

LINEAR ALGEBRA AND MATRICES REVIEW

(1) Let F be a field and $A \in \text{Mat}_{m \times n}(F)$.

(a) Explain why the columns of A generate $\text{im}(t_A)$.

$$\begin{aligned} \text{Write } A &= [a_1 \cdots a_n]. \text{ Then } \text{im}(t_A) = \{Av \mid v \in F^n\} \\ &= \{v_1 a_1 + \cdots + v_n a_n \mid v_1, \dots, v_n \in F\} = F\{a_1, \dots, a_n\}. \end{aligned}$$

(b) The **rank** of A is $\dim(\text{im}(t_A))$. Explain why $\text{rank}(A)$ is the maximal number of linearly independent columns of A .

Let $r = \text{rank}(A)$. Since $S = \{a_1, \dots, a_n\}$ spans $\text{im}(t_A)$, there is a subset $B \subseteq S$ that is a basis for $\text{im}(t_A)$, and by definition, $|B| = r$. In particular, there are r linearly independent columns of A . There can't be $t > r$ linearly independent columns of A , since such a set would be contained in a basis B' for $\text{im}(t_A)$, and we would have $|B'| \geq t > r$, contradicting that every basis has the same size.

(c) Show that the following are equivalent:

- (i) $\text{rank}(A) = m$;
- (ii) t_A is surjective;
- (iii) There is some $B \in \text{Mat}_{n \times m}(F)$ such that $AB = I_m$.

(i) \Leftrightarrow (ii): Since $\text{im}(t_A)$ is a subspace of F^m , we have $\text{im}(t_A) = F^m$ if and only if $\dim(\text{im}(t_A)) = \dim(F^m)$. Since the left-hand side is $\text{rank}(A)$ and the right-hand side is m , we are done.

(iii) \Rightarrow (ii): Let $v \in F^n$. Then $v = (AB)v = A(Bv) = t_A(Bv)$, so t_A is surjective.
 (ii) \Rightarrow (iii): Since t_A is surjective, we can write $e_i = t_A(w_i)$ for some $w_i \in F^n$, where e_i is the i th standard basis vector in F^m . By the UMP for free modules, there is a linear transformation $\phi : F^m \rightarrow F^n$ such that $\phi(e_i) = w_i$ for all i ; let B be the matrix of this transformation (i.e., $B = [w_1 \cdots w_m]$). We claim that $t_A t_B$ is the identity. Again by the UMP for free modules, it suffices to check that $t_A t_B(e_i) = e_i$ for all i , and this follows from the computations above. Thus $t_A t_B = t_A t_B = \text{id} = t_{I_m}$, so $AB = I_m$.

(d) Show that the following are equivalent:

- (i) $\text{rank}(A) = n$;
- (ii) t_A is injective;
- (iii) There is some $B \in \text{Mat}_{n \times m}(F)$ such that $BA = I_n$.

(i) \Leftrightarrow (ii): Note that t_A is injective if and only if $\dim(\ker(t_A)) = 0$. By Rank-Nullity the left-hand side is $n - \text{rank}(A)$, and we are done.

(iii) \Rightarrow (ii): Let $v \in \ker(t_A)$, so $Av = 0$. Then $v = BAv = B0 = 0$. Thus, t_A is injective.

(ii) \Rightarrow (iii): Since t_A is surjective, the vectors $v_i = t_A(e_i)$ for $i = 1, \dots, n$ are linearly independent in F^m . Extend this set to a basis v_1, \dots, v_m of F^m . By the UMP for free modules, we can take a linear transformation $\phi : F^m \rightarrow F^n$ such

that $\phi(v_i) = e_i$ for $i = 1, \dots, n$. Let B be the matrix of ϕ . Then $t_B t_A(e_i) = e_i$ for all i , so $BA = I_n$ by a similar argument to the above.

(e) Suppose that $m = n$. List a bunch of things that are equivalent.

- A is invertible
- t_A is injective
- t_A is surjective
- There is some B such that $BA = I_n$.
- There is some B such that $AB = I_m$.

(2) Let R be a commutative ring and $A \in \text{Mat}_{m \times n}(R)$.

(a) If P is an invertible $m \times m$ matrix and Q is an invertible $n \times n$ matrix,

- (i) Explain why $\ker(t_A) = \ker(t_{PA})$.
 - (ii) Give a formula for $\ker(t_{AQ})$ in terms of $\ker(t_A)$ and t_Q or $t_{Q^{-1}}$.
 - (iii) Explain why $\ker(t_A) \cong \ker(t_{AQ})$.
- (i) If $v \in \ker(t_A)$, then $Av = 0$ and then $PAv = P0 = 0$ so $v \in \ker(t_{PA})$. Conversely, if $v \in \ker(t_{PA})$, then $PAv = 0$ and then $Av = P^{-1}PAv = 0$, so $v \in \ker(t_A)$.
- (ii) We claim that $\ker(t_{AQ}) = t_{Q^{-1}}(\ker(t_A))$. Indeed, if $v \in \ker(t_{AQ})$, then $AQv = 0$, so $Qv \in \ker(t_A)$, and hence $t_{Q^{-1}}(v) \in \ker(t_A)$. The reverse containment is similar.
- (iii) The maps $t_{Q^{-1}}$ and t_Q give mutually inverse isomorphisms from $\ker(t_A)$ to $\ker(t_{AQ})$.

(b) What are the analogous statements for $\text{im}(t_A)$?

- (i) $\text{im}(t_A) = \text{im}(t_{AQ})$.
- (ii) $\text{im}(t_{PA}) = t_P(\text{im}(t_A))$.
- (iii) $\text{im}(t_{PA}) \cong \text{im}(t_A)$.

The proofs are similar to those for the kernels.

(c) What do (a) and (b) say about elementary operations?

EROs preserve the kernel and ECOs preserve the image.

(d) When R is a field, what does (c) say about rank?

EROs and ECOs preserve the rank.

(3) Let R be a commutative ring. Let $\mathcal{P} = \{p_1, \dots, p_m\}$ be a basis for R^m and $\mathcal{Q} = \{q_1, \dots, q_n\}$ be a basis for R^n . For $A \in \text{Mat}_{m \times n}(R)$, find an explicit formula for $[t_A]_{\mathcal{Q}}^{\mathcal{P}}$ in terms of A and the matrices $P = [p_1 \cdots p_m]$ and $Q = [q_1 \cdots q_n]$.

$$[t_A]_{\mathcal{Q}}^{\mathcal{P}} = P^{-1}AQ.$$

One way to see this is by using change of basis matrices: writing std_n for the standard basis of R^n and likewise for R^m , we have $[\text{id}_{R^m}]_{\mathcal{P}}^{\text{std}_m} = P$ and $[\text{id}_{R^n}]_{\mathcal{Q}}^{\text{std}_n} = Q$. Thus

$$[t_A]_{\mathcal{Q}}^{\mathcal{P}} = [\text{id}]_{\text{std}_m}^{\mathcal{P}} [t_A]_{\text{std}_n}^{\text{std}_m} [\text{id}]_{\mathcal{Q}}^{\text{std}_n} = P^{-1}AQ.$$

Alternatively, we can check the definition: the j th column of $[t_A]_{\mathcal{Q}}^{\mathcal{P}}$ is the \mathcal{P} -coordinate vector of $t_A(q_j)$. Then $v = t_A(q_j)$ is the j th column of AQ . If $v = a_1p_1 + \dots + a_mp_m$, then $v = P(a_1, \dots, a_m)$, so $(a_1, \dots, a_m) = P^{-1}v$. Thus, the j th column of $[t_A]_{\mathcal{Q}}^{\mathcal{P}}$ is the j th column of $P^{-1}AQ$.

MODULES AND PRESENTATIONS REVIEW

(1) Let R be a ring, M an R -module, and $N \subseteq M$ be a submodule.

(a) Show that if M can be generated by a elements, then M/N can be generated by a elements.

Suppose that $M = R\{m_1, \dots, m_a\}$. We claim that $\{m_1 + N, \dots, m_a + N\}$ generates M/N . Indeed, $m + N \in M/N$. Then $m = \sum r_i m_i$ for some $r_i \in R$, so $m + N = \sum r_i(m_i + N)$.

(b) Show that if N can be generated by b elements and M/N can be generated by c elements, then M can be generated by $b + c$ elements.

Let n_1, \dots, n_b generate N and $m_1 + N, \dots, m_c + N$ generate M/N . We claim that $n_1, \dots, n_b, m_1, \dots, m_c$ generate M . Indeed, if $m \in M$, we can write $m + N = r_1(m_1 + N) + \dots + r_c(m_c + N)$, so $n := m - (r_1m_1 + \dots + r_cm_c) \in N$. Then we can write $n = s_1n_1 + \dots + s_bn_b$, so $m = r_1m_1 + \dots + r_cm_c + s_1n_1 + \dots + s_bn_b$. This shows the claim.

(2) Let R be a ring and M be an R -module.

(a) Show that M is finitely generated if and only if there is a surjective R -module homomorphism $\pi : R^m \rightarrow M$ for some m .

First, suppose that M is finitely generated and write $M = R\{m_1, \dots, m_a\}$. Consider the homomorphism $\pi : R^a \rightarrow M$ mapping $\pi(e_i) = m_i$. Then since $\{m_1, \dots, m_a\} \subseteq \text{im}(\pi)$, we must have $\text{im}(\pi) = M$, so π is surjective.

Now suppose that we have such a surjection π . Then $M \cong R^m/K$ for some K the First Isomorphism Theorem, so by (1a), M is finitely generated.

(b) The set of **relations** on a (finite) set of elements $a_1, \dots, a_m \in M$ is

$$\text{Rel}(a_1, \dots, a_m) = \{(r_1, \dots, r_m) \in R^m \mid r_1a_1 + \dots + r_ma_m = 0\}.$$

Express $\text{Rel}(a_1, \dots, a_m)$ as the kernel of a homomorphism. Deduce that the set of relations is a module.

Consider the homomorphism from $R^m \rightarrow M$ mapping $e_i \mapsto m_i$. Then $\text{Rel}(a_1, \dots, a_m)$ is the kernel of this homomorphism. Thus, it is a submodule.

- (c) We say that a module M is **finitely presented** if there exists a finite generating set $\{a_1, \dots, a_m\}$ for M such that $\text{Rel}(a_1, \dots, a_m)$ is also finitely generated. Show that M is finitely presented if and only if there is a homomorphism of finite rank free modules $\alpha : R^n \rightarrow R^m$ such that $M \cong R^m/\text{im}(\alpha)$.

Suppose that M is finitely presented, and take a finite generating set $\{a_1, \dots, a_m\}$ for M such that $\text{Rel}(a_1, \dots, a_m)$ is also finitely generated. Let $\{v_1, \dots, v_n\}$ be a generating set for $\text{Rel}(a_1, \dots, a_m)$. Define $\alpha : R^n \rightarrow R^m$ such that $\alpha(e_i) = v_i$. Then the image of α is $\text{Rel}(a_1, \dots, a_m)$ by an argument similar to (2a). As in (2a), we have a surjective homomorphism $\pi : R^m \rightarrow M$ mapping $e_i \mapsto a_i$, and as in (2b) the kernel is $\text{Rel}(a_1, \dots, a_m)$. Using the First Isomorphism Theorem, $M \cong R^m/\ker(\pi) = R^m/\text{Rel}(a_1, \dots, a_m) = R^m/\text{im}(\alpha)$.

Conversely, suppose that $M \cong R^m/\text{im}(\alpha)$ for some $\alpha : R^n \rightarrow R^m$. By (2a), M is finitely generated, namely by the images of e_i in the quotient $R^m/\text{im}(\alpha)$. We claim that $\text{Rel}(a_1, \dots, a_m) = \text{im}(\alpha)$. Indeed, this is just a special case of what we showed in (2b). Finally, we note that $\text{im}(\alpha)$ is generated by $\alpha(e_1), \dots, \alpha(e_n)$.

- (d) Suppose that R is commutative. Show that M is finitely presented if and only if there is some matrix A such that $M \cong R^m/\text{im}(t_A)$.

This follows from (2c), since any α is t_A for some matrix.

- (3) Let R be a commutative ring, and $D \in \text{Mat}_{m \times n}(R)$ be a diagonal matrix (meaning $d_{ij} = 0$ for $i \neq j$) with nonzero diagonal entries d_{11}, \dots, d_{rr} . Prove that the module presented by D is isomorphic to

$$R/(d_{11}) \oplus R/(d_{22}) \oplus \cdots \oplus R/(d_{rr}) \oplus R^{m-r}.$$

This solution is embargoed.