Let's start with leftoves in group theory from the previous lecture, (≡ end of lecture 4 notes) related to normal subgroups ($K \subset G$ st. $aKa^{-1} = K$ $\forall a \in G$) and commuting vs. not commuting.

* We've talked about the center $Z(G) = \{z \in G \mid az = za \ \forall a \in G\}$.

  Since elements of the center commute with everyone, they commute w/ each other, so $Z(G)$ is abelian! Also, $aZ(G)a^{-1} = Z(G)$, so $Z(G)$ is a normal subgroup of G.

* Another interesting object is the commutator subgroup $C(G) = [G,G] = \{\prod_{i=1}^{k} [a_i, b_i] \mid a_i, b_i \in G\}$

  where $[a,b] := aba^{-1}b^{-1}$ (the "commutator" of a & b, $= e$ iff $ab = ba$).

  This is a normal subgroup because $g^{-1} \prod_{i=1}^{k} [a_i, b_i]\, g = \prod_{i=1}^{k} [g^{-1}a_i g, g^{-1} b_i g]$.

  $\Rightarrow g^{-1} C(G)\, g = C(G)$. $\forall g \in G$.

  The quotient $G/[G,G]$ is called the abelianization of G.

  Since $[G,G]$ contains all commutators $[a,b]$, quotienting makes $[a,b] = e$ in the quotient group, ie. $ab = ba$ $\forall a, b \in G/[G,G]$.

  Since $[G,G]$ is generated by commutators, it is the smallest subgroup of G with that property. The abelianization is the largest abelian group onto which G admits a surjective homomorphism.

* The free group F_n on n generators $a_1, \dots, a_n$.

  Elements are all reduced words $a_{i_1}^{m_1} \dots a_{i_k}^{m_k}$ $\quad k \geq 0$ (empty word is e)

  $i_1 \dots i_k \in \{1 \dots n\}$ $\quad i_j \neq i_{j+1}$

  $m_1 \dots m_k \in \mathbb{Z} \setminus \{0\}$

  (non reduced words: reduce by:
  - if $i_j = i_{j+1}$, combine $a_i^m a_i^{m'} \rightsquigarrow a_i^{m+m'}$
  - if an exponent is zero, remove a_i^0).

  Repeat until word is reduced.

  - This is the "largest" group with n generators, all others are $\simeq$ quotients of F_n.

    If G is generated by $g_1, \dots, g_n \in G$, define a homomorphism

    $F_n \twoheadrightarrow G$ by $\prod a_{i_j}^{m_j} \mapsto \prod g_{i_j}^{m_j}$. ($\star$)

  - A finitely generated group is said to be finitely presented if the kernel of ($\star$) is the smallest normal subgroup of F_n containing some finite subset $\{r_1, \dots, r_k\} \subset F_n$, (ie. the subgroup generated by r_j's and their conjugates $x^{-1} r_j x$).

    ↳ words in the generators

    Write $G \cong \langle \underbrace{a_1, \dots, a_n}_{\text{generators}} \mid \underbrace{r_1, \dots, r_k}_{\text{relations}} \rangle$, then $G \cong F_n / \langle \text{conj's of } r_1 \dots r_k \rangle$

    Ex: $\mathbb{Z}^n \cong \langle a_1, \dots, a_n \mid a_i a_j a_i^{-1} a_j^{-1} \ \forall i,j \rangle$.

    Ex: $S_3 \cong \langle t_1, t_2 \mid t_1^2, t_2^2, (t_1 t_2)^3 \rangle$

Now we move on to rings & fields on the way to vector spaces. (Artin ch.3 / Axler ch.1-2)
(groups will return later).

Rings and fields:

Def: A (commutative) ring is a set R with two operations $+, \times$ such that
(1) $(R,+)$ is an abelian group with identity $0 \in R$
(2) $(R, \times)$ is a (commutative) semigroup with identity $1 \in R$, namely
- $1a = a1 = a \quad \forall a \in R$
- $a(bc) = (ab)c \quad \forall a,b,c \in R$.
- ($ab = ba \quad \forall a,b \in R$ if commutative)

(3) distributive law: $a(b+c) = ab + ac \quad \forall a,b,c \in R$.

Def: A field K is a commutative ring such that $\forall a \neq 0, \exists b = a^{-1}$ st. $ab = 1$.
ie. $(K \setminus \{0\}, \times)$ is an abelian group rather than a semigroup.

Rmk:
- the ring axioms imply $0a = a0 = 0 \ \forall a$. ($a0 = a(0+0) = a0 + a0$ + cancellation).
- the trivial ring $R = \{0\}$ is the only case where $0 = 1$. By convention this is not a field.
- most rings of interest to us are commutative. (Matrices are the main exception)
- in a field, $ab = 0 \Rightarrow a = 0$ or $b = 0$. Not necessarily true in a ring.
- hence, in a field, we have usual properties of cancellation (simplification) for both addition & multiplication.

Def: A ring/field homomorphism is a map $\varphi : R \to S$ that respects both operations:
$$\varphi(a+b) = \varphi(a) + \varphi(b)$$
($\leftarrow$ we've seen this implies $\varphi(0) = 0$, $\varphi(-a) = -\varphi(a)$)
$$\varphi(ab) = \varphi(a)\varphi(b)$$
$$\varphi(1_R) = 1_S$$
($\longleftarrow$ this doesn't follow from $\varphi(ab) = \varphi(a)\varphi(b)$, even for fields: consider $\varphi = 0$!)

Prop: If $\varphi : R \to S$ is a field homomorphism, then φ is injective.

Pf: if $a \neq 0$ then $\exists b$ st. $ab = 1_R$, so $\varphi(a)\varphi(b) = \varphi(ab) = 1_S \neq 0_S$ which implies $\varphi(a) \neq 0_R$. So $\ker(\varphi) = \{0\}$, hence φ injective.
↳ as additive group homom. □

Examples:
- $\mathbb{Z}$, $\mathbb{Z}/n$ are rings.
- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields. So is $\mathbb{Z}/p$ for p prime!!
This is denoted $\mathbb{F}_p$ when viewed as a field.

because: if $k \neq 0$ in $(\mathbb{Z}/p, +)$ then its order is p (divides p, $\neq 1$), so $\{0, k, 2k, \dots, (p-1)k\} = \mathbb{Z}/p$.
hence $\exists \ell \in \{0, \dots, p-1\}$ st. $\ell k = 1 \bmod p$. This gives the inverse!

* **Polynomials:** given a field k, the <u>ring of polynomials</u> in one formal variable x is $k[x] := \{a_0 + a_1 x + \dots + a_n x^n \mid a_i \in k,\ n \in \mathbb{N}\}$

<u>Remark:</u> x is a <u>formal</u> variable ie. not an element of anything, though we can <u>evaluate</u> a polynomial at an element of k or of any field containing k.

so: a polynomial $\Leftrightarrow$ a finite tuple of elements $(a_0, \dots, a_n, 0, 0, \dots)$ of k, with component-wise addition [but <u>not</u> componentwise multiplication! $x^i x^j = x^{i+j}$]

* $k[x]$ isn't a field, but it can be turned into a field by considering fractions (just like $\mathbb{Z}$ ring $\rightsquigarrow$ $\mathbb{Q}$ field): the <u>field of rational functions</u> is
$$k(x) = \left\{ \frac{p}{q} \;\middle|\; p, q \in k[x],\ q \neq 0 \right\} \Big/ \tfrac{p}{q} \sim \tfrac{p'}{q'} \text{ iff } pq' = qp'.$$

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

* **Power series:** The ring of <u>formal power series</u> in x is $k[[x]] = \left\{ \sum_{i=0}^{\infty} a_i x^i \;\middle|\; a_i \in k \right\}$

(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).

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

<u>Proof:</u> We want $\sum_{i \geq 0} b_i x^i$ st. $\left(\sum_{i \geq 0} a_i x^i\right)\left(\sum_{i \geq 0} b_i x^i\right) = 1$. 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 $b_i = -\frac{(\dots)}{a_0}$ ✓) $\square$

$\rightsquigarrow$ 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}.

$\to$ <u>Def:</u> The field of <u>Laurent series</u> $k((x)) = \left\{ \sum_{i=m}^{\infty} a_i x^i \;\middle|\; m \in \mathbb{Z},\ a_i \in k \right\}$.

* 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 $\left(\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} \in \mathbb{Q}(\sqrt{2})\right)$

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

Vector spaces:

Def: fix a field k. A vector space over k is a set V with two operations:
(1) addition $+ : V \times V \to V$
(2) scalar multiplication $\times : k \times V \to V$
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 $\times$
(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

(Note: $0v = 0 \ \forall v \in V$ using distributive property).

Def: A subspace 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 $= W$ ↗ ↳ this implies $0 \in W$.

Examples:
- $k^n = \{(a_1, \dots, a_n) \mid a_i \in k\}$ 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 $S = \mathbb{N}$).
- {maps $\mathbb{R} \to \mathbb{R}$} $\supset$ {continuous maps} $\supset$ {differentiable maps $\mathbb{R} \to \mathbb{R}$}

Basic notions about vector spaces: let V be a vector space $/k$.

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

Def: say $v_1 \dots v_n$ span V 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 indept $\Leftrightarrow$ 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 most fields k.
(what's the catch? see next time)

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:
  $a_1 v_1 + \dots + a_k v_k = 0 \quad (a_i \in k,\ v_i \in S) \Rightarrow a_1 = \dots = a_k = 0.$
- S is a basis of V if its elements are linearly indept 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?