Bases and Coordinates

Definition 1. Let V be a vector space over the field F. Let $S \subseteq V$ be a subset. The set S is said to be *linearly dependent over* F if there exist distinct $v_1, \dots, v_m \in S$ and $a_1, \dots, a_m \in F$, with not all $a_i = 0$, $m \geq 1$ so that

$$a_1 v_1 + a_2 v_2 + \cdots + a_m v_m = 0 \ . \tag{1}$$

This equation is called a *dependence relation.* If no such dependence relation exists, the set S is called *linearly independent over* F.

Note that the elements of a linearly independent set mnst be distinct (since there is otherwise an obvious non-trivial dependence relation).

If equation (1) holds for elements v_i of a linearly independent set, then all a_i must be 0.

The following properties are clear:

1. If $S \subseteq T$, then S linearly dependent implies that T is linearly dependent. Similarly, if T is linearly independent, then S is linearly independent.
2. The set $\{0\}$ is linearly dependent: $1 \cdot 0 = 0$ being the required dependence relation. Thus any set S containing 0 is linearly dependent.
3. The empty set ϕ is linearly independent.
4. A set S is linearly independent if and only if every finite subset of S is linearly independent.

Definition 2. A subset $\mathcal{B} \subseteq V$ is a *basis* for V over F if the following hold:

1. $\mathcal{B}$ is linearly independent over F,
2. $\text{Span}_F(\mathcal{B}) = V$.

The vector space V is called *finite dimensional* if it contains a finite snbset S with $\text{Span}_F(S) = V$.

We now introduce notation that will simplify computations, particularly for theoretical arguments. By doing this we manage to avoid awkward argnments where we must renumber lists of vectors which change during the discussion when new ones appear, or might appear. Let $\alpha_b \in F$ for $b \in \mathcal{B}$ be a collection of elements of F with only finitely many being non-zero. We then obtain a vector in V by taking the finite sum of the $\alpha_b b$ for those α_b which are non-zero. We abbreviate this as

$$\sum_{b \in \mathcal{B}} \alpha_b b \ . \tag{2}$$

That is, although this may appear to be an infinite sum (if $\mathcal{B}$ is infinite) it is actually a finite sum since only finitely many terms matter.

Our first lemma will give the primary tool for using bases.

Lemma 3. *Let $\mathcal{B}$ be a basis for the vector space V over the field F. Then every vector in V can be written uniquely as a finite linear combination of elements of $\mathcal{B}$.*

Proof. We must do two things: first show that for any vector $v \in V$ such an expression is possible, and second, show that there is only one such expression.

Since $\mathrm{Span}_F(\mathcal{B}) = V$, given $v \in V$ there exist $\alpha_b \in F$, only finitely many non-zero, so that

$$v = \sum_{b \in \mathcal{B}} \alpha_b b \ .$$

In order to prove the uniqueness of the expression, we assume that we are given a second expression for v:

$$v = \sum_{b \in \mathcal{B}} \beta_b b \ .$$

Subtraction of the second expression from the first yields

$$0 = \sum_{b \in \mathcal{B}} (\alpha_b - \beta_b) b \ .$$

However, $\mathcal{B}$ is linearly independent and hence all coefficients of the last equation are 0, that is $\alpha_b = \beta_b$ for all $b \in \mathcal{B}$. □

We now give a few examples of bases (see the section on "Examples of Vector Spaces").

1. For $1 \le i \le n$ let $e_i = (0, \ldots, 1, \ldots, 0)$ be the vector in F^n with 1 in the i-th position and 0 elsewhere and let $\mathcal{B} = \{ e_1, \ldots, e_n \}$. Then $\mathcal{B}$ is a basis for F^n called the *standard basis.* Consider the equation

$$(a_1, \ldots, a_n) = a_1 e_1 + \cdots + a_n e_n \ .$$

   Reading from left to right gives the formula to show that $\mathcal{B}$ spans; reading from right to left shows that if we assume the linear combination is the 0 vector of F^n, then all of the a_i must be 0, giving linear independence.

2. For $1 \le i \le m$ and $1 \le j \le n$ let e_{ij} be the matrix in $F^{m \times n}$ with 1 in position (i,j) and 0 elsewhere. If $A \in F^{m \times n}$ denotes the matrix with entries $a_{i,j} \in F$ in positions (i,j), then we have

$$A = \sum_{i,j} a_{i,j} e_{i,j} \ .$$

   As in the previous example, we conclude that $\mathcal{B} = \left\{ e_{i,j} \;\middle|\; 1 \le i \le m, \, 1 \le j \le n \right\}$ is a basis, also called the *standard basis.*

3. Let S be a finite, non-empty set and let F^S be the vector space of all functions from S to F. For $s \in S$, define the function $\delta_s : S \longrightarrow F$ by

$$\delta_s(t) = \begin{cases} 0 & t \neq s \\ 1 & t = s \end{cases}$$

We then have for $f \in F^S$ the formula

$$f = \sum_{s \in S} f(s)\delta_s \,.$$

This is easy to verify: given $t \in S$ the left-hand side is just $f(t)$ while the right-hand side has 0 for all terms where $t \neq s$; for the term where $t = s$, it has $f(t) \cdot 1$. And as in the previous examples, this one equation implies that $\mathcal{B} = \{ \delta_s \mid s \in S \}$ is a basis for F^S. WARNING: If S is infinite, the δ_s *do not* form a basis of F^S. They in fact span the subspace $F^{(S)}$ and form a basis for it. Further, the dimension of F^S over F is strictly larger than $|S|$.

4. For our last example, consider $F[x]$, the formal polynomials with coefficients in F, and let $\mathcal{B} = \{ 1, x, x^2, x^3, \ldots, x^i, \ldots \}$. This is a basis: $\mathcal{B}$ spans as every polynomial is a finite linear combination of the monomials x^i, by definition; $\mathcal{B}$ is linearly independent since the representation of a (formal) polynomial is unique, by definition.

Remark 4. The first three examples are really all the "same", or at least the same idea is involved. For F^n one can think of a vector $(a_1, \ldots, a_n)$ as a function a: $\{1, \ldots, n\} \longrightarrow \mathrm{F}$, with $a(i) = a_i$. Similarly, for A with entries $a_{i,j}$, one can think of a as a function on the set of pairs $\{ (i,j) \mid 1 \leq i \leq m, 1 \leq j \leq n \}$ with values in F given by $a(i,j) = a_{i,j}$. And of course the third example is such a set of functions. It should be clear how to give isomorphisms between such examples. In any case, we'll do this explicitly following our discussion of the Universal Mapping Property for Bases in what follows.

Two sets X and Y are said to be the same "size", or more precisely to have the same *cardinality* if there exists a one-to-one, onto function $f : X \longrightarrow Y$. It is easy to check that cardinality is reflexive (the identity function), symmetric (use the inverse), and transitive (use composition). One obtains thereby the analogue of an equivalence relation on the class of all sets. We write $|X|$ to denote the cardinality of the set X; and we write $|X| = |Y|$ to mean that they have the same cardinality (that i, there exists a on-to-one, onto function from X to Y). There is an "arithmetic" for cardinal numbers which we will not develop here. However, we will informally use this notion in our discussions and proofs – we will be careful to state all results on dimension in a manner so that they either remain valid for vector spaces of infinite dimension, or we will add the assumption "finite dimension" to the statements.

In addition we will say that the cardinality of the set X is less than or equal to the cardinality of the set Y if there exists a one-to-one function $f : X \longrightarrow Y$, and we denote this by $|X| \le |Y|$. An equivalent condition is that there is an onto function $g: Y \longrightarrow X$. The Schroeder-Bernstein Theorem (sometimes the name Cantor is also added) asserts that $|X| \le |Y|$ and $|Y| \le |X|$ imply that $|X| = |Y|$ (that is, the existence of two one-to-one functions going in opposite directions implies the existence of a one-to-one, onto function). The proof turns out to be surprisingly easy. See the section on the "Axiom of Choice and Zorn's Lemma" for further information.

The next result is the main theorem about bases we use. A proof for the finite-dimensional case uses the theory behind the solutions of homogeneous systems of linear equations and is given below. The proof in the general case requires the use of the Axiom of Choice, usually in the form of Zorn's Lemma. One may think of this as a way (analogous to mathematical induction) to handle very large sets. See the section on the "Axiom of Choice and Zorn's Lemma" for further explanation and proof of the following theorem.

Theorem 5 (Main Theorem for Bases). *Let V be a vector space over the field F.*

1. *There exists a basis for V.*
2. *If the subset $S \subseteq V$ spans V, then S contains a basis for V.*
3. *If the subset $S \subseteq V$ is linearly independent, then S is contained in some basis for V.*
4. *If $\mathcal{B}_1$ and $\mathcal{B}_2$ are two bases for V, then $|\mathcal{B}_1| = |\mathcal{B}_2|$.*

Corollary 6. *Let V be a vector space over the field F. If $I \subseteq V$ is a linearly independent subset and $S \subseteq V$ is a subset which spans V over F, then*

$$|I| \le |S|$$

(that is, there exists a one-to-one function $h: I \longrightarrow S$).

Proof. By the third part of the Main Theorem, there exists a basis $\mathcal{B}_1$ of V with $I \subseteq \mathcal{B}_1$. By the second part of the Main Theorem there exists a basis $\mathcal{B}_2$ of V with $\mathcal{B}_2 \subseteq S$. By the fourth part of the Main Theorem, there exists a one-to-one, onto function $f: \mathcal{B}_1 \longrightarrow \mathcal{B}_2$. Hence, let $h: I \longrightarrow S$ be the composition

$$I \xrightarrow{\text{inc}} \mathcal{B}_1 \xrightarrow{f} \mathcal{B}_2 \xrightarrow{\text{inc}} S$$

where inc denotes the inclusion function in both cases. That is, $h = \text{inc} \circ f \circ \text{inc}$ is a one-to-one function since it is the composition of three one-to-one functions. Equivalently,

$$|I| \le |S| .$$

□

Definition 7. Let V be a vector space over the field F and let W be a subspace of V. A subspace W' of V is called a *complement* of W if V is the internal direct sum of W and W'.

Corollary 8. *Let V be a vector space over the field F and let W be a subspace of V. Then a complement of W in V exists.*

Proof. Let $\mathcal{A}$ be a basis for W. Clearly $\mathcal{A}$ is a linearly independent subset of V and hence by the third part of the Main Theorem, there exists a basis $\mathcal{B}$ for V containing $\mathcal{A}$. Let $\mathcal{A}'$ be the set $\mathcal{B}$ with $\mathcal{A}$ removed. Then $\mathcal{B}$ is the disjoint union of $\mathcal{A}$ and $\mathcal{A}'$. Let $W' = \mathrm{Span}_F(\mathcal{A}')$. Clearly $W + W' = V$ as every element of a basis of V is contained in $W + W'$. Further $W \cap W' = 0$ since a vector v in the intersection can be expressed as a linear combination of elements in $\mathcal{A}$ and similarly as a linear combination of elements in $\mathcal{A}'$. The difference of these two expressions is 0 and as it is a linear combination of elements of the linearly independent set $\mathcal{B}$, all coefficents must be 0. □

Remark 9. If $W \subseteq V$ is a proper subspace (i.e., neither 0 nor V), then W will have more than one complement. For example, in $V = \mathbb{R}^2$, if W is the span of a non-zero vector, then the span of any vector not in W will be a complement to W.

Corollary 10. *Every short exact sequence of vector spaces splits.*

Proof. This is an easy consequence of the preceding corollary, [See the section on "Short Exact Sequences" for the terminology, and for exercises related to these two corollaries.] □

We now give a proof of the Main Theorem for Bases (Theorem 5) in the case where the vector space V is finite-dimensional.

Proof. The first part of the theorem (that bases exist) is a consequence of the second part, that there is a subset of S which is a basis. Similarly, the first part is also a consequence of the third part since one can start with the linearly independent set $\varnothing$, the empty set.

As this vector space V is finite dimensional, there is a finite subset $S \subseteq V$ which spans V over F.

We now prove that there is a subset of S which is a basis for V. If S is linearly independent, the S itself is a basis since we already know it spans V. If $S = \{v_1, \ldots, v_n\}$ is not linearly independent, then there will exist $a_i \in F$, not all 0, which give a dependence relation:

$$a_1 v_1 + \cdots + a_n v_n = 0 \ .$$

Since not all of the coefficients are 0, there will be some j with $a_j \neq 0$. Thus

$$v_j = \frac{-a_1}{a_j} v_1 + \cdots + \frac{-a_n}{a_j} v_n$$

where the j-th term has been omitted from the right-hand side. Thus the smaller set $S_1 = S \setminus \left\{ v_j \right\}$ will still span V. If S_1 is linearly independent, then it forms a basis for V, and if not, some vector in S_1 will be a linear combination of the remaining ones. Then we can construct a strictly smaller spanning set S_2 by removing that vector as well. Continuing this process we will end up with a basis for V in at most $|S|$ steps.

Let $I = \{u_1, \ldots, u_m\}$ be a linearly independent subset of V. If I spans V, then I itself is a basis and we are done. If it does not span V, then there will be some vector $v_j \in S$ which is not contained in $\mathrm{Span}_F(I)$. Let $I_1 = I \cup \left\{ v_j \right\}$. Then this set I_1 is strictly larger, and is in fact linearly independent. For if not, there exist some $b_i, a \in F$, not all 0 ,with

$$b_1 u_1 + \cdots + b_m u_m + a v_j = 0 .$$

Now if $a \neq 0$, then solving the equation shows that $v_j \in \mathrm{Span}_F(I)$, a contradiction. Thus $a = 0$. But then all $b_k = 0$ since I is a linearly independent set. This contradiction shows that in fact I_1 must be linearly independent (and hence is strictly larger than I). If I_1 spans V, then it is a basis, and we're done. If not, then there is yet another element of S which did not lie in $\mathrm{Span}_F(I)$. We let I_2 be the set obtained as the union of I_1 and this additional vector of S which was not in the span. The same argument as before shows that I_2 is linearly independent, and a strictly larger set. If it spans V we are done. If not, we continue in the same fashion. After at most $|S|$ steps the process must cease since there will be no more vectors from S to add, and hence none that are not in the span of the just constructed set.

Finally, we will verify that any two bases for a finite dimensional V must have the same number of elements. Let $I = \{u_1, \ldots, u_m\}$ be a linearly independent subset of V and let $S = \{v_1, \ldots, v_n\}$ be a spanning set. We now show that $m = |I| \leq |S| = n$, as stated in Corollary 6 for the case of arbitrary V. Since S spans, for each $u_j \in I$ there will exist $a_{ij} \in F$ such that

$$u_j = a_{1j} v_1 + \cdots + a_{nj} v_n .$$

Let $A = (a_{ij})$ be the $n \times m$ matrix with entries the a_{ij}. If $n < m$, then the matrix equation $AX = 0$ would have a non-trivial solution, say with entries $b_1, \ldots, b_m$ (not all 0) so that

$$b_1 u_1 + \cdots + b_m u_m = 0$$

which is impossible as the set I is linearly independent. Thus $n \geq m$ must hold, that is $|S| \geq |I|$ as asserted.

Now let $\mathcal{B}_1$ and $\mathcal{B}_2$ be two bases for V. As $\mathcal{B}_1$ is linearly independent and $\mathcal{B}_2$ spans, we then have $|\mathcal{B}_1| \leq |\mathcal{B}_2|$. Switching the roles of the two bases yields the inequality in the other direction, and thus we must have $|\mathcal{B}_1| = |\mathcal{B}_2|$. □

For a different proof that can be generalized to the infinite diminsional case see Exercise 24.

In our argument we proved the following lemma that is useful in many situations:

Lemma 11. *Let V be a vector space over the field F. If $I \subseteq V$ is a linearly independent subset and $v \in V$ is not in $\mathrm{Span}_F(I)$, then the set $I \cup \{v\}$ is linearly independent.*

Coordinates

Our first application of Theorem 5 will be via Equation (2) to obtain the *coordinates* of a vector with respect to a basis.

Let $\mathcal{B} \subseteq V$ be a basis for the vector space V over F. Lemma 3 asserts that for a vector $v \in V$ the coefficients $\alpha_b \in F$ in Equation 2 are uniquely determined:

$$v = \sum_{b \in \mathcal{B}} \alpha_b b\,.$$

Hence we obtain a function from $\mathcal{B}$ to F, which we denote by $[v]_{\mathcal{B}}$, that is $[v]_{\mathcal{B}}$ evaluated at $b \in \mathcal{B}$ is just the α_b in this equation.

Recall (see the section on "Direct Sums and Products") that the direct sum of $\mathcal{B}$ copies of F, denoted $\bigoplus_{b\in\mathcal{B}} F$, is just the set of functions from $\mathcal{B}$ to F, which are non-zero for at most finitely many elements of $\mathcal{B}$. This is also the same as $F^{(\mathcal{B})}$. Hence we obtain a function

$$[\ \ ]_{\mathcal{B}} : V \longrightarrow \bigoplus_{b\in\mathcal{B}} F = F^{(\mathcal{B})} \tag{3}$$

which when evaluated at $v \in V$, gives the function $[v]_{\mathcal{B}}$.

To restate explicitly, we have a function whose values are also functions:

$[\ \ ]_{\mathcal{B}}$ sends v to the function $[v]_{\mathcal{B}}$

$[v]_{\mathcal{B}}$ is the function that sends $b \in \mathcal{B}$ to α_b

– the last statement, using ordinary notation for functions, is just $[v]_{\mathcal{B}}(b) = \alpha_b$.

Theorem 12 (Coordinates with Respect to a Basis). *Let V be a vector space over the field F with basis $\mathcal{B}$. Taking coordinates with respect to the basis $\mathcal{B}$ gives an isomorphism of V with the direct sum of $\mathcal{B}$ copies of F; that is*

$$[\ \ ]_{\mathcal{B}} : V \longrightarrow \bigoplus_{b\in\mathcal{B}} F = F^{(\mathcal{B})}$$

is an isomorphism of vector spaces.

Proof. Let v and w be two vectors in V and express them as linear combinations of the basis:

$$\begin{aligned} v &= \sum_{b\in\mathcal{B}} \alpha_b b \\ w &= \sum_{b\in\mathcal{B}} \beta_b b\,. \end{aligned}$$

Adding the two yields

$$v + w = \sum_{b \in \mathcal{B}} (\alpha_b + \beta_b) b$$

and thus for any $b \in \mathcal{B}$

$$\begin{aligned} [v + w]_{\mathcal{B}}(b) &= \alpha_b + \beta_b \\ &= [v]_{\mathcal{B}}(b) + [w]_{\mathcal{B}}(b) \\ &= ([v]_{\mathcal{B}} + [w]_{\mathcal{B}})(b) \ . \end{aligned}$$

Hence $[v + w]_{\mathcal{B}} = [v]_{\mathcal{B}} + [w]_{\mathcal{B}}$, since two functions are equal precisely when they have the same value for each element of the domain $\mathcal{B}$.

Similarly for $c \in F$,

$$cv = \sum_{b \in \mathcal{B}} (c\alpha_b) b$$

and thus

$$\begin{aligned} [cv]_{\mathcal{B}}(b) &= c\alpha_b \\ &= c([v]_{\mathcal{B}}(b)) \\ &= (c[v]_{\mathcal{B}})(b) \ . \end{aligned}$$

Hence the two functions are equal: $[cv]_{\mathcal{B}} = c[v]_{\mathcal{B}}$.

We've now verified that $[\ \ ]_{\mathcal{B}}$ is a linear transformation.

The function $[\ \ ]_{\mathcal{B}}$ is one-to-one since a vector v is determined by its coordinates α_b. Finally, $[\ \ ]_{\mathcal{B}}$ is onto for a similar reason; given a function $f \in \bigoplus_{b \in \mathcal{B}} F$, the vector $u \in V$ given by the finite sum

$$u = \sum_{b \in \mathcal{B}} f(b) b$$

will satisfy $[u]_{\mathcal{B}} = f$ since the two functions do the same thing on elements of $\mathcal{B}$. □

Up to this point coordinates with respect to a basis have been treated abstractly, which is a good way to do it if one is interested in proving things. However, sometimes one wants to make concrete computations, and even write them on the blackboard or a piece of paper. How does one write down a function on a basis? One very inefficient way to do it would be to write down the basis element in one column and next to it the value of the function. As we write on a two-dimensional surface, this means in addition we have to make a choice as to the order we write things down and we also need to list the basis elements. This is usually abbreviated by deciding in advance the order we pick, fixing that order throughout the discussion, and taking advantage of the geometry of a two-dimensional surface to indicate the order (as well as our own internal concept of 1^{st}, 2^{nd}, 3^{rd}, ...).

We will mainly restrict our attention now to finite dimensional vector spaces. An *ordered basis* $\mathcal{B}$ for V is simply a basis where we have chosen in advance an order for the elements: $\mathcal{B} = \{ b_1, \ldots, b_n \}$. We will now use the same notation as used above to denote the coordinates of a vector with respect to an ordered basis $\mathcal{B}$. If $v \in V$ can be written as $v = \sum_{i=1}^{n} \alpha_i b_i$ we will write $[v]_{\mathcal{B}} \in F^{n\times 1}$ as follows:

$$[v]_{\mathcal{B}} = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix}$$

We restate the finite dimensional case of Theorem 12:

Corollary 13 (Coordinates with Respect to a Basis). *Let V be a finite dimensional vector space over the field F with ordered basis $\mathcal{B}$. Then taking coordinates with respect to the ordered basis $\mathcal{B}$ gives an isomorphism of V with $F^{n\times 1}$; that is*

$$[\quad]_{\mathcal{B}} : V \longrightarrow F^{n\times 1}$$

is an isomorphism of vector spaces.

Universal Mapping Property for Bases

We now give the usual theorem which describes all linear transformations in terms of a given basis for a vector space stated as a *universal mapping property*.

Theorem 14 (Universal Mapping Property for Bases). *Let U and V be vector spaces over F. Let $\mathcal{B} \subseteq V$ be a basis for V and let $i : \mathcal{B} \longrightarrow V$ be the inclusion map. For any function $t : \mathcal{B} \longrightarrow U$, there exists a unique linear transformation $T : V \longrightarrow U$ such that the following diagram commutes:*

$$\begin{tikzcd}
\mathcal{B} \arrow[r, "i"] \arrow[dr, "t"'] & V \arrow[d, dotted, "T"] \\
& U
\end{tikzcd}$$

that is, $T \circ i = t$.

Proof. In outline, in almost all cases, proofs of universal mapping properties take the following form: first show uniqueness, next use the result of uniqueness (typically a formula) to show existence of the sought-after function, and finally verify that the function just constructed has all of the right properties.

Uniqueness: Our assumption means that $T \circ i(b) = t(b)$ or $T(b) = t(b)$ for any $b \in \mathcal{B}$. Given $v \in V$ we can write $v = \sum_{b\in\mathcal{B}} \alpha_b b$ uniquely as noted earlier. Hence if T exists and is a linear transformation,

$$\begin{aligned} T(v) &= T\Big(\sum_{b\in\mathcal{B}} \alpha_b b\Big) \\ &= \sum_{b\in\mathcal{B}} \alpha_b T(b) \end{aligned}$$

yielding

$$T(v) \;=\; \sum_{b\in\mathcal{B}} \alpha_b t(b)\ . \tag{4}$$

Thus $T(v)$, if it exists, is uniquely determined by t (since the α_b are uniquely determined by $\mathcal{B}$ and v).

Existence: In view of the previous part, we define T by the formula in Equation (4). In contrast to the situation we found for quotient spaces, there is no ambiguity at all (no choices were made, no representatives were used) in this definition. Hence T exists as a *function.*

Properties:. Finally, we must show that T is the right kind of function, a linear transformation. Suppose we also have a vector $w \in V$ and we write $w = \sum_{b\in\mathcal{B}} \beta_b b$ for unique $\beta_b \in F$. Then $v + w = \sum_{b\in\mathcal{B}}(\alpha_b + \beta_b)b$

$$\begin{aligned}
T(v+w) &= T\big(\sum_{b\in\mathcal{B}}(\alpha_b+\beta_b)b\big)\\
&= \sum_{b\in\mathcal{B}}(\alpha_b+\beta_b)t(b)\\
&= \sum_{b\in\mathcal{B}}\alpha_b t(b) + \sum_{b\in\mathcal{B}}\beta_b t(b)\\
&= T(v)+T(w)
\end{aligned}$$

And finally if $c \in F$, then $cv = \sum_{b\in\mathcal{B}} c\alpha_b b$. Hence

$$\begin{aligned}
T(cv) &= T\big(\sum_{b\in\mathcal{B}} c\alpha_b b\big)\\
&= \sum_{b\in\mathcal{B}} c\alpha_b t(b)\\
&= c\big(\sum_{b\in\mathcal{B}}\alpha_b t(b)\big)\\
&= cT(v)
\end{aligned}$$

□

Remark 15. 1. The term “commutes” will more generally mean the following: if one has a diagram with a number of objects (e.g., vector spaces, fields, or whatever) with a number of functions (arrows) between some of the objects, we say that the diagram *commutes* if for every pair of objects which can be connected by a path (all arrows pointing the same direction so that composition of the corresponding functions is possible) in more than one way, the compositions of the functions along the various possible paths must always be equal. Note that in our situation above, this didn't say a lot as there were only two objects that could be connected by two paths this way and hence only one resulting equation.

2. A universal mapping property such as the one just described always gives a one-to-one correspondence (bijection) between two collections of functions. In this case the first is just a collection of ordinary functions, while the second is a set of linear transformations.

$$\theta : \{ t \mid t : \mathcal{B} \longrightarrow U \} \longrightarrow \mathrm{Hom}_F(V, U)$$

where we write $\mathrm{Hom}_F(V,U)$ for the set of all linear transformations from V to U (this is denoted $\mathcal{L}(V,U)$ in some textbooks).

Here $\theta(t) = T$ is given by the theorem. This map is one-to-one as two different functions give two different linear transformations. Further, θ is onto, since given any $T \in \mathrm{Hom}_F(V,U)$ we can define the required t by $t = T \circ i$, i.e., just T restricted to $\mathcal{B}$: $\theta(T \circ i) = T$.

Dimension and Dimension Formulas

Our next application of Theorem 5 will be to define the dimension of a vector space: If V is a vector space over F, then the *dimension* of V is the cardinality of any basis for V. So if $\mathcal{B}$ is a basis for V, we write $\dim_F V = |\mathcal{B}|$. So the examples we had earlier yield $\dim_F F^n = n$, $\dim_F F^{m\times n} = mn$, $\dim_F F^S = |S|$ for a finite non-empty set S, and $\dim_F F[x] = |\mathbb{N}|$ where $\mathbb{N} = \{0, 1, 2, \ldots, i, \ldots\}$. The set $\mathbb{N}$, or any other set with the same cardinality, is said to be *countable*. Many times this cardinal number is denoted by the Hebrew letter aleph with a subscript zero: $|\mathbb{N}| = \aleph_0$. See the section on the "Axiom of Choice and Zorn's Lemma" for further information.

We begin by listing a few simple facts that are easily derived from our previous discussion. Below V and V' will denote vector spaces over the field F. We write $\dim V$ for $\dim_F V$.

Fact 1. Let $\mathcal{B}$ be a basis for V and let $S \subseteq V$.

a. If S is linearly independent, then $|S| \leq |\mathcal{B}|$.

b. If S spans V, then $|S| \geq |\mathcal{B}|$.

c. If $|S| > \dim V$, then S is linearly dependent.

d. If $|S| < \dim V$, then $\mathrm{Span}_F(S) \neq V$.

Proof. By the Main Theorem on Bases (Theorem 5) any linearly independent set can be enlarged to a basis, so part a. is clear as all bases have the same number of elements.

Similarly, any spanning set contains a basis, yielding part b.

Part c. follows as S would contain a basis which is not all of S and any of the other elements of S would have to be a linear combination of some of these these (which gives a dependence relation).

If $\mathrm{Span}_F(S) = V$, then S would contain a basis, so $|S| \geq \dim V$, contradicting the assumption. □

Fact 2. Let $W \subseteq V$ be a subspace. Assume $\dim V < \infty$. Then $W = V$ if and only if $\dim W = \dim V$.

Proof. A basis $\mathcal{A}$ for W can be enlarged to a basis $\mathcal{B}$ for V since $\mathcal{A}$ is a linearly independent set. If $\mathcal{A}$ has fewer elements than $|\mathcal{B}| = \dim V$, then $W \neq V$. If $\mathcal{A}$ has the same number of elements as $\mathcal{B}$, then $\mathcal{A} = \mathcal{B}$, so $W = V$. □

Fact 3. Let $W \subseteq V$ be a subspace, with $\dim W = \dim V$. Assume $\dim V$ is not finite. Then W may or may not be equal to V.

Proof. Consider $V = F[x]$ with basis $\mathcal{B} = \{1, x, x^2, x^3, \ldots, x^i, \ldots\}$ and proper subset $\mathcal{A} = \{x, x^2, x^3, \ldots, x^i, \ldots\}$. Then the function $f : \mathcal{B} \longrightarrow \mathcal{A}$ given by $f(x^i) = x^{i+1}$ is one-to-one and onto. Hence the proper subspace $W = \mathrm{Span}_F(\mathcal{A})$ has the same dimension as V. For an arbitrary infinite dimensional vector space V with basis $\mathcal{B}$ one can embed $\{1, 2, \ldots, n, \ldots\}$ into $\mathcal{B}$ and use the same idea to construct a proper subspace with the same dimension as V. □

Fact 4. Let $\dim V = n < \infty$ and let $S \subseteq V$. Assume $|S| = n$. Then the following are equivalent:

a. The set S is linearly independent.

b. The set S spans V: $\mathrm{Span}_F(S) = V$.

c. The set S is a basis for V.

Proof. This is immediate from the first Fact; or follows directly from the Main Theorem on Bases by using the same ideas: enlarge S to a basis in the first part, find a subset which is a basis in the second part. In either case one ends up with just S as otherwise we have a basis that is too large, or too small. And of course the last part implies the other two. □

Fact 5. If $\mathcal{B}$ is a basis for V, then V is isomorphic to a direct sum of $|\mathcal{B}|$ copies of F.

Proof. This is just the content of Theorem 12 giving coordinates with respect to a basis. □

Fact 6. We have $\dim V = \dim V'$ if and only if $V \approx V'$.

Proof. If $\mathcal{B}$ is a basis for V and $\mathcal{B}'$ is a basis for V', there is a one-to-one onto function $t : \mathcal{B} \longrightarrow \mathcal{B}'$ by the definition of equality of dimension (and the fact that any two bases for a vector space have the same cardinality). The Universal Mapping Property for Bases implies that there is a linear transformation $T : V \longrightarrow V'$ which is t on the basis $\mathcal{B}$. Applying this again for the inverse function $t^{-1} : \mathcal{B}' \longrightarrow \mathcal{B}$ gives a linear transformation T^{-1} which is the inverse of T.

Conversely if $T : V \longrightarrow V'$ is an isomorphism, it is easy to check that $T(\mathcal{B})$ is a basis for V' (so T gives the one-to-one, onto function between bases), yielding $\dim V = \dim V'$. □

Fact 7. Let $A \in F^{n\times n}$ for $n > 0$ an integer. Then the following are equivalent:

a. The rows of A are linearly independent.

b. The columns of A are linearly independent.

c. The rows of A span $F^{1\times n}$.

d. The columns of A span $F^{n\times 1}$.

e. A has a left inverse.

f. A has a right inverse.

g. A has an inverse.

h. The row reduced echelon form of A is I (the $n \times n$ identity matrix).

i. The column reduced echelon form of A is I (the $n \times n$ identity matrix).

j. A is a product of elementary matrices.

Proof. The column space of A is contained in $F^{n\times 1}$ and the row space of A is contained in $F^{1\times n}$, both of which have dimension n. In view of the previous facts, as A has n rows and n columns, a. through d. are equivalent (and are also equivalent to the statements that the rows are a basis for the row space and the columns are a basis of the column space).

Now the first chapter of Hoffman and Kunze, Theorem 12 on page 23 shows that g. through j. are equivalent.

Now A is invertible (part g.) if and only if A has a left inverse (part e.) and A has a right inverse (part f.).

We now tie these different sets of statements together. If we call the rows of A $v_1, \ldots, v_n$ and assume part c. (that the v_i span the row space), then there exist $b_{ij} \in F$ so that

$$\begin{aligned} b_{11}v_1 + \cdots + b_{in}v_n &= e_1 \\ b_{21}v_1 + \cdots + b_{2n}v_n &= e_2 \\ \vdots \qquad & \quad \vdots \\ b_{n1}v_1 + \cdots + b_{nn}v_n &= e_n \end{aligned}$$

where $\{e_1, \ldots, e_n\}$ is the standard basis of $F^{1\times n}$. Letting B be the matrix with entries b_{ij} the system of equations above is just $BA = I$, the $n \times n$ identity matrix. This is just part e. On the other hand the equation $BA = I$ gives a system of equations as above that shows the rows of A span. Similarly part d. (columns span) implies part f., and vice versa. □

The proofs of the next five theorems use the same ideas. We will thus give the most general (abstract) statement and derive the others as consequences. On the other hand, the outline of the proof in this part easily gives the usual (e.g., in many textbooks) proofs of the other results.

Theorem 16. *Let W, V, and U be vector spaces over the field F and assume that*

$$0 \longrightarrow W \longrightarrow V \longrightarrow U \longrightarrow 0$$

is a short exact sequence. Then

$$\dim V = \dim W + \dim U \ .$$

Proof. In outline we do the following: We take a basis $\mathcal{A}$ for W, apply the linear transformation to get a linearly independent set $\mathcal{B}_1$ of the same cardinality in V, enlarge to a basis $\mathcal{B}$ for V. We write $\mathcal{B} = \mathcal{B}_1 \dot{\cup} \mathcal{B}_2$ where $\mathcal{B}_2$ is the set of additional vectors we had to add (disjoint from $\mathcal{B}_1$). We apply the next linear transformation to this basis $\mathcal{B}$. The linear transformation sends $\mathcal{B}_1$ to 0 and we define $\mathcal{C}$ to be the image of $\mathcal{B}_2$ in U. It will have the same cardinality as $\mathcal{B}_2$. This will yield the result:

$$\begin{aligned} \dim V &= |\mathcal{B}| \\ &= |\mathcal{B}_1| + |\mathcal{B}_2| \\ &= |\mathcal{A}| + |\mathcal{C}| \\ &= \dim W + \dim U \ . \end{aligned}$$

Let $S : W \longrightarrow V$ be the first linear transformation and $T : V \longrightarrow U$ the second. The sequence being exact means

- S is one-to-one,
- $\operatorname{im} S = \ker T$,
- T is onto.

We set $\mathcal{B}_1 = S(\mathcal{A})$. Since S is one-to-one, the two sets have the same cardinality. Further, if $w = \sum_{a\in\mathcal{A}} \alpha_a a$ is a linear combination of elements of $\mathcal{A}$, then $S(w) = \sum_{a\in\mathcal{A}} \alpha_a S(a)$, is a linear combination of elements of $\mathcal{B}_1 = S(\mathcal{A})$. This linear combination will be 0 in V if and only if the original linear combination, w, is 0 in W since S is one-to-one. That is, $\mathcal{B}_1$ is a linearly independent subset of V. By the Main Theorem on Bases, there exists a basis $\mathcal{B}$ for V which contains the linearly independent set $\mathcal{B}_1$. We write $\mathcal{B} = \mathcal{B}_1 \dot{\cup} \mathcal{B}_2$ where $\mathcal{B}_2$ (disjoint from $\mathcal{B}_1$) consists of the extra vectors that were needed.

Next we let $\mathcal{C} = T(\mathcal{B}_2)$. As T is onto, $T(\mathcal{B})$ spans U, but $T(\mathcal{B}_1) = TS(\mathcal{A}) = 0$, so $\mathcal{C} = T(\mathcal{B}_2)$ spans U. The only thing left to show is that $\mathcal{C} = T(\mathcal{B}_2)$ is linearly independent. Assume that there exist $\beta_{b,2} \in F$ such that

$$\begin{aligned} 0 &= \sum_{b\in\mathcal{B}_2} \beta_{b,2} T(b) \\ &= T\big(\sum_{b\in\mathcal{B}_2} \beta_{b,2} b\big) \ . \end{aligned}$$

Thus $\sum_{b\in\mathcal{B}_2} \beta_{b,2} b \in \ker T = \operatorname{im} S$. Hence there exist $\beta_{b,1} \in F$ so that

$$\sum_{b\in\mathcal{B}_1} \beta_{b,1} b = \sum_{b\in\mathcal{B}_2} \beta_{b,2} b$$

or

$$0 = \sum_{b\in\mathcal{B}_1} \beta_{b,1} b - \sum_{b\in\mathcal{B}_2} \beta_{b,2} b \ .$$

Now as $\mathcal{B} = \mathcal{B}_1 \dot{\cup} \mathcal{B}_2$ we have produced a linear combination of the basis elements of V which is 0. Hence all $\beta_{b,j} = 0$, and in particular it follows that $\mathcal{C} = T(\mathcal{B}_2)$ is linearly independent, completing the proof. □

Theorem 17. *Let V_1 and V_2 be vector spaces over the field F. Then*

$$\dim(V_1 \oplus V_2) = \dim V_1 + \dim V_2 \ .$$

Proof. Earlier we showed that the following sequence is exact:

$$0 \longrightarrow V_1 \xrightarrow{\iota} V_1 \oplus V_2 \xrightarrow{\pi} V_2 \longrightarrow 0$$

and hence this result follows from the short exact sequence version, Theorem 16. Here ι is inclusion into V_1 and π is projection onto V_2.

If one wants a specific basis, then given bases $\mathcal{B}_1$ for V_1 and $\mathcal{B}_2$ for V_2, a basis $\mathcal{B}$ constructed as above is the union of the two collections of the form $\mathcal{B}_1' = \{(b_1, 0) \mid b_1 \in \mathcal{B}_1\}$ and $\mathcal{B}_2' = \{(0, b_2) \mid b_2 \in \mathcal{B}_2\}$. □

Remark 18. Subtraction of cardinal numbers is neither well-defined nor useful in most cases (e.g., removing an infinite subset from $\{1, 2, \ldots, n, \ldots\}$ can leave a finite or an infinite subset). However, for finite sets we do it all the time which is the content of the last equation in the next two results.

Theorem 19. *Let V be a vector space over the field F with $W \subseteq V$ a subspace. Then*

$$\dim V = \dim W + \dim V/W \ .$$

If V has finite dimension, then

$$\dim V/W = \dim V - \dim W \ .$$

Proof. The construction of quotient spaces gives the exact sequence:

$$0 \longrightarrow W \xrightarrow{i} V \xrightarrow{p} V/W \longrightarrow 0$$

and hence the result follows from the general one. □

Theorem 20. *Let V be a vector space over F with two subspaces $W_1, W_2 \subseteq V$. Then*

$$\dim(W_1 \cap W_2) + \dim(W_1 + W_2) = \dim W_1 + \dim W_2 \ .$$

If W_1 and W_2 have finite dimension, then

$$\dim(W_1 + W_2) = \dim W_1 + \dim W_2 - \dim(W_1 \cap W_2) \ .$$

Proof. Consider the linear transformation $s : W_1 \oplus W_2 \longrightarrow W_1 + W_2$ given by $s(w_1, w_2) = w_1 + w_2$ (the formal pair (w_1, w_2) goes to the actual sum $w_1 + w_2$ in V). Thus s is onto by definition of $W_1 + W_2$ and the kernel consists of pairs (w_1, w_2) such that $w_1 + w_2 = 0$. That is, $w_1 = -w_2$; call this vector w. It is clearly in $W_1 \cap W_2$. We then have an exact sequence

$$0 \longrightarrow W_1 \cap W_2 \xrightarrow{j} W_1 \oplus W_2 \xrightarrow{s} W_1 + W_2 \longrightarrow 0$$

where $j(w) = (w, -w)$, and hence the result follows from the general one. □

Theorem 21. *Let U and V be vector spaces over the field F with $\dim_F U = \dim_F V$ finite. Let $T : U \longrightarrow V$ be a linear transformation. Then the following are equivalent:*

a. T has an inverse.

b. T is one-to-one.

c. T is onto.

Proof. In general we have $\dim_F \ker T = 0$ if and only if $\ker T = 0$ if and only if T is one-to-one. And for finite dimensional V we have in general $\dim_F \operatorname{im} T = \dim_F V$ if and only if $\operatorname{im} T = V$ if and only if T is onto. Since $\dim_F U = \dim_F V = \dim_F \ker T + \dim_F \operatorname{im} T$ the two conditions are the same. Note that the second equality comes from the isomorphism $V/\ker T \approx \operatorname{im} T$. That is, parts b. and c. are equivalent. But part a. is equivalent to both b. and c. holding. This completes the proof. □

Remark 22. This result is false if the two vector spaces have equal but infinite dimension. For example, take $F[x]$ and define the linear transformation $\mathbf{up} : F[x] \longrightarrow F[x]$ on the standard basis by $\mathbf{up}(x^i) = x^{i+1}$. Similarly define the linear transformation $\mathbf{down} : F[x] \longrightarrow F[x]$ by $\mathbf{down}(1) = 0$ and $\mathbf{down}(x^i) = x^{i-1}$ for $i > 0$. It is clear that $\mathbf{down} \circ \mathbf{up} = 1_{F[x]}$ as it has this property on the basis; so **down** is a left inverse to **up**. Thus **up** is one-to-one and **down** is onto. But **up** is not onto as $1 \notin \operatorname{im} \mathbf{up}$ and **down** is not one-to-one as $1 \in \ker \mathbf{down}$. One can give similar examples for any infinite basis $\mathcal{B}$ by embedding $\{1, 2, \ldots, n, \ldots\}$ into $\mathcal{B}$ and using exactly the same idea.

Vector Spaces of Linear Transformations: $\mathrm{Hom}_{\mathbf{F}}(\mathbf{U},\mathbf{V})$

Let U and V be vector spaces over the field F. We denote by $\mathrm{Hom}_F(U,V)$ the set of all linear transformations from U to V (denoted $\mathcal{L}(U,V)$ in some texts).

Addition and scalar multiplication are defined on $\mathrm{Hom}_F(U,V)$ as follows: For $S,T \in \mathrm{Hom}_F(U,V)$, $u \in U$ and $c \in F$ by

$$(S+T)(u) \quad = \quad S(u)+T(u)$$

and

$$(cT)(u) \quad = \quad cT(u)\ .$$

Note that this is a generalization of the idea that was used to define a vector space structure on F^S for a non-empty set S. It is easy to check (and will be left to the reader) that the resulting functions, $S+T$ and cT are indeed linear transformations from U to V, and that the axioms for a vector space are satisfied. For example, one easily checks that the 0 function is the zero of $\mathrm{Hom}_F(U,V)$ and $-T$ is the additive inverse of T.

Theorem 23. *Let U and V be finite dimensional vector spaces over the field F. Then*

$$\dim_F \mathrm{Hom}_F(U,V) = \dim_F U \cdot \dim_F V\ .$$

Proof. Let $\mathcal{A}$ be a basis for U and $\mathcal{B}$ a basis for V. For each $a \in \mathcal{A}$ and $b \in \mathcal{B}$ we define a linear transformation $T_{a,b} : U \longrightarrow V$ via the Universal Mapping Property by specifying it on a basis $\mathcal{A}$ for U:

$$T_{a,b}(a') = \begin{cases} 0 & a' \neq a \\ b & a' = a \end{cases}$$

for $a' \in \mathcal{A}$.

We will show that $\mathcal{C} = \left\{ T_{a,b} \;\middle|\; a \in \mathcal{A},\, b \in \mathcal{B} \right\}$ is a basis for $\mathrm{Hom}_F(U,V)$. We then have

$$\begin{aligned} \dim U \cdot \dim V &= |\mathcal{A}| \cdot |\mathcal{B}| \\ &= |\mathcal{A} \times \mathcal{B}| \\ &= \left| \left\{ T_{a,b} \;\middle|\; a \in \mathcal{A},\, b \in \mathcal{B} \right\} \right| \end{aligned}$$

We first show that the set $\mathcal{C}$ is linearly independent. Suppose that there exist $\gamma_{a,b} \in F$ such that

$$0 = \sum_{a \in \mathcal{A}, b \in \mathcal{B}} \gamma_{a,b} T_{a,b}\ .$$

Note that the 0 on the left is the zero linear transformation from U to V (whereas it is the 0 of F in the next equation below). We apply this linear tranformation to some $a' \in \mathcal{A}$ and obtain

$$\begin{aligned} 0 &= \sum_{a\in\mathcal{A}, b\in\mathcal{B}} \gamma_{a,b} T_{a,b}(a') \\ &= \sum_{b\in\mathcal{B}} \gamma_{a',b} b \end{aligned}$$

and as $\mathcal{B}$ is a basis yields $\gamma_{a',b} = 0$, for any $a' \in \mathcal{A}$ and any $b \in \mathcal{B}$.

We finally show that $\mathcal{C}$ spans $\mathrm{Hom}_F(U,V)$ which completes the proof. Given $S \in \mathrm{Hom}_F(U,V)$ since $\mathcal{B}$ is a basis for V, there exist $\beta_{a,b} \in F$ so that

$$S(a) = \sum_{b\in\mathcal{B}} \beta_{a,b} b$$

and by our definition of $T_{a,b}$ we thus have

$$S(a) = \sum_{b\in\mathcal{B}} \beta_{a,b} T_{a,b}(a) .$$

Thus S and $\sum_{a\in\mathcal{A}} \sum_{b\in\mathcal{B}} \beta_{a.b} T_{a,b}$ agree on every basis element $a' \in \mathcal{A}$ and hence are the same linear transformation, that is

$$S = \sum_{a\in\mathcal{A}, b\in\mathcal{B}} \beta_{a,b} T_{a,b} .$$

□

Remark 24. This result is false for infinite dimensional vector spaces. See the exercises for a more precise description of what happens to $\mathrm{Hom}_F(U,V)$ when the entries are replaced by direct sums or products. For example, even $\mathrm{Hom}_F(F[x],F)$ has strictly greater dimension than that of $F[x]$. This is relevant to a topic we'll consider soon: dual spaces.

Change of Scalars

Let $F \subseteq K$ be two fields. We will refer to F as a subfield of K and to K as an extension field of F. In this section we will briefly consider vector spaces over such pairs of fields. Note that K is a vector space over F. We will call the dimension of K over F the *degree* of K over F and will denote it by $[K:F] = \deg_F K$.

In this section we will discuss the concepts of restriction of scalars and extension of scalars. The former is easy to understand as it simply involves forgetting something we already know. The second concept requires constructing a new vector space which satisfies a universal mapping propery. We give a rather mechanical, ad hoc construction here in some special cases, and later give a natural construction via the tensor product. Mathematically then this section could be omitted with no significant loss. On the other hand in some areas of mathematics these concepts are introduced early in the treatment of linear algebra and are exhibited via concrete constructions as we do below. It thus seems reasonable to make these ideas available now and to later introduce them anew in a more natural setting so that the two approaches may be compared. Many of the details will be left to the reader.

Restriction of Scalars

Let V be a vector space over the field K. Then it is clear that V is also a vector space over the field F (since the required set of conditions over F is a subset of the set of conditions over K). We refer to this as "restriction of scalars".

Proposition 25. *Let $F \subseteq K$ be two fields and V a vector space over K. Then V is a vector space over F and $\dim_F V = [K : F] \deg_K V$.*

The formula is valid in all cases; multiplication denotes the multiplication of cardinal numbers.

Proof. See Exercise 29 for the proof in the case of finite dimension. □

Corollary 26. *Let $F \subseteq K \subseteq L$ be three fields. Then $[L : F] = [L : K]\,[K : F]$. That is, degree is a multiplicative function.*

Extension of Scalars

We now define extension of scalars for a vector space V over a field F to a vector space V_K a field extension $F \subseteq K$ by a Universal Mapping Property.

Definition 27. Let $F \subseteq K$ be an extension of fields. Let V be a vector space over F and let W be a vector space over K. A vector space V_K together with an F-linear transformation $\iota : V \longrightarrow V_K$ is called an *extension of V to K corresponding to the field extension $F \subseteq K$* if for every linear transformation $t \in \mathrm{Hom}_F(V, W)$ there exists a unique linear transformation $T \in \mathrm{Hom}_K(V_K, W)$ so that the diagram

$$\begin{tikzcd}
V \arrow[r, "\iota"] \arrow[dr, "t"'] & V_K \arrow[d, dotted, "T"] \\
& W
\end{tikzcd}$$

commutes, that is, $T \circ \iota = t$.

Remark 28. For the Universal Mapping Property just defined, it must be true that

a. In order for T satisfying the equation $T \circ \iota = t$ to exist, ι must be one-to-one.

b. In order for T satisfying the equation $T \circ \iota = t$ to be unique, it must be true that $\mathrm{Span}_K(\mathrm{im}(\iota)) = V_K$.

See Exercise 30 for the verification of the statements in the previous remark.

Corollary 29. *Let $F \subseteq K$ be an extension of fields and V a vector space over F. If $\iota : V \longrightarrow V_K$ is an extension of V corresponding to the field extension of F to K, then for any vector space W over K there is an F-linear isomorphism*

$$\iota' : \mathrm{Hom}_F(V, W) \longrightarrow \mathrm{Hom}_K(V_K, W)$$

given by the Universal Mapping Property.

Proof. Define $\iota'(t) = T$ for $t \in \mathrm{Hom}_F(V, W)$ where $T \in \mathrm{Hom}_K(V_K, W)$ satisfing $T \circ \iota = t$ is given by the UMP. There is an inverse to this function given by $T \mapsto T \circ \iota = t$. Since the addition in the two vector spaces of linear transformations is given by addition of values, it easily follows that both ι' and its inverse are F-linear transformations. □

Theorem 30. *Let $F \subseteq K$ be an extension of fields and let V be a vector space over F. An extension of vector spaces $\iota : V \longrightarrow V_K$ corresponding to the extension of fields is unique up to unique isomorphism.*

Proof. See Exercise 31 for a proof of this result. □

Example 31 (Complexification of a Real Vector Space)**.** In this example we consider the field extension $\mathbb{R} \subseteq \mathbb{C}$ of the reals sitting inside the complexes. Let V be an arbitrary vector space over $\mathbb{R}$. Define $V_{\mathbb{C}} = V \oplus V$ as the direct sum of two copies of the real vector space V. We make $V_{\mathbb{C}}$ into a vector space over $\mathbb{C}$ as follows: Addition is already defined. Next we define multiplication by complex scalars

$$\cdot : \mathbb{C} \times V_{\mathbb{C}} \longrightarrow V_{\mathbb{C}}$$

via

$$(a + bi) \cdot (u, v) = (au - bv, av + bu) \ .$$

For computational purposes, it's simpler to use the notation $u + vi$ for (u, v) (verify this statement). So the definition of scalar multiplication is

$$(a + bi) \cdot u + vi = (au - bv) + (av + bu)i \ .$$

Using this notation, there is a natural (real linear transformation) $\iota : V \longrightarrow V_{\mathbb{C}}$ given by $\iota(u) = (u, 0) = u + 0i = u$. Verify that these two definitions make $V_{\mathbb{C}}$ into a vector space over $\mathbb{C}$. One can define a real isomorphism on $V_{\mathbb{C}}$

$$\overline{} : V_{\mathbb{C}} \longrightarrow V_{\mathbb{C}}$$

via

$$\overline{u+vi} = u - vi \ .$$

That is, the following hold:

a. For $x \in V_{\mathbb{C}}$, then $\overline{\overline{x}} = x$.

b. For $x, y \in V_{\mathbb{C}}$, $\overline{x+y} = \overline{x} + \overline{y}$.

c. For $c \in \mathbb{C}$ and $x \in V_{\mathbb{C}}$ $\overline{cx} = \overline{c}\,\overline{x}$.

d. For $x \in V_{\mathbb{C}}$, then $x \in V$ if and only if $\overline{x} = x$.

Example 32 (Algebraic Extensions Fields). Using similar ideas we can directly emulate the construction of the previous example in the case of an algebraic extension field.

Let F be a field and let $f \in F[x]$ be a monic irreducible polynomial of degree $k > 1$. Let $K = F[x]/(f(x))$ as studied in EqRel 15. Then $F \subseteq K$ is a field extension of degree $k = \deg f$. Let $\gamma = x + (f(x)) \in K$. This is a root of the irreducble polynomial $f(x)$ over F. $K = F[\gamma]$ is a degree k extension with the powers of γ, $\mathcal{B} = \{\, 1, \gamma, \ldots, \gamma^{k-1} \,\}$, as a basis over F. Given a vector space V over F, define $V_K = V^k$ where one thinks of elements as $v_0 + v_1\gamma + v_2\gamma^2 + \cdots + v_{k-1}\gamma^{k-1}$. Just as was done for the complexes, V_K becomes a vector space over $K = F[\gamma]$ by multiplication in the obvious way (note that γ^k is uniquely a linear combination of lower powers of γ because γ is a root of $f(x)$).

Example 33 (Vector Spaces With a Fixed Basis). Throughout this collection of examples, we consider a fixed field extension $F \subseteq K$. The idea used throughout is to only consider the case where our vector space V over F consists of n-tuples of elements of F, or more generally various collections of functions such as $F^{(S)}$ or F^S for S a non-empty set. At least in the first two cases on can think of these as vector spaces of functions arising via isomorphism after chosing a fixed basis.

a. Let n be a positive integer. Then a field extension $F \subseteq K$ gives rise to a natural inclusion $\iota : F^n \longrightarrow K^n$. Thus we can consider our initial finite dimensional vector space over F to be $V = F^n$ and our extension vector space $V_K = K^n$ with $\iota : V \longrightarrow V_K$. For a given F-linear transformation $t : V \longrightarrow W$ for W a vector space over K, there is an appropriate K-linear transformation $T : K^n \longrightarrow W$ given by $T(e_i) = t(e_i)$ for $1 \le i \le n$. The UMP for a basis thus determines T in terms of t.

b. Now let S be an arbitrary non-empty set. A field extension $F \subseteq K$ gives rise to a natural inclusion $\iota : F^{(S)} \longrightarrow K^{(S)}$. In both cases $\mathcal{B} = \{\, \delta_s \mid s \in S \,\}$ gives a basis over F or K, respectively. For a given F-linear transformation $t : V \longrightarrow W$ for W a vector space over K, there is an appropriate K-linear transformation $T : K^{(S)} \longrightarrow W$ given by $T(\delta_s) = t(\delta_s)$ for each $s \in S$. The UMP for a basis thus determines T in terms of t.

Exercises

The phrase "natural isomorphism" means that no arbitrary choices should be made (e.g., by choosing bases); one should give formulas using only the definitions or whatever other information is given. Do not assume that the vector spaces have finite dimension unless that is stated specifically.

BaseCoord 1. Let F be a field, n a positive integer, and $F^{n\times n}$ be the vector space of all $n \times n$ matrices with entries in F. Let $V = \{ A \in F^{n\times n} \mid A = A^t \}$ be the subspace of symmetric matrices (here A^t denotes the transpose of A). Find a basis for V over F and compute the dimension of V.

BaseCoord 2. Let F be a field, n a positive integer, and $F^{n\times n}$ be the vector space of all $n \times n$ matrices with entries in F. Let $W = \{ A \in F^{n\times n} \mid A = -A^t \}$ be the subspace of skew-symmetric matrices. Find a basis for W over F and compute the dimension of W. Caution: Does the characteristic of F play any role in the computation?

BaseCoord 3. Let F be a field, n a positive integer, and $F^{n\times n}$ be the vector space of all $n \times n$ matrices with entries in F. Show that under a certain condition on F $F^{n\times n}$ is the (internal) direct sum of the symmetric matrices V and the skew-symmetric matrices W. What is the condition on F?

BaseCoord 4. Let F be a field, n a positive integer, and $R = F[x_1, \dots, x_n]$ the ring of formal commutative polynomials with coefficients in F. A monomial $m \in R$ is a polynomial of the form $m = x_1^{d_1} x_2^{d_2} \cdots x_n^{d_n}$ where each $d_i \geq 0$ is an integer. The degree of m in the $i-th$ variable x_i is the integer d_i; we write $\deg_{x_i} m = d_i$. The *total degree* of m is the sum of the degrees in each x_i: $\deg m = d_1 + \cdots + d_n$. Note that R is not only a ring which contains F (so is a vector space over F), but is also an F-algebra.

a. Explain why the set of all monomials $\mathcal{M}$ (including 1) in n variables is a basis for R over F.

b. For an integer $d \geq 0$ let $H_{n,d}$ be the set of all monomials in n variables of total degree equal to d. Give a formula (with proof/explanation) for the size of this set $|H_{n,d}|$. Let $\mathcal{H}n, d$ be the span of $H_{n,d}$ over F. Verify that R is the direct sum of all subspaces $\mathcal{H}_{n,d}$.

c. A formal polynomial $f \in R$ determines a *polynomial function* (which we will denote by $\hat{f}$) $\hat{f} : F^n \longrightarrow F$ given by $(\hat{f})(a) = f(a_1, \dots, a_n) \in F$ for any n-tuple $a = (a_1, \dots, a_n) \in F^n$. This determines a ring homomorphism $e : F \longrightarrow F^{(F^n)}$. Determine precisely when e is not one-to-one.

d. A polynomial $f \in R$ is called *homogeneous of degree d* if for all $c \in F$ the equation

$$f(cx_1, cx_2, \dots, cx_n) = c^d f(x_1, x_2, \dots, x_n)$$

holds. In case F is an infinite field, determine all homogeneous polynomials of degree d for all $d > 0$. Precisely what happens if F is finite? If $d = 0$ and $c^0 = 1$?

e. Give a discussion similar to that of the previous part but change the definition of homogeneous of degree d:

For all $c \in F$ and all $a = (a_1, a_2, \ldots, a_n) \in F^n$ the equation

$$f(ca) = c^d f(a)$$

holds. In case F is an infinite field, determine all homogeneous polynomials of degree d for all $d > 0$. Precisely what happens if F is finite? If $d = 0$ and $c^0 = 1$?

BaseCoord 5. Let V be the real vector space spanned by the rows of the matrix

$$A = \begin{bmatrix} 3 & 21 & 0 & 9 & 0 \\ 1 & 7 & -1 & -2 & -1 \\ 2 & 14 & 0 & 6 & 1 \\ 6 & 42 & -1 & 13 & 0 \end{bmatrix}$$

a. Find a basis for V.

b. Tell which vectors $(x_1, x_2, x_3, x_4, x_5)$ are elements of V.

c. If $(x_1, x_2, x_3, x_4, x_5)$ is in V, what are its coordinates with respect to the basis chosen in part a?

BaseCoord 6. a. Let V be a vector space over the field $\mathbb{R}$ of real numbers. Let u, v, w be linearly independent vectors in V. Prove that $u+v$, $v+w$, and $u+w$ are linearly independent as well.

b. Does the same statement hold when F is replaced by an arbitrary field? Determine precisely what is true.

BaseCoord 7. Suppose F is a finite field of characteristic p. Prove that the number of elements in F is equal to p^n for some integer $n \geq 1$. [What is the prime subfield of F?]

BaseCoord 8. Let $\mathbb{R}$ be the real numbers. Regard $\mathbb{R}$ as a vector space over the field $\mathbb{Q}$ of rational numbers, with the usual operations. Prove that this vector space is not finite-dimensional.
Note that the solution of this problem requires knowing mathematics not developed in this course. Give as many really different proofs as you can find! There at least four which are really different and use ideas from (1) number theory, (2) algebra, (3) analysis, (4) logic. You do not have to prove whatever theorem you use, but when necessary, give the step required to show $\mathbb{R}$ is infinite dimensional over $\mathbb{Q}$ using the theorem(s) you choose.

BaseCoord 9. Let $u = (x_1, x_2)$ and $v = (y_1, y_2)$ be vectors in $\mathbb{R}^2$ such that

$$\begin{gathered} x_1y_1 + x_2y_2 = 0 \\ x_1^2 + x_2^2 = y_1^2 + y_2^2 = 1 \end{gathered}$$

Prove that $\mathcal{B} = \{u, v\}$ is a basis for $\mathbb{R}^2$. Find the coordinates of the vector (a, b) with respect to the ordered basis $\mathcal{B} = \{u, v\}$. (The conditions on u and v say, geometrically, that u and v are perpendicular and that each has length 1.)

BaseCoord 10. Let V be an n-dimensional vector space over a field F and let T be a linear transformation from V to V such that $\operatorname{im} T = \ker T$. Prove that n is even. Give an example of such a linear transformation T.

BaseCoord 11. Let V be a finite-dimensional vector space over F and let $T : V \longrightarrow V$ be a linear transformation. Suppose that $\operatorname{rank}(T^2) = \operatorname{rank}(T)$. Prove that the $\ker T \cap \operatorname{im} T = 0$.

BaseCoord 12. Let V and W be vector spaces over a field F, with V not trivial. Show that

$$W = \sum \{ \operatorname{im} \alpha \mid \alpha \in \operatorname{Hom}_F(V, W) \} .$$

That is, show that W is spanned by the collection of subspaces given by the images of *all* linear transformations from V to W.

BaseCoord 13. Let F be an arbitrary field. Let A be the subspace of $F^{2\times2}$ consisting of all matrices of the form

$$\begin{bmatrix} x & -x \\ y & z \end{bmatrix}$$

for $x, y, z \in F$. Similarly let B be the subspace of $F^{2\times2}$ consisting of all matrices of the form

$$\begin{bmatrix} x & y \\ -x & z \end{bmatrix}$$

for $x, y, z \in F$. Determine $\dim(A)$, $\dim(B)$, $\dim(A + B)$, and $\dim(A \cap B)$. .

BaseCoord 14. $\boxed{\star}$ You may assume that factorization of integers is unique. Let $p_1, p_2, \ldots, p_k$ be k distinct primes.

a. Prove that the set $\{ \sqrt{p_i} \mid 1 \le i \le k \}$ is linearly independent over $\mathbb{Q}$.

b. Compute the dimension of $\mathbb{Q}[\sqrt{p_1}, \ldots, \sqrt{p_k}]$ over $\mathbb{Q}$.

BaseCoord 15. a) Let $f : V \longrightarrow W$ be a linear transformation. Suppose W' is a finite dimensional subspace of W, and that $\ker f$ is finite dimensional. Prove that

$$f^{-1}(W') := \{ v \in V \mid f(v) \in W' \}$$

is a finite dimensional subspace of V (note that it is always a subspace of V, regardless of the finiteness assumptions). Show that $f^{-1}(W')$ will be infinite dimensional if $\ker f$ is infinite dimensional and might be if W' is infinite dimensional.

b) Let $f : V \longrightarrow W$ and $g : W \longrightarrow Y$ be linear transformations such that $\ker f$ and $\ker g$ are finite dimensional. Show that $\ker gf$ is finite dimensional.

BaseCoord 16. Let p, m, and n be positive integers and F a field. Let V be the vector space $F^{m \times n}$, of all $m \times n$ matrices over F and $W = F^{p \times n}$. Let A be a fixed $p \times m$ matrix and define $T(M) = AM$ for $M \in V$. Prove that T is has an inverse if and only if $p = m$ and A is an invertible $m \times m$ matrix.

BaseCoord 17. Let U, V, U_1, U_2, V_1, V_2 be vector spaces over the same field F.

a. Give a natural isomorphism

$$\mathrm{Hom}_F(U_1 \oplus U_2, V) \longrightarrow \mathrm{Hom}_F(U_1, V) \oplus \mathrm{Hom}_F(U_2, V) \ .$$

b. Give a natural isomorphism

$$\mathrm{Hom}_F(U, V_1 \oplus V_2) \longrightarrow \mathrm{Hom}_F(U, V_1) \oplus \mathrm{Hom}_F(U, V_2) \ .$$

BaseCoord 18. Let U, V, $U_i, i \in I$, $V_j, j \in J$ be vector spaces over the same field F.

a. Give a natural isomorphism

$$\mathrm{Hom}_F(\bigoplus_{i \in I} U_i, V) \longrightarrow \prod_{i \in I} \mathrm{Hom}_F(U_i, V) \ .$$

b. Give a natural isomorphism

$$\mathrm{Hom}_F(U, \prod_{j \in J} V_j) \longrightarrow \prod_{j \in J} \mathrm{Hom}_F(U, V_i) \ .$$

c. Is there a similar natural description of

$$\mathrm{Hom}_F(U, \bigoplus_{j \in J} V_j)$$

or of

$$\mathrm{Hom}_F(\prod_{i \in I} U_i, V) \ ?$$

$\boxed{d.}$ Can you use these isomorphisms to give the dimension of the "dual space" of $F[x]$? That is, of the vector space

$$F[x]^* = \mathrm{Hom}_F(F[x], F) \ ?$$

BaseCoord 19. If F is a field with a finite or a countable number of elements and V is an infinite dimensional vector space over F, show that $\dim_F V = |V|$.

BaseCoord 20. Let F be a field and X an infinite set. Show that the two vector spaces

$$\bigoplus_{x\in X} F = F^{(X)}$$

and

$$\prod_{x\in X} F = F^{X}$$

are not isomorphic. Show not only that the natural inclusion is not an isomorphism, but no isomorphism exists.

BaseCoord 21. Let F be any field and let $F[x]$ be the formal polynomials with coefficients in F. Let $\mathcal{A} = \{\, f_i \mid i \geq 1 \,\}$ be a set of non-zero polynomials.

a. If $\mathcal{A}$ satisfies $\deg f_i \neq \deg f_j$ for $i \neq j$, then show that $\mathcal{A}$ is linearly independent.

b. If in addition $\mathcal{A}$ satisfies $\{\, \deg f_i \mid f_i \in \mathcal{A} \,\}$ is the set of all non-negative integers, then $\mathcal{A}$ is a basis for $F[x]$.

c. Let $a \in F$ and let $\mathcal{B} = \left\{\, (x-a)^i \;\middle|\; i \geq 0 \,\right\}$. Prove that $\mathcal{B}$ is a basis for $F[x]$.

d. Let $a_j \in F$ for $j \geq 1$ be a set of distinct elements of F (so F must be infinite). Let $g_j = \prod_{i=1}^{i=j}(x - a_i)$ and let $g_0 = 1$. So $g_1 = x - a_1$, $g_2 = (x-a_1)(x-a_2)$, etc. Show that $\left\{\, g_j \;\middle|\; j \geq 0 \,\right\}$ is a basis for $F[x]$.

BaseCoord 22. Let W be the vector space of all continuous real valued functions on $\mathbb{R}$.

a. Let $\mathcal{E} = \{\, e^{cx} \mid c \in \mathbb{R} \,\}$. Let $V = \operatorname{Span}_{\mathbb{R}}(\mathcal{E})$. Show that $\mathcal{E}$ is a linearly independent subset of W and hence $\dim_{\mathbb{R}} V = |\mathbb{R}|$.

b. Let $P = \{\, r \in \mathbb{R} \mid r > 0 \,\}$. Give a one-to-one, onto function $f :\ \mathbb{R} \longrightarrow P$ thus showing that $|\mathbb{R}| = |P|$.

c. Let $\mathcal{C} = \{\, \cos(cx) \mid c \in \mathbb{R},\ c > 0 \,\}$. Let $V_1 = \operatorname{Span}_{\mathbb{R}}(\mathcal{C})$. Show that $\mathcal{C}$ is a linearly independent subset of W and hence $\dim_{\mathbb{R}} V_1 = |\mathbb{R}|$.

d. Let $\mathcal{S} = \{\, \sin(cx) \mid c \in \mathbb{R},\ c > 0 \,\}$. Let $V_2 = \operatorname{Span}_{\mathbb{R}}(\mathcal{S})$. Show that $\mathcal{S}$ is a linearly independent subset of W and hence $\dim_{\mathbb{R}} V_2 = |\mathbb{R}|$.

e. Compute the kernel and cokernel of the linear transformation given by differentation $D :\ V \longrightarrow V$. Let $V_0 = \operatorname{Span}_{\mathbb{R}}(\mathcal{E} \setminus \{\, 1 \,\})$. Do the same for $D :\ V_0 \longrightarrow V_0$.

f. Compute the kernel and cokernel of the linear transformation given by differentation $D :\ V_1 \longrightarrow V_2$ and $D :\ V_2 \longrightarrow V_1$.

BaseCoord 23. $\boxed{\star}$

a. Let F be an arbitrary field and let F^∞ be the vector space of all infinite sequences $(a_1, a_2, \ldots)$ of elements of F. Addition is coordinatewise and scalar multiplication by $a \in F$ just multiplies each entry by a. Define $\mathbf{L} : F^\infty \longrightarrow F^\infty$ by $\mathbf{L}(a_1, a_2, a_3, \ldots) = (a_2, a_3, a_4, \ldots)$ ("shift left"). Note that $\mathbf{L}$ is a linear transformation. It is onto with a kernel of dimension 1. For $a \in F$ which is non-zero define the vector $v(a) = (1, a, a^2, a^3, \ldots) \in F^\infty$ whose i-th entry is a^{i-1}. Show that $\mathbf{L}(v(a)) = av(a)$. Prove that $\dim_F F^\infty \geq |F|$. (Hint: Show that $\{ v(a) \mid a \in F \}$ is linearly independent.)

b. Show that $\dim_F F^\infty$ is uncountable, i.e., bigger than $\aleph_0 = |\mathbb{Z}| = |\mathbb{Q}|$. Note that it will suffice to do this in case F is countable because ....

BaseCoord 24. Let F be a field and V a vector space over F. Let $\mathcal{C} = \{ u_1, \ldots, u_n \}$ be a subset of V.

a. Let $v \in V$ be a non-zero vector and assume that $\mathrm{Span}_F(\mathcal{C}) = V$. Show that there exists an integer i, $1 \leq i \leq n$ so that for

$$\mathcal{C}' = \{ v \} \cup \mathcal{C} \setminus \{ u_i \}$$

then $\mathrm{Span}_F(\mathcal{C}') = V$. That is, for some i, v can *replace* u_i in the spanning set $\mathcal{C}$ and the result is also a spanning set.

b. Let $\mathcal{A} = \{ v_1, \ldots, v_m \}$ be a linearly independent set in V. Assume that $\mathrm{Span}_F(\mathcal{C}) = V$. Show that there exists a subset of indices $I \subseteq \{ 1, \ldots, n \}$ with $|I| = |\mathcal{A}|$ so that

$$\mathcal{C}' = \mathcal{A} \cup \mathcal{C} \setminus \{ u_i \mid i \in I \}$$

spans V; that is, the independent set $\mathcal{A}$ can replace a subset of exactly the same size in the spanning set $\mathcal{C}$ to yield a new spanning set.

c. Use this result to prove that any two bases $\mathcal{B}_1$ and $\mathcal{B}_2$ have the same number of elements for V a finite dimensional vector space.

BaseCoord 25. a. Let V be a vector space over the field F. Let $f : V \longrightarrow F$ be a non-trivial linear transformation. Show that there will exist a vector $v_0 \in V$ with $f(v_0) = 1$ and further that $V = \ker f \oplus Fv_0$, where $Fv_0 = \{ av_0 \mid a \in F \}$. Conclude that $V/\ker f \approx F$ has dimension 1. The subspace $\ker f$ is called a *hyperplane*, and is said to have codimension 1. In general if $W \subseteq V$ is a subspace, the number $\dim V/W$ is called the *codimension* of W in V.

b. Let $W_1, \ldots, W_k \subset V$ be a collection of of subspaces. Assume each W_i has finite codimension in V. Prove that their intersection has finite codimension in V. Give an upper bound for that number in terms of the codimensions of the W_i.

c. Let $W_1, \ldots, W_k \subset V$ be a collection $\mathcal{C}$ of hyperplanes in V. Let $I, J \subseteq \{1, \ldots, k\}$ be subsets. The collection $\mathcal{C}$ of hyperplanes is said to be in *general position* if $\bigcap_{i \in I} W_i \supset \bigcap_{j \in J} W_j$ are not equal whenever $I \subset J$ are not equal. Show that it is always true that $W = \bigcap_{1 \leq i \leq k} W_i$ has finite codimension in V. In case the collection $\mathcal{C}$ is in general position, compute the codimension of W in V.

BaseCoord 26. The dimension formula

$$\dim(W_1 + W_2) = \dim(W_1) + \dim(W_2) - \dim(W_1 \cap W_2)$$

for finite-dimensional subspaces is analogous to the inclusion-exclusion formula

$$|S_1 \cup S_2| = |S_1| + |S_2| - |S_1 \cap S_2|$$

for sets. For three sets, the inclusion-exclusion formula is:

$$|S_1 \cup S_2 \cup S_3| = |S_1| + |S_2| + |S_3| - |S_1 \cap S_2| - |S_1 \cap S_3| - |S_2 \cap S_3| + |S_1 \cap S_2 \cap S_3|$$

Is the analogous formula for three finite-dimensional subspaces W_1, W_2, W_3 also true? Prove or provide a counterexample. By analyzing the map

$$W_1 \oplus W_2 \oplus W_3 \longrightarrow W_1 + W_2 + W_3$$

given by

$$(w_1, w_2, w_3) \mapsto w_1 + w_2 + w_3 \ ,$$

can you prove that

$$\dim(W_1+W_2+W_3) = \dim(W_1)+\dim(W_2)+\dim(W_3)-\dim(W_1 \cap W_2)-\dim((W_1+W_2) \cap W_3) \ ?$$

BaseCoord 27. Let $\mathbb{F}_q$ be a finite field with q elements and having characteristic p. Prove the assertions you make to answer the following questions.

a. Let m, n be positive integers. Give a formula for the number of elements in $\mathbb{F}_q^n$ and $\mathbb{F}_q^{m \times n}$.

b. Give a formula for the number of different ordered bases of $\mathbb{F}_q^n$.

c. Give a formula for the number of invertible matrices in $\mathbb{F}_q^{n \times n}$.

d. Give a formula for the number of ordered, linearly independent sequences of vectors with m elements in $\mathbb{F}_q^n$.

e. Give a formula for the number of matrices of $\mathbb{F}_q^{m \times n}$ with rank m.

f. For a non-negative integer k determine the number of subspaces of dimension k of $\mathbb{F}_q^n$.

g. For a non-negative integer k determine the number of ordered sequences of k vectors in $\mathbb{F}_q^n$ that span.

BaseCoord 28. Let V be a finite dimensional vector space over the field F. Let $\mathcal{A}$ and $\mathcal{B}$ be any bases for V. Assume we are given a decompostion of the basis $\mathcal{A} = \mathcal{A}_1 \dot{\cup} \mathcal{A}_2$ of the first basis into two disjoint subsets. Show that there is a way to choose a similar decomposition of the second basis $\mathcal{B}$ to obtain four bases for V:

$$\begin{aligned} \mathcal{A} &= \mathcal{A}_1 \dot{\cup} \mathcal{A}_2 \\ \mathcal{B} &= \mathcal{B}_1 \dot{\cup} \mathcal{B}_2 \\ \mathcal{C} &= \mathcal{A}_1 \dot{\cup} \mathcal{B}_2 \\ \mathcal{D} &= \mathcal{B}_1 \dot{\cup} \mathcal{A}_2 . \end{aligned}$$

BaseCoord 29. Let $F \subseteq K$ be fields. Let V be a vector space over K.

a. Explain why V is also a vector space over F.

b. If $\{e_1, \ldots, e_n\}$ is a basis for K over F and if $\mathcal{B} = \{v_1, \ldots, v_m\}$ is a basis for V over K, show that $\mathcal{A} = \left\{ e_i v_j \;\middle|\; 1 \le i \le n,\ 1 \le j \le m \right\}$ is a basis for V over F. This yields the following formula

$$\dim_F V = (\dim_F K) \cdot (\dim_K V)$$

where the subscript on dim denotes the field over which the dimension is computed.

c. For the particular case of the reals contained in the complexes give formulas for the dimensions of the following over both fields:

i. $\mathbb{C}^{m \times n}$,

ii. all polynomials of degree less than n (include 0) with complex coefficients,

iii. all $n \times n$ symmetric matrices with complex coefficients.

d. Let $S : V \longrightarrow V$ be a linear transformation on the vector space V over K. Explain why S is also a linear transformation over F. Assume that the matrix of S with respect to the basis $\mathcal{B}$ has entries a_{ij} for $1 \le i, j \le m$. Choose an appropriate ordering for the basis $\mathcal{A}$ and find the matrix of S considered as a linear transformation over F. (Note that the matrix may be easier to describe if you choose a nice order for the basis. Hint: Use block matrices!)

BaseCoord 30. Verify the statment in Remark 28:

a. In order for the T satisfying the equation $T \circ \iota = t$ to exist, ι must be one-to-one.

b. In order for the T satisfying the equation $T \circ \iota = t$ to be unique, it must be true that $\text{Span}_K(\text{im}(\iota)) = V_K$.

BaseCoord 31. Prove Theorem 30: The extension of vector spaces corresponding to the extension of fields is unique up to unique isomorphism.

[Hint: 4 applications of the UMP!]

BaseCoord 32. Verify the details of Example 32 for a finite algebraic extension.

BaseCoord 33. Let F be a field, $F[x]$ the formal polynomials over F, and $F(x)$ the field of fractions of $F[x]$ (see the exercise EqRel 13). Take $K = F(x)$ and consider the field extension $F \subseteq K$. Let V be an arbitrary vector space over F. Directly construct a vector space V_K that satisfies the appropriate Universal Mapping Property.

BaseCoord 34. Verify the details of Example 33 where there is a fixed basis for the vector spaces V and V_K.

Universal Mapping Properties

Universal Mapping Properties are used in a number of different ways. First of all they give a way of specifying an object (together with maps) that will be the "best" solution to a certain type of problem. There are many types of questions that can be expressed in such terms, but not all will have solutions. So our first problem will be to prove that the given problem does have a solution (the object and necessary maps exist) and then to determine if the solution is unique, or if not, determine "how unique" it is. Secondly, such problems usually descibe how to construct more complicated things (objects or functions) from simpler things. In many cases it will turn out that we get a complete and precise description of a more complicated situation in terms of a simpler one. In our typical application this means that we obtain a one-to-one correspondence between the collection of all the functions satisfying some simple conditions and the collection of functions satisfying some more complicated conditions. This vague description should used as a guide in understanding the concrete examples of Universal Mapping Properties given below, and elsewhere in the course.

The statements below give a natural identification of one collection of functions, usually denoted $\mathrm{Hom}(A, B)$, with another. Here we use subscripts to denote what type of functions are meant. This note should probably really be a bit more formal and use the words "category", "object", and "morphism" but it won't. Nevertheless, that is really the topic.

Informally, the "objects" are the things like sets, vector spaces, modules, groups, etc. while the functions considered in the given context (the "category") are the "morphisms" - ordinary functions, F-linear transformations, R-homomorphisms, group homomorphisms, etc. For convenience **Set**, F-Mod, R-Mod, **Grp** will denote the given context (category) below. One could for example consult an edition of Lang's *Algebra* for a more formal treatment.

After each universal mapping property (UMP), we will give the correspondence of sets of functions one obtains as a result. The UMPs that we will discuss below fall into two classes, those that allow one to define functions out of quotient objects, and those that allow one to extend certain functions from a set to an algebraic object to functions *between* algebraic objects that preserve the algebraic structure (so-called freeness properties).

Quotients

We begin with the quotient construction which is frequently used in mathematics, and in particular, in this course. Let X be a non-empty set and let $\mathcal{E} \subseteq X \times X$ be an equivalence relation (see the section on "Equivalence Relations").

If the equivalence relation $\mathcal{E}$ behaves "nicely" with respect to the structure of X, then $X/\mathcal{E}$ will have the same sort of structure, and the function $p : X \longrightarrow X/\mathcal{E}$

will preserve it. We now elaborate on this idea. The idea is used in the construction of quotient spaces, quotient rings, fields of fractions, tensor products, and others. It gives a method for the construction of "universal" objects via the following:

Theorem 1. *Let $\mathcal{E}$ be an equivalence relation on the set X. If $f : X \longrightarrow Y$ is a function which is constant on the fibers of $p : X \longrightarrow X/\mathcal{E}$, then there exists a unique function $F : X/\mathcal{E} \longrightarrow Y$ such that $f = F \circ p$.*

By "constant on the fibers" we mean $f(x) = f(x')$ whenever $p(x) = p(x')$ or equivalently, $x \sim x'$ for $x \in X$ (i.e., when $(x, x') \in \mathcal{E}$).

We will typically state the condition $f = F \circ p$ by saying that the following diagram commutes:

$$\begin{tikzcd}
X \arrow[r, "p"] \arrow[dr, "f"'] & X/\mathcal{E} \arrow[d, dotted, "F"] \\
& Y
\end{tikzcd}$$

The basic idea introduced in Theorem 1 will be used many times. This gives us a one-to-one correspondence

$$\{\, f \in \mathrm{Hom}_{\mathbf{Set}}(X, Y) \mid f(\mathrm{class}_{\mathcal{E}}(x)) = \mathrm{const} \,\} \longleftrightarrow \mathrm{Hom}_{\mathbf{Set}}(X/\mathcal{E}, Y) .$$

When the equivalence class $\mathcal{E}$ is defined algebraically, often one is able to put an algebraic structure on $X/\mathcal{E}$, the surjection p preserves this structure, and one has a stronger version of the theorem above; namely that F preserves the algebraic struture. We will conclude this section with several examples of this, each of which takes place in a different context that we will need at some point in the semester. For the definitions of ring, module, etc, see the section "Some Useful Definitions".

Theorem 2 (UMP for Quotient Spaces). *Let V be a vector space over the field F and let W be a subspace. For any vector space U and linear transformation $t : V \longrightarrow U$ such that $W \subseteq \ker t$, then there exists a unique linear transformation $T : V/W \longrightarrow U$ such that the following diagram commutes:*

$$\begin{tikzcd}
V \arrow[r, "p"] \arrow[dr, "t"'] & V/W \arrow[d, dotted, "T"] \\
& U
\end{tikzcd}$$

that is, $T \circ p = t$.

Theorem 2 gives a bijective correspondence

$$\{\, f \in \mathrm{Hom}_F(V,U) \mid f(W) = 0 \,\} \longleftrightarrow \mathrm{Hom}_F(V/W, U)\ .$$

In fact, the correspondence is an isomorphism of vector spaces!

The condition that $W \subseteq \ker t$ is often depicted via the diagram

$$\begin{tikzcd}
W \arrow[r] \arrow[dr, "0"'] & V \arrow[r, "p"] \arrow[d, "h"] & V/W \arrow[dl, dotted, "T"] \\
& U &
\end{tikzcd}$$

The hypothesis of the theorem becomes 'the left triangle with solid arrows commutes', and the conclusion becomes 'there exists a unique dotted arrow making the diagram commute'. This theorem is also sometimes called the universal property of cokernels.

One has a version of Theorem 2 for modules over a ring R as well (in fact, Theorem 2 is a special case of this more general version).

Theorem 3 (UMP for Quotient Modules). *Let M be a module over the ring R and let N be a submodule. For any R-module L and R-homomorphism $t : M \longrightarrow L$ such that $N \subseteq \ker t$, then there exists a unique R-homomorphism $T : M/N \longrightarrow L$ such that the following diagram commutes:*

$$\begin{tikzcd}
M \arrow[r, "p"] \arrow[dr, "t"'] & M/N \arrow[d, dotted, "T"] \\
& L
\end{tikzcd}$$

that is, $T \circ p = t$.

As before, one gets a one-to-one correspondence

$$\{\, f \in \mathrm{Hom}_R(M,L) \mid f(N) = 0 \,\} \longleftrightarrow \mathrm{Hom}_R(M/N, L)$$

which is an isomorphism of R-modules (provided each is indeed an R-module).

One can make similar statements for other algebraic structures, such as rings. Special cases of such constructions have already occurred in the exercises: Problems EqRel 11 and EqRel 15 deal with quotient rings. In particular, the field $\mathbb{F}_p$ is usually described by this type of construction. See Exercise 3 at the end.

A different type of structure appears in EqRel 13 which constructs the field of fractions of a commutative domain and gives a Unversal Mapping Property for that construction.

One such example is the field of rational functions which already appeared as an example in the section on "Fields". In most calculus courses one sees such fractions as well. There one learns about partial fractions in order to integrate rational functions, $f(x)/g(x)$ where $f(x), g(x) \in \mathbb{R}[x]$ and $g(x) \neq 0$.

Freeness Properties

In many situations it is useful to describe every element in some object by constructing it from some small, fixed set, of elements. In really nice situations each element can be constructed in only one way. In such a situation, the fixed set is usually referred to as a "basis" for the object, and the object itself is referred to as "free". The "free" simply means that there are no "dependence relations" ("free of dependence relations). As we saw earlier for the case of vector spaces, this can be stated in terms of a universal mapping property. We then reverse the process and use this to define such situations.

Every vector space V has a basis $\mathcal{B}$. The following theorem identifies linear transformations from V to W with (arbitrary!) functions from a basis $\mathcal{B}$ of V to W. This provides an easy way to define linear transformations, provided one has a basis. This result is also stated in terms of a universal mapping property below.

Theorem 4 (UMP for Bases of Vector Spaces). *Let V and W be vector spaces over F, and let $\mathcal{B}$ be a basis for V. Let $i : \mathcal{B} \longrightarrow V$ be the inclusion map. Given any function $t : \mathcal{B} \longrightarrow W$, there exists a unique linear transformation $T : V \longrightarrow W$ such that the following diagram commutes:*

$$\begin{tikzcd}
\mathcal{B} \arrow[r, "i"] \arrow[dr, "t"'] & V \arrow[d, dotted, "T"] \\
& W
\end{tikzcd}$$

that is, $T \circ i = t$.

For F-vector spaces we have a bijective correspondence

$$\operatorname{Hom}_{\mathbf{Set}}(\mathcal{B}, W) \longleftrightarrow \operatorname{Hom}_F(V, W) ,$$

which is in fact an isomorphism of vector spaces.

Note that the correspondence depends on the existence of a basis $\mathcal{B}$ and will be different for different choices of bases.

If R is now a ring (with identity), it is no longer true that an arbitrary module M over R has a basis (consider $\mathbb{Z}/n\mathbb{Z}$ as a module over the ring $\mathbb{Z}$). In this case, the universal mapping property becomes a definition:

Definition 5 (Free Module)**.** Let M be a module over a ring R and let $\mathcal{B}$ be a subset of M. M is a *free* R*-module* with basis $\mathcal{B}$ if for any R-module N and any function $h : \mathcal{B} \longrightarrow N$, there exists a unique R-module homomorphism $H : M \longrightarrow N$ such that the following diagram commutes:

$$\begin{tikzcd}
\mathcal{B} \arrow[r, "i"] \arrow[dr, "h"'] & M \arrow[d, dotted, "H"] \\
& N
\end{tikzcd}$$

that is, $H \circ i = h$.

Again this yields a one-to-one correspondence

$$\mathrm{Hom}_{\mathbf{Set}}(\mathcal{B}, N) \longleftrightarrow \mathrm{Hom}_R(M, N) \ ,$$

which is in fact an R-module isomorphism.

The basis exists by assumption, and as before, the correspondence is dependent upon the choice of basis $\mathcal{B}$.

The previous freeness theorems were for 'linear' objects, that is, objects that did not carry an intrinsic multiplication. We now assume our ring R is commutative and give an example of a universal mapping property for R-algebras. Recall that an R-algebra is a ring A with identity that is also an R-module and for which the ring multiplication and scalar multiplication are compatible: $r(ab) = (ra)b = a(rb)$ for all $r \in R$ and all $a, b \in A$.

Here $R[X]$ denotes the ordinary (formal) (commutative) polynomial ring for the set of variables X. By definition, this means (as it does for fields) that the various monomials in X form a basis of the free R-module $R[X]$. This theorem asserts something you already believe: "it is possible to evaluate polynomials by inserting values for the variables".

Theorem 6 (UMP for Free Commutative Algebras)**.** *Let A be a commutative R-algebra, and let X be any set. Then there exists a commutative R-algebra (denoted $R[X]$) such that for any function $h : X \to A$, there exists a unique homomorphism $H : R[X] \longrightarrow A$ of R-algebras such that the following diagram commutes:*

$$\begin{tikzcd}
X \arrow[r, "i"] \arrow[dr, "h"'] & R[X] \arrow[d, dotted, "H"] \\
& A
\end{tikzcd}$$

that is, $H \circ i = h$.

The set X is the "basis" in this situation - every element of $R[X]$ can be constructed (by addition, multiplication and scalar multiplication, using R and X) and the resulting expressions uniquely represent the elements.

The universal mapping property provides a bijection

$$\mathrm{Hom}_{\mathbf{Set}}(X, A) \longleftrightarrow \mathrm{Hom}_{R\text{-Alg}}(R[X], A) \ ,$$

which is in fact an R-algebra isomorphism.

Note that there is a non-commutative version of this theorem as well (meaning that the R-algebras A are allowed to be non-commutative rings). The replacement for $R[X]$ in the theorem is $R\langle X\rangle$, the (formal) ring of non-commutative polynomials with coefficients in R: that is, the variables commute with the coefficients in the ring, but not with each other (e.g., xy and yx are part of the basis for $R\langle x, y\rangle$). The ring $R\langle X\rangle$ is often referred to as the "free associative R-algebra on X. See Exercise 6.

The following theorems that describe how to give all homomorphisms from $\mathbb{Z}$ or $\mathbb{Z}_n$ to an arbitrary group G are also examples of universal mapping properties:

Theorem 7 (UMP for $\mathbb{Z}$). *Let G be any group. Let $i : \{1\} \longrightarrow \mathbb{Z}$ be the inclusion map. Given any $x \in G$ define $j : \{1\} \longrightarrow G$, by $j(1) = x$. Then there exists a unique group homomorphism $h : \mathbb{Z} \longrightarrow G$ such that the following diagram commutes:*

$$\begin{tikzcd}
\{1\} \arrow[r, "i"] \arrow[dr, "j"'] & \mathbb{Z} \arrow[d, dotted, "h"] \\
 & G
\end{tikzcd}$$

that is, $h \circ i = j$.

Note that this in fact just says that $\mathbb{Z}$ is a free (abelian) group with $\{1\}$ as a basis. Therefore, this universal mapping property identifies group homomorphisms from $\mathbb{Z}$ to G with set maps from $\{1\}$ to G, which may further be identified with G itself.

Now let n be a positive integer, and $\mathbb{Z}_n$ the additive group of integers mod n.

Theorem 8 (UMP for $\mathbb{Z}_n$). *Let G be any group. Let $i : \{1\} \longrightarrow \mathbb{Z}_n$ be the inclusion map. Given $x \in G$, then there exists a group homomorphism $h : \mathbb{Z}_n \longrightarrow G$ satisfying $h(1) = x$ if and only if $o(x)|n$. If h exists, then it is the unique group homomorphism such that the following diagram commutes where $j(1) = x$:*

$$\begin{tikzcd}
\{1\} \arrow[r, "i"] \arrow[dr, "j"'] & \mathbb{Z}_n \arrow[d, dotted, "h"] \\
 & G
\end{tikzcd}$$

that is, $h \circ i = j$.

Remark 9. Since 'abelian group' is really the same thing as '$\mathbb{Z}$-module' (see Exercise 11), the previous two theorems have interpretations in the setting of abelian groups. Indeed, if one restricts Theorem 7 to the case when G is abelian, then one simply obtains that $\mathbb{Z}$ is a free $\mathbb{Z}$-module with basis $\{1\}$, as in Definition 5.

Furthermore, in the case of abelian groups, Theorem 8 is simply a special case of Theorem 3.

Products and Coproducts

Now we look at some standard results in linear algebra.

Theorem 10 (Product Property). *Let F be a field and V_1 and V_2 vector spaces over F. The linear transformations $p_1 : V_1 \oplus V_2 \longrightarrow V_1$ and $p_2 : V_1 \oplus V_2 \longrightarrow V_2$ are such that for any F-vector space Z and linear transformations $h_1 : Z \longrightarrow V_1$ and $h_2 : Z \longrightarrow V_2$ there exists a unique linear transformation $H : Z \longrightarrow V_1 \oplus V_2$ that makes the following diagram commute:*

$$\begin{tikzcd}
 & V_1 \oplus V_2 \arrow[dl, "p_1"'] \arrow[dr, "p_2"] & \\
V_1 & & V_2 \\
 & Z \arrow[ul, "h_1"] \arrow[ur, "h_2"'] \arrow[uu, dotted, "H"'] &
\end{tikzcd}$$

that is, $p_1 \circ H = h_1$ and $p_2 \circ H = h_2$.

Thus there is a one-to-one correspondence

$$\mathrm{Hom}_F(Z, V_1) \times \mathrm{Hom}_F(Z, V_2) \longleftrightarrow \mathrm{Hom}_F(Z, V_1 \oplus V_2)$$

which is an isomorphism.

Theorem 11 (Coproduct Property). *Let F be a field and V_1 and V_2 vector spaces over F. The linear transformations $i_1 : V_1 \longrightarrow V_1 \oplus V_2$ and $i_2 : V_2 \longrightarrow V_1 \oplus V_2$ are such that for any vector space Z and linear transformations $g_1 : V_1 \longrightarrow Z$ and $g_2 : V_2 \longrightarrow Z$ there exists a unique linear transformation $G : V_1 \oplus V_2 \longrightarrow Z$ that* *makes the following diagram commute:*

$$\begin{tikzcd}
 & V_1 \oplus V_2 \arrow[dd, dotted, "G"] & \\
V_1 \arrow[ur, "i_1"] \arrow[dr, "g_1"'] & & V_2 \arrow[ul, "i_2"'] \arrow[dl, "g_2"] \\
 & Z &
\end{tikzcd}$$

that is, $G \circ i_1 = g_1$ *and* $G \circ i_2 = g_2$.

Further this means then that there is a one-to-one correspondence

$$\mathrm{Hom}_F(V_1, Z) \times \mathrm{Hom}_F(V_2, Z) \longleftrightarrow \mathrm{Hom}_F(V_1 \oplus V_2, Z)$$

which is an isomorphism.

The proofs of these two "theorems" are of course easy: one takes $H(z) = (h_1(z), h_2(z))$ in the first and $G(v, w) = g_1(v) + g_2(w)$ in the second.

In the general case one makes these properties the definition: A product is denoted by $V_1 \Pi V_2$ and a coproduct by $V_1 \amalg V_2$. For two vector spaces it turns out that $V_1 \oplus V_2$ and the canonical projection and inclusion maps gives a vector space (plus relevant maps) so that it has both properties. Something similar happens for the product or coproduct of any finite number of vectors spaces. However, for an infinite collection of vector spaces there are two distinct vector spaces (with relevant maps) that are not even isomorphic. See Exercise 12.

Tensor Product

Another example from linear algebra:

Definition 12 (Tensor Product). Let F be a field and let V , W , Z be vector spaces over F. A vector space $V \otimes_F W$ together with a bilinear function $t : V \times W \longrightarrow V \otimes_F W$ is called a *tensor product* if for every bilinear function $b : V \times W \longrightarrow Z$ there exists a unique linear transformation $h : V \otimes_F W \longrightarrow Z$ such that the following diagram commutes:

$$\begin{tikzcd}
V \times W \arrow[r, "t"] \arrow[dr, "b"'] & V \otimes_F W \arrow[d, dotted, "h"] \\
 & Z
\end{tikzcd}$$

that is, $h \circ t = b$.

Note that the above theorem establishes a bijection between the set of F-bilinear maps from $V \times W$ to Z, and ordinary F-linear maps from $V \otimes_F W$ to Z.

$$\mathrm{Hom}_{\mathbf{Bilin}}(V \times W, Z) \longleftrightarrow \mathrm{Hom}_F(V \otimes_F W, Z)\ .$$

We will consider further things like $V \otimes_F V \otimes_F \cdots \otimes_F V$ (n times) and quotients of these to construct something called *exterior powers* which play a major role in the study of determinants,

In fact, even though we're primarily interested in vector spaces, we must use the versions of these theorems for modules over commutative rings. The primary applications will be to any commutative ring since we need determinants for commutative rings, such as $F[x]$. Additionally $F[x]$ allows studying a linear transformation $T: V \longrightarrow V$ by using T to think of V as an $F[x]$-module. See Exercise 15.

Exercises

UMP 1. Prove Theorem 1.

UMP 2. Carefully state the exercise EqRel 13 in the section "Equivalence Relations" as a Universal Mapping Property. Explain how the different parts of the exercise give a proof of the UMP and that this proof also follows the general outline of a proof of a UMP.

UMP 3. Let R be a ring and let $I \subseteq R$ be a two-sided ideal (see "Some Useful Definitions"). State and prove the Universal Mapping Property for Quotient Rings, that is, the ring R/I. (See exercises EqRel 11 and EqRel 15 which deal with two special cases of this construction. Note that by using some earlier UMP theorem you might be able to avoid some work!)

UMP 4. Let R be a commutative ring and $R[x]$ the ring of formal polynomials with coefficients in R.

a. Show that $R[x]$ is a free R-algebra with one generator. Hence $R[x]$ is in particular a free commutative R-algebra with 1 generator.

b. Note that $R[x_1, \dots, x_n, x_{n+1}] = (R[x_1, \dots, x_n])[x_{n+1}]$. For $n > 1$ show that $R[x_1, \dots, x_n]$ is a free commutative R-algebra on n generators.

c. Show that $R[x_1, \dots, x_n]$ is not a free R-algebra on n generators.

UMP 5. Let R be an arbitrary commutative ring with identity. Generalize the previous problem to construct the free commutative R-algebra on an arbitrary set X.

UMP 6. Let F be a field. Let $n \geq 2$ be an integer. Let $F\langle x_1, \dots, x_n\rangle$ be the vector space over F whose basis consists of all monomials in the x_i where the variables are not allowed to commute. Define the degree of a monomial h to be the total number of variables that appear (e.g., $h = x_3^2 x_1 x_2^4 x_3$ has degree 8). An element of this ring is a finite linear combination of these monomials. Two are multiplied via $h_1 \cdot h_2 = h_1 h_2$ (juxtapose – combine any adjacent equal variables by adding the expontents, otherwise do nothing – e.g., $x_1x_2 \cdot x_2x_1 = x_1x_2^2x_1$ and $x_1x_2 \cdot x_3x_1x_2 = x_1x_2x_3x_1x_2$). Elements of F commute with the x_i and the multiplication is extended by the distributive law. This gives a ring structure on $F\langle x_1, \dots, x_n\rangle$ and in fact, it becomes an F-algebra. For any non-zero f in this ring, $\deg f$ is defined to be the maximum of the degrees of the monomials with non-zero coefficients which appear in it. In the following you will show that the informal description above leads to a formal construction.

a. Count the number of monomials of degree exactly k for $k > 0$.

b. Let H_m be the collection of all polynomials of degree less than m together with 0. It is a subspace. What is its dimension?

c. State and prove the Universal Mapping Property analogous to Theorem 6 where the F-algebra A is now allowed to be non-commutative.
Here is an outline of the construction of the free F-algebra: Let M be the vector space with basis $\mathcal{B}$ the set of all non-commuting monomials h in n non-commuting variables as described above. Let $\operatorname{End}_F(M)$ denote the ring of endomorphisms of M. Using the UMP for the basis of M define the linear transformation T_i, $1 \le i \le n$, by as "right multiplication by x_i"

$$T_i(h) = h \cdot x_i$$

where the multiplication of monomials is as described above. [Careful: There are two cases to consider depending on whether or not h has x_i as the last variable on the right.] Let $A \subseteq \operatorname{End}_F(M)$ be the sub-F-algebra generated by all of the T_i. Note that A contains the identity linear transformation by the definition of F-algebra. Hence A contains the set $\mathcal{B}$ of all monomials (note that the identity is the monomial where all degrees on all terms equal 0). Now prove that A is the free (non-commutative) F-algebra on $\mathcal{A} = \{x_1, x_2, \ldots, x_n\}$.

UMP 7. Let R be an arbitrary ring with identity. Combine the ideas in the problems Exercise 4 and Exercise 6 to construct the free (non-commutative) R-algebra in n variables for n a positive integer.

UMP 8. Let R be an arbitrary ring with identity. Generalize the previous problem to construct the free (non-commutative) R-algebra on an arbitrary set X.

UMP 9. Let B be a set and assume $B \subseteq A$ for some abelian group A. Define what it would mean for A to be a *free abelian group* on B. Show that for any arbitrary set B there exists a free abelian group with basis B. Prove that any two free abelian groups on B are isomorphic. Show that if B_1 and B_2 are two sets, then the free abelian group on B_1 is isomorphic to the free abelian group on B_2 if and only if $|B_1| = |B_2|$ (i.e., the two sets have the same cardinality).

UMP 10. Give a definition of a 'free group', and state and prove the universal property that it satisfies.
A brief description of the ideas required: Let X be an arbitrary set. Let $X \dot\cup \overline{X}$ denote the disjoint union of two sets, the first being X and the second being the set of all symbols $\overline{x}$ for all $x \in X$. Let Z be the set of all finite sequences of of elements in $X \dot\cup \overline{X}$ (including the empty sequence $[\ ]$). Let $\mathcal{S}(Z)$ denote the group of all permutations of the set Z. For any $x \in X$ define a "right multiplication" r_x of x on Z analogous to what was done in Exercise 6 (think of $\overline{x}$ as denoting the inverse of x with the product of the two in either order cancelling out). This definition of r_x will basically involve two cases. Let F_X denote the subgroup of $\mathcal{S}(Z)$ generated by all the r_x for $x \in X$. Prove that F_X is the free group on the set X.

UMP 11. Let $n > 1$ be an integer.

a. Show that A being a module over $\mathbb{Z}$ is equivalent to A being an abelian group.

b. Let A be an abelian group. Show that A is a module over the ring $\mathbb{Z}_n$ if and only if $n \cdot a = 0$ for all $a \in A$. [Note that this generalizes one of your early exercises on fields.]

c. Show that $\mathbb{Z}^m$ is a free $\mathbb{Z}$-module for all $m > 0$. Describe all free $\mathbb{Z}$-modules, e.g., those with a basis $\mathcal{B}$.

d. Show that $\mathbb{Z}_n^m$ is a free $\mathbb{Z}_n$-module for all $m > 0$. Describe all free $\mathbb{Z}_n$-modules, e.g., those with a basis $\mathcal{B}$.

UMP 12. Let F be a field and let $\{ V_i \mid i \in I \}$ be a collection of vector spaces over F.

a. If $I = \{1, \ldots, n\}$ is a finite set, define the product $\prod_{i=1}^n V_i$ via a universal mapping property.

b. Verify that the usual direct sum of the V_i with appropriate maps gives the product when $I = \{1, \ldots, n\}$ is a finite set.

c. If $I = \{1, \ldots, n\}$ is a finite set, define the coproduct $\coprod_{i=1}^n V_i$ via a universal mapping property.

d. Verify that the usual direct sum of the V_i with appropriate maps gives the coproduct when $I = \{1, \ldots, n\}$ is a finite set.

e. If I is arbitrary, define the product $\prod_{i \in I} V_i$ and the coproduct $\coprod_{i \in I} V_i$ via universal mapping properties. Consider the vector space $\bigoplus_{i \in I} V_i$. Does it together with some collection of maps give either the product or coproduct? Answer the same question for $\prod_{i \in I} V_i$ as defined in the section on "Direct Sums and Products". [Hint: See the exercises at the end of the section on "Bases and Coordinates".]

UMP 13 (Pushout). Let V, M_1, M_2 be vector spaces over the field F and $\varphi_i : V \to M_i$ linear transformations. Let W be a vector space over F and let $\psi_i' : M_i \to W$ be linear transformations that make the following diagram commute,

$$\begin{tikzcd}
V \arrow[r, "\varphi_1"] \arrow[d, "\varphi_2"'] & M_1 \arrow[d, "\psi_1'"'] \\
M_2 \arrow[r, "\psi_2'"] & W
\end{tikzcd}$$

that is, $\psi_1' \circ \varphi_1 = \psi_2' \circ \varphi_2$.

a. Show that there exists a vector space Y and linear transformations $\psi_i : M_i \to Y$ which makes the diagram commute, and that is universal among all such; that is, there exists a unique $\eta \in \mathrm{Hom}_F(Y, W)$ such that the following diagram commutes:

$$\begin{tikzcd}
V \arrow[r, "\varphi_1"] \arrow[d, "\varphi_2"'] & M_1 \arrow[d, "\psi_1"'] \arrow[ddr, "\psi_1'"] & \\
M_2 \arrow[r, "\psi_2"] \arrow[drr, "\psi_2'"'] & Y \arrow[dr, dotted, "\eta"] & \\
 & & W
\end{tikzcd}$$

b. Show that Y is determined uniquely up to isomorphism by V, M_1, M_2 and the linear transformations φ_1, φ_2.

c. Consider the special case when both φ_1 and φ_1 are zero. Explain why and how the universal object constructed in part a is related to a construction considered earlier.

UMP 14 (Pullback). Start with the same diagram as in the previous problem, and define the *pullback* of the diagram as the object (and arrows) in the upper left-hand corner that is universal with respect to an incoming arrow that makes the appropriate diagram commute. Verify that the the pullback exists for vector spaces and is unique up to isomorphism. Give an analogue to the last part of the previous problem.

UMP 15. Let F be a field and M a module over the formal polynomial ring $F[x]$. Note that M must be a vector space over F. Assume it has finite dimension. Since M is an $F[x]$-module, multiplication by x gives a linear transformation on the underlying vector space of M. Explain.

More precisely, give the one-to-one correspondce between the two collections:

the collection of all finite-dimensional $F[x]$-modules M

and

the collection of pairs (T, V) where V is a finite-dimensional vector space over F and T an endomorphism of V, that is, a linear transformation $T : V \longrightarrow V$.

History of the Notes

The Notes for the course *Math 4330, Honors Linear Algebra* at Cornell University have been developed over the last ten years or so mainly by the following (in chronological order):

Gerhard O. Michler

R. Keith Dennis

Martin Kassabov

W. Frank Moore

Yuri Berest.

Harrison Tsai also contributed a number of interesting exercises that appear at the ends of several sections of the notes.

Most sections have been revised so many times the original author may no longer recognize it. The intent is to provide a modern treatement of linear algebra using consistent terminology and notation. Some sections are written simply to provide a central source of information such as those on "Useful Definitions", "Subobjects", and "Universal Mapping Properties" rather than as a chapter as one might find in a traditional textbook. Additionally there are sections whose intent is to provide proofs of some results which are not given in the lectures, but rather provide them as part of a more thorough development of a tangential topic (e.g., Zorn's Lemma to develop cardinal numbers and the existence of bases and dimension in the general case).

A large number of challenging exercises from many different sources have been included. Although most should be readily solvable by students who have mastered the material, a few even more challenging ones still remain.

Much still remains to be done. Corrections and suggestions for additional exercises, topics and supplements are always welcome.

Keith Dennis

e-mail address: **math4330@rkd.math.cornell.edu**

Math 4330 Handout List

0. **Course information.**

1. **Fields.**

2. **Some Useful Definitions.**

3. **Examples of Vector Spaces.**

4. **Subobjects**

5. **Direct Sums and Products**

6. **Equivalence Relations**

7. **Quotient Spaces**

8. **Exact Sequences**

9. **Bases and Coordinates**

10. **Universal Mapping Properties**

Math 4330 Take-Home Exam 1

Friday, October 16 – Friday, October 23, 2015

Your work on this exam is to be done in accordance with the following:

1. You may use the handouts, your own class notes, but nothing else; e.g., no books (not even the ones you've been referred to) nor the internet.
2. You may not obtain aid nor discuss the exam with any other person.
3. If you have any questions, please send e-mail, call, or come by my office:
   Keith Dennis Malott 524 255-4027 **math4330@rkd.math.cornell.edu**
   Please do not ask the TA any questions about the exam as he has been instructed to refer all questions to me.
4. Please return the exam to me or to the receptionist in the Math Office (third floor, Malott) by 4:00 pm, Friday, October 23. You may instead submit your solutions as a pdf file by e-mail to the address given above (same deadline: 4:00 pm).

PLEASE WRITE YOUR ANSWERS VERY CAREFULLY, EXPLAINING EXACTLY WHAT YOU ARE DOING, AND SHOWING ALL OF THE COMPUTATIONS.

ALL PARTS OF ALL PROBLEMS REQUIRE PROOFS.

Fields 31

Let F be a field. Assume that A is an algebra with identity over F (see "Some Useful Definitions"). Assume further that

(1) If $ab = 0$ for $a, b \in A$, then either $a = 0$ or $b = 0$.

(2) The dimension of A over F is finite.

a. Prove that every non-zero element of A has a multiplicative inverse. [Hint: Let $a \in A$, $a \neq 0$, and define $T_a : A \longrightarrow A$ by $T_a(b) = ba$. Show that T_a is a linear transformation and use theorems about linear transformations to prove that a has a left inverse. Then show that if every non-zero element of A has a left inverse, then the left inverses are actually two-sided inverses. (Note that this last part would not have been necessary if we assumed that A had commutative multiplication.)]

b. Let A be a subset of the complex numbers which is a commutative ring under the usual addition and multiplication of complex numbers. If A contains $\mathbb{Q}$ (the field of rational numbers) and is finite dimensional over $\mathbb{Q}$, conclude that A is a field. In particular, if $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Q}[x]$ and $r \in \mathbb{C}$ is a root of $f(x)$, prove that the set

$$\mathbb{Q}[r] = \{\, q_0 + q_1 r + \cdots + q_{n-1} r^{n-1} \mid q_i \in \mathbb{Q} \,\}$$

is a field.

QuoSpace 15

Let V be a vector space over a field F. We **do not** assume that V is finite-dimensional. (If $\dim V < \infty$, then the equivalence relation defined below is not very interesting. Explain.)

a. Let A and B be subspaces of V. Prove that the following conditions are equivalent:

$$(i)\ \dim(A+B)/(A\cap B) < \infty\,,$$

$$(ii)\ \dim A/(A\cap B) < \infty \quad \text{and} \quad \dim B/(A\cap B) < \infty\,,$$

$$(iii)\ \dim(A+B)/A < \infty \quad \text{and} \quad \dim(A+B)/B < \infty\,.$$

If A and B are subspaces, write $A \sim B$ if they satisfy the above conditions. For example, if $W \subseteq V$ is a subspace with basis $\mathcal{B}$ and we let $\mathcal{B}'$ be a subset obtained from $\mathcal{B}$ by removing a finite number of vectors, then $W \sim \operatorname{Span}_F \mathcal{B}'$. Similarly if $\mathcal{B}''$ is obtained from $\mathcal{B}$ by adding any finite number of vectors from V, then $W \sim \operatorname{Span}_F \mathcal{B}''$.

Describe all subspaces equivalent to 0. Describe all subspaces equivalent to V.

b. Prove that $\sim$ is an equivalence relation on the set of subspaces of V. (Hint: Prove first that if $A \sim B$ and $B \sim C$, then $\dim(A+B+C)/(A\cap B\cap C) < \infty$.)

c. Let A, B, A' and B' be subspaces in V such that $A \sim A'$ and $B \sim B'$. Prove then that

$$A+B \sim A'+B' \quad \text{and} \quad A\cap B \sim A'\cap B'\,.$$

d. Let $\mathbf{C}(V)$ denote the set of the $\sim$ equivalence classes, which we denote by $[W]$ for $W \subseteq V$ a subspace of V. Prove that $+$ gives a binary operation that is commutative, associative, and which has an additive identity. Prove that no element other than the identity of $\mathbf{C}(V)$ has an additive inverse. For any subspace $W \subseteq V$ compute $[W]+[W]$

e.

Consider the case where V has countable dimension over F. For example, let a basis for V be set

$$\mathcal{B} = \{ v_i \in V \mid i \in \mathbb{Z} \} .$$

For every positive integer n prove that there exist subspaces $V_i \subseteq V$, $1 \leq i \leq n$ satisfying

(1) $[V_1] + \cdots + [V_n] = [V]$,

(2) $V_i \cap V_j = 0$ and $[V_i] \neq [V_j]$ for $i \neq j$,

(3) All $[V_i]$ are different from $[0]$ and $[V]$,

(4) There exists an isomorphism of vector spaces $\gamma : V \longrightarrow V$ which induces an isomorphism of $\mathbf{C}(V)$ with itself and is such that $\gamma(V_i) = V_{i+1}$ for $1 \leq i < n$, and $\gamma(V_n) = V_1$.

f.

Same assumptions on V as the previous part. Show that there exist subspaces $Z_i \subseteq V$, $i \geq 1$ such that

(1) $[Z_i]$ are all unequal to $[0]$ and unequal to $[V]$,

(2) for any i, $Z_{i+1} \subset Z_i$ and $[Z_{i+1}]$ is not equal to $[Z_i]$.

That is, there is an infinite chain of non-trivial unequal elements of $\mathbf{C}(V)$ that get smaller and smaller.

g.

Same assumptions on V as the previous part. Start with $Z_1 \subset V$ of the previous part. Show that there is also an infinite ascending chain of unequal elements Y_j $j \geq 2$ with $Z_1 \subset Y_2 \subset Y_3$.
So $\mathbf{C}(V)$ in this case is quite large and has some unusual properties.