Categories, Symmetry and Manifolds

Math 4800, Fall 2020

4. Vector Spaces. A vector space exists in the context of a **scalar field** F, so we need to start with a discussion of fields. The linear maps of abelian groups require a small upgrade to define F-linear morphisms in the categories of vector spaces over the fixed field F, and the symmetries of a finite-dimensional vector space in this category are studied via eigenvalues and eigenvectors.

Definition 4.1. A **field** $(F, +, \cdot, 0, 1)$ consists of a set F with two operations:

$$+ : F \times F \to F \text{ (addition) and } \cdot : F \times F \to F \text{ (multiplication)}$$

and distinct elements $0, 1 \in F$ such that:

- Addition and multiplication are associative and commutative.
- Multiplication distributes across addition (i.e. multiplication is *bilinear*):

$$a \cdot (b + c) = (a \cdot b) + (b \cdot c) \text{ and } (a + b) \cdot c = (a \cdot c) + (b \cdot c)$$

- 0 is the additive identity and each $a \in F$ has a unique additive inverse $-a$ making $(F, +, 0)$ into an abelian group.
- 1 is the multiplicative identity and each $a \in F^*$ has a unique reciprocal $1/a$ making $(F^*, \cdot, 1)$ into an abelian group.

Examples. (a) The fields $\mathbb{Q}$ and $\mathbb{R}$ of rational and real numbers.

(b) The finite fields of prime order $\mathbb{Z}/p\mathbb{Z}$.

(c) The field $\mathbb{C}$ of complex numbers.

(d) The fields $\mathbb{R}(t)$ (and $\mathbb{C}(t)$) of rational functions.

Definition 4.2. A field F is *algebraically closed* if every non-constant polynomial $p(x) \in F[x]$ in one variable with coefficients in F has a root in F, i.e.

$$p(a) = 0 \text{ for some } a \in F$$

Examples. (a) $\mathbb{Q}$ is not algebraically closed. E.g. $x^2 - 2$ has no root in $\mathbb{Q}$.

(b) $\mathbb{R}$ is not algebraically closed. E.g. $x^2 + 1$ has no root in $\mathbb{R}$.

(c) The fields $\mathbb{Z}/p\mathbb{Z}$ are not algebraically closed. If p is odd, then **half** of:

$$x^2 - 1, x^2 - 2, ..., x^2 - (p - 1)$$

have roots in $\mathbb{Z}/p\mathbb{Z}$ because square roots come in pairs! Determining which elements of $\mathbb{Z}/p\mathbb{Z}$ have a square root in $\mathbb{Z}/p\mathbb{Z}$ is the goal of *Quadratic Reciprocity.*

(d) $\mathbb{C}$ is algebraically closed (this is the *Fundamental Theorem of Algebra*).

Definition 4.3. A **vector space over a field** F is an abelian group $(V, +, 0)$ with an additional operation of *scalar multiplication* $\cdot : F \times V \to V$ that is bilinear in F and V and satisfies $1 \cdot \vec{v} = \vec{v}$ and $(ab)\vec{v} = a(b\vec{v})$ for all $a, b, \in F$.

Examples. (a) The abelian groups $F^n = F \times \cdots \times F$ with scalar multiplication:

$$a(b_1, ..., b_n) = (ab_1, ..., ab_n) \text{ are vector spaces over } F$$

(b) The abelian group $\{0\}$ is the zero vector space (over any field).

(c) The field F itself is an F-vector space.

(d) The set $F[x]$ of polynomials with polynomial addition.

Definition 4.4. A linear map $f : V \to W$ of vector spaces over F is F-linear if:

$$f(a\vec{v}) = af(\vec{v}) \text{ for all } a \in F \text{ and } \vec{v} \in V$$

Example. (a) An F-linear map $f : F^m \to F^n$ is determined by the vectors:

$$f(e_1) = \vec{v}_1, ..., f(e_m) = \vec{v}_m \in F^n \text{ since } f(x_1, ..., x_m) = x_1\vec{v}_1 + \cdots x_m\vec{v}_m$$

These are the **column** vectors of the matrix A that realizes f as multiplication of the $n \times m$ matrix A by the column vector $(x_1, ..., x_m)$.

(b) The set $\hom(V, W)$ of F-linear maps $f : V \to W$ is a vector space with:

$$(f + g)(\vec{v}) = f(\vec{v}) + g(\vec{v}) \text{ and } (af)(\vec{v}) = af(\vec{v})$$

In particular, the vector space $\hom(V, F) =: V^\vee$ is the **dual** vector space to V.

(c) When $V = F^n$, then $V^\vee$ is also isomorphic to F^n. Let

$$x_1, ..., x_n \in V^\vee \text{ be defined by } x_i(v_1, ..., v_n) = v_i$$

Then an F-linear map $g \in V^\vee$ is uniquely expressed "in coordinates" as:

$$g = g(e_1)x_1 + g(e_2)x_2 + \cdots + g(e_n)x_n$$

just as a vector $\vec{v} \in V$ is uniquely expressed as $\vec{v} = x_1(\vec{v})e_1 + \cdots + x_n(\vec{v})e_n$.

Definition 4.5. The category $\mathfrak{Vec}_F$ of vector spaces over F is defined by:

- The objects are the vector spaces over F.
- The morphisms are the F-linear maps of vector spaces.

Remark. If $f : V \to W$ is F-linear and a bijection, then $f^{-1} : W \to V$ is F-linear.

Definition 4.6. (a) A subgroup $W \subset V$ of a vector space over F is a **subspace** if:

$$a\vec{w} \in W \text{ for all } a \in F,\ \vec{w} \in W$$

in addition to W being closed under sums and additive inverses.

(b) A set of vectors $\vec{w}_1, ..., \vec{w}_m \in V$ **spans** the subspace:

$$W = \langle \vec{w}_1, ..., \vec{w}_m \rangle = \{a_1\vec{w}_1 + \cdots + a_m\vec{w}_m |\ a_1, ..., a_m \in F\} \subseteq V$$

(c) The vectors $\vec{w}_1, ..., \vec{w}_m \in V$ in (b) are **linearly independent** if:

$$a_1\vec{w}_1 + \cdots + a_m\vec{w}_m = 0 \quad \Leftrightarrow \quad a_1 = a_2 = \cdots = a_m = 0$$

Proposition 4.7. The span $W = \langle \vec{w}_1, ..., \vec{w}_m \rangle \subset V$ is isomorphic to F^m whenever the vectors $\vec{w}_1, ..., \vec{w}_m \in V$ are linearly independent.

Proof. Define $f : F^m \to W$ by $f(x_1, ..., x_m) = x_1\vec{w}_1 + \cdots + x_m\vec{w}_m$. Then f is surjective and also injective, since:

$$f(x_1, ..., x_m) = f(y_1, ..., y_m) \text{ if and only if } f(x_1 - y_1, ..., x_m - y_m) = 0$$

and $(x_1 - y_1)\vec{w}_1 + \cdots + (x_m - y_m)\vec{w}_m = 0$ if and only if $(x_1, ..., x_m) = (y_1, ..., y_m)$ since the vectors $\vec{w}_1, ..., \vec{w}_m$ are linearly independent. □

Proposition 4.8. F^n does not contain more than n linearly independent vectors.

Proof. If $\vec{v}_1, ..., \vec{v}_{n+1} \in F^n$, then row operations on the system of equations:

$$\vec{v}_i = a_{i,1}e_1 + \cdots + a_{i,n}e_n; \quad i = 1, ..., n + 1$$

yield a non-zero linear dependence $b_1\vec{v}_1 + \cdots + b_n\vec{v}_{n+1} = 0$. □

Corollary 4.9. Every vector space V that can be spanned by finitely many vectors is isomorphic to F^n for a unique n. This is the **dimension** of V, and each set of n linearly independent vectors in V is a **basis** of V. Each choice of basis determines an isomorphism $f : F^n \to V$ that is unique to that basis by Proposition 4.7.

As with the standard finite sets $[n]$, the symmetries of the vector spaces F^n transfer to symmetries of any finite dimensional vector space, so we will confine our attention to these *standard* finite dimensional vector spaces.

Lemma 4.10. An F-linear function $f : F^n \to F^n$ is a **symmetry** if and only if

$$f^{-1}(0) = 0$$

Proof. If $f(\vec{v}) = f(\vec{w})$, then $f(\vec{v}-\vec{w}) = 0$, so $\vec{v}-\vec{w} \in f^{-1}(0)$, and by assumption,

$$\vec{v} - \vec{w} = 0, \text{ i.e. } \vec{v} = \vec{w}$$

so f is injective. But this means in particular that $f(e_1), ..., f(e_n) \in F^n$ are linearly independent, so they are a basis for F^n. Thus f is also surjective. $\square$

Definition 4.11. The **kernel** of $f : V \to W$ is the subspace $\ker(f) := f^{-1}(0) \subset V$.

The kernel measures how far away an F-linear map is from being injective.

Definition 4.12. The **quotient** of a vector space V by a subspace $W \subset V$ is:

$$V = \{\vec{v} + W \mid \vec{v} \in V\}$$

where $\vec{v} + W = \vec{u} + W$ if $\vec{v} + \vec{w}_1 = \vec{u} + \vec{w}_2$ for vectors $\vec{w}_1, \vec{w}_2 \in W$, and:

$$(\vec{v} + W) + (\vec{u} + W) = (\vec{v} + \vec{u}) + W, \quad 0 = 0 + W = W \text{ and } a(\vec{v} + W) = a\vec{v} + W$$

Definition 4.13. (a) The **image** of $f : V \to W$ is the image subspace $f(V) \subset W$.

(b) The **cokernel** of $f : V \to W$ is the quotient vector space $W/f(V)$.

The cokernel measures how far an F-linear map is from being surjective.

Proposition 4.14. If $W \subset V$ is a subspace, then:

$$\dim(W) + \dim(V/W) = \dim(V)$$

Proof. A basis $\vec{w}_1, ..., \vec{w}_m$ of W *extends* to a basis of V with additional vectors $\vec{v}_{m+1}, ..., \vec{v}_n$ chosen so that the cosets $\vec{v}_i + W$ are a basis for V/W. $\square$

Corollary 4.15. If $f : V \to W$ is F-linear, then:

$$\dim(\ker(f)) - \dim(\mathrm{coker}(f)) = \dim(V) - \dim(W)$$

Proof. This follows from two applications of the Proposition and the F-linear isomorphism $\overline{f} : V/\ker(f) \to f(V)$ from the coimage to the image, which is the exact analog of Proposition 2.4. $\square$

Now it is time to define the *determinant*.

Definition 4.16. Let $A = (a_{ij})$ be an $n \times n$ matrix with entries in F. Then:

$$\det(A) = \sum_{\sigma:[n]\to[n]} \mathrm{sgn}(\sigma) \cdot \prod_{i=1}^{n} a_{i,\sigma(i)} \in F$$

is the **determinant** of A (the sum is taken over all symmetries of $[n]$).

Examples.

$$\det \begin{bmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{bmatrix} = a_{1,1}a_{2,2} - a_{1,2}a_{2,1}$$

with terms matching the permutations $1_{[2]} = (1)(2)$ and $(1\ 2)$.

$$\det \begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{bmatrix} = \begin{array}{c} a_{1,1}a_{2,2}a_{3,3} + a_{1,2}a_{2,3}a_{3,1} + a_{1,3}a_{2,1}a_{3,2} \\ - a_{1,2}a_{2,1}a_{3,3} - a_{1,3}a_{2,2}a_{3,1} - a_{1,1}a_{2,3}a_{3,2} \end{array}$$

with the two terms matching $1_{[3]}, (1\ 2\ 3), (1\ 3\ 2), (1\ 2)(3), (1\ 3)(2)$ and $(1)(2\ 3)$.

One useful way to think about the determinant is to regard an $n \times n$ matrix A as a list of its column vectors $\vec{v}_1, ..., \vec{v}_n \in F^n$, and then to think it as a function:

$$\det : F^n \times F^n \times \cdots \times F^n \to F$$

From this point of view, det is an *F-multilinear function* (linear in each slot):

$$\det(\vec{v}_1, ..., \vec{v}_i + \vec{w}_i, \dots, \vec{v}_n) = \det(\vec{v}_1, ..., \vec{v}_i, \dots, \vec{v}_n) + \det(\vec{v}_1, ..., \vec{w}_i, \dots, \vec{v}_n)$$

$$\text{and } \det(\vec{v}_1, ..., a\vec{v}_i, \dots, \vec{v}_n) = a \det(\vec{v}_1, ..., \vec{v}_i, \dots, \vec{v}_n)$$

(such a function is also called an *n-tensor*). Every tensor T is determined by what it does to lists of *standard* basis vectors e_i. If the tensor is also *alternating*, i.e. if T alternates sign when two vectors are exchanged, then T maps any list of standard basis vectors with a repetition to zero, and if $\sigma : [n] \to [n]$ is a permutation, then:

$$T(e_{\sigma(1)}, ..., e_{\sigma(n)}) = \operatorname{sgn}(\sigma) \cdot T(e_1, ..., e_n)$$

so T is determined by $T(e_1, ..., e_n)$, i.e. by what it does to the identity matrix.

The determinant **does** alternate as we see from the following Lemma:

Lemma 4.18. (a) $\det(A) = \det(A^T)$, where $A^T = (a_{j,i})$ is the transpose of A.

(b) Swapping two rows (or columns) of A multiplies $\det(A)$ by -1.

Proof. (a) follows from the equality $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\sigma^{-1})$ and:

$$\det(A^T) = \sum_{\sigma} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} a_{\sigma(i),i} = \sum_{\sigma} \operatorname{sgn}(\sigma) \prod_{\sigma(i)=1}^{n} a_{\sigma(i),i} = \sum_{\sigma} \operatorname{sgn}(\sigma^{-1}) \prod_{i=1}^{n} a_{i,\sigma^{-1}(i)}$$

which is $\det(A)$. For a transposition $(j\ k)$, consider the two *right cosets*:

$$A_n \cdot 1 \text{ and } A_n \cdot (j\ k) = \{\tau \circ (j\ k) \mid \tau \in A_n\}$$

of the alternating subgroup A_n of the group S_n of symmetries of $[n]$. Then:

$$\det(A) = \sum_{\tau \in A_n} \prod_{i=1}^{n} a_{i,\tau(i)} - \sum_{\tau \in A_n} \left(\prod_{i \neq j,k} a_{i,\tau(j)} \right) \cdot a_{j,\tau(k)} \cdot a_{k,\tau(j)}$$

since $\operatorname{sgn}(\tau) = 1$ and $\operatorname{sgn}(\tau \circ (j\ k)) = -1$ for all $\tau \in A_n$. But if B is the matrix obtained by swapping rows j and k of the matrix A, then:

$$\det(B) = \sum_{\tau \in A_n} \prod_{i=1}^{n} b_{i,\tau(i)} - \sum_{\tau \in A_n} \left(\prod_{i \neq j,k} b_{i,\tau(j)} \right) \cdot b_{j,\tau(k)} \cdot b_{k,\tau(j)}$$

$$= \sum_{\tau \in A_n} \left(\prod_{i \neq j,k} a_{i,\tau(j)} \right) \cdot a_{j,\tau(k)} \cdot a_{k,\tau(j)} - \sum_{\tau \in A_n} \prod_{i=1}^{n} a_{i,\tau(i)} = -\det(A) \quad \square$$

Corollary 4.19. (a) If two rows or columns of A coincide, then $\det(A) = 0$.

(b) Adding a multiple of one row to another does not change the determinant.

Remarks. (i) The determinant is the *unique* alternating n-tensor with $\det(I_n) = 1$. Any other alternating n-tensor T is therefore a multiple of the determinant. If

$$T(I_n) = b \text{ then } T(A) = b \cdot \det(A)$$

(ii) The absolute value of $\det(\vec{v}_1, ..., \vec{v}_n)$ for vectors in the first orthant of $\mathbb{R}^n$ is the **volume** of the solid enclosed by the vectors. This follows from the fact that the determinant is multilinear, that it is zero when vectors are repeated, and that the absolute value of the determinant does not change when vectors are permuted.

Theorem 4.20. $\det(BA) = \det(B) \cdot \det(A)$ for all pairs of $n \times n$ matrices.

Proof. Fix a matrix B and define an n-tensor T by setting $T(A) = \det(BA)$. This is an alternating n-tensor on the columns of A and $T(I_n) = \det(B)$. So

$$\det(BA) = T(A) = \det(B) \cdot \det(A) \text{ by Remark (i)}$$

Change of Basis. An F-linear map $f : V \to V$ of n-dimensional vector spaces becomes an $n \times n$ matrix when a basis isomorphism $g : F^n \to V$ is chosen, via:

$$A = g^{-1} \circ f \circ g : F^n \to F^n$$

When two bases g_1 and g_2 are chosen, $A_1 = g_1^{-1} \circ f \circ g_1$ and $A_2 = g_2^{-1} \circ f \circ g_2$ are related by the change of basis formula:

$$A_2 = g_2^{-1} \circ g_1 \circ A_1 \circ g_1^{-1} g_2 = (g_1^{-1} \circ g_2)^{-1} \circ A_1 \circ (g_1^{-1} \circ g_2) = B^{-1} A_1 B$$

where B is the matrix associated to the "change of basis:" $g_1^{-1} \circ g_2 : F^n \to F^n$. By Theorem 4.20, we therefore obtain $\det(A_2) = \det(B^{-1}) \det(A) \det(B) = \det(A_1)$. So the determinant of A above is not sensitive to the choice of basis.

One important consequence of this is the following:

Corollary 4.21. $\det(A) \neq 0$ if and only if A is a symmetry of F^n.

Proof. A is a symmetry if and only if $\ker(A) \neq 0$ by Lemma 4.10. If A is a symmetry of F^n, then $\det(AA^{-1}) = \det(I_n) = 1$ implies that $\det(A) \det(A^{-1}) = 1$, and in particular that $\det(A) \neq 0$. On the other hand, if $v \in \ker(A)$ is a nonzero vector, then v can be taken as the first vector in a basis of F^n, and then $\det(A) = 0$ because the matrix for that basis has the zero vector in its first column. $\square$

Questions. (a) The determinant $\det(A)$ is a polynomial function of the entries of an $n \times n$ matrix A. What other polynomial functions of the entries of A satisfy

$$f(A) = f(B^{-1}AB)?$$

(b) Given $f : V \to V$, what bases of V produce the "simplest" matrix A?

Examples. (a) The **trace** of $A = (a_{ij})$ is the linear function $\mathrm{tr}(A) = a_{1,1} + \cdots + a_{n,n}$ (i.e. it is the sum of the diagonal entries). The trace satisfies the relation:

$$\mathrm{tr}(AB) = \mathrm{tr}(BA)$$

for all matrices A and B, and so $\mathrm{tr}(B^{-1}(AB)) = \mathrm{tr}(AB)(B^{-1}) = \mathrm{tr}(A)$.

(b) Suppose V has a basis of vectors $v_1, ..., v_n$ with the property that:

$$f(v_i) = \lambda_i v_i \text{ for all } i = 1, ..., n$$

Then with this basis, A is a **diagonal** matrix. This is a simple as a matrix can be.

Definition 4.22. (a) Each nonzero vector v such that $f(v) = \lambda v$ is called an **eigenvector** of $f : V \to V$ and λ is the **eigenvalue** (stretching factor) of v.

(b) $f : V \to V$ is **semi-simple** if it has a basis of eigenvectors.

Remark. Not all symmetries of F^n are semi-simple!

Four Transformations of the Plane. (i) Every nonzero vector in $\mathbb{R}^2$ is an eigenvector of the scaling matrices $A = \lambda \cdot I_2$.

(ii) Most rotations of $\mathbb{R}^2$ have no real eigenvectors. The exceptions are $\pm I_2$, the latter of which is the reflection through the origin ("scaling" by -1).

(iii) A reflection across a line $\mathbb{R}^2$ has two eigenvectors with eigenvalues 1 and -1, pointing in the direction of the line and in the direction orthogonal to the line.

(iv) The shearing transformation $A = ((1,0),(1,1))$ has only one eigenvector e_1 (and its multiples) with eigenvalue 1, so it is not semi-simple.

The Characteristic Polynomial of a matrix A is:

$$\mathrm{ch}(A) = \det(xI_n - A) \in F[x]$$

This is a monic polynomial of degree n in the variable x, and one can check that:

$$x^n - \mathrm{tr}(A)x^{n-1} + \cdots + (-1)^n \det(A)$$

For example,

$$\det \begin{bmatrix} x - a_{11} & -a_{12} \\ -a_{21} & x - a_{22} \end{bmatrix} = (x - a_{11})(x - a_{22}) - a_{12}a_{21} = x^2 - \mathrm{tr}(A)x + \det(A)$$

Because

$$\det(xI_n - A) = \det(B^{-1}(xI_n - A)B) = \det(xI_n - B^{-1}AB)$$

it follows that the characteristic polynomials of A and $B^{-1}AB$ are the same, and thus that every coefficent of a power of x in the characteristic polynomial is an invariant polynomial of the (a_{ij}) in the sense of Question (a). These polynomials account for all of the invariant polynomials.

Examples. (i) The characteristic polynomial for scaling by λ is $(x - \lambda)^2$.

(ii) The characteristic polynomial for rotation by θ is $x^2 + 2\cos(\theta)x + 1$.

(iii) The characteristic polynomial for all reflections is $x^2 - 1$.

(iv) The characteristic polynomial for the shearing transformation is $(x - 1)^2$.

Eigenvectors. There is a nonzero vector $v \in F^n$ satisfies $Av = \lambda v$ if and only if

$$(\lambda I_n - A)v = 0$$

if and only if λ is a **root** of the characteristic polynomial (Corollary 4.21). Thus:

(i) There are at most n distinct eigenvalues of an $n \times n$ matrix A.

(ii) Each eigenvalue is the eigenvalue of at least one eigenvector.

Remark. In example (ii) above, the characteristic polynomial of the rotation by θ has no **real** roots when $\theta \neq 0, \pi$, but it does have two distinct **complex** roots $e^{\pm i\theta}$. These correspond to complex eigenvalues of the rotation, thought of as a $\mathbb{C}$-linear transformation (with eigenvectors $(1, \pm i)$). Regarding a vector space over F as a vector space over a larger field containing F is called *extension of scalars.* It reveals the fact that the rotation is semi-simple, when viewed over the "right" field.

Proposition 4.23. Eigenvectors with distinct eigenvalues are linearly independent.

Proof. Assume the Proposition is true for $m-1$ vectors with distinct eigenvalues. Let $v_1, ..., v_m \in F^n$ have distinct eigenvalues $\lambda_1, ..., \lambda_m$ for a matrix A. Then $c_1 v_1 + \cdots + c_m v_m = 0$ implies:

$$0 = A(c_1 v_1 + \cdots + c_m v_m) = c_1 \lambda_1 v_1 + \cdots + c_m \lambda_m v_m$$

and so, subtracting $\lambda_1(c_1 v_1 + \cdots + c_m v_m)$ from $c_1 \lambda_1 v_1 + \cdots + c_m \lambda_m v_m$,

$$c_2(\lambda_2 - \lambda_1)v_2 + \cdots + c_m(\lambda_m - \lambda_1)v_m = 0$$

which implies (by the inductive assumption) that $c_2 = \cdots = c_m = 0$, and so $c_1 v_1 = 0$, which implies that $c_1 = 0$, as well, since eigenvectors are nonzero. $\square$

Corollary 4.24. If $\mathrm{ch}(A)$ has n distinct roots, then A is semi-simple.

The converse is not true (I_n is semi-simple, but $\mathrm{ch}(I_n)$ has only one root!). Note that when the field F is $\mathbb{C}$, or any other algebraically closed field, then the characteristic polynomial has n roots, counted with multiplicity. In particular, it always has at least **one** root, and so it has at least one eigenvector.

Proposition 4.25. An orthogonal transformation A of $\mathbb{R}^n$ (see §3) is semi-simple when the field of scalars is extended to $\mathbb{C}$. Moreover, there are mutually orthogonal (real) subspaces:

$$W_1, W_2, ..., W_m \in \mathbb{R}^n \text{ such that either:}$$

(a) $\dim(W_i) = 2$ and A is the rotation by an angle θ_i when restricted to W_i or

(b) $\dim(W_i) = 1$ and A is multiplication by 1 or -1 when restricted to W_i.

Proof. Let $\vec{v}$ be one (possibly complex) eigenvector of A. Then the eigenvalue of $\vec{v}$ is a complex number λ of length one, since:

$$|\vec{v}| = |A\vec{v}| = |\lambda \vec{v}| = |\lambda| \cdot |\vec{v}|$$

Because the characteristic polynomial has real coefficients, it follows that $\lambda = \pm 1$ or else $\lambda = e^{i\theta}$, in which case the complex conjugate $e^{-i\theta} = \overline{e^{i\theta}}$ is also an eigenvalue. The complex conjugate of (the coordinates of) $\vec{v}$ is an eigenvector for $e^{-i\theta}$, and the two vectors $\vec{v}$ and $\overline{\vec{v}}$ determine **real** vectors $\vec{v} + \overline{\vec{v}}$ and $\frac{1}{i}(\vec{v} - \overline{\vec{v}})$ that span a **plane** in $\mathbb{R}^n$ which is rotated by the angle θ via the transformation A. Here's the big idea:

- Given a subspace $V \subset \mathbb{R}^n$ fixed by A, the **orthogonal complement**:

$$V^\perp = \{\vec{w} \in V \mid \vec{w} \cdot \vec{v} = 0 \text{ for all } \vec{v} \in V\}$$

is also fixed by A, and A is an orthogonal transformation when restricted to $V^\perp$. This allows us to conclude the Proposition by induction on the dimension n. $\square$

Corollary 4.26. An orthogonal transformation A of $\mathbb{R}^3$ with $\det(A) = 1$ is a rotation by an angle θ around a fixed axis line in $\mathbb{R}^3$.

Proof. (At least) one of the eigenvalues of A is real, with eigenvalue ± 1. If the other two eigenvalues are complex, then the decomposition from Proposition 4.24 shows that either A is a rotation around a fixed axis (with eigenvalue 1) or else the eigenvalue in the axis direction is -1, but that case would give $\det(A) = -1$. On the other hand, if A has three real eigenvectors, then they must have eigenvalues $1, 1, 1$ (the identity) or else $-1, -1, 1$ (rotation by $\theta = \pi$ around a fixed axis. $\square$

Assignment 4.

1. Prove that the following fields are not algebraically closed.

(i) $\mathbb{Z}/2\mathbb{Z}$.

(ii) $\mathbb{C}(t)$.

2. (a) Fill in the details of the proof of Proposition 2.8 to show that F^n does not contain more than n linearly independent vectors.

(b) Prove the guts of Corollary 4.9. That is, prove that if a vector space V has a basis of n vectors, then **any** set of n linearly independent vectors in V must span.

3. Prove the expansion formula for the determinant:

$$\det(A) = \sum_{j=1}^{n} (-1)^{i+j} a_{i,j} \det(A_{i,j}) \text{ for each fixed } i$$

where $A_{i,j}$ is the "minor" of A obtained by striking out the ith row and jth column. Recall that this is the formula that allows us to conclude Cramer's Rule. If:

$$B \text{ is the matrix with coordinates } (-1)^{i+j}\det(A_{j,i})$$

then:

$$AB = \det(A) \cdot I_n, \text{ i.e. } A^{-1} = \frac{1}{\det(A)} B$$

4. Prove that if A and B are $n \times n$ matrices, then $\mathrm{tr}(AB) = \mathrm{tr}(BA)$.

5. What are the product and coproduct of subspaces W_1, W_2 of a fixed vector space in the category $\mathfrak{S}ub_V$ of subspaces of a fixed vector space V (with inclusion)?

6. Recall that if $V = F^n$, then the vector space of linear maps (one-tensors):

$$V^\vee = \mathrm{Hom}_F(V, F)$$

has a basis $x_1, ..., x_n$ defined by $x_i(a_1, ..., a_n) = a_i$. The space of 2-tensors:

$$V \times V \to F$$

is similarly a vector space of dimension n^2 with basis $\{x_i \otimes x_j\}$ defined by:

$$x_i \otimes x_j((a_1, ..., a_n), (b_1, ..., b_n)) = a_i b_j$$

(a) From this point of view, verify that the dot product is the symmetric 2-tensor:

$$x_1 \otimes x_1 + \cdots + x_n \otimes x_n$$

and that if $n = 2$, the determinant is the alternating 2-tensor: $x_1 \otimes x_2 - x_2 \otimes x_1$.

In general, a 2-tensor $\sum a_{ij} x_i \otimes x_j$ is represented by the matrix $A = (a_{ij})$, and:

- A symmetric 2-tensor is represented by a symmetric matrix, and
- An alternating 2-tensor is represented by a skew-symmetric matrix.

(b) Check that every 2-tensor T is the sum

$$T = T_{Sym} + T_{Alt}$$

of a symmetric and an alternating 2-tensor and that this expression is unique.