Lecture 18 – Friday Oct 16 2020

Recall: • $V^{\otimes d}$ = vector space gen^d by pure tensors $v_1 \otimes \dots \otimes v_d$, $v_i \in V$
tensor power with relations so that $V \times \dots \times V \xrightarrow{\mu} V^{\otimes d}$ is multilinear
$(v_1, \dots, v_d) \mapsto v_1 \otimes \dots \otimes v_d$

(+ multilinear maps $V \times \dots \times V \underset{m}{\to} U \longleftrightarrow$ linear maps $V^{\otimes d} \underset{\varphi}{\to} U$
$m = \varphi \circ \mu$

+ $\mathrm{Sym}^d V$ same for symmetric multilinear maps.

Exterior algebra: do the same thing for skew-symmetric, aka alternating, multilinear forms.

Def: $\eta \in V^{\otimes d}$ is alternating if $\sigma(\eta) = (-1)^\sigma \eta \quad \forall \sigma \in S_d$.
$\Lambda^d(V) = \{\text{alternating tensors}\} \subset V^{\otimes d}$.

sign of σ :: -1 for transpositions & products of odd # of them.

• In characteristic zero, we can view $\Lambda^d(V)$ as the image of skew-symmetrization operator $\beta : V^{\otimes d} \longrightarrow V^{\otimes d}$

$$\beta(v_1 \otimes \dots \otimes v_d) = \frac{1}{d!} \sum_{\sigma \in S_d} (-1)^\sigma v_{\sigma(1)} \otimes \dots \otimes v_{\sigma(d)} \overset{\text{def}^n/\text{notation:}}{=:} v_1 \wedge \dots \wedge v_d.$$

This is zero whenever $v_i = v_j$ for some $i \neq j$ ... and so by multilinearity, whenever $v_1 \dots v_d$ are linearly dependent. Thus $\Lambda^d(V) = 0$ whenever $d > \dim V$!

• Alternative definitions: $\Lambda^d(V)$ = quotient of $V^{\otimes d}$ by the subspace spanned by $v_1 \otimes v_2 \otimes v_3 \otimes \dots \otimes v_d + v_2 \otimes v_1 \otimes v_3 \otimes \dots \otimes v_d$ and similarly for other transpositions swapping two factors

Or: $\Lambda^d(V)$ vector space with an alternating multilinear map $V \times \dots \times V \longrightarrow \Lambda^d V$
$(v_1, \dots, v_d) \mapsto v_1 \wedge \dots \wedge v_d$ $\quad (v_1 \wedge v_2 = -v_2 \wedge v_1$ etc.)

and universal for alternating multilinear maps on $V \times \dots \times V$.

• If $(e_1, \dots, e_n)$ are a basis of V then $e_{i_1} \wedge \dots \wedge e_{i_d}$, $i_1 < \dots < i_d$ basis of $\Lambda^k V$.

• We have a product $\Lambda^k V \times \Lambda^\ell V \longrightarrow \Lambda^{k+\ell} V$ induced by tensor algebra + skew symmetrization. $(v_1 \wedge \dots \wedge v_k) \wedge (w_1 \wedge \dots \wedge w_\ell) = v_1 \wedge \dots \wedge v_k \wedge w_1 \wedge \dots \wedge w_\ell$.

This makes the exterior algebra $\Lambda^\bullet V = \bigoplus_{d \geq 0} \Lambda^d V$ into a (skew-commutative) ring

ie. if $\eta \in \Lambda^k V$, $\xi \in \Lambda^\ell V$ then $\eta \wedge \xi = (-1)^{k\ell} \xi \wedge \eta$.

(check: $\dim \Lambda^\bullet V = 2^{\dim V}$).

Volume & determinant:

②

- If $\dim V = n$, then $\dim \Lambda^n V = 1$ (if $e_1 \dots e_n$ basis of $V \rightsquigarrow e_1 \wedge \dots \wedge e_n \in \Lambda^n V$)

  A <u>choice</u> of isomorphism $\Lambda^n V \xrightarrow{\sim} k$ is determined by the data of a <u>volume form</u> $vol \in \Lambda^n V^* = (\Lambda^n V)^*$, $vol \neq 0$, ie. a nondegenerate alternating multilinear map

$$V \times \dots \times V \to k$$
$$v_1, \dots, v_n \mapsto vol(v_1, \dots, v_n)$$

  (Think of: signed volume of parallelepiped with edge vectors $v_1, \dots, v_n$ is naturally $v_1 \wedge \dots \wedge v_n \in \Lambda^n V$, becomes a scalar given $\Lambda^n V \xrightarrow{\sim} k$).

- Eg, in a real inner product space with orthonormal basis $(e_1, \dots, e_n)$, the natural volume form is $vol = e_1^* \wedge \dots \wedge e_n^*$, so $vol(e_1, \dots, e_n) = 1$. (⚠ reordering basis gives ± 1... <u>orientation</u>!) (volume of unit cube is 1). Using basis to identify $V \simeq \mathbb{R}^n$,

$$vol(v_1, \dots, v_n) = (e_1^* \wedge \dots \wedge e_n^*)(v_1, \dots, v_n) = \sum_{\sigma \in S_n} (-1)^\sigma (e^*_{\sigma(1)} \otimes \dots \otimes e^*_{\sigma(n)})(v_1 \dots v_n)$$

$v_j = \begin{pmatrix} v_{1j} \\ \vdots \\ v_{nj} \end{pmatrix}$ for each j

$$= \sum_{\sigma \in S_n} (-1)^\sigma v_{\sigma(1)1} \dots v_{\sigma(n)n} = \det(v_1 \dots v_n)$$

the determinant of an $n \times n$ matrix!

Recall that the determinant of a matrix is $\det(A) = \sum_{\sigma \in S_n} (-1)^\sigma \prod a_{\sigma(j)j}$.

$\det(A)$ is the only quantity which is
- multilinear in the columns of the matrix
- alternating (swap two columns $\rightsquigarrow -\det$).
- $\det(Id) = 1$.

- Even though the notion of determinant / volume of $n = \dim V$ vectors requires a choice of volume form (isom. $\Lambda^n V \xrightarrow{\sim} k$) the notion of <u>determinant of a linear operator</u> requires no such choice!

→ Usual definition: given $T: V \to V$, define $\det(T) = \det(A)$, $A = \mathcal{M}(T)$ in any basis, using $\det(AB) = \det A \det B$, so under change of basis, $\det(P^{-1}AP) = \det A$.
↳ usual proof is painfully explicit.

→ Better definition: exterior power is a functor, so $T: V \to V$ induces a linear operator $\Lambda^n T : \Lambda^n V \to \Lambda^n V$ (explicitly, $(\Lambda^n T)(v_1 \wedge \dots \wedge v_n) = T(v_1) \wedge \dots \wedge T(v_n)$)
But $\dim(\Lambda^n V) = 1$, and any linear operator on a 1-dim. vector space is a scalar multiple of id. ⇒ define $\det(T) \in k$ such that $\Lambda^n T = \det(T)\, id$.

(This expresses the fact that T scales volume of parallelepipeds in V by a factor of $\det(T)$, without having to choose $\Lambda^n V \xrightarrow{\sim} k$ to measure those volumes).

Using this definition of the determinant via $\Lambda^n T$, independence of choice of basis is manifest, and so is the fact that $\det(T_1 T_2) = \det(T_1)\det(T_2)$!

Linear algebra over rings: modules (Artin §14.1 - 14.2)

Let R be a commutative ring (with $1 \neq 0$) (ie. relax field axioms to not require multiplicative inverses). Main examples $R = \mathbb{Z}, \mathbb{Z}/n, k[x], k[x_1, \dots x_n]$.

<u>Def</u>: A <u>module</u> M over a ring R is a set with two operations:
- $+ : M \times M \to M$ addition, st. $(M, +)$ is an abelian group.
- $\times : R \times M \to M$ scalar multiplication, st. $(ab)v = a(bv)$, $a(v+w) = av + aw$, $(a+b)v = av + bv$, $0v = 0$, $1v = v$.

<u>Ex</u>:
- $R^n = \{(x_1, \dots x_n) \mid x_i \in R\}$ with componentwise operations is the <u>free module</u> of rank n over R.
- any abelian group is a $\mathbb{Z}$-module $(n \cdot g = \overbrace{g + \dots + g}^{n \text{ times}})$ - check details (homework)

<u>Def</u>:
- $\Gamma \subset M$ <u>spans</u> M (or <u>generating set</u>) if every element of M is a (finite) linear combination $\sum a_i v_i$, $v_i \in \Gamma$, $a_i \in R$.
  Equivalently: the map $\varphi : R^\Gamma \to M$, $(a_i) \mapsto \sum a_i v_i$ is surjective.
  M is <u>finitely generated</u> if it has a finite spanning set.
- the elements of $\Gamma \subset M$ are <u>(linearly) independent</u> if $\varphi : R^\Gamma \to M$ is injective, ie $\sum a_i v_i = 0$, $v_i \in \Gamma$, $a_i \in R \Rightarrow a_i = 0 \ \forall i$
- the elements of $\Gamma \subset M$ form a <u>basis</u> if $\varphi : R^\Gamma \to M$ is an isomorphism.
  In this case, say M is a <u>free module</u>.

General fact about modules: <u>nothing is true</u>!
- A basis need not exist!
  <u>Ex</u>: $M = \mathbb{Z}/n$ as $\mathbb{Z}$-module: $nx = 0 \ \forall x \in M$ so $\varphi : \mathbb{Z}^\Gamma \to M$ can't be injective!
- Even if M is free (admits a basis):
  - a linearly independent set may not be a subset of a basis.
    <u>Ex</u>: $M = \mathbb{Z}$ as $\mathbb{Z}$-module, $\nexists$ basis $\ni 2$.

- a spanning set need not contain a subset which is a basis

  Ex: $M = \mathbb{Z}$ as $\mathbb{Z}$-module, $\{4,5\}$ span $\mathbb{Z}$ (since $n = n.5 - n.4$) but aren't independent $(5.4 - 4.5 = 0)$, & neither subset $\{4\}$ or $\{5\}$ spans all of $\mathbb{Z}$.

- A submodule of a finitely generated module need not be finitely generated

  Ex: $R = k[x_1, x_2, \dots]$ polynomials in ∞ many variables
  $M = R$ as R-module is generated by the element 1.
  $M' = \{$polynomials whose constant term is zero$\} \subset M$ is a submodule, but not finitely gen^{d} (any finite subset only involves finitely many x_i's, can't span the other x_k's).

  (by contrast, this holds for modules over <u>Noetherian rings</u>, including $\mathbb{Z}$, $k[x_1 \dots x_n]$ and many others).

Def: M, N modules over R, a module homomorphism $\varphi \in \mathrm{Hom}_R(M,N)$ is a map $\varphi: M \to N$ st. $\varphi(v+w) = \varphi(v) + \varphi(w)$ and $\varphi(av) = a\varphi(v)$.

Observe: $\mathrm{Hom}_R(M,N)$ is itself an R-module: $(\varphi + \psi)(v) = \varphi(v) + \psi(v)$
$(a\varphi)(v) = a\varphi(v)$.

For free modules, things work as expected: $\mathrm{Hom}_R(R^m, R^n) \cong R^{m \times n}$
(φ is determined by images $\varphi(e_i) \in R^n$ of the basis vectors of R^m)

but we can have nonzero modules M, N st. $\mathrm{Hom}_R(M,N) = 0$!

Ex: $R = k[x]$, $M = k$ with multiplication $(a_0 + a_1 x + \dots).b = a_0 b$.
Then $\mathrm{hom}_R(k, k[x]) = 0$ (because $1 \in k$ satisfies $x.1 = 0$ so must map to $\varphi(1) = p(x) \in k[x]$ st. $x p(x) = 0 \Rightarrow p = 0$.

Remarks:
- R is a module over itself (free module of rank 1)

  A submodule of R is called an <u>ideal</u>: this is a subset $N \subset R$ st.
  - N is an abelian subgroup of $(R, +)$
  - $R \cdot N \subseteq N$: mult. by <u>any</u> element of R takes N to itself

  Ex: Ideals in $\mathbb{Z}$ are $n\mathbb{Z}$
  $k[x]$ are $p(x)\,k[x]$
  $\}$ ie. generated by a single element. This is very special.

  ($\mathbb{Z}$ and $k[x]$ are "principal ideal domains". This has to do with Euclidean division algorithms: $\mathrm{span}(p,q) = \mathrm{span}(\gcd(p,q))$).

- The quotient of an R-module by a submodule is an R-module.

  Ex: $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/n$ as $\mathbb{Z}$-module

  $k[x]/xk[x] = k$ as $k[x]$-module (example above).

  (The quotient of R itself by a submodule = ideal is, in fact, not just an R-module but also a ring in its own right).

The study of modules is a vast subject, which we won't study further, with one exception: we're returning to group theory, but we start with a short account of the classification of <u>finitely generated abelian groups</u> (= $\mathbb{Z}$-modules)

<u>Theorem</u>: Any finitely generated abelian group is isom. to a product of cyclic groups

$$G \cong (\mathbb{Z}/n_1 \times \dots \times \mathbb{Z}/n_k) \times \mathbb{Z}^l$$

(+ using $\mathbb{Z}/mn \simeq \mathbb{Z}/m \times \mathbb{Z}/n$ iff $\gcd(m,n)=1$, can rearrange the finite factors eg. to arrange all n_i = powers of primes).