Algebra 1

Homework 4 — Monday, 14/09/2026

Lilian — Prof. Upendra

Homework

Submit: 2 (one of the four proofs, in your own words), 5 (only the computation), 6(c), 7(a), 11(a) and (c). Most are computational: justify all computations. A computer may verify row reduction; setting up and interpreting must be your own.

Problem 2: Towards invariance of dimension

Show that if S is a finite spanning set in a vector space V, then for any linearly independent set I, the cardinality of I is at most the cardinality of S. Give four proofs, the first two by contradiction. (For the HW, submit one.)

(a) Assume $|I| > |S|$. Express the vectors in I as linear combinations of vectors in S. Express these equations using a wide matrix A by defining a new notion of multiplying a matrix of numbers by a row of abstract vectors. Show appropriate associativity for this new operation and use the fact that $A\mathbf{x} = \mathbf{0}$ has a nontrivial solution for a wide matrix A.

(b) Assume $|I| > |S|$ and again express the vectors in I as linear combinations of vectors in S. This is a tall system of equations. Imitate row operations on this tall system to get the last equation as $0 =$ some linear combination of vectors in I. Why must the RHS of this equation be a nontrivial combination?

(c) Proof by reduction to $\mathbb{R}^n$. One way is to use the notion of isomorphism, the fact that having a finite basis for V gives an isomorphism of V with $\mathbb{R}^n$.

(d) Look up the statement of the Steinitz exchange lemma. Try to prove it on your own. Uncover the proof one line at a time and repeat.

Proof.

I'll do (a). Let $S = \{\mathbf{s}_1, \ldots, \mathbf{s}_n\}$. If I is infinite, we can just take $n+1$ vectors from it, which are still independent. So suppose $I = \{\mathbf{u}_1, \ldots, \mathbf{u}_m\}$ with $m > n$.

Since S spans V, we can write

$$\mathbf{u}_j = \sum_{i=1}^{n} a_{ij}\mathbf{s}_i$$

for each j. Let $A = \left(a_{ij}\right)$, which is $n \times m$, so wide. We define a row of vectors times a matrix the same way as for numbers, i.e. $(\mathbf{s}_1, \ldots, \mathbf{s}_n)A$ is the row whose jth entry is $\sum_i a_{ij}\mathbf{s}_i$. Then the above says

$$(\mathbf{u}_1, \ldots, \mathbf{u}_m) = (\mathbf{s}_1, \ldots, \mathbf{s}_n)A.$$

This is associative, in the sense that for $\mathbf{x} \in \mathbb{R}^m$,

$$((\mathbf{s}_1, \ldots, \mathbf{s}_n)A)\mathbf{x} = \sum_j x_j \sum_i a_{ij}\mathbf{s}_i$$
$$= \sum_i \left(\sum_j a_{ij} x_j \right) \mathbf{s}_i = (\mathbf{s}_1, \ldots, \mathbf{s}_n)(A\mathbf{x})$$

by rearranging the (finite) sum.

Now since A is wide, $A\mathbf{x} = \mathbf{0}$ has a non-trivial solution (a REF of A has at most n pivots, so there is a free variable). For this $\mathbf{x}$,

$$\sum_j x_j \mathbf{u}_j = ((\mathbf{s}_1, \ldots, \mathbf{s}_n)A)\mathbf{x}$$
$$= (\mathbf{s}_1, \ldots, \mathbf{s}_n)(A\mathbf{x}) = \mathbf{0},$$

which is a non-trivial linear combination of the $\mathbf{u}_j$ equal to $\mathbf{0}$. But I is independent, a contradiction. Thus $|I| \leq |S|$.

Problem 5 (computation)

Let $A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 5 & 6 & 0 \end{pmatrix}$. Show that A is invertible, write A as a product of elementary matrices and find the inverse of A.

Proof.

We row reduce $(A \mid I)$:

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 1 & 4 & 0 & 1 & 0 \\ 5 & 6 & 0 & 0 & 0 & 1 \end{array}\right) \xrightarrow{R_3 - 5R_1} \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 1 & 4 & 0 & 1 & 0 \\ 0 & -4 & -15 & -5 & 0 & 1 \end{array}\right)$$

$$\xrightarrow{R_3 + 4R_2} \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 1 & 4 & 0 & 1 & 0 \\ 0 & 0 & 1 & -5 & 4 & 1 \end{array}\right) \xrightarrow{R_2 - 4R_3} \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 1 & 0 & 20 & -15 & -4 \\ 0 & 0 & 1 & -5 & 4 & 1 \end{array}\right)$$

$$\xrightarrow{R_1 - 3R_3} \left(\begin{array}{ccc|ccc} 1 & 2 & 0 & 16 & -12 & -3 \\ 0 & 1 & 0 & 20 & -15 & -4 \\ 0 & 0 & 1 & -5 & 4 & 1 \end{array}\right) \xrightarrow{R_1 - 2R_2} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -24 & 18 & 5 \\ 0 & 1 & 0 & 20 & -15 & -4 \\ 0 & 0 & 1 & -5 & 4 & 1 \end{array}\right)$$

Since $\mathrm{RREF}(A) = I$, A is invertible, and

$$A^{-1} = \begin{pmatrix} -24 & 18 & 5 \\ 20 & -15 & -4 \\ -5 & 4 & 1 \end{pmatrix}.$$

The row operations above are given by the elementary matrices

$$E_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -5 & 0 & 1 \end{pmatrix}, \quad E_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 4 & 1 \end{pmatrix}, \quad E_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -4 \\ 0 & 0 & 1 \end{pmatrix},$$

$$E_4 = \begin{pmatrix} 1 & 0 & -3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad E_5 = \begin{pmatrix} 1 & -2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

so $E_5 E_4 E_3 E_2 E_1 A = I$, and thus

$$A = E_1^{-1} E_2^{-1} E_3^{-1} E_4^{-1} E_5^{-1},$$

where E_i^{-1} is E_i with the sign of the off-diagonal entry flipped, i.e. the elementary matrices for $R_3 + 5R_1$, $R_3 - 4R_2$, $R_2 + 4R_3$, $R_1 + 3R_3$ and $R_1 + 2R_2$.

Problem 6(c)

Let $A = \begin{pmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix}$. Show that A has infinitely many right inverses. Find them all. Now give a matrix B having infinitely many right inverses and find them all.

Proof.

Note that $AR = I$ for a 3×2 matrix R iff its columns $\mathbf{r}_1, \mathbf{r}_2$ satisfy $A\mathbf{r}_1 = \mathbf{e}_1$ and $A\mathbf{r}_2 = \mathbf{e}_2$. Row reducing both at once,

$$\left(\begin{array}{ccc|cc} 2 & 3 & 1 & 1 & 0 \\ 1 & 2 & 3 & 0 & 1 \end{array}\right) \xrightarrow{R_1 \leftrightarrow R_2} \left(\begin{array}{ccc|cc} 1 & 2 & 3 & 0 & 1 \\ 2 & 3 & 1 & 1 & 0 \end{array}\right) \xrightarrow{R_2 - 2R_1} \left(\begin{array}{ccc|cc} 1 & 2 & 3 & 0 & 1 \\ 0 & -1 & -5 & 1 & -2 \end{array}\right)$$

$$\xrightarrow{-R_2} \left(\begin{array}{ccc|cc} 1 & 2 & 3 & 0 & 1 \\ 0 & 1 & 5 & -1 & 2 \end{array}\right) \xrightarrow{R_1 - 2R_2} \left(\begin{array}{ccc|cc} 1 & 0 & -7 & 2 & -3 \\ 0 & 1 & 5 & -1 & 2 \end{array}\right)$$

So x_3 is free in both, and the solutions are

$$\mathbf{r}_1 = \begin{pmatrix} 2 + 7s \\ -1 - 5s \\ s \end{pmatrix}, \quad \mathbf{r}_2 = \begin{pmatrix} -3 + 7t \\ 2 - 5t \\ t \end{pmatrix}$$

for $s, t \in \mathbb{R}$. Thus the right inverses of A are

$$R = \begin{pmatrix} 2 + 7s & -3 + 7t \\ -1 - 5s & 2 - 5t \\ s & t \end{pmatrix}, \quad s, t \in \mathbb{R},$$

and there are infinitely many of them.

For B, take $B = \begin{pmatrix} 1 & 1 \end{pmatrix}$. Its right inverses are $\begin{pmatrix} a \\ b \end{pmatrix}$ with $a + b = 1$, i.e. $\begin{pmatrix} t \\ 1-t \end{pmatrix}$ for $t \in \mathbb{R}$.

Problem 7(a)

Let $\mathbf{v}_1 = (1,2,1)^T$, $\mathbf{v}_2 = (0,1,2)^T$, $\mathbf{v}_3 = (2,0,1)^T$. Show that $B = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ is a basis of $\mathbb{R}^3$. What is the change of basis matrix P when the old basis is the standard basis and the new basis is B? Find $\mathbf{w}$ such that $[\mathbf{w}]_B = (4,5,5)^T$. Find $[\mathbf{v}]_B$ for $\mathbf{v} = (4,5,5)^T$.

(Recall: the i-th column of P is the coordinate vector of the i-th new basis vector in terms of the old basis, $B' = BP$, and $[\mathbf{v}]_B = P[\mathbf{v}]_{B'}$.)

Proof.

Let P be the matrix with columns $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$. Row reducing,

$$P = \begin{pmatrix} 1 & 0 & 2 \\ 2 & 1 & 0 \\ 1 & 2 & 1 \end{pmatrix} \xrightarrow{R_2-2R_1, R_3-R_1} \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & -4 \\ 0 & 2 & -1 \end{pmatrix} \xrightarrow{R_3-2R_2} \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & -4 \\ 0 & 0 & 7 \end{pmatrix}$$

which has a pivot in every row and column, so the columns are independent and span $\mathbb{R}^3$, i.e. B is a basis.

P is also the change of basis matrix, since its ith column is $\mathbf{v}_i$ written in the standard basis.

Then $\mathbf{w} = P[\mathbf{w}]_B$, so

$$\mathbf{w} = 4\mathbf{v}_1 + 5\mathbf{v}_2 + 5\mathbf{v}_3 = \begin{pmatrix} 14 \\ 13 \\ 19 \end{pmatrix}.$$

For $[\mathbf{v}]_B$, we solve $P\mathbf{y} = \mathbf{v}$:

$$\left(\begin{array}{ccc|c} 1 & 0 & 2 & 4 \\ 2 & 1 & 0 & 5 \\ 1 & 2 & 1 & 5 \end{array}\right) \xrightarrow{R_2-2R_1, R_3-R_1} \left(\begin{array}{ccc|c} 1 & 0 & 2 & 4 \\ 0 & 1 & -4 & -3 \\ 0 & 2 & -1 & 1 \end{array}\right) \xrightarrow{R_3-2R_2} \left(\begin{array}{ccc|c} 1 & 0 & 2 & 4 \\ 0 & 1 & -4 & -3 \\ 0 & 0 & 7 & 7 \end{array}\right)$$

which gives $y_3 = 1$, $y_2 = 1$ and $y_1 = 2$, so $[\mathbf{v}]_B = (2,1,1)^T$.

Problem 11(a)

Write a formula, with justification, for the linear function $f : \mathbb{R}^2 \to \mathbb{R}^2$ that takes $(1, 2)^T$ to $(3, 4)^T$ and $(2, 5)^T$ to $(10, 13)^T$.

Proof.

Let $C = \begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix}$. C is invertible, with $C^{-1} = \begin{pmatrix} 5 & -2 \\ -2 & 1 \end{pmatrix}$, so $(1, 2)^T$ and $(2, 5)^T$ form a basis, and f is determined by where it sends them. If $f(\mathbf{x}) = M\mathbf{x}$, then

$$MC = \begin{pmatrix} 3 & 10 \\ 4 & 13 \end{pmatrix},$$

so

$$M = \begin{pmatrix} 3 & 10 \\ 4 & 13 \end{pmatrix}\begin{pmatrix} 5 & -2 \\ -2 & 1 \end{pmatrix} = \begin{pmatrix} -5 & 4 \\ -6 & 5 \end{pmatrix},$$

i.e. $f(x, y) = (-5x + 4y, -6x + 5y)$.

Problem 11(c)

Write a formula, with justification, for reflection in the line $y = kx$ for a real number k. Do this in two ways: first, directly working with the standard basis. Second, start with a more convenient basis and then change it to the standard basis. Maybe it helps to name an angle?

Proof.

Let $\mathbf{d} = (1, k)^T$, which spans the line, and $\mathbf{m} = (-k, 1)^T$, which is perpendicular to it. The reflection T fixes $\mathbf{d}$ and sends $\mathbf{m}$ to $-\mathbf{m}$.

First, directly. Writing $\mathbf{v}$ as its projection onto the line plus the rest, T flips the rest, so

$$T(\mathbf{v}) = 2\frac{\mathbf{v}\cdot\mathbf{d}}{\mathbf{d}\cdot\mathbf{d}}\mathbf{d} - \mathbf{v} = \frac{2(\mathbf{v}\cdot\mathbf{d})}{1+k^2}\begin{pmatrix}1\\k\end{pmatrix} - \mathbf{v}.$$

Plugging in $\mathbf{e}_1$ and $\mathbf{e}_2$,

$$T(\mathbf{e}_1) = \frac{1}{1+k^2}\begin{pmatrix}1-k^2\\2k\end{pmatrix}, \quad T(\mathbf{e}_2) = \frac{1}{1+k^2}\begin{pmatrix}2k\\k^2-1\end{pmatrix},$$

so

$$[T] = \frac{1}{1+k^2}\begin{pmatrix}1-k^2 & 2k\\2k & k^2-1\end{pmatrix}.$$

Second, in the basis $B' = \{\mathbf{d}, \mathbf{m}\}$, T is just $D = \begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}$. The change of basis matrix is $P = \begin{pmatrix}1 & -k\\k & 1\end{pmatrix}$, with $P^{-1} = \frac{1}{1+k^2}\begin{pmatrix}1 & k\\-k & 1\end{pmatrix}$, so

$$\begin{aligned}[T] = PDP^{-1} &= \frac{1}{1+k^2}\begin{pmatrix}1 & k\\k & -1\end{pmatrix}\begin{pmatrix}1 & k\\-k & 1\end{pmatrix}\\ &= \frac{1}{1+k^2}\begin{pmatrix}1-k^2 & 2k\\2k & k^2-1\end{pmatrix}.\end{aligned}$$

If θ is the angle the line makes with the x-axis, then $k = \tan\theta$, and this is

$$[T] = \begin{pmatrix}\cos 2\theta & \sin 2\theta\\\sin 2\theta & -\cos 2\theta\end{pmatrix}.$$

Rest of Tutorial 4

Not part of the homework.

Problem 1: Basic language

Recall the definition of an abstract vector space. Many terms seen in $\mathbb{R}^n$ carry over: subspace, linear combination, span, linear (in)dependence, basis, dimension. Prove the basic observations made in class about span, linear dependence/independence and equivalent ways to think of a basis. Let S be a multiset (repetitions allowed) of vectors in V.

(a) If $\mathbf{v} \in S$ and $\mathbf{v}$ is a linear combination of the other vectors in S, then $\text{span}(S) = \text{span}(S - \{\mathbf{v}\})$. Converse?

(b) If S is independent and $\mathbf{v} \notin \text{span}(S)$, then $S \cup \{\mathbf{v}\}$ is independent. Converse?

Let f be a linear map from V to W. State if (c) and (d) are true or false. If false, is there a condition on f under which the statement becomes true?

(c) "If S is linearly independent, then $f(S)$ is linearly independent." Converse?

(d) "If S spans V then $f(S)$ spans W." Converse?

(e) Show that the following are equivalent for a subset B of V: (1) B is a linearly independent spanning set, i.e. a basis; (2) B is a maximal linearly independent set; (3) B is a minimal spanning set; (4) each vector in V is a unique linear combination of elements of B.

Proof.

Problem 3: Payoff

Deduce several consequences of problem 2 for a finite dimensional vector space.

(a) Invariance of dimension. (We proved that any finite basis of $\mathbb{R}^n$ has exactly n elements. What if there is an infinite basis? Can you answer this objection?)

(b) Growing strategy to get a basis: any linearly independent set can be enlarged to a basis. Note a variation stated in Artin: "If I is linearly independent in V and S spans V, then one can add vectors from S to I to build a basis of V." Compare the two proofs. Does one give a stronger statement than the other?

(c) The dimension of a proper subspace W of V is always less than the dimension of V.

Proof.

Problem 4: Algebra of linear maps and matrix operations

Imagine you do not know any operations involving matrices, not even matrix-vector multiplication. But you have defined abstract vector spaces and proved the existence of a basis. Fixing a basis gives a dictionary between V of dimension n and $\mathbb{R}^n$ via the coordinate map. Recall also our commutative square where a linear map $f : V \to W$ is "translated into a matrix" using a basis for V and one for W.

(a) Show that function application $f(\mathbf{v})$ translates into matrix-vector multiplication, so you can define matrix-vector multiplication this way.

(b) Show how composition of two linear maps translates into multiplication of matrices, so you can define matrix multiplication this way. Deduce associativity of matrix multiplication.

(c) Given vector spaces V and W, let $L(V, W)$ be the set of all linear maps from V to W. Show how to make $L(V, W)$ a vector space and show that it is isomorphic to the vector space of matrices of a certain size. (Hint: choose bases.) Under your isomorphism, which linear map corresponds to the matrix unit E_{ij}?

Proof.

Problem 5 (theory)

Let A be any square matrix. Show that the following are equivalent:

(a) A is invertible, i.e. there exists A' with $AA' = A'A = I$. (b) $f(\mathbf{x}) = A\mathbf{x}$ is a bijection. (c) A has a left inverse L, i.e. $LA = I$. (d) A has a right inverse R, i.e. $AR = I$. (e) $\text{RREF}(A) = I$. (f) A is a product of elementary matrices.

Proof.

Problem 6(a), (b), (d): Faux generality?

Let A be an $r \times c$ matrix; I denotes the identity matrix of whatever size makes the equation make sense. The problems may become more transparent if you think in terms of the associated linear map.

(a) Call A "invertible" if it has a left inverse L and a right inverse R. Show that then $L = R$, and this common inverse is unique.

(b) Suppose A has a two-sided inverse A' ($AA' = I$ and $A'A = I$), necessarily $c \times r$. Show that then $r = c$.

(d) Characterize non-square matrices that have a left inverse. Show that such a matrix must have infinitely many left inverses. Give an explicit numerical example illustrating both statements. Do the same for right inverses. (Also look at Artin's problem M.8 in chapter 1.)

Proof.

Problem 7(b)–(d): Change of coordinates

(b) Consider $p(t) = 1 + 2t + t^2$ on $t \in [0, 1]$. Find its coordinate vector $[p]_B$ with respect to the Bernstein basis $B = \{b_0, b_1, b_2\}$, where $b_0(t) = (1-t)^2$, $b_1(t) = 2t(1-t)$, $b_2(t) = t^2$. (Search "Bernstein polynomials" or "Bézier curves".)

(c) In the general situation (old basis B, new basis B', change of basis matrix P), justify why P must be invertible.

(d) Two alternative ways to prove the change of basis formulas without hypervector notation: (i) read off a formula from the equations expressing B' in terms of B; (ii) operationalize the commutative square for the identity map from V to V.

Proof.

Problem 8: Universal property of a basis

(a) Suppose $B \subset V$. Show that if B is a basis of V, then for any vector space W, any function from the set B to W extends uniquely to a linear map $L : V \to W$. (Show that the forced formula actually defines a linear function.)

(b) (Optional) Show that the property in (a) characterizes those subsets of V that are bases. Do you find the verbiage in the formulation worthwhile?

Proof.

Problem 9: A "vector space" without a basis? (not part of the course)

Suppose only integers $\mathbb{Z}$ are allowed as scalars in the definition of a vector space.

(a) Let $V = \mathbb{Q}$ under ordinary operations. See that all axioms hold. Show that V cannot have a basis for a rather easy reason. What fails?

(b) What happens if $V = \mathbb{R}$? $V = \mathbb{Z}^2$?

Proof.

Problem 10: Other perspectives on rank-nullity

(a) Our proof of abstract rank-nullity: "extend a basis of the kernel of f". Find a proof that directly uses a given basis of the image of f.

(b) We proved rank-nullity earlier for $f(\mathbf{x}) = A\mathbf{x}$ from $\mathbb{R}^c$ to $\mathbb{R}^r$ by counting pivots and free variables in $\mathrm{REF}(A)$. Prove the general abstract theorem by reducing to that case via the commutative square.

(c) Using the bases from our proof in class, write a simple matrix for f. Recall Tutorial 3 problem 9 (row and column operations, reduced form), row/column operations as matrix multiplication, and the change of basis formula $Q^{-1}AP$. Meld these into a unified understanding.

Proof.

Problem 11(b), (d)

(b) Counterclockwise rotation by angle θ.

(d) Composition of two maps from parts (b) and (c). There are three possibilities to work out. Afterwards, see problem B2 from the 2025 CMI entrance exam and its posted solution. Which solution do you prefer?

Proof.

Problem 12: Determinants

(a) Prove (and fix in your mind) the usual formula for the inverse of a 2×2 matrix A when $\det(A)$ is an invertible scalar. (Artin does the $n \times n$ version in section 1.6; his cofactor matrix is our $\operatorname{adj}(A)$. Not in syllabus.)

(b) Artin section 1.4: do 1, 2, 4 in your head (1(d) should be instantaneous). The matrix in 3 is the Cartan matrix of type A.

(c) Artin chapter 1, Miscellaneous problem 7.

Proof.