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) $x*(y*z)=(x*y)*z$ $\forall x,y,z\in G$.

(G2) (identity) there exists a unique $e\in G$ such that $e*x=x=x*e$ $\forall x\in G$.

(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) $x*y=y*x$ $\forall x,y\in G$. □

1.1.2 Example (groups)

(a) $(\mathbb{Z},+)$ is an abelian group. Identity element: 0. Inverse of $n\in\mathbb{Z}$: $-n$.

(b) $(\mathbb{R}\setminus\{0\},\cdot)$ is an abelian group. Identity: 1. Inverse of $x\in\mathbb{R}\setminus\{0\}$: $\frac{1}{x}$

(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) $(\mathbb{Z}_n,\cdot)$ where $\overline{m}_1\cdot\overline{m}_2:=\overline{m_1m_2}$ is not a group in general. For example, $\overline{0}$ has no multiplicative inverse. □

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 $-x$.

(F2) $(F\setminus\{0\},\cdot)$ is an abelian group. The mult. identity is denoted 1. The inverse of $x\in F\setminus\{0\}$ is x^{-1} or $\frac{1}{x}$.

(F3) (distributive law) $a(b+c)=ab+ac$ $\forall a,b,c\in F$. □

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 Bezout's 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) $a\cdot 0=0$ $\forall a\in F$

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

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

1.1.8 Definition The **characteristic** of a field F is the smallest positive integer n for which
$$\underbrace{1+1+\cdots+1}_{n\text{ summands}}=0.$$
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 $\underbrace{\overline{1}+\overline{1}+\cdots+\overline{1}}_{p\text{-times}}=\overline{p}=\overline{0}$. 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. □

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 $\alpha\in F$

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

(b) $(-\alpha)v=-(\alpha v)$

(c) $\alpha 0=0$ (zero vector)

(d) If $\alpha v=0$, then $\alpha=0$ 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
$$F^{n\times m}=\operatorname{Mat}_{n\times m}(F):=\{A=(a_{ij})\mid a_{ij}\in F\ \ i=1,\dots,n,\ j=1,\dots,m\}$$
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
$$F[x]:=\left\{\sum_{i=0}^n a_ix^i\ \middle|\ a_i\in F\ i=0,\dots,n\right\}$$
is a vector space over F

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

(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 function - they 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.

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

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

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 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. Equivalently,

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

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

Remark: Notice that a subspace W of V has the same zero vector as V: say 0_W and 0_V are the zero vectors. then
$$0_W+0_V=0_W=0_W+0_W\Rightarrow 0_V=0_W.$$

1.3.2 Example (Subspaces) Let F be a field.

(a) A vector space V always has two subspaces: $\{0\}$, V.

(b) Let $W\subseteq F^n$ be the set of solutions to the system of m linear equations over F:
$$\begin{aligned}a_{11}x_1+\cdots+a_{1n}x_n&=0\\a_{21}x_1+\cdots+a_{2n}x_n&=0\\&\vdots\\a_{m1}x_1+\cdots+a_{mn}x_n&=0\end{aligned}$$
then W is a subspace of F^n.

(c) Let $F_n[x]$ denote the set of polynomials in $F[x]$ w/ degree $\leq n$. This is a subspace of $F[x]$.

(d) $F^{n\times n}=\operatorname{Mat}_{n\times n}(F)$ has lots of interesting subspaces:

(i) diagonal matrices: $A=(a_{ij})$ w/ $a_{ij}=0$ if $i\neq j$

(ii) symmetric matrices: $A=(a_{ij})$ w/ $a_{ij}=a_{ji}$.

(iii) skew-symmetric matrices: $A=(a_{ij})$ w/ $a_{ij}=-a_{ji}$.

(iv) upper triangular matrices: $A=(a_{ij})$ w/ $a_{ij}=0$ if $i>j$

(v) Magic squares: a square matrix is magic if all its rows, columns, and main diagonals have the same sum:

all have the same sum "magic sum":
(rows) $\sum_{j=1}^n a_{ij}$, $i=1,\dots,n$
(columns) $\sum_{i=1}^n a_{ij}$, $j=1,\dots,n$
(main diag) $\sum_{i=1}^n a_{ii}$
(off diag) $\sum_{i=1}^n a_{i,n+1-i}$

$\begin{bmatrix}1&2&0\\0&1&2\\2&0&1\end{bmatrix}\in Mag_3(\mathbb{Z}_3)$ $\quad\begin{bmatrix}2&7&6\\9&5&1\\4&3&8\end{bmatrix}\in Mag_3(\mathbb{Q})$

The set $Mag_n(F)$ of $n\times n$ magic sq. is a subspace of $F^{n\times n}$.

(e) Subspaces of $\mathbb{R}^n$

$(n=1)$ only $\{0\}$, $\mathbb{R}$

$(n=2)$ $\{0\}$, $\mathbb{R}^2$, and any line through origin.

$(n=3)$ $\{0\}$, $\mathbb{R}^3$, lines through the origin, planes through the origin. □

1.3.3 Proposition (intersection of subspaces) Let V be a vector space over F. The intersection of any collection of subspaces of V is again a subspace of V.

Proof. Exercise. □

1.3.4 Definition Let S be a subset of a vector space V over F. The **span** of S is the subspace
$$\operatorname{Span}(S):=\bigcap_{\substack{W\text{ is a subspace of }V\\ S\subseteq W}}W.$$
By Prop 1.3.3, it is a genuine subspace. Note: $\operatorname{Span}(\emptyset)=\{0\}$. Thus, $\operatorname{Span}(S)$ is the smallest subspace of V that contains S.

1.3.5 Definition Let $v_1,\dots,v_n$ be vectors in a vector space V over F. A **linear combination** of $v_1,\dots,v_n$ is a vector of the form
$$\sum_{i=1}^n\alpha_iv_i=\alpha_1v_1+\cdots+\alpha_nv_n$$
for some $\alpha_1,\dots,\alpha_n\in F$. A linear combination is called **trivial** if $\alpha_1=\alpha_2=\cdots=\alpha_n=0$. □

1.3.6 Proposition (span) Let S be a subset of a vector space V over F. Then
$$\operatorname{Span}(S)=\left\{\sum_{i=1}^n\alpha_iv_i\ \middle|\ n\in\mathbb{N},\ \alpha_1,\dots,\alpha_n\in F,\ v_1,\dots,v_n\in V\right\}$$
That is, $\operatorname{Span}(S)$ is the set of all possible linear combinations of vectors from S.

Proof. (⊆) Let W_0 denote the RHS. To show that $\operatorname{Span}(S)\subseteq W_0$, it suffices to show that W_0 is a subspace of V that contains S. Clearly, $S\subseteq W_0$ and the sum or scalar multiple of elements of W_0 is again an element of W_0. Moreover, $0\in W_0$ by taking a trivial linear combo. So W_0 is a subspace V.

(⊇) Clear that $W_0\subseteq\operatorname{Span}(S)$ since $\operatorname{Span}(S)$ is a subspace.

Note that S could be an infinite set. If $S=\{s_1,\dots,s_n\}$ is finite, then $\operatorname{Span}(S)=\left\{\sum_{i=1}^n\alpha_is_i\ \middle|\ \alpha_i\in F\right\}$. □

1.3.7 Example (span) Consider $S:=\{1,x\}\subseteq F[x]$. Then $\operatorname{Span}S=F_1[x]$. More gen, $\operatorname{Span}\{1,x,\dots,x^n\}=F_n[x]$. □