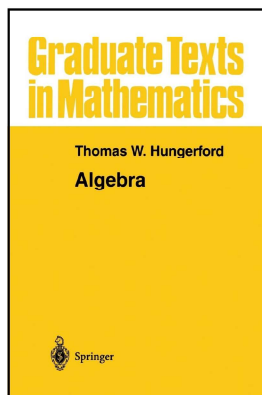


Modern Algebra

Chapter IV. Modules

IV.2. Free Modules and Vector Spaces—Proofs of Theorems



Theorem IV.2.1

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

Proof. (i) \Rightarrow (ii). Suppose F has a nonempty basis X and let $x \in X$. The map $R \rightarrow x$ given by $r \mapsto rx$, is an R -module epimorphism by Theorem IV.1.5(i).

Theorem IV.2.1 (continued 1)

Proof (continued). If $rx = 0$ then $r = 0$ since X is a linearly independent set, whence the map is a monomorphism (one to one, by Theorem I.2.3; see the comment on page 170). Of course the mapping is onto (by the definition of Rx) and so $R \cong Rx$ as left modules.

By Theorem IV.1.5(iii), the elements of F are of the form $\sum_{i=1}^s r_i x_i$ where $s \in \mathbb{N}$, $r_i \in R$, and $x_i \in X$ (since basis X is a generating set of F). By Theorem IV.1.5(iv), the sum of family $\{Rx \mid x \in X\}$ consists of all finite sums $r_1 x_1 + r_2 x_2 + \cdots + r_n x_n$ where $r_i x_i \in Rx_i$ and $x_i \in X$. So F is the sum of the family $\{Rx \mid x \in X\}$. Denote as Rx_k^* the sum of the family $\{Rx \mid x \in X, x \neq x_k\}$. By Theorem IV.1.5(iv), Rx_k^* consists of elements of the form $r_1 x_1 + r_2 x_2 + \cdots + r_n x_n$ where $x_i \neq x_k$, so Rx_k (which consists of elements of the form rx_k) intersects Rx_k^* only consists of 0 (since the x 's are distinct) Now Theorem IV.1.15 holds and so $F \cong \sum_{x \in X} Rx$ (or $F = \sum_{x \in X} Rx$; see Note IV.1.G) as claimed.

Theorem IV.2.1 (continued 2)

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

- (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 .

Proof (continued). (ii) \Rightarrow (iii). Suppose F is the internal direct sum of a family of cyclic R -modules, each of which is isomorphic as a left R -module to R . Then, by Theorem IV.1.5, F is the sum of the family of cyclic R -modules, say $F = \sum_{i \in I} R_i$. By Exercise IV.1.8 (which extends Theorem I.8.10 to R -modules), since each $R_i \cong R$, then F is given as the internal direct sum $F = \sum_{i \in I} R$ (Theorem I.8.10 deals with internal weak direct products, but these are equivalent to internal direct sums in additive notation).

Theorem IV.2.1 (continued 3)

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

Proof (continued). (iii) \Rightarrow (i). Suppose F is isomorphic to a direct sum of copies of R , say $F \cong \sum_X R$. For $x \in X$, let θ_x denote the element $\{r_i\} \in \sum_X R$ where $r_i = 0$ for $i \neq x$ and $r_x = 1_R$. Let $Y = \{\theta_x \mid x \in X\}$. Notice that $0 \in \sum_X R$ is the element $\{r_i\} \in \sum_X R$ where $r_i = 0$ for all $i \in X$. Let distinct $\theta_{x_1}, \theta_{x_2}, \dots, \theta_{x_n} \in Y$ and let $r_1, r_2, \dots, r_n \in R$. Suppose $r_1\theta_{x_1} + r_2\theta_{x_2} + \dots + r_n\theta_{x_n} = 0$. If $r_1\theta_{x_1} + r_2\theta_{x_2} + \dots + r_n\theta_{x_n} = \{s_i\} \in \sum_X R$, then we have $s_1 = r_i$ for $i = x_j$ and $s_i = 0$ if $i \neq x_j$. So we must have $r_i = 0$ for each i . That is, set Y is linearly independent.

Theorem IV.2.1 (continued 4)

Proof (continued). To show that Y spans $\sum_X R$ it suffices (by Note IV.2.A) to show that any $y \in \sum_X R$ is of the form $r_1\theta_{x_1} + r_2\theta_{x_2} + \dots + r_x\theta_{x_n}$ for some $r_i \in R$ and $\theta_{x_i} \in Y$. Since $\sum_X R$ is a direct sum, then it is (in multiplicative notation) a weak direct product (see Definition I.8.3) so that $y_x = 0$ for all but finitely many $x \in X$. Say $y_x \neq 0$ for $x \in \{x_1, x_2, \dots, x_n\}$ where $y_{x_i} = r_i \neq 0$. Then $y = r_1\theta_{x_1} + r_2\theta_{x_2} + \dots + r_x\theta_{x_n}$. Therefore Y is a linearly independent spanning set of $\sum_X R$; that is, Y is a basis of $\sum_X R$.

Let $f : F \rightarrow \sum_X R$ be an isomorphism, and let A be the additive abelian group of R -module F . With B as the additive abelian group of R -module $\sum_X R$, we have $f : A \rightarrow B$ satisfying $f(a + c) = f(a) + f(c)$ and $f(ra) = rf(a)$ for all $a, c \in A$ and $r \in R$ by Definition IV.1.2; that is, f preserves linear combinations.

Theorem IV.2.1 (continued 5)

Proof (continued). Define $A = \{f^{-1}(\theta_x) \mid \theta_x \in Y\}$. Then for distinct $f^{-1}(\theta_{x_1}), f^{-1}(\theta_{x_2}), \dots, f^{-1}(\theta_{x_n}) \in Z$ and any $r_1, r_2, \dots, r_n \in R$ with $r_1f^{-1}(\theta_{x_1}) + r_2f^{-1}(\theta_{x_2}) + \dots + r_nf^{-1}(\theta_{x_n}) = 0$ we have (applying f to both sides of this equation) $r_1\theta_{x_1} + r_2\theta_{x_2} + \dots + r_n\theta_{x_n} = f(0) = 0$. Since the θ_{x_i} are linearly independent in $\sum_X R$, then we must have $r_1 = r_2 = \dots = r_n = 0$. Therefore Z is a linearly independent set in F . For any $z \in F$, $f(z) \in \sum_X R$ so that $f(z) = r_1\theta_{x_1} + r_2\theta_{x_2} + \dots + r_n\theta_{x_n}$ for some $\theta_{x_1}, \theta_{x_2}, \dots, \theta_{x_n} \in Y$ and some $r_1, r_2, \dots, r_n \in R$. Therefore $f(z) = r_1\theta_{x_1} + r_2\theta_{x_2} + \dots + r_n\theta_{x_n}$ and $z = r_1f^{-1}(\theta_{x_1}) + r_2f^{-1}(\theta_{x_2}) + \dots + r_nf^{-1}(\theta_{x_n})$. Therefore Z is a linearly independent spanning set of F ; that is, F has a bases and (i) holds, as claimed.

Theorem IV.2.1 (continued 6)

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

Proof (continued). (i) \Rightarrow (iv). Let X be a basis of F and $\iota : X \rightarrow F$ the inclusion map. Let A be a unitary R -module and $f : X \rightarrow A$. For any $u \in F$ we have $u = \sum_{i=1}^n r_i x_i$ for some $r_i \in R$ and some $x_i \in X$, since X is a spanning set (see Note IV.2.A) and by Note IV.2.B this representation is unique. So the map $\bar{f} : F \rightarrow A$ given by $\bar{f}(u) = \bar{f}(\sum_{i=1}^n r_i x_i) = \sum_{i=1}^n r_i f(x_i)$ is well-defined, and $\bar{f}\iota = f$.

Theorem IV.2.1 (continued 7)

Proof (continued). To show that \bar{f} is an R -module homomorphism, let $a, c \in A$. Then $a = \sum_{i=1}^n r_i x_i$ and $c = \sum_{i=1}^m r'_i x'_i$ for some $r_i, r'_i \in R$ and some $x_i, x'_i \in X$. In the notation of Note IV.2.B,

$$a + c = \sum_{i=1}^{\ell} (r_i + r'_i) x_i + \sum_{i=\ell+1}^n r_i x_i + \sum_{i=\ell+1}^m r'_i x'_i$$

and so

$$\begin{aligned} \bar{f}(a + c) &= \sum_{i=1}^{\ell} (r_i + r'_i) f(x_i) + \sum_{i=\ell+1}^n r_i f(x_i) + \sum_{i=\ell+1}^m r'_i f(x'_i) \\ &= \sum_{i=1}^{\ell} r_i f(x_i) + \sum_{i=1}^{\ell} r'_i f(x'_i) + \sum_{i=\ell+1}^n r_i f(x_i) + \sum_{i=\ell+1}^m r'_i f(x'_i) \\ &\quad \text{since } x_i = x'_i \text{ for } 1 \leq i \leq \ell \\ &= \sum_{i=1}^n r_i f(x_i) + \sum_{i=1}^m r'_i f(x'_i) = \bar{f}(a) + \bar{f}(c). \end{aligned}$$

()

Theorem IV.2.1 (continued 8)

Proof (continued). Also $\bar{f}(ra) = \bar{f}(r \sum_{i=1}^n r_i x_i) = \bar{f}(\sum_{i=1}^n r r_i x_i) = \sum_{i=1}^n r r_i f(x_i) = r \sum_{i=1}^n r_i f(x_i) = r \bar{f}(a)$. So \bar{f} is an R -module homomorphism by Definition IV.1.2.

Since X generates F (i.e., every element of A is a linear combination of elements of X by Note IV.2.A) then any R -module homomorphism mapping $F \rightarrow A$ is uniquely determined by its values on X . If $\bar{g} : F \rightarrow A$ is any R -module homomorphism such that $\bar{g}\iota = f$, then for all $x \in X$ we have $\bar{g}(x) = \bar{g}(\iota(x)) = f(x) = \bar{f}(x)$. Therefore $\bar{g} = \bar{f}$ and so \bar{f} is unique. By Note IV.1.D, the unitary R -modules form a concrete category. By the definition of “free object F on set X ” of a concrete category (Definition I.7.7), we see that F is a free object on set X where i is ι , A as a unitary R -module, and \bar{f} as the unique morphism $\bar{f} : F \rightarrow A$.

()

Theorem IV.2.1 (continued 9)

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

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

Proof (continued). (iv) \Rightarrow (iii). Let X be the nonempty set and $\iota : X \rightarrow F$ hypothesized to exist. Consider the direct sum $\sum_X R$ and let $Y = \{\theta - x \mid x \in X\}$ be the basis of the unitary R -module $\sum_X R$ given in the (iii) \Rightarrow (i) part of the proof above.

()

Theorem IV.2.1 (continued 10)

Proof (continued). We have established (iii) \Rightarrow (i) \Rightarrow (iv) so we have (replacing F with $\sum_X R$ in (iii) and replacing X with Y in (i)) that $\sum_X R$ is a free object on set Y in the category of unitary R -modules (with $Y \rightarrow \sum_X R$ by the inclusion map, as is done in the proof of (i) \Rightarrow (iv)). Since $|X| = |\{\theta_x \mid x \in X\}| = |Y|$, then by Theorem I.7.8 in [Section I.7. Categories: Products, Coproducts, and Free Objects](#), F and $\sum_X R$ are equivalent. As shown in the proof of Theorem I.7.8, equivalence is given between two objects F and F' as $\varphi : F \rightarrow F'$ and $\psi : F' \rightarrow F$ where $\psi \circ \varphi = 1_F$ and $\varphi \circ \psi = 1_{F'}$. Since the morphisms in the category of unitary R -modules are R -module homomorphisms, then φ and ψ are R -module homomorphisms. By Theorem 0.3.1, φ and ψ are bijections, therefore we have that φ and ψ are R -module isomorphisms. Therefore, $F \cong \sum_X R$, as claimed. \square

()

Corollary IV.2.2

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.

Proof. Let X be a set of generators of A (A itself is a set of generators, so such a set exists). Let F be the free R -module on set X . Then X is a basis of F by the convention given in Note IV.2.F. As shown in the (i) \Rightarrow (iv) of Theorem IV.2.1, we see that set X satisfies the conditions of part (iv) of Theorem IV.2.1. We take function $f : X \rightarrow A$ of part (iv) to be the inclusion map (not to be confused with functions $\iota : X \rightarrow F$). Then part (iv) implies the existence of unique R -module homomorphism $\bar{f} : F \rightarrow A$. We just need to show \bar{f} is a surjection. We also have by part (iv) that $\bar{f}\iota = f$. Since $\iota : X \rightarrow F$, $\bar{f} : F \rightarrow A$, and $X \subset A$ then $\text{Im}(\bar{f})$ includes $f(X) \subset A$ where $f(X) = X$ since $f : X \rightarrow A$ is just the inclusion mapping. That is, $X \subset \text{Im}(\bar{f}) \subset A$.

Corollary IV.2.2 (continued)

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.

Proof (continued). Since the homomorphic image of an R -module is an R -module (see Example IV.1.B), then $\text{Im}(\bar{f})$ is an R -module containing generating set X of A , and therefore $\text{Im}(\bar{f}) = A$. That is, arbitrary unitary module A over ring R is the homomorphic image of free R -module F , as claimed.

If A is finitely generated, then generating set X can be taken to be finite and hence free R -module F (which has X as a basis) is finitely generated, as claimed. \square

Lemma IV.2.3

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 .

Proof. With X as a maximal linearly independent subset of V , let W be the subspace of V spanned by set X . Since X is linearly independent and spans W , then X is a basis of W . ASSUME $W \neq V$. Then there is a nonzero vector $a \in V$ with $a \notin W$. Consider the set $X \cup \{a\}$. If $ra + r_1x_1 + r_2x_2 + \cdots + r_nx_n = 0$ where $r, r_i \in D$ and $x_i \in X$ for each i . If $r \neq 0$, then $a = -r^{-1}r_1x_1 = r^{-1}r_2x_2 - \cdots - r^{-1}r_nx_n \in W$. But this CONTRADICTS the choice of nonzero $a \in V \setminus W$. So we must have $r = 0$. Then $ra + r_1x_1 + r_2x_2 + \cdots + r_nx_n = r_1x_1 + r_2x_2 + \cdots + r_nx_n = 0$ and hence $r_i = 0$ for all i since X is a linearly independent set. But this implies that the set $X \cup \{a\}$ is linearly independent, CONTRADICTING the maximality of linearly independent set X . So the assumption that $W \neq V$ is false, and hence $V = W$ and X is a basis for V , as claimed. \square

Theorem IV.2.4

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 .

Proof. Let X be any linearly independent subset of V . Let \mathcal{S} be the set of all linearly independent subsets of V that contain X . Since $X \in \mathcal{S}$ then $\mathcal{S} \neq \emptyset$. Partially order \mathcal{S} by set theoretic inclusion; that is, $S_1 \leq S_2$ for $S_1 \subset S_2$. Let $\{C_i \mid i \in I\}$ be a chain in \mathcal{S} (that is, for any c_j, c_k with $j, k \in I$ we have either $c_j \leq c_k$ or $c_k \leq c_j$; see [Section 0.7. The Axiom of Choice, Order, and Zorn's Lemma](#) for more on this).

Define $C = \cup_{i \in I} C_i$. Let $x_1, x_2, \dots, x_n \in C$, $r_1, r_2, \dots, r_n \in D$, and suppose $r_1x_1 + r_2x_2 + \cdots + r_nx_n = 0$. Then for each $1 \leq i \leq n$ we have $x_i \in C_j$ for some $j \in I$. Say, WLOG, $x_i \in C_j$. Since all C_i for $i \in I$ are comparable, then there is some C_1, C_2, \dots, C_n , say C^* , such that $C_i \leq C^*$ or $C_i \subset C^*$ for each $1 \leq i \leq n$.

Theorem IV.2.4 (continued)

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 .

Proof (continued). Therefore $x_1, x_2, \dots, x_n \in C^*$ and since $C^* \in \mathcal{S}$ then C^* is a linearly independent subset of V , so $r_1x_1 + r_2x_2 + \dots + r_nx_n = 0$ implies $r_i = 0$ for $1 \leq i \leq n$. Therefore C is a linearly independent subset of V and $C \in \mathcal{S}$. Of course $C_i \leq C = \bigcup_{i \in I} C_i$ is an upper bound for chain $\{C_i \mid i \in I\}$. Since $\{C_i \mid i \in I\}$ is an arbitrary chain, then we can apply Zorn's Lemma to conclude that \mathcal{S} contains a maximal element B . Then B contains X and is a maximal linearly independent subset of V . That is, B contains X and is a basis of V by Lemma IV.2.3, as claimed. \square

Theorem IV.2.5

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 .

Proof. Similar to the proof of Theorem IV.2.4, let \mathcal{S} be the set of all linearly independent subsets of X and partially order \mathcal{S} by subset inclusion. \mathcal{S} contains singletons of X , so $\mathcal{S} \neq \emptyset$. As in the proof of Theorem IV.2.4, we have any chain $\{C_i \mid i \in I\}$ of elements of \mathcal{S} has $C = \bigcup_{i \in I} C_i$ as an upper bound so that we can apply Zorn's Lemma to \mathcal{S} to get a maximal element Y of \mathcal{S} . Every element of X is a linear combination of elements of Y , or else we could find $a \in X$ which is not in the span of Y . This then gives $Y \cup \{a\}$ as an element of \mathcal{S} where $Y \subsetneq Y \cup \{a\}$ so that Y is not maximal, contradicting the maximality of Y (this is the same argument as given in the proof of Lemma IV.2.3). Since X spans V and Y spans X , then Y spans V (a linear combination of linear combinations is itself a linear combination). Therefore Y is a linearly independent spanning set of V . That is, Y is a basis of V which is contained in X , as claimed. \square

Theorem IV.2.6

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 .

Proof. Let Y be a basis of F other than X . ASSUME that Y is finite. Since Y generates F and every element of Y is a linear combination of a finite number of elements of X (because X is a basis of F), then there is a finite subset $\{x_1, x_2, \dots, x_m\}$ of X (namely, the x_i 's in the linear combinations that give the elements of Y) which generates F (because Y is assumed to be a basis of F). Since X is infinite then there exists $x \in X \setminus \{x_1, x_2, \dots, x_m\}$. Then $x = r_1x_1 + r_2x_2 + \dots + r_mx_m$ for some $r_i \in R$ since $\{x_1, x_2, \dots, x_m\}$ generates F . Then $r_1x_1 + r_2x_1 + \dots + r_mx_m \in X$ and not all coefficients are 0, CONTRADICTING the fact that X is linearly independent. Hence the assumption that Y is finite is false and, therefore, Y is infinite.

Theorem IV.2.6 (continued 1)

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 .

Proof (continued). Let $K(Y)$ be the set of all finite subsets of Y . Define $f : X \rightarrow F(Y)$ as $x \mapsto \{y_1, y_2, \dots, y_n\}$ where $x = r_1y_1 + r_2y_2 + \dots + r_ny_n$ for nonzero $r_i \in R$. Since Y is a basis of F , then set $\{y_1, y_2, \dots, y_n\}$ is uniquely determined by x and f is well-defined. ASSUME $\text{Im}(f)$ is finite. Then $\bigcup_{S \in \text{Im}(f)} S$ is a finite subset of Y that generates set X . Since X is a basis for F , then this finite subset of Y generates F . But Y is a linearly independent set, so $\bigcup_{S \in \text{Im}(f)} S \subset Y$ is linearly independent and hence is a finite basis of F . But as shown above, a basis of F cannot be finite and so we have a CONTRADICTION. The assumption that $\text{Im}(f)$ is finite is false and hence we must have that $\text{Im}(f)$ is infinite.

Theorem IV.2.6 (continued 2)

Proof (continued). Let $T \in \text{Im}(f) \subset K(Y)$. Notice this means that T is a finite subset of basis Y . We'll show that $f^{-1}(T)$ is a finite subset of X . Now $T \subset Y$ generates some submodule F_T of F . By Theorem IV.1.5(iii), F_T consists of all possible linear combinations of elements of T . If $x \in f^{-1}(T)$ then x is a linear combination of the elements of T , and $x \in F_T$. That is, $f^{-1}(T) \subset F_T$. Since T is finite and each $y \in T$ is a linear combination of a finite number of elements of basis X , then there is a finite subset S of X such that F_T is contained in the submodule F_S generated by set $S \subset X$. So $x \in f^{-1}(T)$ implies $x \in F_S$ and (again by Theorem IV.1.5(iii)) x is a linear combination of elements of S . Since $S \subset X$ is a finite set, if $x \notin S$ then, as argued above when considering $x \in X \setminus \{x_1, x_2, \dots, x_m\}$ at the beginning of the proof, a contradiction the the linear independence of X results. Hence, we must have $x \in S$. Since x is an arbitrary element of $f^{-1}(T)$ then we have $f^{-1}(T) \subset S$ and, since S is finite, then $f^{-1}(T)$ is finite.

Theorem IV.2.6 (continued 4)

Proof (continued). Also, for any $x \in X \subset F$, x is some linear combination of elements of Y with nonzero coefficients (since Y is a basis of F), say $x = r_1''y_1'' + r_2''y_2'' + \dots + r_k''y_k''$ where $r_i'' \in R$ and $r_i'' \neq 0$ for $1 \leq i \leq k$. Let $T'' = \{y_1'', y_2'', \dots, y_k''\} \in K(Y)$ and then we have $x \in f^{-1}(T'')$. Therefore the sets $f^{-1}(T)$ for $T \in \text{Im}(f)$ partition X .

Define a map $X \rightarrow \text{Im}(f) \times \mathbb{N}$ as $x \mapsto g_T(x)$ where $x \in f^{-1}(T)$. Sw just showed that the $f^{-1}(T)$ s partition X , so the mapping $x \mapsto g_T(x)$ takes x , "associates" it with unique $f^{-1}(T)$ containing it, and then g_T takes this $f^{-1}(T)$ to $(T, x_k) \in \text{Im}(f) \times \mathbb{N}$ where the notation x_k is introduced above in the ordering of the finite set $f^{-1}(T)$. Now each $x \in X$ occurs in exactly one $f^{-1}(T)$ and each $x \in f^{-1}(T)$ is associated with exactly one x_k in the ordering of $f^{-1}(T)$. So the mapping $x \mapsto g_T(x)$ is well-defined and injective. Hence, there is an injection from X to $\text{Im}(f) \times \mathbb{N}$.

Theorem IV.2.6 (continued 3)

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 .

Proof (continued). For each $T \in \text{Im}(f)$, order the finite number of elements of $f^{-1}(T)$ as, say, x_1, x_2, \dots, x_n . Define $g_T : f^{-1}(T) \rightarrow \text{Im}(f) \times \mathbb{N}$ as $x_k \mapsto (T, k)$. Mapping g_T is an injection (since for $i \neq j$, $g_T(x_i) = (T, i) \neq (T, j) = g_T(x_j)$). For $T = \{y_1, y_2, \dots, y_n\} \in \text{Im}(f)$, we only have $x \in f^{-1}(T)$ if $x \in X$ and x is some linear combination of y_1, y_2, \dots, y_n with nonzero coefficients. For $T, T' \in \text{Im}(f)$, ASSUME $x \in f^{-1}(T) \cap f^{-1}(T')$. Then $x = r_1y_1 + r_2y_2 + \dots + r_ny_n = r'_1y'_1 + r'_2y'_2 + \dots + r'_my'_m$ where $T' = \{y'_1, y'_2, \dots, y'_m\}$, $r_1, r'_i \in R$, $r_i \neq 0$ for $1 \leq i \leq n$, and $r'_i \neq 0$ for $1 \leq i \leq m$. But then x is written in two different ways as a linear combination of elements of X with nonzero coefficients, a CONTRADICTION to Note IV.2.B. Therefore $f^{-1}(T) \cap f^{-1}(T') = \emptyset$.

Theorem IV.2.6 (continued 5)

Proof (continued). We now have by results from [Section 0.8. Cardinal Numbers](#):

$$\begin{aligned} |X| &\leq |\text{Im}(f) \times \mathbb{N}| \text{ by Definition 0.8.4, since } x \mapsto g_T(x) \text{ is an injection} \\ &= |\text{Im}(f)| |\mathbb{N}| \text{ by Definition 0.8.3 of } |A \times B| \\ &= |\text{Im}(f)| \aleph_0 \text{ since } \mathbb{N} \text{ is countable} \\ &= |\text{Im}(f)| \text{ by Theorem 0.8.11 with } \alpha = |\text{Im}(f)| \text{ and } \beta = \aleph_0 \\ &\leq |K(Y)| \text{ since } \text{Im}(f) \subset K(Y) \\ &= |Y| \text{ by Corollary 0.8.13.} \end{aligned}$$

Now X and Y are any infinite bases of F , then we can interchange X and Y to conclude $|Y| \leq |X|$. Then by the Schroeder-Bernstein Theorem (Theorem 0.8.6) we have $|X| = |Y|$, as claimed. \square

Theorem IV.2.7

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

Proof. Let X and Y be bases of V . If either X or Y is infinite, then $|X| = |Y|$ by Theorem IV.2.6. So we can assume WLOG that both X and Y are finite, say $X = \{x_1, x_2, \dots, x_n\}$ and $Y = \{y_1, y_2, \dots, y_m\}$. Since Y is a basis then $y_m \neq 0$, then $y_m = r_1x_1 + r_2x_2 + \dots + r_nx_n$ for some $r_i \in D$. Let r_k be the first nonzero r_i (under the ordering r_1, r_2, \dots, r_n ; notice that not all x_i may be required to write y_m as a linear combination of the elements of X). Then $x_k = r_k^{-1}y_m - r_k^{-1}r_{k+1}x_{k+1} - \dots - r_k^{-1}r_nx_n$. Therefore the set $x' = \{y_m, x_1, x_2, \dots, x_{k-1}, x_{k+1}, \dots, x_n\}$ spans V (since X spans V). We now iterate this process of replacing X_i 's with y_j 's. Since X' spans V , we can write $y_{m-1} = s_my_m + t_1x_1 + t_2x_2 + \dots + t_{k-1}x_{k-1} + t_{k+1}x_{k+1} + \dots + t_nx_n$ for some $s_m \in D$ and $x_i \in D$. Not all of the t_i 's are zero (otherwise $y_{m-1} - s_my_m = 0$, contradicting the linear independence of Y).

Theorem IV.2.7 (continued 1)

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

Proof (continued). If t_j is the first nonzero t_i (similar to the above argument) then x_j is a linear combination of y_{m-1}, y_m , and the s_i for $i \neq j, k$. Then, as above, the set $\{y_{m-1}, y_m\} \cup \{x_i \mid 1 \leq i \leq n, i \neq j, k\}$ spans V (since X' spans V). Again, this implies that y_{m-2} is a linear combination of y_{m-1}, y_m , and the x_i with $1 \leq i \leq n, i \neq j, k$. Using the first nonzero coefficient of an x_i in this linear combination allows us to eliminate some x_i where $i \neq j, k$, and replace it with y_{m-2} to create a spanning set of V . After k applications of this replacement process, we have a set containing this replacement process, we have a set containing $y_m, y_{m-1}, \dots, y_{m-k+1}$ and $n - k$ of the x_i which spans V .

Theorem IV.2.7 (continued 2)

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

Proof (continued). ASSUME $n < m$. Then after n steps we have that set $\{y_m, y_{m-1}, \dots, y_{m-n+1}\}$ spans V . But with $n < m$ we have $m - n > 0$ or $m - n \geq 1$ or $m - n + 1 \geq 2$. Since $y_1 \in V$, then implies that y_1 is a linear combination of y_2, y_3, \dots, y_m , CONTRADICTING the linear independence of set Y . So the assumption $n < m$ is false, and hence $n \geq m$. We can now interchange the roles of finite bases X and Y to conclude that $m \geq n$. Therefore, $n = m$ and $|X| = |Y|$, as claimed. \square

Theorem IV.2.13

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

Proof. Let Y be a basis of W (which exists by Theorem IV.2.4).

(i) By Theorem IV.2.4, there is a basis of X of V containing Y . Since $Y \subset X$ then $\dim_D(X) = |Y| \leq |X| = \dim_D(V)$, as claimed.

(ii) If $|Y| = |X|$ and \mathbb{N} is finite then since $Y \subset X$ we must have $Y = X$, whence (!) $W = V$, as claimed.

Theorem IV.2.13 (continued 1)

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

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

Proof (continued). (iii) Notice W is a submodule of V and so by Theorem IV.1.6, V/W is also a module over D (and since D is an integral domain, then V/W is a vector space). We will show that $U = \{x + W \mid x \in X \setminus Y\}$ is a basis of V/W . If $v \in V$ then, because X is a basis, $v = \sum_i r_i y_i + \sum_j s_j x_j$ where $r_i, s_j \in D$, $y_i \in Y$, and $x_j \in X \setminus Y$. Then

$$\begin{aligned} v + W &= \left(\sum_i r_i y_i + \sum_j s_j x_j \right) + W \\ &= \left(\sum_j s_j x_j \right) + W \text{ since } y_i \in Y \subset W \text{ so that } \sum_i r_i y_i \in W \end{aligned}$$

()

Theorem IV.2.13 (continued 2)

Proof (continued). ...

$$v + W = \sum_j s_j (x_j + W) \text{ by Theorem IV.1.6.}$$

Since $x_j \in X \setminus Y$ then $U = \{x + W \mid x \in X \setminus Y\}$ spans V/W . If $\sum_j r_j (x_j + W) = 0$ where $r_j \in D$ and $x_j \in X \setminus Y$, then $0 = \sum_j r_j (x_j + W) = \left(\sum_j r_j x_j \right) + W$ so that $\sum_j r_j x_j \in W$ (since W is the additive identity in V/W). Since Y is a basis for W , then $\sum_j r_j x_j = \sum_k s_k y_k$ where $s_k \in D$ and $y_k \in Y$. But $X = Y \cup (X \setminus Y)$ is linearly independent and we have two representations of the same element of V , a contradiction to Note IV.2.B, unless each $r_i = 0$ (and each $s_k = 0$). Therefore $U = \{x + W \mid x \in X \setminus Y\}$ and we have $|U| = |X \setminus Y|$. By Definition 0.8.3,

$\dim_D(V) = |X| = |Y| + |X \setminus Y| = |Y| + |U| = \dim_D(W) + \dim_D(V/W)$, as claimed. \square

()

Corollary IV.2.14

Corollary IV.2.14. If $f : V \rightarrow V'$ 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, $\dim_D(f) = \dim_D(\text{Ker}(f)) + \dim_D(\text{Im}(f))$.

Proof. By Example IV.1.B, $\text{Ker}(f)$ is a submodule of V (and, since D is a division ring, a subspace of V). Let $W = \text{Ker}(f)$ let Y be a basis of W (which exists by Theorem IV.2.4) and let X be a basis of V containing Y (which exists by Theorem IV.2.4). Then $X \cap \text{Ker}(f) = Y$ is a basis of $\text{Ker}(f)$, as claimed. By Theorem IV.1.7 (the "in particular" part), $\text{Im}(f) \cong V/W$. As shown in the proof of Theorem IV.2.13,

$$\begin{aligned} U &= \{x + W \mid x \in X \setminus Y\} = \{x + W \mid x \in X \setminus \text{Ker}(f)\} \\ &= \{x + W \mid x \in X, f(x) \neq 0\} \end{aligned}$$

is a basis of V/W .

()

Corollary IV.2.14 (continued)

Corollary IV.2.14. If $f : V \rightarrow V'$ 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, $\dim_D(f) = \dim_D(\text{Ker}(f)) + \dim_D(\text{Im}(f))$.

Proof (continued). Also by Theorem IV.1.7, there is a unique D -module isomorphism $\bar{f} : V/W \rightarrow \text{Im}(f)$ such that

$$\bar{f}(U) = \{\bar{f}(x + W) \mid x \in X, f(x) \neq 0\} = \{f(x) \mid f(x) \neq 0\} \subset \text{Im}(f) \subset V'.$$

Since \bar{f} is an isomorphism and U is a basis of V/W then $\bar{f}(U) = \{f(x) \mid f(x) \neq 0\}$ is a basis for $\text{Im}(f)$, as claimed.

Also, since $V/W \cong \text{Im}(f)$ then $\dim_D(V/W) = \dim_D(\text{Im}(f))$. By Theorem IV.2.13(iii), $\dim_D(V) = \dim_D(W) + \dim_D(V/W)$ or $\dim_D(V) = \dim_D(\text{Ker}(f)) + \dim_D(\text{Im}(f))$, as claimed. \square

()

Corollary IV.2.15

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

Proof. First, the intersection $V \cap W$ is a submodule (see Definition IV.1.4), and the sum $V + W$ is defined in Section IV.1. Modules, Homomorphisms, and Exact Sequences as the submodule generated by $V \cap W$. All of these are modules over integral domain D , and so are vector spaces. Let X be a finite basis of $V \cap W$, Y a finite basis of V that contains X , and Z be a (finite) basis of W that contains X (each of these bases exist by Theorem IV.2.4).

We now show that $Y \cup Z = X \cup (Y \setminus X) \cup (Z \setminus X)$ is a basis of $V + W$. By Theorem IV.1.5(iv), $V + W$ consists of all elements of the form $v + w$ where $v \in V$ and $w \in W$.

Corollary IV.2.15 (continued 1)

Proof (continued). Since Y is a basis for V then $v = r_1v_1 + r_2v_2 + \cdots + r_nv_n$ for some $r_i \in D$ and $v_i \in V$; since Z is a basis of W then $z = s_1w_1 + s_2w_2 + \cdots + s_mw_m$ for some $s_i \in D$ and $w_i \in W$. Now $Y \subset X \cup (Y \setminus X) \cup (Z \setminus X)$ and $Z \subset X \cup (Y \setminus X) \cup (Z \setminus X)$, so $v + w$ is in the span of $X \cup (Y \setminus X) \cup (Z \setminus X)$ where $x_i \in X$, $u_i \in Y \setminus X$, and $z_i \in Z \setminus X$, and suppose

$$(r_1x_1 + r_2x_2 + \cdots + r_jx_j) + (s_1y_1 + s_2 + \cdots + s_ky_k) + (t_1z_1 + t_2z_2 + \cdots + t_\ell z_\ell) = 0. \quad (*)$$

Then

$$u = (r_1x_1 + r_2x_2 + \cdots + r_jx_j) + (s_1y_1 + s_2 + \cdots + s_ky_k) = -(t_1z_1 + t_2z_2 + \cdots + t_\ell z_\ell).$$

But then $u = -(t_1z_1 + t_2z_2 + \cdots + t_\ell z_\ell) \in W$ since $\{z_1, z_2, \dots, z_\ell\} \subset Z$ and $u = (r_1x_1 + r_2x_2 + \cdots + r_jx_j) + (s_1y_1 + s_2 + \cdots + s_ky_k) \in V$ since $\{x_1, x_2, \dots, x_j, y_1, y_2, \dots, y_k\} \subset Y$ and hence vector u is in $V \cap W$.

Corollary IV.2.15 (continued 2)

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

Proof (continued). So u has a unique representation as a linear combination of elements of X (by Note IV.2.B). Also, since $Y = X \cup (Y \setminus X)$ is a basis of V then u can be written as a unique linear combination of elements of Y . But $X \subset Y$ so we must have $s_1 = s_2 = \cdots = s_k = 0$ above. Similarly, we must have $t_1 = t_2 = \cdots = t_\ell = 0$ above. So from (*), we have $r_1x_1 + r_2x_2 + \cdots + r_jx_j = 0$ and, since X is a linearly independent set, we must have $r_1 = r_2 = \cdots = r_j = 0$. Therefore $X \cup (Y \setminus X) \cup (Z \setminus X)$ is linearly independent. That is, it is a basis for $V + W$, as claimed.

Corollary IV.2.15 (continued 3)

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

Proof (continued). Therefore

$$\begin{aligned} \dim_D(V + W) &= |X \cup (Y \setminus X) \cup (Z \setminus X)| = |X| + |Y \setminus X| + |Z \setminus X| \\ &= |X| + (|Y| - |X|) + (|Z| - |X|) = |Y| + |Z| - |X| \\ &= \dim_D(V) + \dim_D(W) - \dim_D(V \cap W), \end{aligned}$$

or $\dim_D(V) + \dim_D(W) = \dim_D(V \cap W) + \dim_D(V + W)$, as claimed. \square

Theorem IV.2.16

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.

Proof. Let U be a basis of T over S , and let V be a basis of S over R . Consider the set $B = \{vu \mid v \in V, u \in U\}$. We'll show that B is a basis of T over R .

If $u \in T$ then $u = \sum_{i=1}^n s_i u_i$ for some $s_i \in S$ and some $u_i \in U$, since U is a basis of T as a vector space over S . Since S is a vector space over R with basis V then each s_i can be written in the form $s_i = \sum_{j=1}^{m_i} r_{ij} v_j$ for some $r_{ij} \in R$ and $v_j \in V$. Then

$$u = \sum_{i=1}^n s_i u_i = \sum_{i=1}^n \left(\sum_{j=1}^{m_i} r_{ij} v_j \right) u_i = \sum_{i=1}^n \sum_{j=1}^{m_i} r_{ij} (v_j u_i).$$

()

Theorem IV.2.16 (continued 2)

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.

Proof (continued). So from (*) we have that B is a linearly independent set over R . Therefore $B = \{vu \mid v \in V, u \in U\}$ is a basis of T over R .

Next, the elements vu of B are all distinct since U is a linearly independent set over S and $V \subset S$. So $\dim_R(T) = |B| = |U||V| = \dim_S(T)\dim_R(S)$, as claimed. If both $\dim_S(T)$ and $\dim_R(S)$ are finite then, of course, $\dim_R(T)$ is finite. If either $\dim_S(T)$ or $\dim_R(S)$ is infinite then, by Theorem 0/8/11, $\dim_R(T)$ is infinite, as claimed. \square

()

Theorem IV.2.16 (continued 1)

Proof (continued). So u is written as a linear combination of elements of $B = \{vu \mid v \in D, u \in U\}$ with coefficients from R . Since u is an arbitrary element of T , then B spans T as a vector space over R .

Now suppose

$$\sum_{i=1}^n \sum_{j=1}^m r_{ij} (v_j u_i) = 0 \text{ for } r_{ij} \in R, v_j \in V, \text{ and } u_i \in U. \quad (*)$$

For each i let $s_i = \sum_{j=1}^m r_{ij} v_j \in S$. Then

$$0 = \sum_{i=1}^n \sum_{j=1}^m r_{ij} (v_j u_i) = \sum_{i=1}^n \left(\sum_{j=1}^m r_{ij} v_j \right) u_i = \sum_{i=1}^n s_i u_i.$$

Since U is a linearly independent set over S , then $s_i = 0$ for $1 \leq i \leq n$. So $s_i = \sum_{j=1}^m r_{ij} v_j = 0$ and the linear independence of V over R implies that $r_{ij} = 0$ for $1 \leq i \leq n$ and $1 \leq j \leq m$.

()

Exercise IV.2.6(b)

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

Proof. ASSUME field K satisfies $\mathbb{R} \subsetneq K \subsetneq \mathbb{C}$. With $R = \mathbb{R}$, $S = F$, and $T = \mathbb{C}$ in Theorem V.2.6 (notice that \mathbb{R} and \mathbb{C} are both division of rings) we have $\dim_{\mathbb{R}}(\mathbb{C}) = \dim_F(\mathbb{C}) \dim_{\mathbb{R}}(F)$. So $2 = \dim_F(\mathbb{C}) \dim_{\mathbb{R}}(F)$ and either $\dim_F(\mathbb{C}) = 1$ or $\dim_{\mathbb{R}}(F) = 1$.

If $\dim_F(\mathbb{C}) = 1$, then by Theorem V.2.13(ii) with $D = W = F$ and $V = \mathbb{C}$ we have $\dim_F(F) = \dim_F(\mathbb{C}) = 1$ so that $F = \mathbb{C}$, a CONTRADICTION. Similarly, if $\dim_{\mathbb{R}}(F) = 1$ then, again, by Theorem V.2.13(ii) with $D = W = \mathbb{R}$ and $V = F$ we have $\dim_{\mathbb{R}}(\mathbb{R}) = \dim_{\mathbb{R}}(F) = 1$ so that $F = \mathbb{R}$, a CONTRADICTION. Therefore, no field F exists such that $\mathbb{R} \subsetneq K \subsetneq \mathbb{C}$, as claimed. \square

()

Lemma IV.2.10

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 $\pi : F \rightarrow F/IF$ the canonical epimorphism. Then F/IF is a free R/I -module with basis $\pi(X)$ and $|\pi(X)| = |X|$.

Proof. Recall that $IF = \{\sum_{i=1}^n r_i a_i \mid r_i \in I, a_i \in F, n \in \mathbb{N}\}$ by Theorem IV.1.5, and the action of R/I on F/IF is given by $(r + I)(a + IF) = ra + IF$ by Exercise IV.1.3(b). If $u + IF \in F/IF$ then $u = \sum_{j=1}^n r_j x_j$ for some $r_j \in R$ and $x_j \in X$ since $u \in F$ and X is a basis of F by hypothesis. Consequently,

$$\begin{aligned} u + IF &= \left(\sum_{j=1}^n r_j x_j \right) + IF & (*) \\ &= \sum_{j=1}^n (r_j x_j + IF) \text{ by the definition of addition} \\ &\text{in the additive quotient group} \end{aligned}$$

()

Lemma IV.2.10 (continued 1)

Proof (continued). ...

$$\begin{aligned} u + IF &= \sum_{j=1}^n (r_j + I)(x_j + IF) \text{ by Exercise IV.1.3(b)} \\ &= \sum_{j=1}^n (r_j + I)\pi(x_j) \text{ by the definition of } \pi. \end{aligned}$$

Since u is an arbitrary element of F/IF , then $\pi(X)$ generates F/IF as an R/I -module (so that the coefficients are cosets of I in R). On the other hand, if $\sum_{k=1}^m (r_k + I)\pi(x_k) = 0$ for some $r_k \in R$ and distinct x_1, x_2, \dots, x_m in X , then

$$\begin{aligned} 0 &= \sum_{k=1}^m (r_k + I)\pi(x_k) = \sum_{k=1}^m (r_k + I)(x_k + IF) \text{ by the definition of } \pi \\ &= \sum_{k=1}^m (r_k x_k + IF) \text{ by Exercise IV.1.3(b)} \end{aligned}$$

()

Lemma IV.2.10 (continued 2)

Proof (continued). ...

$$0 = \left(\sum_{k=1}^m r_k x_k \right) + IF \text{ by the definition of addition}$$

in the additive quotient group.

Since IF is the additive identity in F/IF then we have $\sum_{k=1}^m r_k x_k \in IF$. Then $\sum_{k=1}^m r_k x_k = \sum_j s_j u_j$ for some $s_j \in I$ and $u_j \in F$ by Theorem IV.1.5, as mentioned above. Since X is a basis for F and $u_j \in F$, then each u_j is a linear combination of elements of X with coefficients from R . Since $s_j \in I$ where I is an ideal of R , then the coefficients from R multiplied by s_j give another element of I (by the definition of "ideal," Definition III.2.1). So $\sum_{k=1}^m r_k x_k = \sum_j s_j u_j = \sum_{t=1}^d c_t y_t$ for some $c_t \in I \subset R$ and $y_t \in X$. Since the x_k and y_t are all from X , and X is a linearly independent set (over R) then ("after reindexing and inserting $0x_k$ and $0y_t$ if necessary," as Hungerford says on page 186) then we can take $m = d$, $x_k = y_k$, and $r_k = c_k \in I$ for every k .

()

Lemma IV.2.10 (continued 3)

Proof (continued). Hence $r_k + I = 0$ (since $r_k \in I$) in R/I for every k . Therefore in the equation $0 = \sum_{k=1}^m (r_k + I)\pi(x_k)$ we must have $r_k + I = 0$ (in R/I). Therefore $\pi(X)$ is a linearly independent set over R/I . We now have that $\pi(X)$ is a linearly independent generating set of F/IF over R/I . That is, $\pi(X)$ is a basis of F/IF over R/I . Hence F/IF is a free R/I -module by Theorem IV.2.1(i), as claimed.

Finally, for the cardinality claim. We know the canonical epimorphism restricted to basis X , $\pi : X \rightarrow \pi(X)$ is surjective. Let $x, x' \in X$ with $\pi(x) = \pi(x')$ in F/IF . Then $(1_R + I)\pi(x) = \pi(x) + I$ and $(1_R + I)\pi(x') = \pi(x') + I$. So $(1_R + I)\pi(x) - (1_R + I)\pi(x') = 0$ in F/IF . If $x \neq x'$ then the same argument as given above in (*) (where it is shown that $r_k \in I$) implies that $1_R \in I$. But then $I = R$, contradicting the hypothesis that $I \neq R$. Therefore $x = x'$ and $\pi : X \rightarrow \pi(X)$ is injective. That is, $\pi : X \rightarrow \pi(X)$ is a bijection and hence $|X| = |\pi(X)|$, as claimed. □

()

Proposition IV.2.11

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

Proof. Let $I = \text{Ker}(f)$. Then by the First Isomorphism Theorem (for rings; Corollary III.2.10) $S \cong R/I$. Let F be a free R -module with X as a basis. Also let Y be a basis of F and let $\pi : F \rightarrow F/IF$ be the canonical epimorphism. By Lemma IV.2.10, F/IF is a free R/I -module (and hence is a free S -module. . . well, up to isomorphism) with bases $\pi(X)$ and $\pi(Y)$, where $|X| = |\pi(X)|$ and $|Y| = |\pi(Y)|$. Since S has the invariant property then $|\pi(X)| = |\pi(Y)|$ and hence $|X| = |Y|$. That is, R has the invariant dimension property also, as claimed. \square

Corollary IV.2.12

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.

Proof. Suppose homomorphism $f : R \rightarrow S'$ where $S' = \text{Im}(f)$ is a division ring. Then S' is an epimorphic image of f . If V is a free S' -module, then V is a vector space. Then S' has the invariant dimension property by Theorem IV.2.7. Now by Proposition IV.2.11, R also has the invariant dimension property, as claimed.

If R is a commutative ring with identity, then R contains a maximal ideal M by Theorem III.2.18. Then by Theorem III.2.20, R/M is a field. Since a field is a commutative division ring, then we have that R has the invariant dimension property by the first part of the proof (we can take the homomorphism as the identity in this case, so that R is the homomorphic image of itself), as claimed. \square