

ME 550. FOUNDATIONS OF ENGINEERING SYSTEMS ANALYSIS

Chapter 2: Algebraic Structure of Vector Spaces

Let S be a nonempty set. An m -ary operation ($m \in \mathbf{N}$), $\otimes(\bullet, \bullet, \dots, \bullet)$ is a function mapping $S^m \equiv \underbrace{S \times S \times \dots \times S}_{m \text{ times}}$

into S . That is, $\otimes: S^m \rightarrow S$. Most commonly encountered operations are binary, i.e., $m = 2$ where $\otimes: S \times S \rightarrow S$. In this section, we denote the algebra of the binary operation \otimes as $\langle S; \otimes \rangle$ which we call as a binary algebra in the sequel.

Definition 2-1: An element $e_l \in S$ is said to be a left identity of the binary algebra $\langle S; \otimes \rangle$ if $e_l \otimes \alpha = \alpha \forall \alpha \in S$. Similarly, an element $e_r \in S$ is said to be a right identity of the binary algebra $\langle S; \otimes \rangle$ if $\alpha \otimes e_r = \alpha \forall \alpha \in S$. Finally, an element $e \in S$ is said to be an identity of the binary algebra $\langle S; \otimes \rangle$ if $\alpha \otimes e = e \otimes \alpha = \alpha \forall \alpha \in S$.

Definition 2-2: An element $0_l \in S$ is said to be a left zero of the binary algebra $\langle S; \otimes \rangle$ if $0_l \otimes \alpha = 0_l \forall \alpha \in S$. Similarly, an element $0_r \in S$ is said to be a right zero of the binary algebra $\langle S; \otimes \rangle$ if $\alpha \otimes 0_r = 0_r \forall \alpha \in S$. Finally, an element $0 \in S$ is said to be a zero of the binary algebra $\langle S; \otimes \rangle$ if $\alpha \otimes 0 = 0 \otimes \alpha = 0 \forall \alpha \in S$.

Semigroups, Monoids, and Groups

Definition 2-3: A binary algebra $\langle S; \otimes \rangle$ is called a semigroup if the associativity property is satisfied. That is, $\alpha \otimes (\beta \otimes \gamma) = (\alpha \otimes \beta) \otimes \gamma \forall \alpha, \beta, \gamma \in S$.

Definition 2-4: A semigroup with an identity element is called a monoid. That is, a monoid is a binary algebra which satisfies the associative property and has an identity element.

Definition 2-5: A monoid $\langle S; \otimes \rangle$ is called commutative if the following additional property: $\alpha \otimes \beta = \beta \otimes \alpha \forall \alpha, \beta \in S$ is satisfied.

Example 2-1: Let Σ be a nonempty finite set of letters called an alphabet. Let Σ^* be the set of all finite-length strings, including the empty string denoted as ε , over the alphabet Σ . We form a binary algebra $\langle \Sigma^*; \bullet \rangle$ where \bullet denotes the string concatenation operator defined as:

$$s_1 s_2 \equiv s_1 \bullet s_2 \text{ for any } s_1, s_2 \in \Sigma^*. \text{ Verify that } \langle \Sigma^*; \bullet \rangle \text{ is a monoid in this example with } \varepsilon \text{ as the identity.}$$

HW#2-1: Let $S = \{1, \alpha, \beta, \gamma, \delta\}$ and the operator \otimes be defined as follows:

\otimes	1	α	β	γ	δ
1	1	α	β	γ	δ
α	α	α	β	δ	δ
β	β	β	δ	α	α
γ	γ	δ	α	β	β
δ	δ	δ	α	β	β

Verify that $\langle S; \otimes \rangle$ is a semigroup. Is $\langle S; \otimes \rangle$ commutative?

Definition 2-6: Let $\langle S; \otimes \rangle$ be a monoid with identity e . Then, an element $\alpha \in S$ is called left invertible if $\exists \alpha_l^{-1} \in S$ such that $\alpha_l^{-1} \otimes \alpha = e$. Similarly, an element $\alpha \in S$ is called right invertible if $\exists \alpha_r^{-1} \in S$ such that $\alpha \otimes \alpha_r^{-1} = e$. An element $\alpha \in S$ is called invertible if $\exists \alpha^{-1} \in S$ such that $\alpha^{-1} \otimes \alpha = \alpha \otimes \alpha^{-1} = e$.

Definition 2-7: A monoid whose every element is invertible is called a group. That is, a binary algebra $\langle S; \otimes \rangle$ is called a group if the following properties are satisfied:

- $\alpha \otimes \beta \in S \forall \alpha, \beta \in S$ Closure property $\otimes : S \times S \rightarrow S$
- $\alpha \otimes (\beta \otimes \gamma) = (\alpha \otimes \beta) \otimes \gamma \forall \alpha, \beta, \gamma \in S$ Associative property
- $\exists e \in S$ such that $\alpha \otimes e = e \otimes \alpha = \alpha \forall \alpha \in S$ Existence of an identity
- $\forall \alpha \exists \alpha^{-1} \in S$ such that $\alpha^{-1} \otimes \alpha = \alpha \otimes \alpha^{-1} = e$ Invertibility property

Definition 2-8: A group $\langle S; \otimes \rangle$ is called commutative (also called Abelian) if the following additional property: $\alpha \otimes \beta = \beta \otimes \alpha \forall \alpha, \beta \in S$ is satisfied. It is customary to denote the binary operator as $+$ for commutative groups. That is, $\langle S; + \rangle$ indicates an Abelian group. Its identity element is often denoted as 0 and the inverse of an element α is often denoted as α^{-1} .

Example 2-2: Let $S = \mathfrak{R} = (-\infty, \infty)$ and let $+$ be the ordinary addition operator. Then, $\langle S; + \rangle$ is an Abelian group and its identity element is 0 .

Example 2-3: Let $S = \mathfrak{R} - \{0\} = (-\infty, 0) \cup (0, \infty)$ and \cdot be the operation of ordinary multiplication. Then, $\langle S; \cdot \rangle$ is an Abelian group and its identity element is 1 .

Example 2-4: Let S be the set of all $n \times n$ invertible matrices with real entries. Let \otimes denote the operation of matrix multiplication. Then, $\langle S; \otimes \rangle$ is a group but it is NOT Abelian. The identity element is the identity matrix I_n . Note that if S be the set of all $n \times n$ matrices with real entries, then $\langle S; \otimes \rangle$ is not a group because some of the matrices in S are not invertible.

Example 2-5: Let S be the set of all $(n \times n)$ matrices with real entries. Let \oplus denote the operation of matrix addition. Then, $\langle S; \oplus \rangle$ is an Abelian group and the identity element is the zero matrix $0_{n \times n}$.

Subgroups

Definition 2-9: Let $\langle S; \otimes \rangle$ be a group. Let $\tilde{S} \subseteq S$ be closed under \otimes , i.e., $\otimes : \tilde{S} \times \tilde{S} \rightarrow \tilde{S}$. If $\langle \tilde{S}; \otimes \rangle$ satisfies the properties of a group as delineated in Definition 2-7, then $\langle \tilde{S}; \otimes \rangle$ is called a subgroup of the group $\langle S; \otimes \rangle$. In this case, if \tilde{S} is a proper subset of S , then $\langle \tilde{S}; \otimes \rangle$ is called a proper subgroup of the group $\langle S; \otimes \rangle$. If $\tilde{S} = S$ or if $\tilde{S} = \{e\}$ where e is the identity element, then $\langle \tilde{S}; \otimes \rangle$ is called a trivial subgroup of $\langle S; \otimes \rangle$. The largest proper subgroup of $\langle S; \otimes \rangle$ is called the maximal subgroup.

Example: $\langle \mathcal{Q}; + \rangle$ is a proper subgroup of the group $\langle \mathfrak{R}, + \rangle$.

Rings, Modules, and Fields

Definition 2-10: Let $\langle S; +; \bullet \rangle$ be an algebraic system, i.e., $+: S \times S \rightarrow S$ and $\bullet : S \times S \rightarrow S$. Then, $\langle S; +; \bullet \rangle$ is called a ring if $\langle S; + \rangle$ is an Abelian group (with $0 \in S$ as the additive identity element) and if, for every $\alpha, \beta, \gamma \in S$, the following conditions are satisfied:

- $\alpha \bullet (\beta \bullet \gamma) = (\alpha \bullet \beta) \bullet \gamma$ Associative property
- $\alpha \bullet (\beta + \gamma) = \alpha \bullet \beta + \alpha \bullet \gamma$ and $(\beta + \gamma) \bullet \alpha = \beta \bullet \alpha + \gamma \bullet \alpha$ Distributive property

A ring is called commutative if, in addition, it satisfies the commutative property, i.e., $\alpha \bullet \beta = \beta \bullet \alpha \forall \alpha, \beta \in S$.

Remark 2-1: A ring may or may not satisfy the following properties:

- $\exists 1 \in S$ such that $1 \bullet \alpha = \alpha \bullet 1 = \alpha \forall \alpha \in S$ Existence of multiplicative identity
- If $\alpha \neq 0$, then $\forall \beta, \gamma \in S$ $\begin{cases} \alpha \bullet \beta = \alpha \bullet \gamma \Rightarrow \beta = \gamma \\ \beta \bullet \alpha = \gamma \bullet \alpha \Rightarrow \beta = \gamma \end{cases}$ Cancellation property

Definition 2-11: Let $\langle S; +; \bullet \rangle$ be a ring. Then, an element $\alpha \in S - \{0\}$ is called a left [resp. right] zero-divisor if $\exists \beta \in S - \{0\}$ such that $\alpha \bullet \beta = 0$ (resp. $\beta \bullet \alpha = 0$). An element of S , which is both a left and a right zero-divisor, is called a zero-divisor.

Definition 2-12: Let $\langle S; +; \bullet \rangle$ be a ring with $\mathbf{1}$ as the identity element (i.e., the identity with respect to the operation \bullet). Then, an element $\alpha \in S$ is called a left [resp. right] invertible if $\exists \chi \in S$ [resp. $\beta \in S$] such that $\chi \bullet \alpha = \mathbf{1}$ (resp. $\alpha \bullet \beta = \mathbf{1}$). The element χ [resp. β] is called a left [resp. right] inverse of α . If an element $\alpha \in S$ is both left and right invertible, then α is called an invertible element.

Definition 2-13: Let $\langle S; +; \bullet \rangle$ be a ring. Then, a (left) S -module is an additive abelian (i.e., commutative) group M together with a function $S \times M \rightarrow M$, where the image of (s, v) is denoted as sv , such that $\forall r, s \in S$ and $\forall u, v \in M$ the following conditions hold:

- (i) $r(u \oplus v) = ru \oplus rv$;
- (ii) $(r + s)u = ru \oplus su$; and
- (iii) $r(su) = (rs)u$;

If $\langle S; +; \bullet \rangle$ has an identity element $\mathbf{1}$, and if $\mathbf{1}u = u \forall u \in M$, then M is called a unitary left S -module. If $\langle S; +; \bullet \rangle$ is a division ring, then a unitary left S -module is called a left vector space.

Similar definitions hold for right S -module, unitary right S -module, and right vector space.

Modules over a ring are generalization of Abelian groups that, in turn, are modules over \mathbf{Z} .

Definition 2-14: Let A and B be modules (with additive operators \oplus and \otimes , respectively) over a ring $\langle S; +; \bullet \rangle$. A function $f : A \rightarrow B$ is called an S -module homomorphism if $\forall u, v \in A$ and $\forall s \in S$, the following conditions hold:

$$f(u \oplus v) = f(u) \oplus f(v); \text{ and}$$

$$f(ru) = rf(u).$$

An S -module homomorphism is called monomorphism [resp. epimorphism, isomorphism] if it is injective [resp. surjective, bijective]. The kernel of the homomorphism $f : A \rightarrow B$ is its kernel as a homomorphism of abelian groups, namely, $\text{Ker } f \equiv \{u \in A : f(u) = \mathbf{0}\}$. Similarly, the image of the homomorphism $f : A \rightarrow B$ is the set $\text{Im } f \equiv \{v \in B : v = f(u) \text{ for some } u \in A\}$

Furthermore, if $\langle S; +; \bullet \rangle$ is a division ring, then an S -module homomorphism is called a linear transformation.

The following results are derived from the above definition:

- (i) f is a monomorphism iff $\text{Ker } f = \mathbf{0}$;
- (ii) $f : A \rightarrow B$ is an S -module isomorphism iff \exists an S -module homomorphism $g : B \rightarrow A$ such that

$$g \circ f = \mathbf{1}_A \text{ and } f \circ g = \mathbf{1}_B.$$

Definition 2-15: Let $\langle S; +; \bullet \rangle$ be a ring. If $\langle S; +; \bullet \rangle$ has the identity $\mathbf{1} \neq \mathbf{0}$ and every non-zero element is invertible, then $\langle S; +; \bullet \rangle$ is called a division ring.

Definition 2-16: Let $\langle S; +; \bullet \rangle$ be a commutative ring. If $\langle S; +; \bullet \rangle$ has the identity $\mathbf{1} \neq \mathbf{0}$ and no zero-divisors, then $\langle S; +; \bullet \rangle$ is called an integral domain.

Definition 2-17: A commutative division ring is called a field. That is, the following conditions hold for a field.

Let $\langle F; +; \bullet \rangle$ be a commutative ring. Then, $\langle F; +; \bullet \rangle$ is called a field if the following conditions are satisfied:

- $\exists \mathbf{1} \in F \quad \mathbf{1} \bullet \alpha = \alpha \bullet \mathbf{1} = \alpha \quad \forall \alpha \in F$ Existence of multiplicative identity
- If $\alpha \in F - \{0\}$, then $\exists \alpha^{-1} \in F$ such that $\alpha^{-1} \bullet \alpha = \alpha \bullet \alpha^{-1} = 1$ Existence of multiplicative inverse

Example 2-6: $\langle \mathbf{R}; +; \bullet \rangle$ and $\langle \mathbf{C}; +; \bullet \rangle$ are fields which are very commonly used in engineering analysis. $\langle \mathbf{Q}; +; \bullet \rangle$ is also a field but it is seldom used because, as we will see later, \mathbf{Q} is not a complete set where as \mathbf{R} and \mathbf{C} are. Note that $\langle \mathbf{Z}; +; \bullet \rangle$ is a commutative ring but it is not a field because no element of $\mathbf{Z} - \{1\}$ has a multiplicative inverse.

Example 2-7: Fields can be both infinite and finite. Examples of infinite fields are: $\langle \mathbf{Q}; +; \bullet \rangle$, $\langle \mathbf{R}; +; \bullet \rangle$ and $\langle \mathbf{C}; +; \bullet \rangle$. An example of a finite field (also called Galois field) is $\langle \{0,1\}; \oplus_2; \otimes_2 \rangle$, where \oplus_2 is addition under modulo 2 and \otimes_2 is multiplication under modulo 2. This is the smallest field and is often denoted as $GF(2)$.

Example 2-8: A polynomial over a field $\langle F; +; \bullet \rangle$ is defined as an expression of the form: $a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ where $a_i \in F$; n is a non-negative integer; and x is called the indeterminate.

Vector Spaces

Definition 2-18: An Abelian group $\langle V; \oplus \rangle$ is called a vector space over the field $\langle F; +; \bullet \rangle$ if the following conditions are satisfied:

- $\forall \alpha \in F \forall x \in V$, $\alpha \otimes x$ is defined and $\alpha \otimes x \in V$ Closure property $\otimes : F \times V \rightarrow V$
- $\alpha \otimes (\beta \otimes x) = (\alpha \bullet \beta) \otimes x \forall \alpha, \beta \in F \forall x \in V$ Associativity property
- $\left. \begin{aligned} \alpha \otimes (x \oplus y) &= (\alpha \otimes x) \oplus (\alpha \otimes y) \\ (\alpha + \beta) \otimes x &= (\alpha \otimes x) \oplus (\beta \otimes x) \end{aligned} \right\} \forall \alpha, \beta \in F \forall x, y \in V$ Distributive property
- $\forall x \in V, 1 \otimes x = x$ where 1 is the multiplicative identity of $\langle F; +; \bullet \rangle$ multiplicative identity

The elements of $\langle V; \oplus \rangle$ are called vectors and the elements of $\langle F; +; \bullet \rangle$ are called scalars. Often the multiplicative operators \bullet and \otimes are simply omitted, i.e., we write $\alpha \bullet \beta = \alpha\beta$ and $\alpha \otimes x = \alpha x$. However, it is important to distinguish between the operators of the scalar addition $+$ and the vector addition \oplus . Let us denote the additive identity of the field $\langle F; +; \bullet \rangle$ as 0, the multiplicative identity of the field $\langle F; +; \bullet \rangle$ as 1 and the zero of the vector space $\langle V; \oplus \rangle$ as $\mathbf{0}$.

Remark 2-2: It follows from Definition 2-12 that, $\forall x \in V \forall \alpha \in F$,

- $0x = \mathbf{0}$ because $\begin{cases} x = 1x = (1+0)x = 1x \oplus 0x = x \oplus 0x = 0x \oplus x \\ \Rightarrow 0x = 0x \oplus \mathbf{0} = 0x \oplus (x \oplus (-x)) = (0x \oplus x) \oplus (-x) = x \oplus (-x) = \mathbf{0} \end{cases}$
- $-x = (-1)x$ because $x \oplus (-1)x = 1x \oplus (-1)x = (1 + (-1))x = 0x = \mathbf{0}$
- $\alpha \mathbf{0} = \mathbf{0}$ because $\alpha \mathbf{0} = \alpha(x \oplus (-x)) = \alpha x \oplus \alpha(-x) = \alpha x \oplus \alpha((-1)x) = \alpha x \oplus (-\alpha)x = (\alpha + (-\alpha))x = 0x = \mathbf{0}$

Remark 2-3: Every vector space must contain the zero vector $\mathbf{0}$. That is, the set V in a vector space $\langle V; \oplus \rangle$ can never be empty.

Definition 2-19: Let $\langle V; \oplus \rangle$ be a vector space over the field $\langle F; +; \bullet \rangle$. Let $U \subseteq V$ such that $\langle U; \oplus \rangle$ is a vector space over the field $\langle F; +; \bullet \rangle$. Then, $\langle U; \oplus \rangle$ is a subspace of $\langle V; \oplus \rangle$.

Remark 2-4: $\langle U; \oplus \rangle$ can be viewed as a subgroup of the group $\langle V; \oplus \rangle$,

Theorem 2-1: Let $U \subseteq V$ be nonempty. Then, $\langle U; \oplus \rangle$ is a subspace of $\langle V; \oplus \rangle$ (which is a vector space over the field $\langle F; +; \bullet \rangle$) if and only if the following condition holds: $(\alpha x \oplus y) \in U \forall x, y \in U \forall \alpha \in F$.

Proof: The proof follows directly from Definitions 2-12 and 2-13. ♦

Definition 2-20: Let $\langle V; \oplus \rangle$ and $\langle W; \tilde{\oplus} \rangle$ be two vector spaces over the same field $\langle F; +; \bullet \rangle$. Then, $\langle V; \oplus \rangle$ and $\langle W; \tilde{\oplus} \rangle$ are said to be isomorphic if there exists a linear bijective mapping $f : V \rightarrow W$. That is,

- $f(\alpha x \oplus \beta y) = \alpha f(x) \tilde{\oplus} \beta f(y) \quad \forall x, y \in V \text{ and } \forall \alpha, \beta \in F$ Linearity property
- $f(x) = f(y) \Rightarrow x = y \quad \forall x, y \in V$ Injective property
- $\{f(x) : x \in V\} = W$ Surjective property

HW#2-1: Exercises 1,4,5,6 of Naylor and Sell (p. 181).

Definition 2-21: Let $\langle V; \oplus \rangle$ be a vector space over the same field $\langle F; +; \bullet \rangle$, and S be a set of (finite or countably infinite or uncountable) vectors. Then, $x \in V$ is said to be a linear combination of vectors in S if \exists a finite set of vectors $\{u^j : j = 1, 2, \dots, n\}$ and a finite set of scalars $\{\alpha_j : j = 1, 2, \dots, n\}$ such that $x = \sum_{j=1}^n \alpha_j u^j$.

Definition 2-22: Let $\langle V; \oplus \rangle$ be a (finite or countable infinite or uncountable) vector space over a field. A vector $x \in V$ is said to be a linear combination of vectors in V if \exists a **finite** set of vectors $\{x^1, x^2, \dots, x^n\}$ and a **finite** set of scalars $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ such that $x = \sum_{k=1}^n \alpha_k x^k$.

Definition 2-23: Let $\langle V; \oplus \rangle$ be a (finite or countable infinite or uncountable) vector space over a field. A set $U \subseteq V$ is said to be linearly independent if $\forall x \in U$ is **not** a linear combination of vectors in $U - \{x\}$; otherwise $U \subseteq V$ is a linearly dependent set.

Definition 2-24: A set B of vectors is said to be a Hamel basis for $\langle V; \oplus \rangle$ if: (i) B is a linearly independent set in $\langle V; \oplus \rangle$; and (ii) B spans the vector space, i.e., $\forall x \in V$ can be expressed as a linear combination of the vectors in B .

Definition 2-25: The cardinality of a Hamel basis of a vector space $\langle V; \oplus \rangle$ is said to be the dimension of the space that is denoted as $\dim(V)$.

Theorem 2-2: Let $\langle V; \oplus \rangle$ be an n-dimensional vector space over $\langle F; +; \bullet \rangle$. Then, $\langle V; \oplus \rangle$ is isomorphic to F^n .

HW#2-2: Prove Theorem 2-2.

Corollary to Theorem 2-2: Let $\langle V; \oplus \rangle$ and $\langle W; \oplus \rangle$ be two vector spaces over the same field $\langle F; +; \bullet \rangle$. Then, $\langle V; \oplus \rangle$ and $\langle W; \oplus \rangle$ are isomorphic if and only if $\dim(V) = \dim(W)$.

HW#2-3: Prove Corollary to Theorem 2-2.

Definition 2-26: Let $\langle V; \oplus \rangle$ and $\langle W; \oplus \rangle$ be two vector spaces defined over the same field $\langle F; +; \bullet \rangle$, and $L : V \rightarrow W$ be a linear transformation. The null space of L is defined as: $N(L) = \{x \in V : Lx = \mathbf{0}_W\}$, and the range space of L is defined as: $R(L) = \{y = Lx : x \in V\}$.

Remark 2-5: $\langle N(L); \oplus \rangle$ is a subspace of $\langle V; \oplus \rangle$ and $\langle R(L); \oplus \rangle$ is a subspace of $\langle W; \oplus \rangle$.

Theorem 2-3: Let $L : V \rightarrow W$ be a linear transformation from the vector space $\langle V; \oplus \rangle$ to the vector space $\langle W; \oplus \rangle$ over the same field $\langle F; +; \bullet \rangle$. The dimensions of $N(L)$, $R(L)$, and V are related as: $\dim(N(L)) + \dim(R(L)) = \dim(V)$.

HW#2-4: Prove Theorem 2-3.

HW#2-5: Exercises 1,2,3,4,5,9, and 10 of Naylor and Sell (pp. 186-187).