Chapter 1

Basic Concepts

1.1 Fields

Definition 1.1.1. A *field* F is a non-empty set together with two binary operations (denoted by $+$ and $\cdot$) and two distinguished elements (denoted by 0 and 1), satisfying the following properties:

(i) $(F,+)$ is an abelian group, i.e.,

- (a) $(F,+)$ is closed:- $\forall\, x,y\in F \;\; x+y\in F$,
- (b) $(F,+)$ is associative:- $\forall\, x,y,z\in F \;\; (x+y)+z=x+(y+z)$,
- (c) 0 is the *additive identity* of $(F,+)$:- $\forall\, x\in F \;\; x+0=x=0+x$,
- (d) each element of F has the *additive inverse*:- $\forall\, x\in F\; \exists\, y\in F\; x+y=0=y+x$; moreover, we write $-x$ as the additive inverse of x for each $x\in F$,
- (e) $(F,+)$ is abelian:- $\forall\, x,y\in F \;\; x+y=y+x$,

(ii) $(F^*,\cdot)$ is an abelian group, where $F^* := F\backslash\{0\}$, i.e.,

- (a) $(F^*,\cdot)$ is closed:- $\forall\, x,y\in F^* \;\; x\cdot y\in F^*$,
- (b) $(F^*,\cdot)$ is associative:- $\forall\, x,y,z\in F^* \;\; (x\cdot y)\cdot z=x\cdot(y\cdot z)$,
- (c) 1 is the *multiplicative identity* of $(F^*,\cdot)$:- $\forall\, x\in F^* \;\; x\cdot 1=x=1\cdot x$,
- (d) each element of F^* has the *multiplicative inverse*:- $\forall\, x\in F^*\; \exists\, y\in F^*\; x\cdot y=1=y\cdot x$; moreover, we write x^{-1} as the multiplicative inverse of x for each $x\in F^*$,
- (e) $(F^*,\cdot)$ is abelian:- $\forall\, x,y\in F^* \;\; x\cdot y=x\cdot y$,

(iii) F satisfies the *left* and *right distributive laws*, i.e., $\forall\, x,y,z\in F \;\; x\cdot(y+z)=x\cdot y+x\cdot z=(y+z)\cdot x$.

Remark 1.1.2. From now on, we write F instead of a field $(F,+,\cdot)$, $x-y$ instead of $x+(-y)$ and xy instead of $x\cdot y$ for all $x,y\in F$. Moreover, we write x/y or $\frac{x}{y}$ instead of xy^{-1} for all $x\in F$ and $y\in F^*$.

Example 1.1.3.

(i) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are examples of (infinite) fields.

(ii) $\mathbb{Z}_p$, where p is a prime number, is a finite filed with order p.

Recall that $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$ is the set of integers modulo p where the addition and multiplication are the ones modulo p.

(iii) $\mathbb{Z}$ is not a field because

Lemma 1.1.4. *Let F be a field.*

(i) If $x \in F$ satisfies the property that $\forall\, y \in F \;\; x + y = y$, then $x = 0$.

(ii) If $x \in F$ satisfies the property that $\forall\, y \in F^* \;\; xy = y$, then $x = 1$.

(iii) $\forall\, x \in F \;\; x\,0 = 0 = 0\,x$.

(iv) If $x, y \in F \;\; xy = 0$, then $x = 0$ or $y = 0$.

Definition 1.1.5. A field F is *algebraically closed* if every non-constant polynomial with coefficients in F has a root in F.

Equivalently, F is algebraically closed if and only if for each polynomial $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ with $a_0, a_1, \ldots, a_n \in F$, $a_n \neq 0$ and $n \geq 1$ there exists $\alpha \in F$ such that $p(\alpha) = 0$.

Theorem 1.1.6. *The field $\mathbb{C}$ of complex numbers is algebraically closed.*

Definition 1.1.7. Let F be a field and K a subset of F. Then K is a *subfield* of F if

(i) $0_F, 1_F \in K$

(ii) K is closed under the operations $+$ and $\cdot$

(iii) K is a field with the identities 0_F and 1_F and with the restrictions of $+$ and $\cdot$ to K.

Theorem 1.1.8. *Let K be a field. Then there exists an algebraically closed field F having K as a subfield.*

Example 1.1.9. $\mathbb{Q}$ is not algebraically closed (why?). However, $\mathbb{Q}$ is a subfield of $\mathbb{C}$ which is algebraically closed.

Definition 1.1.10. Let F be a field. If there is a positive integer m such that

$$\underbrace{1 + 1 + \cdots + 1}_{m \text{ times}} = 0,$$

then the *characteristic* of F, denoted by $\operatorname{char} F$, is defined by

$$\operatorname{char} F = \min\Big\{ m \in \mathbb{N} \;\Big|\; \underbrace{1 + 1 + \cdots + 1}_{m \text{ times}} = 0 \Big\}.$$

Otherwise, we call F a field of *characteristic zero*, denoted by $\operatorname{char} F = 0$.

Example 1.1.11.

(i) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields of characteristic   .

(ii) $\operatorname{char} \mathbb{Z}_p =$ where p is a prime number.

1.2 Systems of Linear Equations

Definition 1.2.1. Let F be a field. A *system of m linear equations in n unknowns* $x_1, x_2, \ldots, x_n$ is of the form

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots & \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m \end{aligned}$$

where $b_1, b_2, \ldots, b_m$ and a_{ij} with $1 \le i \le m$ and $1 \le j \le n$ belong to F. Note that we may write $AX = B$ for the above system, where

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}, \qquad X = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}, \qquad \text{and} \qquad B = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}.$$

We call A the *matrix of coefficients* (or *coefficient matrix*), X the *variable matrix* and B the *constant matrix* of the system.

Any n-tuple $(x_1, x_2, \ldots, x_n)$ of elements of F which satisfies each of the above equations is called a *solution* to the system. If $b_1 = b_2 = \cdots = b_m = 0$, then we say that the system is *homogeneous*.

Theorem 1.2.2. *Let F be a field with* $\operatorname{char} F = 0$. *Given a system of linear equations over F. Then one of the followings holds.*

(i) There is no solution to the system.

(ii) There is a unique solution to the system.

(iii) There are infinitely many solutions to the system.

1.3 Matrices and Elementary Row Operations

Definition 1.3.1. Let A be an $m \times n$ matrix over a field F. There are three *elementary row operations* on A as follows:

(i) interchanging of two rows of A,

(ii) multiplication of one row of A by a non-zero scalar c,

(iii) replacement of the rth row of A by the row r plus c times the row s where $c \in F \setminus \{0\}$ and $r \neq s$.

Definition 1.3.2. If A and B are $m \times n$ matrices over a field, we say that B is *row-equivalent to* A if B can be obtained from A by a finite sequence of elementary row operations.

Note 1.3.3. We can show that row-equivalence is an equivalence relation.

Theorem 1.3.4. *If A and B are $m \times n$ equivalent matrices over a field, the homogeneous systems of linear equations $AX = 0$ and $BX = 0$ have exactly the same solutions.*

1.4 Row-Reduced Echelon Matrices

Definition 1.4.1. An $m \times n$ matrix R is *row-reduced* if

(i) all rows of R consisting only of 0s appear at the bottom of R;

(ii) in any non-zero row of R, the first non-zero entry must be 1, called the *leading one* or *leading entry*;

(iii) for any two consecutive rows, the leading entry of the lower row is to the right of the leading entry of the upper row.

Theorem 1.4.2. *Every $m \times n$ matrix over a field is row-equivalent to a row-reduced matrix.*

Definition 1.4.3. An $m \times n$ matrix R is a *row-reduced echelon matrix* if

(i) R is row-reduced;

(ii) any column that contains a leading entry has 0s in all other positions.

Theorem 1.4.4. *Every $m \times n$ over a field matrix is row-equivalent to a row-reduced echeleon matrix.*

Theorem 1.4.5. *If A is an $m \times n$ matrix over a field and $m < n$, then the homogeneous system of linear equations $AX = 0$ has a non-trivial solution.*

Theorem 1.4.6. *If A is an $n \times n$ (square) matrix over a field, then A is row-equivalent to the $n \times n$ identity matrix if and only if the system of linear equations $AX = 0$ has only the trivial solution.*

Definition 1.4.7. An $m \times n$ matrix over a field is an *elementary matrix* if it can be obtained from the $m \times n$ identity matrix by means of a single elementary row operation.

Theorem 1.4.8. *Let A and B be $m \times n$ matrices over a field. Then B is row-equivalent to A if and only if $B = PA$ where P is a product of $m \times m$ elementary matrices.*

1.5 Invertible Matrices

Theorem 1.5.1. *If A is an $n \times n$ matrix, the followings are equivalent.*

(i) *A is invertible.*

(ii) *A is row-equivalent to the $n \times n$ identity matrix.*

(iii) *A is a product of elementary matrices.*

Corollary 1.5.2. *If A is an invertible $n \times n$ matrix, and if a sequence of elementary row operations reduces A to the identity I, then that same sequence of operations when applied to I yields A^{-1}.*

Corollary 1.5.3. *Let A and B be $m \times n$ matrices. Then B is row-equivalent to A if and only if $B = PA$ where P is an invertible $m \times m$ matrix.*

Theorem 1.5.4. *If A is an $n \times n$ matrix, the followings are equivalent.*

(i) *A is invertible.*

(ii) *The homogeneous system $AX = 0$ has only the trivial solution $X = 0$.*

(iii) *The system of equations $AX = B$ has a solution X for each $n \times 1$ matrix B.*

1.6 Vector Spaces

Definition 1.6.1. A *vector space* (or *linear space*) consists of the followings:

(i) a field F of *scalars*;

(ii) a set V of objects, called *vectors*;

(iii) a rule (or operation) $+$, called *vector operation*, which associates with each pair of vectors $u, v \in V$ a vector $u + v \in V$, called the *sum of u and v*, in such a way that $(V, +)$ is an abelian group with the identity 0, the *zero vector*.

(iv) a rule (or operation), called *scalar operation*, which associates with each scalar $\alpha \in F$ and vector $v \in V$ a vector $\alpha v \in V$, called the *product of α and v*, in such a way that

(a) $1v = v$ for every $v \in V$;

(b) $(\alpha\beta)v = \alpha(\beta v)$ for all $\alpha, \beta \in F$ and $v \in V$;

(c) $\alpha(u + v) = \alpha u + \alpha v$ for all $\alpha \in F$ and $u, v \in V$;

(d) $(\alpha + \beta)v = \alpha v + \beta v$ for all $\alpha, \beta \in F$ and $v \in V$.

We also say that V is a *vector space over the field F*.

Example 1.6.2. The followings are examples of vector spaces.

(i) Let F be a field, $n \in \mathbb{N}$ and let

$$F^n = \{(x_1, x_2, \ldots, x_n) \mid x_i \in F \text{ for all } 1 \le i \le n\}.$$

For each $x = (x_1, x_2, \ldots, x_n), y = (y_1, y_2, \ldots, y_n) \in F^n$ and $\alpha \in F$, define

$$x + y = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n) \quad \text{and} \quad \alpha x = (\alpha x_1, \alpha x_2, \ldots, \alpha x_n).$$

Then F^n is a vector space over F and is called the *n-tuple space*. In particular, F is a vector space over F.

(ii) Let F be a field and $m, n \in \mathbb{N}$. Define

$$M_{mn}(F) := \Big\{A = [a_{ij}]_{m\times n} \;\Big|\; a_{ij} \in F \text{ for all } i, j\Big\}.$$

For each $A = [a_{ij}], B = [b_{ij}] \in M_{mn}(F)$ and $\alpha \in F$, define

$$A + B = [a_{ij} + b_{ij}] \quad \text{and} \quad \alpha A = [\alpha a_{ij}].$$

Then $M_{mn}(F)$ is a vector space over F and is called the *space of $m \times n$ matrices*.

(iii) Let F be a field and S a non-empty set. Define

$$F^S := \{f \mid f : S \to F\}.$$

For each $f, g \in F^S$ and $\alpha \in F$, define

$$(f + g)(x) = f(x) + g(x) \quad \text{and} \quad (\alpha f)(x) = \alpha\big(f(x)\big) \quad \text{for all } x \in S.$$

Then F^S is a vector space over F and is called the *space of functions from the set S to the field F*.

(iv) Let F be a field. Define

$$F_n[x] := \{p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \mid a_i \in F \text{ for all } 0 \le i \le n\}, \text{ where } n \in \mathbb{N}.$$
$$F[x] := \{p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \mid n \in \mathbb{N}_0 \text{ and } a_i \in F \text{ for all } 0 \le i \le n\}.$$

Then $F_n[x]$ (where $n \in \mathbb{N}$) and $F[x]$ are vector spaces over F and are called the *space of polynomials of degree not more than n* and *space of polynomials*, respectively.

(v) $\mathbb{C}$ is a vector space over $\mathbb{R}$. In general, if we let

$$V = \{(x_1, x_2, \ldots, x_n) \mid x_i \in \mathbb{C} \text{ for all } 1 \le i \le n\}.$$

For each $x = (x_1, x_2, \ldots, x_n), y = (y_1, y_2, \ldots, y_n) \in V$ and $\alpha \in \mathbb{R}$, define

$$x + y = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n) \quad \text{and} \quad \alpha x = (\alpha x_1, \alpha x_2, \ldots, \alpha x_n).$$

Then we obtain that V is a vector space over $\mathbb{R}$ which is quite different from the space $\mathbb{C}^n$ over $\mathbb{C}$ (as in (i) while $F = \mathbb{C}$) and the space $\mathbb{R}^n$ over $\mathbb{R}$.

(vi) Let R be a ring with identity 1 and suppose that R has a subfield F such that $1 \in F$. Let $\bar{0}$ be the zero element of R, the addition is the addition operation already defined on R, and for $\alpha \in F$ and $v \in R$, since $F \subseteq R$, we have $\alpha, v \in R$ so that αv may be defined to be the usual product of elements of R. Then R is a vector space over F.

Theorem 1.6.3. *Let V be a vector space over a field F.*

(i) *If $u \in V$ is such that $u + v = v$ for some $v \in V$, then $u = 0$.*

(ii) $\forall\, v \in V \;\; 0v = \bar{0}$.

(iii) $\forall \alpha \in F \;\; \alpha\bar{0} = \bar{0}$.

(iv) $\forall\, v \in V \;\; -v = (-1)v$.

(v) $\forall\, \alpha \in F\; \forall\, u, v \in V \;\; \alpha(u - v) = \alpha u - \alpha v$.

1.7 Subspaces

Definition 1.7.1. Let V be a vector space over a field F and W a non-empty subset of V. We call W a *subspace* of V, denoted by $W \preceq V$, if W is a vector space over F with the same operations of vector addition and scalar multiplication on V.

Theorem 1.7.2. *Let V be a vector space over a field F. Then W is a subspace of V if and only if*

(i) $\emptyset \neq W \subseteq V$

(ii) $\forall\, v, w \in W\; \forall\, \alpha, \beta \in F \;\; \alpha v + \beta w \in W$.

Example 1.7.3. Let F be a field.

(i) For a vector space V, we have $V \preceq V$ and $\{\bar{0}\} \preceq V$. Note that $\{\bar{0}\}$ is called the *zero space* of V.

(ii) Let $W = \big\{(\alpha, \alpha, \dots, \alpha) \;\big|\; \alpha \in F\big\} \subseteq F^n$ where $n \in \mathbb{N}$. Then $W \preceq F^n$.

(iii) $\big\{(0, x_2, x_3, \dots, x_n) \;\big|\; x_2, x_3, \dots, x_n \in F\big\} \preceq F^n$ where $n \in \mathbb{N}$.

(iv) Let $n \in \mathbb{N}$ and $n \geq 2$. Then $\big\{(1 + x_2, x_2, x_3, \dots, x_n) \;\big|\; x_2, x_3, \dots, x_n \in F\big\}$ is not a subspace of F^n because

(v) Let

$$V := \big\{f : F \to F \;\big|\; \text{there exists a non-negative interger } n \text{ such that } f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \text{ for all } x \in F, \text{ where } a_i \in F \text{ for all } 0 \leq i \leq n\big\}.$$

Then $V \preceq F^F$.

(vi) Let $n \in \mathbb{N}$. Then $F_n[x] \preceq F[x]$.

Here, the zero polynomial has degree $-\infty$. Recall that for each $p(x), q(x) \in F[x]$, we have

$$\deg\big(p(x)q(x)\big) = \deg p(x) + \deg q(x) \quad \text{and} \quad \deg\big(p(x) + q(x)\big) \leq \max\{\deg p(x), \deg q(x)\}.$$

(vii) $\{f : \mathbb{R} \to \mathbb{R} \mid f \text{ is continuous}\} \preceq \mathbb{R}^{\mathbb{R}}$.

(viii) $\{f : \mathbb{R} \to \mathbb{R} \mid f \text{ is differentiable}\} \preceq \mathbb{R}^{\mathbb{R}}$.

(ix) A matrix $A = [a_{ij}] \in M_{mn}(F)$ is *symmetric* if and only if $a_{ij} = a_{ji}$ for all i, j.

We have $\{A \in M_{mn}(F) \mid A \text{ is symmetric}\} \preceq M_{mn}(F)$.

(x) Let $A \in M_{mn}(F)$. Then $W = \{X \in M_{n\times 1}(F) \mid AX = 0\} \preceq M_{n\times 1}(F)$. We call W the *solution space of a system of homogeneous linear equations*.

Theorem 1.7.4. *Let V be a vector space over a field and $\{W_\gamma \mid \gamma \in \Lambda\}$ be a collection of subspaces of V. Then $\bigcap_{\gamma\in\Lambda} W_\gamma$ is also a subspace of V.*

Definition 1.7.5. Let V be a vector space over a field and $S \subseteq V$. Let $\{W_\gamma \mid \gamma \in \Lambda\}$ denote the collection of all subspaces of V containing S. That is

$$\{W_\gamma \mid \gamma \in \Lambda\} = \{W \mid W \preceq V \text{ and } S \subseteq W\}.$$

The *subspace (of V) spanned by* S is defined to be $\bigcap_{\gamma\in\Lambda} W_\gamma$ and denoted by $\langle S\rangle$.

When S is finite, i.e., $S = \{v_1, v_2, \ldots, v_n\}$, we shall simply call $\langle S\rangle$ the *subspace (of V) spanned by the vectors* $v_1, v_2, \ldots, v_n$ and write $\langle v_1, v_2, \ldots, v_n\rangle$ instead of $\langle S\rangle$.

Note 1.7.6. Let S be a subset of a vector space of V. Then $\langle S\rangle$ is the smallest subspace of V containing S. In another word, $\langle S\rangle$ satisfies the followings:

(i) $\langle S\rangle \preceq V$

(ii) $S \subseteq \langle S\rangle$

(iii) $\forall\, W \preceq V \quad S \subseteq W \Longrightarrow \langle S\rangle \subseteq W$.

Note also that $\langle\emptyset\rangle = \{0\}$, the zero space.

Theorem 1.7.7. *Let V be a vector space over F and $S \subseteq V$. If $S \neq \emptyset$, then*

$$\langle S\rangle = \{\alpha_1x_1 + \alpha_2x_2 + \cdots + \alpha_nx_n \mid n \in \mathbb{N},\ \alpha_1, \alpha_2, \ldots, \alpha_n \in F,\ \text{and}\ x_1, x_2, \ldots, x_n \in S\}.$$

Note that such the $\alpha_1x_1 + \alpha_2x_2 + \cdots + \alpha_nx_n$ is called a linear combination of $x_1, x_2, \ldots, x_n$ (over F).