# Ring Theory

Alec Zabel-Mena

**Text**

Herstein (1965). Topics in Algebra. Blaisdel Publishing Co.

June 3, 2021

# Chapter 1

# Groups.

## 1.1 Definitions and Examples

**Definition.** We call a nonemty set $V$ a **vector space** over a field $F$, if given a binary operation $+ : V \times V \to V$ called **vector addition** and an operation $\cdot : F \times V \to V$ called **scalar multiplication**, we have that $(V, +)$ forms an abelian group, and for all $v, w \in V$ and $\alpha, \beta \in F$:

(1) $\alpha(v + w) = \alpha v + \alpha w$.

(2) $(\alpha + \beta)v = \alpha v + \beta v$.

(3) $\alpha(\beta v) = (\alpha\beta)v$.

(4) $1v = v$, where 1 as the identity element of $F$ under its multiplication.

**Lemma 1.1.1.** *Let $V$ be a vector space over a field $F$. Then the operation $\cdot : F \times V \to V$ of scalar mutliplication as a group homomorphism of $V$ into $V$.*

*Proof.* Taking $\cdot : F \times V \to V$ by $(\alpha, v) \to \alpha v$, restrict $\cdot$ to $V$, i.e. consider $\cdot|_V : V \to V$ by $v \to \alpha v$ for $\alpha \in F$. By (1) of the scalar multiplication rules, we get that $\cdot|_V$ as a homomorphism; which makes $\cdot$ a homomorphism. ■

**Example 1.1.** (1) Let $F$ be a field and $F \subseteq K$ a field extension of $F$. Then $K$ as a vector space over $F$ with $+$ the usual addition of $K$ and $\cdot$ the multiplication of $K$ restricted to $F$ by the first part, i.e. the product $\cdot : v \to \alpha v$ with $\alpha \in F$.

(2) Let $F$ be a field and consider $F^n$ the set of ordered $n$-tuples of elements of $F$, for some $n \in \mathbb{Z}^+$. Take $+ : (v, w) \to v+w$ by $(v_1, \ldots, v_n)+(w_1, \ldots, w_n) = (v_1+w_1, \ldots, v_n+w_n)$, where $v = (v_1, \ldots, v_n), w = (w_1, \ldots, w_n) \in F^n$, and $\cdot : (\alpha, v) \to \alpha v$ by $\alpha(v_1, \ldots, n_n) = (\alpha v_1, \ldots, \alpha v_n)$. Then $F^n$ as a vector space over $F$.

(3) Let $F$ be any field and let $F[x]$ be the polynomial field over $F$. Take $+$ to be polynomial addition, and $\cdot$ the multiplication of a constant in $F$ by a polynomial in $F[x]$. Then $F[x]$ as a vector space over $F$.

(4) LEt $F[x]$ be the polynomial field over a field $F$ and consider the set $P_n = \{f \in Fx : \deg f < n\}$. Then $P_n$ as a subset of $F[x]$ forms a vector space over $F$ under the same operations $+$ and $\cdot$ (thas last example motivates the following definition).

**Definition.** LEt $V$ be a vector space over a field $F$. We say a subset $W \subseteq V$ as a **subspace** of $V$ if $W$ as also a vector space over $F$.

**Lemma 1.1.2.** *Let $V$ be a vector space over a field $F$, and let $W \subseteq V$ be a subspace of $V$. Then for all $w_1, w_2 \in W$ and $\alpha, \beta \in F$, $\alpha w_1 + \beta w_2 \in W$.*

*Proof.* Since $W$ as a vector space we have that $\alpha w_1, \beta w_2 \in W$; then by closure of vector addition, $\alpha w_1 + \beta w_2 \in W$. ■

**Definition.** Let $U$ and $V$ be vector spaces over a filed $F$. We call a mapping $T : U \to V$ a **homomorphism** of $U$ into $V$ if:

(1) $T(u_1 + u_2) = T(u_1) + T(u_2)$.

(2) $T(\alpha u_1) = \alpha T(u_1)$.

for all $u_1, u_2 \in U$ and $\alpha \in F$. If $T$ as $1-1$ from $U$ onto $V$, then we call $T$ an **isomorphism** and we say $U$ as **ismorphic** to $V$ and write $U \simeq V$. We define the **kernal** of $T$ to be $\ker T = \{u \in U : T(u) = 0\}$. We call the set of all homomorphism of $U$ into $V$ $\hom(U, V)$.

**Example 1.2.** Let $F$ be a field and consider the vector spaces $F^n$ and $P_n$ defined in examples (2) and (4). Then $P_n \simeq F^n$. Take the map $a_0 + a_1 x + \cdots + a_n x^{n-1} \to (a_0, \ldots, a_{n-1})$, which defines an isomorphism.

**Lemma 1.1.3.** *If $V$ as a vector space over a field $F$, then for all $\alpha \in F$ and $v \in V$:*

*(1)* $\alpha 0 = 0$.

*(2)* $0v = 0$.

*(3)* $(-\alpha)v = -(\alpha v)$.

*(4)* $\alpha v = 0$ *and* $v \neq 0$ *implies* $\alpha = 0$.

*Proof.* (1) $\alpha 0 = \alpha(0 + 0) = \alpha 0 + \alpha 0$, hence $\alpha 0 = 0$.

(2) $0v = (0 + 0)v = 0v + 0v$, hence $0v = 0$.

(3) He have $0 = 0v$, that as $0 = (\alpha + (-\alpha))v = \alpha v + (-\alpha)v$. Adding both sided by $-(\alpha v)$ we get the desired result.

(4) If $\alpha \neq 0$ and $v \neq 0$, then $0 = \alpha^{-1}0 = \alpha^{-1}(\alpha v) = 1v = v$ which makes $v = 0$, which cannot happen. So $\alpha = 0$.

■

**Lemma 1.1.4.** *Let $V$ be a vector space over a field $F$ and let $W \subseteq V$ be a subsapce of $V$. Then $V/W$ as a vector space over $F$ where for $v_1 + W, v_2 + W \in V/W$ and $\alpha \in F$ we have:*

*(1)* $(v_1 + W) + (v_2 + W) = (v_1 + v_2 + W)$.

*(2)* $(v_1 + W) = \alpha v_1 + W$.

*Proof.* Since $V$ as an abelian group, and $W$ a subgroup of $V$ under $+$, we get that $V/W$ as the quotient group of $V$ over $W$; which as abelian since $W$ as abelian.

Suppose now that for $v, v' \in V$ that $v+W = v'+W$, then for $\alpha \in F$ we have $\alpha(v+W) = \alpha(v'+W)$, and by hypotheses, we have $v-v' \in W$. Now since $W$ as a subspace, $\alpha(v-v') \in W$ as well, so $\alpha v + W = \alpha v' + W$, so the product as well defined.

Now consider $v, v' \in W$ and $\alpha, \beta \in F$. By our product we have that $\alpha(v + w + W) = \alpha(v+w)+W = (\alpha v+\alpha w)+W = (\alpha v+W)+(\alpha v'+W)$, $(\alpha+\beta)(v+W) = (\alpha+\beta)v+W = (\alpha v + \beta v) + W = \alpha(v + W) + \beta(v + W)$, $\alpha(\beta v + W) = \alpha\beta v + W = (\alpha\beta)v + W$, and finally, $1(v + w) = 1v + W = v + W$. Therefore $V/W$ as a vector space over $F$. ■

**Definition.** Let $V$ be a vector space over $F$ and let $W \subseteq V$ be a subsapce of $V$. We call the vector space formed by taking the quotient group of $V$ over $W$, $V/W$ the **quotient space** of $V$ over $W$.

**Theorem 1.1.5** (The First Isomorphism Theorem for Vector Spaces)**.** *If $T : U \to V$ as a hmomorphism of $U$ onto $V$, and $W = \ker T$, then $V \simeq U/W$. If $U$ as a vector space and $W \subseteq U$ as a subsapce of $U$, then there as a hoomomorphism of $U$ onto $U/W$.*

*Proof.* By the fundamental theorem of homomorphisms, we have that, as groups, $V \simeq U/W$. That there as a hmomorphism from $U$ onto $U/W$ follows immediately. ■

**Definition.** Let $V$ bhe a vector space over a field $F$ and let $\{U_i\}_{i=1}^n$ be a collection of subspaces of $V$. We call $V$ the **internal direct sum** of $\{U_i\}$ if every element of $V$ can be written uniquely as a vector sum of elements of each $U_i$ for $1 \leq i \leq n$; That as for $v \in V$, $v = u_1 + \cdots + u_n$ as unique where $u_i \in U_i$.

**Lemma 1.1.6.** *Let $\{V_i\}_{i=1}^n$ be a collection of vector spaces over a field $F$ and let $V = \prod_{i=1}^n V_i$ and define $+ : V \times V \to V$ by $(v_1, \ldots, v_n) + (v_1', \ldots, v_n') = (v_1 + v_1', \ldots, v_n + v_n')$ and define $\cdot : F \times V \to V$ by $\alpha(v_1, \ldots, v_n) = (\alpha v_1, \ldots, \alpha v_n)$. Then $V$ as a vector space over $F$.*

*Proof.* Since $V_i$ as a vector space for all $1 \leq i \leq n$, they are all abelian groups, hence $V$ as closed under $+$, and inherits associativity, as well a s commutativity. Now letting $0 = (0_1, \ldots, 0_n)$, where $0_i$ as the identity of $V_i$, we get for any $v \in V$ that $v + 0 = o + v = v$, so 0 as the identity. Likewise for any $v \in V$, $-v = (-v_1, \ldots, -v_n)$ serves as the inverse for $v$. So $(V, +)$ forms an abelian group.

Now by the axioms of scalar multiplication on each of the $V_i$, let $v = (v_1, \ldots, v_n), w = (w_1, \ldots, w_n) \in V$ and $\alpha, \beta \in F$. We get $\alpha(v + w) = \alpha(v_1 + w_1, \ldots v_n + w_n) = (\alpha(v_1 + w_1), \ldots, \alpha(v_n + w_n)) = (\alpha v_1 + \alpha w_1, \ldots, \alpha v_n + \alpha w_n) = (\alpha v_1, \ldots, \alpha v_n) + (\alpha w_1, \ldots, \alpha w_n) = \alpha v + \alpha w$. We also get $(\alpha + \beta)v = ((\alpha + \beta)v_1, \ldots, (\alpha + \beta)v_n) = (\alpha v_1 + \beta v_1, \ldots, \alpha v_n + \beta v_n) = (\alpha v_1, \ldots, \alpha v_n) + (\beta v_1, \ldots, \beta v_n) = \alpha v + \beta v$. Through similar calculation, we get that $\alpha(\beta v) = (\alpha\beta)v$ and $1v = v$; which makes $V$ into a vector space. ■

**Definition.** Let $\{V_i\}_{i=1}^n$ be a collection of vector spaces over a field $F$ and let $V = \prod_{i=1}^n V_i$ and define $+ : V \times V \to V$ by $(v_1, \ldots, v_n) + (v_1', \ldots, v_n') = (v_1 + v_1', \ldots, v_n + v_n')$ and define $\cdot : F \times V \to V$ by $\alpha(v_1, \ldots, v_n) = (\alpha v_1, \ldots, \alpha v_n)$. We call $V$, as a vector space over $F$ the **external direct sum** of $\{V_i\}$ and write $V = V_1 \oplus \cdots \oplus V_n$, or $V = \bigoplus_{i=1}^n V_i$.

**Theorem 1.1.7.** *Let $V$ be a vector space and let $\{U_i\}_{i=1}^n$ be a collection of subspaces of $V$. If $V$ is the internal direct sum of $\{U_i\}$ then $V$ is isomorphic to the external direct sum of $\{U_i\}$; that is: $V \simeq \bigoplus_{i=1}^n U_i$.*

*Proof.* Let $v \in V$. By hypothesis $v = u_1 + \cdots + u_n$ with $u_i \in U_i$ for $1 \leq i \leq n$, and it is a unique representation of $v$. Define then, the map $T : V \to \bigoplus_{i=1}^n U_i$ by the map $v = v = u_1 + \cdots + u_n \to (u_1, \ldots, u_n)$. Since $v$ has a unique representation by definition, $T$ is well defined; moreover it is $1-1$, as $(u_1, \ldots, u_n) = (w_1, \ldots w_n)$ implies $u_i = w_i$ for all $1 \leq i \leq n$, hence $u_1 + \cdots + u_u = w_1 + \cdots + w_n$, and since this sum is unique, they both represent a vector $v \in V$. That $T$ is onto follows directly from definition.

Finally, let $v, w \in V$, then $v = u_1 + \cdots + u_n$ and $w = w_1 + \cdots + w_n$. Hence $T(v+w) = T(u_1+w_1+\cdots+u_n+w_n) = (u_1+w_1, \ldots, u_n+w_n) = (u_1, \ldots, u_n)+(w_1, \ldots, w_n) = T(v)+T(w)$. Similarly, $T(\alpha v) = (v)$. ■

*Remark.* That $V$ is the internal direct sum of $\{U_i\}$ and that $V \simeq U_1 \oplus \cdots \oplus U_n$ by the above theorem permits us to write $V = U_1 \oplus \cdots \oplus U_n$, or $V = \bigoplus_{i=1}^n U_i$.

## 1.2 Linear Independence and Bases.

**Definition.** If $V$ is a vector space over a field $F$ and ive $v_1, \ldots, v_n \in V$, then we call any element $v \in V$ of the form $v = \alpha_1 v_1 + \cdots + \alpha_n v_n$ for $\alpha_1, \ldots, \alpha_n \in F$ a **linear comination** of $v_1, \ldots, v_n$ over $F$.

**Definition.** Let $V$ be a vector space. We call the set of all linear combinations of finite sets of elements of a nonempty subset $S \subseteq V$ the **linear span** of $S$; and we write $\operatorname{span} S$.

**Lemma 1.2.1.** *If $V$ is a vector space, and $S \subseteq V$ is nonempty, then* $\operatorname{span} S$ *is a subspace of $V$.*

*Proof.* Since $\operatorname{span} S$ is the set of all linear combinations of finite sets of elements of $S$, it is clear that $\operatorname{span} S \subseteq V$. Now let $v, w \in \operatorname{span} S$, then $v = \lambda_1 v_1 + \cdots + \lambda_n v_n$ and $w = \mu_1 w_1 + \cdots + \mu_m w_m$; where $\lambda_i, \mu_j \in F$ and $v_i, w_j \in S$ for $1 \leq i \leq n$ and $1 \leq j \leq m$. Now consider $\alpha, \beta \in F$, then $\alpha v + \beta w = \alpha(\lambda_1 v_1 + \cdots + \lambda_n v_n) + \beta(\mu_1 w_1 + \cdots + \mu_m w_m) = (\alpha\lambda_1)v_1 + \cdots + (\alpha\lambda_n)v_n + (\beta\mu_1)w_1 + \cdots + (\beta\mu_m)w_m$ which is a linear combination of the finite set $\{v_1, \ldots, v_n, w_1, \ldots, w_m\}$ of elements of $S$. Therefore $\alpha v + \beta w \in \operatorname{span} S$. ■

**Lemma 1.2.2.** *If $S, T \subseteq V$, then:*

*(1)* $S \subseteq T$ *implies* $\operatorname{span} S \subseteq \operatorname{span} T$.

*(2)* $\operatorname{span}(S \cup T) = \operatorname{span} S + \operatorname{span} T$.

*(3)* $\operatorname{span}(\operatorname{span} S) = \operatorname{span} S$.

*Proof.* (1) Let $v \in \operatorname{span} S$, then $v = \lambda_1 v_1 + \cdots + \lambda_n v_n$, with $v_1, \ldots, v_n \in S$. Since $S \subseteq T$, $v_1, \ldots, v_n \in T$, hence $v \in \operatorname{span} T$.

(2) Let $v \in \operatorname{span}(S \cup T)$, then $v = \lambda_1 v_1 + \cdots + \lambda_n v_n + \mu_1 w_1 + \cdots + \mu_m w_m = (\lambda_1 v_1 + \cdots + \lambda_n v_n) + (\mu_1 w_1 + \cdots + \mu_m w_m)$, where $v_i \in S$ and $w_j \in T$. Then $v \in \operatorname{span} S + \operatorname{span} T$.

Now for $v \in \operatorname{span} S + \operatorname{span} T$, $v = u + w$ with $u \in \operatorname{span} S$ and $w \in \operatorname{span} T$, hence $v$ is a linear combination of the finite set $\{u_1, \ldots, u_n, w_1, \ldots, w_n\}$ of elements of $S \cup T$, hence $v \in \operatorname{span}(S \cup T)$.

(3) Clearly $\operatorname{span} S \in \operatorname{span}(\operatorname{span} S)$. Suppose then that $v \in \operatorname{span}(\operatorname{span} S)$. Then $v =_1 v_1 + \cdots + \alpha_n v_n$ where $v_i = \beta_{i1} v_{i1} + \cdots + \beta_{im} v_{im}$ where $v_{ij} \in S$. Hence $v = ((\alpha_1 \beta_{11}) v_{11} + \cdots + (\alpha_1 \beta_{1m}) v_{1m}) + \cdots + (\alpha_n \beta_{n1}) v_{n1} + \cdots + (\alpha_n \beta_{nm}) v_{nm}$. Therefore $\operatorname{span}(\operatorname{span} S) \subseteq \operatorname{span} S$. ■

**Definition.** We call a vector space $V$ over a field $F$ **finite dimensional** over $F$ of there is a finite subset $S \subseteq V$ whose linear span is $V$; that is $\operatorname{span} S = V$.

**Example 1.3.** $F^n$ is finite dimensional. Let $S = \{(1, 0, \ldots, 0), (0, 1, \ldots, 0), \ldots, (0, 0, \ldots, 1)\}$. Then $\operatorname{span} S = F^n$.

**Definition.** Let $V$ be a vector space over a field $F$. We say that a set of $\{v_1, \ldots, v_n\}$ of elements of $V$ **linearly dependent** over $F$ if there exist $\lambda_1, \ldots, \lambda_n \in F$, not all 0 such that $\lambda_1 v_1 + \cdots + \lambda_n v_n = 0$. We call $\{v_1, \ldots v_n\}$ **linearly independent** over $F$ if it is not linearly dependent over $F$; that is $\lambda_1 v_1 + \cdots + \lambda_n v_n = 0$ implies $\lambda_1 = \cdots = \lambda_{n=0}$.

**Example 1.4.** (1) In $F^3$, the vectors $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$ are linearly independent, where as $(1, 1, 0)$, $3, 1, 3$, $(5, 3, 3)$ are linearly dependent.

(2) Consider the set $\mathbb{C}$ of complex numbets as a vector space over $\mathbb{R}$. The vectors $1, i$ are linearly independent over $\mathbb{R}$ since $i \notin \mathbb{R}$. However, $1, i$ is not linearly independent over $\mathbb{C}$, as $i^2 + 1 = 0$ by definition; where $\lambda_1 = i$ and $\lambda_2 = 1$.

**Lemma 1.2.3.** *If $v_1, \ldots, v_n \in V$ are linearly independent, then every element in* $\operatorname{span}\{v_1, \ldots, v_n\}$ *can be represented unqiuely as a linear combination of $v_1, \ldots, v_n$.*

*Proof.* Let $v \in \operatorname{span}\{v_1, \ldots, v_n\}$ such that $v = \lambda_1 v_1 + \cdots + \lambda_n v_n$ and $v = \mu_1 v_1 + \cdots + \mu_n v_n$. Then $\lambda_1 v_1 + \cdots + \lambda_n v_n = \mu_1 v_1 + \cdots + \mu_n v_n$, then $(\lambda_1 - \mu_1) v_1 + \cdots + (\lambda_n - \mu_n) v_n$. By linear independence, this implies that $\lambda_i - \mu_i = 0$, for all $1 \leq i \leq n$. Therefore $v$ is uniquely represented. ■

**Theorem 1.2.4.** *If $v_1, \ldots, v_n \in V$, then they are linearly independent, or $v_k$ is a linear combination of $v_1, \ldots, v_{k-1}$ for $1 \leq k \leq n$.*

*Proof.* If $v_1, \ldots, v_n$ are linearly independent, then we are done. Now suppose that they are linearly dependent, then $\lambda_1 v_1 + \cdots + \lambda_n v_n = 0$ for $\lambda_1, \ldots, \lambda_n$ not all 0. Let $k$ be the largest such integer for which $\lambda_k \neq 0$, and $\lambda_i = 0$ for all $k < i$. Then $\lambda_1 v_1 + \cdots + \lambda_n v_n = \lambda_1 v_1 + \cdots + \lambda_k v_k$ where $\lambda_1, \ldots, \lambda_k$ are not all 0 for $1 \leq i \leq k$. Then we have that $v_k = (\lambda_k^{-1} \lambda_1) v_1 + \cdots + (\lambda_k^{-1} \lambda_{k-1}) v_{k-1}$ which is a linear combination of $v_1, \ldots, v_{k-1}$. ■

**Corollary.** *If $v_1, \ldots, v_n \in V$ have $W$ as a linear span, and if $v_1, \ldots, v_k$ are linearly independent, then there is a linearly independent subset of $\{v_1, \ldots, v_n\}$ of the form $\{v_1, \ldots v_k, v_{i_1}, \ldots, v_{i_r}\}$ which span $W$.*

*Proof.* If $v_1, \dots, v_n$ are linearly independent, then we are done. If not, let $j$ be the smallest such integer for which $v_j$ is a linear combination of its predecessors. Since $v_1, \dots, v_k$ are linearly independent, we get $k < j$. then consider the set $S = \{v_1, \dots, v_n\} \backslash v_j = \{v_1, \dots, v_k, \dots, v_{j-1}, v_{j+1}, \dots, v_n\}$ which has $n-1$ elements. Clearly, span $S \subseteq W$.

Now let $w \in W$, then $w = \lambda_1 v_1 + \cdots + \lambda_n v_n$. Since $v_j$ is a linear combination of $v_1, \dots, v_{j-1}$, we get that $w = \lambda_1' v_1 + \cdots + \lambda_k' v_k + \cdots + \lambda_{j-1}' v_{j-1} + \lambda_{j+1} v_{j+1} + \cdots + \lambda_n v_n$ which makes $W \subseteq$ span $S$.

Now if we proceed by removing all voctors which are linear combinations of their predecessors, we get a set $\{v_1, \dots, v_k, v_{i_1}, \dots, v_{i_r}\}$ with span $S$; by the preceding argument, we get again that $W \subseteq$ span $S$. ■

**Corollary.** *If $V$ is a finite dimensional vector space, then there is a finite set of linearly independent vectors $\{v_1, \dots, v_n\}$ such that* span $\{v_1, \dots, v_n\} = V$.

*Proof.* By definition, since $V$ is finite dimensional, there is a finite set of vectors $\{u_1, \dots, u_m\}$ with linear span $V$. Then by the previous corollary, there is a subset $\{v_1, \dots, v_n\}$ of linearly independent vectors whose span is also $V$. ■

**Definition.** We call a subset $S$ of a vector space $V$ a **basis** if $S$ consists of linearly independent vectors, and span $S = V$.

What the above corollary states, is that if $V$ is a finite dimensional vector space, and $u_1, \dots, u_m$ (not necessarily independent), span $V$, then $u_1, \dots, u_m$ contain a basis of $V$.

**Example 1.5.** A basis need not be finite. Consider the polynomial field $F[x]$, the set $\{1, x, x^2, \dots, x_n, \dots\}$ forms a basis of $F[x]$. However, the set $\{1, x, x^2, \dots, x^n\}$ span the subspace $P_n$ of $F[x]$.

**Lemma 1.2.5.** *If $V$ is a finite dimensional vector space, then $V \simeq F^n$ for some $n \in \mathbb{Z}^+$.*

*Proof.* By lemma 1.2.3 and the above corollary, any $v \in V$ is the unique combination of basis elements $v_1, \dots, v_n$; that is $v = \lambda_1 v_1 + \cdots + \lambda_n v_n$. Now take the map $v \to (\lambda_1, \dots, \lambda_n)$ is well defined, $1-1$ by linear independence and onto. Hence $V \simeq F^n$. ■

*Remark.* In fact if $\{v_1, \dots, v_n\}$ is a basis for $V$, then $|\{v_1, \dots, v_n\}| = n$.

**Lemma 1.2.6.** *If $v_1, \dots, v_n \in V$ forms a basis, and $w_1, \dots, w_m \in V$ are linearly independent, then $m \leq n$. Moreover, the set $\{v_1, \dots, v_n\}$ is maximally linearly independent.*

*Proof.* For any arbitrary vector $v \in V$, $v$ is a linear combination of $v_1, \dots, v_n$ by lemma 1.2.3, hence $\{v_1, \dots, v, v\}$ is linearly dependent. This makes $\{v_1, \dots, v_n\}$ maximally independent.

Now $w_m \in V$ is a linear combination of $v_1, \dots, v_n$; moreover they span $V$ by theorem 1.2.4, therefore, by the previous corollary there is a subset $\{w_m, v_{i_1}, \dots, v_{i_k}\}$ with $k \leq n-1$ which is a basis of $V$.

Repeating by taking $w_{m-1}, w_m, \dots, v_{i_k}$; we get, eventually, a basis $\{w_{m-1}, w_m, \dots, v_{j_1}, dots, v_{j_s}\}$, with $s \leq n-1$. Repeating then of the vectors $w_2, \dots, w_{m-2}$, we get a basis $\{w_2, \dots, w_{m-1}, \dots, v_\alpha\}$. Since $w_1, \dots, w_m$ are linearly independent, $w_1$ is not a linear combiantion of the others, hence the basis contains some $v$. Now the basis above has $m-1$ $w_i$'s, at the cost of one $v \in V$, hence $m-1 \leq n-1$; thus $m \leq n$. ■

**Corollary.** *Any two bases have the same number of elements.*

*Proof.* Let $\{v_1, \ldots, v_n\}$ and $\{w_1, \ldots, w_m\}$ be bases with $n$ and $m$ elements respectively. Since they are both linearly independent, by above we get $m \leq n$ and $n \leq m$. Therefore $m = n$. ■

**Corollary.** *$F^n \simeq F^m$ if and only if $n = m$.*

*Proof.* $F^n$ has the basis $\{(1, 0, \ldots, 0)_n, \ldots, (0, 0, \ldots, 1)_n\}$ and $F^m$ has basis $\{(1, 0, \ldots, 0)_m, \ldots, (0, 0, \ldots, 1)_m$ and any isomorphism must map a basis to a basis. ■

**Corollary.** *If $V$ is finite dimensional over $F$, with $V \simeq F^n$ for some unque $n$, then any basis in $V$ has exactly $n$ elements.*

**Definition.** If $V$ is a finite dimensional vector space over a field $F$, with a basis $\{v_1, \ldots, v_n\}$ of $n$ elements, we call the $n$ **dimension** of $V$ over $F$ and write $\dim_F V = n$ or $\dim V = n$.

**Example 1.6.** (1) $\dim F^n = n$.

(2) $\dim_F P_n = n$, and $\dim F[x] = \infty$ (since $F[x]$) is infinite dimensional.

(3) $\dim_{\mathbb{R}} \mathbb{C} = 2$.

**Corollary.** *If $V$ and $U$ are finite dimensional vector spaces over a field $F$, with $\dim_F V = \dim_F U$, then $V \simeq U$.*

*Proof.* $V \simeq F^n$ and $F^n \simeq U$. By transitivity, we get $V \simeq U$. ■

**Lemma 1.2.7.** *If $V$ is a finite dimensional vector space over $F$ and of $u_1, \ldots, u_m \in V$ are linearly independent, then there exis $u_{m+1}, \ldots, u_{m+r} \in V$ such that $\{u_1, \ldots, u_m, u_{m+1}, u_{m+r}\}$ is a basis of $V$.*

*Proof.* By finite dimensionality, there is a basis $v_1, \ldots, v_n$ of $V$, which span $V$. Hene $\operatorname{span}\{u_1, \ldots, u_m, v_1, \ldots, v_n\} = V$, therefore by theorem 1.2.4 there is a subset $\{u_1, \ldots, u_m, v_{i_1}, \ldots, v_{i_r}\}$ which is a basis of $V$. Now just map $v_{i_j} \to u_{m+j}$ for each $1 \leq j \leq r$. ■

*Remark.* This gives us a method for constructing bases of vector spaces.

**Lemma 1.2.8.** *If $V$ is finite dimensional, and if $W$ is a subspace of $V$, then $W$ is also finite dimensional. Moreoverm $\dim W \leq \dim V$ and $\dim V/W = \dim V - \dim W$.*

*Proof.* If $\dim V = n$, then any set of $n+1$ vectors in $V$ is linearly dependent, by maximality, hence so is any set of $n + 1$ vectors in $W$. Then there exists a maximal set of linearly independent elements in $W$, $w_1, \ldots, w_m$, with $m \leq n$. If $w \in W$, then $w_1, \ldots, w_m, w$ are linearly dependent with $\lambda_1 w_1 + \cdots + \lambda_m w_m + \lambda w = 0$. Now $\lambda \neq 0$, for that would imply $w_1, \ldots, w_n, w$ linearly independent. Hence $w = \mu_1 w_1 + \cdots + \mu_m w_m$ where $\mu_i = \lambda^{-1}\lambda_i$. Thus we get $w \in \operatorname{span}\{w_1, \ldots, w_m\}$, i.e. $W = \operatorname{span}\{w_1, \ldots, w_m\}$, thus $w_1, \ldots w_m$ form a basis of $W$. Therefore $m = \dim W \leq \dim V = n$.

Now take $V \to V/W$ by $v_1, \ldots, v_r \to v_1', \ldots, v_r'$. By lemma 1.2.7, if $\{w_1, \ldots, w_m\}$ form a basis of $W$, then there exist $v_{m+1}, \ldots, v_{m+r}$ such that $\{w_1, \ldots, wm, v_{m+1}, v_{m+r}\}$ form a basis for $V$. That is, for any $v \in V$, $v = \lambda_1 w_1 + \cdots + \lambda_m w_m + \mu_1 v_1 + \cdots + \mu_r v_r$. Then we get that $v' = \mu_1 v_1' + \cdots + \mu_r v_r'$, hence $\operatorname{span}\{v_1', \ldots, v_r'\} = V/W$. Now if $\gamma_1 v_1' + \cdots + \gamma_r v_r' = 0$, then $\gamma_1 v_1' + \cdots + \gamma_r v_r \in W$, making $\gamma_1 v_1' + \cdots + \gamma_r v_r = \lambda_1 w_1 + \cdots + \lambda_m v_m$. By linear independence, $\gamma_i, \lambda_j = 0$ for all $1 \leq i \leq r$ and $1 \leq j \leq m$. This $V/M$ has a basis of $r = \dim V - \dim W$ elements. Therefore $\dim V/W = \dim v - \dim W$. ■

**Corollary.** *If $U$ and $W$ are finite dimensional subspaces of a vector space $V$, then $U + W$ is finite dimensional, and* $\dim(A + B) = \dim A + \dim B - \dim_A \cap B$.

*Proof.* We have $U + W/W \simeq U/U \cap W$. Hence we get that $\dim U + W/W = \dim(U + W) - \dim W = \dim U/U \cap W = \dim U - \dim U \cap W$. Then $\dim(U + W) = \dim W = \dim U - m_9 U \cap W$. ■

## 1.3 Dual Spaces.

**Lemma 1.3.1.** *Let $V$ and $W$ be vector spaces over a field $F$. Then* $\hom(V, W)$ *is a vector space over $F$.*

*Proof.* First, let $T, L \in \hom(V, W)$, and $\alpha, \beta \in F$. Then $T + L(\alpha v + \beta u) = \alpha T(v) + \beta T(u) + \alpha L(v) + \beta L(u) = \alpha(T + L) + \beta(T + L)$, so $T + L \in \hom(V, W)$. Since $+$ is just function addition, it is associative. Likewise, the zero map $0 : V \to W$ by $v \to 0$ and the map $-T : V \to W$ by $v \to -v$ define the identity of $\hom(V, W)$ and the inverse of $T$ respectively. This makes $(\hom(V, W), +)$ into a group. Now by the properties of homomorphisms, we also see that $\alpha(T + L) = \alpha T + \alpha L$, $(\alpha + \beta)T = \alpha T + \beta T$, $\alpha(\beta T) = (\alpha\beta)T$ and $T(1v) = 1T(v)$. This makes $\hom(V, W)$ a vector space. ■

**Theorem 1.3.2.** *If $V$ and $W$ are vector spaces with* $\dim V = m$ *and* $\dim W = n$, *then* $\dim \hom(V, W) = mn$.

*Proof.* Let $\{v_1, \ldots, v_m\}$ and $\{w_1, \ldots, w_n\}$ be bases for $V$ and $W$, respectively. Then for any $v \in V$, $v = \lambda_1 v_1 + \cdots + \lambda_m v_m$ for unique $\lambda_1, \ldots, \lambda_n \in F$. Now let $T_{ij} \in \hom(V, W)$ be defined such that $T_{ij}(v_i) = 0$ for $i \neq j$ and $T_{ij}(v) = \lambda_i w_j$; for $1 \leq i \leq m$ and $1 \leq j \leq n$. We see there are $mn$ possible such $T_{ij}$. Now let $S \in \hom(V, W)$, then $S(v_i) \in W$, hence $S = \mu_{11} w_1 + \cdots + \mu_n w_{1n}$ for unique $\mu_{11}, \ldots, \mu_{1n} \in F$. Then $S(v_i) = \mu_{i1} w_1 + \cdots + \mu_{in} w_n$ for unique $\mu_{i1}, \ldots, \mu_{in} \in F$. Now let $S_0 = \mu_{11} T_{11} + \cdots + \mu_{1n} T_{1n} + \cdots + \mu_{m1} T_{m1} + \cdots + \mu_{mn} T_{mn}$. Then $S_0(v_k) = (\mu_{11} T_{11} + \cdots + \mu_{1n} T_{1n} + \cdots + \mu_{m1} T_{m1} + \cdots + \mu_{mn} T_{mn})(v_k) = \mu_{11} T_{11}(v_k) + \cdots + \mu_{1n} T_{1n}(v_k) + \cdots + \mu_{m1} T_{m1}(v_k) + \cdots + \mu_{mn} T_{mn}(v_k)$. Since $T_{ij}(v_k) = 0$ for $i \neq k$ we get $S_0(v_k) = \alpha_{k1} w_1 + \cdots + \alpha_{kn} wn$. So $S_0(vk) = S(v_k)$ for the basis $\{v_1, \ldots, v_m\}$ of $V$; this makes $S_0 = S$.

Now since $S = S_0$ is arbitrary, and subsequentially a linear combination of the $T_{ij}$, we get that span $\{T_{11}, \ldots, T_{1n}, \ldots, T_{m1}, \ldots, T_{mn}\} = \hom(V, W)$. Now suppose for $\beta_{11}, \ldots, \beta_{1n}, \ldots, \beta_{m1}, \ldots, \beta_{mn} \in F$ that $\beta_{11} T_{11} + \cdots + \beta_{1n} T_{1n} + \cdots + \beta_{m1} T_{m1} + \cdots + \beta_{mn} T_{mn} = 0$. Then we get that $(\beta_{11} T_{11} + \cdots + \beta_{1n} T_{1n} + \cdots + \beta_{m1} T_{m1} + \cdots + \beta_{mn} T_{mn})(v_k) = \beta_{k_1} w_1 + \cdots + \beta_{kn} w_n = 0$. Since $\{w_1, \ldots, w_n\}$ is a basis of $W$, this makes $\beta_{kj} = 0$ for all $1 \leq n$. Thus $\{T_{11}, \ldots, T_{1n}, \ldots, T_{m1}, \ldots, T_{mn}$ linearly independent, and hence a basis of $\hom(V, W)$. Therefore, $\dim \hom(V, W) = mn$. ■

**Corollary.** $\dim \hom(V, V) = m^2$.

**Corollary.** $\dim \hom(V, F) = m$.

**Definition.** Let $V$ be a vector space over a field $F$. We call the vector space $\hom(V, F)$ the **dual space** of $V$ and denote it $\operatorname{dual} V$. We call elements of $\operatorname{dual} V$ **linear functionals** on $V$ into $F$.

If $V$ is an infinite dimensional vector space, the dual $V$ is very big and of no interest. In these cases, we use properties of other possible structures of dual $V$ to find a restricted subspace. If $V$ is finite dimensional, then dual $V$ is finite and always defined.

**Lemma 1.3.3.** *If $V$ is a finite dimensional vector space, and $v \neq 0 \in V$, then there is a linear functional $\hat{v} \in$ dual $V$ such that $\hat{v}(v) \neq 0$.*

*Proof.* Let $\{v_1, \ldots, v_n\}$ be a bases of $V$ and let $\hat{v}_i \in$ dual $V$ be defined by $\hat{v}_i(v_j) = 0$ whenerver $i \neq j$ and $\hat{v}_i(v_j) = 1$ otherwise. Then if $v = \lambda_1 v_1 + \cdots + \lambda_n v_n$, $\hat{v}_i(v) = \lambda_i$. Then $\{\hat{v}_i, \ldots, \hat{v}_n\}$ forms a basis of dual $V$. Now if $v \neq 0 \in V$. by lemma 1.2.7, we get a basis $v_1 = v, v_2, \ldots, v_n$. Thence there is a linear functional $\hat{v}_1(v_1) = \hat{v}_1(v) = 1$. ■

**Definition.** Let $V$ be a finite dimensional vector space with basis $\{v_1, \ldots, v_n\}$. We define the **dual basis** of $\{v_1, \ldots, v_n\}$ to be a basis of linear functionals $\{\hat{v}_1, \ldots, \hat{v}_n\}$ of dual $V$ such that $\hat{v}_i(v_j) = 0$ wheberver $i \neq j$ and $\hat{v}_i(v_i) = 1$ otherwise.

**Lemma 1.3.4.** *If $V$ is a finite dimensional vector space, and $T \in$ dual $V$ such that $T(v)$ is fixed, then the map $\psi : v \to T_v$, where $T_v(T) = T(v)$ defines an isomorphism of $V$ onto* dual(dual $V$).

*Proof.* Let $v_0 \in V$. Let $T \in$ dual $V$ be a linear functional such that $T(v_0)$ is fixed. Then $T(v_0)$ defines a linear functional of dual $V$ into $F$. Let $T_{v_0} :$ dual $V \to F$ be defined by $T_{v_0}(T) = T(v_0)$, for any $T \in$ dual $V$. Notice that for $T, L \in$ dual $V$ and $\alpha, \beta \in F$, we have $T_{v0}(\alpha T + \beta L) = \alpha T(v_0) + \beta L(v_0) = \alpha T_{v0}(T) + \beta T_{v0}(L)$, which makes $T_{v0} \in$ dual(dual $V$).

Now given any $v \in V$, we can associate it with a $T_v \in$ dual(dual $V$). Now define $\psi : V \to$ dual(dual $V$) by $\psi : v \to T_v$. Then for $v, w \in V$ and $\alpha, \beta \in F$ we have $T_{\alpha v + \beta w}(T) = \alpha T(v) + \beta T(w) = \alpha T_v(T) + \beta T_w(T)$, so $\psi$ is a homomorphism of $V$ onto dual(dual $V$); $\psi$ is onto by definition.

Now let $v \in \ker \psi$. So $\psi(v) = 0$; that means $t_v(T) = T(v) = 0$ for all $T \in$ dual $V$. However, by lemma 1.3.3, there must be a $T \in$ dual $V$ for which $T(v) \neq 0$ when $v \neq 0$. Therefore, if $v \in \ker T$, it must be that $v = 0$, that is $\ker T = (0)$. Thus $\psi$ is $1 - 1$, which makes it an isomorphism. ■

**Definition.** Let $W$ be a subspace of a vector space $V$. We denote the **annihilator** of $W$ to be $A(W) = \{T \in$ dual $V : T(v) = 0\}$.

Let $\tilde{T} \in$ dual $W$ such that $\tilde{T}(w) = T(w)$ for any $w \in W$; where $T \in$ dual $V$. Now define the map $\psi :$ dual $V \to$ dual $W$ by $\psi : T \to \tilde{T}$. Then we see that $A(W) = \ker \psi$, which makes it a subspace.

**Theorem 1.3.5** (The Second Homomorphism Theorem for Vector Spaces)**.** *If $V$ is a finite dimensional vector space, and $W \subseteq V$ is a subspace of $V$, then* dual $W \simeq$ dual $V/A(W)$*, and* $\dim A(W) = \dim V - \dim W$.

*Proof.* Consider again the map $\psi :$ dual $V \to$ dual $W$ by $T \to \tilde{T}$, where $\tilde{T}(w) = T(w)$ for all $w \in W$; and recalling above that $A(W) = \ker T$.

Let $h \in$ dual $W$. By lemma 1.2.7, if $\{w_1, \ldots, w_m\}$ is a basis of $W$, then there is a basis $\{w_1, \ldots, w_m, v_1, \ldots, v_r\}$; hence $\dim V = r + m$. Let $W_1$ be a subspace of $V$ such that

$Span\{v_1, \ldots, v_r\} = W_1$. Then $V = W \oplus W_1$. Now if $h \in \operatorname{dual} W$, let $f \in \operatorname{dual} V$ be defined by $f(v) = w$ where $v = w + w_1 \in W \oplus W_1$. By definition, we have that $f \in \operatorname{dual} V$ and $f = h$. So $\psi(f) = h$ making $\psi$ onto. Since $A(W) = \ker \psi$, by the first homomorphism theorem for vector spaces, we get $\operatorname{dual} W \simeq \operatorname{dual} V/A(W)$.

Moreover, we get $\dim \operatorname{dual} W = \dim \operatorname{dual} V/A(W) = \dim \operatorname{dual} V - \dim A(W)$, and since $\dim \operatorname{dual} V = \dim V$ and $\dim \operatorname{dual} W = \dim W$; we get $\dim A(W) = \dim V - \dim W$. ■

**Corollary.** $A(A(W)) = W$.

*Proof.* Notice that $A(A(W)) \subseteq \operatorname{dual}(\operatorname{dual} V)$. Clearly, $W \subseteq A(A(W))$, for if $\psi(w) = T_w$ by $T_w(f) = f(w)$ and $T_w = 0$ for all $f \in A(W)$. Now by above we get $\dim A(A(W)) = \dim \operatorname{dual} V - \dim A(W) = \dim V - (\dim V - \dim W) = \dim W$. This makes $W \simeq A(A(W))$; and since $W \subseteq A(A(W))$, we get $W = A(A(W))$. ■

**Theorem 1.3.6.** *The system of homogeneous linear equations:*

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &= 0 \\ &\vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n &= 0 \end{aligned} \tag{1.1}$$

*where $a_{ij} \in F$ is of rank $r$, then there are $n - r$ linearly independent solutions in $F^n$.*

*Proof.* Consider the system described by equation 1.1, with $a_{ij} \in F$ for $1 \leq i \leq m$ and $1 \leq j \leq n$. Let $U$ be a subspace of $m$ vectors generated by $\{(a_{11}, \ldots, a_{1n}), \ldots, (a_{m1}, \ldots, a_{mn})\}$. Consider the basis $\{(1, 0, \ldots, 0), \ldots, (0, 0, \ldots, 1)\}$ of $F^n$ and let $\{\hat{v}_1, \ldots, \hat{v}_n\}$ be its dual basis. Then $T \in \operatorname{dual} F^n$ has the form $T = x_1\hat{v}_1 + \cdots + x_n\hat{v}_n$, with $x_i \in F$. for $1 \leq i \leq n$.

Now for $(a_{11}, \ldots, a_{1n}) \in U$, $T(a_{11}, \ldots, a_{1n}) = (x_1\hat{v}_1 + \cdots + x_n\hat{v}_n)(a_{11}, \ldots, a_{1n}) = a_{11}x_1 + \cdots + a_{1n}x_n$, since $\hat{v}_i(v_j) = 0$ for $i \neq j$. Conversely, every solution $(x_1, \ldots, x_n)$ gives an element of the form $x_1\hat{v}_1 + \cdots + x_n\hat{v}_n$ in $A(U)$. Therefore, the number of linearly independent solutions of equation 1.1 is $\dim A(U) = \dim V - \dim U = n - r$. ■

**Corollary.** *If $n > m$, then there is a solution $(x_1, \ldots, x_n)$ where not all $x_i$ is 0.*

## 1.4 Inner Product Spaces.