z}/2\mathbb{Z}$. Similarly $G_5 \approx \mathbb{Z}/5\mathbb{Z}$. But there are two possibilities for G_3: Either $G_3 \approx \mathbb{Z}/9\mathbb{Z}$ or $G_3 \approx \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Thus either

$$G \approx \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \approx \mathbb{Z}/90\mathbb{Z} \text{ or } G \approx \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \approx \mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

2. *Let V be a vector space. Let $\varphi \in \mathrm{GL}_K(V)$ have finite order n.*

2a. *What can you say about the eigenvalues of* φ?

Let λ be an eigenvalue for φ. Then there is a nonzero vector $v \in V$ such that $\varphi(v) = \lambda v$ and $v = \varphi^n(v) = \lambda^n v$. Since $v \neq 0$, this implies that $\lambda^n = 1$. Therefore all the eigenvalues of φ are nth roots of unity.

2b. *Should such a φ have to have eigenvalues*?

No. Take $K = \mathbb{R}$, $V = \mathbb{R}^2$ and φ to be a rotation of $\pi/2$ radians (90 degrees). Then $\varphi^4 = 1$ and φ has no eigenvalues.

3. *Let V be a vector space over a field K of characteristic $p > 0$. Let $\varphi \in \mathrm{End}_K(V)$.*

3a. *Show that* $(\varphi - 1)^{p^k} = \varphi^{p^k} - 1$.

Proceeding by induction on k (taking pth power k times) it is enough to show for $k = 1$. We just compute in the ring $\mathrm{End}_K(V)$: $(\varphi - 1)^p = \sum_{i=0}^{p} \binom{p}{i} (-1)^i \varphi^{p-i} = \varphi^p - 1$ since p divides $\binom{p}{i}$ if $i \neq 0, p$ and $\mathrm{char}(K) = p$.

3b. *Conclude that if φ has order p^k for some $k > 0$, then a nonzero vector of V is fixed by* φ.

Let r be the smallest natural number such that $(\varphi - 1)^{r+1} = 0$. Then $(\varphi - 1)^r \neq 0$ and there is a nonzero vector $v \in V$ such that $(\varphi - 1)^r(v) \neq 0$. If $w = (\varphi - 1)^r(v)$, then $\varphi(w) = w$.

4. *Let $V \neq 0$ be a finite dimensional vector space over an algebraically closed field K and let $A \leq \mathrm{GL}_K(V)$ be an abelian group. Show that the elements of A have a common nonzero eigenvector.*

We proceed by induction on $\dim(V)$. If $\dim(V) = 1$ this is clear. If all the elements of A act as scalars, we are done also. Assume otherwise. Let $a \in A$ be nonscalar. Since K is algebraically closed, a has an eigenvalue λ. Let V_λ be the λ-eigenspace of a, i.e. $V_\lambda = \{v \in V : a(v) = \lambda v\}$. Since A is abelian, for $b \in A$ and $v \in V_\lambda$, $ab(v) = ba(v) = b(\lambda v) = \lambda b(v)$. This shows that $A(V_\lambda) = V_\lambda$. Since a is nonscalar, $V_\lambda < V$ so that we can apply the induction hypothesis to V_λ. This shows that A (or the image of A in $\mathrm{GL}_K(V_\lambda)$) has a common nonzero eigenvector in V_λ, hence in V.

5. *Let K be a field and $f \in K[X]$ a polynomial.*

5a. *What is the necessary and sufficient condition on f for $K[X]/\langle f\rangle$ to be a pid?*

Any ideal of $K[X]/\langle f\rangle$ is the quotient of an ideal I of $K[X]$ containing f, therefore any ideal of $K[X]/\langle f\rangle$ is principle. But this is not enough to make $K[X]/\langle f\rangle$ a pid (principle ideal **domain**). Further, $K[X]/\langle f\rangle$ should have no nonzero zerodivisors. This means that either $f = 0$ or is irreducible.

5b. *And in that case what are the invertible elements of the ring $K[X]/\langle f\rangle$?*

If $f = 0$, then the invertible elements are just the constants. If f is irreducible, then $K[X]/\langle f\rangle$ is a field and all its nonzero elements are invertible.

6. Let R be a ring and M and N left R-modules.

6a. *Is* $\mathrm{Hom}_R(M, N)$ *naturally an R-module?*

No, not always. In general, one needs R to be commutative for this because if $r \in R$ and $f \in \mathrm{Hom}_R(M, N)$, for rf to be in $\mathrm{Hom}_R(M, N)$, one needs in particular $rsf(m) = r(f(sm)) = (rf)(sm) = s((rf)(m)) = srf(m)$ for all $s \in R$ and $m \in M$, i.e. $(rs - sr)f(M) = 0$ for all $s \in R$. If R is not commutative, this may not be the case.

6b. *Show that* $\mathrm{End}_R(M)$ *is a (not necessarily commutative) ring with identity* Id_M.

$\mathrm{End}_R(M)$ is a ring under addition and composition of maps as one can show easily.

6c. *What is the necessary and sufficient condition for the submodule* $R\mathrm{Id}_M$ *of* $\mathrm{End}_R(M)$ *to be* ***naturally*** *isomorphic to R?*

(Note that here we view R as a left-module over itself). The map $r \mapsto r\mathrm{Id}_M$ is an R-module surjection. This map is one-to-one iff $rM \neq 0$ for any $r \in R \setminus \{0\}$, i.e. if $\mathrm{ann}_R(M) = 0$.

7. Let R be a ring and M a left R-module generated by one element.

7a. *Show that $M \approx R/I$ (as left R-modules) for some left ideal I of R.*

Let $m \in M$ be a generator. Then the map $r \mapsto rm$ is a surjective left module homomorphism from R into M. If I is the kernel of this homomorphism ($I = \mathrm{ann}_R(m)$), $R/I \approx M$.

7b. *Show that M is irreducible*[1] *iff I is a maximal left ideal of R.*

Clear from above.

8. **(Schur's Lemma)** *Let R be a ring and M and N be two irreducible left R-modules.*

8a. *Show that any homomorphism $\varphi : M \to N$ is either 0 or an isomorphism.*

Assume $\varphi \neq 0$. Then since $\varphi(M) \leq N$ and $\mathrm{Ker}(\varphi) \leq M$ and since M and N are irreducible modules, $\varphi(M) = N$ and $\mathrm{Ker}(\varphi) = 0$, i.e. φ is an isomorphism.

8b. *Show that* $\mathrm{End}_R(M)$ *is a division ring.*

Clear from above.

9. *Assume V is a vector space of finite dimension over a field K. Let $A \in \mathrm{End}_K(V)$.*

9a. *Show that the subring $K[A]$ of* $\mathrm{End}_K(V)$ *generated by A and the scalar multiplications* $\lambda\mathrm{Id}_V$ *(for $\lambda \in K$) is isomorphic to $K[X]/\langle f\rangle$ for some polynomial $f \in K[X]$.*

Clearly $K[A] = \{\lambda_0 + \lambda_1 A + ... + \lambda_k A^k : k \in \mathbf{N}, \lambda_0, ..., \lambda_k \in K\}$, i.e. $K[A]$ is the image of the evaluation map (which is a ring homomorphism from $K[X]$ into $\mathrm{End}_K(V)$) that evaluates X at A. Thus if $\langle f\rangle$ is the kernel of this homomorphism, then $K[A] \approx K[X]/\langle f\rangle$. Note also that this is

[1] A module is called **irreducible** if its only submodules are 0 and itself.

also a vector isomorphism and that f is a polynomial of minimum degree such that $f(A) = 0$. Since K is a field, one can take f to be monic.

9b. *Can you bound the degree of f in terms of* $\dim_K(V)$?

Yes: $\deg(f) = \dim_K(K[X]/\langle f\rangle) = \dim_K K[A] \le \dim_K(\mathrm{End}_K(V)) = \dim_K(V)^2$.

9b. *Find f when*

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

$$K = \mathbf{F}_7 \text{ and } A = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$$

In the first case $f(X) = (X - 1)^2$. In the second case the answer depends on a. If $a = 1$ then $f(X) = X - 1$. If $a \neq 1$, then $f(X) = (X - 1)(X - a)$.

10. *Consider $\mathbb{Z} \times \mathbb{Z}$ as a group (i.e. as a* **Z***-module). For $A \in$* $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z} \times \mathbb{Z})$ *consider the subring $\mathbb{Z}[A]$ of* $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z} \times \mathbb{Z})$ *generated by A.*

10a. *Find the number of minimal generators of $\mathbb{Z}[A]$ as a $\mathbb{Z}$-module when*

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

As in number 9, $\mathbb{Z}[A] \approx \mathbb{Z}[X]/I$ where $I = \{f \in \mathbb{Z}[X] : f(A) = 0\}$. But this time, we cannot say right away that I is generated by some polynomial since $\mathbb{Z}[X]$ is not a pid. (However $\mathbb{Z}[X]$ is a Noetherian ring by Hilbert's Basis Theorem from Basic Algebra, but we do not really need this result, and I is generated by finitely many polynomials). We will work with $\mathbb{Z}[X]/I$ rather that with $\mathbb{Z}[A]$. Note that

$$\mathrm{Id} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

$$A^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

Thus no nonzero polynomial of degree ≤ 1 is in I and $a + bX + cX^2 \in A$ iff $a + b + c = b + 2c = 0$ iff $b = -2a = -2c$. Taking $a = 1$, we see that $1 - 2X + X^2 \in I$. This shows that $I = \langle 1 - 2X + X^2\rangle$ because this polynomial is monic and the division algorithm still works in $\mathbb{Z}[X]$. Thus the $\mathbb{Z}$-module $\mathbb{Z}[A]$ is generated by 1 and A.

10b. *Find the invertible and nilpotent elements of $\mathbb{Z}[A]$ and its idempotents*[2].

Change variables. Set $Y = X - 1$. Then $\mathbb{Z}[X]/\langle 1 - 2X + X^2\rangle = \mathbb{Z}[Y]/Y^2$. Compute in this latter ring. Let y be the image of Y in $\mathbb{Z}[Y]/Y^2$. An element of $\mathbb{Z}[Y]/Y^2$ can be uniquely written as $a + by$. Since $(a + by)^n = a^n + naby$, the element $a + by$ is nilpotent iff $a = 0$. Therefore only the elements of the form by are nilpotent and these correspond to the elements $b(x - 1)$ of $\mathbb{Z}[X]/\langle 1 - 2X + X^2\rangle$, i.e. to the elements $b(A - 1)$ of $\mathbb{Z}[A]$. Taking $n = 2$, we see that $a + by$ is

[2] An element r of a ring is nilpotent if $r^n = 0$ for some n and it is idempotent if $r^2 = r$.

idempotent iff $a^2 = a$ and $2ab = b$, which gives two pairs of solutions: $a = b = 0$ and $a = 1$, $b = 0$. Therefore the only idempotents of this ring are 0 and 1.

11. *Let G be a group and K a field. In this and the next exercise, it is advised to write G multiplicatively. Consider the formal elements of the form*

$$\sum_{g\in G}\lambda_g g$$

where $\lambda_g \in K$ *and only finitely many of them are nonzero. Let* $K[G]$ *be the set of such elements.* (This is the direct sum of $|G|$ copies of *K and G is a basis*).

11a. *Find the elements of* $\mathbf{F}_2[\mathbb{Z}/3\mathbb{Z}]$.

Write $\mathbb{Z}/3\mathbb{Z} = \{1, x, x^2\}$ (multiplicatively!). Then easily $\mathbf{F}_2[\mathbb{Z}/3\mathbb{Z}] = \mathbf{F}_2[X]/\langle X^3-1\rangle$.

Define +, × *and scalar multiplication formally on* $K[G]$ *as follows*:

$$\left(\sum_{g\in G}\lambda_g g\right)+\left(\sum_{g\in G}\mu_g g\right)=\sum_{g\in G}(\mu_g+\lambda_g)g$$

$$\left(\sum_{g\in G}\lambda_g g\right)\times\left(\sum_{g\in G}\mu_g g\right)=\sum_{g\in G}\left(\sum_{hk=g}\mu_h\lambda_k\right)g$$

$$\lambda\left(\sum_{g\in G}\lambda_g g\right)=\sum_{g\in G}\lambda\lambda_g g$$

Then $K[G]$ *becomes a* (*not necessarily commutative*) *ring with* 1 *and also a K-vector space satisfying* $\lambda(ab) = (\lambda a)b = a(\lambda b)$ (*such a structure is called an* **algebra** *or a* ***K*-algebra**, *e.g.* $\mathrm{End}_K(V)$ *is a K-algebra*).

11b. *Show that* $G \le K[G]^*$.

Imbed G in $K[G]$ by sending $h \in G$ to $\sum_g \delta_{g,h} g \in K[G]$ where $\delta_{g,h}$ is the Kronecker symbol. Ignoring the zeroes, this map sends in fact an element h of G to the element h of $K[G]$. Clearly this imbedding is a homomorphism of G into $K[G]^*$. In fact the inverse of the element $h \in K[G]$ is h^{-1}.

11c. *Find the invertible and the nilpotent elements and the idempotents of* $\mathbf{F}_2[\mathbf{Z}/3\mathbf{Z}]$.

Compute in $\mathbf{F}_2[X]/\langle X^3-1\rangle$. We know from 11b that 1, x and x^2 are invertible.

the element	its square	
0	0	
1	1	
x	x^2	invertible
$x + 1$	$x^2 + 1$	
x^2	x	invertible
$x^2 + 1$	$x + 1$	
$x^2 + x$	$x^2 + x$	idempotent
$x^2 + x + 1$	$x^2 + x + 1$	idempotent

We still have to decide the nilpotency of $x + 1$ and (of its square) $x^2 + 1$. But $(x + 1)^3 = x^2 + x$ which an idempotent and so cannot be nilpotent.

11d. *If G is finite what is* $\left(\sum_{g\in G} g\right)^2$?

If α is this element, an easy computation shows that $\alpha^2 = |G|\alpha$. Let us check it:

$\alpha^2 = \left(\sum_{g\in G} g\right)^2 = \left(\sum_{g\in G} g\right)\left(\sum_{g\in G} g\right) = \left(\sum_{g\in G} g\right)\left(\sum_{h\in G} h\right) = \sum_{g\in G}\left(g\sum_{h\in G} h\right) = \sum_{g\in G}\sum_{h\in G} gh = \sum_{g\in G}\alpha = |G|\alpha$.

11e. *Show that if G has torsion elements, then* $K[G]$ *has zero-divisors.*

If $g \in G$ has order n then $(1 - g)(1 + g + ... + g^{n-1}) = 0$.

11f. *Show that* $K[\mathbf{Z}]$ *is has no zero-divisors.*

If x is the generator of $\mathbb{Z}$, any element of $K[\mathbb{Z}]$ can be written as a linear combination of x^n for $n \in \mathbb{Z}$. The multiplication is like in the polynomial ring.

11g. *Show that the set of elements of the form* $\sum_{g\in G}\lambda_g g$ where $\sum_{g\in G}\lambda_g = 0$ *forms an ideal of* $K[G]$.

The set of such elements is closed under addition and multiplication by some eleemnt $g \in G$. Therefore it is an ideal.

11h. *Let G be a group, K a field and* $\varphi : G \to \mathrm{GL}(V) \subseteq \mathrm{End}_K(V)$ *a group homomorphism. Show that* φ *extends uniquely to a K-algebra homomorphism* $\underline{\varphi} : K[G] \to \mathrm{End}_K(V)$.

Clear... Just send an element $\sum_{g\in G}\lambda_g g$ of $K[G]$ to the element $\sum_{g\in G}\lambda_g \varphi(g)$ of $\mathrm{End}_K[G]$ (there is no possible answer!). In fact any group homomorphism $\varphi : G \to H$ extends uniquely to a K-algebra homomorphism from $K[G]$ into $K[H]$.

11i. *Note that, defining av as* $\varphi(a)(v)$ *for* $a \in K[G]$ *and* $v \in G$, *V becomes a* $K[G]$*-module via* $\underline{\varphi}$.

Clear

12. *The purpose of this exercise is to prove* ***Maschke's Theorem*** *that states the following: Let G be a finite group, K a field whose characteristic does not divide* $|G|$ *and V a* $K[G]$*-module. Then V is completely reducible, i.e. any submodule of V has a complement in V.*

12a. *Show that a vector space endomorphism u of V is a* $K[G]$*-module endomorphism iff* $u(gv) = gu(v)$ *for all* $g \in G$ *and* $v \in V$.

Clear!

12b. *Let W be a* $K[G]$*-submodule of V. Let U be a complement of W in V (as a vector space over K). Thus* $V = W \oplus U$. *Let* π *be the projection of V onto W according to this decomposition. Let* $u : V \to V$ *be defined by* $u(v) = \sum_{g\in G} g\pi g^{-1}v$. *Show that* $u(V) \le W$, *that u is a* $K[G]$*-module homomorphism, that in case G is finite* $u_{|W} = |G|\,\mathrm{Id}_W$ *and that* $u \circ u = |G|\, u$.

Since $\pi(V) \le W$ and W is a $K[G]$-module, it is clear that $u(V) \le W$.

To show that u is a $K[G]$-module homomorphism, it is enough to show that $u(hv) = hu(v)$ for all $h \in G$ and $v \in V$. Let us check: $u(hv) = \sum_{g\in G} g\pi g^{-1}hv = \sum_{g\in G} hh^{-1}g\pi g^{-1}hv = h\sum_{g\in G} h^{-1}g\pi g^{-1}hv = h\sum_{g\in G}(h^{-1}g)\pi(h^{-1}g)^{-1}v = hu(v)$.

For $w \in W$, since $\pi g^{-1}w = g^{-1}w$ (because $g^{-1}w \in W$), it is clear that $u_{|W} = |G|\,\mathrm{Id}_W$.

12c. *Assume now that G is finite and that* $\mathrm{char}(K)$ *does not divide* $|G|$. *Let* $\rho = \frac{1}{|G|}u$. *Show that* $V = W \oplus \mathrm{Ker}(\rho)$. (*Now* $\mathrm{Ker}(\rho)$ *is a* $K[G]$*-module.*)

By the second question of 12b, ρ is a G-module homomorphism from V into W. By the third qyestion of 12b, $\rho(V) = W$. By the last question of 12b, $\rho \circ \rho = \rho$. Thus $v - \rho(v) \in \mathrm{Ker}(\rho)$ for any $v \in V$. Since $v = \rho(v) + (v - \rho(v))$, we get $V = \rho(V) + \mathrm{Ker}(\rho) = W + \mathrm{Ker}(\rho)$. If $w \in \rho(V) \cap \mathrm{Ker}(\rho)$, then $w = \rho(v)$ for some $v \in V$ and so $w = \rho(v) = \rho^2(v) = \rho(\rho(v)) = \rho(w) = 0$ and we have $V = W \oplus \mathrm{Ker}(\rho)$.

12d. Show that if further $\dim_K(V) < \infty$ then V is a direct sum of irreducible modules. (5 pts.)

If V is irreducible we are done. Otherwise, let $U \neq 0$, V be a submodule of V. By 12c, $V = U \oplus W$ for some submodules W of V. By induction on the dimension, U W are direct sum of irreducible submodules.