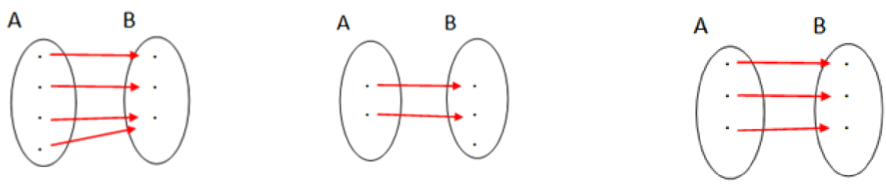
H1: Elementary algebraic structures

1.1 sets, maps and relations

1.1.1 sets

def: set	= a gathering together into a whole of definite, distinct objects of our perception or our thought > contains elements notation: capital letters vb: A = {0,1,2,3}
def: element/members	= objects in a set not: small letters a,b,c,... vb: $B = \{a \mid (a \in A) \wedge (\exists b \in A, a = 2b)\} = \{a \in A \mid \exists b \in A, a = 2b\}$
logical operators	not: $\neg$ and: $\wedge$ or: $\vee$
logical quantifiers	for all: $\forall$ there exists: $\exists$
def: cardinality of A	= the number of elements of a set A > can be finite or infinite not: |A| or #A
> def: countability of infinite sets	countable set = infinite set where there is a way to count/enumerate all element vb: natural, integer and rational numbers uncountable set = infinite set that isn't countable vb: real and complex number
important sets	• $\emptyset = \{\}$: the **empty set** with no elements • $\mathbb{N}$: the set of all natural numbers (which we take to include zero, thus following to the ISO 80000-2 standard)[2]; we use $\mathbb{N}_0 = \mathbb{N} \setminus \{0\}$ if zero is not included[3] • $\mathbb{Z}$: the set of all integer numbers • $\mathbb{Q}$: the set of all rational numbers • $\mathbb{R}$: the set of all real numbers • $\mathbb{C}$: the set of all complex numbers
def: positive real numbers def: non-negative real numbers	= $\mathbb{R}_{>0} = \{x \in \mathbb{R} \mid x > 0\}$ > doesn't include 0 = $\mathbb{R}_{\geq 0} = \{x \in \mathbb{R} \mid x \geq 0\}$ > includes 0
def: extended real line	= $\overline{\mathbb{R}} = \mathbb{R} \cup \{-\infty, +\infty\}$
def: subset def: superset	= B is a subset of A if $\forall b \in B : b \in A$ not: $B \subseteq A$ = the set A which contains B
def: non-trivial subset	= all subsets B that are not A nor Ø
set operations	• For two sets A and B, the **union** $A \cup B = \{x \mid (x \in A) \vee (x \in B)\}$. • For two sets A and B, the **intersection** $A \cap B = \{x \mid (x \in A) \wedge (x \in B)\}$. • for $B \subseteq A$, the **complement** of B in A, denoted as $B^c = A \setminus B = \{x \in A \mid \neg(x \in B)\} = \{x \in A \mid x \notin B\}$. In the set difference notation, it is not always required that B is actually a subset of A.
operations on a set of sets	The union and intersection are trivially generalised to a family of sets, which we would represent as a set $\mathcal{S} = \{A, B, \ldots\}$ of sets[4], with finite or infinite cardinality: $\bigcup \mathcal{S} = \{a \mid \exists A \in \mathcal{S} : a \in A\} \qquad \bigcap \mathcal{S} = \{a \mid \forall A \in \mathcal{S} : a \in A\}. \qquad (1.1)$

logical operations	• Commutativity: $A \cup B = B \cup A$ and $A \cap B = B \cap A$ • Associativity: $(A \cup B) \cup C = A \cup (B \cup C)$ and $(A \cap B) \cap C = A \cap (B \cap C)$ • Distributivity: $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$ and $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$ • de Morgan relations: $(A \cup B)^c = A^c \cap B^c$ and $(A \cap B)^c = A^c \cup B^c$
def: Cartesian product	the cartesian product of two set A and B = A x B : { (a,b)| a∈A, b∈B} > set whose elements are tuples
1.1.2 maps	
def: map	= a rule that assigns to each element a∈A an element b∈B not: $\varphi : A \to B$
def: domain def: codomain	= the set A in the previous definition > dom(φ) = the set B in the previous definition > codom(φ)
def: composition	= given two maps: $\varphi : A \to B$ and $\psi : B \to C$ the composition is: $\psi \circ \varphi : A \to C$ using the assignment: $a \mapsto \psi(\varphi(a))$. >> this is associative: $\chi \circ (\psi \circ \varphi) = (\chi \circ \psi) \circ \varphi$
def: identity map	= map that maps each element to itself: $\mathrm{id}_A : A \to A : a \mapsto a$ = neutral element for maps: $\varphi = \mathrm{id}_B \circ \varphi = \varphi \circ \mathrm{id}_A$.
def: image	= the set of all function values $\varphi(A) = \{\varphi(a) \| a \in A\} \subseteq B$
def: inverse image of b∈B	= the set $\{a \in A \| \varphi(a) = b\}$
map characteristics	- surjective: the image of the domain covers the whole codomain - injective: each b∈B is the image of at most one a∈A - bijective: the map is sur- and injective 
def: inverse map	= $\varphi^{-1} : B \to A$ such that $\varphi^{-1}(\varphi(a)) = a, \forall a \in A$ or $\varphi^{-1} \circ \varphi : A \to A = \mathrm{id}_A$ and $\varphi \circ \varphi^{-1} : B \to B = \mathrm{id}_B$.
1.1.3 set cardinality revisited	
ordering of candinality	- |A| ≤ |B| if there exists an injective map between A and B - |A| = |B| if there exists a bijective map between A and B
countability and maps	an infinite set is countable if there exists an injective map to ℕ > denote as $\mathfrak{N}_0$ known as *aleph* an infinite set is uncountable if their cardinality is higher than $\mathfrak{N}_0$ > label the possible cardinalities as: $\aleph_0 < \aleph_1 < \aleph_2 < \ldots$
def: cardinality $\mathfrak{N}_i$	sets with cardinality $\mathfrak{N}_i$ would allow for injective mappings into sets with cardinality $\mathfrak{N}_j$ with i≤j but not with $\mathfrak{N}_n$ with i>n
def: powerset P(A) of a set A	= the set of all subsets of A

1.1.4 relations	
def: relation	= list of couples which satisfy a certain chosen 'relation' > relations are a kind of cartesian product, i.e. a subset of AxB maps are a kind of relation known as the *graph* of φ: $\{(a, \varphi(a)) \| a \in A\} \subseteq A \times B,$
def: equivalence relation ~	= a relation of the set A with itself, so a subset of AxA > a couple (a,b) is denoted as a~b if it satisfies: • $a \sim a$: any element is related to itself, i.e. the relation is **reflexive**. • $a \sim b \implies b \sim a$: the relation is **symmetric**. • $a \sim b \wedge b \sim c \implies a \sim c$: the relation is **transitive**.
def: equivalence class [a]	= set all elements related to a by a certain ~
def: partition	= collection of subsets A_i such that: $\bigcup_i A_i = A$ with $A_i \cap A_j = \emptyset$ for all $i \neq j$ > if this partition is the equivalence relation, the set of equivalence classes $\{A_1, A_2, \ldots\}$ is known as the *quotient set* A/~
def: partial order relation ≼	= relation between a set A and itself which satisfies: • $a \preccurlyeq a$: the relation is **reflexive**. • $a \preccurlyeq b \wedge b \preccurlyeq a \implies a = b$: referred to as the relation being **antisymmetric**. • $a \preccurlyeq b \wedge b \preccurlyeq c \implies a \preccurlyeq c$: the relation is **transitive**. > A set A with a partial order relation $\preccurlyeq$ is called a **partially ordered set** or simply a **poset** and denoted as $(A, \preccurlyeq)$.
def: total order relation	= partial order relation where all elements are ordered ie: for any a,b∈A there exist either a≼b or b≼a
def: greatest/largest element	= an element a∈A such that b≼a for all b∈A for a poset (A,≼)
def: bounded above	a subset B⊆A of a poset (A,≼) is bounded above > if there exists an a∈A so that b≼a for all b∈B, with a the *upper bound*
def: maximal element	a poset (A,≼) has a maximal element a∈A > if no b≠a∈A satisfies a≼b
1.2 groups, rings and fields	
1.2.1 groups	
def: binary operation .	A **binary operation**[12] $\cdot$ on a set A is a map $A \times A \to A : (a, b) \mapsto a \cdot b$.
properties of binary operations	a binary operation **can** have the following properties: 1. **Associativity**: $\forall a, b, c \in A,\ a \cdot (b \cdot c) = (a \cdot b) \cdot c$, so that parenthesis are not needed. 2. **Neutral element**: $\exists e \in A,\ \forall a \in A,\ a \cdot e = e \cdot a = a$. 3. **Inverse elements**: $\forall a \in A,\ \exists b \in A,\ a \cdot b = b \cdot a = e$, where b is then denoted as a^{-1}. 4. **Commutativity**: $\forall a, b \in A,\ a \cdot b = b \cdot a$.
def: group (G,.)	= a set G with a binary operation . that is: - associative - has a neutral element - every element has an inverse
def: abelian group	= a group that also is commutative
def: trivial group	= group with neutral element as single element: {e}
def: semigroup	= set with a binary operation that is associative
def: monoid group	= semigroup whose binary operation also has a neutral element

1.2.2 homomorphisms, isomorphisms and automorphisms	
def: homomorphism	consider a set with additional structure > a map that preserves this structure is called a *homomorphism*
def: endomorphism	= a homomorphism where the domain and codomain coincide
def: isomorphism	= bijective homomorphism
def: automorphism	= bijective endomorphism > not: A≅B
def: automorphism group	= the set aut(A) of automorphisms for a set A with composition as binary operator
def: involution	= a non trivial automophism $\phi : A \to A$ for which $\phi \circ \phi = \mathrm{id}_A$
def: group homomorphism	a group homomorphism between groups (G, .) and (H,*) = a map: $\varphi : G \to H$ that satisfies $\varphi(g_1 \cdot g_2) = \varphi(g_1) \circ \varphi(g_2), \forall g_1, g_2 \in G.$ > φ maps the neutral element e_G of G to the neutral element $\varphi(e_G) = e_H$ of H, and an inverse element g^{-1} to the corresponding inverse element $\varphi(g^{-1}) = \varphi(g)^{-1}$.
def: anti-homomorphisms	= maps that preserve structure up to the fact that they reverse the order of group multiplication: $\varphi(g_1 \cdot g_2) = \varphi(g_2) \circ \varphi(g_1)$
1.2.3 group actions	
def: group action	a group action $\lambda : G \to \mathrm{Aut}(A)$ = a group homomorphism from a group G to the automorphism group of a set A not: If we denote λ_g as the image of λ for $g \in G$, then it needs to satisfy $\lambda_e = \mathrm{id}_A$ and $\lambda_{g_1} \circ \lambda_{g_2} = \lambda_{g_1 \cdot g_2}$. Even more explicitly, $\forall a \in A$, $\lambda_e(a) = a$ and $\lambda_{g_1}(\lambda_{g_2}(a)) = \lambda_{g_1 \cdot g_2}(a)$. extra notation: We sometimes denote $\lambda_g(a) = g \triangleright a$, and can thus interpret a group action as a map $\triangleright : G \times A \to A : (g, a) \mapsto g \triangleright a$, with $e \triangleright a = a$ and $h \triangleright (g \triangleright a) = (h \cdot g) \triangleright a$, $\forall a \in A$.
properties of group actions	A group action α (left or right) can (but must not) have a number of properties: • **faithful** : if $g \neq h$ implies $\alpha_g \neq \alpha_h$, which requires that there exists at least one $a \in A$ for which $\alpha_g(a) \neq \alpha_h(a)$. • **free** : $\forall g \neq e$, $\alpha_g(a) \neq a$ for all $a \in A$, or in its contrapositive: if there is an $a \in A$ such that $\alpha_g(a) = \alpha_h(a)$, this implies $g = h$ (free implies faithful and is stronger). • **transitive** : if for any $a, b \in A$, there exists a $g \in G$ such that $\alpha_g(a) = b$.
def: representation	= a map from group elements g∈G to invertible matrices in a general linear group
1.2.4 kernels, normal subgroups, quotient groups	
def: kernel	= the subset of G that is mapped to e_H for a group homomorphism $\varphi : G \to H$. not: denoted as $\ker \varphi = \varphi^{-1}(e_H) \subseteq G$.
prop: kernel and subgroup	For two groups G and H > The kernel of a group homomorphism φ: G->H is a subgroup of G
def: normal subgroup N ⊆ G	= a subgroup such that ∀g∈G, $\forall n \in N$, $gng^{-1} \in N$.

1.2.5 rings and fields	
def: ring	= an abelian group (A,+) together with a second binary operation (A, .) for the group (A,+): 0 is the neutral element for the group (A, .): - is associative - 1 is the unit element > such that . has the property of distribution over +: • *left distributivity*: $\forall a,b,c \in A,\ a\cdot(b+c) = (a\cdot b)+(a\cdot c)$ • *right distributivity*: $\forall a,b,c \in A,\ (b+c)\cdot a = (b\cdot a)+(c\cdot a)$
def: commutative ring	= ring where . is also commutative
def: idempotent	= element that squares to itself: a.a=a
def: multiplicative inverse	= element a^{-1} such that $a.a^{-1} = a^{-1}.a = 1$
def: zero divisors	= two elements a,b∈A where both a,b≠0 which satisfy a.b = 0
def: nilpotent	= an element a≠0 where a.a = 0
def: nilpotent with degree n	= an element a≠0 where $a^n = 0$
prop: rings and inverses	In a finite ring, all elements must either have multiplicative inverses, or must be zero divisors
def: field	= a commutative ring where all non-zero element have multiplicative inverses
def: characteristic of a field	= the number of times one has to add the unit element in order to obtain the neutral element > in a *finite ring* the characteristic is finite *infinite ring* not finite
def: algebraically closed field	= field F in which every non-constant polynomial $p \in \mathbb{F}[z]$ has a root $r \in \mathbb{F}$ so that $p(r) = 0$.
1.3 vector spaces	
1.3.1 definitions and examples	
def: vector space V over a field $\mathbb{F}$	= an abelian group (V, +v) together with a binary operation, namely scalar multiplic. for which: (V,+v): - +v is the vector addition - 0_v is the zero vector - -v is the additive inverse and the scalar multiplication: $\mathbb{F}\times V \to V : (a,v) \mapsto av$ for which • Distributivity with respect to vector addition: $\forall a \in \mathbb{F}$ and $\forall v,w \in V : a(v +_V w) = av +_V aw$ • Distributivity with respect to scalar addition: $\forall a,b \in \mathbb{F}$ and $\forall v \in V : (a+b)v = av +_V bv$ • Mixed associativity of scalar multiplication: $\forall a,b \in \mathbb{F}$ and $\forall v \in V : a(bv) = (a\cdot b)v$ • scalar unit is the neutral element for multiplying with vectors: $\forall v \in V : 1v = v$
def: subspace	= a non-empty subset W⊆V of a vector space V where W is also a vectorspace

1.3.2 vector space homomorphisms, endomorphisms and isomorphisms	
def: linearity	A map $\varphi : V \to W$ between two vector spaces $(V, +_V, o_V)$ and $(W, +_W, o_W)$ over the same field $\mathbb{F}$ is a (vector space) homomorphism if it satisfies • $\forall u, v \in V$: $\varphi(u +_V v) = \varphi(u) +_W \varphi(v)$ • $\forall v \in V, \forall a \in \mathbb{F}$: $\varphi(av) = a\varphi(v)$ It follows automatically that φ also satisfies $\varphi(o_V) = o_W$. These two properties are referred to as **linearity** and collectively presented as $$\forall u, v \in V, \forall a, b \in \mathbb{F} : \varphi(au + bv) = a\varphi(u) + b\varphi(v) \quad (1.9)$$
def: linear operation	= a linear map from V->V, ie vector space endomorphism
def: linear transformation	= a bijective linear map from V->W
def: general linear group GL(V)	= linear transformations from V->V
1.3.3 linear combination, span and completeness	
def: linear combination	= $$v = \sum_{i=1}^{m} a^i v_i \quad (1.10)$$ with scalars $a^i \in \mathbb{F}$, vectors $v_i \in S$, with $i = 1, \ldots, m$ for some finite[21] integer $m \leq \|S\|$.
def: linear span	= the union of all possible linear combinations that can be built from a finite number of vectors from S not: $\text{span}_{\mathbb{F}}$(S) or span(S)
def: completeness	a set S⊆V is called complete > if span(S) = V ie: any vector in V can be written as a lin. comb. of a finite number of vector in S
def: dimension of a set	= the smallest integer n∈ℕ such that V can be spanned by a set S with cardinality |S|=n > *finite-dimensional* = dimension is a finite number *infinite-dimensional* = dimension is an infinite number
1.3.4 linear independence and basis	
def: linear independence	The set of vectors S is linearly independent > if for any finite subset $\{v_1, \ldots, v_m\} \subseteq S$, $$o = \sum_{i=1}^{m} a^i v_i \implies a^i = 0, \forall i = 1, \ldots, m.$$
prop: decomposition of a vector	for a set S ⊆ V that is linear independent > the decomposition of any vector v∈span(S) as a lin. comb. is unique in the form: $$v = \sum_{i=1}^{m} a^i v_i$$
def: basis	= a set B⊆V that is both complete and linearly independent > ie: any v∈V can be decomposed uniquely in an expansion using finite number of vectors in B
prop: span and basis	For S⊆V linearly independent For no v∈V can be added to S without making it linearly dependent > than span(S) = V and S is a basis of V
prop: subset and basis	For any complete set S⊆V > we can extract a subset from S that is a basis for V
prop: basis of a vector space	ANY vector space has a basis

prop: lin.ind. sets and basis	For any linearly independent S⊆V > S can be extended to be a basis for V ie: there exists a set S'⊆V such that $V = \mathbb{F}(S \cup S')$
prop: subsets and dimension	For S={v_1, ...,v_m} linearly independent subset of V > then m ≤ dim(V) = n ie: an n-dimensional space does not admit more than n linearly independent vectors
> prop: basis cardinality & dimension	For any basis B of a finite-dimensional vector space V: |B| = dim(V) For any linearly independent set S with |S|=dim(V): S is complete and a basis for V
def: coordinates	For a finite-dimensional vector space V with basis B = {e_1,...,e_n} > any vector can be written: $$v = \sum_{i=1}^{n} v^i e_i$$ define the scalars v^i as *coordinates of v* with respect to B
def: coordinate map	in the previous definition we define: $\phi_B : V \to \mathbb{F}^n : v \mapsto \mathbf{v} = (v^1, v^2, \ldots, v^n)$ as the **coordinate map**.
prop: dimension and isomorphism	For any two dimensional spaces V and W With dim(V) = dim(W) = n > there applies: V and W are isomorphic, so V≅W
1.3.5 free vector space	
def: free vector space	For a set S > the free vector space *S* = the space of all formal linear combinations of a finite number of elements from S
1.3.6 index notation and Einstein summation	
not: Einstein summation	For a vector v that is expended by linear combinations: $$v = \sum_{i=1}^{n} v^i e_i$$ we omit the summation symbol and write: $$v = v^i e_i.$$ So if there is one index i in superscript and one index i in subscript in one expression > it implies the Einstein summation
def: Kronecker δ symbol	$$\delta^i_j = \begin{cases} 1, & \text{for } i = j \\ 0, & \text{for } i \neq j \end{cases}$$
1.3.7 combining and manipulating spaces and subspaces	
prop: ≼ and dimension	the relation W≼V implies dim(W) ≤ dim(V)
prop: ≼ with equal dimension	For W≼V with W and V finite-dimensional > if dim(W) = dim(V), then W = V
prop: ≼ with multiple W_i	For two subspaces W_i ≼ V , with i = 1,2 > then their intersection is still a subspace: $W_1 \cap W_2 \preccurlyeq V$
def: disjoint subspaces	For two subspaces W_1,W_2 ≼ V > these are *disjoint subspaces* if $W_1 \cap W_2$ = {0} , the trivial space

def: sum of subspaces	the sum of subspaces $W_i \preccurlyeq V$ is the subspace of V defined as: $\sum_{i\in I} W_i = \{v \in V \mid v = \sum_{i\in I'} w_i \text{ with } w_i \in W_i \text{ for } i \text{ in some finite subset } I' \text{ of } I\}$ > this is the smallest subspace containing al W_i
prop: dimension of a sum	If W_1 and W_2 are finite-dimensional, then: $\dim(W_1 + W_2) = \dim(W_1) + \dim(W_2) - \dim(W_1 \cap W_2)$
def: direct sum	For two disjoint subspaces $W_1, W_2 \preccurlyeq V$ > their sum is the direct sum, denoted as $W_1 \oplus W_2$
def: complement	= two subspaces $W_1, W_2 \preccurlyeq V$ that satisfy $V = W_1 \oplus W_2$
def: codimension of W_1	= the dimension of a subspace that is complementary to W_1 so if: $V = W_1 \oplus W_2$ > then: $\dim(V) = \dim(W_1) + \dim(W_2)$ > thus: $\dim(W_2) = \dim(V) - \dim(W_1)$ is fixed by W_1 not: $\mathrm{codim}(W_1)$
prop: vector addition and multipl.	For two vector spaces W_1 and W_2 For a common field $\mathbb{F}$ > the cartesian product $W_1 \times W_2 = \{(w_1, w_2), \forall w_1 \in W_1, w_2 \in W_2\}$ is a vector space over $\mathbb{F}$ if defined: vector addition: $(v_1, v_2) + (w_1, w_2) = (w_1 + v_1, w_2 + v_2)$ scalar multiplication: $a(w_1, w_2) = (aw_1, aw_2), \forall a \in \mathbb{F}.$
def: external direct sum	= the cartesian product of two general vector spaces W_1 and W_2 over a common field $\mathbb{F}$ not: $W_1 \oplus W_2$
prop: existence of complementary space	For a subspace $W \preccurlyeq V$ > there always exists a complementary subspace $U \preccurlyeq V$ such that $V = U \oplus W$
def: quotient space V/W	= for subspace $W \preccurlyeq V$, the quotient set V/~ under equivalence relation $v_1 \sim v_2$ if $v_1 - v_2 \in W$ > which given the structure of a vector space by defining addition and scalar multiplication of the equivalence class as: $(v_1 + W) + (v_2 + W) = (v_1 + v_2 + W), \qquad a(v + W) = (av + W).$
prop: dimension of quotient space	$\dim(V/W) = \dim(V) - \dim(W)$
> prop: isomorphic partition	All complements of a given subspace $W \preccurlyeq V$ are isomorphic to W/V > alle complements are isomorphic to each other
1.3.8 affine spaces	
def: affine space	= a set A of points {P,Q,…} together with a vector space V > for this space V the abelian group (V,+) of vector addition has a transitive free action on A

1.4 Algebras	
def: algebra	= a vector space V with a binary operation ⨀: VxV -> V, called a product of elements in V > this must satisfy: • left distributivity : $\forall u, v, w \in V$, $(u+v) \odot w = u \odot w + v \odot w$ • right distributivity : $\forall u, v, w \in V$, $u \odot (v+w) = u \odot v + u \odot w$ • compatibility with scalar multiplication: $\forall a, b \in \mathbb{F}$, $\forall v, w \in V$, $(av) \odot (bw) = a(v \odot (bw)) = b((av) \odot w) = ab(v \odot w)$. > bilinear operation
def: bilinear operation	= an operation that is linear in both arguments separately • $(a_1 v_1 + a_2 v_2) \odot w = a_1(v_1 \odot w) + a_2(v_2 \odot w)$ • $v \odot (b_1 w_1 + b_2 w_2) = b_1(v \odot w_1) + b_2(v \odot w_2)$ Ten opzichte van een basis $B = \{e_1, \ldots, e_n\}$: $(v^i e_i) \odot (w^j e_j) = v^i w^j (e_i \odot e_j) = v^i v^j \underbrace{f_{ij}^k}_{\text{structuurconstanten}} e_k$
def: alternating map	= a bilinear map that satisfies v⨀v = 0, ∀v∈V > this type of map is always anticommutative
def: lie algebra	= an algebra based on an alternating bilinear product referred to as *Lie Bracket* lie bracket: (v,w) ↦ [v,w], which satisfies the Jacobi identity: $[u,[v,w]] + [v,[w,u]] + [w,[u,v]] = o.$
prop: commutator	For an associative algebra (V,+, .) > we can always construct a Lie algebra by defining the lie bracket as: $[v, w] = v \cdot w - w \cdot v$ with *commutator* known as v.w - w.v = 0
def: division algebra	= an associative algebra in which non-zero elements have multiplicative inverses ie: for all $v \in V \setminus \{o\}$, a multiplicative inverse v^{-1}, so that $v \odot v^{-1} = v^{-1} \odot v = u$.
prop: dimension of an algebra	Any finite-dimensional division algebra V over an algebraically closed field 𝔽 is isomorphic to 𝔽 itself an thus has dim(V) = 1
prop: isomorphism of algebras	the only finite-dimensional division algebras over ℝ are isomorphic to ℝ, ℂ and ℍ