1 Fields

1.1 Definition

Definition. A **field** is a triple $(F, +, \cdot)$, where F is a set, and $+, \cdot$ are maps:

$$+ : F \times F \to F$$
$$\cdot : F \times F \to F$$

such that:

- C^+: $\forall x, y \in F : x + y = y + x$
- A^+: $\forall x, y, z \in F : (x + y) + z = x + (y + z)$
- N^+: $\exists 0 \in F : \forall x \in F : x + 0 = x$
- I^+: $\forall x \in F : \exists (-x) \in F : x + (-x) = 0$
- $C^\cdot$: $\forall x, y \in F : x \cdot y = y \cdot x$
- $A^\cdot$: $\forall x, y, z \in F : (x \cdot y) \cdot z = x \cdot (y \cdot z)$
- $N^\cdot$: $\exists 1 \in F^* : \forall x \in F : x \cdot 1 = x$
- $I^\cdot$: $\forall x \in F^* : \exists x^{-1} \in F : x \cdot x^{-1} = 1$
- $D^{+,\cdot}$: $\forall x, y, z \in F : x \cdot (y + z) = x \cdot y + x \cdot z$

where $F^* = F \setminus \{0\}$.

1.2 Properties

Claim. *The neutral element with respect to $+$ is unique.*

Proof. Suppose 0 and $0'$ are both neutral elements, then

$$\forall a \in F : a + 0 = a \wedge a + 0' = a$$

Observe that

$$\begin{aligned} 0' &= 0' + 0 && [N^+] \\ &= 0 + 0' && [C^+] \\ &= 0 && [N^+] \end{aligned}$$

Therefore, $0 = 0'$ which makes 0 unique. □

Claim. *For every $a \in F$, there exists a **unique** $(-a) \in F$.*

Proof. Suppose $(-a)$ and $(\sim a)$ satisfy the property of the additive inverse. Then we know that

$$\forall a \in F : a + (-a) = 0 \wedge a + (\sim a) = 0$$

Observe that

$$\begin{aligned} \sim a &= \sim a + 0 && [N^+] \\ &= \sim a + (a + -a) && [I^+] \\ &= (\sim a + a) + -a && [A^+] \\ &= (a + \sim a) + -a && [C^+] \\ &= 0 + -a && [I^+] \\ &= -a + 0 && [C^+] \\ &= -a && [N^+] \end{aligned}$$

Therefore, $\sim a = -a$ which makes $-a$ unique for all a. □

Claim. *The neutral element with respect to $\cdot$ is unique.*

Proof. Suppose 1 and $1'$ are both neutral elements, then

$$\forall a \in F : a \cdot 1 = a \wedge a \cdot 1 = a$$

Observe that

$$\begin{aligned} 1' &= 1' \cdot 1 && [N^{\cdot}] \\ &= 1 \cdot 1' && [C^{\cdot}] \\ &= 1 && [N^{\cdot}] \end{aligned}$$

Therefore, $1 = 1'$ which makes 1 unique. □

Claim. *For every $a \in F^*$, there exists a **unique** $A^{-1} \in F$.*

Proof. Suppose a^{-1} and $a^{\sim 1}$ satisfy the property of the multiplicative inverse. Then we know that

$$\forall a \in F^* : a \cdot a^{-1} = 1 \wedge a \cdot a^{\sim 1} = 1$$

Observe that

$$\begin{aligned} a^{\sim 1} &= a^{\sim 1} \cdot 1 && [N^{\cdot}] \\ &= a^{\sim 1} \cdot (a \cdot a^{-1}) && [I^{\cdot}] \\ &= (a^{\sim 1} \cdot a) \cdot a^{-1} && [A^{\cdot}] \\ &= (a \cdot a^{\sim 1}) \cdot a^{-1} + -a && [C^{\cdot}] \\ &= 1 \cdot a^{-1} && [I^{\cdot}] \\ &= a^{-1} \cdot 1 && [C^{\cdot}] \\ &= a^{-1} && [N^{\cdot}] \end{aligned}$$

Therefore, $a^{\sim 1} = a^{-1}$ which makes a^{-1} unique for all a. □

Claim. $0 \cdot a = 0$

Proof.

$$\begin{aligned} a + 0 \cdot a &= a + a \cdot 0 && [C^{\cdot}] \\ &= a \cdot (1 + 0) && [D^{+,\cdot}] \\ &= a \cdot 1 && [N^{+}] \\ &= a && [N^{\cdot}] \end{aligned}$$

$$a + 0 \cdot a = a \iff 0 \cdot a = 0$$

□

Claim. $\forall a \in F : (-1) \cdot a = -a$

Proof. By definition, $1 + (-1) = 0$. So:

$$\begin{aligned} a \cdot 0 = 0 &\iff a \cdot (1 + (-1)) = 0 && [I^{+}] \\ &\iff a \cdot 1 + a \cdot (-1) = 0 && [D^{+,\cdot}] \\ &\iff a + (-1) \cdot a = 0 && [N^{\cdot}, C^{\cdot}] \\ &\iff (-1) \cdot a = -a && [I^{+}] \end{aligned}$$

□

Claim. $\forall a, b \in F : a \cdot b = 0 \implies a = 0 \vee b = 0$

Proof. Consider two cases:

- $a = 0$, in which case $a \cdot b = 0 \cdot b = 0$ and $0 = 0 \vee b = 0$
- $a \neq 0$, in which case $a \in F^*$ and $a^{-1} \in F^*$ such that $a \cdot a^{-1} = 1$. Observe that $a \cdot b = 0 \iff b = 0 \cdot a^{-1} = 0$, so $a = 0 \vee b = 0$ is true.

□

Example. Examples of fields include:

- $(\mathbb{Q}, \boxplus, \boxdot)$ from the Foundations of Mathematics,
- $(\mathbb{R}, +, \cdot)$ as axiomatically introduced in Analysis I,
- $(\mathbb{C}, \oplus, \odot)$, called the 'complex numbers',
- $(\mathbb{Z}/_{\sim_p}, +, \cdot)$, where p is a prime number,
- 'Galois fields', denoted $GF(p^k)$ where p is a prime number and $k \in \mathbb{N}^*$[1].

1.3 Special case of $(\mathbb{C}, \oplus, \odot)$

Definition. $\mathbb{C} := \mathbb{R} \times \mathbb{R}$

Definition.

$$\oplus : \mathbb{C} \to \mathbb{C}$$
$$(a, b) \oplus (c, d) := (a + c, b + d)$$

Definition.

$$\odot : \mathbb{C} \to \mathbb{C}$$
$$(a, b) \odot (c, d) := (ac - bd, ad + bc)$$

Claim. *$(\mathbb{C}, \oplus, \odot)$ is a field, where $1_{\mathbb{C}} = (1, 0)$ and $0_{\mathbb{C}} = (0, 0)$.*

Proof. Let us prove each law separately; let $(a, b), (c, d), (e, f) \in \mathbb{C}$:

- C^+: $(a, b) \oplus (c, d) = (a + c, b + d) = (c + a, d + b) = (c, d) \oplus (a, b)$
- A^+:

$$\begin{aligned}((a, b) \oplus (c, d)) \oplus (e, f) &= (a + c, b + d) \oplus (e, f) \\ &= (a + c + e, b + d + f) \\ &= (a, b) \oplus (c + e, d + f) \\ &= (a, b) \oplus ((c, d) \oplus (e, f))\end{aligned}$$

- N^+: $(a, b) + 0_{\mathbb{C}} = (a, b) + (0, 0) = (a + 0, b + 0) = (a, b)$
- I^+: Set $-(a, b) := (-a, -b)$. Observe that $(a, b) + (-(a, b)) = (a, b) + (-a, -b) = (a - a, b - b) = (0, 0) = 0_{\mathbb{C}}$
- $C^\cdot$: $(a, b) \odot (c, d) = (ac - bd, ad + bc) = (ca - db, cb + da) = (c, d) \odot (a, b)$
- $A^\cdot$:

$$\begin{aligned}((a, b) \odot (c, d)) \odot (e, f) &= (ac - bd, ad + bc) \odot (e, f) \\ &= (e(ac - bd) - f(ad + bc), f(ac - bd) + e(ad + bc)) \\ &= (ace - bde - adf - bcf, acf - bdf + ade + bce) \\ &= (ace - adf - bcf - bde, acf + ade + bce - bdf) \\ &= (a(ce - df) - b(cf + de), a(cf + de) + b(ce - df)) \\ &= (a, b) \odot (ce - df, cf + de) \\ &= (a, b) \odot ((c, d) \odot (e, f))\end{aligned}$$

[1] Not on the exam

- $N^{\cdot}$: $(a,b)\cdot 1_{\mathbb{C}} = (a,b)\cdot(1,0) = (a\cdot 1 - b\cdot 0, a\cdot 0 + b\cdot 1) = (a,b)$
- $I^{\cdot}$: Set $(a,b)^{-1} := (a\cdot(a^2+b^2)^{-1}, -b\cdot(a^2+b^2)^{-1})$ (using the convention that $x^n = \underbrace{x\cdot x\cdot \ldots \cdot x}_{n \text{ times}}$).

  Observe that:

$$\begin{aligned}&(a,b)\odot(a\cdot(a^2+b^2)^{-1}, -b\cdot(a^2+b^2)^{-1})\\ &= ((a^2+b^2)\cdot(a^2+b^2)^{-1}, ab\cdot(a^2+b^2)^{-1} - ab\cdot(a^2+b^2)^{-1})\\ &= (1,0)\end{aligned}$$

- $D^{+,\cdot}$:

$$\begin{aligned}(a,b)\odot((c,d)\oplus(e,f)) &= (a,b)\odot(c+e,d+f)\\ &= (a(c+e)-b(d+f), a(d+f)+b(c+e))\\ &= (ac+ae-bd-bf, ad+af+bc+be)\\ &= (ac-bd+ae-bf, ad+bc+af+be)\\ &= (ac-bd, ad+bc)\oplus(ae-bf, af+be)\\ &= ((a,b)\odot(c,d))\oplus((a,b)\odot(e,f))\end{aligned}$$

□

Definition.

$$\begin{aligned}\text{com} : \mathbb{R} &\to \mathbb{C}\\ a &\mapsto (a,0)\end{aligned}$$

Theorem. com *is injective.*

Proof. Given $\text{com}(a) = \text{com}(b)$, we know that $(a,0) = (b,0)$, and by the theorem of ordered pairs, we know that $a = b \wedge 0 = 0 \implies a = b$, so com is injective. □

Notice the following facts:

- $\text{com}(a+b) = (a+b,0) = (a,0)\oplus(b,0) = \text{com}(a) + \text{com}(b)$
- $\text{com}(a\cdot b) = (a\cdot b, 0) = (a\cdot b - 0\cdot 0, a\cdot 0 + 0\cdot b) = (a,0)\odot(b,0) = \text{com}(a)\odot\text{com}(b)$
- $\text{com}(1_{\mathbb{R}}) = 1_{\mathbb{C}}$

Because of this, com is an embedding of $\mathbb{R}$ into $\mathbb{C}$ (as their fields).

Remark. Traditional notation:

1. $i := (0,1)$
2. com will be written in 'invisible ink', which is sort of justified because com is an embedding

Fun facts:

1. $i^2 := i\odot i = (0,1)\odot(0,1) = (0\cdot 0 - 1\cdot 1, 0\cdot 1 + 1\cdot 0) = (-1,0) = \text{com}(-1)$, and with invisible chalk, $i^2 = -1$.
2. $\forall z\in\mathbb{C} : \exists a,b\in\mathbb{R} : z = a + bi$. Proof: rather obviously, for those a, b, $z = (a,b) = (a,0)\oplus(0,b) = (a,0)\oplus i\odot(b,0) = \text{com}(a) + i\,\text{com}(b)$ which is then $a + ib$.
3. $(a,b)\cdot i = (a,b)\cdot(0,1) = (a\cdot b - b\cdot 1, a\cdot 1 + b\cdot 0) = (-b,a)$

1.4 Finite fields

Definition. A field $(F, +, \cdot)$ is called **finite** if and only if F is a finite set.

Definition. $\text{ord}(F) := |F|$

Definition. $\text{char}(F) :=$ smallest number of times that we must add 1_F to itself to arrive at 0_F. In other words, $\underbrace{1_F + 1_F + \ldots + 1_F}_{\text{char}(F) \text{ times}} = 0_F$

Remark. The characteristic of an infinite field has been redefined to 0.

Example. Let p be a prime number, then define $\sim_p \subseteq \mathbb{Z} \times \mathbb{Z}$ such that

$$a \sim_p b :\iff \exists n \in \mathbb{Z} : a - b = n \cdot p$$

Claim. *$\sim_p$ is an equivalence relation.*

Proof. Let us prove all conditions of an equivalence relation:

- $\sim_p$ is reflexive: let $a \in \mathbb{Z}$, then $a \sim_p a \iff \exists n \in Z : a - a = n \cdot p \iff 0 = n \cdot p$, let $n = 0$ and thus $0 = 0$ which is a tautology
- $\sim_p$ is symmetric: let $a, b \in \mathbb{Z}$, then if $a \sim_p b$, we can find an n such that $a - b = n \cdot p$. To prove symmetry we should prove that there exists some $m \in \mathbb{Z}$ such that $b - a = m \cdot p$. Let $m = -n$. Then $b - a = -n \cdot p$ and thus $a - b = n \cdot p$, which is true
- $\sim_p$ is transitive: let $a, b, c \in \mathbb{Z}$. Assume that $a \sim_p b$ and $b \sim_p c$, e.g. we can find n, m such that $a - b = n \cdot p$ and $b - c = m \cdot p$. Adding both equations we find that $a - c = (n + m) \cdot p$, so $a \sim_p c$.

□

Definition.

$$\boxplus : \mathbb{Z}/_{\sim_p} \times \mathbb{Z}/_{\sim_p} \to \mathbb{Z}/_{\sim_p}$$
$$[a] \boxplus [b] := [a + b]$$

Claim. *$\boxplus$ is well-defined.*

Proof. Suppose $a, b, a', b' \in \mathbb{Z}$, $a \sim_p a'$ and $b \sim_p b'$. Thus, $a - a' = n \cdot p$ and $b - b' = m \cdot p$. Now, $[a] \boxplus [b] = [a + b] = [a' + n \cdot p + b' + m \cdot p] = [a' + b'] = [a'] \boxplus [b']$. □

Definition.

$$\boxdot : \mathbb{Z}/_{\sim_p} \times \mathbb{Z}/_{\sim_p} \to \mathbb{Z}/_{\sim_p}$$
$$[a] \boxdot [b] := [ab]$$

Claim. *$\boxdot$ is well-defined.*

Proof. Suppose $a, b, a', b' \in \mathbb{Z}$, $a \sim_p a'$ and $b \sim_p b'$. Thus, $a - a' = n \cdot p$ and $b - b' = m \cdot p$. Now, $[a] \boxdot [b] = [ab] = [(a' + n \cdot p)(b' + m \cdot p)] = [a'b' + (\ldots) \cdot p] = [a'b'] = [a'] \boxdot [b']$. □

2 Vector spaces over a field

2.1 Definition of the key object of study

Definition. Let $(F, +, \cdot)$ be a field. Then a **vector space over** F (alternatively called an F**-vector space**) is a triple $(V, \oplus, \odot)$, where V is a set, and

$$\oplus : V \times V \to V$$

$$\otimes : F \times V \to V$$

called **vector addition** and **scaling** respectively, such that:

- $C^{\oplus}$: $\forall v, w \in V : v \oplus w = w \oplus v$
- $A^{\oplus}$: $\forall, u, v, w \in V : (u \oplus v) \oplus w = u \oplus (v \oplus w)$
- $N^{\oplus}$: $\exists 0_V \in V : \forall v \in V : v \oplus 0_V = v$
- $I^{\oplus}$: $\forall v \in V : \exists (-v) \in V : v \oplus (-v) = 0_V$
- $A^{\cdot,\odot}$: $\forall \lambda, \mu \in F : \forall v \in V : \lambda \odot (\mu \odot v) = (\lambda \cdot \mu) \odot v$
- $D^{\odot,\oplus}$: $\forall \lambda \in F : \forall v, w \in V : \lambda \odot (v \oplus w) = \lambda \odot v \oplus \lambda \odot w$
- $D^{+,\oplus,\odot}$: $\forall \lambda, \mu \in F : \forall v \in V : (\lambda + \mu) \odot v = \lambda \odot v \oplus \mu \odot v$
- $U^{\odot}$: $\forall v \in V : 1_F \odot v = v$

Remark. Obviously, **CANIADDU** require extensive mutual relationships between $(F, +, \cdot, V, \oplus, \odot)$, but there are still many different concrete implementations/examples of this structure.

Remark. A case of jargon: people really like to say 'Let v be a vector'. Though, without context, this statement does not make sense and thus there is no such thing as **a** vector. Instead, one should say 'Let v be an element of the set V that underlies the vector space $(V, \oplus, \odot)$'.

Remark. (hold your horses, this one is rare) Applications!!! Is …a vector?

- Is a **position vector** a vector? No.
- Is a **velocity vector** a vector? Yes!
- Is an **acceleration vector** a vector? Yes!
- Is an **angular momentum vector** a vector? No.
- Is a **wave vector** a vector? No.
- Is a **momentum vector** a vector? No.
- Is a **gradient vector** a vector? No.

Remark. The same structure but over a ring $(R, +, \cdot)$ is called an R**-module**.

Theorem.

- 0_V *is unique.*
- $(-v)$ *is the unique additive inverse of* v *for all* $v \in V$*.*
- $0_F \odot v = 0_V$*.*
- $(-1_F) \odot v = (-v)$ *for all* $v \in V$*.*
- $\lambda \odot 0_V = 0_V$ *for all* $v \in V$

Proof. The first two items are precisely analogous to the theorems for a field (since they have identical laws with simply different symbols). The next two items are similar to the proofs for a field, but sometimes use another law. The last one, though, is not so trivial though.
Let $v \in V$, $\lambda \in F$. Consider two cases:

- **Case 1**: $\lambda = 0_F$, in which case $0_F \odot 0_V = 0_V$ by the third property of this theorem.
- **Case 2**: $\lambda \neq 0_F$. Consider the expression $v \oplus \lambda \odot 0_V$. We would like to show that this is equal to v, thus $\lambda \odot 0_V = 0_V$.

$$\begin{aligned}
v \oplus \lambda \odot 0_V &= 1_F \odot v \oplus \lambda \odot 0_V && [U^{\odot}] \\
&= (\lambda \cdot \lambda^{-1}) \odot v \oplus \lambda \odot 0_V && [I^{\cdot}] \\
&= \lambda \odot (\lambda^{-1} \odot v) \oplus \lambda \odot 0_V && [A^{\cdot,\odot}] \\
&= \lambda \odot (\lambda^{-1} \odot v \oplus 0_V) && [D^{\odot,\oplus}] \\
&= \lambda \odot (\lambda^{-1} \odot v) && [N^{\oplus}] \\
&= (\lambda \cdot \lambda^{-1}) \odot v && [A^{\cdot,\odot}] \\
&= 1_F \odot v && [I^{\cdot}] \\
&= v && [U^{\odot}]
\end{aligned}$$

□

Remark. Notice that we use a different proof technique/idea than we usually do: here we attempt to show unique properties.

Example. Let $V := \{\clubsuit\}$ with an arbitrary field $(F, +, \cdot)$.

$$\oplus : V \times V \to V$$

$$\clubsuit \oplus \clubsuit := \clubsuit$$

$$\odot : F \times V \to V$$

$$\lambda \odot \clubsuit := \clubsuit$$

CANI inherited from definition of $\oplus, \odot$, set $0_V := \clubsuit$, set $(-\clubsuit) := \clubsuit$, so all laws work.

Example. $V := F$, $v \oplus w := v + w$, $v \odot w := v \cdot w$. 'F is an F-vector space'.

Example. '$\mathbb{C}$ is an $\mathbb{R}$-vector space'. Choose $V := \mathbb{C}$, $F := \mathbb{R}$, $v \oplus w := v +_{\mathbb{C}} w$, $\lambda \odot v := \mathrm{com}(\lambda) \cdot_{\mathbb{C}} v$.

Example. For all $n \in N$, take $F := \mathbb{R}$ and

$$V := P^n_{\mathbb{R}} := \left\{ p \in \mathcal{P}(\mathbb{R} \times \mathbb{R}) \;\middle|\; \left(p(x) := \sum_{i=0}^{n} \lambda_i \cdot x^i \right) \wedge \lambda_0, \lambda_1, \ldots, \lambda_n \in \mathbb{R} \right\}$$

$$\oplus : V \times V \to V$$

$$(p \oplus q)(x) := p(x) + q(x) \quad [2]$$

$$\odot : \mathbb{R} \times V \to V$$

$$(\lambda \odot q)(x) := \lambda \cdot q(x)$$

Example. $V := F^n$.

$$(f_1, \ldots, f_n) \oplus (g_1, \ldots, f_n) := (f_1 + g_1, \ldots, f_n + g_n)$$

$$\lambda \odot (f_1, \ldots, f_n) := (\lambda \cdot f_1, \ldots, \lambda \cdot f_n)$$

3 Morphisms

In general, a morphism is a map that preserves the structure of some mathematical object. In linear algebra, we will therefore look at the morphisms of vector spaces.

[2] By the way, this type of definition is called a 'pointwise definition of a map'

3.1 Definitions

Throughout the entire lecture, it will be convenient to define $(V, \oplus, \odot)$ and $(W, \boxplus, \boxdot)$ to be F-vector spaces.

Definition. A map $\phi : V \to W$ is called a **vector space homomorphism** if for all $v, v' \in V$ and for all $\lambda \in F$,

$$\phi \text{ is linear } :\iff \begin{cases} \phi(v \oplus v') = \phi(v) \boxplus \phi(v'), & \text{(additivity)} \\ \phi(\lambda \odot v) = \lambda \boxdot \phi(v) & \text{(scalability).} \end{cases}$$

Remark. Other terminology for the same definition (depending on the field of maths): 'linear map' and 'linear transformation'[3].

Terminology (to scare little children):

- **mono**morphism: an injective homomorphism
- **epi**morphism: a surjective homomorphism
- **iso**morphism: a bijective homomorphism
- **endo**morphism: a homomorphism $\phi : V \to V$ (where the 'extra structure' that is considered in the domain and codomain is also identical)
- **auto**morphism: a bijective endomorphism

3.2 Examples

Example. Pick $a, b, c, d \in \mathbb{R}$. Then define

$$\phi : \mathbb{R}^2 \to \mathbb{R}^2$$
$$(x, y) \mapsto (ax + by, cx + dy)$$

So ϕ, if it is a homomorphism, is an endomorphism. Check additivity:

$$\begin{aligned} \phi((x,y) \oplus (u,v)) &= \phi((x+u, y+v)) && [\oplus] \\ &= (a(x+u) + b(y+v), c(x+u) + d(y+v)) && [\phi] \\ &= (ax + au + by + bv, cx + cu + dy + dv) && [D^{+,\cdot}] \\ &= (ax + by, cx + dy) \oplus (au + bv, cu + dv) && [A^+, C^+, \oplus] \\ &= \phi((x,y)) \oplus \phi((u,v)) && [\phi] \end{aligned}$$

Check scalability:

$$\begin{aligned} \phi(\lambda \odot (x,y)) &= \phi((\lambda x, \lambda y)) && [\odot] \\ &= (a\lambda x + b\lambda y, c\lambda x + d\lambda y) && [\phi] \\ &= (\lambda ax + \lambda by, \lambda cx + \lambda dy) && [C^{\cdot}, A^{\cdot}] \\ &= (\lambda(ax + by), \lambda(cx + dy)) && [D^{+,\cdot}] \\ &= \lambda \odot (ax + by, cx + dy) && [\odot] \\ &= \lambda \odot \phi((x,y)) && [\phi] \end{aligned}$$

Thus ϕ is homo[4] and endo.

Remark. Something something devil says: the most general is $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \dagger \begin{bmatrix} x \\ y \end{bmatrix} = \dots$

[3] Looks like we are finally *doing* something

[4] Yeah, this definitely generated some laughs in lecture

Example. Define

$$C^\infty(\mathbb{R}) := \{(f : \mathbb{R} \to \mathbb{R}) \in \mathcal{P}(\mathbb{R} \times \mathbb{R}) \mid \text{'f is arbitrarily often differentiable'}\}$$

$C^\infty(\mathbb{R})$ has a nickname, namely 'the set of all smooth functions'. Let us now define an $\mathbb{R}$-vector space on it.

$$\begin{aligned} \oplus &: C^\infty(\mathbb{R}) \times C^\infty(\mathbb{R}) \to C^\infty(\mathbb{R}) \\ (f \oplus g)(x) &:= f(x) + g(x) \\ \odot &: \mathbb{R} \times C^\infty(\mathbb{R}) \to C^\infty(\mathbb{R}) \\ (\lambda \odot g)(x) &:= \lambda \cdot g(x) \end{aligned}$$

Now, $CANI$ are satisfied by fact that $\oplus$ is inherited from the field $\mathbb{R}$. Let us now prove $ADDU$.

- $A^{\cdot,\odot}$:

$$\begin{aligned} (\lambda \odot (\mu \odot f))(x) &= \lambda \cdot (\mu \cdot f(x)) && [\odot] \\ &= (\lambda \cdot \mu) \cdot f(x) && [A^{\cdot}] \\ &= ((\lambda \cdot \mu) \odot f)(x) && [\odot] \end{aligned}$$

  Therefore $\lambda \odot (\mu \odot f) = (\lambda \cdot \mu) \odot f$.

- $D^{\odot,\oplus}$:

$$\begin{aligned} (\lambda \odot (f \oplus g))(x) &= \lambda \cdot (f(x) + g(x)) && [\oplus, \odot] \\ &= \lambda \cdot f(x) + \lambda \cdot g(x) && [D^{+,\cdot}] \\ &= (\lambda \odot f)(x) + (\lambda \odot g)(x) && [\odot] \end{aligned}$$

  Therefore $\lambda \odot (f \oplus g) = \lambda \odot f \oplus \lambda \odot g$.

- $D^{+,\oplus,\odot}$:

$$\begin{aligned} ((\lambda + \mu) \odot v)(x) &= (\lambda + \mu) \cdot v(x) && [\odot] \\ &= v(x) \cdot (\lambda + \mu) && [C^{\cdot}] \\ &= v(x) \cdot \lambda + v(x) \cdot \mu && [D^{+,\cdot}] \\ &= \lambda \cdot v(x) + \mu \cdot v(x) && [C^{\cdot}] \\ &= (\lambda \odot v)(x) + (\mu \odot v)(x) && [\odot] \end{aligned}$$

  Therefore $(\lambda + \mu) \odot v = \lambda \odot v \oplus \mu \odot v$

- $U^{\odot}$: $(1_\mathbb{R} \odot v)(x) = 1_\mathbb{R} \cdot v(x) = v(x)$, therefore $1_\mathbb{R} \odot v = v$.

Thus $(C^\infty(\mathbb{R}), \oplus, \odot)$ is an $\mathbb{R}$-vector space. Now define

$$\begin{aligned} &' : C^\infty(\mathbb{R}) \to C^\infty(\mathbb{R}) \\ &\underbrace{f \to f'}_{\text{as defined in analysis later}} \end{aligned}$$

By the (thus far unproven and undefined) linearlity of the derivative operator, we know that $'$ is a homo.

Example. Define $\mathbb{R}_+ := \{r \in \mathbb{R} \mid r > 0\}$, and equip it with the maps

$$\begin{aligned} \oplus &: \mathbb{R}_+ \times \mathbb{R}_+ \to \mathbb{R}_+ \\ r \oplus s &:= r \cdot s \\ \odot &: \mathbb{R} \times \mathbb{R}_+ \to \mathbb{R}_+ \\ \lambda \odot r &:= r^\lambda \end{aligned}$$

As seen on the problem sheet, $\mathbb{R}_+^n$ for $n \in \mathbb{N}^*$ equipped with similar maps is an $\mathbb{R}$-vector space. In this case, $n = 1$, $(R_+, \oplus, \odot)$ is also an $\mathbb{R}$-vector space. Now consider the map $\log : \mathbb{R}_+ \to \mathbb{R}$. Notice that this is a homo in our vector space (what do you mean high school teachers, that log is not a linear map)!

- log is 'additive': $\log(r \oplus s) = \log(r \cdot s) = \log(r) + \log(s) = \log(r) \oplus \log(s)$.
- log is 'scaling': $\log(\lambda \odot r) = \log(r^\lambda) = \lambda \cdot \log(r)$.

3.3 Kernel and image of a homomorphism

Let $\phi : V \to W$ such that it is a homomorphism.

Definition. The **kernel** of ϕ with respect to the related vector spaces is the set

$$\ker \phi := \{v \in V \mid \phi(v) = 0_W\}$$

Definition. The **image** of ϕ with respect to the related vector spaces is the set

$$\operatorname{im} \phi := \{w \in W \mid \exists v \in V : \phi(v) = w\}$$

Theorem. *For any homomorphism ϕ,*

- $0_V \in \ker \phi$
- $v, v' \in \ker \phi \implies v \oplus v' \in \ker \phi$
- $\forall \lambda \in F : v \in \ker \phi \implies \lambda \odot v \in \ker \phi$

In other words, ker *is a* ***vector subspace*** *of* $(V, \oplus, \odot)$.

Proof. Done in lecture and not terribly interesting to copy here. □

Theorem. *ϕ is a monomorphism if and only if* $\ker \phi = \{0_V\}$.

Proof. Firstly, assume ' $\implies$ ', so we already know that ϕ is injective. By a previous fact we also know that $0_V \in \ker \phi \iff \phi(0_V) = 0_W$. Suppose there exists another $v \in \ker \phi$. This implies that $\phi(v) = 0_W$. By transitivity of $=$ we know that $\phi(v) = \phi(0_V)$. But ϕ is injective, so $v = 0_V$. Thus there is only a single unique element in $\ker \phi$, namely 0_V.

Now, assume ' $\impliedby$ ', so we already know that $\ker \phi = \{0_V\}$. To show injectivity we can assume $\phi(v) = \phi(v')$. Thus $\phi(v) \boxplus (-\phi(v') = 0_W$. Because ϕ is a homo, $\phi(v \oplus (-v')) = 0_W$, so $v \oplus (-v') \in \ker \phi$. Then $v \oplus (-v') = 0_V$ because there is only one element in $\ker \phi$. And so $v = v'$, which means ϕ is injective. □

4 Vector subspaces, quotient spaces and FTH

So far, we have defined certain structures, and finally we will now use those structures to induce new structures.

Remark. Inducing new structures on existing structures is a recurrent theme in mathematics.

Throughout this section, we shall consider:

- Let $(F, +, \cdot)$ be a field.
- Let $(V, \oplus, \odot)$ be an F-vector space.
- Let $(W, \boxplus, \boxdot)$ be an F-vector space.

4.1 Subspaces

Note: a **space** filosophically is a set with some additional stucture.

Definition. A subset $U \subseteq V$ is called a **subspace** of the vector space $(V, \oplus, \odot)$ if:

(a) $U \neq \varnothing$

(b) $\forall v, v' \in U : v \oplus v' \in U$

(c) $\forall \lambda \in F : \forall v \in U : \lambda \odot v \in U$

To denote such a subspace, we write $U \leqslant V$.

Corollary. *Let $U \leqslant V$, then $0_V \in U$.*

Proof. $U \neq \varnothing \implies \exists v \in U : 0_F \odot v \in U \implies 0_F \in U$ □

Example. (a) $\phi : V \to W$, where ϕ is a homo. By an earlier theorem, $\ker \phi \leqslant V$.

(b) $\operatorname{im} \phi \leqslant W$ (which we will show on the problem sheet)

(c) $\{0_V\} \leqslant V$ (trivially almost)

(d) $V \leqslant V$

Theorem. *Let C be a set that contains as elements only vector subspaces of $(V, \oplus, \odot)$. In other words*

$$X \in C \iff X \leqslant V$$

Then $\bigcap C \leqslant V$.

Proof. Let us prove all properties of the claim $\bigcap C \leqslant V$.

(a) $\bigcap C$ must not be $\varnothing$: $\forall X \in C : 0_V \in X \implies 0_V \in C$.

(b) Suppose $v, v' \in \bigcap C$. Thus $\forall X \in C : v \in X \wedge v' \in X$. Since $X \leqslant V$, $v \oplus v' \in X$ for all X, so $v \oplus v' \in \bigcap X$.

(c) Suppose $\lambda \in F, v \in \bigcap C$. Thus $\forall X \in C : v \in X$. Since $X \leqslant V$, $\lambda \odot v \in X$ for all X, so $\lambda \odot v \in \bigcap X$.

□

Definition. Let $S \subseteq V$ (yes, any subset of V). Then S induces a subspace $\operatorname{span}(S)$ defined as follows:

$$\operatorname{span}(S) := \bigcap \{U \in \mathcal{P}(V) \mid U \leqslant V \wedge S \subseteq U\}$$

Shorthand:

$$\operatorname{span}(S) := \bigcap \{U \leqslant V \mid S \subseteq U\}$$

In human language: 'The span of S is the intersection of all subspaces of V that contain S as a subset'.

Claim. $\operatorname{span}(S)$ *is indeed a subspace.*

Proof. By the theorem, an intersection of a set of subspaces of V is a subspace of V. □

Remark.

- Your choice of S may as well be infinite (redundant remark). Recall what it means to have an infinite set: you can find another set such that it is a proper subset that is nonetheless set theoretically isomorphic:
$$S \text{ is infinite} :\iff \exists T \subset C : T \cong_{\text{set}} S$$
- Spans will come back later, but we will not use them for now.
- $\operatorname{span}(\varnothing) = \{0_F\}$ since it will be the intersection of all subspaces, including $\{0_F\}$.

4.2 Quotient vector spaces

Definition. Let $U \leqslant V$, then define on U the relation $\sim \subseteq V \times V$:

$$v \sim_U v' :\iff v - v' \in U$$

Claim. $\sim_U$ *is an equivalence relation.*

Proof.

- Reflexivity: $v \sim_U v \iff v - v \in U \iff 0_V \in U$, which is true by definition of a vector subspace.

- Symmetry:

$$\begin{aligned} v \sim_U v' &\iff v - v' \in U \\ &\iff v \oplus (-v') \in U \\ &\implies -1_F \odot (v \oplus (-v')) \in U \\ &\iff -1_F \odot v \oplus -1_F \odot (-v')) \in U \\ &\iff (-v) \oplus v' \in U \\ &\iff v' \oplus (-v) \in U \\ &\iff v' - v \in U \\ &\iff v' \sim_U v \end{aligned}$$

- Transitivity: Assume $u \sim_U v$ and $v \sim_U w$. Want to show: $u \sim_U w$. By the assumptions, we know that $u - v \in U$ and $v - w \in U$. By one of the properties of a vector subspace, we can add two elements in U to find a new one in U: $u - v + v - w \in U \iff u - w \in U \iff u \sim_U w$.

□

Remark. You can read this definition as saying 'we define an equivalence relation on a subspace, which induces a quotient set $V/_{\sim_U}$'. Notation: we write this set as $V/_U$.

Definition. Let $U \leqslant V$, then equip $V/_U$ with:

$$\begin{gathered} \oplus : V/_U \times V/_U \to V/_U \\ [v] \oplus [v'] := [v \oplus v'] \\ \odot : F \times V/_U \to V/_U \\ \lambda \odot [v] := [\lambda \odot v] \end{gathered}$$

Claim. *$\oplus$ and $\odot$ are well-defined. (no proof)*

Theorem. *Let $U \leqslant V$. Then $(V/_U, \oplus, \odot)$ is an F-vector space, called the **quotient vector space** of V with respect to U.*

Proof. I will do this later. □

Definition.

$$\begin{gathered} \pi : V \to V/U \\ v \mapsto [v] \end{gathered}$$

is called **a projection map** or **the canonical quotient projection** of V onto the quotient space of U.

Claim. *π is a homomorphism.*

Proof. Check whether the properties of a vector homomorphism hold:

- $\pi(v \oplus w) = [v \oplus w] = [v] \oplus [w]$
- $\pi(\lambda \odot v) = [\lambda \odot v] = \lambda \odot v$

□

Definition. Let $S \leqslant W$. Then define $\iota : S \to W$ such that $s \mapsto s$ (since $S \subseteq W$). ι is called the **canonical inclusion map**.

Claim. *ι is a monomorphism. That is, ι is a vector space homomorphism and is injective.*

Proof. The properties of a homomorphism hold trivially because ι is essentially an indentity map. Furthermore, since the identity map is injective, ι is also injective. Note that while the identity map is also surjective, this is not neccesarily true for ι, since its domain and codomain differ. □

4.3 Fundamental theorem on homomorphisms

Theorem. *Let $\phi : V \to W$ be a homomorphism. Then*

$$V/_{\ker \phi} \cong_{vec} \operatorname{im} \phi$$

Proof. We would like to find some isomorphism ρ. Let

$$\rho : V/_{\ker \phi} \to \operatorname{im} \phi$$

$$[v] \mapsto \phi(v)$$

First of all, let us prove that ρ is a homomorphism.

- $\rho([v] \boxplus [w]) = \rho([v \oplus w]) = \phi(v \oplus w) = \phi(v) \boxplus \phi(w) = \rho([v]) \boxplus \rho([w])$
- $\rho(\lambda \boxdot [v]) = \rho([\lambda \odot v]) = \phi(\lambda \odot v) = \lambda \boxdot \phi(v) = \lambda \boxdot \rho([v])$

Surjectivity is almost trivial, so what is left to prove is the ρ is injective. Assume $\rho([v]) = \rho([v'])$. Then $\phi(v) = \phi(v') \iff \phi(v) - \phi(v') = 0_W \iff \phi(v - v') = 0_W$. Therefore, $v - v' \in \ker \phi$ and thus $v \sim v'$, thus $[v] = [v']$. □

5 Dual of a vector space and multilinear maps

Throughout the lecture, we use $(V, +, \cdot)$ and $(W, +, \cdot)$ as F-vector spaces. Yes, we start dropping the decorations now as it should be 'clear'. We shall derive a comprehensive taxonomy later of linear structures over fields.

5.1 Dual of a vector space

Definition. Define the set

$$V^* := \operatorname{Hom}(V, F) := \{(\phi : V \to F) \in \mathcal{P}(V \times F) \mid \phi \text{ is a homo}\}$$

Furthermore define two maps (pointwise, definition omitted):

- $\oplus : V^* \times V^* \to V^*$
- $\odot : F \times V^* \to V^*$

Theorem. $(V^*, \oplus, \odot)$ *constitutes an F-vector space, called the* ***dual vector space*** *of V.*

Proof. Cumbersome exercise, do it. □

Example. Recall that $C^\infty(\mathbb{R})$ as an $\mathbb{R}$-vector space and a homo $' : C^\infty(\mathbb{R}) \to C^\infty(\mathbb{R})$ defined by $f \mapsto f'$. Now consider the map $'(0) : C^\infty(\mathbb{R}) \to \mathbb{R}$ defined by $f \mapsto f'(0)$, so $'(0) \in C^\infty(\mathbb{R})^*$. Well, as long as it is a homomorphism. Well, it is, because of rules of differentiation to be defined in Analysis.

Example. Consider a map $\int_0^1 : P^n_{\mathbb{R}} \to \mathbb{R}$. How should we define this? Consider that $f \in P^n_{\mathbb{R}}$ means that $f : \mathbb{R} \to \mathbb{R}$ of the form $x \mapsto \sum_{i=0}^n \lambda_i \cdot x^i$. By high-school calculus, we can compute its integral:

$$\begin{aligned}\int_0^1 \sum_{i=0}^n \lambda_i \cdot x^i \, dx &= \sum_{i=0}^n \int_0^1 \lambda_i \cdot x^i \, dx \\ &= \sum_{i=0}^n \frac{\lambda_i}{i+1} \cdot x^{i+1} \Big|_0^1 \\ &= \sum_{i=0}^n \frac{\lambda_i}{i+1}\end{aligned}$$

So it makes sense to define $\int_0^1 := \sum_{i=0}^n \frac{\lambda_i}{i+1}$. Sadly this no longer depends on the original polynomial so this will not work, sadly.

Remark. Terminology: an element of the set underlying the dual space of a given vector space is usually called either,

- a dual vector, or
- a covector.

Again, the same remarks apply as for the terminology of 'vector'.

5.2 Dual of a homomorphism

Definition. Let $\xi : V \to W$ be a homomorphism. Then define the following map:

$$\xi^* : W^* \to V^*$$

$$\alpha \mapsto \alpha \circ \xi$$

Such a map ξ^* is called the **dual map** of ξ.

Example. Consider the homomorphism

$$\ln : \mathbb{R}_+ \to \mathbb{R}$$

Well, notice that $\ln^*$ is defined by $\alpha \mapsto \alpha \circ \ln$. But $\alpha \in \mathbb{R}^*$ where $\mathbb{R}$ acts as an $\mathbb{R}$-vector space, so $\alpha : \underbrace{\mathbb{R}}_{\text{as a v.s.}} \to \underbrace{\mathbb{R}}_{\text{as a field}}$ and linear. But (as can be shown, probably), the only form that satisfies linearity is $\alpha(x) := a \cdot x$.

5.3 Multilinear maps

Definition. Let $A_1, \ldots, A_N$, each equipped with their own $(+, \cdot)$, all be F-vector spaces and $(V, +, \cdot)$ as well. Then a map

$$\phi : (A_1 \times \ldots \times A_N) \to V$$

is called **multilinear** if:

- ϕ is **additive separately** (in each Cartesian factor), that is

$$\begin{aligned}
\phi(a_1 + a_1', \ldots, a_N) &= \phi(a_1, \ldots, a_N) + \phi(a_1', \ldots, a_N) \\
\phi(a_1, a_2 + a_2', \ldots, a_N) &= \phi(a_1, a_2, \ldots, a_N) + \phi(a_1, a_2', \ldots, a_N) \\
&\vdots \\
\phi(a_1, \ldots, a_N + a_N') &= \phi(a_1, \ldots, a_N) + \phi(a_1, \ldots, a_N')
\end{aligned}$$

- ϕ is **scaling separately** (in each Cartesian factor), that is

$$\begin{aligned}
\phi(\lambda \cdot a_1, \ldots, a_N) &= \lambda \cdot \phi(a_1, \ldots, a_N) \\
\phi(a_1, \lambda \cdot a_2, \ldots, a_N) &= \lambda \cdot \phi(a_1, a_2, \ldots, a_N) \\
&\vdots \\
\phi(a_1, \ldots, \lambda a_N) &= \lambda \cdot \phi(a_1, \ldots, a_N)
\end{aligned}$$

Example. (a) linear maps are multilinear (trivial, set $N = 1$),

(b) bilinear maps are such maps where $N = 2$,

(c) Define the 'pseudo inner-product'

$$g : V \times V \to F$$

which preserves symmetry, e.g. $\forall v, v' \in V : g(v, v') = g(v', v)$.

5.4 Tensors

Definition. A (p, q)**-tensor** over V is a multilinear map of the form

$$T : \underbrace{V^* \times \dots V^*}_{p \text{ times}} \times \underbrace{V \times \dots V}_{q \text{ times}} \to F$$

6 Bases and dimension

6.1 Definitions

Definition. Let $G \subseteq V$, $(V, \oplus, \odot)$ as F-vector space.

(a) G is called a **generating set** of said vector space if $\operatorname{span}(G) = V$.

(b) G is called a **linearly independent set** of said vector space if for any finite subset $\{l_1, \dots, l_n\} \subseteq G$ we have that the homomorphism

$$\sigma : F^n \to V$$
$$(\lambda_1, \dots, \lambda_n) \mapsto \bigoplus_{i=1}^{n} \lambda_i \odot l_i$$

has **trivial kernel**, that is, $\ker \sigma = \{0_{F^n}\}$.

(c) G is called a (Hamel) **basis** of said vector space if it is both a generating set and a linearly independent set of the vector space.

Remark. If $0_V \in G$, can such a choice for $G \subseteq V$ be a linearly independent set?

Claim. *Let $G \subseteq V$. Then if $0_V \in G$, G is not linearly independent.*

Proof. Consider the finite subset $\{0_V\} \subseteq G$. Then we have $n = 1$ and our map looks like:

$$\sigma : F \to V$$

$$\lambda \mapsto \lambda \odot 0_V = 0_V$$

So $\forall \lambda \in F : \sigma(\lambda) = 0_V$, so $\ker \sigma = F$, which is not trivial. □

Remark. If G is finite, then we can take $G \subseteq G$ to 'collapse' the definition of G being linearly independent to (the following, where we take $G := \{g_1, \dots, g_d\}$): G is linearly independent if **the** homomorphism

$$\sigma : F^d \to V$$

$$(\lambda_1, \dots, \lambda_d) \mapsto \bigoplus_{i=1}^{d} \lambda^i \odot g_i$$

has trivial kernel.

Remark. Every vector space has a generating set. Well, take $V \subseteq V$, then

$$\operatorname{span}(V) = \bigcap \{U \in \mathcal{P}(V) \mid U \leq V \wedge V \subseteq U\} = \bigcap \{U \in \mathcal{P}(V) \mid U = V\} = V$$

so V is a generating set for V.

Example. The set $\{(0, 0, 1), (0, 1, 0), (1, 0,)\}$ is a generating set for F^3 (as an F-vector space). Proof: consider that

$$\lambda^1 \odot (0, 0, 1) \oplus \lambda^2 \odot (0, 1, 0) \oplus \lambda^3 \odot (1, 0, 0) = (\lambda^1, \lambda^2, \lambda^3)$$

Theorem. *Every vector space has a basis.*

Remark. The proof for this theorem is stupidly complicated in general, which uses the axiom of choice. Even better, it turns out that this theorem is equivalent to the axiom of choice, somehow. We will later on prove that for finitely generated vector spaces, this theorem holds.

6.2 Finitely generated vector spaces

Definition. A vector space $(V, \oplus, \odot)$ is called **finitely generated** if there exists some finite set G that is a generating set for V.

Theorem. *Every finitely generated vector space has a basis (constructively proven, even). The proof for this theorem will be on Canvas. Study it. Will be examined.*

6.3 Dual bases on dual vector spaces

From now on, we will solely focus on finitely generated vector spaces.

Definition. A 'dual basis' is a basis on a dual vector space.

Remark. In order to discuss these objects, it turns out useful to use a form of consistent labeling throughout, which amounts to first establishing two rules:

- We commonly denote a 'regular' basis 'vector' by a Latin letter with a 'downstairs' index, for example, $e_1, e_2, \ldots, e_d$.
- We commonly denote a 'dual' basis 'vector' by a Greek letter (that is somewhat similar to its 'regular Latin counterpart') with a 'downstairs' index, for example, $\varepsilon^1, \varepsilon^2, \ldots, \varepsilon^d$.

Notice that the choice of basis for a vector space is completely arbitrary. We are fine with that, but if we also have to deal with a totally unrelated dual basis (e.g. two choices), we will not be able to do any useful mathematics. This is why we will define a canonical dual basis for each choice of basis.

Definition. Let $e_1, e_2, \ldots, e_d$ be a basis on $(V, \oplus, \odot)$. Then $\varepsilon^1, \varepsilon^2, \ldots, \varepsilon^d$ as a basis on $(V^*, \boxplus, \boxdot)$ is called **the (canonical) dual basis** with respect to $e_1, \ldots, e_d$ if:

$$\varepsilon^a(e_b) = \delta^a_b := \begin{cases} 1_F & \text{if } a = b, \\ 0_F & \text{otherwise.} \end{cases}$$

for all $a, b = 1, \ldots, d$ (you know what we mean by this).

6.4 Components of tensors with respect to a choice of basis

Definition. Let T be a (p, q)-tensor, e.g. let T be a multilinear map of the form:

$$T : \underbrace{V^* \times \ldots \times V^*}_{p} \times \underbrace{V \times \ldots \times V}_{q} \to F$$

Then the **components** of T with respect to a chosen basis $\{e_1, \ldots, e_d\}$ and its dual $\{\varepsilon^1, \ldots, \varepsilon^d\}$ are:

$$T^{a_1, \ldots, a_p}{}_{b_1, \ldots, b_q} := T(\varepsilon^{a_1}, \ldots, \varepsilon^{a_p}, e^{b_1}, \ldots, e^{b_q})$$

where a_i, b_i are 'indices' in $1, \ldots, d$.

This is a very abstract definition, but we will mostly use examples for some small choices of p, q, such that we define the components for those.

Example. Consider a $(1, 1)$-tensor, e.g. a multilinear map $T : V^* \times V \to F$. Consider already proven the theorems about 'decomposing' vectors and covectors a sum of scalings of basis (co)vectors. Then if we let

$$v := \bigoplus_{1 \leq i \leq d} v^i \odot e_i$$

$$\sigma := \bigboxplus_{1 \leq i \leq d} \sigma_i \boxdot \epsilon^i$$

we might consider that

$$\begin{aligned} T(\sigma, v) &= T\left(\boxplus_{1\leq i\leq d} \sigma_i \boxdot \epsilon^i, \bigoplus_{1\leq i\leq d} v^i \odot e_i \right) \\ &= \sum_{i=1}^{d}\sum_{j=1}^{d} T(\sigma_i \boxdot \varepsilon^i, v^j \odot e_j) \\ &= \sum_{i=1}^{d}\sum_{j=1}^{d} \sigma_i \cdot v^j \cdot T(\varepsilon^i, e_j) \\ &= \sum_{i=1}^{d}\sum_{j=1}^{d} \sigma_i \cdot v^j \cdot T^i_j \end{aligned}$$

Remark. A 'wild convention' is to arrange these components in a square, where the 'top indices' denote the row in the square, and the 'bottom indices' denote the column.

7 Two plus ε good ways to deal with linear structures

Throughout the lecture, we have our usual V, W as F-vector spaces. Both are finitely generated, and we have $e_1, \ldots, e_d$ as the basis on V. We induce a dual basis $\varepsilon^1, \ldots, \varepsilon^d$.

Theorem. *Let $v \in V$ and $\sigma \in V^*$. Then we have:*

1) $v = \bigoplus_{m=1}^{d} \varepsilon^m(v) \odot e_m$

2) $\sigma = \boxplus_{m=1}^{d} \sigma(e_m) \boxdot \varepsilon^m$

Proof. Consider that

$$\begin{aligned} \varepsilon^m(v) &= \varepsilon^m\left(\bigoplus_{a=1}^{d} v^a \odot e_a \right) \\ &= \sum_{a=1}^{d} v^a \cdot \varepsilon^m(e_a) \\ &= v^m \end{aligned}$$

So $v = \bigoplus_{a=1}^{d} v^a \odot e_a = \bigoplus_{a=1}^{d} \varepsilon^a(v) \odot e_a$. Furthermore consider that

$$\begin{aligned} \sigma(e_m) &= \left(\boxplus_{i=1}^{d} \sigma_i \boxdot \varepsilon^i \right)(e_m) \\ &= \sum_{i=1}^{d} \sigma_i \cdot \varepsilon^i(e_m) \\ &= \sigma_m \end{aligned}$$

So $\sigma = \boxplus_{i=1}^{d} \sigma_i \boxdot \varepsilon^i = \boxplus_{m=1}^{d} \sigma(e_m) \boxdot \varepsilon^m$. □

The rest of the lecture continues giving examples on how to interpret some objects (1 good way) in terms of their components (1 good way) and in terms of a 'cemetery' (some $\varepsilon > 0$, imagine it tiny, good way). Some key takeaways I will write down.

(a) Let $\phi : V \to V$ be an endomorphism. Consider that $\phi^a{}_b = \varepsilon^a(\phi(e_b))$. Now let $v \in V$. Then $\phi(v) \in V$. But what are its components?

$$\begin{aligned}(\phi(v))^a &= \varepsilon^a(\phi(v)) \\ &= \varepsilon^a(\phi(\bigoplus_{i=1}^{d} v^i \odot e_i)) \\ &= \sum_{i=1}^{d} v^i \varepsilon^a(\phi(e_i)) \\ &= \sum_{i=1}^{d} v^i \phi^a{}_i\end{aligned}$$

This motivates to write ϕ as its cemetery representation:

$$\begin{bmatrix} \phi^1_1 & \dots & \phi^1_d \\ \vdots & \ddots & \vdots \\ \phi^d_1 & \dots & \phi^d_d \end{bmatrix}$$

And v as well:

$$\begin{bmatrix} v^1 \\ \vdots \\ v^d \end{bmatrix}$$

Then a miracle occurs and we write the operation of finding all of the components of the vector $\phi(v)$ at once by a weird 'flower procedure' (which I omit since there is no LaTeX symbol for it)

$$\begin{bmatrix} \phi^1_1 & \dots & \phi^1_d \\ \vdots & \ddots & \vdots \\ \phi^d_1 & \dots & \phi^d_d \end{bmatrix} \begin{bmatrix} v^1 \\ \vdots \\ v^d \end{bmatrix} = \begin{bmatrix} \phi(v)^1 \\ \vdots \\ \phi(v)^d \end{bmatrix}$$

Notice however that the flower procedure can be characterized by the map for a single component of $\phi(v)$ that we produced above. It resembles some sort of 'row times column' operation. This is equivalent to just writing out all components of $\phi(v)$, no weird surprises here, just some funny notation.

(b) Let there still be our endo ϕ and declare $\phi^* : V^* \to V^*$. Of course, we define

$$\phi^*(\tau) := \tau \circ \phi$$

Consider the components of ϕ^*:

$$\begin{aligned}\phi^{*a}{}_b &:= \phi^*(\varepsilon^a)(e_b) \\ &= (\varepsilon^a \circ \phi)(e_b) \\ &= \varepsilon^a(\phi(e_b)) \\ &= \phi^a{}_b\end{aligned}$$

So the components of a dual map are the same as the components of the regular map!

(c) We can play the same tricks as before to consider the dual map, its cemetery, and observe

> 'It is the freaking flower again!'
>
> — Prof. Dr. F.P. Schuller

Same thing can be done for two monos ψ, ϕ to compute their composition, 'matrix-matrix multiplication'.

8 Augmented matrices

Througout the lecture, let $(V, +, \cdot)$ and $(W, +, \cdot)$ be F-vector spaces, let $e_1, \dots, e_n$ be a basis on V and let $\varepsilon^1, \dots, \varepsilon^n$ be its corresponding dual basis, let $g_1, \dots, g_m$ be a basis on W and let $\gamma^1, \dots, \gamma^m$ be its corresponding dual basis, such that $n = \dim V$ and $m = \dim W$.
Given $\phi : V \to W$ and thus its matrix $[\phi^i_j]$ and a $b \in W$, and we are tasked to find $v \in V$ such that $\phi(v) = b$, e.g. we find b^i and v^j for $i = 1, \dots, m$, $j = 1, \dots, n$, and solve (using the Einstein convention)

$$v^j \phi^i_j = b^i$$

As matrices:

$$\begin{bmatrix} \phi^1_1 & \dots & \phi^1_n \\ \vdots & \ddots & \vdots \\ \phi^m_1 & \dots & \phi^m_n \end{bmatrix} \begin{bmatrix} v^1 \\ \vdots \\ v^n \end{bmatrix} = \begin{bmatrix} b^1 \\ \vdots \\ b^m \end{bmatrix}$$

Definition. The **augmented matrix** (not a mathematical object, just a tool) is equivalent to the above notation and is denoted by

$$\left[\begin{array}{ccc|c} \phi^1_1 & \dots & \phi^1_n & b^1 \\ \vdots & \ddots & \vdots & \vdots \\ \phi^m_1 & \dots & \phi^m_n & b^m \end{array}\right]$$

Elementary row operations on this augmented matrix (analogous to χ, α, μ) are:

- Adding a scaling of a row to another row,
- Scaling a row by an element in F^*,
- Interchanging rows.

Definition. A linear system is called **consistent** if it has at least one solution. Otherwise, the linear system is called **inconsistent**.

Definition. A matrix is said to be in **row reduced echelon form** if:

(i) All rows without pivot elements are below rows with pivots.

(ii) The pivot of each row is to the right of all preceding rows.

(iii) Each pivot element equals 1_F and is the only nonzero element in its column.

Theorem. *A linear system is consistent if and only if the row reduced echelon form has no pivot element in its last column, when written as an augmented matrix.*

Proof. Later. □

Remark. 'No pivot element in the last column' in this context means that there is no row of the form

$$\left[\begin{array}{ccc|c} 0 & \dots & 0 & b \end{array}\right]$$

where $b \in F^*$.

Lemma. *Let $(V, \oplus, \odot)$ be an F-vector space and $\dim V < \infty$. Let $W \leqslant V$. Then*

$$\dim V/W = \dim V - \dim W$$

Proof. Let $n = \dim W$, let $m = \dim V$. Let $w_1, \dots, w_n$ be a basis for W. Let $v_1, \dots, v_m$ be a basis for V. By the Steinitz exchange theorem, we have $n \leq m$ (since $W \subseteq V$) and we can relabel the basis for V as follows:

$$w_1, \dots, w_n, v_{n+1}, \dots, v_m$$

which is then a basis for V.

Subclaim. $[v_{n+1}], \dots, [v_m]$ is a basis for V/W.
Subproof.

(i) Linear independence: let $\lambda^{n+1}, \dots, \lambda^m \in F$ such that

$$\boxplus_{j=n+1}^{m} \lambda^j \boxdot [v_j] = O_{V/W} := [0_V]$$

By the definition of the equivalence relation and $\boxplus, \boxdot$ being homomorphisms, we have that

$$\implies \bigoplus_{j=n+1}^{m} \lambda^j \odot v_j \oplus -0_V \in W$$
$$\implies \bigoplus_{j=n+1}^{m} \lambda^j \odot v_j \in W$$

Then we let $\lambda^1, \dots, \lambda^n \in F$ such that

$$\bigoplus_{j=n+1}^{m} \lambda^j \odot v_j = \bigoplus_{j=1}^{n} -\lambda^j \odot w_j$$
$$\implies 0_V = -\bigoplus_{j=n+1}^{m} -\lambda^j \odot v_j \oplus \bigoplus_{j=1}^{n} \lambda^j \odot w_j$$
$$\implies 0_V = \bigoplus_{j=n+1}^{m} \lambda^j \odot v_j \oplus \bigoplus_{j=1}^{n} \lambda^j \odot w_j$$
$$\implies 0_V = \oplus \bigoplus_{j=1}^{m} \lambda^j \odot v_j$$
$$\implies \forall j = 1, \dots m : \lambda^j = 0$$

Therefore, the 'linear combination map' has trivial kernel, thus the set is linearly independent.

(ii) Generating: let $v \in V$. Since we can relabel the basis on V, there exists $\lambda^1, \dots \lambda^m \in F$ such that

$$v = \bigoplus_{i=1}^{n} \lambda^i \odot w_i \oplus \bigoplus_{j=n+1}^{m} \lambda^j \odot v_i$$

Consider

$$[v] = \left[\bigoplus_{i=1}^{n} \lambda^i \odot w_i \oplus \bigoplus_{j=n+1}^{m} \lambda^j \odot v_i \right]$$
$$= \boxplus_{i=1}^{n} \lambda^i \boxdot [w_i] \boxplus \boxplus_{j=n+1}^{m} \lambda^j \boxdot [v_i]$$
$$= \boxplus_{j=n+1}^{m} \lambda^j \boxdot [v_i] \in \operatorname{span}\{[v_{n+1}], \dots, [v_m]\}$$

Therefore, $V/W \subseteq \operatorname{span}\{[v_{n+1}], \dots, [v_m]\}$, but we already know that $V/W \supseteq \operatorname{span}\{[v_{n+1}], \dots, [v_m]\}$, thus the set spans V/W and is a generating set.

Therefore, $[v_{n+1}], \dots, [v_m]$ is a basis for V/W and we have that $\dim V/W = m - n = \dim V - \dim W$. □

Theorem. *Let $\phi : V \to W$ be a homomorphism, let $(V, +, \cdot)$ and $(W, +, \cdot)$ be F-vector spaces, and $\dim V < \infty$. Then*

$$\dim V = \dim \ker \phi + \dim \operatorname{im} \phi$$

Proof. By the Fundamental theorem on homomorphisms, we have

$$V/_{\ker\phi} \cong_{\text{vec}} \operatorname{im}\phi$$

Therefore, using the result of the lemma, and setting $W := \operatorname{im}\phi$, we have

$$\dim\operatorname{im}\phi = \dim V - \dim\ker\phi$$

□

Theorem.

1. $\dim\ker\phi = \begin{cases} \#\text{ of zero rows} & \text{if } \dim V = \dim W, \\ \#\text{ of non-pivot columns} & \text{if } \dim V \neq \dim W. \end{cases}$
2. *(corollary of previous)* $\dim\operatorname{im}\phi = \#$ of non-zero rows

xm

Definition. $\operatorname{rank}\phi := \dim\operatorname{im}\phi$

Definition. Let $(V, \oplus, \odot)$ be an F-vector space. Let $e_1, \dots e_d$ be a basis for V and let $\varepsilon^1, \dots, \varepsilon^d$ be the canonical dual basis w.r.t. e_i, where $d = \dim V$. Let $\Omega \in \bigwedge^d(V)$ be a top-form on V. Let $\phi : V \to V$ be an endomorphism. Then define:

$$\det\phi = \frac{\Omega(\phi(e_1), \dots, \phi(e_d))}{\Omega(e_1, \dots, e_d)}$$

$$f : \mathbb{R}^d \to \mathbb{R}$$

$$(\operatorname{grad} f)(x_1, \dots, x_d) := \begin{bmatrix} \frac{\partial f}{\partial x_1}(x_1, \dots, x_d) \\ \vdots \\ \frac{\partial f}{\partial x_d}(x_1, \dots, x_d) \end{bmatrix}$$

$$f : \mathbb{R}^3 \to \mathbb{R}$$

$$(\operatorname{grad} f)(x, y, z) := \begin{bmatrix} \frac{\partial f}{\partial x}(x, y, z) \\ \frac{\partial f}{\partial y}(x, y, z) \\ \frac{\partial f}{\partial z}(x, y, z) \end{bmatrix} = \frac{\partial f}{\partial x}(x, y, z)i + \frac{\partial f}{\partial y}(x, y, z)j + \frac{\partial f}{\partial z}(x, y, z)k$$