* **Recall**: a field $(k,+,\times)$ = set with two operations, $(k,+)$ abelian group with identity 0, $(k^* = k \setminus \{0\}, \times)$ abelian group with identity 1, distributive law.

* Polynomials: $k[x] := \{a_0 + a_1 x + \dots + a_n x^n \mid a_i \in k,\ n \in \mathbb{N}\}$ is a ring $\rightsquigarrow$ field of fractions = field of rational functions

$$k(x) = \left\{ \frac{p}{q} \;/\; p,q \in k[x],\ q \neq 0 \right\} \Big/ \frac{p}{q} \sim \frac{p'}{q'} \text{ iff } pq' = qp'.$$

(This generalizes to polynomials & rational functions in any number of variables)

* Power series: The ring of formal power series in x is $k[[x]] = \left\{ \sum_{i=0}^{\infty} a_i x^i \mid a_i \in k \right\}$
(add and multiply just like polynomials, term by term. check each coefficient in $(\sum a_i x^i)(\sum b_j x^j)$ is a finite expression).

Lemma: $\sum a_i x^i$ has a multiplicative inverse in $k[[x]]$ iff $a_0 \neq 0$.

Proof: We want $\sum_{i\geq 0} b_i x^i$ s.t. $\left(\sum_{i\geq 0} a_i x^i\right)\left(\sum_{i\geq 0} b_i x^i\right) = 1$. This gives

$$\left.\begin{array}{l} a_0 b_0 = 1 \\ a_0 b_1 + a_1 b_0 = 0 \\ a_0 b_2 + a_1 b_1 + a_2 b_0 = 0 \\ \dots \end{array}\right\}$$

$\to$ if $a_0 = 0$, clearly no solution; if $a_0 \neq 0$, we can solve inductively: $b_0 = \frac{1}{a_0}$, $b_1 = -\frac{a_1 b_0}{a_0}$, ...
(each step is $b_i = -(\dots)/a_0$ ✓). □

$\rightsquigarrow$ since every nonzero element of $k[[x]]$ is of the form

$$\underset{\substack{\uparrow \\ \text{first nonzero coefficient}}}{a_m} x^m + a_{m+1} x^{m+1} + \dots = x^m \underbrace{(a_m + a_{m+1} x + \dots)}_{\text{invertible}},$$

to get a field we just need to allow x^{-m}.

$\to$ **Def**: The field of Laurent series $k((x)) = \left\{ \sum_{i=m}^{\infty} a_i x^i \mid m \in \mathbb{Z},\ a_i \in k \right\}$.

* Given a field k, and a polynomial $f \in k[x]$ (of degree >0), we can evaluate $f(r)$, $r \in k$, and look for roots $r \in k$ st. $f(r) = 0$.
If there are none in k, we can form a field $K \supset k$ in which f has a root.

Ex: $k = \mathbb{Q}$, $x^2 - 2$ has no roots, but we can form
$\mathbb{Q}(\sqrt{2}) := \{a + b\sqrt{2} \mid a,b \in \mathbb{Q}\}$ which is a field: $\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} \in \mathbb{Q}(\sqrt{2})$

Ex: $k = \mathbb{R}$, $x^2 + 1 \rightsquigarrow \mathbb{R}(\underbrace{\sqrt{-1}}_{\text{usually called } i}) = \mathbb{C}$.

$\to$ On the other hand, over an algebraically closed field such as $\mathbb{C}$, every nonconstant polynomial already has a root, and there are no further algebraic extensions

* Given a field k, we always have a ring homomorphism $\varphi : \mathbb{Z} \to k$, $1 \mapsto 1_k$
(this determines φ, since 1 generates $\mathbb{Z}$) $\hookrightarrow$ $\varphi(a+b) = \varphi(a)+\varphi(b)$, $\varphi(ab) = \varphi(a)\varphi(b)$

Is this injective? For most fields we'll consider (eg. $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{R}(x), \mathbb{R}((x)), \dots$), it is.
If so, say k has <u>characteristic zero</u>. Otherwise:

<u>Prop:</u> $\ker(\varphi : \mathbb{Z} \to k) = \mathbb{Z}p$ for some prime p.

<u>Pf:</u> $\ker(\varphi)$ is a subgroup of $\mathbb{Z}$, hence of the form $\mathbb{Z}n$. If n is not prime, write $n = ab$ for $1 < a, b < n$. Then $\varphi(n) = \varphi(ab) = \varphi(a)\varphi(b) = 0 \in k$, but this implies $\varphi(a) = 0$ or $\varphi(b) = 0$ (if $\varphi(a) \neq 0$, multiply by $\varphi(a)^{-1}$ to get $\varphi(b) = 0$). Since by assumption n is the smallest positive integer s.t. $\varphi(n) = 0$, this is a contradiction. $\square$

<u>Def:</u> Say k has <u>characteristic p</u> if $\ker(\varphi) = \mathbb{Z}p$. (This means $p \cdot 1_k = \underbrace{1 + \dots + 1}_{p \text{ times}} = 0$!)

So far our only example of such a field is $\mathbb{Z}/p$, but there are more.

<u>Theorem:</u> For all $n \geq 1$ and prime p, there exists a unique field with p^n elements (up to isomorphism), and these are all the finite fields.

(There are also infinite fields of characteristic p, for example $\mathbb{Z}/p((x))$!).

<u>Vector spaces:</u>

<u>Def:</u> Fix a field k. A <u>vector space</u> over k is a set V with two operations:
(1) addition $+ : V \times V \to V$
(2) scalar multiplication $\cdot : k \times V \to V$
such that
(1) $(V, +)$ is an abelian group (denote by 0 the identity element)
(2) $1v = v \;\; \forall v \in V$
(3) $(ab)v = a(bv) \;\; \forall a, b \in k, \forall v \in V$ } identity and associativity for $\cdot$
(4) $(a+b)v = av + bv \;\; \forall a, b \in k \;\; \forall v \in V$
(5) $a(v+w) = av + aw \;\; \forall a \in k \;\; \forall v, w \in V$ } distributive property

(<u>Note:</u> $0v = 0 \;\; \forall v \in V$ using distributive property).

<u>Def:</u> A <u>subspace</u> of a vector space is a nonempty subset $W \subset V$ that is preserved by addition and scalar multiplication: $W + W \subset W$, $k \cdot W \subset W$.
(so W is also a vector space!) in fact $= W$ $\hookrightarrow$ this implies $0 \in W$.

<u>Examples:</u>
- $k^n = \{(a_1, \dots, a_n) \mid a_i \in k\}$ with componentwise addition / scalar mult.
- $k^\infty = \{(a_i)_{i \in \mathbb{N}} \mid a_i \in k\}$ (sequences in k) $\supset$ {sequences which are eventually zero}

- $k[[x]] \supset k[x]$ (isomorphic to the previous example!)
- given any set S, $k^S = \{\text{maps } f: S \to k\}$ ($k^\infty \Leftrightarrow$ case $S = \mathbb{N}$).
- $\{\text{maps } \mathbb{R} \to \mathbb{R}\} \supset \{\text{continuous maps}\} \supset \{\text{differentiable maps } \mathbb{R} \to \mathbb{R}\}$

<u>Span, linear independence, basis:</u> let V be a vector space $/k$.

<u>Def:</u> Given $v_1, \dots, v_n \in V$, the <u>span</u> of $v_1, \dots, v_n$ is the smallest subspace of V which contains $v_1, \dots, v_n$. Concretely, $\text{span}(v_1, \dots, v_n) = \{a_1 v_1 + \dots + a_n v_n \mid a_i \in k\}$

<u>Def:</u> say $v_1 \dots v_n$ <u>span V</u> if $\text{span}(v_1, \dots, v_n) = V$.

<u>Def:</u> We say $v_1, \dots, v_n \in V$ are <u>linearly independent</u> if

$$a_1 v_1 + \dots + a_n v_n = 0 \Rightarrow a_1 = a_2 = \dots = a_n = 0.$$

Equivalently, given $v_1, \dots v_n \in V$, we have a linear map $\phi: k^n \longrightarrow V$, $(a_1, \dots, a_n) \mapsto \sum a_i v_i$

$v_1, \dots v_n$ are linearly indep^t $\Leftrightarrow$ ϕ injective

$v_1 \dots v_n$ span V $\Leftrightarrow$ ϕ surjective.

<u>Def:</u> $(v_1, \dots, v_n)$ are a <u>basis</u> of V if they are linearly independent and span V.

Then any element of V can be expressed <u>uniquely</u> as $\sum a_i v_i$ for some $a_i \in k$.

<u>Ex:</u> $(1,0)$ and $(0,1)$ are a basis of k^2. So are $(1,1)$ and $(1,-1)$ for <u>most</u> fields k. (what if $\text{char}(k) = 2$?)

* We will see soon: if V has a basis with n elements, then every basis of V has n elements. We say the <u>dimension</u> of V is $\dim(V) = n$.

One can also consider infinite-dimensional vector spaces: for $S \subset V$ any subset,

<u>Def</u>
- $\text{span}(S)$ = smallest subspace of V containing S
  $= \{a_1 v_1 + \dots + a_k v_k \mid k \in \mathbb{N},\ a_i \in k,\ v_i \in S\}$
  (all <u>finite</u> linear combinations of elements of S)
- The elements of S are linearly independent if there are no <u>finite</u> linear relations:
  $a_1 v_1 + \dots + a_k v_k = 0$ $(a_i \in k,\ v_i \in S) \Rightarrow a_1 = \dots = a_k = 0.$
- S is a basis of V if its elements are linearly indep^t and span V.

<u>Example:</u>
- $\{1, x, x^2, x^3, \dots\}$ is a basis of $k[x]$.
- does $k[[x]]$ have a basis? what is it?

Linear maps:

Def. Let V, W be vector spaces $/k$. A homomorphism of vector spaces, or linear map, $\varphi: V \to W$, is any map that is compatible with the operations:
$$\varphi(u+v) = \varphi(u) + \varphi(v), \quad \varphi(\lambda v) = \lambda\varphi(v) \quad \forall \lambda \in k, \ \forall u, v \in V.$$

Prop: The set of linear maps $V \to W$ is itself a vector space$/k$, denoted $Hom(V,W)$.

Proof: Given $\varphi, \psi \in Hom(V,W)$, $\lambda \in k$, define $\begin{cases} \varphi+\psi \text{ by } (\varphi+\psi)(v) = \varphi(v) + \psi(v). \ \forall v \in V \\ \lambda\varphi \text{ by } (\lambda\varphi)(v) = \lambda \cdot \varphi(v) \end{cases}$

One can check that
- $\varphi + \psi$ and $\lambda\varphi$ defined in this way are linear maps (so we do have operations $+, \cdot$ on $Hom(V,W)$)
- these operations on $Hom(V,W)$ satisfy the axioms of a vector space. $\square$

(rather boring, but worth checking if you're not sure!)

- We'll soon see: if $\dim(V) = n$ and $\dim(W) = m$ then $\dim(Hom(V,W)) = mn$.
  (in bases for V and W, linear maps become $m \times n$ matrices!)

★ How does the choice of the field k matter when discussing vector spaces?
Given a subfield $k' \subset k$ (eg. $\mathbb{R} \subset \mathbb{C}$ or $\mathbb{Q} \subset \mathbb{R}$), a vector space over k can also be viewed as a vector space over k', by "restriction of scalars".
(namely, only look at scalar multiplication restricted to domain $k' \times V \subset k \times V$).
In particular, k itself is a vector space over k'!

Ex: $\mathbb{C}$ is a vector space over itself (of dim. 1, $\{1\}$ is a basis)
It is also a vector space over $\mathbb{R}$ (of dim 2, with basis $\{1, i\}$)

If V, W are $\mathbb{C}$-vector spaces hence also $\mathbb{R}$-vector spaces, any $\mathbb{C}$-linear map is also $\mathbb{R}$-linear, but the converse isn't true: $Hom_{\mathbb{C}}(V,W) \subsetneq Hom_{\mathbb{R}}(V,W)$

For example, complex conjugation $\begin{matrix} \mathbb{C} \longrightarrow \mathbb{C} \\ z = a+bi \mapsto \bar{z} = a-bi \end{matrix}$ is $\mathbb{R}$-linear: $\begin{cases} \overline{z_1+z_2} = \bar{z}_1 + \bar{z}_2 \\ \overline{az} = a\bar{z} \ \forall a \in \mathbb{R} \end{cases}$ but not $\mathbb{C}$-linear ($\overline{iz} \neq i\bar{z}$).

So: the choice of field k matters.

Bases and dimension:

★ Say V is finite-dimensional if there is a finite subset $\{v_1, \dots, v_m\}$ which spans V, ie. all elts of V are linear combinations $\sum a_i v_i$.

★ **Lemma:** if $\{v_1, \dots, v_m\}$ spans V, then a subset of $\{v_1 \dots v_m\}$ is a basis.

Proof: If the $\{v_i\}$ are linearly independent, they form a basis.
Otherwise, there is some linear relation $\sum a_i v_i = 0$, a_i not all zero.

This can be solved for v_i = a linear combination of the others if $a_i \neq 0$.
$\to$ remove v_i, $\{v_j / j \neq i\}$ still spans V.
Continue removing elements until the remaining ones are linearly indep^t. $\square$

* Thus, every finite-dimensional vector space has a basis.

* <u>Lemma:</u> If $\{v_1, \dots, v_m\}$ are linearly indep^t, there exists a basis of V which contains $\{v_1, \dots v_m\}$

<u>Proof:</u> Let $\{w_1, \dots, w_r\}$ be a spanning set for V. by induction we enlarge $\{v_1, \dots, v_m\}$ to a basis of $W_j = \mathrm{span}(\{v_1, \dots, v_m, w_1, \dots, w_j\}) \subset V$ for each $j = 0, \dots, r$.
For $j = 0$: $\{v_1, \dots, v_m\}$ basis of W_0.
Assuming $\{v_1, \dots, v_m, w_{i_1}, \dots w_{i_k}\}$ is a basis of $W_{j-1} = \mathrm{span}(\{v_1 \dots v_m, w_1, \dots, w_{j-1}\})$,
if $w_j \in W_{j-1}$ then we already have a basis of $W_j = W_{j-1}$.
otherwise, $\{v_1 \dots v_m, w_{i_1}, \dots, w_{i_k}, w_j\}$ are linearly indept. (why?) and span W_j.
This ends with a basis of $W_r = V$ (since $\{w_1, \dots, w_r\}$ span). $\square$

* <u>Theorem:</u> If $\{v_1, \dots, v_m\}$ and $\{w_1, \dots, w_n\}$ are bases of V, then $m = n$. (same # elements)

<u>Proof:</u>
- We claim $\exists j \in \{1..n\}$ st. $\{v_1, \dots, v_{m-1}, w_j\}$ is a basis.
  Indeed, $\{v_1, \dots, v_{m-1}\}$ are linearly independent, but don't span V
  (else $v_m \in \mathrm{span}\{v_1 \dots v_{m-1}\}$ gives a linear relation $\sum_{i=1}^{m-1} a_i v_i - v_{m+1} = 0$).
  So $\exists j$ st. $w_j \notin \mathrm{span}\{v_1 \dots v_{m-1}\}$ (else $w_1 \dots w_n$ can't span all V).
  Now $\{v_1, \dots, v_{m-1}, w_j\}$ are linearly independent (why?),
  but using all the v's, can write $w_j = \sum_{i=1}^{m} a_i v_i$ (necess. $a_m \neq 0$)
  So $v_m = \frac{1}{a_m}\left(w_j - \sum_{i=1}^{m-1} a_i v_i\right) \in \mathrm{span}(\{v_1 \dots v_{m-1}, w_j\})$
  and this implies $\{v_1 \dots v_{m-1}, w_j\}$ span V hence are a basis.
- Repeat this process to exchange one v for one w each time
  (we don't use the same w twice since the new w we pick has to be independent of the rest of our basis)
  We end up with only w's & get an m-element subset of $\{w_1, \dots, w_n\}$ that is also a basis. Necessarily this is all of $\{w_1 \dots w_n\}$, and $m = n$. $\square$

* <u>Def:</u> The <u>dimension</u> of V is the cardinality of any basis.