Linear Algebra: Some things to know

Jonathan L.F. King
University of Florida, Gainesville FL 32611-2082, USA
squash@ufl.edu
Webpage http://squash.1gainesville.com/
27 March, 2024 (at *17:39*)

§Outline

Entrance. [Look ahead to **Shorthands** on P.3.] For each defn to follow, know several examples where the objects *fulfill* the defn, and several examples where the objects *fail* the defn. [E.g, exhibit a set of vectors that is *not* LI. What is an example of a pair of VSes and a map T between them that: *is* linear? *fails* to be linear? –what specific axiom fails?]

Defn: Group. A ***commutative group*** is a triple $(\mathbf{V},+,\mathbf{0})$ where $\mathbf{V}$ is a set, $+$ is a binary operation $\mathbf{V}\times\mathbf{V}\to\mathbf{V}$, and $\mathbf{0}\in\mathbf{V}$, satisfying the following axioms for all $\mathbf{x},\mathbf{y},\mathbf{z}\in\mathbf{V}$:

CG1: Element $\mathbf{0}$ is an ***identity element*** for "+", i.e,

$$\mathbf{x}+\mathbf{0} = \mathbf{x} = \mathbf{0}+\mathbf{x}.$$

CG2: Addition is associative: $\mathbf{x}+[\mathbf{y}+\mathbf{z}] = [\mathbf{x}+\mathbf{y}]+\mathbf{z}$.

CG3: Every element $\mathbf{x}$ has an ***additive inverse*** $\mathbf{x}'$ satisfying: $\mathbf{x}+\mathbf{x}' = \mathbf{0} = \mathbf{x}'+\mathbf{x}$.

CG4: Addition is commutative: $\mathbf{x}+\mathbf{y} = \mathbf{y}+\mathbf{x}$.

[Note: A ***group*** $(\mathbf{V},+,\mathbf{0})$, but which is not necessarily commutative, is required to satisfy (CG 1–3) but is not required to satisfy (CG 4).] □

It is an easy theorem that $\mathbf{0}$ is the unique identity element for "+" and that additive inverses are unique. The additive inverse of $\mathbf{x}$ is usually written as "$-\mathbf{x}$".

Defn: VS. A ***vectorspace*** is a four-tuple

$$(\mathbf{V},+,\vec{\mathbf{0}},\mathsf{F}),$$

where $\mathbf{V}$ is a *set* [of vectors], with $\vec{\mathbf{0}}\in\mathbf{V}$, where F is a field (e.g, $\mathbb{R}$ or $\mathbb{Q}$ or $\mathbb{C}$), and where the ***scalar-vector multiplication*** operation $\cdot$ is a map $\mathsf{F}\times\mathbf{V}\to\mathbf{V}$.

Using ***SVM*** to abbreviate ***scalar-vector multiplication*** [usually called "scalar multiplication"], the four-tuple must satisfy the following.

For all $\alpha,\beta\in\mathsf{F}$ *and* $\mathbf{x},\mathbf{y}\in\mathbf{V}$:

SV1: Triple $(\mathbf{V},+,\vec{\mathbf{0}})$ is a commutative group.

SV2: The SVM distributes over *vector* addition: $\alpha[\mathbf{x}+\mathbf{y}] = \alpha\mathbf{x}+\alpha\mathbf{y}$.

Also, SVM distributes over *scalar* addition: $[\alpha+\beta]\mathbf{x} = \alpha\mathbf{x}+\beta\mathbf{x}$.

SV3: Multiplication associates with SVM, i.e $[\alpha\cdot\beta]\mathbf{x} = \alpha\cdot[\beta\mathbf{x}]$.

SV4: Scalars 1 and 0 act as follows: $1\cdot\mathbf{x} = \mathbf{x}$ and $0\cdot\mathbf{x} = \vec{\mathbf{0}}$.

A consequence of these axioms is that $-1\mathbf{u} \stackrel{\text{notation}}{=\!=} -\mathbf{u}$ is the additive-inverse of $\mathbf{u}$. □

Trivial VS. For the zero-*vector* in VS $\mathbf{X}$, use $\vec{\mathbf{0}}_{\mathbf{X}}$ or $\vec{\mathbf{0}}$. For the zero-dim'al VS (or VSubSp) $\{\vec{\mathbf{0}}\}$, I will sometimes use $\mathbf{0}$ for $\{\vec{\mathbf{0}}\}$, and $\mathbf{0}_{\mathbf{X}}$ for $\{\vec{\mathbf{0}}_{\mathbf{X}}\}$ if there are several spaces under discussion.

Use $\mathbf{0}_{K\times N}$ for the $K\times N$ *matrix* of all zeros; if the dimensions are understood, use $\mathbf{0}_{\mathtt{Mat}}$. For the zero-lin.map $\mathbf{V}\to\mathbf{X}$ which sends each $\mathbf{V}$-vector to $\vec{\mathbf{0}}_{\mathbf{X}}$, use $\mathbf{0}_{\mathtt{Trn}}$ or $\mathbf{0}_{\mathbf{V}\to\mathbf{X}}$. [Of course, this $\mathbf{0}_{\mathtt{Trn}}$ is the zero-*vector* in vector space $\mathrm{LIN}(\mathbf{V}\to\mathbf{X})$.] □

Shorthands. VS(es), vector space(s). VSubSp, vector subspace. trn, transformation. lin.trn, linear trn. colvec, column-vector. rowvec, row-vector. LI, Linearly Independent. LD, Linearly Dependent. eVec, eigenvector. eVal, eigenvalue. eSpace, eigenspace. □

Nomenclature. Our symbols and our textbook's.

SVM = scalar-vector multiplication = scalar multiplication.

$\mathrm{Dim}(\mathbf{W}) = \dim(\mathbf{W})$ = [Dimension of VS **W**].

$\mathrm{Nul}(\mathsf{T}) = \mathsf{N}(\mathsf{T})$ = [Nullspace, i.e, Kernel of map T].
$\mathrm{Nullity}(\mathsf{T}) = \mathrm{nullity}(\mathsf{T}) = \mathrm{Dim}(\mathrm{Nul}(\mathsf{T}))$.

$\mathrm{Range}(\mathsf{T}) = \mathsf{R}(\mathsf{T})$ = [Range of T].
$\mathrm{Rank}(\mathsf{T}) = \mathrm{rank}(\mathsf{T}) = \mathrm{Dim}(\mathrm{Range}(\mathsf{T}))$.

$\mathrm{MAT}_{K\times L}(\mathbb{Q}) = \mathsf{M}_{K\times L}(\mathbb{Q})$ = [Space of $K\times L$-matrices] with rational entries.
$\mathrm{LIN}(\mathbf{V}\to\mathbf{X}) = \mathcal{L}(\mathbf{V}, \mathbf{X})$ = [Space of linear maps $\mathbf{V}\to\mathbf{X}$]; may also be written $\mathrm{LIN}(\mathbf{X}\leftarrow\mathbf{V})$. Space $\mathrm{LIN}(\mathbf{V}\to\mathbf{V})$ will be written as $\mathrm{LIN}(\mathbf{V})$ or, for emphasis, $\mathrm{LIN}(\mathbf{V}\circlearrowleft)$.

VS = vector space. VSes = vector spaces.
VSS = vector-subspace.

We'll typically using lowercase greek letters for scalars; $\alpha, \beta, \gamma, \ldots$, and often use script $\mathcal{B}, \mathcal{E}, \mathcal{U}, \mathcal{R}$ for bases; our textbook uses (ugh!) β. □

Convention. We use ***map*** or ***mapping*** for a fnc going from one set to a (*possibly different*) set. E.g,

$$\mathrm{OwnerOf}\colon \mathrm{BIKES}\to\mathrm{PEOPLE}\,.$$

In contrast, let's use ***transformation*** (abbreviated as ***trn***) as a map from a set to *itself*. In these notes, "*transformation*" (unless explicitly stated otherwise) is a "*linear transformation*". □

Subset-sum. Thw "***sum of subsets***" $S_1, \ldots, S_N \subset \mathbf{V}$, written $\sum_{j=1}^N S_j$ or $S_1 + \ldots + S_N$, is the set of all sums $\mathbf{u}_1 + \ldots + \mathbf{u}_N$ with each $\mathbf{u}_j \in S_j$. In general

$$*: \qquad \sum_{j=1}^N S_j \quad \subset \quad \mathrm{Spn}\Big(\bigcup_{j=1}^N S_j\Big)$$

If each S_j is a sub<u>space</u>, then there is *equality* in $(*)$.□

Linear-independence of <u>subspaces</u>. Consider a collection $\mathcal{U}$ of *subspaces* of VS $\mathbf{V}$. This $\mathcal{U}$ <u>is</u> ***linearly independent*** (LI) if each finite subset $\{\mathbf{W}_1, \ldots, \mathbf{W}_N\} \subset \mathcal{U}$ satisfies: *The <u>only</u> tuple* $(\mathbf{u}_1, \ldots, \mathbf{u}_N)$ *of vectors having each* $\mathbf{u}_j \in \mathbf{W}_j$, *and satisfying* $\sum_{j=1}^N \mathbf{u}_j = \vec{\mathbf{0}}$, *is the* $\vec{\mathbf{0}} = \mathbf{u}_1 = \ldots = \mathbf{u}_N$ ***trivial soln***.

If no subspace in $\mathcal{U}$ is the trivial subspace $\mathbf{0}$ then: *Collection* $\mathcal{U}$ *is* LI *IFF no* $\mathbf{W} \in \mathcal{U}$ *can be deleted without reducing the span:*

$$\forall \mathbf{W} \in \mathcal{U}: \qquad \mathrm{Spn}(\mathcal{U} \setminus \{\mathbf{W}\}) \subsetneqq \mathrm{Spn}(\mathcal{U})\,. \qquad \square$$

ASIDE: The negation of *Linearly Independent* (LI) is ***Linearly Dependent*** (LD).

Defn: Span. A ***linear combination*** (***lin-comb***) of a *finite* list $\mathbf{u}_1, \ldots, \mathbf{u}_N$ of vectors, is a sum of form $\sum_{j=1}^N \alpha_j \mathbf{u}_j$, where each α_j is a scalar.

Given a [finite or infinite] set $\mathcal{C}$ of vectors, $\mathrm{Spn}(\mathcal{C})$ is the set of <u>*all*</u> (finite) linear combinations of vectors from $\mathcal{C}$.

Collection $\mathcal{C}$ is ***span-minimal*** if no member can be deleted without reducing the span. I.e each $\mathbf{u} \in \mathcal{C}$ has $\mathrm{Spn}(\mathcal{C} \setminus \{\mathbf{u}\}) \subsetneqq \mathrm{Spn}(\mathcal{C})$.

In vectorspace $\mathbf{V}$, collection $\mathcal{C}$ "***generates***" or "is ***spanning***" or "spans $\mathbf{V}$" or "spans the VS" if $\mathrm{Spn}(\mathcal{C}) = \mathbf{V}$. Our $\mathcal{C}$ is ***generating-minimal*** if $\mathcal{C}$ spans the VS *and* is span-minimal.

Our $\mathbf{V}$ is ***finite dimensional*** if $\mathbf{V}$ admits a *finite* generating-set $\mathcal{C}$. □

Linear-independence of ***vectors***. Vector-collection $\mathcal{C}$ is ***linearly independent*** (LI) if each finite subset $\{\mathbf{u}_1, \ldots, \mathbf{u}_N\} \subset \mathcal{C}$ satisfies: *The <u>only</u> tuple* $(\alpha_1, \ldots, \alpha_N)$ *of scalars satisfying* $\sum_{j=1}^N \alpha_j \mathbf{u}_j = \vec{\mathbf{0}}$ *is* $0 = \alpha_1 = \ldots = \alpha_N$; *the* ***trivial soln***.

An LI collection $\mathcal{B}$ which generates, is called a ***basis*** for the VS. □

1: Proposition. *Subset* $\mathcal{C} \subset \mathbf{V}$ *is span-minimal IFF* $\mathcal{C}$ *is linearly independent.* ◊

Pf (⇒). Were $\mathcal{C}$ *not* LI then WLOG we have $\mathcal{C}$-vectors and scalars s.t $\sum_{j=1}^N \alpha_j \mathbf{u}_j = \vec{\mathbf{0}}$, with some scalar non-zero. WLOG $\alpha_1 \neq 0$. Letting $\beta_j := -\alpha_j/\alpha_1$, then,

$$\mathbf{u}_1 = \sum_{j=2}^N \beta_j \mathbf{u}_j \overset{\text{note}}{\in} \mathrm{Spn}(\mathbf{u}_2, \ldots, \mathbf{u}_N)\,.$$

So $\mathcal{C}$ is <u>not</u> span-minimal. ♦

Pf (⇐). Supposing $\mathcal{C}$ *not* span-minimal, there exists a $\mathcal{C}$-vector $\mathbf{w}$ and *other* $\mathcal{C}$-vectors $\mathbf{u}_1, \ldots, \mathbf{u}_L$ and scalars $\{\alpha_j\}_j$, satisfying $\mathbf{w} = \sum_{j=1}^L \alpha_j \mathbf{u}_j$. Thus

$$-1\mathbf{w} + \alpha_1 \mathbf{u}_1 + \ldots + \alpha_L \mathbf{u}_L$$

is a non-trivial way of writing $\vec{\mathbf{0}}$. [I.e, our $\mathcal{C}$ is LD.] ♦

Defn: Support. Consider a fnc $h:\Omega^{\text{Set}}\to\mathsf{R}$ where R is a field (or ring). The "***support*** of h" is

$$\operatorname{Supp}(h) \;:=\; \{\omega \in \Omega \mid h(\omega) \neq 0\}\,.$$

Consider a VS $\mathbf{V}$ over field F. A ***FSSF*** (Finitely-Supported Scalar Function) is a map $h:\mathbf{V}\to\mathsf{F}$ such that $\operatorname{Supp}(h)$ is finite. Thus, given a collection $\mathcal{C} \subset \mathbf{V}$,,

$$\operatorname{Spn}(\mathcal{C}) \;=\; \Big\{\sum\nolimits_{\mathbf{u}\in\mathcal{C}} h(\mathbf{u})\mathbf{u} \;\Big|\; h \text{ is a FSSF}\Big\}\,.$$

Use $\operatorname{FFS}(\mathcal{C}\to\mathsf{F})$ for the set of Fncs-of-Finite-Support from $\mathcal{C}$ to F. □

2: Uniqueness Lemma. *Given a linearly-independent collection $\mathcal{C}\subset\mathbf{V}$ and $\mathbf{w}\in\operatorname{Spn}(\mathcal{C})$, there is a unique $h\in\operatorname{FFS}(\mathcal{C}\to\mathsf{F})$ with $\big[\sum_{\mathbf{u}\in\mathcal{C}} h(\mathbf{u})\cdot\mathbf{u}\big] = \mathbf{w}$.* ♢

Pf. Suppose $\sum_{\mathbf{u}\in\mathcal{C}} f(\mathbf{u})\mathbf{u} = \mathbf{w} = \sum_{\mathbf{u}\in\mathcal{C}} g(\mathbf{u})\mathbf{u}$ for two FFS. Thus

$$\vec{\mathbf{0}} \;=\; \mathbf{w}-\mathbf{w} \;\overset{\text{steps}}{=\!=}\; \sum_{\mathbf{u}\in\mathcal{C}} [f-g](\mathbf{u})\cdot\mathbf{u}$$

As, $\operatorname{Supp}(f-g)\subset\operatorname{Supp}(f)\cup\operatorname{Supp}(g)$, our $f-g$ is a FFS. Thus LI of $\mathcal{C}$ forces $f-g \overset{\text{identically}}{=\!=\!=} 0$. ♦

3: Basis ∃ence. *Each finite dim'al VS has a finite basis.* ♢

Proof. Fix a finite generating-set $\mathcal{C}$. If no $\mathbf{u}\in\mathcal{C}$ lies in $\operatorname{Spn}(\mathcal{C}\smallsetminus\{\mathbf{u}\})$, then $\mathcal{C}$ is LI; done.

Else: Remove $\mathbf{u}$ from $\mathcal{C}$. *Wash, rinse, repeat....* ♦

4a: Vec-replacement thm. *Fix a set $\mathcal{G}$ generating $\mathbf{V}$, with $\Gamma := |\mathcal{G}|$ finite. Then each LI-set L satisfies that $\Lambda := |L| \leq \Gamma$. Further, there exists a cardinality $\Gamma-\Lambda$ subset $H\subset\mathcal{G}$ such that $L\cup H$ generates $\mathbf{V}$.* ♢

Pf. For $\Lambda=0$, let $H:=\mathcal{G}$. Assuming the proposition for natnum Λ, we establish it for $\Lambda+1$.

Fix LI-set $L=\{\mathbf{v}_1,\dots,\mathbf{v}_\Lambda,\mathbf{v}_{\Lambda+1}\}$. Automatically $\widehat{L}=\{\mathbf{v}_1,\dots,\mathbf{v}_\Lambda\}$ is LI, whence the induc.hyp gives $\boxed{\Lambda\leq\Gamma}$. Letting $D:=\Gamma-\Lambda$ be the difference, there exists a cardinality-D subset $\widehat{H}:=\{\mathbf{g}_1,\dots,\mathbf{g}_D\}\subset\mathcal{G}$ with $\widehat{L}\cup\widehat{H}$ generating $\mathbf{V}$. In particular,

$$\dagger:\qquad \mathbf{v}_{\Lambda+1} \;=\; \Big[\sum_{j=1}^{\Lambda}\alpha_j\mathbf{v}_j\Big] + \Big[\sum_{k=1}^{D}\beta_k\mathbf{g}_k\Big]\,,$$

for some scalars $\alpha_1,\dots,\alpha_\Lambda$, $\beta_1,\dots,\beta_D$. Thus *some* β_k is non-zero [else $\mathbf{v}_{\Lambda+1}$ lies in $\operatorname{Spn}(\widehat{L})$, ※], whence $D\geq 1$ and WLOG $\beta_1\neq 0$. Happily, then, $\Lambda+1\leq\Gamma$ since $D\geq 1$.

Let $H:=\{\mathbf{g}_2,\mathbf{g}_3,\dots,\mathbf{g}_D\}$. Rewriting (†) as

$$\ddagger:\quad \mathbf{g}_1 \;=\; \frac{1}{\beta_1}\Big[\mathbf{v}_{\Lambda+1} - \Big[\sum_{j=1}^{\Lambda}\alpha_j\mathbf{v}_j\Big] - \Big[\sum_{k=2}^{D}\beta_k\mathbf{g}_k\Big]\Big]$$

shows that $\mathbf{g}_1\in\operatorname{Spn}(L\cup H)$. Thus

$$\operatorname{Spn}(L\cup H) \;=\; \operatorname{Spn}(L\cup\widehat{H}) \supset \operatorname{Spn}(\widehat{L}\cup\widehat{H})\,,$$

since $L\supset\widehat{L}$. Hence, $\boxed{\operatorname{Spn}(L\cup H)\text{ equals }\mathbf{V}.}$ ♦

4b: Corollary. *In finite dim'al VS $\mathbf{V}$, all bases have the same (finite) cardinality.* ♢

Proof. Courtesy (3), our $\mathbf{V}$ *has* a finite basis, hence has a basis $\mathcal{B}$ of minimum cardinality.

Consider another (possbily infinite) basis $\mathcal{E}$. Since $\mathcal{B}$ generates, and $\mathcal{E}$ is LI, our (4a) [the Vec-replacement thm] applies to say that $|\mathcal{E}|\leq|\mathcal{B}|$.

Reversing roles shows $|\mathcal{E}|=|\mathcal{B}|$. ♦

5: Gen. Basis thm. *Assuming the* AXIOM OF CHOICE, *every VS (whether finite-dim'al or not) admits a basis, and each two bases have the same cardnality.* ♢

Defn: Linear and Affine maps

(Here)

Defn. Over F, the ***affine-span*** of vector-set $\{\mathbf{v}_1, ..., \mathbf{v}_N\}$ is

$$\text{AffSpn}(\mathbf{v}_1, \ldots, \mathbf{v}_N) := \Big\{ \sum_{j=1}^{N} \alpha_j \mathbf{v}_j \;\Big|\; \begin{matrix}\text{Each } \alpha_j \in \mathsf{F} \text{ with} \\ \big[\sum_{j=1}^{N} \alpha_j\big] = 1\end{matrix} \Big\}.$$

To emphasise that a (affine-)span is wrt a particular field F, I might write, e.g, $\text{AffSpn}_{\mathbb{C}}$ or $\text{Spn}_{\mathbb{Q}}$ or $\text{Spn}_{\mathbb{Z}_5}$.

The affine-span of just a *pair* of vectors is

$$\text{Line}(\mathbf{u}, \mathbf{w}) := \{\alpha\mathbf{u} + [1-\alpha]\mathbf{w} \mid \alpha \in \mathsf{F}\}.$$

The "***dimension*** *of an affine-subspace* $\mathbf{A} \subset \mathbf{V}$" is the dimension of the vector-subspace were $\mathbf{A}$ translated to pass through the origin. That is, picking any vector $\mathbf{u} \in \mathbf{A}$: $\text{Dim}(\mathbf{A}) := \text{Dim}(\mathbf{A} - \mathbf{u})$.

A ***flat*** is another name for an affine-subspce.

A map $\mathsf{A}\colon \mathbf{V} \to \mathbf{X}$ between VSes is ***affine*** if it respects *averages*. That is, for all $\sum_{j=1}^{N} \alpha_j \mathbf{v}_j$, we have that

$$\mathsf{A}\Big(\sum_{j=1}^{N} \alpha_j \mathbf{v}_j\Big) = \sum_{j=1}^{N} \alpha_j \mathsf{A}(\mathbf{v}_j)$$

whenever $\big[\sum_{j=1}^{N} \alpha_j\big] = 1.$ □

6: Lemma. *Suppose* $\mathsf{A}\colon \mathbf{V} \to \mathbf{X}$ *is affine. Then* A *is* linear *IFF* $\mathsf{A}(\vec{\mathbf{0}}_{\mathbf{V}}) = \vec{\mathbf{0}}_{\mathbf{X}}$. ◊

Proof. For scalar β and vector $\mathbf{v}$, note

$$\begin{aligned}\mathsf{A}(\beta\mathbf{v}) &= \mathsf{A}\Big(\beta\mathbf{v} + [1-\beta]\cdot\vec{\mathbf{0}}_{\mathbf{V}}\Big) \\ &\overset{\text{affine}}{=\!=} \beta\mathsf{A}(\mathbf{v}) + [1-\beta]\cdot\mathsf{A}(\vec{\mathbf{0}}_{\mathbf{V}}) \\ &= \beta\mathsf{A}(\mathbf{v}) + [1-\beta]\cdot\vec{\mathbf{0}}_{\mathbf{X}} = \beta\,\mathsf{A}(\mathbf{v}).\end{aligned}$$

For vector sums, note

$$\begin{aligned}\tfrac{1}{2}\mathsf{A}(\mathbf{u}+\mathbf{w}) &\overset{\text{by above}}{=\!=} \mathsf{A}(\tfrac{1}{2}[\mathbf{u}+\mathbf{w}]) = \mathsf{A}(\tfrac{1}{2}\mathbf{u} + \tfrac{1}{2}\mathbf{w}) \\ &\overset{\text{affine}}{=\!=} \tfrac{1}{2}\mathsf{A}(\mathbf{u}) + \tfrac{1}{2}\mathsf{A}(\mathbf{w}).\end{aligned}$$

Doubling shows that $\mathsf{A}(\mathbf{u}+\mathbf{w}) = \mathsf{A}(\mathbf{u}) + \mathsf{A}(\mathbf{w})$. ♦

Nullspace and Range

We examine forward/backward-images of subspaces. Below $\mathsf{T}\colon \mathbf{V} \to \mathbf{X}$ is a lin.map

7: Lemma. *For each subspace $\mathbf{U} \subset \mathbf{V}$, its **forward-image forward/inverse-image***

$$\mathsf{T}(\mathbf{U}) \;:=\; \{\mathsf{T}(u) \mid u \in \mathbf{U}\}$$

*is a vector-subspace (**VSS**) of $\mathbf{X}$.*

*For each subspace $\mathbf{Y} \subset \mathbf{X}$, its **inverse-image***

$$\mathsf{T}^{-1}(\mathbf{Y}) \;:=\; \{v \in \mathbf{V} \mid \mathsf{T}(v) \in \mathbf{Y}\}$$

is a vector-subspace of $\mathbf{V}$. *Proof.* Exercise. ◊

Nullity, Rank. The ***kernel*** or ***nullspace*** of T is the inverse-image

$$\operatorname{Nul}(\mathsf{T}) \;:=\; \mathsf{T}^{-1}(\{\vec{0}_{\mathbf{X}}\}) \;=\; \mathsf{T}^{-1}(\mathbf{0}_{\mathbf{X}}).$$

$$\textit{And} \quad \operatorname{Nullity}(\mathsf{T}) \;:=\; \operatorname{Dim}(\operatorname{Nul}(\mathsf{T}))\,.$$

So the ***nullity*** of T is a cardinality.

The ***rank*** of T is cardinality

$$\operatorname{Rank}(\mathsf{T}) \;:=\; \operatorname{Dim}(\operatorname{Range}(\mathsf{T}))\,, \quad \textit{where}$$
$$\operatorname{Range}(\mathsf{T}) \;:=\; \mathsf{T}(\mathbf{V})\,.$$ □

8: R+N Theorem. *Over field* F, *a linear* $\mathsf{T}:\mathbf{V}\to\mathbf{X}$ *has*

$$\text{Rank}(\mathsf{T}) + \text{Nullity}(\mathsf{T}) \;=\; \text{Dim}(\text{Dom}(\mathsf{T})) \stackrel{\textit{note}}{=\!=} \text{Dim}(\mathbf{V}) \diamond$$

[*Many textbooks call this the* Rank+Nullity thm. *Our text calls it the* Dimension thm, 2.3.]

Prelim. Fix a basis $\mathcal{U} \subset \mathbf{V}$ for $\mathbf{U} := \text{Nul}(\mathsf{T}) \stackrel{\text{note}}{\subset} \mathbf{V}$, and a basis $\mathcal{R} \subset \mathbf{X}$ for $\mathbf{R} := \text{Range}(\mathsf{T}) \stackrel{\text{note}}{\subset} \mathbf{X}$.

For each $\mathbf{x}\in\mathcal{R}$, pick [*possibly using AC, if* $\mathbf{R}$ *is* ∞*-dim'al*] a vector $\mathbf{v_x} \in \mathbf{V}$ such that $\boxed{\mathsf{T}(\mathbf{v_x}) = \mathbf{x}}$. Let

$$\mathcal{Q} \;:=\; \left\{\mathbf{v_x} \;\middle|\; \mathbf{x}\in\mathcal{R}\right\}.$$

As $\mathsf{T}\!\downharpoonright_{\mathcal{Q}}$ is a bijection, $|\mathcal{Q}| = |\mathcal{R}|$. To establish

$$*: \qquad \text{Dim}(\mathbf{V}) \stackrel{?}{=} |\mathcal{Q}| + |\mathcal{U}|$$

is our goal.

If some vector $\mathbf{v_x} \in \mathcal{Q}$ also lay in $\mathbf{U}$-basis $\mathcal{U}$, then $\mathbf{x} \stackrel{\text{def}}{=\!=} \mathsf{T}(\mathbf{v_x}) = \vec{\mathbf{0}}_{\mathbf{X}}$; ※, as $\mathbf{x}$ is part of a basis [for $\mathbf{R}$], hence is *not* the zero-vector. Thus $\boxed{\mathcal{Q}\cap\mathcal{U} = \varnothing}$. So $(*)$ will follow from showing $\mathcal{Q}\sqcup\mathcal{U}$ is a $\mathbf{V}$-basis. □

Pf: $\mathcal{Q}\sqcup\mathcal{U}$ *is* LI. Consider FSSFs $g:\mathcal{Q}\to\mathsf{F}$ and $h:\mathcal{U}\to\mathsf{F}$ st.

$$\dagger: \qquad \vec{\mathbf{0}}_{\mathbf{V}} \;=\; \Big[\sum_{\mathbf{v_x}\in\mathcal{Q}} g(\mathbf{v_x})\,\mathbf{v_x}\Big] + \sum_{\mathbf{u}\in\mathcal{U}} h(\mathbf{u})\,\mathbf{u}\,.$$

Applying T to both sides,

$$\ddagger: \qquad \vec{\mathbf{0}}_{\mathbf{X}} \;=\; \Big[\sum_{\mathbf{x}\in\mathcal{R}} g(\mathbf{v_x})\,\mathbf{x}\Big] + \sum_{\mathbf{u}\in\mathcal{U}} h(\mathbf{u})\,\overbrace{\mathsf{T}(\mathbf{u})}^{=\vec{\mathbf{0}}_{\mathbf{X}}}.$$

Thus $\vec{\mathbf{0}}_{\mathbf{X}} = \sum_{\mathbf{x}\in\mathcal{R}} g(\mathbf{v_x})\,\mathbf{x}$. But $\mathcal{R}$ is LI, whence $g \equiv 0$.

Courtesy (†), $\vec{\mathbf{0}}_{\mathbf{V}} = \sum_{\mathbf{u}\in\mathcal{U}} h(\mathbf{u})\,\mathbf{u}$. Our $\mathcal{U}$ is linearly independent; consequently $h \equiv 0$. ♦

Pf: $\mathcal{Q}\sqcup\mathcal{U}$ *generates* $\mathbf{V}$. Fix an arbitrary vector $\mathbf{w}\in\mathbf{V}$. Since $\mathsf{T}(\mathbf{w}) \in \mathbf{R}$, there exists a FSSF $\varphi:\mathcal{R}\to\mathsf{F}$ st.

$$\mathsf{T}(\mathbf{w}) \;=\; \sum_{\mathbf{x}\in\mathcal{R}} \varphi(\mathbf{x})\,\mathbf{x}\,. \quad \textit{Define}$$

$$\mathbf{v_w} \;:=\; \sum_{\mathbf{v_x}\in\mathcal{Q}} \varphi(\mathbf{x})\,\mathbf{v_x} \stackrel{\text{note}}{\in} \text{Spn}(\mathcal{Q})\,.$$

Difference $\mathbf{w}-\mathbf{v_w}$ is in $\text{Nul}(\mathsf{T})$, since $\mathsf{T}(\mathbf{w}-\mathbf{v_w})$ equals

$$\mathsf{T}(\mathbf{w}) - \mathsf{T}(\mathbf{v_w}) \;=\; \Big[\sum_{\mathbf{x}\in\mathcal{R}} \varphi(\mathbf{x})\,\mathbf{x}\Big] - \sum_{\mathbf{x}\in\mathcal{R}} \varphi(\mathbf{x})\,\mathbf{x}\,.$$

As $\mathbf{w}$ equals $\mathbf{v_w} + [\mathbf{w}-\mathbf{v_w}]$, it follows that $\mathbf{w}$ lies in $\text{Spn}(\mathcal{Q}\cup\mathcal{U})$, as claimed. ♦

Matrices from vectors & lin.maps

Consider linear-maps $\mathbf{W} \xleftarrow{\mathsf{T}} \mathbf{V} \xleftarrow{\mathsf{S}} \mathbf{U}$ where the VSes have ordered bases $\mathcal{W} = (\mathbf{w}_1, ..., \mathbf{w}_4)$, $\mathcal{V} = (\mathbf{v}_1, ..., \mathbf{v}_7)$, $\mathcal{U} = (\mathbf{u}_1, ..., \mathbf{u}_3)$, respectively. A vector $\mathbf{q} \in \mathbf{U}$ has a unique description $\mathbf{q} = \sum_{i=1}^{3} \alpha_i \mathbf{u}_i$ Let $[\mathbf{q}]^{\mathcal{U}}$ be the *colvec of* $\mathbf{q}$ *w.r.t* $\mathcal{U}$, i.e

$$[\mathbf{q}]^{\mathcal{U}} := \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{bmatrix}.$$

Our text uses a subscript, $[\mathbf{q}]_{\mathcal{U}}$, rather than a superscript; please *use the superscript in your essays.*

Use $[\![\mathsf{S}]\!]_{\mathcal{U}}^{\mathcal{V}}$ for the 7×3 matrix M whose lefthand-action, L_{M}, equals S. Thus:

For $\mathrm{j} = 1, 2, 3$*: The* j^{th}*-column of* M *is* $[\mathsf{S}(\mathbf{u}_j)]^{\mathcal{V}}$.

ITOf scalars $\alpha_{i,j}$, writing $\mathsf{S}(\mathbf{u}_j) = \sum_{i=1}^{7} \alpha_{i,j} \mathbf{v}_i$ gives

$$[\![\mathsf{S}]\!]_{\mathcal{U}}^{\mathcal{V}} = \begin{bmatrix} \alpha_{1,1} & \alpha_{1,2} & \alpha_{1,3} \\ \alpha_{2,1} & \alpha_{2,2} & \alpha_{2,3} \\ \vdots & \vdots & \vdots \\ \alpha_{7,1} & \alpha_{7,2} & \alpha_{7,3} \end{bmatrix} \stackrel{\text{Nota}}{=\!=} \big[\alpha_{i,j}\big]_{\substack{i=1,...,7 \\ j=1,...,3}}.$$

9: Lemma. *Using the above notation,*

$$[\mathsf{S}(\mathbf{q})]^{\mathcal{V}} = [\![\mathsf{S}]\!]_{\mathcal{U}}^{\mathcal{V}} \cdot [\mathbf{q}]^{\mathcal{U}}, \text{ for each } \mathbf{q} \in \mathbf{U}.$$

$$\text{And} \quad [\![\mathsf{T} \circ \mathsf{S}]\!]_{\mathcal{U}}^{\mathcal{W}} = [\![\mathsf{T}]\!]_{\mathcal{V}}^{\mathcal{W}} \cdot [\![\mathsf{S}]\!]_{\mathcal{U}}^{\mathcal{V}}.$$

Proof. Exercise: Chase definitions. ◊

Remark. For lin.maps, henceforth, I'll typically write TS rather than $\mathsf{T} \circ \mathsf{S}$. A consequence of the above lemma is that $\underbrace{[[\mathsf{TS}](\mathbf{q})]^{\mathcal{W}}}_{4\times1} = \underbrace{[\![\mathsf{T}]\!]_{\mathcal{V}}^{\mathcal{W}}}_{4\times7} \cdot \underbrace{[\![\mathsf{S}]\!]_{\mathcal{U}}^{\mathcal{V}}}_{7\times3} \cdot \underbrace{[\mathbf{q}]^{\mathcal{U}}}_{3\times1}$. □

Inverses. On a set Ω, the ***identity map*** $Id_\Omega : \Omega \to \Omega$ is defined by $Id_\Omega(x) = x$, for each $x \in \Omega$.

The identity map on a VS $\mathbf{V}$ is a lin.trn, so I'll usually write it as either $Id_{\mathbf{V}}$ or $\mathbf{I}_{\mathbf{V}}$

The "$n \times n$ ***identity matrix***", written $\mathbf{I}_{n\times n}$ or $\mathbf{I}_n$ or [if n is understood] as just $\mathbf{I}$, is

$$\mathbf{I}_{n\times n} := \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix};$$

all zeros, except for ones down the main diagonal.

Consider a lin.maps $\mathsf{T} : \mathbf{V} \to \mathbf{W}$ and $\mathsf{L}, \mathsf{R} : \mathbf{W} \to \mathbf{V}$. This R is a *RInverse* [***righthand inverse***] of T, if $\mathsf{TR} = \mathbf{I}_{\mathbf{W}}$. And R is a *LInverse* of T, if $\mathsf{LT} = \mathbf{I}_{\mathbf{V}}$.

Multiple one-sided inverses. Let $\mathbf{X} := \mathbb{R}^{\mathbb{N}}$, the VS of seqs. $\vec{\mathbf{x}} = (x_0, x_1, \dots)$. The ***left-shift*** and ***right-shift*** lin.trns are

$$\mathsf{S}_{\mathrm{L}}(\vec{\mathbf{c}}) := (c_1, c_2, c_3, c_4, c_5, \dots) \quad \textit{and}$$
$$\mathsf{S}_{\mathrm{R}}(\vec{\mathbf{a}}) := (0, a_0, a_1, a_2, a_3, \dots)$$

As $\mathsf{S}_{\mathrm{L}}\mathsf{S}_{\mathrm{R}} = \mathbf{I}_{\mathbf{X}}$, our S_{R} is a RInverse of S_{L}. Indeed, S_{L} has ∞ly-many RInverses; another one is

$$\vec{\mathbf{a}} \mapsto (8a_7 - 5a_3, a_0, a_1, a_2, a_3, \dots).$$

Our S_{R} has ∞ly many LInverses; S_{L}, but also, e.g

$$\vec{\mathbf{c}} \mapsto (c_1 + 4c_0, c_2, c_3 - 6c_0, c_4, c_5, \dots).$$ □

10a: **Observation.** *Suppose $T: \mathbf{V} \to \mathbf{W}$ has at least one LInverse L, and at least one RInverse R. Then $L = R$, and there are no other one-sided inverses.* ◊

Pf. Note $L = L\,\mathbf{I}_{\mathbf{W}} = L\,[TR] \stackrel{\text{assoc.}}{=\!=} [LT]R = \mathbf{I}_{\mathbf{V}}\,R = R$. Were Λ another LInverse of T, then $\Lambda = R = L$. ♦

10b: *Aside:* The above argument applies to an arbitrary associative binary-operator [a ***binop***] with a 2-sided identity element. [Such a structure is called a ***monoid***.] □

10c: *Matrix inverse.* A 2-sided (multiplicative)-***inverse*** of $n{\times}n$ matrix M, is an $n{\times}n$ matrix U s.t $MU = \mathbf{I} = UM$. The forgoing shows that this U is unique; we write M^{-1} for the matrix-inverse of M.

For the next example, we define the ***determinant*** of 2×2-matrix $M := \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ as $\text{Det}(M) := ad - bc$. □

10d: **Fact.** *Matrix $M := \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is invertible exactly when $\Delta := \text{Det}(M)$ is non-zero. When that occurs,*

$$M^{-1} = \frac{1}{\Delta} \cdot \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \begin{bmatrix} d/\Delta & -b/\Delta \\ -c/\Delta & a/\Delta \end{bmatrix}.$$

Proof. Multiply and check. ◊

Matrix-inv 1. Real-matrix $T := \begin{bmatrix} 2 & 5 \\ 3 & 4 \end{bmatrix}$ has determinant $\text{Det}(T) = 2{\cdot}4 - 5{\cdot}3 = -7$. Whence

$$T^{-1} = \frac{1}{-7} \cdot \begin{bmatrix} 4 & -5 \\ -3 & 2 \end{bmatrix} \stackrel{\text{note}}{=\!=} \begin{bmatrix} -4/7 & 5/7 \\ 3/7 & -2/7 \end{bmatrix}.$$ □

Matrix-inv 2. We now work over field $F := \mathbb{Z}_{11}$, and let $\equiv$ mean $\equiv_{11}$. The $\mathbb{Z}_{11}$ reciprocal-table is

x	$\langle 1/x \rangle_{11}$	x	$\langle 1/x \rangle_{11}$
± 1	± 1		
± 2	∓ 5	± 4	± 3
± 3	± 4	± 5	∓ 2

Now $\mathbb{Z}_{11}$-matrix $M := \begin{bmatrix} 2 & 5 \\ 3 & 4 \end{bmatrix}$ has

$$\text{Det}(M) \equiv 2{\cdot}4 - 5{\cdot}3 = -7 \equiv 4.$$

Hence $\langle 1/\text{Det}(M) \rangle_{11} \equiv 3$.
Thus

$$M^{-1} \equiv 3 \cdot \begin{bmatrix} 4 & -5 \\ -3 & 2 \end{bmatrix} = \begin{bmatrix} 12 & -15 \\ -9 & 6 \end{bmatrix} \equiv \begin{bmatrix} 1 & -4 \\ 2 & -5 \end{bmatrix}.$$

Note: APPENDIX B in these notes has reciprocal-tables for various primes. *And*... you can always compute mod-N reciprocals *yourself*, using LIGHTNING-BOLT (the Euclidean algorithm). □

Change-of-basis matrix

The common case is two bases $\mathcal{E}$ and $\mathcal{B}$ on $\mathbf{V}$. A $\mathbf{u}\in\mathbf{V}$ engenders a colvec $[\mathbf{u}]^{\mathcal{E}}$, but we need $\mathbf{u}$ written ITOf basis $\mathcal{B}$. What we need is the ***change-of-basis*** [**CoB**] matrix $\mathsf{H} := [\![Id]\!]^{\mathcal{B}}_{\mathcal{E}}$, since

$$[\mathbf{u}]^{\mathcal{B}} = [\![Id]\!]^{\mathcal{B}}_{\not{\mathcal{E}}} \cdot [\mathbf{u}]^{\not{\mathcal{E}}} = \mathsf{H}\cdot[\mathbf{u}]^{\mathcal{E}}.$$

Similarly, consider $\mathbf{V} \xleftarrow{\mathsf{S}} \mathbf{V}$ and its matrix $\mathsf{M} := [\![\mathsf{S}]\!]^{\mathcal{E}}_{\mathcal{E}}$. *Alas*, we need S w.r.t $\mathcal{B}$. And indeed

$$\dagger\text{:}\quad [\![\mathsf{S}]\!]^{\mathcal{B}}_{\mathcal{B}} = \underbrace{\mathsf{H}\,\mathsf{M}\,\mathsf{H}^{-1}}_{\text{Conjugating }\mathsf{M}\text{ by }\mathsf{H}} = [\![Id]\!]^{\mathcal{B}}_{\not{\mathcal{E}}}\cdot[\![\mathsf{S}]\!]^{\not{\mathcal{E}}}_{\not{\mathcal{E}}}\cdot[\![Id]\!]^{\not{\mathcal{E}}}_{\mathcal{B}}$$
$$= [\![Id\circ\mathsf{S}\circ Id]\!]^{\mathcal{B}}_{\mathcal{B}} = [\![\mathsf{S}]\!]^{\mathcal{B}}_{\mathcal{B}}.$$

CoB example. On $\mathbb{R}^2$, consider (ordered-)bases

$$*\text{:}\quad \mathcal{E} = \Big(\overbrace{\begin{bmatrix}1\\0\end{bmatrix}}^{\mathbf{e}_1}, \overbrace{\begin{bmatrix}0\\1\end{bmatrix}}^{\mathbf{e}_2}\Big) \quad\textit{and}\quad \mathcal{B} = \Big(\overbrace{\begin{bmatrix}1\\-1\end{bmatrix}}^{\mathbf{b}_1}, \overbrace{\begin{bmatrix}-1\\2\end{bmatrix}}^{\mathbf{b}_2}\Big),$$

and matrix $\mathsf{M} := \begin{bmatrix}-5 & -3\\12 & 7\end{bmatrix}$. We seek to understand the lefthand action of M, the lin.trn $\mathsf{S} := \mathsf{L}_{\mathsf{M}}$, and some nice person has told us that S's mapping is clearer in the $\mathcal{B}$ basis.

As $(*)$ gives $\mathcal{B}$ ITOf $\mathcal{E}$, e.g, $\mathbf{b}_2 = [-1]\mathbf{e}_1 + 2\mathbf{e}_2$, the easy matrix to compute is $\mathsf{C} := [\![Id]\!]^{\mathcal{E}}_{\mathcal{B}}$. *Why?* The first column of C is

$$\mathsf{C}\cdot\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right] \overset{\text{meaning}}{=\!=\!=} [\![Id]\!]^{\mathcal{E}}_{\not{\mathcal{B}}}\cdot[\mathbf{b}_1]^{\not{\mathcal{B}}} = [Id(\mathbf{b}_1)]^{\mathcal{E}} = \begin{bmatrix}1\\-1\end{bmatrix}.$$

It follows that

$$\mathsf{C} = [\![Id]\!]^{\mathcal{E}}_{\mathcal{B}} = \begin{bmatrix}1 & -1\\-1 & 2\end{bmatrix} \quad\textit{whence}\quad \mathsf{C}^{-1} = [\![Id]\!]^{\mathcal{B}}_{\mathcal{E}} = \begin{bmatrix}2 & 1\\1 & 1\end{bmatrix},$$

<u>*since* $\mathrm{Det}(\mathsf{C}) = 1$</u>.

Applying (†), our $[\![\mathsf{S}]\!]^{\mathcal{B}}_{\mathcal{B}} = \mathsf{C}^{-1}\mathsf{M}\,\mathsf{C}$, i.e,

$$\begin{bmatrix}2 & 1\\1 & 1\end{bmatrix}\begin{bmatrix}-5 & -3\\12 & 7\end{bmatrix}\begin{bmatrix}1 & -1\\-1 & 2\end{bmatrix} = \begin{bmatrix}2 & 1\\1 & 1\end{bmatrix}\overbrace{\begin{bmatrix}-2 & -1\\5 & 2\end{bmatrix}}^{\mathsf{M}\cdot\mathsf{C}}$$
$$= \begin{bmatrix}1 & 0\\3 & 1\end{bmatrix},$$

a shear in the $\mathbf{b}_2$ direction. Specifically, $\mathsf{S}(\mathbf{b}_2) = \mathbf{b}_2$ and $\mathsf{S}(\mathbf{b}_1) = \mathbf{b}_1 + 3\mathbf{b}_2$. [So $\mathbf{b}_2$ is a ***Fixed-point*** *of* S. Later, we'll call $\mathbf{b}_2$ an S-*eigenvector* with *eigenvalue* 1.]

Checking! using S and $\mathbf{b}_1$,$\mathbf{b}_2$, all expressed in the $\mathcal{E}$ basis:

$$[\mathsf{S}(\mathbf{b}_2)]^{\mathcal{E}} = \mathsf{M}\cdot\begin{bmatrix}-1\\2\end{bmatrix} = \begin{bmatrix}-1\\2\end{bmatrix} = [\mathbf{b}_2]^{\mathcal{E}}, \quad\textit{and}$$

$$[\mathsf{S}(\mathbf{b}_1)]^{\mathcal{E}} = \mathsf{M}\cdot\begin{bmatrix}1\\-1\end{bmatrix} = \begin{bmatrix}-2\\5\end{bmatrix} \overset{\text{note}}{=\!=} \begin{bmatrix}1\\-1\end{bmatrix} + 3\begin{bmatrix}-1\\2\end{bmatrix}$$

which indeed equals $[\mathbf{b}_1 + 3\mathbf{b}_2]^{\mathcal{E}}$. So that ✓s out. □

...continuing. Given vector $\begin{bmatrix} -5 \\ 2 \end{bmatrix} = [\mathbf{u}]^{\mathcal{E}}$, we can write this same vector in basis $\mathcal{B}$ as:

$$[\mathbf{u}]^{\mathcal{B}} = \underbrace{[\![Id]\!]^{\mathcal{B}}_{\mathcal{E}}}_{\mathsf{C}^{-1}} \cdot [\mathbf{u}]^{\mathcal{E}} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} -5 \\ 2 \end{bmatrix} = \begin{bmatrix} -8 \\ -3 \end{bmatrix}. \square$$

CoB generalized. A less common usage of CoB matrices is comes from a lin.map $\mathbf{W} \xleftarrow{\mathsf{T}} \mathbf{V}$ and ordered-bases $\mathcal{W}, \mathcal{W}'$ for $\mathbf{W}$, as well as ordered-bases $\mathcal{V}, \mathcal{V}'$ for $\mathbf{V}$.

$$\mathsf{M} := [\![\mathsf{T}]\!]^{\mathcal{W}}_{\mathcal{V}} \quad \textit{and} \quad \mathsf{M}' := [\![\mathsf{T}]\!]^{\mathcal{W}'}_{\mathcal{V}'}.$$

If we know the bases and M, you can compute M' as product

$$\mathsf{M}' = [\![Id]\!]^{\mathcal{W}'}_{\mathcal{W}} \cdot \mathsf{M} \cdot [\![Id]\!]^{\mathcal{V}}_{\mathcal{V}'} = [\![Id]\!]^{\mathcal{W}'}_{\cancel{\mathcal{W}}} \cdot [\![\mathsf{T}]\!]^{\cancel{\mathcal{W}}}_{\cancel{\mathcal{V}}} \cdot [\![Id]\!]^{\cancel{\mathcal{V}}}_{\mathcal{V}'}$$
$$= [\![Id \circ \mathsf{T} \circ Id]\!]^{\mathcal{W}'}_{\mathcal{V}'} = [\![\mathsf{T}]\!]^{\mathcal{W}'}_{\mathcal{V}'}.$$

Examples of Subspaces

Over of field F, consider a lin.map $\mathsf{S}:\mathbf{X}\to\mathbf{V}$ and subspaces $\mathbf{X}_0 \subset \mathbf{X}$ and $\mathbf{V}_0 \subset \mathbf{V}$. Then

Forward-image $\mathsf{S}(\mathbf{X}_0)$ *is a* $\mathbf{V}$*-subspace. And inverse-image* $\mathsf{S}^{-1}(\mathbf{V}_0) := \left\{\mathbf{y}\in\mathbf{X} \;\middle|\; \mathsf{S}(\mathbf{y})\in\mathbf{V}_0\right\}$ *is an* $\mathbf{X}$*-subspace.*

In particular, $\mathrm{Nul}(\mathsf{S}) := \mathsf{S}^{-1}(\mathbf{0}_{\mathbf{V}})$ is a subspace of $\mathrm{Dom}(\mathsf{S})$.

We now consider a lin.trn $\mathsf{T}:\mathbf{X}\circlearrowleft$ mapping a space to *itself*.

Invariant subspaces of $\mathsf{T}:\mathbf{X}\to\mathbf{X}$. Subspace $\mathbf{U}\subset\mathbf{X}$ is T-***invariant*** if $\mathsf{T}(\mathbf{U}) \subset \mathbf{U}$. This allows the defn of ***restriction*** $\mathsf{R} := \mathsf{T}\!\downharpoonright_{\mathbf{U}}$ which is a lin.trn $\mathsf{R}:\mathbf{U}\to\mathbf{U}$.

If $\mathsf{T}(\mathbf{U}) = \mathbf{U}$, we'll say that $\mathbf{U}$ is "*precisely*-T-*invariant*". [Textbooks differ in terminology for this.]

11: Lemma. *Suppose $\mathcal{C}$ is a collection (possibly infinite) of T-invariant subspaces. Then*

$$\bigcap(\mathcal{C}) \stackrel{\text{def}}{=} \bigcap_{\mathbf{U}\in\mathcal{C}} \mathbf{U}$$

is a T-invariant subspace. *Proof.* Exercise. ◊

Ex: Range. Set $\mathbf{U}_0 := \mathbf{X}$, and $\mathbf{U}_{n+1} := \mathsf{T}(\mathbf{U}_n)$. [So $\mathrm{Range}(\mathsf{T}) \stackrel{\text{def}}{=} \mathbf{U}_1$.] Then $\mathbf{U}_0 \supset \mathbf{U}_1 \supset \mathbf{U}_2 \supset \cdots$, and each $\mathbf{U}_n$ is T-invariant. Moreover,

$$\mathbf{U}_\infty := \bigcap_{n=0}^{\infty} \mathbf{U}_n$$

is also T-invariant. Evidently, if $\mathbf{X}$ is finite dim'al then $\mathbf{U}_\infty$ is *precisely*-T-*invariant*. (Posting decathlon. Prove or give CEX: "Even when $\mathrm{Dim}(\mathbf{X}) = \infty$, intersection $\mathbf{U}_\infty$ must be *precisely*-T-*invariant*.")

Fixed-pt subspace. For an arbitrary map $h:\Omega\circlearrowleft$ on an arbitrary set, define

$$\mathrm{Fix}(h) := \{\alpha\in\Omega \mid h(\alpha)=\alpha\},$$

the set of "***fixed-points*** of h".

When $\mathsf{T}:\mathbf{X}\circlearrowleft$ is *linear*, then $\mathrm{Fix}(\mathsf{T})$ is <u>the</u> (full) "***fixed-point*** ***<u>subspace</u>*** of T". This will later be called: "*The eigenspace of* T *with eigenvalue* 1."

Each subspace $\mathbf{U} \subset \mathrm{Fix}(\mathsf{T})$ is <u>a</u> "T-*fixed-pt subspace*"

Eigenspaces. Fix an element $\lambda \in \mathsf{F}$. We have this important defn: *The "λ-**eigenspace** of* T*" is*

$$\{\mathbf{y}\in\mathbf{X} \mid \mathsf{T}(\mathbf{y}) = \lambda\cdot\mathbf{y}\}.$$

Examples of transformations

[Before starting, consider a map $h{:}\Omega\to\Omega$ on a set Ω. Then "h is an ***involution***" if $h\circ h = Id_\Omega$. In contrast, "h is ***idempotent***" if $h\circ h = h$.]

2-dim rotations. On $\mathbb{R}\times\mathbb{R}$, *rotation* matrix

$$\mathsf{R}_\theta := \begin{bmatrix}\cos(\theta) & -\sin(\theta)\\ \sin(\theta) & \cos(\theta)\end{bmatrix}.$$

rotates the plane CCW by angle θ. Note $\mathsf{R}_\theta^{-1} = \mathsf{R}_{-\theta}$. As examples, $[\mathsf{R}_{\pi/6}]^{12} = \mathbf{I} = [\mathsf{R}_{\pi/4}]^8$.

Projections, Reflections, Shears. Consider a direct-sum decomposition $\mathbf{X}\oplus\mathbf{U} = \mathbf{V}$. [I.e, $\mathbf{X},\mathbf{U}$ are *transverse* subspaces ($\mathbf{X}\cap\mathbf{U}=\mathbf{0}$) whose union generates $\mathbf{V}$.] When spaces are finite dim'al, $r := \mathrm{Dim}(\mathbf{X})$ and $n := \mathrm{Dim}(\mathbf{U})$, we'll use ordered-bases $\mathcal{X} := (\mathbf{x}_1,\dots,\mathbf{x}_r)$ and $\mathcal{U} := (\mathbf{u}_1,\dots,\mathbf{u}_n)$ and

¥: $$\mathcal{V} := (\mathbf{x}_1,\dots,\mathbf{x}_r,\mathbf{u}_1,\dots,\mathbf{u}_n).$$

Each projection, reflection, shear (see below) *fixes* $\mathbf{X}$ pointwise; so $\mathbf{X}$ is a pointwise-fiXed subspace, a subspace of $\mathrm{Fix}(\mathsf{T})$.

A *projection* $\mathsf{P}{:}\mathbf{V}\circlearrowleft$ uses that each $\mathbf{v}\in\mathbf{V}$ has a *unique* description as $\mathbf{v} = \mathbf{x}+\mathbf{u}$ with $\mathbf{x}\in\mathbf{X}$ and $\mathbf{u}\in\mathbf{U}$.
Define ***projection-onto-X***-parallel-to-**U** by

†: $$\mathsf{P}(\mathbf{v}) = \mathsf{P}(\mathbf{x}+\mathbf{u}) := \mathbf{x}. \qquad \textit{In contrast}$$
‡: $$\mathsf{H}(\mathbf{v}) = \mathsf{H}(\mathbf{x}+\mathbf{u}) := \mathbf{x} - \mathbf{u}$$

is ***reflection-across-X***-parallel-to-**U**.

12: Obs. *Suspose lin.trn $\mathsf{P}{:}\mathbf{V}\circlearrowleft$ is idempotent. Then P is projection onto $\mathbf{X} := \mathrm{Range}(\mathsf{P})$, projecting parallel to $\mathbf{U} := \mathrm{Nul}(\mathsf{P})$.* ◊

Pf Union $\mathbf{X}\cup\mathbf{U}$ generates $\mathbf{V}$. Fix $\mathbf{v}\in\mathbf{V}$ and define $\mathbf{x} := \mathsf{P}(\mathbf{v}) \in \mathbf{X}$ and $\mathbf{u} := \mathbf{v}-\mathbf{x}$. Since $\mathbf{v} = \mathbf{x}+\mathbf{u}$, we need but show that $\mathbf{u}$ is in $\mathrm{Nul}(\mathsf{P})$. Well...

$$\mathsf{P}(\mathbf{u}) \stackrel{\text{linearity}}{=\!=} \mathsf{P}(\mathbf{v}) - \mathsf{P}(\mathbf{x}) \stackrel{\text{def}}{=} \mathsf{P}(\mathbf{v}) - \mathsf{P}(\mathsf{P}(\mathbf{v})) \stackrel{\text{idem}}{=\!=} \mathsf{P}(\mathbf{v}) - \mathsf{P}(\mathbf{v}) \stackrel{\text{def}}{=} \vec{\mathbf{0}}.$$ ♦

Pf $\mathbf{X}\cap\mathbf{U} = \mathbf{0}$. Fix $\mathbf{x}\in\mathbf{X}\cap\mathbf{U}$; so there exists $\mathbf{v}\in\mathbf{V}$ with $\mathsf{P}(\mathbf{v}) = \mathbf{x}$. Thus

$$\vec{\mathbf{0}} \stackrel{\mathbf{x}\in\mathbf{U}}{=\!=} \mathsf{P}(\mathbf{x}) \stackrel{\text{def}}{=} \mathsf{P}(\mathsf{P}(\mathbf{v})) \stackrel{\text{idem}}{=\!=} \mathsf{P}(\mathbf{v}) \stackrel{\text{def}}{=} \mathbf{x}.$$ ♦

As a corollary, suppose $\mathbf{X}$ and $\mathbf{U}$ are finite dim'al. Then, wrt basis (¥), the projection and reflection matrices are diagonal. Specifically,

†∗: $$[\![\textit{Proj}\ \mathsf{P}]\!]_{\mathcal{V}}^{\mathcal{V}} = \begin{bmatrix}\mathbf{I}_{r\times r} & \\ & \mathbf{0}_{n\times n}\end{bmatrix} \quad \textit{and}$$

‡∗: $$[\![\textit{Refl}\ \mathsf{H}]\!]_{\mathcal{V}}^{\mathcal{V}} = \begin{bmatrix}\mathbf{I}_{r\times r} & \\ & -\mathbf{I}_{n\times n}\end{bmatrix}.$$

A *shear* $\mathsf{S}{:}\mathbf{V}\circlearrowleft$ is determined by $\mathbf{X}\oplus\mathbf{U} = \mathbf{V}$, *together with* a linear map $\mathsf{M}{:}\mathbf{U}\to\mathbf{X}$. Each $\mathbf{v}\in\mathbf{V}$ has a *unique* decomposition $\mathbf{v} = \mathbf{x}+\mathbf{u}$ with $\mathbf{x}\in\mathbf{X}$ and $\mathbf{u}\in\mathbf{U}$. The corresponding shear, S, is

‡‡: $$\mathsf{S}(\mathbf{v}) := \mathbf{v} + \mathsf{M}(\mathbf{u}) \stackrel{\text{note}}{=\!=} \overbrace{[\mathbf{x}+\mathsf{M}(\mathbf{u})]}^{\text{in }\mathbf{X}} + \overbrace{\mathbf{u}}^{\text{in }\mathbf{U}}.$$

Let $\mathsf{M}_{r\times n}$ denote matrix $[\![\mathsf{M}]\!]_{\mathcal{U}}^{\mathcal{X}}$. Then

‡‡∗: $$[\![\textit{Shear}\ \mathsf{S}]\!]_{\mathcal{V}}^{\mathcal{V}} = \begin{bmatrix}\mathbf{I}_{r\times r} & \mathsf{M}_{r\times n}\\ & \mathbf{I}_{n\times n}\end{bmatrix}.$$

Exercise: Prove that shear S is invertible, and

$$\mathsf{S}^{-1}(\mathbf{v}) := \mathbf{v} - \mathsf{M}(\mathbf{u}) = \underbrace{[\mathbf{x}-\mathsf{M}(\mathbf{u})]}_{\text{in }\mathbf{X}} + \underbrace{\mathbf{u}}_{\text{in }\mathbf{U}}.$$

Letting P be projection of $\mathbf{V}$ onto $\mathbf{U}$ parallel to $\mathbf{X}$, our shear can be written as $\mathsf{S} = \mathbf{I} + [\mathsf{M}\circ\mathsf{P}]$.

Nilpotent trns & matrices. An $n{\times}n$ matrix M is ***nilpotent*** if *there exists* natnum k with $\mathsf{M}^k = \mathbf{0}_{n\times n}$ (the 0-matrix). The *smallest* such k is the ***nilpotency degree*** of M, written $\mathrm{NilDeg}(\mathsf{M})$.

Analogously *lin.trn* $\mathsf{T}{:}\mathbf{V}\circlearrowleft$ is ***nilpotent*** if there exists natnum k with $\mathsf{T}^k = \mathbf{0}_{\mathtt{Trn}}$, etc.

13: Lem. *Suppose* $\mathsf{T}{:}\mathbf{V}\circlearrowleft$ *is nilpotent, and* $N := \mathrm{Dim}(\mathbf{V})$ *is finite. Then* $\mathrm{NilDeg}(\mathsf{T}) \le N$. [*Ditto for* $N{\times}N$ *matrices.*] ♢

Proof. Set $\mathbf{U}_0 := \mathbf{V}$ and, for $j = 1, 2, \ldots$, define $\mathbf{U}_{j+1} := \mathsf{T}(\mathbf{U}_j)$. Automatically $\mathbf{U}_1 \subset \mathbf{U}_0$. Hence

$$\cdots \subset \mathbf{U}_2 \subset \mathbf{U}_1 \subset \mathbf{U}_0\,,$$

since inclusion $\mathbf{U}_j \subset \mathbf{U}_{j-1}$ implies that $\mathsf{T}(\mathbf{U}_j) \subset \mathsf{T}(\mathbf{U}_{j-1})$, i.e that $\mathbf{U}_{j+1} \subset \mathbf{U}_j$.

Suppose, for $j = 1, 2, 3, \ldots$ up to some k, we have *proper* inclusion $\mathbf{U}_j \subsetneqq \mathbf{U}_{j-1}$. Then each

$$\mathrm{Dim}(\mathbf{U}_j) \;\le\; \mathrm{Dim}(\mathbf{U}_{j-1}) - 1\,,$$

so $\mathrm{Dim}(\mathbf{U}_k) \le \mathrm{Dim}(\mathbf{U}_0) - k = N - k$. Thus $k \le N$. And T is nilpotent IFF $\mathbf{U}_k = \mathbf{0}$. ♦

Gauss-Jordan, *RREF*

The Gauss-Jordan[♡1] algorithm does row-ops to convert a matrix into Reduced Row-Echelon-Form.

Row operations. Below, i and g are row-indices, and j and h are column-indices, and α, ρ are F-scalars. The three ***elementary row-operations*** are:

$\mathcal{A}_{i,\alpha:g}$: Add [row-i times α] to row-g. Inverse: $\mathcal{A}_{i,-\alpha:g}$.

$\mathcal{P}_\nu$: Permute the rows according to permutation ν. Inverse: $\mathcal{P}_{\nu^{-1}}$.

This is usually used to ...

$\mathcal{P}_{i\leftrightarrow g}$: ... exchange row-i and row-g. Inverse: $\mathcal{P}_{i\leftrightarrow g}$.

$\mathcal{U}_{i,\rho}$: M<u>**u**</u>ltiply row i by non-zero ρ. Inverse: $\mathcal{U}_{i,1/\rho}$:

14: *RREF algorithm.* With $M \in \mathrm{MAT}_{6\times 9}(F)$, use $m_{i,j}$ for the entry in row-i and column-j. I'll use the term ***pivot column*** and, for a non-pivot column, a ***free column***.

Init: Initialize row-counter $\mathcal{R} := 1$ and column-counter $\mathcal{C} := 1$. *Then ...*

NewCol: Is there an index $i \in [\mathcal{R} .. 6]$ with $m_{i,\mathcal{C}}$ non-zero?

IF "*no*" [so column-$\mathcal{C}$ is *free*] then Increment($\mathcal{C}$) and goto (**NewCol**).

ELSE, exchange one such row with row-$\mathcal{R}$, using $\mathcal{P}_{i\leftrightarrow\mathcal{R}}$. Now $m_{\mathcal{R},\mathcal{C}}$ is <u>*not*</u> zero, so let ρ be the reciprocal-in-F of $m_{\mathcal{R},\mathcal{C}}$. Apply $\mathcal{U}_{\mathcal{R},\rho}$; now $\boxed{m_{\mathcal{R},\mathcal{C}} = 1}$. And $(\mathcal{R},\mathcal{C})$ is a ***pivot position***.

ZeroizeCol: For each row-index $i \neq \mathcal{R}$ [greater or less than $\mathcal{R}$] with $\alpha := -m_{i,\mathcal{C}}$ non-zero, apply $\mathcal{A}_{\mathcal{R},\alpha:i}$. [So pivot-position $(\mathcal{R},\mathcal{C})$ now has the *only* non-zero entry in column-$\mathcal{C}$.] Now Increment($\mathcal{R}$) and Increment($\mathcal{C}$), then goto (**NewCol**). □

When is a matrix in RREF? In a $B = [b_{i,j}]_{i,j}$ matrix, row-i being NOTAZ means it is Not-All-Zero; let Col(i) be the column-index of its *leftmost* non-zero entry; thus $b_{i,\mathrm{Col}(i)}$ is the leftmost non-zero entry in row-i.

Our B *is in RREF* (***reduced row-echelon-form***) *if*

i: The NOTAZ rows are above the ALL-ZERO rows.

ii: With P denoting the number of NOTAZ rows, we have

$$\mathrm{Col}(1) < \mathrm{Col}(2) < \ldots < \mathrm{Col}(P).$$

iii: For $i = 1, \ldots, P$, the *only* non-zero entry in column Col(i) is at position $(i, \mathrm{Col}(i))$. Moreover $b_{i,\mathrm{Col}(i)} = 1$.

For $i = 1, 2, \ldots, P$, we call row-i a ***pivot row***, column Col(i) a ***pivot column***, and position $(i, \mathrm{Col}(i))$ a ***pivot position***.

The *RREF* of a matrix is unique. However, removing "reduced" gives **row-echelon-form**, and different textbooks have slightly varying definitions of REF. While *RREF* is unique, REF is *not* unique. Nonetheless, useful properties can be read-off from an REF of a matrix. □

[♡1] A version of Gaussian elimination was described by ***Wilhelm Jordan*** in 1888; —not to be confused with ***Camille Jordan***, who stated Jordan Canonical Form thm in 1870.

Row/Column Ops. Say that two $N \times K$ matrices A and B are ***row-equivalent***, written $\mathsf{A} \overset{r}{\sim} \mathsf{B}$, if we can get from A to B by a sequence of elem.row-ops.

Analogous, if we can get from A to B by elem.col-ops, then $\mathsf{A} \overset{c}{\sim} \mathsf{B}$, and the matrices are ***column-equivalent***.

An elem.**row**-op can be realized by multiplying from the *left* by a $N \times N$ matrix; to get this matrix, simply *apply the row-op to* $\mathbf{I}_{N \times N}$.

Similarly, an elem.**col**-op can be realized by multiplying from the *right* by a $K \times K$ matrix; etc.

Row-op invariants. Suppose $\mathsf{A} \overset{r}{\sim} \mathsf{B}$. Then

$$\begin{aligned} \mathrm{RowSpn}(\mathsf{A}) &= \mathrm{RowSpn}(\mathsf{B}) \\ \mathrm{LNul}(\mathsf{A}) &= \mathrm{LNul}(\mathsf{B}) \\ \mathrm{Rank}(\mathsf{A}) &= \mathrm{Rank}(\mathsf{B}), \end{aligned}$$

where **LNul** means the *nullspace of the lefthand-action of* A. [Statement $\mathrm{LNul}(\mathsf{A}) = \mathrm{LNul}(\mathsf{B})$ says that row-ops preserve the linear relations among columns.]

Row-ops...

...Preserve linear-relations among columns and *preserve* the span of rows [rowspan].

...Alter linear-relations among rows and *alter* the span of columns [colspan].

Obtaining bases. For $N \times K$ matrix M over field F, let $\mathbf{r}_1, \ldots, \mathbf{r}_N$ denote the rowvecs, and have $\mathbf{c}_1, \ldots, \mathbf{c}_K$ denote the colvecs.

In $\widehat{\mathsf{M}} := \mathit{RREF}(\mathsf{M})$, use $\widehat{\mathbf{r}_1}, \ldots, \widehat{\mathbf{r}_N}$ and $\widehat{\mathbf{c}_1}, \ldots, \widehat{\mathbf{c}_K}$ for the row and column vectors. Let P [$\leq \mathrm{Min}(N, K)$] denote the number of pivot-rows in $\widehat{\mathsf{M}}$. Then

a: $\mathrm{Rank}(\mathsf{M}) = \mathrm{Rank}(\widehat{\mathsf{M}}) = P$.

b: Rowvec-set $\{\widehat{\mathbf{r}_1}, \ldots, \widehat{\mathbf{r}_P}\}$ is a *basis* for $\mathrm{RowSpn}(\mathsf{M}) = \mathrm{RowSpn}(\widehat{\mathsf{M}})$.

c: Let $\mathrm{Col}(1), \ldots, \mathrm{Col}(P)$ denote the column-indices of the pivot-cols in $\widehat{\mathsf{M}}$. Then

$$\{\mathbf{c}_{\mathrm{Col}(1)}, \mathbf{c}_{\mathrm{Col}(2)}, \ldots, \mathbf{c}_{\mathrm{Col}(P)},\}$$

is a basis for $\mathrm{ColSpn}(\mathsf{M})$.

d: A basis for $\mathrm{LNul}(\mathsf{M}) = \mathrm{LNul}(\widehat{\mathsf{M}})$ is obtained via the method of ***back substitution***.

Basis for **$\mathrm{RNul}(\mathsf{M})$.** Here, let $\mathbf{e}_j$ be the $1 \times K$ *rowvec* which is all-zero, except for a 1 at position j. E.g $\mathbf{e}_2 = [010\ldots0]$.

Our $\widehat{\mathsf{M}}$ looks like

$$\begin{matrix} P \text{ many pivot rows} \\ \\ N-P \text{ many all-zero rows} \end{matrix} \begin{cases} \\ \\ \end{cases} \begin{bmatrix} 1 & 0 & 5 & \cdots & & \\ & 1 & 7 & \cdots & & \\ & & \vdots & \vdots & \vdots & \\ & & 1 & \cdots & \cdots & \\ 0 & 0 & & \cdots & & 0 \\ \vdots & \vdots & & \cdots & & \vdots \\ 0 & 0 & & \cdots & & 0 \end{bmatrix}.$$

Consequently, a basis for $\mathrm{RNul}(\widehat{\mathsf{M}})$ is the set of rowvecs $\mathbf{e}_j$, for $j \in (P\,..\,N]$.

Let L be the $N \times N$ invertible matrix that *RREF*s M to $\widehat{\mathsf{M}}$, i.e, $\mathsf{L}\mathsf{M} = \widehat{\mathsf{M}}$.

15: Lemma. *With notation from above: This set*

$$*: \quad \left\{\mathbf{e}_j \cdot \mathsf{L} \;\middle|\; j \in (P\,..\,N]\right\} = \left\{\begin{matrix}\textit{The bottom-most} \\ N-P \textit{ rows of } \mathsf{L}\end{matrix}\right\}$$

of rowvecs is a basis for $\mathrm{RNul}(\mathsf{M})$. ◊

LinA Equivalence relations. (Repeating some material): Two 5×7 matrices X and Y are ***row equivalent***, written $\mathsf{X} \stackrel{r}{\sim} \mathsf{Y}$, if X can be transformed to Y via elementary row-ops. Equivalently, $\exists \mathsf{L}_{5\times5}$ invertible such that $\mathsf{LX} = \mathsf{Y}$.

Matrices X,Y are ***column equivalent***, $\mathsf{X} \stackrel{c}{\sim} \mathsf{Y}$, if column-ops carry X to Y; equivalently, $\exists \mathsf{R}_{7\times7}$ invertible such that $\mathsf{XR} = \mathsf{Y}$.

Two $N{\times}N$ matrices P,Q are ***similar*** , or ***conjugate*** to each other,, written, $\mathsf{P} \stackrel{\text{sim}}{\sim} \mathsf{Q}$ if *there exists* invertible $\mathsf{C}_{N\times N}$ with $\mathsf{CPC}^{-1} = \mathsf{Q}$.

Looking ahead. Applied to a square matrix G, operation $\mathcal{A}$ does not affect determinant, and operation $\mathcal{P}_{\mathsf{i}\leftrightarrow\mathsf{g}}$ only multiplies it by -1. Use "$\mathsf{G} \stackrel{\mathcal{AP}}{\sim} \mathsf{H}$" to indicate that, using only row-ops $\mathcal{A}$ and $\mathcal{P}$, one can alter G to become H.

RREF example

Over field $\mathbb{Z}_{13}$ we have matrices $\overset{4\times 6}{\mathsf{M}}$ and "target" colvecs $\overset{4\times 1}{\mathsf{S}}$ and $\overset{4\times 1}{\mathsf{U}}$. We seek to find bases for:

RowSpn(M), ColSpn(M), LNul(M), RNul(M),

and describe the set of solns $\overset{6\times 1}{\mathsf{X}}$, *to* $\mathsf{MX} = \mathsf{S}$ *and* $\mathsf{MX} = \mathsf{U}$.

Our given M, S, U matrices are

$$\begin{bmatrix} -2 & -5 & 16 & 11 & 0 & -23 \\ -25 & 26 & 6 & -13 & 31 & -17 \\ -1 & -23 & -15 & 1 & 18 & -17 \\ 19 & -31 & 12 & 29 & 30 & -27 \end{bmatrix}, \begin{bmatrix} 29 \\ 3 \\ -30 \\ -31 \end{bmatrix}, \begin{bmatrix} 0 \\ 4 \\ 25 \\ -2 \end{bmatrix}.$$

Step 1. Produce an augmented matrix...

```
(setq A (mat-Horiz-concat M S U))
```

$$\left[\begin{array}{cccccc|cc} -2 & -5 & 16 & 11 & 0 & -23 & 29 & 0 \\ -25 & 26 & 6 & -13 & 31 & -17 & 3 & 4 \\ -1 & -23 & -15 & 1 & 18 & -17 & -30 & 25 \\ 19 & -31 & 12 & 29 & 30 & -27 & -31 & -2 \end{array}\right]$$

...and reduce A mod-13. Non-negative residues reduces A to

$$\left[\begin{array}{cccccc|cc} 11 & 8 & 3 & 11 & 0 & 3 & 3 & 0 \\ 1 & 0 & 6 & 0 & 5 & 9 & 3 & 4 \\ 12 & 3 & 11 & 1 & 5 & 9 & 9 & 12 \\ 6 & 8 & 12 & 3 & 4 & 12 & 8 & 11 \end{array}\right]$$

whereas *symmetric*-residues reduces A to

$$\left[\begin{array}{cccccc|cc} -2 & -5 & 3 & -2 & 0 & 3 & 3 & 0 \\ 1 & 0 & 6 & 0 & 5 & -4 & 3 & 4 \\ -1 & 3 & -2 & 1 & 5 & -4 & -4 & -1 \\ 6 & -5 & -1 & 3 & 4 & -1 & -5 & -2 \end{array}\right]$$

which has form $[\mathsf{M} \mid \mathsf{S}\ \mathsf{U}]$. In the sequel, I use symmetric-residues.

Step 2. Compute *RREF*(A). Extract submatrices:

```
(setq Tableau (rref-mtab-beforecol A))
  JK: Found 4 pivots before the eighth column.

   x0  x1  x2  x3  x4  x5  hatS hatU    Row operations
  |--------------------------------|
  | 1   0   6   0   5  -4 |   3    0 |  -6   5   6  -6
  | 0   1  -3   0   4   5 |  -6    0 |   6   5  -3   5
  | 0   0   0   1  -2   3 |   4    0 |  -3   2  -5   0
  | 0   0   0   0   0   0 |   0    1 |  -5  -1   5  -5
  |--------------------------------|
```

```
(setq L (MTB-ROM Tableau) hatA (MTB-Alt Tableau) )
  [ -6   5   6  -6 ]    [ 1  0   6  0   5  -4   3  0 ]
  [  6   5  -3   5 ]    [ 0  1  -3  0   4   5  -6  0 ]
  [ -3   2  -5   0 ],   [ 0  0   0  1  -2   3   4  0 ]
  [ -5  -1   5  -5 ]    [ 0  0   0  0   0   0   0  1 ]
```

Matrix L describes the row-ops that were done on A to produces $\widehat{\mathsf{A}}$. And indeed `(mat-mul L A)` produces

$$\begin{bmatrix} 1 & 0 & 6 & 0 & 5 & -4 & 3 & 0 \\ 0 & 1 & -3 & 0 & 4 & 5 & -6 & 0 \\ 0 & 0 & 0 & 1 & -2 & 3 & 4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

which is indeed $\widehat{\mathsf{A}}$.

Looking ahead, the $\widehat{\mathsf{U}}$ column is a pivot column, so there are <u>*no*</u> *solns* X to MX = U; the soln-set is *empty*.

So we only need to extract $\widehat{\mathsf{M}}$ and $\widehat{\mathsf{S}}$:

```
(setq hatM (extract-cols hatA 0 6)
      hatS (extract-cols hatA 6 1) )
```

$$\underbrace{\overset{\begin{matrix} x_0 & x_1 & x_2 & x_3 & x_4 & x_5 \end{matrix}}{\begin{bmatrix} 1 & 0 & 6 & 0 & 5 & -4 \\ 0 & 1 & -3 & 0 & 4 & 5 \\ 0 & 0 & 0 & 1 & -2 & 3 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}}}_{\widehat{\mathsf{M}}}, \underbrace{\overset{\text{Target}}{\begin{bmatrix} 3 \\ -6 \\ 4 \\ 0 \end{bmatrix}}}_{\widehat{\mathsf{S}}}$$

Step 3. Use row/col-info from $\widehat{\mathsf{M}}$ to obtain bases for row/col span of M. The pivot rows of $\widehat{\mathsf{M}}$ form a basis of $\mathrm{RowSpn}(\mathsf{M}) = \mathrm{RowSpn}(\widehat{\mathsf{M}})$. This basis is

$$\Big\{ [1, 0, 6, 0, 5, -4], [0, 1, -3, 0, 4, 5], [0, 0, 0, 1, -2, 3] \Big\}.$$

The pivot-cols of $\widehat{\mathsf{M}}$ are cols *0,1,3*. The *corresponding columns* of M thus form a basis for ColSpn(M). This basis is

$$\left\{ \begin{bmatrix} -2 \\ 1 \\ -1 \\ 6 \end{bmatrix}, \begin{bmatrix} -5 \\ 0 \\ 3 \\ -5 \end{bmatrix}, \begin{bmatrix} -2 \\ 0 \\ 1 \\ 3 \end{bmatrix} \right\}$$

Step 4. Give names "a,b,c,…" to the free-cols. Use back-substition to describe the set of X satisfying $\widehat{\mathsf{M}}\,\mathsf{X} = \widehat{\mathsf{S}}$, which is the *same* set of X satisfying $\mathsf{M}\,\mathsf{X} = \mathsf{S}$, since row-ops preserve lin-rels among cols.

We use matrix $[\widehat{\mathsf{M}} \mid \widehat{\mathsf{S}}]$ as follows.

$$\begin{array}{cccccc|c} x_0 & x_1 & \mathsf{a} & x_3 & \mathsf{b} & \mathsf{c} & \widehat{\mathsf{S}} \\ \end{array}$$
$$\left[\begin{array}{cccccc|c} 1 & 0 & 6 & 0 & 5 & -4 & 3 \\ 0 & 1 & -3 & 0 & 4 & 5 & -6 \\ 0 & 0 & 0 & 1 & -2 & 3 & 4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right]$$

Put in the appropriate identity matrix.

$$\begin{bmatrix} x_0 \\ x_1 \\ \mathsf{a} = x_2 \\ x_3 \\ \mathsf{b} = x_4 \\ \mathsf{c} = x_5 \end{bmatrix} = \mathsf{a}\cdot\begin{bmatrix} \\ \\ 1 \\ \\ 0 \\ 0 \end{bmatrix} + \mathsf{b}\cdot\begin{bmatrix} \\ \\ 0 \\ \\ 1 \\ 0 \end{bmatrix} + \mathsf{c}\cdot\begin{bmatrix} \\ \\ 0 \\ \\ 0 \\ 1 \end{bmatrix} + \begin{bmatrix} \\ \\ 0 \\ \\ 0 \\ 0 \end{bmatrix}.$$

Insert the back-substitution values, for x_3…

$$\begin{bmatrix} x_0 \\ x_1 \\ \mathsf{a} = x_2 \\ x_3 \\ \mathsf{b} = x_4 \\ \mathsf{c} = x_5 \end{bmatrix} = \mathsf{a}\cdot\begin{bmatrix} \\ \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \mathsf{b}\cdot\begin{bmatrix} \\ \\ 0 \\ 2 \\ 1 \\ 0 \end{bmatrix} + \mathsf{c}\cdot\begin{bmatrix} \\ \\ 0 \\ -3 \\ 0 \\ 1 \end{bmatrix} + \begin{bmatrix} \\ \\ 0 \\ 4 \\ 0 \\ 0 \end{bmatrix}$$

…and for the rest of the variables:

$$\begin{bmatrix} x_0 \\ x_1 \\ \mathsf{a} = x_2 \\ x_3 \\ \mathsf{b} = x_4 \\ \mathsf{c} = x_5 \end{bmatrix} = \mathsf{a}\cdot\begin{bmatrix} -6 \\ 3 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \mathsf{b}\cdot\begin{bmatrix} -5 \\ -4 \\ 0 \\ 2 \\ 1 \\ 0 \end{bmatrix} + \mathsf{c}\cdot\begin{bmatrix} 4 \\ -5 \\ 0 \\ -3 \\ 0 \\ 1 \end{bmatrix} + \begin{bmatrix} 3 \\ -6 \\ 0 \\ 4 \\ 0 \\ 0 \end{bmatrix}.$$

Step 5. Matrix M acts from the right on rowvecs of length 4. As $\mathrm{Rank}(\mathsf{M}) = \mathrm{Rank}(\widehat{\mathsf{M}}) = 3$, it follows that the $\mathrm{RNul}(\mathsf{M})$ [nullspace of the righthand action of M] is $4 - 3 = 1$ dim'al.

Courtesy Lemma (15), singleton $\{[-5, -1, 5, -5]\}$ is a basis for $\mathrm{RNul}(\mathsf{M})$

Know the following terms: The ***cardinality*** of a set S is the number of elements in S, and written $|S|$, or sometimes $^{\#}S$. A ***subspace*** of a vectorspace. [Recall that the ***trivial subspace*** $\{\vec{\mathbf{0}}\}$ is the unique 0-dimensional subspace. Recall that the emptyset, $\varnothing = \{\}$, is *not* a vectorspace, because it has no identity element.]

A ***linear combination*** of a set of vectors. The ***span*** of a set of vectors. [Recall that the span of a set of vectors in $\mathbf{V}$ is always a subspace of $\mathbf{V}$. Recall that $\text{Spn}(\varnothing) = \{\vec{\mathbf{0}}\}$.] Recall that a collection $S \subset \mathbf{V}$ is ***linearly independent*** if the only linear combination of vectors in S which equals $\vec{\mathbf{0}}$, is the ***trivial combination***, that is, the combination where all scalars are 0. A ***basis*** for $\mathbf{V}$ is a linearly independent subset of $\mathbf{V}$ which spans $\mathbf{V}$.

Some important theorems. In a vectorspace $\mathbf{V}$:

16: Theorem. *Every vectorspace has a basis. Each linearly-independent set can be extended to (i.e, is a subset of) a basis. Each generating set can be cut down to (i.e, is a superset of) a basis.* ♢

17: Theorem. *The cardinality of every spanning set is greater-equal the cardinality of every linearly-independent set. In particular, each two bases have the same cardinality; this number is called the **dimension** of $\mathbf{V}$.* ♢

Terms and algorithms. Know the definitions of the following terms, and how to perform the following algorithms:

"Algorithm". "Augmented matrix". Know the three "elementary row operations", and what "row equivalence" is. Be able to precisely describe the Gaussian Elimination algorithm. "Reduced row-echelon form". A "pivot" position. "Free column". A "consistent" system of linear equations. Know how to compute the "solution set" to a system of linear equations or to a vector equation $A\mathbf{x} = \mathbf{b}$ [where A is a $k{\times}n$ matrix, $\mathbf{b} \in \mathsf{F}^k$ is known, and $\mathbf{x} \in \mathsf{F}^n$ is the unknown], and how to describe the solution set parametrically. Recall that such a solution set is either empty, or is a translated vector subspace of F^n, ie "an ***affine subspace***" or "a ***flat***".

The "column-span" and "row-span" of a matrix, as well as the "column-rank" and "row-rank", and know how to compute these four things.

"Linear transformation". The "inverse" of a linear transformation. The "inverse of an invertible square matrix", and how to compute it. Know how to compute the matrix corresponding to a given linear transformation.

"Change-of-basis matrix" and how to compute such.

Eigen Ideas

Below $\mathsf{T}{:}\mathbf{X}\circlearrowleft$ is a linear transformation.

The simplest kind of T-invariant subspace $\mathbf{E} \subset \mathbf{X}$, is where $\mathsf{T}\!\downharpoonright_{\mathbf{E}}$ a dilation, $\mathbf{u} \mapsto \lambda\mathbf{u}$ for some fixed scalar λ. Each λ determines a subspace

$$\mathbf{E}_\lambda \;=\; \mathbf{E}_{\lambda,\mathsf{T}} \;:=\; \{\mathbf{z} \in \mathbf{X} \mid \mathsf{T}\mathbf{z} = \lambda\mathbf{z}\}\,.$$

When $\mathbf{E}_{\lambda,\mathsf{T}}$ is not the trivial space $\mathbf{0}$, then we call $\mathbf{E}_{\lambda,\mathsf{T}}$ the "λ-***eigenspace*** of T", and λ is a T-***eigenvalue***. Each non-zero vector in $\mathbf{E}_{\lambda,\mathsf{T}}$ is an ***eigenvector*** of T. [*e*Space=eigenspace, *e*Val=eigenvalue, *e*Vec=eigenvector]

18: Eigenspace LI theorem. *The collection, $\mathcal{C}$, of T-eigenspaces is linearly independent.* ♢

Proof. FTSOC, suppose $\exists N \geq 1$ and *e*Vecs satisfying

$$\dagger: \qquad \vec{\mathbf{0}} \;=\; \mathbf{z}_1 + \mathbf{z}_2 + \ldots + \mathbf{z}_N$$

with distinct *e*Vals $\lambda_1, \ldots, \lambda_N$, and choose (†) to *minimize* N. Necessarily, $N \geq 2$ since *e*Vecs are non-$\vec{\mathbf{0}}$.

Applying T to (†) yields

$$\ddagger: \quad \begin{aligned} \vec{\mathbf{0}} \;=\; \mathsf{T}(\vec{\mathbf{0}}) \;&=\; \mathsf{T}(\mathbf{z}_1) + \mathsf{T}(\mathbf{z}_2) + \ldots + \mathsf{T}(\mathbf{z}_N) \\ &=\; \lambda_1\mathbf{z}_1 \;+\; \lambda_2\mathbf{z}_2 + \ldots + \lambda_N\mathbf{z}_N\,. \end{aligned}$$

Subtracting product $\lambda_N\cdot(\dagger)$ from $(\ddagger)$ produces

$$*: \qquad \vec{\mathbf{0}} \;=\; \sum_{j=1}^{N-1} [\lambda_j - \lambda_N]\cdot\mathbf{z}_j\,.$$

As the *e*Vals are distinct, each $\lambda_j - \lambda_N \neq 0$, so $[\lambda_j - \lambda_N]\cdot\mathbf{z}_j \neq \vec{\mathbf{0}}$. Equation $(*)$ writes $\vec{\mathbf{0}}$ as a sum of $N{-}1$ eigenvectors with distinct eigenvalues, contradicting the minimality of N. ♦

Defn. Consider two fncs $f,g{:}\Omega\circlearrowleft$ on a set Ω. We say "f ***commutes with*** g" if $f \circ g = g \circ f$, and write this as $f \leftrightarrows g$. □

19a: Lemma. *Suppose linear transformations $\mathsf{S},\mathsf{T}{:}\mathbf{X}\circlearrowleft$ commute with each other. Then S maps each T-eigenspace E into itself; $\mathsf{S}(\mathbf{E}) \subset \mathbf{E}$.* ♢

Proof. WLOG, fix a vector $\mathbf{z} \in \mathbf{E}_{5,\mathsf{T}}$. [We seek to show that $\mathsf{S}\mathbf{z}$ is also in $\mathbf{E}_{5,\mathsf{T}}$.] Computing,

$$\mathsf{T}(\mathsf{S}\mathbf{z}) \;\overset{\text{commutes}}{=\!=\!=}\; \mathsf{S}(\mathsf{T}\mathbf{z}) \;=\; \mathsf{S}(5\mathbf{z}) \;=\; 5{\cdot}\mathsf{S}\mathbf{z}\,.$$

Hence $\mathsf{S}\mathbf{z}$ lies in $\mathbf{E}_{5,\mathsf{T}}$. ♦

19b: Coro. *Linear $\mathsf{T}{:}\mathbf{X}\circlearrowleft$ has eigenbasis $\mathcal{B}$; let $\lambda_{\mathbf{b}}$ denote the T-eigenvalue of $\mathbf{b} \in \mathcal{B}$. Suppose also the T-eVals are distinct [i.e $\lambda_{\mathbf{b}} = \lambda_{\mathbf{c}}$ implies $\mathbf{b} = \mathbf{c}$ for all $\mathbf{b},\mathbf{c} \in \mathcal{B}$].*

Then linear S commutes with T IFF $\mathcal{B}$ is an eigenbasis of S. ♢

Proof of (⇒). Each T-*e*Space is 1-dim'al, and the foregoing lemma shows S maps this 1-dim'al subspace to itself. The only lin-trn of a 1-dim'al space is multiplying by a scalar, hence this T-*e*Space is also an S-*e*Space. [Of course, the T and S *e*Vals may be different, and S need not have distinct *e*Vals.] ♦

Pf of (⇐). To show two lin-trns commute, ISTShow they commute on each vector of a basis. Since multiplication of scalars is commutative, and each $\mathbf{b} \in \mathcal{B}$ is an eigenvector for both S and T, we have that $\mathsf{TS}\mathbf{b} = \mathsf{ST}\mathbf{b}$. ♦

Diagonalizability. A trn is ***diagonalizable*** (most often applied to a matrix) if it admits an eigenbasis.

A *family* $\mathcal{F}$ of lin-trns is ***simultaneously diagonalizable*** if there is an basis $\mathcal{B}$ which is an eigenbasis for each trn in $\mathcal{F}$. A corollary of the above proof is

19c: *If trn-family $\mathcal{F}$ is simultaneously diagonalizable, then each $\mathsf{S},\mathsf{T} \in \mathcal{F}$ commute.* □

Eigenvalues of rotations. Fix an angle $\theta \notin \{0, \pi\}$. [Our final result, (‡), will be valid for those angles too.] With $\mathcal{C} := \cos(\theta)$ and $\mathcal{S} := \sin(\theta)$, note

$$\boldsymbol{\nu} := \mathrm{e}^{\mathrm{i}\theta} = \mathcal{C} + \mathbf{i}\mathcal{S} \quad \textit{and} \quad \overline{\boldsymbol{\nu}} = \mathrm{e}^{-\mathrm{i}\theta} = \mathcal{C} - \mathbf{i}\mathcal{S}.$$

We seek to diagonalize rotation

$$†: \qquad \mathsf{R} = \mathsf{R}_\theta \overset{\text{recall}}{=\!=} \begin{bmatrix} \mathcal{C} & -\mathcal{S} \\ \mathcal{S} & \mathcal{C} \end{bmatrix}.$$

Easily $\mathrm{Det}(\mathsf{R}) = 1$, since rotations preserve area and orientation. [Or $\mathcal{C}^2 + \mathcal{S}^2 = 1^2$.] For CharPoly $h := \wp_{\mathsf{R}}$, we *could* compute $\mathrm{Det}(\mathsf{R} - t\mathbf{I})$, but more elegant and quicker is

$$\begin{aligned} h(t) &= t^2 - \mathrm{Tr}(\mathsf{R}) \cdot t + \mathrm{Det}(\mathsf{R}) \\ &= t^2 - 2\mathcal{C} \cdot t + 1. \end{aligned}$$

So $\mathrm{Discr}(h) = [2\mathcal{C}]^2 - 4 \cdot 1 \cdot 1 = 2^2[\mathcal{C}^2 - 1^2] \overset{\text{note}}{=\!=} [2\mathcal{S}]^2 \cdot \mathbf{i}^2$. Thus

$$\begin{aligned} \mathrm{Roots}(h) &= \tfrac{1}{2}\Big[2\mathcal{C} \pm \sqrt{\mathrm{Discr}(h)}\,\Big] \\ &= \tfrac{1}{2}\Big[2\mathcal{C} \pm 2\mathcal{S}\,\mathbf{i}\Big] = \{\boldsymbol{\nu}, \overline{\boldsymbol{\nu}}\} \end{aligned}$$

is the set of R-*e*Vals.

Diagonalizing R over $\mathbb{C}$. As $\overline{\boldsymbol{\nu}} \neq \boldsymbol{\nu}$ (recall $\theta \neq 0, \pi$) our R [viewed as acting on $\mathbb{C}^2$] has two 1-dim'al eigenspaces. We thus know that R is similar ($\overset{\text{sim}}{\sim}$) to diagonal matrix

$$\mathsf{D} := \begin{bmatrix} \boldsymbol{\nu} & \\ & \overline{\boldsymbol{\nu}} \end{bmatrix}.$$

THE PLAN: To diagonalize R we seek a $\boldsymbol{\nu}$-*e*Vec $\begin{bmatrix} a \\ c \end{bmatrix}$, and a $\overline{\boldsymbol{\nu}}$-*e*Vec $\begin{bmatrix} b \\ d \end{bmatrix}$. Then matrix $\mathsf{M} := \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ will give us the sought $\mathsf{M}^{-1}\mathsf{R}\mathsf{M} = \mathsf{D}$ equality.

COMPUTING: Looking ahead, $\mathcal{C} - \boldsymbol{\nu} = -\mathbf{i}\mathcal{S}$ so

$$*: \qquad \frac{\mathcal{C} - \boldsymbol{\nu}}{\mathcal{S}} = -\mathbf{i}.$$

An $\boldsymbol{\nu}$-*e*Vec is a non-$\vec{\mathbf{0}}$ vector in $\mathrm{LNul}(\mathsf{R} - \boldsymbol{\nu}\mathbf{I})$. Matrix $\mathsf{R} - \boldsymbol{\nu}\mathbf{I} \overset{\text{note}}{=\!=} \begin{bmatrix} \mathcal{C} - \boldsymbol{\nu} & -\mathcal{S} \\ \mathcal{S} & \mathcal{C} - \boldsymbol{\nu} \end{bmatrix}$ is row-equiv to

$$\begin{bmatrix} \mathcal{S} & \mathcal{C} - \boldsymbol{\nu} \\ \mathcal{C} - \boldsymbol{\nu} & -\mathcal{S} \end{bmatrix} \overset{r}{\sim} \begin{bmatrix} 1 & \frac{\mathcal{C} - \boldsymbol{\nu}}{\mathcal{S}} \\ \mathcal{C} - \boldsymbol{\nu} & -\mathcal{S} \end{bmatrix} \overset{\text{by } (*)}{=\!=} \begin{bmatrix} 1 & -\mathbf{i} \\ \mathcal{C} - \boldsymbol{\nu} & -\mathcal{S} \end{bmatrix}.$$

Thus $\mathsf{R} - \boldsymbol{\nu}\mathbf{I} \overset{r}{\sim} \begin{bmatrix} 1 & -\mathbf{i} \\ 0 & 0 \end{bmatrix}$, as the $\boldsymbol{\nu}$-*e*Space is 1-dim'al. Hence $\begin{bmatrix} \mathbf{i} \\ 1 \end{bmatrix}$ is a $\boldsymbol{\nu}$-*e*Vec for R.

Field-automorphism $z \mapsto \overline{z}$ leaves R invariant, carries $\boldsymbol{\nu}$ to $\overline{\boldsymbol{\nu}}$, and consequently carries $\boldsymbol{\nu}$-*e*Vec $\begin{bmatrix} \mathbf{i} \\ 1 \end{bmatrix}$ to $\overline{\boldsymbol{\nu}}$-*e*Vec $\begin{bmatrix} -\mathbf{i} \\ 1 \end{bmatrix}$. I prefer to multiply this by $\mathbf{i}$, so I'll use $\begin{bmatrix} 1 \\ \mathbf{i} \end{bmatrix}$ as my $\overline{\boldsymbol{\nu}}$-*e*Vec. My conjugating matrix is thus

$$‡: \qquad \begin{aligned} &\mathsf{M} := \begin{bmatrix} \mathbf{i} & 1 \\ 1 & \mathbf{i} \end{bmatrix} \quad \textit{and} \quad \mathsf{M}^{-1} = \tfrac{1}{2}\begin{bmatrix} -\mathbf{i} & 1 \\ 1 & -\mathbf{i} \end{bmatrix} \\ &\textit{yielding} \quad \mathsf{M}^{-1}\mathsf{R}\mathsf{M} = \begin{bmatrix} \boldsymbol{\nu} & \\ & \overline{\boldsymbol{\nu}} \end{bmatrix}. \end{aligned}$$

Duality ideas

Setting. We explore the $\mathbb{C}$-IPS $\mathbf{V} := \mathbb{C}^N$ equipped with dot-product. The vectors in $\mathbf{V}$ are colvecs. For colvecs $\mathbf{u},\mathbf{w} \in \mathbf{V}$, their ***outer product*** is $N\times N$-matrix $\mathbf{u}\cdot\mathbf{w}^*$.

Consider a direct-sum decomposition $\mathbf{V} = \mathbf{A} \oplus \mathbf{B}$ with $\mathbf{A} \perp \mathbf{B}$. (I.e, $\mathbf{A}^\perp = \mathbf{B}$ and $\mathbf{B}^\perp = \mathbf{A}$.) With Proj denoting orthogonal projection, note

$$*:\quad \mathrm{Proj}_{\mathbf{A}} + \mathrm{Proj}_{\mathbf{B}} = \mathit{Id} = \mathrm{Orth}_{\mathbf{B}} + \mathrm{Proj}_{\mathbf{B}},$$

where Id is the identity operator. Consequently $\boxed{\mathrm{Orth}_{\mathbf{B}} = \mathrm{Proj}_{\mathbf{A}}}$, and vice versa.

It follows that (orthogonal) *reflection across* $\mathbf{B}$ is

$$**:\quad \begin{aligned}\mathrm{Proj}_{\mathbf{B}} - \mathrm{Orth}_{\mathbf{B}} &= [\mathit{Id} - \mathrm{Proj}_{\mathbf{A}}] - \mathrm{Proj}_{\mathbf{A}} \\ &= \mathit{Id} - 2\mathrm{Proj}_{\mathbf{A}}.\end{aligned}$$

We now consider when $\mathrm{Dim}(\mathsf{A}) = 1$.

Ortho-projection matrix. Given a non-zero column vector $\boldsymbol{\delta}$ [a "direction" vector], use $\boldsymbol{\delta}^\perp$ for the ortho-complement of $\mathrm{Spn}(\boldsymbol{\delta})$. Let D denote the matrix [w.r.t the std basis] of ortho-projection on $\mathrm{Spn}(\boldsymbol{\delta})$.

Use P for the matrix of ortho-projection on $\boldsymbol{\delta}^\perp$, and employ R for *reflection across* $\boldsymbol{\delta}^\perp$.

20: Lemma. *When the* $\boldsymbol{\delta}$ *from above is a unit vector,*

$$\dagger:\quad \mathsf{D} = \boldsymbol{\delta}\cdot\boldsymbol{\delta}^*, \quad \mathsf{P} = \mathbf{I} - \boldsymbol{\delta}\boldsymbol{\delta}^*, \quad \mathsf{R} = \mathbf{I} - 2\boldsymbol{\delta}\boldsymbol{\delta}^*.$$

Hence, the action of these matrices on an arbitrary vector $\mathbf{v}$ *satisfy*

$$\begin{aligned} \mathsf{D}\mathbf{v} &= \mathrm{Proj}_{\boldsymbol{\delta}}(\mathbf{v}) = \langle\boldsymbol{\delta},\mathbf{v}\rangle\,\mathbf{v}\,; \\ \ddagger:\quad \mathsf{P}\mathbf{v} &= \mathrm{Proj}_{\boldsymbol{\delta}^\perp}(\mathbf{v}) = \mathbf{v} - \langle\boldsymbol{\delta},\mathbf{v}\rangle\,\mathbf{v}\,; \qquad \diamond \\ \mathsf{R}\mathbf{v} &= [\mathit{Id} - \mathrm{Proj}_{\boldsymbol{\delta}^\perp}](\mathbf{v}) = \mathbf{v} - 2\langle\boldsymbol{\delta},\mathbf{v}\rangle\,\mathbf{v}\,. \end{aligned}$$

Proof. First consider projecting on $\mathrm{Spn}(\mathbf{e}_1)$. That maps a general vector

$$\begin{bmatrix}\alpha_1\\ \alpha_2\\ \vdots\\ \alpha_N\end{bmatrix} \mapsto \begin{bmatrix}\alpha_1\\ 0\\ \vdots\\ 0\end{bmatrix}.$$

The matrix whose lefthand action realizes this

$$\begin{bmatrix}1 & 0 & \cdots & 0\\ 0 & 0 & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \cdots & 0\end{bmatrix} \stackrel{\text{note}}{=\!=} \underbrace{\mathbf{e}_1}_{N\times 1}\cdot\underbrace{\mathbf{e}_1^*}_{1\times N}.$$

Change of coordinates. Let U be unitary matrix (which preserves the IP) and carries of $\boldsymbol{\delta}$ to $\mathbf{e}_1$. Note

$$\begin{aligned}\mathbf{e}_1\cdot\mathbf{e}_1^* &= \mathsf{U}\boldsymbol{\delta}\cdot[\mathsf{U}\boldsymbol{\delta}]^* = \mathsf{U}\boldsymbol{\delta}\cdot\boldsymbol{\delta}^*\mathsf{U}^* \\ &\stackrel{\text{since } \mathsf{U} \text{ is unitary}}{=\!=\!=} \mathsf{U}\boldsymbol{\delta}\cdot\boldsymbol{\delta}^*\mathsf{U}^{-1}.\end{aligned}$$

To project a vector $\mathbf{v}$ on $\boldsymbol{\delta}$, we carry $\mathbf{v}$ to $\mathsf{U}\mathbf{v}$, project on $\mathbf{e}_1$, then carry the result back via U^{-1}. So

$$\begin{aligned}\mathsf{D}\cdot\mathbf{v} &= \mathsf{U}^{-1}\cdot\mathbf{e}_1\mathbf{e}_1^*\cdot\mathsf{U}\mathbf{v} \\ &= \mathsf{U}^{-1}\cdot\mathsf{U}\boldsymbol{\delta}\boldsymbol{\delta}^*\mathsf{U}^{-1}\cdot\mathsf{U}\mathbf{v} = \boldsymbol{\delta}\boldsymbol{\delta}^*\cdot\mathbf{v}.\end{aligned}$$

This holds for *all* $\mathbf{v}$, hence $\mathsf{D} = \boldsymbol{\delta}\boldsymbol{\delta}^*$. ♦

Dual spaces in general

A VS, $\mathbf{V}$, over an arbitrary field F has a ***dual space***

$$\mathbf{V}^{*} := \{L \mid \text{Map } L\colon \mathbf{V}\to\mathsf{F} \text{ is linear}\}.$$

So $\mathbf{V}^{*}$ is the VS of "***linear functionals*** on $\mathbf{V}$", with pointwise addition, and pointwise scalar-multiplication.

A linear map $\mathsf{A}\colon\mathbf{S}\to\mathbf{V}$ between F-VSes has an ***adjoint operator*** $\mathsf{A}^{*}\colon\mathbf{V}^{*}\to\mathbf{S}^{*}$, defined by

$$\mathsf{A}^{*}(L) := [\mathbf{s}\mapsto L(\mathsf{A}(\mathbf{s}))] \overset{\text{note}}{=\!=} L\circ\mathsf{A}.$$

Double dual. VS $\mathbf{V}$ has a ***canonical embedding*** into its double-dual. It is the F-linear map

$$\mathbf{V}\hookrightarrow\mathbf{V}^{**} \text{ which sends } \mathbf{u}\mapsto [L\mapsto L(\mathbf{u})].$$

If the canonical embedding is a bijection, then it is a linear isomorphism and we say $\mathbf{V}$ and $\mathbf{V}^{**}$ are "*canonically*" or "*naturally*" isomorphic, In this case, $\mathbf{V}$ is called a ***reflexive*** space. [Well..., the term is usually reserved for the category of *topological* VSes.]

Duality in IPSes. Fix a complex VS $\mathbf{V}$.

21a: *Defn.* For $v\in\mathbf{V}$, define linear fnc'al $L_{\mathbf{v}}$ by

$$L_{\mathbf{v}}(\mathbf{w}) := \langle\mathbf{v},\mathbf{w}\rangle. \qquad \square$$

21b: Lemma. *For all vectors $\mathbf{u}_0,\mathbf{u}_1$, if $L_{\mathbf{u}_0}=L_{\mathbf{u}_1}$ then $\mathbf{u}_0=\mathbf{u}_1$.*

When $\mathbf{V}$ is finite dimensional: *For each linear functional Λ, there exists a vector $\mathbf{v}$ st. $L_{\mathbf{v}}=\Lambda$.* ♢

Pf. With $\mathbf{v}:=\mathbf{u}_0-\mathbf{u}_1$, difference $L_{\mathbf{v}}=L_{\mathbf{u}_0}-L_{\mathbf{u}_1}$ is the zero-fnc'al. Thus $0=L_{\mathbf{v}}(\mathbf{v})=\langle\mathbf{v},\mathbf{v}\rangle$, so $\mathbf{v}=\vec{\mathbf{0}}$.

Fix an ortho-normal basis $\mathbf{b}_1,\dots,\mathbf{b}_N$. Lin fnc'al Λ gives values $\lambda_j := \Lambda(\mathbf{b}_j)$. With $\mathbf{v}:=\sum_{j=1}^{N}\overline{\lambda}_j\mathbf{b}_j$ note $\langle\mathbf{v},\mathbf{b}_5\rangle=\langle\overline{\lambda}_5\mathbf{b}_5,\mathbf{b}_5\rangle=\lambda_5\langle\mathbf{b}_5,\mathbf{b}_5\rangle=\lambda_5$. Similarly, $\langle\mathbf{v},\mathbf{b}_j\rangle=\lambda_j$. Thus $L_{\mathbf{v}}=\Lambda$. ♦

Henceforth. All VSes are finite dim'al. The inner product on $\mathbf{V}$ allows us to identify $\mathbf{V}^{*}$ with $\mathbf{V}$, by identifying each lin fnc'al $\langle\mathbf{v},\cdot\rangle$ with $\mathbf{v}$. Using a blue $\bullet$ for scalar-vector mult, then $\alpha\bullet\langle\mathbf{v},\cdot\rangle=\langle\alpha\mathbf{v},\cdot\rangle$. □

Consider a linear $\mathsf{A}\colon\mathbf{V}\to\mathbf{S}$. The identification allows us to interpret A^{*} as mapping $\mathbf{S}\to\mathbf{V}$, by

21c: $$\forall\mathbf{r}\in\mathbf{S},\forall\mathbf{u}\in\mathbf{V},\quad \langle\mathsf{A}^{*}\mathbf{r},\mathbf{u}\rangle = \langle\mathbf{r},\mathsf{A}\mathbf{u}\rangle.$$

21d: Prop'n. *Eqn (21c) uniquely defines a linear operator $\mathsf{A}^{*}\colon\mathbf{S}\to\mathbf{V}$. Moreover, $\mathsf{A}^{**}=\mathsf{A}$.* ♢

Pf(existence/uniqueness). Composition $\langle\mathbf{r},\cdot\rangle\circ\mathsf{A}$ is linear, so Lemma (21b) asserts a unique vector $\mathbf{v}$ with $\langle\mathbf{v},\cdot\rangle=\langle\mathbf{r},\mathsf{A}(\cdot)\rangle$. Define $\mathsf{A}^{*}\mathbf{r}:=\mathbf{v}$. ♦

Pf(linearity). As $\langle\mathsf{A}^{*}(\mathbf{r}+\mathbf{s}),\mathbf{u}\rangle=\langle\mathbf{r}+\mathbf{s},\mathsf{A}\mathbf{u}\rangle$, additive-linearity gives

$$\begin{aligned}\langle\mathsf{A}^{*}(\mathbf{r}+\mathbf{s}),\mathbf{u}\rangle &= \langle\mathbf{r},\mathsf{A}\mathbf{u}\rangle+\langle\mathbf{s},\mathsf{A}\mathbf{u}\rangle\\ &= \langle\mathsf{A}^{*}\mathbf{r},\mathbf{u}\rangle+\langle\mathsf{A}^{*}\mathbf{s},\mathbf{u}\rangle\\ &= \langle\mathsf{A}^{*}\mathbf{r}+\mathsf{A}^{*}\mathbf{s},\ \mathbf{u}\rangle.\end{aligned}$$

This holds for all $\forall\mathbf{u}$, so $\mathsf{A}^{*}(\mathbf{r}+\mathbf{s})=\mathsf{A}^{*}\mathbf{r}+\mathsf{A}^{*}\mathbf{s}$.

Similarly, for scalar α,

$$\begin{aligned}\langle\mathsf{A}^{*}(\alpha\mathbf{r}),\mathbf{u}\rangle = \langle\alpha\mathbf{r},\mathsf{A}\mathbf{u}\rangle &= \langle\mathbf{r},\mathsf{A}(\overline{\alpha}\mathbf{u})\rangle\\ &= \langle\mathsf{A}^{*}\mathbf{r},\overline{\alpha}\mathbf{u}\rangle = \langle\alpha\,\mathsf{A}^{*}\mathbf{r},\mathbf{u}\rangle.\end{aligned}$$

This holds for all $\mathbf{u}$, whence $\mathsf{A}^{*}(\alpha\mathbf{r})=\alpha\,\mathsf{A}^{*}\mathbf{r}$. ♦

Pf(Involution). The complex-conjugate of (21c) is

$$\forall\mathbf{r}\in\mathbf{S},\forall\mathbf{u}\in\mathbf{V},\quad \langle\mathbf{u},\mathsf{A}^{*}\mathbf{r}\rangle = \langle\mathsf{A}\mathbf{u},\mathbf{r}\rangle,$$

showing that A^{**} is A. ♦

The Adjoint involution. We now consider (linear) operators $\mathbf{V}\to\mathbf{V}$.

22.1: Lemma. *W.r.t an ortho-normal basis, let* $\mathsf{A} = [\alpha_{i,j}]$ *be the matrix of* $\mathsf{S}:\mathbf{V}\circlearrowleft$, *and* $\mathsf{B} = [\beta_{i,j}]$ *the matrix of* S^*. *Then* $\mathsf{B} = \overline{\mathsf{A}^t} \stackrel{\text{note}}{=\!=} \overline{\mathsf{A}}^t$. ♢

Pf. The 1×1 matrix $[\beta_{5,2}] = \mathbf{e}_5^t \mathsf{B} \mathbf{e}_2 = [\langle \mathbf{e}_5, \mathsf{S}^*\mathbf{e}_2\rangle]$. So

$$[\beta_{5,2}] \;=\; [\langle \mathsf{S}\mathbf{e}_5, \mathbf{e}_2\rangle] \;=\; \mathbf{e}_5^t\,\overline{\mathsf{A}}^{\,t}\cdot\mathbf{e}_2 \;=\; \left[\mathbf{e}_2^t\cdot\overline{\mathsf{A}}\,\mathbf{e}_5\right]^t \;=\; \mathbf{e}_2^t\cdot\overline{\mathsf{A}}\,\mathbf{e}_5\,,$$

as the transpose of a 1×1 is itself. Thus $\beta_{5,2} = \overline{\alpha_{2,5}}$. ♦

Defn. On a $\mathbb{C}$-VS, operator $\mathsf{U}:\mathbf{V}\to\mathbf{V}$ is ***unitary*** if it preserves the unit-sphere: $\forall\mathbf{x}\in\mathbf{V}$: $\|\mathsf{U}\mathbf{x}\| = \|\mathbf{x}\|$. We say that U is ***norm-preserving***. It turns out norm-preserving implies the seeming stronger property,

22.2: $$\forall \mathbf{x},\mathbf{y}\in\mathbf{V}:\; \langle \mathsf{U}\mathbf{x}, \mathsf{U}\mathbf{y}\rangle \;=\; \langle \mathbf{x},\mathbf{y}\rangle\,,$$

of preserving the IP.

On an $\mathbb{R}$-VS, a U satisfying (22.2) preserves orthogonality; hence it is called an ***orthogonal operator***.

For an operator satisfying (22.2): On a $\mathbb{R}$-VS it called ***orthogonal***, but on a $\mathbb{C}$-VS we say ***unitary***; this is just a convention. [*Norm/IP-preserving forces* U *to be injective. The above definitions will apply to an operator on an* ∞*-dim'al IPS, once we adjoin the requirement that* U *be surjective; hence, is an invertible operator.* (*Surjectivity is automatic on a finite-dim'al space.*)]

Operator A is ***self-adjoint*** if $\mathsf{A}^* = \mathsf{A}$. □

22.3: Lemma. *Operator* U *is unitary IFF* $\mathsf{U}^{-1} = \mathsf{U}^*$. ♢

Pf (⇒). For all $\mathbf{v},\mathbf{w}$:

$$\langle \mathsf{U}^*\mathsf{U}\mathbf{v}, \mathbf{w}\rangle = \langle \mathsf{U}\mathbf{v}, \mathsf{U}\mathbf{w}\rangle = \langle \mathbf{v},\mathbf{w}\rangle = \langle \mathsf{U}^{-1}\mathsf{U}\mathbf{v}, \mathbf{w}\rangle.$$

Holds $\forall\mathbf{w}$, so $\mathsf{U}^*\mathsf{U}\mathbf{v} = \mathsf{U}^{-1}\mathsf{U}\mathbf{v}$. Holds $\forall\mathbf{v}$, so $\mathsf{U}^*\mathsf{U} = \mathsf{U}^{-1}\mathsf{U}$. Last U is invertible, so. . . .

The reverse direction is left as an exercise. ♦

22.4: Lemma. *Suppose self-adjoint* A *satisfies* $\langle \mathbf{y}, \mathsf{A}\mathbf{y}\rangle = 0$ *for each* $\mathbf{y}\in\mathbf{V}$. *Then* A *is the zero-operator.* ♢

Pf. Fix $\mathbf{x}\in\mathbf{V}$. Then

$$\begin{aligned} 0 &= \langle \mathbf{x}{+}\mathsf{A}\mathbf{x}, \mathsf{A}(\mathbf{x}{+}\mathsf{A}\mathbf{x})\rangle = \langle \mathbf{x}{+}\mathsf{A}\mathbf{x},\ \mathsf{A}\mathbf{x}{+}\mathsf{A}^2\mathbf{x}\rangle \\ &= \underbrace{\langle \mathbf{x}, \mathsf{A}\mathbf{x}\rangle}_{=0} + \langle \mathbf{x}, \mathsf{A}^2\mathbf{x}\rangle + \langle \mathsf{A}\mathbf{x}, \mathsf{A}\mathbf{x}\rangle + \underbrace{\langle \mathsf{A}\mathbf{x}, \mathsf{A}^2\mathbf{x}\rangle}_{=0} \\ &= \langle \mathbf{x},\ \mathsf{A}^*\mathsf{A}\mathbf{x}\rangle + \langle \mathsf{A}\mathbf{x}, \mathsf{A}\mathbf{x}\rangle \stackrel{\text{note}}{=\!=} 2\cdot\|\mathsf{A}\mathbf{x}\|^2. \end{aligned}$$

Hence [since our field is not char=2] $\mathsf{A}\mathbf{x} = \vec{\mathbf{0}}$. ♦

22.5: Theorem. *A norm-preserving* $\mathsf{T}:\mathbf{V}\circlearrowleft$ *automatically preserves the inner-product.* ♢

Proof. Note that $\mathsf{A} := \mathsf{T}^*\mathsf{T} - \mathbf{I}$ is self-adjoint. By (22.4), ISTEstablish that A is the zero-operator, hence that $\langle \mathbf{y}, [\mathsf{T}^*\mathsf{T} - \mathbf{I}]\mathbf{y}\rangle$ is zero. Computing

$$\begin{aligned} \langle \mathbf{y}, [\mathsf{T}^*\mathsf{T} - \mathbf{I}]\mathbf{y}\rangle &= \langle \mathbf{y}, \mathsf{T}^*\mathsf{T}\mathbf{y}\rangle - \langle \mathbf{y},\mathbf{y}\rangle \\ &= \langle \mathsf{T}\mathbf{y}, \mathsf{T}\mathbf{y}\rangle - \langle \mathbf{y},\mathbf{y}\rangle \\ &\stackrel{\text{norm}}{\underset{\text{preserving}}{=\!=\!=}} \langle \mathbf{y},\mathbf{y}\rangle - \langle \mathbf{y},\mathbf{y}\rangle \;=\; 0\,. \end{aligned}$$ ♦

§A Appendix

23.1:**SV**Buried Treasure Problem [BTP]. *Floating in the ocean you spy a bottle containing a pirate's map to fabulous treasure. You sell your possessions, purchase a robot-crewed ocean-catamaran, and sail to the island, discovering it is a vast plateau. The map says:*

> *Arrrgh, Matey! Count your paces from the gallows to the a quartz boulder, turn Left* 90° *and walk the same distance; hammer a gold spike into the ground.*
>
> *Count your paces from the gallows to the giant oak, turn Right* 90° *and walk the counted distance; hammer a silver spike into the ground.*
>
> *Find Ye Buried Treasure midway between the spikes.*

With joy, you bound up the plateau [with the treasure you can say *bye bye* to *annoying Math classes!*] *and immediately spot the giant oak, and quartz boulder. But the gallows has rotted away without a trace.*

Nonetheless, you find the Treasure. How? ♢

[Hint: Using B, K, w for the Bolder's, oaK's and (unknown) galloWs' location, write the treasure's spot as a fnc $\mathbf{t}_{B,K}(w)$ by using $\mathbb{C}$ addition and multiplication.] Alphabetic-order mnemonic:

*B*oulder	*L*eft	gold
oa*K*	*R*ight	silver

Solved by: *Matthew C, Junhao Z., Hani S.*, 2020t. *Nathan T.*, 2021t.

(*Partial soln*) *Sreeram V.*, 2022g. *Maxime A.*, 2023g.

Are we rich, yet? In $\mathbb{C}$, multiplication by $+\mathbf{i}$ and $-\mathbf{i}$ rotates the plane by 90° (counter-)clockwise. In $\mathbb{C}$, our gold and silver spikes are

$$\text{(turned Left)}\quad g := B + \mathbf{i}[B-w]\,;$$

$$\text{(turned Right)}\quad s := K - \mathbf{i}[K-w]\,.\quad \textit{Averaging,}$$

$$\mathbf{t} = \frac{g+s}{2} \overset{\text{note}}{=\!=} \frac{B+K}{2} + \mathbf{i}\cdot\frac{B-K}{2}.$$

For convenience, we can WLOG orient $\mathbb{C}$ relative to the plateau so as have $B = -K$ and thus $\mathbf{t} = -\mathbf{i}\cdot K$.

The boring case is when the oak is growing out of the boulder, giving $0=K=B=\mathbf{t}$.

The *interesting* case is when $B \neq K$. Now we can orient $\mathbb{C}$ so that $K := \mathbf{i}$ and thus $\mathbf{t} = -\mathbf{i}\cdot\mathbf{i} = 1$. So the treasure is the right-angle vertex of an isosceles right-triangle, whose other vertices are the oaK and Boulder, in appropriate order. ♦

§B $\mathbb{Z}_p$ Reciprocal/Multiplication tables

Reciprocals

Modulo 2:

x	$\langle 1/x \rangle_2$
1	1

Modulo 3:

x	$\langle 1/x \rangle_3$
± 1	± 1

Modulo 5:

x	$\langle 1/x \rangle_5$	x	$\langle 1/x \rangle_5$
± 1	± 1	± 2	∓ 2

Modulo 7:

x	$\langle 1/x \rangle_7$	x	$\langle 1/x \rangle_7$
± 1	± 1		
± 2	∓ 3	± 3	∓ 2

Modulo 11:

x	$\langle 1/x \rangle_{11}$	x	$\langle 1/x \rangle_{11}$
± 1	± 1		
± 2	∓ 5	± 4	± 3
± 3	± 4	± 5	∓ 2

Modulo 13:

x	$\langle 1/x \rangle_{13}$	x	$\langle 1/x \rangle_{13}$
± 1	± 1	± 4	∓ 3
± 2	∓ 6	± 5	∓ 5
± 3	∓ 4	± 6	∓ 2

Modulo 17:

x	$\langle 1/x \rangle_{17}$	x	$\langle 1/x \rangle_{17}$
± 1	± 1	± 5	± 7
± 2	∓ 8	± 6	± 3
± 3	± 6	± 7	± 5
± 4	∓ 4	± 8	∓ 2

Modulo 19:

x	$\langle 1/x \rangle_{19}$	x	$\langle 1/x \rangle_{19}$
± 1	± 1		
± 2	∓ 9	± 6	∓ 3
± 3	∓ 6	± 7	∓ 8
± 4	± 5	± 8	∓ 7
± 5	± 4	± 9	∓ 2

Modulo 23:

x	$\langle 1/x \rangle_{23}$	x	$\langle 1/x \rangle_{23}$
± 1	± 1		
± 2	∓ 11	± 7	± 10
± 3	± 8	± 8	± 3
± 4	± 6	± 9	∓ 5
± 5	∓ 9	± 10	± 7
± 6	± 4	± 11	∓ 2

Multiplication

```
  7 |  2   3
----|--------
  2 | -3
  3 | -1   2
```

```
 11 |   2   3   4   5
----|----------------
  2 |   4
  3 |  -5  -2
  4 |  -3   1   5
  5 |  -1   4  -2   3
```

```
 13 |   2   3   4   5   6
----|--------------------
  2 |   4
  3 |   6  -4
  4 |  -5  -1   3
  5 |  -3   2  -6  -1
  6 |  -1   5  -2   4  -3
```

```
 17 |   2   3   4   5   6   7   8
----|----------------------------
  2 |   4
  3 |   6  -8
  4 |   8  -5  -1
  5 |  -7  -2   3   8
  6 |  -5   1   7  -4   2
  7 |  -3   4  -6   1   8  -2
  8 |  -1   7  -2   6  -3   5  -4
```

```
 19 |   2   3   4   5   6   7   8   9
----|--------------------------------
  2 |   4
  3 |   6   9
  4 |   8  -7  -3
  5 |  -9  -4   1   6
  6 |  -7  -1   5  -8  -2
  7 |  -5   2   9  -3   4  -8
  8 |  -3   5  -6   2  -9  -1   7
  9 |  -1   8  -2   7  -3   6  -4   5
```

```
 23 |   2   3   4   5   6   7   8   9  10  11
----|----------------------------------------
  2 |   4
  3 |   6   9
  4 |   8 -11  -7
  5 |  10  -8  -3   2
  6 | -11  -5   1   7 -10
  7 |  -9  -2   5 -11  -4   3
  8 |  -7   1   9  -6   2  10  -5
  9 |  -5   4 -10  -1   8  -6   3 -11
 10 |  -3   7  -6   4  -9   1  11  -2   8
 11 |  -1  10  -2   9  -3   8  -4   7  -5   6
```

§Index, with symbols and abbrevs at the End

That's All, Folks! –*Bugs Bunny*