3.3.3. Find all abelian groups of order 144. Find both the elementary divisor decomposition and the invariant factor decomposition of each group.

3.3.4. How many abelian groups are there of order 128, up to isomorphism?

3.3.5. How many abelian groups are there of order p^5q^4, where p and q are distinct primes?

3.3.6. Show that $\mathbb{Z}_a \times \mathbb{Z}_b$ is not cyclic if g.c.d.$(a, b) \geq 2$.

3.3.7. Let G be a finite abelian group and let p be a prime dividing $|G|$. Let p^k be the largest power of p dividing $|G|$. For $x \in G$, show that $x \in G[p] \Leftrightarrow p^j x = 0$ for some $j \Leftrightarrow p^k x = 0$.

3.3.8. Let G be a finite abelian group, let $p_1, \ldots, p_k$ be the primes dividing $|G|$. For $b \in G$, write $b = b_1 + \cdots + b_k$, where $b_i \in G[p_i]$. Show that $o(b) = \prod_i o(b_i)$.

3.3.9. Suppose a finite abelian group G has invariant factors $(m_1, m_2, \ldots, m_k)$. Show that G has an element of order s if, and only if, s divides m_1.

3.3.10. Recall that if a and b are relatively prime natural numbers, then $\mathbb{Z}_{ab} \cong \mathbb{Z}_a \times \mathbb{Z}_b$ *as rings.*

(a) If a, b are relatively prime natural numbers, show that the ring isomorphism $\mathbb{Z}_{ab} \cong \mathbb{Z}_a \times \mathbb{Z}_b$ implies that $\Phi(ab) \cong \Phi(a) \times \Phi(b)$.

(b) Show that if $N = p_1^{k_1} \cdots p_s^{k_s}$ is the prime decomposition of N, then

$$\Phi(N) \cong \Phi(p_1^{k_1}) \times \cdots \times \Phi(p_s^{k_s}).$$

(c) Since these group isomorphisms are obtained independently of our earlier computations of $\varphi(N)$, show that we can recover the multiplicativity of the Euler φ function from the group theory results. Namely, conclude from from parts (a) - (c) that $\varphi(ab) = \varphi(a)\varphi(b)$ if a, b are relatively prime, and that if $N = p_1^{k_1} \cdots p_s^{k_s}$, then $\varphi(N) = \prod_i \varphi(p_i^{k_i})$.

3.3.11. Find the structure of the group $\Phi(n)$ for $n \leq 20$.

3.4. Vector Spaces

You can use your experience with group theory to gain a new appreciation of linear algebra. In this section K denotes one of the fields $\mathbb{Q}$, $\mathbb{R}, \mathbb{C}$, or $\mathbb{Z}_p$, or any other favorite field of yours.

Definition 3.4.1. A *vector space* V over a field K is a abelian group with a product $K \times V \to V$, $(\alpha, v) \mapsto \alpha v$ satisfying the following conditions:

(a) $1v = v$ for all $v \in V$.
(b) $(\alpha\beta)v = \alpha(\beta v)$ for all $\alpha, \beta \in K$, $v \in V$.
(c) $\alpha(v + w) = \alpha v + \alpha w$ for all $\alpha \in K$ and $v, w \in V$.
(d) $(\alpha + \beta)v = \alpha v + \beta v$ for all $\alpha, \beta \in K$ and $v \in V$.

Compare this definition with that contained in your linear algebra text; notice that we were able to state the definition more concisely by referring to the notion of an abelian group.

A vector space over K is also called a K–vector space. A vector space over $\mathbb{R}$ is also called a real vector space and a vector space over $\mathbb{C}$ a complex vector space.

Example 3.4.2.

(a) K^n is a vector space over K, and any vector subspace of K^n is a vector space over K.
(b) The set of K–valued functions on a set X is a vector space over K, with pointwise addition of functions and the usual multiplication of functions by scalars.
(c) The set of *continuous* real–valued functions on $[0, 1]$ (or, in fact, on any other metric or topological space) is a vector space over $\mathbb{R}$ with pointwise addition of functions and the usual multiplication of functions by scalars.
(d) The set of polynomials $K[x]$ is a vector space over K, as is the set of polynomials of degree $\leq n$, for any natural number n.

Let's make a few elementary deductions from the vector space axioms: Note that the distributive law $\alpha(v+w) = \alpha v+\alpha w$ says that the map $L_\alpha : v \mapsto \alpha v$ is a group homomorphism of $(V, +)$ to itself. It follows that $L_\alpha(0) = 0$ and $L_\alpha(-v) = -L_\alpha(v)$ for any $v \in V$. This translates to $\alpha\, 0 = 0$ and $\alpha(-v) = -(\alpha v)$.

Similarly, $(\alpha + \beta)v = \alpha v + \beta v$ says that $R_v : \alpha \mapsto \alpha v$ is a group homomorphism of $(K, +)$ to $(V, +)$. Consequently, $0\, v = 0$, and $(-\alpha)v = -(\alpha v)$. In particular, $(-1)v = -(1v) = -v$.

Lemma 3.4.3. *Let V be a vector space over the field K. then for all $\alpha \in K$ and $v \in V$,*

(a) $0v = \alpha 0 = 0$.

(b) $\alpha(-v) = -(\alpha v) = (-\alpha)v$.
(c) $(-1)v = -v$.
(d) *If* $\alpha \neq 0$ *and* $v \neq 0$, *then* $\alpha v \neq 0$.

Proof. Parts (a) through (c) were proved above. For (d), suppose $\alpha \neq 0$ but $\alpha v = 0$. Then

$$0 = \alpha^{-1}0 = \alpha^{-1}(\alpha v) = (\alpha^{-1}\alpha)v = 1v = v.$$

■

We define linear independence, span, and basis for abstract vector spaces, and linear transformations between abstract vector spaces exactly as for vector subspaces of K^n. (Vector subspaces of K^n are treated in Appendix E.) We give the definitions here for the sake of completeness.

Definition 3.4.4. A *linear combination* of a subset S of a vector space V is any element of V of the form $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_s v_s$, where for all i, $\alpha_i \in K$ and $v_i \in S$. The *span* of S is the set of all linear combinations of S. We denote the span of S by span(S).

The span of the empty set is the set containing only the zero vector $\{0\}$.

Definition 3.4.5. A subset S of vector space V is *linearly independent* if for all natural numbers s, for all $\boldsymbol{\alpha} = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_s \end{bmatrix} \in K^s$, and for all sequences $(v_1, \ldots v_s)$ of *distinct* vectors in S, if $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_s v_s = 0$, then $\boldsymbol{\alpha} = 0$. Otherwise, S is *linearly dependent*.

Note that a linear independent set cannot contain the zero vector. The empty set is linearly independent, since there are no sequences of its elements!

Example 3.4.6. Define $e_n(x) = e^{inx}$ for n an integer and $x \in \mathbb{R}$. Then $\{e_n : n \in \mathbb{Z}\}$ is a linearly independent subset of the (complex) vector space of $\mathbb{C}$–valued functions on $\mathbb{R}$. To show this, we have to prove that for all natural numbers s, any set consisting of s of the functions e_n is linearly independent. We prove this statement by

induction on s. For $s = 1$, suppose $\alpha \in \mathbb{C}$, $n_1 \in \mathbb{Z}$, and $\alpha e_{n_1} = 0$. Evaluating at $x = 0$ gives $0 = \alpha e^{in_1 0} = \alpha$. This shows that $\{e_{n_1}\}$ is linearly independent. Now fix $s > 1$ and suppose that any set consisting of fewer than s of the functions e_n is linearly independent. Let $n_1, \ldots, n_s$ be distinct integers, $\alpha_1, \ldots, \alpha_s \in \mathbb{C}$, and suppose that

$$\alpha_1 e_{n_1} + \cdots + \alpha_s e_{n_s} = 0.$$

Notice that $e_n e_m = e_{n+m}$ and $e_0 = 1$. Also, the e_n are differentiable, with $(e_n)' = ine_n$. Multiplying our equation by e_{-n_1} and rearranging gives

$$-\alpha_1 = \alpha_2 e_{n_2 - n_1} + \cdots + \alpha_s e_{n_s - n_1}. \tag{3.4.1}$$

Now we can differentiate to get

$$0 = i(n_2 - n_1)\alpha_2 e_{n_2 - n_1} + \cdots + i(n_s - n_1)\alpha_s e_{n_s - n_1}.$$

The integers $n_j - n_1$ for $2 \leq j \leq s$ are all nonzero and distinct, so the induction hypothesis entails $\alpha_2 = \cdots = \alpha_s = 0$. But then Equation (3.4.1) gives $\alpha_1 = 0$ as well.

Definition 3.4.7. Let V be a vector space over K. A subset of V is called a *basis* of V if the set is linearly independent and has span equal to V.

Example 3.4.8.

(a) The set $\{1, x, x^2, \ldots, x^n\}$ is a basis of the vector space (over K) of polynomials in $K[x]$ of degree $\leq n$.

(b) The set $\{1, x, x^2, \ldots\}$ is a basis of $K[x]$.

Definition 3.4.9. Let V and W be vector spaces over K. A map $T : V \to W$ is called a *linear transformation* or *linear map* if $T(x + y) = T(x) + T(y)$ for all $x, y \in V$ and $T(\alpha x) = \alpha T(x)$ for all $\alpha \in K$ and $x \in V$.

Example 3.4.10.

(a) Fix a polynomial $f(x) \in K[x]$. The map $g(x) \mapsto f(x)g(x)$ is a linear transformation from $K[x]$ into $K[x]$.

(b) The formal derivative $\sum_k \alpha_k x^k \mapsto \sum_k k\alpha_k x^{k-1}$ is a linear transformation from $K[x]$ into $K[x]$.

(c) Let V denote the complex vector space of $\mathbb{C}$–valued continuous functions on the interval $[0, 1]$. The map $f \mapsto f(1/2)$ is a linear transformation from V to $\mathbb{C}$.

(d) Let V denote the complex vector space of $\mathbb{C}$–valued continuous functions on the interval $[0,1]$ and let $g \in V$. The map $f \mapsto \int_0^1 f(t)g(t)\,dt$ is a linear transformation from V to $\mathbb{C}$.

Linear transformations are the homomorphisms in the theory of vector spaces; in fact, a linear transformation $T : V \to W$ between vector spaces is a homomorphism of abelian groups that additionally satisfies $T(\alpha v) = \alpha T(v)$ for all $\alpha \in K$ and $v \in V$. A linear *isomorphism* between vector spaces is a bijective linear transformation between them.

Definition 3.4.11. A *subspace* of a vector space V is a (nonempty) subset that is a vector space with the operations inherited from V.

As with groups, we have a criterion for a subset of a vector space to be a subspace, in terms of closure under the vector space operations:

Proposition 3.4.12. *For a nonempty subset of a vector space to be a subspace, it suffices that the subset be closed under addition and under scalar multiplication.*

Proof. Exercise 3.4.3. ■

Again as with groups, the kernel of a vector space homomorphism (linear transformation) is a subspace of the domain, and the range of a vector space homomorphism is a subspace of the codomain.

Proposition 3.4.13. *Let $T : V \to W$ be a linear map between vector spaces. Then the range of T is a subspace of W and the kernel of T is a subspace of V.*

Proof. Exercise 3.4.5. ■

If V is a vector space over K and W is a subspace, then in particular W is a subgroup of the abelian group V, so we can form the quotient *group* V/W, whose elements are cosets $v + W$ of W in V. The additive group operation in V/W is $(x + W) + (y + W) = (x + y) + W$. Now attempt to define a multiplication by scalars on V/W in the obvious way: $\alpha(v + W) = (\alpha v + W)$. We have to check

that this this is well–defined. But this follows from the closure of W under scalar multiplication; namely, if $v + W = v' + W$ and, then $\alpha v - \alpha v' = \alpha(v - v') \in \alpha W \subseteq W$. Thus $\alpha v + W = \alpha v' + W$, and the scalar multiplication on V/W is well-defined.

Theorem 3.4.14. *If W is subspace of a vector space V over K, then V/W has the structure of a vector space, and the quotient map $\pi : v \mapsto v + W$ is a surjective linear map from V to V/W with kernel equal to W.*

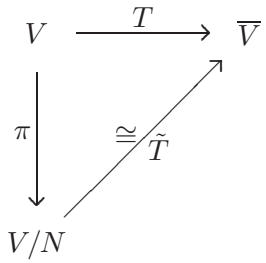
Proof. We know that V/W has the structure of an abelian group, and that, moreover, there is a well-defined product $K \times V/W \longrightarrow V/W$ given by $\alpha(v + W) = \alpha v + W$. It is straighforward to check the remaining vector space axioms. Let us indclude one verification for the sake of illustration. For $\alpha \in K$ and $v_1, v_2 \in V$,

$$\begin{aligned}\alpha((v_1 + W) + (v_2 + W)) &= \alpha((v_1 + v_2) + W)) \\ &= \alpha(v_1 + v_2) + W = (\alpha v_1 + \alpha v_2) + W \\ &= (\alpha v_1 + W) + (\alpha v_2 + W) = \alpha(v_1 + W) + \alpha(v_2 + W)\end{aligned}$$

Finally, the quotient map π is already known to be a group homomorophism. To check that it is linear, we only need to verify that $\pi(\alpha v) = \alpha\pi(v)$ for $v \in V$ and $\alpha \in K$. But this is immediate from the definition of the product, $\alpha v + W = \alpha(v + W)$. ■

V/W is called the *quotient vector space* and $v \mapsto v + W$ the *quotient map*. We have a homomorphism theorem for vector spaces that is analogous to, and in fact follows from, the homomorphism theorem for groups.

Theorem 3.4.15. *(Homomorphism theorem for vector spaces). Let $T : V \longrightarrow \overline{V}$ be a surjective linear map of vector spaces with kernel N. Let $\pi : V \longrightarrow V/N$ be the quotient map. There is linear isomorphism $\tilde{T} : V/N \longrightarrow \overline{V}$ satisfying $\tilde{T} \circ \pi = T$. (See the following diagram.)*



Proof. The homomorphism theorem for groups (Theorem 2.7.6) gives us an isomorphism of abelian groups $\tilde{T}$ satisfying $\tilde{T} \circ \pi = T$. We have only to verify that $\tilde{T}$ also respects multiplication by scalars. But this follows at once from the definitions: $\tilde{T}(\alpha(x+N)) = \tilde{T}(\alpha x + N) = T(\alpha x) = \alpha T(x) = \alpha \tilde{T}(x+N)$. ■

The next three propositions are analogues for vector spaces and linear transformations of results that we have established for groups and group homomorphisms in Section 2.7. Each is proved by adapting the proof from the group situation. Some of the details are left to you.

Proposition 3.4.16. *(Correspondence theorem for vector spaces) Let $T : V \to \overline{V}$ be a surjective linear map, with kernel N. Then $\overline{M} \mapsto T^{-1}(\overline{M})$ is a bijection between subspaces of $\overline{V}$ and subspaces of V containing N.*

Proof. According to Proposition 2.7.12, $\overline{B} \mapsto T^{-1}(\overline{B})$ is a bijection between the subgroups of $\overline{V}$ and the subgroups of V containing N. I leave it as an exercise to verify that $\overline{B}$ is a vector subspace of $\overline{V}$ if, and only if, $T^{-1}(\overline{B})$ is a vector subspace of V; see Exercise 3.4.6. ■

Proposition 3.4.17. *Let $T : V \to \overline{V}$ be a surjective linear transformation with kernel N. Let $\overline{M}$ be a subspace of $\overline{V}$ and let $M = T^{-1}(\overline{M})$. Then $x + M \mapsto T(x) + \overline{M}$ defines a linear isomorphism of V/M to $\overline{V}/\overline{M}$. Equivalently,*

$$(V/N)/(M/N) \cong V/M,$$

as vector spaces.

Proof. By Proposition 2.7.13, the map $x + M \mapsto T(x) + \overline{M}$ is a group isomorphism from V/M to $\overline{V}/\overline{M}$. But the map also respects

multiplication by elements of K, as

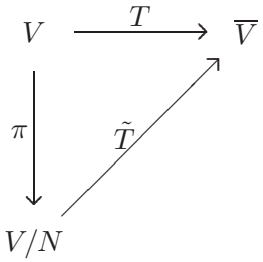
$$\begin{aligned}\alpha(v+M) &= \alpha v + M \mapsto T(\alpha v) + \overline{M} \\ &= \alpha T(v) + \overline{M} = \alpha(T(v) + \overline{M})\end{aligned}$$

We can identify $\overline{V}$ with V/N, by the homomorphism theorem for vector spaces, and this identification carries the subspace $\overline{M}$ to the image of M in V/N, namely M/N. Therefore

$$(V/N)/(M/N) \cong \overline{V}/\overline{M} \cong V/M.$$

■

Proposition 3.4.18. *Let V and $\overline{V}$ be vector spaces over a field K, and let $T : V \longrightarrow \overline{V}$ be a surjective linear map with kernel M. Let $N \subseteq M$ be a vector subspace and let $\pi : V \longrightarrow V/N$ denote the quotient map. The there is a surjective homomorphism $\tilde{T} : V/N \longrightarrow \overline{V}$ such that $\tilde{T} \circ \pi = T$. (See the following diagram.) The kernel of $\tilde{T}$ is $M/N \subseteq V/N$.*



Proof. By Proposition 2.7.14, $\tilde{T} : v + N \mapsto T(v)$ defines a group homomorphism from V/N onto $\overline{V}$ with kernel M/N. We only have to check that this map respects multiplication by elements of K. This follows from the computation:

$$\begin{aligned}\tilde{T}(\alpha(v+N)) &= \tilde{T}(\alpha v + N) = T(\alpha v) \\ &= \alpha T(v) = \alpha \tilde{T}(v+N).\end{aligned}$$

■

Proposition 3.4.19. *Let A and N be subspaces of a vector space V. Let π denote the quotient map $\pi : V \to V/N$. Then $\pi^{-1}(\pi(A)) = A + N$ is a subspace of V containing both A and N. Furthermore, $(A+N)/N \cong \pi(A) \cong A/(A \cap N)$.*

Proof. Exercise 3.4.8. ■

We now consider bases and dimension for abstract vector spaces. This rests on the theory developed for subspaces of K^n in Appendix E.

Definition 3.4.20. A vector space is said to be *finite–dimensional* if it has a finite spanning set. Otherwise, V is said to be *infinite–dimensional*.

Proposition 3.4.21. *If V is finite dimensional, then V has a finite basis. In fact, any finite spanning set has a subset that is a basis.*

Proof. Suppose that V is finite dimensional and that T is a finite subset with $\text{span}(T) = V$. We will show that T has a subset that is a basis of V.

Suppose that $S = \{v_1, \ldots, v_s\}$ is a subset of T such that $\text{span}(S) = V$, but S is linearly dependent. I claim that S has a proper subset which spans V. In fact, suppose that $\sum_i \alpha_i v_i = 0$, and $\alpha_j \neq 0$. then $v_j = \sum_{i \neq j}(-\alpha_i/\alpha_j)v_i$. If a vector $x \in V$ is written as linear combination of $\{v_1, \ldots, v_s\}$, we can substitute for v_j the expression $\sum_{i \neq j}(-\alpha_i/\alpha_j)v_i$, and thus express x as a linear combination of the set $S \setminus \{v_j\}$.

Consider a subset B of T which is minimal spanning. That is, B spans V and no proper subset of B spans V. It follows that B is linearly independent, and thus a basis. ■

An *ordered basis* of a finite–dimensional vector space is a finite sequence whose entries are the elements of a basis listed without repetition; that is, an ordered basis is just a basis endowed with a particular linear order. Corresponding to an ordered basis $B = (v_1, \ldots, v_n)$ of a vector space V over K, we have a linear isomorphism $S_B : V \to K^n$ given by

$$S_B : \sum_i \alpha_i v_i \mapsto \sum_i \alpha_i \hat{\boldsymbol{e}}_i = \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix},$$

where $(\hat{\boldsymbol{e}}_1, \ldots, \hat{\boldsymbol{e}}_n)$ is the standard ordered basis of K^n. $S_B(v)$ is called the *coordinate vector of v with respect to B*.

Since a linear isomorphism carries linearly independent sets to linearly independent sets, spanning sets to spanning sets, and bases to bases, it follows (from the corresponding results for K^n) that

1. Any linearly independent set in V has no more than n elements.
2. Any spanning set in V has at least n elements.
3. Any basis in V has exactly n elements.
4. Any subspace of V is finite–dimensional.
5. Any linearly independent subset of V is contained in a basis.

See Appendix E for the results for K^n. The unique cardinality of a basis of a finite–dimensional vector space V is called the *dimension* of V and denoted $\dim(V)$. If V is infinite–dimensional, we write $\dim(V) = \infty$.

Proposition 3.4.22. *Any two n–dimensional vector spaces over K are linearly isomorphic.*

Proof. The case $n = 0$ is left to the reader.

For $n \geq 1$, any two n–dimensional vector spaces over K are each isomorphic to K^n, and hence isomorphic to each other. ■

This proposition reveals that (finite–dimensional) vector spaces are not very interesting, as they are completely classified by their dimension. That is why the actual subject of finite–dimensional linear algebra is not vector spaces but rather linear maps, which have more interesting structure than vector spaces themselves.

Proposition 3.4.23. *Let V be a vector space over K and let S be a basis of V. Then any function $f : S \to W$ from S into a vector space W extends uniquely to a linear map $T : V \to W$.*

Proof. We will assume that $S = \{v_1, \ldots, v_n\}$ is finite, in order to simplify the notation, although the result is equally valid if S is infinite.

Let $f : S \to W$ be a function. Any element $v \in V$ has a unique expression as a linear combination of elements of S, $v = \sum_i \alpha_i v_i$. There is only one possible way to define $T(v)$, namely $T(v) = \sum_i \alpha_i f(v_i)$. It is then straightforward to check that T is linear. ■

Direct sums and complements

The (external) *direct sum* of several vectors spaces V_1, V_2, ..., V_n over a field K is the Cartesian product $V_1 \times V_2 \times \cdots \times V_n$ with component–by–component operations:

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n))$$

and

$$\alpha(a_1, a_2, \ldots, a_n) = (\alpha a_1, \alpha a_2, \ldots, \alpha a_n),$$

for $a_i, b_i \in V_i$ and $\alpha \in K$. The direct sum is denoted by $V_1 \oplus V_2 \oplus \cdots \oplus V_n$.

How can we recognize that a vector space V is isomorphic to the direct sum of several subspaces $A_1, A_2, \ldots, A_n$? It is neccessary and sufficient that V be be isomorphic to the direct product of the A_i, regarded as abelian groups.

Proposition 3.4.24. *Let V be a vector space over a field K with subspaces $A_1, \ldots A_s$ such that $V = A_1 + \cdots + A_s$. Then the following conditions are equivalent:*

(a) *$(a_1, \ldots, a_s) \mapsto a_1 + \cdots + a_s$ is a group isomorphism of $A_1 \times \cdots \times A_s$ onto V.*

(b) *$(a_1, \ldots, a_s) \mapsto a_1 + \cdots + a_s$ is a linear isomorphism of $A_1 \oplus \cdots \oplus A_s$ onto V.*

(c) *Each element $x \in V$ can be expressed as a sum $x = a_1 + \cdots + a_s$, with $a_i \in A_i$ for all i, in exactly one way.*

(d) *If $0 = a_1 + \cdots + a_s$, with $a_i \in A_i$ for all i, then $a_i = 0$ for all i.*

Proof. The equivalence of (a), (c), and (d) is by Proposition 3.3.1. Clearly (b) implies (a). We have only to show that if (a) holds, then the map $(a_1, \ldots, a_s) \mapsto a_1 + \cdots + a_s$ respects multiplication by elements of K. This is immediate from the computation

$$\begin{aligned}\alpha(a_1, \ldots, a_s) &= (\alpha a_1, \ldots, \alpha a_s) \\ &\mapsto \alpha a_1 + \cdots + \alpha a_s = \alpha(a_1 + \cdots + a_1 + \cdots + a_s).\end{aligned}$$

■

If the conditions of the proposition are satisfied, we say that V is the *internal direct sum* of the subspaces A_i, and we write $V = A_1 \oplus \cdots \oplus A_s$.

In particular, if M and N are subspaces of V such that $M + N = V$ and $M \cap N = \{0\}$, then $V = M \oplus N$.

Let N be a subspace of a vector space V. A subspace M of V is said to be a *complement* of M if $V = M \oplus N$. Subspaces of finite–dimensional vector spaces *always* have a complement, as we shall now explain.

Proposition 3.4.25. *Let $T : V \to W$ be a surjective linear map of a finite–dimensional vector space V onto a vector space W. Then T admits a right inverse; that is, there exists a linear map $S : W \to V$ such that $T \circ S = \mathrm{id}_W$.*

Proof. First, let's check that W is finite–dimensional, with dimension no greater than $\dim(V)$. If $\{v_1, \ldots, v_n\}$ is a basis of V, then $\{T(v_1), \ldots, T(v_n)\}$ is a spanning subset of W, so contains a basis of W as a subset.

Now let $\{w_1, \ldots, w_s\}$ be a basis of W. For each basis element w_i, let x_i be a preimage of w_i in V (i.e., choose x_i such that $T(x_i) = w_i$). The map $w_i \mapsto x_i$ extends uniquely to a linear map $S : W \to V$, defined by $S(\sum_i \alpha_i w_i) = \sum_i \alpha_i x_i$, according to Proposition 3.4.23. We have $T \circ S(\sum_i \alpha_i w_i) = T(\sum_i \alpha_i x_i) = \sum_i \alpha_i T(x_i) = \sum_i \alpha_i w_i$. Thus $T \circ S = \mathrm{id}_W$. ■

In the situation of the previous proposition, let W' denote the image of S. I claim that

$$V = \ker(T) \oplus W' \cong \ker(T) \oplus W.$$

Suppose $v \in \ker(T) \cap W'$. Since $v \in W'$, there is a $w \in W$ such that $v = S(w)$. But then $0 = T(v) = T(S(w)) = w$, and, therefore, $v = S(w) = S(0) = 0$. This shows that $\ker(T) \cap W' = \{0\}$. For any $v \in V$, we can write $v = S \circ T(v) + (v - S \circ T(v))$. The first summand is evidently in W', and the second is in the kernel of T, as $T(v) = T \circ S \circ T(v)$. This shows that $\ker(T) + W' = V$. We have shown that $V = \ker(T) \oplus W'$. Finally, note that S is an isomorphism of W onto W', so we also have $V \cong \ker(T) \oplus W$. We have shown the following:

Proposition 3.4.26. *If $T : V \to W$ is a linear map and V is finite–dimensional, then $V \cong \ker(T) \oplus \mathrm{range}(T)$. In particular, $\dim(V) = \dim(\ker(T)) + \dim(\mathrm{range}(T))$.*

Now let V be a finite–dimensional vector space and let N be a subspace. The quotient map $\pi : V \to V/N$ is a a surjective linear

map with kernel N. Let S be a right inverse of π, as in the proposition, and let M be the image of S. The preceding discussion shows that $V = N \oplus M \cong N \oplus V/N$. We have proved the following:

Proposition 3.4.27. *Let V be a finite–dimensional vector space and let N be a subspace. Then $V \cong N \oplus V/N$. In particular,* $\dim(V) = \dim(N) + \dim(V/N)$.

Corollary 3.4.28. *Let V be a finite–dimensional vector space and let N be a subspace. Then there exists a subspace M of V such that $V = N \oplus M$.*

Warning: Complements of a subspace are never unique. For example, both $\{(0,0,c) : c \in \mathbb{R}\}$ and $\{(0,c,c) : c \in \mathbb{R}\}$ are complements of $\{(a,b,0) : a,b \in \mathbb{R}\}$ in $\mathbb{R}^3$.

Exercises 3.4

3.4.1. Show that the intersection of an arbitrary family of linear subspaces of a vector space is a linear subspace.

3.4.2. Let S be a subset of a vector space. Show that $\text{span}(S) = \text{span}(\text{span}(S))$. Show that $\text{span}(S)$ is the unique smallest linear subspace of V containing S as a subset, and that it is the intersection of all linear subspaces of V that contain S as a subset.

3.4.3. Prove Proposition 3.4.12.

3.4.4. Show that any composition of linear transformations is linear. Show that the inverse of a linear isomorphism is linear.

3.4.5. Let $T : V \to W$ be a linear map between vector spaces. Show that the range of T is a subspace of W and the kernel of T is a subspace of V.

3.4.6. Prove Proposition 3.4.16.

3.4.7. Give another proof of Proposition 3.4.17 by adapting the proof of Proposition 2.7.13 rather than by using that proposition.

3.4.8. Prove Proposition 3.4.19 by using Proposition 2.7.18, or by adapting the proof of that proposition.

3.4.9. Let A and B be finite–dimensional subspaces of a not necessarily finite–dimensional vector space V. Show that $A+B$ is finite–dimensional and that $\dim(A+B)+\dim(A\cap B) = \dim(A)+\dim(B)$.

3.4.10. Show that the following conditions are equivalent for a vector space V:

(a) V is finite dimensional.
(b) V has a finite spanning set.
(c) Every linearly independent subset of V is finite.

(To prove that (c) implies (a), you need the fact that every vector space has a maximal linearly independent subset; this does not follow from the theory we have presented, but requires *Zorn's lemma* or the *Hausdorff maximal principal.*)

3.4.11. Show that the following conditions are equivalent for a vector space V:

(a) V is infinite–dimensional.
(b) V has an infinite linearly independent subset.
(c) For every $n \in \mathbb{N}$, V has a linearly independent subset with n elements.

3.4.12. Prove Corollary 3.4.28 directly as follows: Let $\{v_1, v_2, \ldots, v_s\}$ be a basis of N. Then there exist vectors $v_{s+1}, \ldots, v_n$ such that

$$\{v_1, v_2, \ldots, v_s, v_{s+1}, \ldots, v_n\}$$

is a basis of V. Let $M = \operatorname{span}(\{v_{s+1}, \ldots, v_n\})$. Show that $V = M \oplus N$.

3.5. The dual of a vector space and matrices

Let V and W be vector spaces over a field K. We observe that the set $\operatorname{Hom}_K(V,W)$ of linear maps from V and W also has the structure of a vector space. The sum of two linear maps is defined using the addition in W: if $S, T \in \operatorname{Hom}_K(V,W)$, define $S+T$ by $(S+T)(v) = S(v)+T(v)$ for all $v \in V$. It is straightforward to check that $S+T$ is also linear. For example,

$$\begin{aligned}(S+T)(v_1+v_2) &= S(v_1+v_2)+T(v_1+v_2)\\ &= S(v_1)+S(v_2)+T(v_1)+T(v_2)\\ &= (S(v_1)+T(v_1))+(S(v_2)+T(v_2))\\ &= (S+T)(v_1)+(S+T)(v_2).\end{aligned}$$

The product of a scalar $\alpha \in K$ with a linear map T is defined using the scalar multiplication in W: $(\alpha T)(v) = \alpha T(v)$ for $v \in V$. Again it is straightforward to check that that αT is linear. The zero element

0 of $\mathrm{Hom}_K(V,W)$ is the linear map which sends every element of V to the zero vector in W. The additive inverse of a linear map T is the map defined by $(-T)(v) = -T(v)$ We now have to check that $\mathrm{Hom}_K(V,W)$, with these operations, satisfies all the axioms of a K–vector space. The verifications are all straightforward computations. For example, associativity of addition follows from associativity of addition in W:

$$\begin{aligned}(A+(B+C))(v) &= A(v)+(B+C)(v) = A(v)+(B(v)+C(v))\\ &= (A(v)+B(v))+C(v)\\ &= (A+B)(v)+C(v) = ((A+B)+C)(v),\end{aligned}$$

for $A, B, C \in \mathrm{Hom}_K(V,W)$ and $v \in V$. The reader is invited to check the remaining details in Exercise 3.5.1.

An important special instance of the preceeding construction is the *vector space dual* to V, $\mathrm{Hom}_K(V,K)$, which we also denote by V^*. A linear map from V into the one dimensional vector space of scalars K is called a *linear functional* on V. V^* is the space of all linear functionals on V.

Let us summarize our observations:

Proposition 3.5.1. *Let V be a vector space over a field K.*

(a) *For any vector space W, $\mathrm{Hom}_K(V,W)$ is a vector space.*
(b) *In particular, $V^* = \mathrm{Hom}_K(V,K)$ is a vector space.*

Suppose now that V is finite dimensional with ordered basis $B = (v_1, v_2, \ldots, v_n)$. Every element $v \in V$ has a unique expansion $v = \sum_{i=1}^n \alpha_i v_i$. For $1 \le j \le n$ define $v_j^* \in V^*$ by $v_j^*(\sum_{i=1}^n \alpha_i v_i) = \alpha_j$. The functional v_j^* is the unique element of V^* satisfying $v_j^*(v_i) = \delta_{i,j}$ for $1 \le i \le n$. [2]

I claim that $B^* = (v_1^*, v_2^*, \ldots, v_n^*)$ is a a basis of V^*. In fact, for any $f \in V^*$, consider the functional $\tilde{f} = \sum_{j=1}^n f(v_j) v_j^*$. We have

$$\tilde{f}(v_i) = \sum_{j=1}^n f(v_j) v_j^*(v_i) = \sum_{j=1}^n f(v_j)\delta_{i,j} = f(v_i).$$

Thus $f(v_i) = \tilde{f}(v_i)$ for each element $v_i \in B$. It follows from Proposition 3.4.23 that $f = \tilde{f}$. This means that B^* spans V^*. Next we check the linear independence of B^*. Suppose $\sum_{j=1}^n \alpha_j v_j^* = 0$ (the

[2] Here $\delta_{i,j}$ is the so called "Kronecker delta", defined by $\delta_{i,j} = 1$ if $i = j$ and $\delta_{i,j} = 0$ otherwise.

zero functional in V^*). Applying both sides to a basis vector v_i, we get

$$0 = \sum_{j=1}^{n} \alpha_j v_j^*(v_i) = \sum_{j=1}^{n} \alpha_j \delta_{i,j} = \alpha_i.$$

Thus all the coefficients α_i are zero, which shows that B^* is linearly independent. B^* is called the *basis of V^* dual to B*.

We showed above that for $f \in V^*$, the expansion of f in terms of the basis B^* is

$$f = \sum_{j=1}^{n} f(v_j) v_j^*.$$

Equivalently, the coordinate vector of f with respect to the orderd basis B^* is

$$S_{B^*}(f) = \begin{bmatrix} f(v_1) \\ f(v_2) \\ \vdots \\ f(v_n) \end{bmatrix}$$

For $v \in V$, the expansion of v in terms of the basis B is expressed with the help of the dual basis B^* as

$$v = \sum_{j=1}^{n} v_j^*(v) v_j.$$

Equivalently, the coordinate vector of v with respect to the ordered basis B is

$$S_B(v) = \begin{bmatrix} v_1^*(v) \\ v_2^*(v) \\ \vdots \\ v_n^*(v) \end{bmatrix}$$

In fact, this is clear because for $v = \sum_{j=1}^{n} \alpha_j v_j$, we have $\alpha_j = v_j^*(v)$ for each j, and therefore $v = \sum_{j=1}^{n} v_j^*(v) v_j$.

We have proved:

Proposition 3.5.2. *Let V be a finite dimensional vector space with basis $B = \{v_1, v_2, \ldots, v_n\}$.*

(a) *For each j ($1 \leq j \leq n$), there is a linear functional v_j^* on V determined by $v_j^*(v_i) = \delta_{i,j}$ for $1 \leq i \leq n$.*

(b) *$B^* = \{v_1^*, v_2^*, \ldots, v_n^*\}$ is a a basis of V^*.*

(c) *The dimension of V^* is equal to the dimension of V.*

(d) *For each $f \in V^*$, the expansion of f in terms of the basis B^* is*

$$f = \sum_{j=1}^{n} f(v_j) v_j^*.$$

(e) *For each $v \in V$, the expansion of v in terms of the basis B is*

$$v = \sum_{j=1}^{n} v_j^*(v) v_j.$$

The second dual

Vectors $v \in V$ and $f \in V^*$ pair up to give a number $f(v)$. We can regard this pairing as a function from $V \times V^*$ to K, $(v, f) \mapsto f(v)$. In order to view the two variables on an equal footing, let us introduce a new notation for the pairing, $f(v) = \langle v, f \rangle$. This function of two variables is *bilinear*, that is, linear in each variable separately. This means that for all scalars α and β and all $v, v_1, v_2 \in V$ and $f, f_1, f_2 \in V^*$, we have

$$\langle \alpha v_1 + \beta v_2, f \rangle = \alpha \langle v_1, f \rangle + \beta \langle v_2, f \rangle,$$

and

$$\langle v, \alpha f_1 + \beta f_2 \rangle = \alpha \langle v, f_1 \rangle + \beta \langle v, f_2 \rangle.$$

Linearity in the first variable expresses the linearity of each $f \in V^*$,

$$\begin{aligned} \langle \alpha v_1 + \beta v_2, f \rangle &= f(\alpha v_1 + \beta v_2) = \alpha f(v_1) + \beta f(v_2) \\ &= \alpha \langle v_1, f \rangle + \beta \langle v_2, f \rangle. \end{aligned}$$

Linearity in the second variable, on the other hand, reflects the definition of the vector operations on V^*,

$$\begin{aligned} \langle v, \alpha f_1 + \beta f_2 \rangle &= (\alpha f_1 + \beta f_2)(v) = \alpha f_1(v) + \beta f_2(v) \\ &= \alpha \langle v, f_1 \rangle + \beta \langle v, f_2 \rangle. \end{aligned}$$

The following observation applies to this situation:

Lemma 3.5.3. *Suppose that V and W are vector spaces over a field K, and $b : V \times W \longrightarrow K$ is a bilinear map. Then b induces linear maps $\iota : V \longrightarrow W^*$ and $\kappa : W \longrightarrow V^*$, defined by $\iota(v)(w) = b(v, w)$ and $\kappa(w)(v) = b(v, w)$.*

Proof. Since b is bilinear, for each $v \in V$ the map $w \mapsto b(v, w)$ is linear from W to K, that is, an element of W^*. We denote this element of W^* by $\iota(v)$.

Moreover, the map $v \mapsto \iota(v)$ is linear from V to W^*, because of the linearity of b in its first variable:

$$\begin{aligned}\iota(\alpha v_1 + \beta v_2)(w) &= b(\alpha v_1 + \beta v_2, w) = \alpha b(v_1, w) + \beta b(v_2, w) \\ &= \alpha\, \iota(v_1)(w) + \beta\, \iota(v_2)(w) \\ &= (\alpha\, \iota(v_1) + \beta\, \iota(v_2))(w)\end{aligned}$$

The proof for $\kappa : W \longrightarrow V^*$ is the same. ■

Applying this observation to the bilinear map $(v, f) \mapsto \langle v, f\rangle = f(v)$ from $V \times V^*$ to K, we obtain a linear map $\iota : V \longrightarrow (V^*)^*$, defined by the formula $\iota(v)(f) = \langle v, f\rangle = f(v)$.

Lemma 3.5.4. *Let V be a finite dimensional vector space over a field K. For each non-zero $v \in V$, there is a linear functional $f \in V^*$ such that $f(v) \neq 0$.*

Proof. We know that any linearly independent subset of V is contained in a basis. If v is a non-zero vector in V, then $\{v\}$ is linearly independent. Therefore, there is a basis B of V with $v \in B$. Let f be any function from B into K with $f(v) \neq 0$. By Proposition 3.4.23, f extends to a linear functional on V. ■

Theorem 3.5.5. *If V is a finite dimensional vector space, then $\iota : V \longrightarrow V^{**}$ is a linear isomorphism.*

Proof. We already know that ι is linear.

If v is a non-zero vector in V, then there is an $f \in V^*$ such that $f(v) \neq 0$, by Lemma 3.5.4. Thus $\iota(v)(f) = f(v) \neq 0$, and $\iota(v) \neq 0$. Thus ι is injective. Applying Proposition 3.5.2(c) twice, we have $\dim(V^{**}) = \dim(V^*) = \dim(V)$. Therefore any injective linear map from V to V^{**} is necessarily surjective, by Proposition 3.4.26. ■

Finite dimensionality is essential for this theorem. For an infinite dimensional vector space, $\iota : V \longrightarrow (V^*)^*$ is injective, but not surjective.

Duals of subspaces and quotients

Let V be a finite dimensional vector space over K. For any subset $S \subseteq V$, let S° denote the set of $f \in V^*$ such that $\langle v, f\rangle = 0$ for all $v \in S$. Likewise, for $A \subseteq V^*$, let A° denote the set of $v \in V$ such

that $\langle v, f\rangle = 0$ for all $f \in A$. (We identify V with V^{**}.) S° is called the *annihilator* of S in V^*.

Lemma 3.5.6. *Let S and T be subsets of V, and W a subspace of V.*

(a) *S° is a subspace of V^*.*
(b) *If $S \subseteq T$, then $T^\circ \subseteq S^\circ$ and $S^{\circ\circ} \subseteq T^{\circ\circ}$*
(c) *$T \subseteq T^{\circ\circ}$.*
(d) *$W = W^{\circ\circ}$.*
(e) *$S^\circ = \mathrm{span}(S)^\circ$ and $S^{\circ\circ} = \mathrm{span}(S)$.*

Proof. Parts (a) through (c) are left to the reader as exercises. See Exercise 3.5.6.

For part (d), we have $W \subseteq W^{\circ\circ}$, by part (c). Suppose that $v \in V$ but $v \notin W$. Consider the quotient map $\pi : V \longrightarrow V/W$. Since $\pi(v) \neq 0$, by Lemma 3.5.4, there exists $g \in (V/W)^*$ such that $g(\pi(v)) \neq 0$. Write $\pi^*(g) = g \circ \pi$. We have $\pi^*(g) \in W^\circ$ but $\langle v, \pi^*(g)\rangle \neq 0$. Thus $v \notin W^{\circ\circ}$.

Since $S^{\circ\circ}$ is a subspace of V containing S by parts (a) and (c), we have $S \subseteq \mathrm{span}(S) \subseteq S^{\circ\circ}$. Taking annihilators, and using part (b), we have $S^{\circ\circ\circ} \subseteq \mathrm{span}(S)^\circ \subseteq S^\circ$. But $S^\circ \subseteq S^{\circ\circ\circ}$ by part (c), so all these subspaces are equal. Taking annihilators once more gives $S^{\circ\circ} = \mathrm{span}(S)^{\circ\circ} = \mathrm{span}(S)$, where the final equality results from part (d). ■

With the aid of annihilators, we can describe the dual space of subspaces and quotients.

Proposition 3.5.7. *Let W be a subpace of a finite dimensional vector space V. The restriction map $f \mapsto f_{|W}$ is a surjective linear map from V^* onto W^* with kernel W°. Consequently, $W^* \cong V^*/W^\circ$.*

Proof. I leave it to the reader to check that $f \mapsto f_{|W}$ is linear and has kernel W°.

Let us check the surjectivity of this map. According to Proposition 3.4.27, W has a complement in V, so $V = W \oplus M$ for some subspace M. We can use this direct sum decomposition to define a surjective linear map π from V to W with kernel M, namely $\pi(w + m) = w$, for $w \in W$ and $m \in M$. Now for $g \in W^*$, we have $\pi^*(g) = g \circ \pi \in V^*$, and $\pi^*(g)(w) = g(\pi(w)) = g(w)$ for $w \in W$. Thus g is the restriction to W of $\pi^*(g)$.

Finally, we have $W^* \cong V^*/W^\circ$ by the homomorphism theorem for vector spaces. ■

What about the dual space to V/W? Let $\pi : V \longrightarrow V/W$ denote the quotient map. For $g \in (V/W)^*$, $\pi^*(g) = g \circ \pi$ is an element of V^* that is zero on W, that is, an element of W°. The proof of the following proposition is left to the reader.

Proposition 3.5.8. *The map $g \mapsto \pi^*(g) = g \circ \pi$ is a linear isomorphism of $(V/W)^*$ onto W°.*

Proof. Exercise 3.5.8. ■

Corollary 3.5.9. . $\dim W + \dim W^\circ = \dim V$.

Proof. Exercise 3.5.9. ■

Matrices

Let V and W be finite dimensional vector spaces over a field K. Let $B = (v_1, \ldots, v_m)$ be an ordered basis of V and $C = (w_1, \ldots, w_n)$ an ordered basis of W. Let $C^* = (w_1^*, \ldots, w_n^*)$ denote the basis of W^* dual to C. Let $T \in \mathrm{Hom}_K(V, W)$.

The *matrix $[T]_{C,B}$ of T with respect to the ordered bases B and C* is the n–by–m matrix whose (i, j) entry is $\langle Tv_j, w_i^* \rangle$.

Equivalently, the j–th column of the matrix $[T]_{C,B}$ is

$$S_C(T(v_j)) = \begin{bmatrix} \langle T(v_j), w_1^* \rangle \\ \langle T(v_j), w_2^* \rangle \\ \vdots \\ \langle T(v_j), w_n^* \rangle \end{bmatrix},$$

the coordinate vector of $T(v_j)$ with respect to the ordered basis C.

Another useful description of $[T]_{C,B}$ is the following: $[T]_{C,B}$ is the *standard matrix* of $S_C T S_B^{-1} : K^m \longrightarrow K^n$. Here we are indicating composition of linear maps by juxtaposition; i.e., $S_C T S_B^{-1} = S_C \circ T \circ S_B^{-1}$. As discussed in Appendix E, the standard matrix M of a linear transformation $A : K^m \longrightarrow K^n$ has the property that

$$Mx = A(x),$$

for all $x \in K^m$, where on the left side Mx denotes matrix multiplication of the n–by–m matrix M and the column vector x. Our assertion is equivalent to:

$$[T]_{C,B}\,\hat{\boldsymbol{e}}_j = S_C T S_B^{-1}(\hat{\boldsymbol{e}}_j),$$

for each standard basis vector $\hat{\boldsymbol{e}}_j$ of K^m. To verify this, we note that the left hand side is just the j–th column of $[T]_{C,B}$, while the right hand side is

$$S_C T S_B^{-1}(\hat{\boldsymbol{e}}_j) = S_C T(v_j),$$

which is also the j–th column of $[T]_{C,B}$, according to our previous description of $[T]_{C,B}$.

Proposition 3.5.10.

(a) *The map* $T \mapsto [T]_{B,C}$ *is a linear isomorphism from* $\mathrm{Hom}_K(V,W)$ *to* $\mathrm{Mat}_{n,m}(K)$

(b) $\mathrm{Hom}_K(V,W)$ *has dimension* $\dim(V)\dim(W)$.

Proof. The reader is invited to check that the map is linear.

The map $S_C : W \longrightarrow K^n$, which takes a vector in W to its coordinate vector with respect to C, is a linear isomorphism. For any $T \in \mathrm{Hom}_K(V,W)$, the j–th column of $[T]_{C,B}$ is $S_C(T(v_j))$. If $[T]_{C,B} = 0$, then $S_C(T(v_j)) = 0$ for all j and hence $T(v_j) = 0$ for all j. It follows that $T = 0$. This shows that $T \mapsto [T]_{C,B}$ is injective.

Now let $A = (a_{i,j})$ be any n–by–m matrix over K. We need to produce a linear map $T \in \mathrm{Hom}_K(V,W)$ such that $[T]_{C,B} = A$. If such a T exists, then for each j, the coordinate vector of $T(v_j)$ with respect to C must be equal to the j–th column of A. Thus we require $T(v_j) = \sum_{i=1}^n a_{i,j} w_i := a_j$. By Proposition 3.4.23, there is a unique $T \in \mathrm{Hom}_K(V,W)$ such that $T(v_j) = a_j$ for all j. This proves that $T \mapsto [T]_{B,C}$ is surjective.

Assertion (b) is immediate from (a). ■

Proposition 3.5.11. *Let V, W, X be finite–dimensional vector spaces over K with ordered bases B, C, and D. Let $T \in \mathrm{Hom}_K(V,W)$ and $S \in \mathrm{Hom}_K(W,X)$. Then*

$$[ST]_{D,B} = [S]_{D,C}[T]_{C,B}.$$

Proof. We use the characterization of $[S]_{D,C}$ as the standard matrix of $S_D S S_C^{-1}$, $[S]_{D,C} = [S_D S S_C^{-1}]$. Similarly $[T]_{C,B} = [S_C T S_B^{-1}]$,

and $[ST]_{D,B} = [S_D S T S_B^{-1}]$. Using part (d) of Proposition E.7 from Appendix E,

$$[S]_{D,C}\,[T]_{C,B} = [S_D S S_C^{-1}][S_C T S_B^{-1}] = [S_D S S_C^{-1} S_C T S_B^{-1}]$$
$$= [S_D S T S_B^{-1}] = [ST]_{D,B}$$

■

For a vector space V over a field K, we denote the set of K–linear maps from K to K by $\mathrm{End}_K(V)$. Since the composition of linear maps is linear, $\mathrm{End}_K(V)$ has a product $(S,T) \mapsto ST$. The reader can check that $\mathrm{End}_K(V)$ with the operations of addition and and composition of linear operators is a ring with identity. To simplify notation, we write $[T]_B$ instead of $[T]_{B,B}$ for the matrix of a linear transformation T with respect to a single basis B of V.

Corollary 3.5.12. *Let V be a finite dimensional vector space over K. Let n denote the dimension of V and let B be an ordered basis of V.*

(a) *For all $S, T \in \mathrm{End}_K(V)$, $[ST]_{B,B} = [S]_B[T]_B$.*
(b) *$T \mapsto [T]_B$ is a ring isomorphism from $\mathrm{End}_K(V)$ to $\mathrm{Mat}_n(K)$.*

Lemma 3.5.13. *Let $B = (v_1, \ldots, v_n)$ and $C = (w_1, \ldots, w_n)$ be two bases of a vector space V over a field K. Denote the dual bases of V^* by $B^* = (v_1^*, \ldots, v_n^*)$ and $C^* = (w_1^*, \ldots, w_n^*)$. Let* id *denote the identity linear transformation of V.*

(a) *The matrix $[\mathrm{id}]_{B,C}$ of the identity transformation with respect to the bases C and B has (i,j) entry $\langle w_j, v_i^* \rangle$.*
(b) *$[\mathrm{id}]_{B,C}$ is invertible with inverse $[\mathrm{id}]_{C,B}$.*

Proof. Part (a) is immediate from the definition of the matrix of a linear transformation on page 193. For part (b), note that

$$E = [\mathrm{id}]_B = [\mathrm{id}]_{B,C}[\mathrm{id}]_{C,B}.$$

■

Let us consider the problem of determining the matrix of a linear transformation T with respect to two different bases of a vector space V. Let B and B' be two ordered bases of V. Then

$$[T]_B = [\mathrm{id}]_{B,B'}[T]_{B'}[\mathrm{id}]_{B',B},$$

by an application of Proposition 3.5.11. But the "change of basis matrices" $[\mathrm{id}]_{B,B'}$ and $[\mathrm{id}]_{B'B}$ are inverses, by Lemma 3.5.13 Writing $Q = [\mathrm{id}]_{B,B'}$, we have

$$[T]_B = Q[T]_{B'}Q^{-1}.$$

Definition 3.5.14. We say that two linear transformations T, T' of V are *similar* if there exists an invertible linear transformation S such that $T = ST'S^{-1}$. We say that two n–by–n matrices A, A' are *similar* if there exists an invertible n–by–n matrix Q such that $A = QA'Q^{-1}$.

Proposition 3.5.15.

(a) *Let V be a finite dimensional vector space over a field K. The matrices of a linear transformation $T \in \mathrm{End}_K(V)$ with respect to two different ordered bases are similar.*

(b) *Conversely, if A and A' are similar matrices, then there exists a linear transformation T of a vector space V and two ordered bases B, B' of V such that $A = [T]_B$ and $A' = [T]_{B'}$.*

Proof. Part (a) was proved above.

For part (b), let A be an n–by–n matrix, Q an invertible n–by–n matrix, and set $A' = QAQ^{-1}$.

Let $\mathbb{E} = (\hat{\boldsymbol{e}}_1, \ldots, \hat{\boldsymbol{e}}_n)$ be the standard ordered basis of K^n, and let $B' = (Q^{-1}\hat{\boldsymbol{e}}_1, \ldots, Q^{-1}\hat{\boldsymbol{e}}_n)$; thus B' consists of the columns of Q^{-1}. Because Q is invertible, B' is a basis of K^n. The change of basis matrix $[\mathrm{id}]_{\mathbb{E},B'}$ is just Q^{-1}.

Define $T \in \mathrm{End}_K(K^n)$ by $T(v) = Av$ for $v \in K^n$. Then $A = [T]_{\mathbb{E}}$, and

$$A' = QAQ^{-1} = [\mathrm{id}]_{B',\mathbb{E}}[T]_{\mathbb{E}}[\mathrm{id}]_{\mathbb{E},B'} = [T]_{B'}$$

■

Example 3.5.16. In order to compute the matrix of a linear transformation with respect to different bases, it is crucial to be able compute change of basis matrices $[\mathrm{id}]_{B,B'}$. Let $B = (v_1, \ldots, v_n)$ and $B' = (w_1, \ldots, w_n)$ be two ordered bases of K^n. Because $[\mathrm{id}]_{B,B'} = [\mathrm{id}]_{B,\mathbb{E}}[\mathrm{id}]_{\mathbb{E},B'}$, to compute $[\mathrm{id}]_{B,B'}$, it suffices to be able to compute $[\mathrm{id}]_{B,\mathbb{E}}$ and $[\mathrm{id}]_{\mathbb{E},B}$. One of these requires no computation: $[\mathrm{id}]_{\mathbb{E},B'}$ is the matrix $Q_{B'}$ whose columns are the elements of B'. Similarly,

$[\mathrm{id}]_{\mathbb{E},B}$ is the matrix Q_B whose columns are the elements of B, so $[\mathrm{id}]_{B,\mathbb{E}} = Q_B^{-1}$. Thus, in order to complete the calculation, we have to invert one matrix.

Similarly is an equivalence relation on $\mathrm{Mat}_n(K)$ (or on $\mathrm{End}_K(V)$). A *similarity invariant* is a function on $\mathrm{Mat}_n(K)$ which is constant on similarity classes. Given a similarity invariant f, in makes sense to define f on $\mathrm{End}_K(V)$ by $f(T) = f(A)$, where A is the matrix of T with respect to some basis of V. Since the matrices of T with respect to two different bases are similar, the result does not depend on the choice of the basis. Two important similarity invariants are the determinant and the trace.

Because the determinant satisfies $\det(AB) = \det(A)\det(B)$, and $\det(E) = 1$, it follows that $\det(C^{-1}) = \det(C)^{-1}$ and $\det(CAC^{-1}) = \det(C)\det(A)\det(C)^{-1} = \det(A)$. Thus determinant is a similarity invariant.[3]

The trace of a square matrix is the sum of its diagonal entries. Let $A = (a_{i,j})$. Let $C = (c_{i,j})$ be an invertible matrix and let $C^{-1} = (d_{i,j})$. Since $(d_{i,j})$ and $(c_{i,j})$ are inverse matrices, we have $\sum_i d_{k,i}c_{i,j} = \delta_{kj}$ for any k, j. Using this, we compute:

$$\begin{aligned}\mathrm{tr}(CAC^{-1}) &= \sum_i (CAC^{-1})(i,i) = \sum_i \sum_j \sum_k c_{i,j}a_{j,k}d_{k,i} \\ &= \sum_j \sum_k (\sum_i d_{k,i}c_{i,j})a_{j,k} \\ &= \sum_j \sum_k \delta_{k,j}a_{j,k} = \sum_j a_{j,j} = \mathrm{tr}(A).\end{aligned}$$

Thus the trace is also a similarity invariant.

Exercises 3.5

3.5.1. Complete the details of the verification that $\mathrm{Hom}_K(V, W)$ is a K–vector space, when V and W are K–vector spaces.

3.5.2. Consider the ordered basis $B = (\begin{bmatrix}1\\1\\1\end{bmatrix}, \begin{bmatrix}1\\1\\0\end{bmatrix}, \begin{bmatrix}1\\0\\0\end{bmatrix})$ of $\mathbb{R}^3$. Find the dual basis of $(\mathbb{R}^3)^*$.

[3] The determinant is dicussed systematically in Section M.3.

3.5.3. Define a bilinear map from $K^n \times K^n$ to K by

$$[\begin{bmatrix}\alpha_1\\ \alpha_2\\ \vdots\\ \alpha_n\end{bmatrix}, \begin{bmatrix}\beta_1\\ \beta_2\\ \vdots\\ \beta_n\end{bmatrix}] = \sum_{j=1}^{n} \alpha_j\beta_j.$$

Show that the induced map $\kappa : K^n \longrightarrow (K^n)^*$ given by $\kappa(\boldsymbol{v})(\boldsymbol{w}) = [\boldsymbol{w}, \boldsymbol{v}]$ is an isomorphism.

3.5.4. Using the previous exercise, identify $(\mathbb{R}^3)^*$ with $\mathbb{R}^3$ via the inner product $\langle \begin{bmatrix}\alpha_1\\ \alpha_2\\ \alpha_3\end{bmatrix}, \begin{bmatrix}\beta_2\\ \beta_2\\ \beta_3\end{bmatrix} \rangle = \sum_{j=1}^{3} \alpha_j\beta_j$. Given an ordered basis $B = (\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3)$ of $\mathbb{R}^3$, the dual basis $B^* = (\boldsymbol{v}_1^*, \boldsymbol{v}_2^*, \boldsymbol{v}_3^*)$ of R^3 is defined by the requirements $\langle \boldsymbol{v}_i, \boldsymbol{v}_j^* \rangle = \delta_{i,j}$, for $1 \leq i, j \leq 3$. Find the dual basis of $B = (\begin{bmatrix}1\\ 2\\ 1\end{bmatrix}, \begin{bmatrix}1\\ 0\\ 1\end{bmatrix}, \begin{bmatrix}0\\ 1\\ 1\end{bmatrix})$.

3.5.5. Give a different proof of Lemma 3.5.4 as follows: Let V be a finite dimensional vector space with ordered basis $B = (v_1, v_2, \ldots, v_n)$. Let $B^* = (v_1^*, v_2^*, \ldots, v_n^*)$ be the dual basis of V^*. If $v \in V$ is nonzero, show that $v_j^*(v) \neq 0$ for some j.

3.5.6. Prove parts (a) to (c) of Lemma 3.5.6.

3.5.7. Let V be a finite dimensional vector space and let W be a subspace. Show that $f \mapsto f_{|W}$ is a linear map from V^* to W^*, and that the kernel of this map is W°.

3.5.8. Let V be a finite dimensional vector space and let W be a subspace. Let $\pi : V \longrightarrow V/W$ be the quotient map. Show that $g \mapsto \pi^*(g) = g \circ \pi$ is a linear isomorphism of $(V/W)^*$ onto W°.

3.5.9. Prove Corollary 3.5.9.

3.5.10. Consider the $\mathbb{R}$-vector space $\mathcal{P}_n$ of polynomials of degree $\leq n$ with $\mathbb{R}$-coefficients, with the ordered basis $(1, x, x^2, \ldots, x^n)$.

(a) Find the matrix of differentiation $\frac{d}{dx} : \mathcal{P}_7 \to \mathcal{P}_7$.
(b) Find the matrix of integration $\int : \mathcal{P}_6 \to \mathcal{P}_7$.
(c) Observe that multiplication by $1 + 3x + 2x^2$ is linear from $\mathcal{P}_5$ to $\mathcal{P}_7$, and find the matrix of this linear map.

3.5.11. Let $B = (v_1, \ldots, v_n)$ be an ordered basis of a vector space V over a field K. Denote the dual basis of V^* by $B^* = (v_1^*, \ldots, v_n^*)$.

Show that for any $v \in V$ and $f \in V^*$,

$$\langle v, f\rangle = \sum_{j=1}^{n} \langle v, v_j^*\rangle\langle v_j, f\rangle.$$

3.5.12. Let $B = (v_1, \ldots, v_n)$ and $C = (w_1, \ldots, w_n)$ be two bases of a vector space V over a field K. Denote the dual bases of V^* by $B^* = (v_1^*, \ldots, v_n^*)$ and $C^* = (w_1^*, \ldots, w_n^*)$. Recall that $[\mathrm{id}]_{B,C}$ is the matrix with (i, j) entry equal to $\langle w_j, v_i^*\rangle$, and similarly, $[\mathrm{id}]_{C,B}$ is the matrix with (i, j) entry equal to $\langle v_j, w_i^*\rangle$.

Use the previous exercise to show that $[\mathrm{id}]_{B,C}$ and $[\mathrm{id}]_{C,B}$ are inverse matrices.

3.5.13. Let V, W be finite–dimensional vector spaces over K. Let B, B' be two ordered bases of V, and let C, C' be two ordered bases of W. Write $F = [\mathrm{id}]_{C',C}$ and $G = [\mathrm{id}]_{B',B}$. Let $T \in \mathrm{Hom}_K(V, W)$ and $S \in \mathrm{End}_K(V)$. Show that $[T]_{C',B'} = F\,[T]_{C,B}\,G^{-1}$.

3.5.14. Suppose that T and T' are two linear transformations of a finite dimensional vector space V, and that B and B' are two ordered bases of V. Show that $[T]_B$ and $[T']_{B'}$ are similar matrices if, and only if, T and T' are similar linear transformations.

3.5.15. Let T be the linear transformation of $\mathbb{R}^3$ with standard matrix $\begin{bmatrix} 1 & 5 & 2 \\ 2 & 1 & 3 \\ 1 & 1 & 4 \end{bmatrix}$. Find the matrix of $[T]_B$ of T with respect to the ordered basis $B = (\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix})$.

3.5.16. Show that $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ is not similar to any matrix of the form $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$. (Hint: Suppose the two matrices are similar. Use the similarity invariants determinant and trace to derive information about a and b.)

3.5.17. Let V be a vector space over K. Show that $\mathrm{End}_K(V)$ is a ring with identity.