Definition of a group

State the definition of a group.

A group is a set G together with a binary operation composed with : G x G -> G satisfying:

Closure:	$g_1 \circ g_2 \in G \quad \forall\, g_1, g_2 \in G$
Associativity:	$(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3) \quad \forall\, g_1, g_2, g_3$
Identity:	$\exists\, e \in G : \; e \circ g = g \circ e = g \quad \forall\, g \in G$
Inverse:	$\exists\, g^{-1} \in G : \; g \circ g^{-1} = g^{-1} \circ g = e \quad \forall\, g \in G$

Left identity and left inverse

Let (M, *) be a group with right identity e (a*e = a) and right inverse a^-1 (a*a^-1 = e). Show that the right identity is also a left identity and the right inverse is also a left inverse.

Step 1 — Left inverse: a^-1 * a = e

Let b = a^-1. Then b has its own right inverse b^-1 with b * b^-1 = e.

$$b \cdot a = (b \cdot a) \cdot e = (b \cdot a)(b \cdot b^{-1}) = b \cdot (a \cdot b) \cdot b^{-1} = b \cdot e \cdot b^{-1} = b \cdot b^{-1} = e$$

Step 2 — Left identity: e * a = a

Using the left inverse result above:

$$e \cdot a = (a \cdot a^{-1}) \cdot a = a \cdot (a^{-1} \cdot a) = a \cdot e = a$$

Uniqueness of the inverse

Let (M, *) be a group. Show that the inverse element a^-1 of a in M is unique.

Proof: assume a second inverse c exists and derive that c = a^-1.

Suppose c in M also satisfies a * c = e.

Then: $c = e \cdot c = (a^{-1} \cdot a) \cdot c = a^{-1} \cdot (a \cdot c) = a^{-1} \cdot e = a^{-1}$

Therefore c = a^-1, so the inverse is unique. ■

Which sets form a group?

Which of the following sets forms a group under matrix multiplication? Prove or disprove.

(a) $G_1 = \{A \in \mathbb{R}^{n \times n} \mid \det(A) \neq 0,\ A^\top = A\}$

Not a group.

Closure fails: (AB)^T = B^T A^T = BA which is not AB in general — product may not be symmetric.

(b) $G_2 = \{A \in \mathbb{R}^{n \times n} \mid \det(A) = -1\}$

Not a group.

No identity: det(I)=1 not equal to -1. Closure fails: det(AB)=(-1)(-1)=1, not in G2.

(c) $G_3 = \{A \in \mathbb{R}^{n \times n} \mid \det(A) > 0\}$

Group — subgroup of GL(n).

Identity: det(I)=1>0. Closure: det(AB)=det(A)det(B)>0. Inverse: det(A^-1)=1/det(A)>0.

Groups from the lecture

Which groups were mentioned in the lecture? Write down names and correct inclusions.

GL(n)	General Linear Group: $\{A \in \mathbb{R}^{n \times n} \mid \det(A) \neq 0\}$
SL(n)	Special Linear Group: $\{A \in GL(n) \mid \det(A) = 1\}$
O(n)	Orthogonal Group: $\{R \mid R^\top R = I\}$, $\det(R) = \pm 1$
SO(n)	Special Orthogonal Group: $\{R \in O(n) \mid \det(R) = +1\}$ — 3D rotations
A(n)	Affine Group: $L(x) = Ax + b$, $A \in GL(n)$
E(n)	Euclidean Group: $L(x) = Rx + T$, $R \in O(n)$
SE(n)	Special Euclidean Group: $R \in SO(n)$ — rigid-body motions

Inclusion relations:

$$SO(n) \subset O(n) \subset GL(n) \qquad SO(n) \subset SL(n) \subset GL(n) \qquad SE(n) \subset E(n) \subset A(n) \subset GL(n+1)$$

Definition of a vector space

State the definition of a vector space V over a field K. Does V have to satisfy the group properties? What additional properties does V have?

Definition:

- $(V, +)$ is a commutative (abelian) group (closure, assoc., identity 0, inverse -v)
- Scalar multiplication $\cdot : \mathbb{K} \times V \to V$ satisfying:
- $1 \cdot v = v$
- $\alpha(\beta v) = (\alpha\beta)v$ (compatibility)
- $(\alpha + \beta)v = \alpha v + \beta v$ (distributive over scalar addition)
- $\alpha(v + w) = \alpha v + \alpha w$ (distributive over vector addition)

Yes — (V,+) must be a group. Additional structure: scalar multiplication with its axioms.

Linear independence, span, basis

Let V be a vector space over K. State the definition of:

Linear independence of v1, ..., vk in V

$v_1, \ldots, v_k$ are linearly independent if:

$$\sum_{i=1}^{k} \alpha_i v_i = 0 \Rightarrow \alpha_i = 0 \; \forall \, i$$

Span of a set M subset V

All finite linear combinations of elements of M:

$$\text{span}(M) = \{ \sum_{i=1}^{k} \alpha_i v_i \mid v_i \in M, \; \alpha_i \in \mathbb{K} \}$$

Basis of a subspace U subset V

A linearly independent subset $B \subset V$ such that $\text{span}(B) = U$.

Checking linear independence & basis

Show (without using the determinant) for each set whether it is (1) linearly independent, (2) spans R^3, and (3) forms a basis of R^3.

(a) M1 = { (1,1,1)^T , (0,1,1)^T , (0,0,1)^T }

Linear independence:

From $\alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3 = 0$: 1st comp. $\Rightarrow \alpha_1 = 0$, 2nd $\Rightarrow \alpha_2 = 0$, 3rd $\Rightarrow \alpha_3 = 0$. Independent. ✓

Spanning R^3:

Any $x = (x_1, x_2, x_3)^\top = x_1(v_1 - v_2) + (x_2 - x_1)v_2 + (x_3 - x_2)v_3$. Spans $\mathbb{R}^3$. ✓

M1 is a basis of R^3. (check)

(b) M2 = { (2,1,0)^T , (1,1,0)^T }

Linear independence: (check)

$2\alpha_1 + \alpha_2 = 0$ and $\alpha_1 + \alpha_2 = 0$ give $\alpha_1 = \alpha_2 = 0$. ✓

Does NOT span R^3: (X)

Both vectors have zero 3rd component — cannot represent (0,0,1)^T.

M2 is NOT a basis of R^3.

Definition of an inner product

A Hilbert space H is a (finite-dimensional) vector space over K endowed with an inner product. State the definition of an inner product.

An inner product is a map <*, *> : H x H -> K satisfying:

Symmetry:	$\langle u, w\rangle = \langle w, u\rangle$
Linearity:	$\langle v, \alpha u\rangle = \alpha\langle v, u\rangle$ and $\langle v, u + w\rangle = \langle v, u\rangle + \langle v, w\rangle$
Positive def.:	$v \neq 0 \Rightarrow \langle v, v\rangle > 0$

The inner product induces a norm |v| = sqrt(<v,v>) and a metric d(v,w) = |v-w|, making H a Hilbert space.

Hilbert spaces

Do the following form Hilbert spaces with the given inner product?

(a) $\mathbb{R}^n$ $\quad \langle x, y \rangle = x^\top y$ **YES — Hilbert space**

- Symmetry: $x^\top y = \sum_i x_i y_i = y^\top x$ ✓
- Linearity: straightforward ✓
- Pos. def.: $x^\top x = \sum_i x_i^2 > 0$ for $x \neq 0$ ✓

(b) $\mathbb{R}^{n \times m}$ $\quad \langle A, B \rangle = \mathrm{tr}(A^\top B)$ **YES — Hilbert space**

- Write $A = [a_1, \ldots, a_m]$. Then $\mathrm{tr}(A^\top B) = \sum_k a_k^\top b_k$ = sum of standard inner products.
- All three properties follow from (a). ✓

Frobenius norm from inner product

Show that the Frobenius norm ||A||_F = sqrt(sum_ij a_ij^2) for A in R^(n x m) is the norm induced by the inner product <A,B> = tr(A^T B).

We show that sqrt(<A,A>) = ||A||_F.

$$\sqrt{\langle A, A\rangle} = \sqrt{\operatorname{tr}(A^\top A)} = \|A\|_F$$

$$\langle A, A\rangle = \operatorname{tr}(A^\top A)$$ — by definition of the inner product

$$= \sum_{k=1}^{m} a_k^\top a_k$$ — expanding the trace over columns a_k

$$= \sum_k \sum_i a_{ik}^2 = \sum_{i,j} a_{ij}^2$$ — collecting all squared entries

$$\therefore \quad \sqrt{\langle A, A\rangle} = \sqrt{\sum_{i,j} a_{ij}^2} = \|A\|_F \qquad \blacksquare$$

Orthogonality of eigenvectors

Let A be a real symmetric matrix with eigenvalues lambda_a, lambda_b and eigenvectors v_a, v_b. Prove: if v_a and v_b are not orthogonal, then lambda_a = lambda_b.

Hint: Consider <Av_a, v_b> computed in two ways.

Direction 1 — use the eigenvalue equation:

$$\langle Av_a, v_b \rangle = \langle \lambda_a v_a, v_b \rangle = \lambda_a \langle v_a, v_b \rangle$$

Direction 2 — use A = A^T (symmetry):

$$\langle Av_a, v_b \rangle = v_b^\top A v_a = (A^\top v_b)^\top v_a = \langle Av_b, v_a \rangle = \lambda_b \langle v_a, v_b \rangle$$

Conclusion:

$$(\lambda_a - \lambda_b)\langle v_a, v_b \rangle = 0 \;\Rightarrow\; \text{if } \langle v_a, v_b \rangle \neq 0 \text{ then } \lambda_a = \lambda_b \quad \blacksquare$$

ker(A) = ker(ATA)

Let A in R^(m x n). Prove that kernel(A) = kernel(A^T A).

We prove both set inclusions separately.

Direction (a): x in ker(A) => x in ker(A^T A)

$$Ax = 0 \Rightarrow A^\top Ax = A^\top (Ax) = A^\top 0 = 0 \qquad \checkmark$$

Direction (b): x in ker(A^T A) => x in ker(A)

$$A^\top Ax = 0 \Rightarrow x^\top A^\top Ax = 0 \Rightarrow \|Ax\|^2 = 0 \Rightarrow Ax = 0 \checkmark$$

$$\therefore \quad \ker(A) = \ker(A^\top A) \qquad \blacksquare$$

SVD: properties and interpretation

SVD: Let A = U Sigma V^T be the SVD of A in R^(m x n). Answer (a)-(d).

(a) Dimensions:

$U \in \mathbb{R}^{m \times m}$ (or $\mathbb{R}^{m \times r}$ thin SVD) $\Sigma \in \mathbb{R}^{m \times n}$ (diagonal) $V \in \mathbb{R}^{n \times n}$

(b) SVD vs eigenvalue decomposition:

Applies to	Any matrix	Square matrix only
Always exists	Yes	No (non-diagonalizable cases)
Bases used	Two orthogonal (U and V)	One (P)
Form	$U\Sigma V^\top$	PDP^{-1}

(c) Relationship to eigendecomposition of A^T A:

Cols of V = eigenvectors of $A^\top A$. Cols of U = eigenvectors of $AA^\top$. σ_i^2 = eigenvalues of $A^\top A$.

(d) Interpretation of singular values:

nonzero σ_i = rank(A). $\sigma_1 = \|A\|_2$. $\sum_i \sigma_i^2 = \|A\|_F^2$. Geometrically: semi-axes of the ellipsoid A maps the unit sphere to.

Rank-Nullity via SVD

Rank-Nullity via SVD. Let A in R^(m x n) with SVD A = U Sigma V^T and r nonzero singular values.

(a) Show rank(A) = r and null space = last n-r columns of V.

For $i = 1, \ldots, r$: $Av_i = \sigma_i u_i \neq 0 \Rightarrow \text{range}(A) = \text{span}\{u_1, \ldots, u_r\}$, $\text{rank}(A) = r$.

For $i = r+1, \ldots, n$: $Av_i = 0 \Rightarrow \ker(A) = \text{span}\{v_{r+1}, \ldots, v_n\}$.

(b) Rank-Nullity theorem:

$$\text{rank}(A) + \dim(\ker(A)) = r + (n - r) = n \qquad \checkmark$$

(c) Compute SVD and verify for A = [[1,2],[2,4],[3,6]].

$A = (1, 2, 3)^\top (1\ 2)$ — rank 1 (outer product of two vectors).

Column space: $\text{span}\{(1, 2, 3)^\top\}$. Null space: $\text{span}\{(-2, 1)^\top\}$ (dim = 1).

$$\text{rank}(A) + \dim(\ker(A)) = 1 + 1 = 2 = n \qquad \checkmark$$

Low-Rank Approximation

Low-Rank Approximation. The Eckart-Young theorem: best rank-k approximation in Frobenius norm is A_k = sum_{i=1}^k sigma_i u_i v_i^T.

(a) Show ||A - A_k||^2_F = sum_{i=k+1}^r sigma_i^2.

$A - A_k = U(\Sigma - \Sigma_k)V^\top$ where Σ_k has first k singular values, zeros elsewhere.

By unitary invariance $\|UBV^\top\|_F = \|B\|_F$:

$$\|A - A_k\|_F^2 = \|\Sigma - \Sigma_k\|_F^2 = \sigma_{k+1}^2 + \cdots + \sigma_r^2 \quad \blacksquare$$

(b) Storage comparison.

Full matrix $A \in \mathbb{R}^{m \times n}$: mn entries.

Rank-k approx: $U_k \in \mathbb{R}^{m \times k}$ (mk) + diag Σ_k (k) + $V_k \in \mathbb{R}^{n \times k}$ (nk) $\approx k(m+n)$ entries.

(c) When does rank-k save storage?

Save storage when $k(m+n) < mn$, i.e. $k < \dfrac{mn}{m+n}$.

For a square $n \times n$ matrix: $k < \dfrac{n}{2}$.