Chapter I: Abstract Vector Spaces

1.1 Groups and Fields

A vector space consists of two sets: a set V of "vectors" and set F of "scalars". There are also several binary operations involved $V\times V\to V$, $F\times F\to F$, $F\times F\to F$, $F\times V\to V$ subject to several axioms each, and also compatibility conditions. In order to organize all of this data, we use the language of abstract algebra.

1.1.1 Definition A **group** is a pair $(G,*)$, where G is a set and $*: G\times G\to G$ is a binary operation, subject to the following axioms:

- **(G1)** (associativity) $x*(y*z)=(x*y)*z \quad \forall x,y,z\in G$.
- **(G2)** (identity) there exists a unique $e\in G$ such $e*x=x=x*e \quad \forall x\in G$.
- **(G3)** (inverses) For every $x\in G$, there exists a unique $x^{-1}\in G$, such that $x*x^{-1}=e=x^{-1}*x$.

A group $(G,*)$ is called **abelian** if additionally it satisfies

- **(G4)** (commutativity) $x*y=y*x \quad \forall x,y\in G$.

□

1.1.2 Example (groups)

(a) $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$ are all abelian groups. Identity: 0. Inverse of x is $-x$.

(b) $(\mathbb{Q}\setminus\{0\},\cdot)$, $(\mathbb{R}\setminus\{0\},\cdot)$, $(\mathbb{C}\setminus\{0\},\cdot)$ are all abelian groups. Identity: 1. Inverse of x is $\frac{1}{x}$.

$(\mathbb{Z}\setminus\{0\},\cdot)$ is not a group: no inverses.

(c) Let S_n be the set of all bijective funct. $\sigma:\{1,\dots,n\}\to\{1,\dots,n\}$. Then $(S_n,\circ)$ is a group where $\circ$ is funct. composition. This is called the Symmetric Group.

(d) Let $\mathbb{Z}_n$ (or $\mathbb{Z}/n\mathbb{Z}$) be the set of residue classes of integers modulo n. I.e.

$$\mathbb{Z}_n=\{\overline{m}\mid m\in\mathbb{Z}\} \text{ where } \overline{m}=\{k\in\mathbb{Z}\mid k\equiv m \bmod n\}.$$

Define $+:\mathbb{Z}_n\times\mathbb{Z}_n\to\mathbb{Z}_n$ via $\overline{m_1}+\overline{m_2}:=\overline{m_1+m_2}$. One can prove that $+$ is well-defined making $(\mathbb{Z}_n,+)$ into an abelian group.

(e) $(\mathbb{Z}_n\setminus\{0\},\cdot)$ where $\overline{m_1}\cdot\overline{m_2}:=\overline{m_1\cdot m_2}$ is not a group in general. For example, $\overline{2}$ has no multiplicative inverse in $\mathbb{Z}_4$.

□

1.1.3 Definition A **field** is a triple $(F,+,\cdot)$ where F is a set together with binary operations $+: F\times F\to F$ and $\cdot: F\times F\to F$ satisfying the following conditions:

- **(F1)** $(F,+)$ is an abelian group. The additive identity is denoted 0. The inverse of $x\in F$ is denoted $-x$.
- **(F2)** $(F\setminus\{0\},\cdot)$ is an abelian group. The mult. identity is denoted 1. The inverse of $x\in F\setminus\{0\}$ is denoted x^{-1} or $\frac{1}{x}$
- **(F3)** (distributive law) $a(b+c)=ab+ac \quad \forall a,b,c\in F$.

□

Using F1 and F2, we can define **subtraction** and **division** as follows:

$$x-y := x+(-y)$$
$$\frac{x}{y} := xy^{-1} = x\cdot\frac{1}{y}.$$

So a field is an algebraic structure where we can do arithmetic.

1.1.4 Example (fields)

(a) $\mathbb{Q},\mathbb{R},\mathbb{C}$ are fields under the usual operations of addition and multiplication.

(b) $\mathbb{Z}_n$ is a field (under $+$ and $\cdot$ as defined in Ex 1.1.2) if and only if n is a prime number. This is a good exercise. Use Bezouts lemma.

(c) $\mathbb{Q}(\sqrt{2})=\{a+b\sqrt{2}\mid a,b\in\mathbb{Q}\}$ is a field using the same operations from $\mathbb{R}$.

□

1.1.5 Proposition (field properties) If F is a field, then

(a) (cancellation law) $a+b=a+c$ implies $b=c$.

(b) $a\cdot 0=0 \quad \forall a\in F$

(c) $(-1)\cdot a=-a \quad \forall a\in F$

Proof. (of (c)) I have to prove that $(-1)\cdot a$ is the additive inverse of $a\in F$. We have

$$a+(-1)\cdot a = 1\cdot a+(-1)\cdot a = (1+(-1))\cdot a = 0\cdot a \overset{(b)}{=} 0.$$

By uniqueness of inverses, $(-1)a=-a$.

□

1.1.6 Definition (subfields) A subset K of a field F is called a subfield of F if it is also a field under the operations inherited from F. Equivalently, $0,1\in K$ and K is closed under addition, multiplication, subtraction, and division.

□

1.1.7 Example (subfields) We have the following chain of subfields

$$\mathbb{Q}\subseteq\mathbb{Q}(\sqrt{2})\subsetneq\mathbb{R}\subsetneq\mathbb{C}.$$

Fact: $\mathbb{Q}$ has no proper subfields.

□

1.1.8 Definition The **characteristic** of a field F is the smallest positive integer n for which

$$\underbrace{1+1+\dots+1}_{n \text{ summands}}=0.$$

We write $\operatorname{ch}F$ for the characteristic of F. If no smallest integer exists, then $\operatorname{ch}F:=0$.

□

1.1.9 Example (characteristic)

(a) $\operatorname{ch}\mathbb{Q}=0=\operatorname{ch}\mathbb{Q}(\sqrt{2})=\operatorname{ch}\mathbb{R}=\operatorname{ch}\mathbb{C}$.

(b) $\operatorname{ch}\mathbb{Z}_p=p$ because $\underbrace{\overline{1}+\overline{1}+\dots+\overline{1}}_{p\text{-times}}=\overline{p}=\overline{0}$. p is a prime number.

(c) One can prove: the characteristic of a field is either 0 or prime! There are other examples of fields of prime characteristic. Fields of characteristic zero contain $\mathbb{Q}$ as a subfield. Fields of characteristic p contain $\mathbb{Z}_p$ as a subfield.

□

1.2 Vector Spaces

1.2.1 Definition Let F be a field. A **vector space** over F is an abelian group $(V,+)$ together with an additional operation $F\times V\to V$, $(\alpha,v)\mapsto\alpha v$ subject to the following conditions:

- **(V1)** $1v=v$ for all $v\in V$.
- **(V2)** $(\alpha\beta)v=\alpha(\beta v)$ for all $\alpha,\beta\in F$, $v\in V$.
- **(V3)** $(\alpha+\beta)v=\alpha v+\beta v$ and $\alpha(v+w)=\alpha v+\alpha w$ for all $\alpha,\beta\in F$ and $v,w\in V$.

□

Terminology:

- "V is a vector space over F" & "V is an F-vector space" mean the same thing.
- elements of V are called "vectors", elements of F are called "scalars".
- A vector space over $\mathbb{R}$ is called a "real vector space".
- A vector space over $\mathbb{C}$ is called a "Complex vector space."

1.2.2 Proposition (vector space properties) Let V be a vector space over F. Then for all $v\in V$ and $a\in F$

(a) $0v=0$ zero vector in V, zero in F

(b) $(-a)v=-(av)$

(c) $a0=0$ zero vector, zero vector

(d) If $av=0$, then $a=0$ or $v=0$.

Proof. (of (a)) I have to prove that $0v$ is the zero vector, i.e., the additive identity in $(V,+)$. We have

$$0v+0v=(0+0)v=0v.$$

By adding $-(0v)$ to both sides, we get $0v=0$.

□

1.2.3 Example (vector spaces) Let F be a field.

(a) $F^n:=\{(a_1,\dots,a_n)\mid a_i\in F \ i=1,\dots,n\}$ is an F-vector space under the operations

(addition) $(a_1,\dots,a_n)+(b_1,\dots,b_n):=(a_1+b_1,\dots,a_n+b_n)$

(scalar mult) $\alpha(a_1,\dots,a_n):=(\alpha a_1,\dots,\alpha a_n)$.

This is the most important example!

(b) The trivial or zero vector space $V=\{0\}\subseteq F$.

(c) The set of $n\times m$ matrices over F

$$F^{n\times m}:=\operatorname{Mat}_{n\times m}(F):=\{A=(a_{ij})\mid a_{ij}\in F \ \substack{i=1,\dots,n\\ j=1,\dots,m}\}$$

is a vector space over F under the operations: $A=(a_{ij})$ $B=(b_{ij})$ $\alpha\in F$

(addition) $A+B:=(a_{ij}+b_{ij})$

(scalar mult) $\alpha A:=(\alpha a_{ij})$

(d) Polynomials w/ coefficients from F

$$F[x]:=\{\sum_{i=0}^{n}a_ix^i \mid a_i\in F \ i=0,\dots,n\}$$

is a vector space over F w/

(addition) $\sum_{i=0}^{n}a_ix^i+\sum_{j=0}^{m}b_jx^j:=\sum_{i=0}^{\max(m,n)}(a_i+b_i)x^i$

(scalar mult) $\alpha\sum_{i=0}^{n}a_ix^i:=\sum_{i=0}^{n}(\alpha a_i)x^i$.

Note: we do not view polynomials as functions $F\to F$. They are just formal sums in the "indeterminate" x. So two polynomials $\sum a_ix^i$ and $\sum b_ix^i$ are equal iff $a_i=b_i$ for all i. Here's why:

> $F=\mathbb{Z}_2$ $\quad p(x)=x+1 \quad q(x)=x^3+1$
> In $F[x]$, $p(x)\neq q(x)$. But as functions from $F\to F$, $p(x)=q(x)$.

(e) Let X be any set and let V be a vector space over F. The set

$$V^X:=\operatorname{Maps}(X,V):=\operatorname{Fun}(X,V)$$

of all functions $f: X\to V$ from X to V is a vector space over F under the operations:

(addition) $(f+g)(x):=f(x)+g(x) \quad \forall f,g\in V^X,$

(scalar mult) $(\alpha f)(x):=\alpha f(x) \quad \forall\alpha\in F.$

For example, $X=\mathbb{N}$, $V=F$. Then $F^{\mathbb{N}}$ is the space of sequences w/ entries from F. Or if $X=\{1,\dots,n\}$, $V=F$, then $F^X\cong F^n$.

(f) Let K be a subfield of F and V any F-vector space. Then V is a K-vector space using the same operations. For ex, $\mathbb{C}$ can be can be considered as a real or complex vector space.

□

1.3 Subspaces

1.3.1 Definition Let W be a subset of a vector space V over a field F. Then W is called a **subspace** of V if W is also a vector space over F under the operations inherited from V. Equivalenty,

(a) $0_V\in W$ $\quad(\Leftrightarrow W\neq\emptyset)$

(b) W is closed under addition and scalar multiplication, i.e. $\forall\alpha,\beta\in F$, $w_1,w_2\in W$, $\alpha w_1+\beta w_2\in W$.

□