Ring Theory

Alec Zabel-Mena

<u>Text</u>

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

May 25, 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 $(v_1, \dots, v_n) + (w_1, \dots, w_n) = (v_1 + w_1, \dots, v_n + w_n)$, where $v = (v_1, \dots, v_n), w = (w_1, \dots, w_n) \in F^n$, and $\cdot : (\alpha, v) \to \alpha v$ by $\alpha(v_1, \dots, n_n) = (\alpha v_1, \dots, \alpha v_n)$. 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 $a_0 + a_1x + \cdots + a_nx^{n-1} \to (a_0, \ldots, a_{n-1})$, 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 $v_1, \ldots, v_n$.