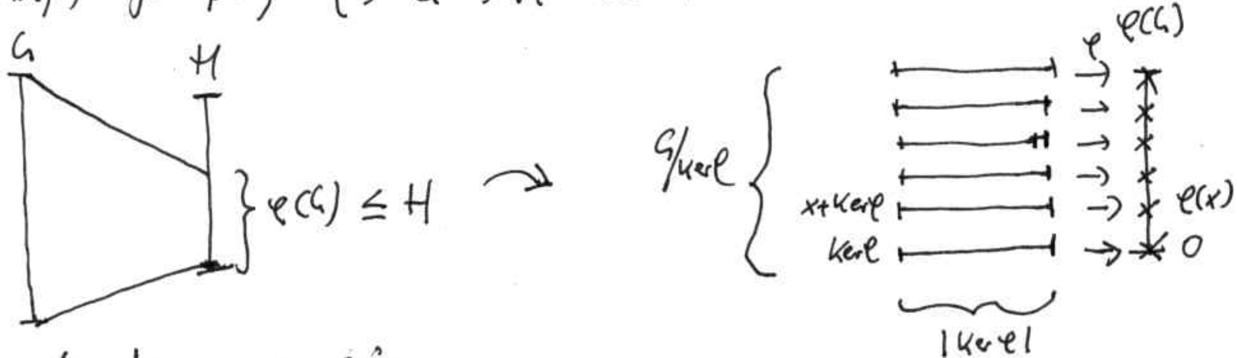
recap: Euclidean algorithm, types of rings

<u>homomorphism theorem again</u>

$(G,+)$, $(H,+)$ groups, $\varphi: G \to H$ hom.



<u>factor structures again</u>

- $\mathbb{Z}$ integers, $\mathbb{Z}/3\mathbb{Z}$ integers "mod 3"
- G group/ring, G/H group/ring elements "mod H"

<u>homomorphisms again</u>

$\varphi: G \to H$ group hom.

$\varphi(ab) = \varphi(a)\varphi(b)$

visualization as commutative diagrams:

1.)
$$\begin{tikzcd} a \arrow[r, "\cdot b"] \arrow[d, "\varphi"] \arrow[dr, phantom, "///"] & ab \arrow[d, "\varphi"] & \leftarrow \text{in } G \\ \varphi(a) \arrow[r, "\cdot \varphi(b)"] & \varphi(ab) & \leftarrow \text{in } H \end{tikzcd}$$

2.)
$$\begin{tikzcd} (a,b) \arrow[r, "\cdot \swarrow \text{in } G"] \arrow[d, "\varphi\times\varphi"] \arrow[dr, phantom, "///"] & ab \arrow[d, "\varphi"] & \leftarrow \text{in } G \\ (\varphi(a),\varphi(b)) \arrow[r, "\cdot \swarrow \text{in } H"] & \varphi(ab) & \leftarrow \text{in } H \end{tikzcd}$$

φ bijective (isom.) $\Rightarrow$ φ^{-1} exists and $ab = \varphi^{-1}(\varphi(a)\varphi(b))$

Vector spaces (linear spaces)

Linear algebra = theory of vector spaces

$\boxed{\text{Definition}}$: Let $\mathbb{F}$ be a field ($\mathbb{Q}, \mathbb{R}, \mathbb{C}$) and V a set with two operations

$$+: V \times V \to V$$
$$\cdot: \mathbb{F} \times V \to V$$

V is called an $\mathbb{F}$-vector space (often $\mathbb{F}$ is implicit and not mentioned) if:

a.) $(V, +)$ is a <u>comm.</u> group

b.) $\alpha(\beta x) = (\alpha\beta)x$, $1 \cdot x = x$

c.) $(\alpha+\beta)x = \alpha x + \beta x$, $\alpha(x+y) = \alpha x + \alpha y$

Examples:

a.) (prototype) $\mathbb{F}^n = \{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mid x_i \in \mathbb{F} \}$ with elementwise $+$ and $\alpha \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \alpha x_1 \\ \vdots \\ \alpha x_n \end{pmatrix}$.

b.) $\mathbb{F} = \mathbb{F}^1$

c.) $\mathbb{C}$ is an $\mathbb{R}$-VS

d.) $\mathbb{Q}$ is a $\mathbb{Z}$-VS $\lightning$

e.) continuous functions (set of) $\mathbb{R} \to \mathbb{R}$: $C(\mathbb{R})$ or $C^0(\mathbb{R})$.
set of one time differentiable functions $C^1(\mathbb{R})$

f.) $\mathbb{F}^{n \times n}$ ✓, $GL_n(\mathbb{F})$ $\lightning$

Note: very few comm. groups V can be made a VS.

g.) $\mathbb{F}[x]$, $\mathbb{F}(x)$, $\mathbb{F}[[x]] = \{ \sum_{n \geq 0} a_n x^n / a_n \in \mathbb{F} \}$
space of formal power series

h.) $\{0\}$, ~~~~

$\boxed{\text{Generators}}$:

$$V = \langle x_1, \dots, x_n \rangle_{VS} = \{ \underbrace{\sum_{i=1}^{n} \alpha_i x_i}_{\text{linear combination}} \mid \alpha_i \in \mathbb{F} \} \qquad x_1, \dots, x_n \text{ "span } V\text{"}$$

$\{x_1, \dots, x_n\}$: called generating system (or set) or spanning set for V.

Example:

$$\left\langle \begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix} \right\rangle_{\mathbb{R}\text{-VS}} = \left\{ \begin{pmatrix}\alpha\\\beta\\0\end{pmatrix} \;\middle|\; \alpha,\beta \in \mathbb{R} \right\} \qquad (\text{plane in } \mathbb{R}^3)$$

Note: linear combinations are <u>always finite</u>

<u>Definition:</u> $\{x_1, \dots, x_n\} \subset V$ is called "linearly independent" if $\alpha_1 x_1 + \dots + \alpha_n x_n = 0$ implies all $\alpha_i = 0$.
Otherwise: "linearly dependent".

$$\{x_1, \dots, x_n\} \text{ lin. dep.} \iff \alpha_1 x_1 + \dots + \alpha_n x_n = 0 \quad \text{with } \alpha_i \neq 0$$

$$\iff x_i = -\frac{\alpha_1}{\alpha_i} x_1 + \underbrace{\dots}_{\text{"}i\text{" omitted}} + \left(-\frac{\alpha_n}{\alpha_i}\right) x_n$$

$\iff$ x_i can be omitted in $\langle x_1, \dots, x_n \rangle_{VS}$.

<u>Definition:</u> $B \subseteq V$ is called a basis of V if

a.) B lin. indep.

b.) $\langle B \rangle_{VS} = V$

<u>Theorem:</u> Every VS has a basis provided the axiom of choice. All bases have the same size (cardinality).

- explain AOC (info at Wikipedia)
- formulated 1904 by Ernst Zermelo (1871-1953)

<u>Definition:</u> If B is a basis of V then $|B| = \dim(V)$ is called the dimension of V.
(note: is well-defined)

Examples:

a.) $V = \mathbb{F}^n$, $B = \{e_1, \dots, e_n\}$, $e_i = \begin{pmatrix}0\\\vdots\\1\\\vdots\\0\end{pmatrix} \leftarrow i$ "canonical base vectors", $\dim = n$

b.) $V = \mathbb{F}[x]$, $B = \{1, x, x^2, \dots\}$ $\dim = \infty$

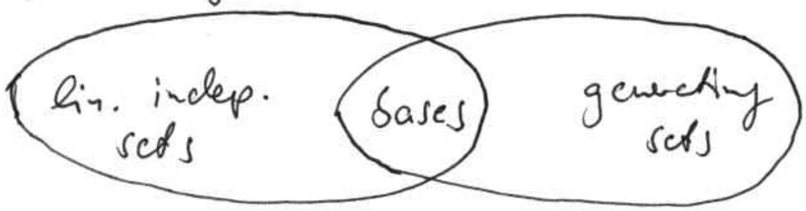
c.) $V = \mathbb{F}[[x]]$, $B = ?$ $\dim = \infty$ d.) $\{0\}$, $\dim = 0$

Some facts (without proof):

a.) a basis is a minimal generating set

" maximal lin. indep. set

b.) every lin. indep. set can be extended to a basis
(connection to Matroids and greedy algorithms)
every generating set can be reduced to a basis



$\boxed{\text{Subspaces}}$:

Definition: Let V be a VS. $U \subseteq V$ is called a subvector space, written $U \leq V$, if U is again a VS (w.r.t. the same operations)

test for subspace: $x, y \in U$, $\alpha, \beta \in \mathbb{F} \Rightarrow \alpha x + \beta y \in U$

trivial subspaces: $\{0\}$ and V

Equivalence relation: $x \sim y \Leftrightarrow x - y \in U \qquad (U \leq V)$

$\Leftrightarrow x \in \underbrace{y + U}_{\text{equ. classes}}$

V/U vector space?

$[x] + [y] = [x+y]$ is well-defined since $(U,+) \trianglelefteq (V,+)$

$\alpha [x] = [\alpha x]$?

$\alpha \in \mathbb{F}, x \sim y \xRightarrow{\text{to show}} [\alpha x] = [\alpha y] \Leftarrow$

$\Downarrow$

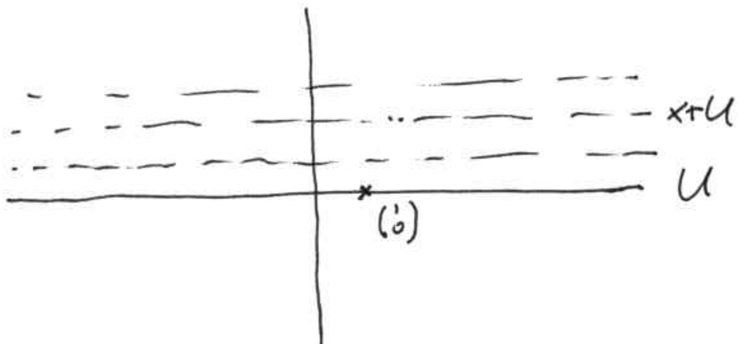
$x - y \in U \Rightarrow \alpha(x-y) \in U \Rightarrow \alpha x - \alpha y \in U \Rightarrow \alpha x \sim \alpha y$

✓

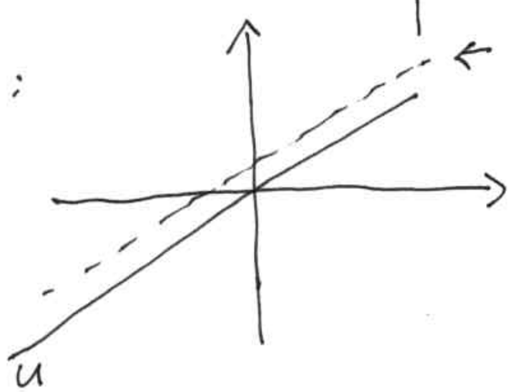
$\boxed{V/U \text{ is a VS for } \underline{\text{all}} \text{ subspaces of } V}$

Example: $V = \mathbb{R}^2$, $U = \langle \binom{1}{0} \rangle = \{ \binom{\alpha}{0} \mid \alpha \in \mathbb{R} \}$

$V/U = \{ x + U \mid x \in \mathbb{R}^2 \}$ = set of lines parallel to U



note:



← not a subspace since $0 \notin$ but a coset $x + U$

<u>Definition</u>: Let $U, V \leq W$. $U + V = \{ x + y \mid x \in U, y \in V \}$ is called the sum of U and V.

<u>Theorem</u>: $U, V \leq W$

a.) $U + V$ is again a VS

b.) ~~the intersection of VSs is a VS~~ $U \cap V$ is a VS

c.) ~~dim U + dim V~~ $\dim(U+V) = \dim U + \dim V - \dim(U \cap V)$

visualization (but careful):

if $U \cap V = \{0\}$,
then $\dim(U+V) = \dim U + \dim V$ and we write

$U \oplus V = U + V$

↑

direct sum