Section IV.2. Free Modules and Vector Spaces

Note. In this section, we consider free objects (in the sense of Definition I.7.7) in the category of modules over a ring (see Note IV.1.D.). We define linearly independent sets and basis for an R-module. Conditions are given under which all bases are of the same cardinality (and in those cases this cardinality gives the dimension of the R-module). As a special case, we consider vector spaces, which will play a role when we explore field extensions and field theory in Chapter V.

Note. Three results from this section are used in Chapter V. Fields and Galois Theory. Theorem IV.2.4 is used in Section V.5. Finite Fields; it's used in the proof of Corollary V.5.2 concerning the characteristic and order of a finite field). Theorem IV.2.5 is used in Section V.2.Appendix. Symmetric Rational Functions. Theorem IV.2.16 is also used in Appendix V.2.A as well as in the proof of the very fundamental Theorem V.1.1 concerning dimensions of extension fields.

Definition. A subset X of an R-module A is *linearly independent* provided that for distinct $x_1, x_2, \ldots, x_n \in X$ and $r_i \in R$, $r_1x_1 + r_2x_2 + \cdots + r_nx_n = 0$ implies $r_i = 0$ for all i. A set that is nor linearly independent is *linearly independent*. If A is generated as an R-module by a set Y, then Y *spans* A.

Note IV.2.A. If R has an identity and A is unitary then X spans A if and only if every element of A may be written as $r_1x_1 + r_2x_2 + \cdots + r_nx_n$ (where $r_i \in R$ and $x_i \in X$); see Theorem IV.1.5(iii).

Definition. A linearly independent subset of an R-module A that spans A is a *basis* for A.

Note. Since a vector space is a unitary R-module where R is an integral domain, then the previous two definitions are the ones we use in the vector space setting (which plays a large role in Chapter V. Fields and Galois Theory).

Note IV.2.B. If X is a basis for unitary R-module A, then we claim that each nonzero $u \in A$ has a unique representation as a linear combination of elements of X. Suppose $u = \sum_{i=1}^{n} r_i x_i$ and $u = \sum_{i=1}^{m} r'_i x'_i$ where WLOG we may take $r_i, r'_i \neq 0$ for all i and j. Let $X_1 = \{x_1, x_2, \ldots, x_n\} \setminus \{x'_1, x'_2, \ldots, x'_m\}$, $X_2 = \{x_1, x_2, \ldots, x_n\} \cap \{x'_1, x'_2, \ldots, x'_m\}$, and $X_3 = \{x'_1, x'_2, \ldots, x'_n\} \setminus \{x_1, x_2, \ldots, x_m\}$. Say (reindexing the x's, x''s, and corresponding coefficients as needed) $X_1 = \{x_{\ell+1}, x_{\ell+2}, \ldots, x_n\}$, $X_2 = \{x_1 = x'_1, x_2 = x'_2, \ldots, x_\ell = x'_\ell\}$, and $X_3 = \{x'_{\ell+1}, x'_{\ell+2}, \ldots, x'_m\}$. Then

$$0 = u - u = \sum_{i=1}^{n} r_i s_i - \sum_{i=1}^{m} r'_i x'_i = \sum_{i=1}^{\ell} (r_i - r'_i) x_i + \sum_{i=\ell+1}^{n} r_i x_i - \sum_{i-\ell+1}^{m} r'_i x'_i$$

so that by linear independence, $r_i - r'_i = 0$ (or $r_i = r'_i$) for $1 \leq i \leq \ell$, $r_i = 0$ for $\ell + 1 \leq i \leq n$, and $r'_i = 0$ for $\ell + 1 \leq i \leq m$. Since we assumed $r_1, r'_i \neq 0$, then we must have $\ell = m = n$ and $u = \sum_{i=1}^{\ell} r_i x_i$ representation of u as a linear combination of elements of X.

Theorem IV.2.1. Let R be a ring with identity. The following on a unitary R-module F are equivalent.

(i) F has a nonempty basis.

(ii) F is the internal sum of a family of cyclic R-modules, each of which is isomorphic as a left R-module to R.

(iii) F is R-module isomorphic to a direct sum of copies of the left R-module R.

(iv) There exists a nonempty set X and a function $\iota : X \to F$ with the following property: given any unitary R-module A and function $f : X \to A$ there exists a unique R-module homomorphism $\overline{f} : F \to A$ such that $\overline{f}\iota = f$. In other words, F is a free object in the category of unitary R-modules.

Definition. A unitary module F over a ring R with identity, which satisfies the equivalent conditions of Theorem IV.2.1 is a *free R-module* on set X.

Note IV.2.C. Part (iii) gives a relatively easy classification of a free R-module. Unitary R-module F is a free R-module if (and only if) it is isomorphic to $\sum_X R$ where X is a basis for F. A basis for $\sum_X R$ is given by $\{\theta_x \mid x \in X\}$ is as defined in the (iv) $\Rightarrow$ (iii) part of the proof of Theorem IV.2.1.

Note. By part (iv) of Theorem IV.2.1, a free R-module F is a free object on set X (where X is a basis of F) in the category of unitary R-modules. But such F is not a free object on any set in the category of all R-modules, as is to be shown in Exercise IV.2.15.

Note IV.2.D. The definition of a free module given by the conditions of Theorem IV.2.1 requires that ring R has an identity 1_R and that R-module F is unitary (that is, $1_R f = f$ for all $f \in F$). Notice that without an identity in R, we loose the property of generating set Y which satisfies the linear combination property given in Note IV.2.A. Notice that without an identity in R, we lose the property of generating set X satisfying the linear combination property given in Note IV.2.A. The following definition is given in Exercise IV.2.2 and does not require R to have an identity or (when it does) F to be unitary.

> **Definition.** Let R be any ring (possibly without an identity) and let X be a nonempty set. An R module F is a *free module on* X if F is a free object on X in the category of <u>all</u> (left) R-modules.

It is shown in Exercise IV.2.2 that for any ring and any set X, there is a free module on X (in the sense of this definition). However, these free modules (unlike those based on a unitary R-module above) are no isomorphic to a direct sum of copies of R (even when R does contain an identity; see Exercise IV.2.2(b)). In the remainder of these notes, we use the term "free module" as in the sense defined by Theorem IV.2.1 (unless state otherwise).

Note IV.2.E. The proof of Theorem IV.2.1 established some other results. If F is a free R-module on set X then by (iv) of Theorem IV.2.1 we have $\iota : X \to F$ and (as argues in the (iv) $\Rightarrow$ (iii) part of Theorem IV.2.1, in the notation of the proof of Theorem I.7.8, but with $i : X \to F$ of Theorem I.7.8 replaces with ι here and F' there replaces with $\sum_X R$ here) $\varphi \circ \iota : X \to \sum_X R$ or $\varphi : \iota : X \to \sum_X R$ where $\iota X \subset F$ is mapped to basis Y of $\sum_X R$. Since φ is an R-module isomorphism and

Y is a basis of $\sum_X R$, then ιX is a basis of F. Conversely, if X is a basis of F then, as shown in the (i) $\Rightarrow$ (iv) part of Theorem IV.2.1, unitary R-module F over ring R with identity is free on X, with $i : X \to F$ as the inclusion map.

Note IV.2.F. For nonempty set X and ring R with identity, we can create free R-module F by letting $F = \sum_X R$. Then a basis for F given by $\{\theta_x \mid x \in X\}$; see Note IV.2.C above. Notice that $R\theta_x \cong R$ and elements of $R\theta_x$ are of the from $\{s_i\}_{i \in x}$ where $s_i \in r$ for $i = x$ and $s_i = 0$ for $i \neq x$. The direct sum $\sum_{x \in X} R\theta_x$ is the same as $\sum_X R$, so that $F = \sum_{x \in X} R\theta_x$. The map $\iota : X \to F$ defined as $x \mapsto \theta_x$ is injective and we then have that F is a free R-module on set X since it satisfies (iv) of Theorem IV.2.1 (we just need to verify that for any given unitary R-module A and any function $f : X \to A$, there is a unique homomorphism $\bar{f} : F \to A$ such that $\bar{f}\iota = f$; this follows easily since $\iota X = \{\theta_x \mid x \in X\}$ is a basis of F). Under these conditions, **by convention we adopt the notation where we replace x by $\iota(x) = \theta_x$.** In this way, we treat $\iota X = X$, or $\{x \mid x \in X\} = \{\theta_x \mid x \in X\}$ so that X is teated as a basis of F, and we write $F = \sum_{x \in X} Rx$. An element of F is then, under this convention, of the form $r_1x_1 + r_2x_2 + \cdots + r_nx_n$ where $r_i \in R$ and $x_i \in X$.

Corollary IV.2.2. Every unitary module A over a ring R (with identity) is the homomorphic image of a free R-module F. If A is finitely generated, then F may be chosen to be finitely generated.

Note IV.2.G. Hungerford claims (see his "Remark" on page 182) that Corollary IV.2.2 also holds if the parenthetic words are dropped and the term "free module" is replaced with the more general idea of a free module in the category of all (left) R-modules over arbitrary given ring R (see Note IV.2.D and Exercise IV.2.2).

Note IV.2.H. Every subgroup of a free abelian group is free abelian and the rank of the subgroup is at most the rank of the given group. This follows from a result in Section IV.6. Modules over a Principal Ideal Domain, namely Theorem IV.6.1, and the facts that every additive abelian group G is a unitary $\mathbb{Z}$-module (see Example IV.1.A), and $\mathbb{Z}$ is a principal ideal domain since every ideal of $\mathbb{Z}$ is of the form $\langle n \rangle$ $\{kn \mid k \in \mathbb{Z}\}$. This is not the case for free modules, however. For example, $\{\bar{0}, \bar{2}, \bar{4}\}$ is not a free $\mathbb{Z}_6$-module, since $\{\bar{0}, \bar{2}, \bar{4}\}$ can have no basis because $\bar{3}(\bar{2}) = \bar{2}(\bar{4}) = \bar{0}$ and there can be no linearly independent subset of $\{\bar{0}, \bar{2}, \bar{4}\}$.

Note. Recall that a vector space is a unitary D-module where D is a division ring. We'll prove below (in Theorem IV.2.4) that every vector space is a free D-module. Well do so by showing that every vector space has a basis. You may see it proved that a vector space has a basis in other classes. For example, this is shown in Fundamentals of Functional Analysis (MATH 5740) for a vector space over a field in Supplement/Section 5.1. Groups, Fields, and Vector Spaces. In the analysis setting, the type of bases we describe in this section is called a "Hamel basis." The existence of such a basis does not tell us what the basis is, and this leads us to explore other types of bases in the analysis setting (namely, a "Schauder basis"

which requires the existence of a metric, or at least a topology, since ti allows for infinite linear combinations in the form of series). Before we prove that all vector spaces over a unitary D-module are free D-modules, we need a preliminary lemma.

Lemma IV.2.3. A maximal linearly independent subset X of a vector space V over a division ring D is a basis of V.

Note. In light of Lemma IV.2.3, to show that a vector space has a basis, it is sufficient to show the existence of a maximal linearly independent set in the vector space. The proof requires Zorn's Lemma and the proof is virtually identical to the proof of the existence of a Hamel basis for a vector space that you might see in an analysis class.

Theorem IV.2.4. Every vector space V over a division ring D has a basis and is therefore a free D-module. More generally every linearly independent subset of V is contained in a basis of V.

Note. The converse of Theorem IV.2.4 holds in the following sense: If every unitary module over a ring D with identity is free, then D is a division ring. This is to be proved in Exercise IV.3.14 of the next section.

Note. The next theorem shows that every spanning set of a vector space over a division ring contains a basis. Again, Zorn's Lemma is used in the proof so that we do not know which elements of the generating set are in the resulting basis.

Theorem IV.2.5. If V is a vector space over a division ring D and X is a subset that spans V, then X contains a basis of V.

Note IV.2.I. We now turn our attention to the cardinality of a basis of a free R-module. We expect any two bases of a free R-module to be of the same cardinality. After all, this is how we define the dimension of a vector space (see my online Linear Algebra [MATH 2010] on Section 3.2. Basic Concepts of Vector Spaces and notice Corollary 3.2.A, "Invariance of Dimension for Finitely Generated Spaces," and Definition 3.7 of *dimension*). We have seen that this preservation of cardinality between bases holds for $\mathbb{Z}$-modules (that is, for free abelian groups see Note IV.1.A) by Theorem II.1.2. We will see in the next two theorems that it also holds for free R-modules with an infinite basis and holds for vector spaces over integral domains. However, it does not hold for free modules over arbitrary rings with identity. This is to be shown in Exercise IV.2.13.

Theorem IV.2.6. Let R be a ring with identity and F a free R-module with an infinite basis X. Then every basis of F has the same cardinality as X.

Theorem IV.2.7. If V is a vector space over a division ring D, then two bases of V have the same cardinality.

Note IV.2.J. Theorems IV.2.6 and IV.2.7 do not cover all possible free R-modules. The hypotheses of Theorem IV.2.6 require that the free R-module has an infinite basis. Theorem IV.2.7 covers all free D-modules where D is a division ring. So the cardinality of a free R-module over a ring R with identity which id *not* a division ring and which does *not* have an infinite basis, my still have (finite) bases of different cardinality (a most disturbing possibility, based on our experience with vector spaces!). In Exercise IV.2.13, a ring R with identity is given for which, it is to be shown, for all $n \in \mathbb{N}$ the free (left) R-module has a basis of cardinality n. As a consequence, we cannot define the dimension of a free R-module in general, but we can in several special cases. This observation motivates the next definition.

Definition IV.2.8. Let R be a ring with identity such that for every free R-module F, any two bases of F have the same cardinality. Then E is said to have the *invariant dimension property* and the cardinal number of any basis of F is called the *dimension* (or *rank*) of F over R.

Note. Notice that the invariance dimension property is defined in terms of free R-modules, but it is a property of ring R itself (and not a property of any particular free R-module). Hungerford adopts the convention of using the term "dimension" in connection with vector spaces, and using the term "rank" in connection with free modules over a ring (though he admits that this is not a universal convention; see his page 185). If V is a vector space over division ring D then the dimension of V is denoted $\dim_D(V)$. We now temporarily skip Proposition IV.2.9 through

Corollary IV.2.12; these results are needed in Section IV.6. Modules over a Principal Ideal Domain (this section is necessary for a graduate-level Linear Algebra class based on Hungerford's *Algebra* book) and Section VII.5, "The Characteristic Polynomial, Eigenvectors and Eigenvalues" (which is part of the graduate-level Linear Algebra class). First, we consider properties of $\dim_D(V)$ starting with the following definition.

Definition. A vector space V over a division ring D is *finite dimensional* if $\dim_D(V)$ is finite.

Theorem IV.2.13. Let W be a subspace of a vector space V over a division ring D.

(i) $\dim_D(W) \leq \dim_D(V)$;

(ii) if $\dim_D(W) = \dim_D(V)$ and $\dim_D(V)$ is finite, then $W = V$;

(iii) $\dim_D(V) = \dim_D(W) + \dim_D(V/W)$.

Note IV.2.K. Recall that linear transformation from $\mathbb{R}^n$ to $\mathbb{R}^m$ are represented by $m \times n$ matrices; see my online notes for Linear Algebra (MATH 2010) on Section 2.3. Linear Transformations of Euclidean Spaces and notice Corollary 2.3.A. The *nullspace* of $m \times n$ matrix A (also sometimes called the "kernel" of A) is the set of vectors in $\mathbb{R}^n$ mapped to the zero vector in $\mathbb{R}^m$ when the vectors are multiplied (on the left) by the matrices. The *range* of A is the column space of A (in $\mathbb{R}^m$). The dimension of the nullspace is the *nullity* of matrix A and the dimension of the

column space is the *rank* of matrix A. The Rank Equation (see Theorem 2.5 in my Linear Algebra notes on Section 2.2. The Rank of a Matrix) states that for $m \times n$ matrix A, $\text{rank}(A)+\text{nullity}(A) = n$ (where n is the number of columns of A and the dimension of the domain, $\mathbb{R}^n$, of the linear transformation determined by A). The next corollary concerns linear transformation between vector spaces over a common division ring. In the corollary, the kernel of the linear transformation plays the role of the nullity of matrix A, the image of the linear transformation plays the role of the column space of matrix A, and the domain of the linear transformation plays the role of the domain of matrix A.

Corollary IV.2.14. If $f : V \to V'$ is a linear transformation of vector spaces over a division ring D, then there exists a basis X of V such that $X \cap \text{Ker}(f)$ is a basis of $\text{Ker}(f)$ and $\{f(x) \mid f(x) \neq 0, x \in X\}$ is a basis of $\text{Im}(f)$. In particular, $\dim_D(f) = \dim_D(\text{Ker}(f)) + \dim_D(\text{Im}(f))$.

Corollary IV.2.15. If V and W are finite dimensional subspaces of a vector space over a division ring D, then $\dim_D(V)+\dim_D(W) = \dim_D(V \cap W)+\dim_D(V+W)$.

Note. If R is a division ring contained in division ring S, then S is a vector space over R with the product rs, where $r \in R$ and $s \in S$, as the usual product in S. The next theorem is restated in Section V.1. Field Extensions as Theorem V.1.2 and is used again in the proof of Lemma V.2.19 of Section V.2.Appendix. Symmetric Rational Functions (an appendix to Section V.2. The Fundamental Theorem (of Galois Theory)).

Theorem IV.2.16. Let R, S, T be division rings such that $R \subseteq S \subseteq T$. Then $\dim_R(T) = (\dim_S(T))(\dim_R(S))$. Furthermore, $\dim_R(T)$ is finite if and only if $\dim_S(T)$ and $\dim_R(S)$ are finite.

Note IV.2.L. Let $\mathbb{R}$ and $\mathbb{C}$ be the fields of real and complex numbers, respectively. There is no purely algebraic definition of $\mathbb{R}$; we need the analytic ideas of completeness or of a "continuum." In Analysis 1 (MATH 4217/5217), the real numbers are defined as a complete ordered field (see my online notes for Analysis 1 on Section 1.2. Properties of the Real Numbers as an Ordered Field and Section 1.3. The Completeness Axiom). In fact, up to isomorphism, there is only one complete ordered field; see my Analysis 1 notes on Supplement. The Real Numbers are the Unique Complete Ordered Field. With the real numbers defined, we can algebraically define the complex numbers as the algebraic extension $\mathbb{R}(i)$ where i is a root of $x^2 + 1 \in \mathbb{R}[x]$; see Section VI.1. Field Extensions and notice Example V.1.A. In terms of vector spaces, we treat $\mathbb{R}$ and $\mathbb{C}$ as vector spaces over division ring $D = \mathbb{R}$. We immediately have $\dim_{\mathbb{R}}(\mathbb{F} = 1$ since a basis is given by $\{1\}$. In Complex Analysis 1 (MATH 5510; see my online notes on Section I.2. The Field of Complex Numbers), the field of complex numbers is defined as $\mathbb{C} = \{(a, b) \mid a, b \in \mathbb{R}\}$ where addition and multiplication are defined as $(a, b) + (c, d) = (a + c, b + d)$ and $(a, b) \cdot (c, d) = (ac - bd, bc + ad)$. The multiplicative identity is $(1, 0)$ and we denote $(0, 1)$ as i and we have $i^2 = -1$. In general, we denote (a, b) as $a + ib$. Notice that $a + ib = c + id$ (i.e., $(a, b) = (c, d)$) if and only if $a = c$ and $b = d$. So we take $\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}\}$, and claim that $\{1, i\}$ is a basis for $\mathbb{C}$ as a vector space over $\mathbb{R}$. Suppose $r_1(1) + r_2(i) = 0$, i.e. $r_1 + ir_2 = 0$ in $\mathbb{C}$. Then $r_1 = r_2 = 0$. That is, $\{0, i\}$

is a linearly independent set. Also for any $a+ib \in \mathbb{C}$ we have $a+ib = a(1)+b(i)$ and $\{1, i\}$ is a spanning set. Therefore $\{1, i\}$ is a basis for $\mathbb{C}$ as a vector space over $\mathbb{R}$, $\dim_{\mathbb{R}}(\mathbb{C}) = 2$. This establishes part (a) of Exercise IV.2.6. A proof of part (b) is given in the "Proofs of Theorems" supplement:

Exercise IV.2.6(b). There is no field K such that $\mathbb{R} \subsetneq K \subsetneq \mathbb{C}$.

Note. We now return to results IV.2.9 to IV.2.12 which are referenced in Section IV.6. Modules over a Principal Ideal Domain and needed for a graduate-level course on Linear Algebra. The proof of Proposition IV.2.9 is left as Exercise IV.2.A.

Proposition IV.2.9. Let E and F be free modules over a ring R that has the invariant dimension property. Then $E \cong F$ if and only if E and F have the same rank.

Note. The last two main results we consider involve conditions under which the invariant dimension property holds. We first need a preliminary lemma.

Lemma IV.2.10. Let R be a ring with identity, I $(\neq R)$ an ideal of R, F a free R-module with basis X and $\pi : F \to F/IF$ the canonical epimorphism. Then F/IF is a free R/I-module with basis $\pi(X)$ and $|\pi(X)| = |X|$.

Proposition IV.2.11. Let $f : R \to S$ be a nonzero epimorphism of rings with identity. If S has the invariant dimension property, then so does R.

Corollary IV.2.12. If R is a ring with identity that has a homomorphic image which is a division ring, then R has the invariant dimension property. In particular, every commutative ring with identity has the invariant dimension property.

Revised: 1/7/2024