recap: Euclidean algorithm, types of rings

homomorphism theorem again

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

\[
\begin{array}{ccc}
G & \xrightarrow{\Phi} & H \\
\{\Phi(x) \leq H \rightarrow \text{ker}\} & & \\
\end{array}
\]

Factor structures again

- \(\mathbb{Z}\) integers, \(\mathbb{Z}/n\mathbb{Z}\) integers "mod \(n\)
- \(G\) group by \(G/\text{ker}\) group by "elements "mod \(H\)"

homoomorphisms again

\(\Phi: G \to H\) group hom.

\(\Phi(ab) = \Phi(a) \Phi(b)\)

Visualization as commutative diagrams:

1)

\[
\begin{array}{ccc}
a & \xrightarrow{b} & ab \\
\downarrow{\Phi} & & \downarrow{\Phi} \\
\Phi(a) & \xrightarrow{\Phi(b)} & \Phi(ab) \\
\end{array}
\]

2)

\[
\begin{array}{ccc}
(a, b) & \xrightarrow{\cdot} & ab \\
\downarrow{\Phi \times \Phi} & & \downarrow{\Phi} \\
(\Phi(a), \Phi(b)) & \xrightarrow{\cdot} & \Phi(ab) \\
\end{array}
\]

\(\Phi\) surjective (isom.) \(\Rightarrow\) \(\exists \Phi^{-1}\) exists and \(ab = \Phi^{-1}(\Phi(a) \Phi(b))\)
Vector spaces (linear spaces)

Linear algebra = theory of vector spaces

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:

1. $(V, +)$ is a comm. group
2. $\alpha(\beta x) = (\alpha \beta) x$, $1 \cdot x = x$
3. $(\alpha + \beta) x = \alpha x + \beta x$, $\alpha(x + y) = \alpha x + \alpha y$

Examples:

1. (prototype) $\mathbb{F} = \{ (x_1, x_2) \mid x_1, x_2 \in \mathbb{F} \}$ with elementwise $+$ and $\alpha (x_1, x_2) = (\alpha x_1, \alpha x_2)$.
2. $\mathbb{F}^n$.
3. $\mathbb{C}$ is an $\mathbb{R}$-VS
4. $\mathbb{Q}$ is a $\mathbb{Z}$-VS
5. Continuous functions (set of) $\mathbb{R} \to \mathbb{R} = C(\mathbb{R})$ or $C^\infty(\mathbb{R})$.
6. $\mathbb{F}[x]$.
7. $\mathbb{F}{(x)}$, $\mathbb{F}{[x]} = \{ \sum_{i=0}^{\infty} a_i x^i \mid a_i \in \mathbb{F} \}$

Generators:

$$V = \langle x_1, \ldots, x_n \rangle_{\mathbb{F}} = \left\{ \sum_{i=1}^{n} a_i x_i \mid a_i \in \mathbb{F} \right\}$$

linear combination

$\{x_1, \ldots, x_n\}$: called generating system (or set) or spanning set for $V$. 
Example:
\[ \langle (0), (0) \rangle_{\mathbb{R}^2} = \{ (0) \} = \mathbb{R}^2 \] (plane in \( \mathbb{R}^3 \))

Note: linear combinations are always finite.

Definition: \( \{ x_1, \ldots, x_n \} \subseteq V \) is called "linearly independent" if \( \alpha_1 x_1 + \cdots + \alpha_n x_n = 0 \) implies all \( \alpha_i = 0 \).

Otherwise: "linearly dependent."

\( \{ x_1, \ldots, x_n \} \text{ lin. dep.} \iff \alpha_1 x_1 + \cdots + \alpha_n x_n = 0 \) with \( \alpha_i \neq 0 \)

\[ \Rightarrow \ x_i = -\frac{\alpha_i}{\alpha_j} x_1 + \cdots + (\frac{\alpha_i}{\alpha_j}) x_n \]

\[ \Leftarrow \ x_i \text{ can be omitted in } \langle x_1, \ldots, x_n \rangle_{\mathbb{R}}. \]

Definition: \( \mathfrak{b} \subseteq V \) is called a basis of \( V \) if

a.) \( \mathfrak{b} \text{ lin. indep.} \)

b.) \( \langle \mathfrak{b} \rangle_{\mathbb{R}} = V \)

Theory: Every \( V \) 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)

Definition: If \( \mathfrak{b} \) is a basis of \( V \) then \( |\mathfrak{b}| = \dim(V) \)

is called the dimension of \( V \).

(note: is well-defined)

Examples:

a.) \( V = \mathbb{R}^n \), \( \mathfrak{b} = \{ e_1, \ldots, e_n \} \), \( e_i = (0, \ldots, 0, 1, 0, \ldots, 0) \) "canonical base vectors"

b.) \( V = \mathbb{F}^3 \), \( \mathfrak{b} = \{ e_1, e_2, e_3 \} \)

dim = 3

c.) \( V = \mathbb{F}^2 \), \( \mathfrak{b} = \{ e_1, e_2 \} \)

dim = 2

d.) \( \mathbb{C}^3 \), \( \dim = 3 \)
Some facts (without proof):

a) A basis is a minimal generating set
   \[ \text{u maximal lin. indep. set} \]

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

Subspaces:

Definition: Let \( V \) be a VS, \( U \subseteq V \) is called a subspace,
\( V \), if \( U \) is again a VS
(c.a.v. the same operations)

Test for subspace: \( x, y \in U, \alpha \beta \in F \rightarrow \alpha x + \beta y \in U \)

Trivial subspaces: 0 and \( V \)

Equivalence relation: \( x \sim y \Leftrightarrow x - y \in U \)

\( V/U \) vector space?

\( cx + cy = cx + y = \) is well-defined since \( (U, +) \leq (V, +) \)
\( \alpha x = [cx] \)?
\[ x \in F, x \sim y \rightarrow [\alpha x] = [\alpha y] \]
\[ x - y \in U \rightarrow x(x - y) \in U \rightarrow \alpha x - \alpha y \in U \rightarrow \alpha x \sim \alpha y \]

\( V/U \) is a VS for all subspaces of \( V \)
Example: \( V = \mathbb{R}^2, U = \langle (0) \rangle = \{ (0) | x \in \mathbb{R}^2 \} \)
\( V/U = \{ x + U | x \in \mathbb{R}^2 \} \) = set of lines parallel to \( U \)

**Note:** not a subspace since \( 0 \notin U \) but a coset \( x + U \)

**Definition:** Let \( U, V \subseteq W \). \( U + V = \{ x + y | x \in U, y \in V \} \) is called the sum of \( U \) and \( V \).

**Theorem:** \( U, V \subseteq W \)

a.) \( U + V \) is again a VS
b.) The intersection of \( U \) and \( V \) is a VS \( U \cap V \) is a VS
c.) Geometrically \( \dim(U + V) = \dim U + \dim V - \dim(U \cap V) \), visualization (but careful):

\[
\begin{array}{c}
U \\
\cap \\
V
\end{array}
\]

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

direct sum