Week 8

Exterior Algebra

8.1 Linear Algebra Review and Rational Canonical Form

2/20:

- Nori's change of heart.
  - We've all seen linear algebra; thus, we'll speedrun it and then do exterior algebra and determinants. That's where we'll finish.
- The following is part 1 of a linear algebra course.
- Let F be a field.
- **Vector space**: An F-module. *Denoted by* $\boldsymbol{V}$.
- **Linearly independent** (subset $S \subset V$): Same definition we're familiar with.
- **Spanning** (subset $S \subset V$): A subset S of V that is a set of generators of V.
- **Basis** (subset $S \subset V$): A subset S of V that generates V and is linearly independent.
- Theorem: Every linearly independent subset of V can be extended to a basis.
- Theorem: Every spanning set S contains a basis.
  - Any maximal linearly independent subset of S is a basis.
- Theorem: S_1, S_2 are bases for V implies that $|S_1| = |S_2|$.
  - The replacement theorem in Dummit and Foote (2004) is a good way to prove this.
- **Dimension** (of a vector space): The cardinality of a basis set of V. *Denoted by* $\dim \boldsymbol{V}$.
- We will focus on *finite dimensional* vector spaces herein.
- Theorem: If V' is a linear subspace of V, then $\dim(V) = \dim(V/V') + \dim(V')$.
- We are now done with part 1; what's next constitutes part 2 of a linear algebra course.
- Let $T : V \to V$ denote a linear transformation.
- Let A be a ring. What is an $A[X]$-module M?
  - It is an abelian group $(M, +)$ and a ring homomorphism $\rho : A[X] \to \mathrm{End}(M, +)$.
    - Refer to Dummit and Foote (2004, pp. 340–42), which is in Section 10.1.
  - Since $A \hookrightarrow A[X]$, $\rho|_A$ turns M into an A-module as well.

- An alternate perspective from which to view $A[X]$-modules such as M.
  - Define $\rho(X) : M \to M$ by $\rho(X)(m) = Xm$ for all $m \in M$ and some fixed $X \in A$.
  - As in Lecture 1.2, we postulate the commutativity of A (at least that $C_A(X) = A$) so that $aX = Xa$ for all $a \in A$.
  - It follows since ρ is a ring homomorphism that
$$\rho(aX) = \rho(Xa)$$
$$\rho(a)\rho(X) = \rho(X)\rho(a)$$
  - But since we consider M to be a module, we write $a := \rho(a)$. Thus, $a\rho(X)(m) = \rho(X)(am)$ for all $m \in M$.
  - Additionally, note that $\rho(X) \in \mathrm{End}_A(M)$ (which is the set of all A-module endomorphisms).
  - It follows from everything above that $\rho(X) : M \to M$ is an A-module homomorphism.
  - Put $T := \rho(X)$. Thus, an $A[X]$-module gives rise to a pair (M, T), where M is an A-module and $T \in \mathrm{End}_A(M)$.
  - Conversely, such (M, T) gives rise to an $A[X]$-module with action
$$\left(\sum_{n=0}^{\ell} a_n X^n\right) m = \sum_{n=0}^{\ell} a_n T^n m$$
- Let F be a field, and consider (V, T) where V is any (finite dimensional) F-vector space and $T : V \to V$ is a linear transformation.
  - This turns V into an $F[X]$-module.
- (V, T) with V finite dimensional induces $\rho : F[X] \to \mathrm{End}_F(V) \cong M_n(F)$ defined by $X \mapsto T$.

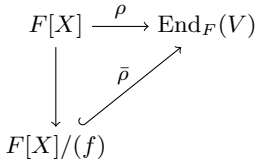

Figure 8.1: $F[X]$-module actions.

  - To define ρ on all of $F[X]$, the universal property of a polynomial ring asserts that we need only state $\rho(X) = T$ and $\rho(c) = c$ for all $c \in F$.
- Let's talk about $\ker(\rho)$.
  - $\ker(\rho) = (f)$ for some monic polynomial f of degree $d \leq n^2$.
    - We know that $\dim \mathrm{End}_F(V) = n^2$. Thus, the list $I, T, T^2, \ldots, T^{n^2}$ *must* be linearly dependent since it contains $n^2 + 1$ elements of $\mathrm{End}_F(V)$.
    - It follows that $1 + \cdots + X^{n^2} \in \ker(\rho)$, so if we are to have $1 + \cdots + X^{n^2} \in (f)$, we must have $\deg(f) \leq n^2$.
  - We have the constraint on the degree of f by the isomorphism from Lecture 3.1.
- **Minimal polynomial** (of T): The polynomial f that generates $\ker(\rho)$.
  - Alternate definition: The monic polynomial f of least degree such that the linear transformation $f(T) : V \to V$ equals the zero transformation.

- In particular, since the minimal polynomial f kills everything in V, we have that V is a torsion $F[X]$-module. The hypothesis that V is finite dimensional further proves that V is finitely generated.
  - Note that we do not even need the definition of the minimal polynomial to conclude that a finite dimensional vector space is torsion.
  - Indeed, let $v \in V$ be arbitrary. Then by the dimensional constraint on $\mathrm{End}_F(V)$, the sequence of vectors $v, Tv, T^2v, \dots$ becomes linearly dependent at some k. At this k, we obtain
$$T^k v = a_0 v + a_1 Tv + \cdots + a_{k-1} T^{k-1} v$$
  - Defining
$$g_v(T) = T^k - (a_0 + a_1 T + \cdots + a_{k-1} T^{k-1})$$
    implies that
$$g_v(T)v = T^k v - (a_0 v + a_1 Tv + \cdots + a_{k-1} T^{k-1} v) = 0$$
    i.e., $v \in \mathrm{Tor}(M)$ since $g_v(X) \in F[X]$.
- **Cyclic vector** (for T): A vector $v \in V$ belonging to (V, T) such that $v, Tv, T^2v, \dots$ spans V.
- Using cyclic vectors to compute the minimal polynomial.
  - Assume $v, Tv, T^2v, \dots, T^{k-1}v$ are linearly independent, but $v, Tv, \dots, T^k v$ are not.
  - Then
$$T^k v = a_0 v + a_1 Tv + \cdots + a_{k-1} T^{k-1} v$$
    where all $a_i \in F$ and not all $a_i = 0$.
  - Let $W = \langle v, Tv, \dots, T^{k-1}v \rangle$. It follows that $T^m v \in W$ for all $m \in \mathbb{Z}_{\geq 0}$.
  - Let
$$g(X) = X^k - (a_{k-1} X^{k-1} + \cdots + a_1 X + a_0)$$
  - Then $g(T)v = 0$. This implies that g is the minimal polynomial of T as follows.
    - Any polynomial f of degree less than k will map v to a linear combination of the k linearly independent elements $v, Tv, T^2v, \dots, T^{k-1}v$. But since these are linearly independent, if f annihilates them, we must have $f = 0$.
    - Thus, k is the minimum degree that the minimal polynomial can have.
    - To recap, at this point, we have proven that $g \in \ker(\rho)$ and no element of $\ker(\rho)$ besides 0 has lesser degree.
    - We now prove that $\ker(\rho) = (g)$. Let $f \in \ker(\rho)$. Then $f = qg + r$ by the Euclidean algorithm for monic polynomials, where $\deg(r) < k$. Additionally,
$$0 = f(T)v = q(T)g(T)v + r(T)v = q(T) \cdot 0 + r(T)v = r(T)v$$
      so $r \in \ker(\rho)$. It follows by the above that $r = 0$. Therefore, $f = qg \in (g)$. The inclusion $(g) \subset \ker(\rho)$ follows from the definition of an ideal and the fact that $\ker(\rho)$ is an ideal by a previous result.
  - Let $h \in \mathbb{Z}_{\geq 0}$ be arbitrary. Then
$$\begin{aligned} 0 &= T^h(0) \\ &= T^h g(T)v \\ &= T^h(T^k - (a_{k-1}T^{k-1} + \cdots + a_1 T + a_0))v \\ &= (T^{h+k} - (a_{k-1}T^{h+k-1} + \cdots + a_1 T^{h+1} + a_0 T^h)) \\ &= (T^k - (a_{k-1}T^{k-1} + \cdots + a_1 T + a_0))T^h v \\ &= g(T)T^h v \end{aligned}$$
    as well.

    - We can also rationalize $g(T)T^h = T^h g(T)$ by pulling everything back to the domain of polynomials and noting that polynomial multiplication is commutative.
  - It follows that $g(T)w = 0$ for all $w \in W$.
  - Assume v is a cyclic vector. Then $W = V$. It follows that $g(T)v = 0$ for all $v \in V$.

- We now summarize many of the above results (and a further one to come) in the following lemma.
  - This lemma is taken from the Week 8 summary.

- Lemma: Let $T : V \to V$ be a linear transformation of a finite dimensional vector space V over a field. Then TFAE.

  (i) There exists a cyclic vector $v \in V$ for T.

  (ii) V has a basis $e_1, \ldots, e_n$ such that $Te_i = e_{i+1}$ for all $i = 1, \ldots, n-1$

  (iii) V, when regarded as an $F[X]$-module, is isomorphic to $F[X]/(f)$ for some monic polynomial $f \in F[X]$.

- Let $V = F[X]/(f)$.
  - Recall that if $\deg(f) = d$, then this is a vector space with basis $1, \overline{X}, \ldots, \overline{X^{d-1}}$.
  - Let $T : V \to V$ be the left multiplication by $\overline{X}$ linear transformation.
  - It follows that if $v_i = \overline{X^{i-1}}$ $(i = 1, \ldots, d)$, then

$$Tv_i = v_{i+1}$$

    for $i = 1, \ldots, d-1$.
  - Additionally, $Tv_d = \overline{X^d}$ will be expressable in terms of the basis, i.e.,

$$Tv_d = -(a_0 v_1 + a_1 v_2 + \cdots + a_{d-1} v_d)$$

  - If $d = 3$, then we have

$$M(T) = \begin{pmatrix} 0 & 0 & -a_0 \\ 1 & 0 & -a_1 \\ 0 & 1 & -a_2 \end{pmatrix}$$

  - The above matrix is called the **companion matrix** of f, for f monic of degree 3.

- **Rational canonical form**: The decomposition of the $F[X]$-module (V, T) defined as follows, where $f_2 \mid f_1$, …, $f_s \mid f_{s-1}$, and $\deg(f_s) > 0$. *Given by*

$$F[X]/(f_1) \oplus \cdots \oplus F[X]/(f_s)$$

  - When $V = 0$, then $s = 0$. In this case, f_1 is the minimal polynomial of T.
  - The form consisting of a block diagonal matrix of companion matrices.

- ***a*-eigenspace** (of a linear transformation): The set of all vectors $v \in V$ for which $Tv = av$, where T is the linear transformation in question and $a \in F$. *Given by*

$$\{v \in V : Tv = av\}$$

  - Note: In $F[X]$, any $p = X - a$ is a prime. It follows that the a-eigenspace of T is the collection of all $v \in V$ that are annihilated by $(X - a)$.

- ***p*-primary** ($F[X]$-module): An $F[X]$-module (V, T) for which there exists an n such that $(T-a)^n v = 0$ for all $v \in V$.

- How exactly is $(T - a)^n$ a linear transformation?

  - $1_V : V \to V$ is the identity.
  - $a \cdot 1_V = a_V : V \to V$.
  - $(T - a_v)^n = 0 \in \mathrm{End}_F(V)$.

- **Generalized a-eigenspace** (of a linear transformation): The $(X-a)$-primary component of V, when regarded as an $F[X]$-module.
  - Alternative definition: The collection of all $v \in V$ such that $(T-a)^k v = 0$ for some $k \in \mathbb{Z}_{\geq 0}$, where T is the linear transformation of interest.
- **Algebraically closed** (field): A field F for which every irreducible polynomial $f \in F[X]$ is of degree 1.
- Example: $\mathbb{C}$ is algebraically closed.
- **Jordan canonical form** (of a linear transformation): The decomposition of the corresponding $F[X]$-module (V, T), where T is the linear transformation of interest, as the direct sum of $F[X]/(X-a_i)^{k_i}$ where the a_i are not necessarily distinct.
  - Has to do with p-primary components!
  - See Theorem **??** and the associated discussion for more.
- Let $V = F[X]/(X-a)^n$. We now seek to compute $T : V \to V$ defined by $T(v) = l_X(v)$. In particular, this is what we do to every component in the Jordan decomposition. What we do here is take the basis

$$e_i = \overline{(X-a)^{n-i}}$$

  for $i = 1, \ldots, n$ and then realize that

$$T(e_1) = ae_1 \qquad T(e_2) = e_1 + ae_2 \qquad T(e_3) = e_2 + ae_3 \qquad \cdots \qquad Te_n = e_{n-1} + ae_n$$

  - This lends itself to the creation of a typical Jordan block.
- More specifically, let $V = F[X]/(X-a)^n$, and let $v_1 = \overline{1}$, $v_2 = \overline{X-a}$, $\ldots$, $v_n = \overline{(X-a)^{n-1}}$.
  - Under the same definition of T as above, we know that

$$Tv_{r+1} = Xv_{r+1} = X(X-a)^r = (X-a+a)(X-a)^r = (X-a)^{r+1} + a(X-a)^r = v_{r+2} + av_{r+1}$$

  - The matrix of this linear transformation is the Jordan block

$$\begin{pmatrix} a & 0 & 0 & 0 \\ 1 & a & 0 & 0 \\ 0 & 1 & a & 0 \\ 0 & 0 & 1 & a \end{pmatrix}$$

    - Note that Nori writes Jordan blocks as above, not with 1's in the superdiagonal.
    - Thus, the *last* generalized eigenvector is an eigenvector here, instead of the *first*.
- There's one more canonical form, too.
- Since no one knows what canonical forms are and we very much need them for what Nori was planning to do, Nori will change his plans. No tensors in the last week, either.

8.2 Office Hours (Nori)

- Midterm: We never covered the universal property of a quotient in class, did we?
  - That's the special lemma from last office hours.
- PSet 7: 7.3 and 7.4 typos.
- Wednesday lecture?
  - Seventh week summary will suffice.
- What do you need us to know about the rational canonical form? Should I still read Dummit and Foote (2004), Section 12.2 or is that no longer necessary?
  - Nori will probably push ahead with 12.2. Thus I should read it. He's not sure what he'll do beyond that, though, since he doesn't want to jam tensors into the last week.
  - I will need tensor products for representation theory, regardless, so if I want to take it, I should self-study it.
  - No chance tensor products will be covered next quarter.
  - Serre is a terrific mathematician whose wife is a super chemist, and that's why he wrote his book on representation theory (and wrote it in a less terse manner than usual).
  - No tensors means no exterior algebra, too.
  - Nori hasn't read any of Dummit and Foote (2004).
  - The transfer theory of groups arises in a later chapter, and that's important for representation theory, though.
- Nori doesn't think any teacher pays attention to what courses are supposed to cover as stated in the course catalog.
  - We will never do modules, multilinear and quadratic forms.
  - p-adic field and Galois theory.
  - Nori thinks the proof of Theorem 12.4 is very difficult to follow for a first-timer.
  - Solvable groups were supposed to be a MATH 25700 topic, but got cut because of 9-week quarters.
  - Syclotomic fields have applications to the representation theory of finite groups; there are theorems of representation theory that you need syclotomic fields to prove.
  - Emil Artin: Galois Theory is worth looking up.
  - Gauss and constructions of 17-gons also needs syclotomic fields.

8.3 Office Hours (Nori)

2/21:

- Lecture 6.1: Proposition proof?
- Lecture 6.1: $(2) \subsetneq \mathbb{Z}$ example?
- Lecture 6.1: The end of the theorem proof.
- Lecture 6.2: Does the first theorem you proved not appear in the book until Chapter 12?
- Lecture 6.2: What is A in the proof?
- Resources for the proofs in Week 6?
- Lecture 7.1: Quotient stuff.

- Lecture 7.2: Why does $\text{Ann}(v) = (p^k)$, why not just $(p^k) \subset \text{Ann}(v)$? Additionally, how does $p^k w' = 0$ imply that $p^k \in \text{Ann}(w)$?
  - R is a PID!
  - $\text{Ann}(w)$ should be $\text{Ann}(w')$ in the centered line.
  - We don't need to know the theorem from the book for a while (second year of graduate school at least).
  - It's good to know the proofs from class just for going forward in math, but we probably will not be asked to reproduce them on an exam.
- Lecture 7.3: RCF proof?
  - It's not $m_i, 1$, it's $m_{i,1}$!
  - Rewrite the proof when I'm awake enough to understand it.

8.4 Noncommutative Polynomial Rings

2/22:

- Adjusted syllabus for those of us who haven't seen block matrices.
  - We're not gonna cover all of the stuff in Sections 12.2-12.3.
  - We'll define determinants via exterior algebras and use them to prove the Cayley-Hamilton theorem.
- Notation for today:
  - We fix R a commutative ring.
  - Any other ring considered is potentially noncommutative.
  - c denotes an element of R.
- ***R*-algebra**: A pair (A, ϕ) where A is a ring and $\phi : R \to A$ is a ring homomorphism such that

$$\phi(c)a = a\phi(c)$$

  for all $a \in A$ and $c \in R$.
  - I.e., we have commutativity with the "integers."
  - Notation: We suppress the letter ϕ.
    - Justification: A can be considered an R-module in a natural manner, so we can use the standard notation $c \cdot a$ in place of $\phi(c) \cdot a$ because we can think of ϕ as the action of R on A.
  - R-algebras are automatically R-modules.
  - $\phi(R)$ is a subring of A (and, specifically, the center of A).
- Now we get into noncommutative polynomial rings.
  - We've defined polynomial rings on one variable, and on multiple variables by induction.
  - There, the variables commuted. However, they need not! We can construct rings such that $XY \neq YX$.
- Consider the ring consisting of n potentially noncommutative variables over the coefficients in R.
  - Essentially, we postulate that $1, X_1, X_2, \ldots, X_n$ are in the ring and consider the set of everything that can be generated from these elements via addition, multiplication, and the action of R.
  - Thus, things like $X_i X_j$ exist. Note that there are n^2 of these. Things like $X_i X_j X_k$ also exist (and there are n^3 of these).

- Polynomials will be of the form

$$c_0 + \sum_{i=1}^{n} c_i X_i + \sum_{\substack{1\le i\le n\\ 1\le j\le n}} c_{i,j} X_i X_j + \cdots$$

  - This polynomial has degree at most n.
    - Really?? How does Nori define degree? This would appear to be a break from the convention introduced in Section 9.1.
  - Note that since this is not a **noncommutative power series ring**, we assume that all polynomials have a finite degree.

- **Free R-algebra** (on the set S): The free R-module on the set $\{1\} \sqcup S \sqcup S \times S \sqcup S \times S \times S \sqcup \cdots$. *Denoted by* $\boldsymbol{F_R(S)}$.
  - Elements of the set include 1, X_s for all $s \in S$, $X_s X_t$ for all $s, t \in S$, etc.
  - Multiplication is still associative: $(X_{s_1} X_{s_2})(X_{t_1} X_{t_2} X_{t_3}) = X_{s_1} X_{s_2} X_{t_1} X_{t_2} X_{t_3}$.
  - We still have commutativity for coefficients (i.e., $X_s c = c X_s$ for all $c \in R$ and $s \in S$) since $F_R(S)$ is an R-algebra.
    - Did Nori qualify this?? Did he say that we do not write the c_i's at the front any more?

- ***R*-algebra homomorphism**: A function $h : A \to B$, where A, B are R-algebras, such that...
  (i) h is a ring homomorphism;
  (ii) $h(c) = c$ for all $c \in R$.

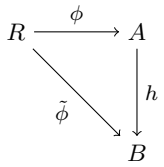

Figure 8.2: Visualizing R-algebra homomorphisms.

  - For clarity: If we momentarily drop our convention of suppressing ϕ, (ii) means $h(\phi(c)) = \tilde{\phi}(c)$ for all $c \in R$.
  - Alternate form of (ii): h is an R-module homomorphism.
    - This expresses the idea that the action of elements $c \in R$ on A is preserved under h, i.e., if $c \cdot a = ca$, then $ch(a) = c \cdot h(a) = h(c) \cdot h(a) = h(c \cdot a) = h(ca)$.

- Universal property of $F_R(S)$: Consider $i : S \to F_R(S)$ defined by $i(s) = X_s$. It is a map of sets since S has no additional structure. Given an R-algebra A and function $j : S \to A$, there exists a unique R-algebra homomorphism $h : F_R(S) \to A$ such that the following diagram commutes, i.e., $h(i(s)) = j(s)$ for all $s \in S$.

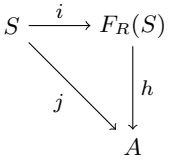

Figure 8.3: Universal property of $F_R(S)$.

- The principle of this universal property is the same as that of the universal property of polynomial rings. Seeing this:
  - Since $i(s) = X_s$, the statement $h(i(s)) = j(s)$ becomes $h(X_s) = j(s)$ for all $s \in S$.
  - This combined with the fact that h is an R-algebra homomorphism forces both existence and uniqueness for a reason symmetric to the proof of the universal property of polynomial rings in Lecture 1.2.
- We now develop a related object that appears in Chapter 10 called a **tensor algebra**.
  - A tensor algebra is very similar to a noncommutative polynomial ring.
- **Tensor algebra** (of M): A pair (A, α), where A an R-algebra and $\alpha : M \to A$ is an R-module homomorphism. *Denoted by* $\boldsymbol{\mathcal{T}(M)}$.
- Universal property of the tensor algebra $\mathcal{T}(M)$: $\mathcal{T}(M)$ is an R-algebra, $u : M \to \mathcal{T}(M)$ is an R-module homomorphism such that for all pairs $(A, \alpha : M \to A)$, there exists a unique R-algebra homomorphism $f : \mathcal{T}(M) \to A$ such that the following diagram commutes, i.e., $f \circ u = \alpha$.

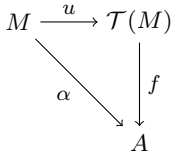

Figure 8.4: Universal property of $\mathcal{T}(M)$.

- Example: We now work out one specific case.
- Let's construct $\mathcal{T}(M)$ when M is a free R-module with S as the basis.
  - We have
$$M = \left\{ \sum_{s \in S} c_s e_s : c_s \in R,\ S \text{ is finite} \right\}$$
  - There's only finitely many nonzero s??
  - If S is finite, then $M = R^S$??
  - Let $\alpha : M \to A$ with M as above.
  - To specify α, you need only specify its action on a basis of M; thus, there is a bijection between the collection of all α and the set S (??) given by j??
  - This induces a ring homomorphism $h : F_R(S) \to A$ given by $h(X_s) = a_s$.
  - Here, $\mathcal{T}(M) = F_R(S)$.
  - How do you know it doesn't depend on the basis chosen? By the universal property (is this what he said??).
  - Any module is the quotient of a free module.
- There will be more questions on the final like questions 1-2 on the midterm!!!
- Certain zeroes exist in $F_R(S)$.
- We now start on Section 10.4 and exterior algebras.
- $F_R(S)/\langle X_s X_t - X_t X_s : s, t \in S \rangle$ is the two-sided ideal generated by the given elements. It is the usual/commutative polynomial ring in the X_s ($s \in S$)??

- We now move on to the Grassmann algebra.
- In calculus, we get things like $v \wedge v = 0$ and $v_1 \wedge v_2 = -v_2 \wedge v_1$.
- M will always be a free R-module on the set S (i.e., with basis S) for us.
- We now define the **exterior algebra** of M.
- **Exterior algebra** (of M): A pair (A, α) where A is an R-algebra and $\alpha : M \to A$ is an R-module homomorphism such that for all $m \in M$, $\alpha(m)^2 = 0$. *Denoted by* $\boldsymbol{\Lambda(M)}$.
  - We can prove the existence and uniqueness of $\Lambda(M)$.
- Conditions (is this the universal property??).
  1. Condition (*) holds for the horizontal arrow, i.e., for $\Lambda(M)$, $u(m)^2 = 0$ for all $m \in M$.
  2. If (*) holds for (A, α), then there exists a unique h such that the diagram below commutes.

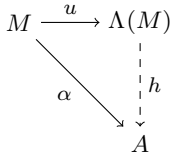

Figure 8.5: Existence and uniqueness of the exterior algebra.

- h is an R-algebra homomorphism such that $(h \circ u)(m) = \alpha(m)$ for all $m \in M$.
- Rather than write out the proof, just ask, "why not take $F_R(S) = \Lambda(M)$?"

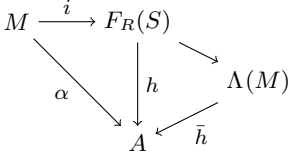

Figure 8.6: The free R-algebra on the set S and the exterior algebra.

  - Consider the above commutative diagram.
  - Then replace $F_R(S)$ by $F_R(S)/\left\langle i(m)^2 : m \in M \right\rangle = \Lambda(M)$ and extend the commutative diagram.
- Let $m = \sum_{s \in S} c_s e_s \mapsto \sum_{s \in S} c_s X_s$. We have

$$\left(\sum_s c_s X_s \right)^2 = \sum_{s \in S} c_s^2 X_s^2 + \sum_{\substack{\{s,t\} \\ s \neq t}} c_s c_t (X_s X_t + X_t X_2)$$

- For the moment, the R-module spanned modules X_s^2 for all $s \in S$, including $X_s X_t + X_t X_s$ and $(X_s + X_t)^2 = X_s^2 + X_t^2 + (X_s X_t + X_t X_s)$.
- Something on the difference between $v^2 = 0$ and $v_1 v_2 = -v_2 v_1$ in normal calculus and what we've done today...??

8.5 Office Hours (Callum)

- Lecture 7.3: Why did you use the direct product instead of the direct sum in your proof of the RCF theorem? Also, do we still need the N condition on the $m_{i,j}$, or did the way I phrase it suffice? How do you know that there's only finitely many distinct primes?
  - If you have a finitely generated PID R and an R-module M, then is any submodule of M finitely generated?
- Problem 7.3?
  - It is a straight-up ring problem; we shouldn't be doing anything fancy with modules.

8.6 Office Hours (Nori)

2/23:

- Lecture 6.1: Proposition proof?
- Lecture 6.1: $(2) \subsetneq \mathbb{Z}$ example?
- Lecture 6.1: The end of the theorem proof.
- Lecture 6.2: Does the first theorem you proved not appear in the book until Chapter 12?
- Lecture 6.2: What is A in the proof?
- Resources for the proofs in Week 6?
- Lecture 7.1: Quotient stuff.
- Is my proof for Q7.1(ii) sufficiently not hand-wavey?
- Question 7.7?
  - Note: The four given submodules satisfy the $T(N) \subset N$ condition even if M does not have the particular form given! It just so happens that in this case, these four are the only allowable ones.
- Solving Question 7.7?
  - WTS: $N = pM$ or $\ker(p_M)$.
  - We know that

$$pM = pR/(p^2) \oplus 0 \qquad \ker(p_M) = pR/(p^2) \oplus R/(p)$$

  - $\ker(p_M)$ is a 2D vector space over $R/(p)$.
  - WTS: $N \cap \ker(p_M) \neq 0$ iff $N \neq 0$.
    - We know that $pN \subset N$ by the definition of N as a submodule.
    - Let $n \in N$ be nonzero. Suppose $n \notin \ker(p_M)$. Then $pn \in \ker(p_M)$. We know that $pn \in N$ as well. Thus, $pn \in N \cap \ker(p_M)$.
  - $N \cap \ker(p_M) \subset \ker(p_M)$. Thus, $N \cap \ker(p_M)$ is either a 1D or a 2D vector space over $R/(p)$. We WTS that if it's 2D, then it equals $\ker(p_M)$, and if it's 1D, then it equals pM.
  - 2D case.
    - We know that $N \cap \ker(p_M) \subset \ker(p_M)$.
    - 2D implies that $N \not\subseteq \ker(p_M)$.
    - Thus, either $N = \ker(p_M)$ or $N \supsetneq \ker(p_M)$.
    - In the first case, we are done.
    - In the second case, we can show that this implies that $N = M$.

- 1D case.
  - We know that $pM \cap \ker(p_M) = p_M$.
  - Assume $N \neq pM$.
  - Then $N \cap \ker(p_M) = \langle (pa, 1) \rangle$.
  - But T exists, where $T : M \to M$ sends $T(1,0) = (1,0)$ and $T(0,1) = (p,1)$.
  - Therefore we must have $N \cap \ker(p_M) = pM$.
- Suppose that $N \supsetneq pM$.
  - $N/pM \subset M/pM$. Then use $T(1,0) = (1,1)$ and $T(0,1) = (0,1)$.

8.7 Exterior Algebra and Determinants

2/24:

- Last time, we were defining the exterior algebra.
- Recall:
  - We have shown that $\Lambda(M)$, where M is a free R-module with S as basis, equals $F_R(S)/I$.
  - $F_R(S)$ is a noncommutative polynomial ring in variables X_s, with $s \in S$ as variables.
  - I is the two-sided ideal generated by everything m^2 for all $m \in M$ (e.g., $(\sum_{s \in S} c_s X_s)^2$).
    - This is also the two-sided ideal generated by X_s^2 for all $s \in S$ and $X_s X_t + X_t X_s$ for all $t, s \in S$ with $t \neq s$.
    - Note that we don't need the $t \neq s$ condition; it just helps to not repeat things.
- In $F_R(S)/I$, we have $\overline{X_s^2} = 0$ and $X_s X_t = -X_t X_s$. Over real numbers, this is differential forms.
- To stop things from repeating, we take a linear ordering of S.
  - Assume $S = \{1, \ldots, n\}$ for simplicity of notation.
  - We will not have repeated elements in a product, and we can assume that everything comes in linear order.
  - Let $X_I = X_{i_1} \cdots X_{i_k}$ for $1 \leq i_1 < \cdots < i_k \leq n$. $I \in \mathcal{P}(\{1, \ldots, n\})$.
  - Thus, we see that the X_I, for all $I \in \mathcal{P}(\{1, \ldots, n\})$, generates $F_R(S)/I$ as an R-module.
  - We would like to prove this, but Nori will not for time's sake.
- We want to show that the X_I are, in fact, a basis.
- First approach: Suppose $M = Re_1 \oplus \cdots \oplus Re_n$.
  - Then let $\mathcal{A}$ be the free R-module with $e_I = e_{i_1} \cdots e_{i_k}$ as basis, where $I = \{i_1, \ldots, i_k\}$ is in ascending order.
  - Note: We could put the wedge in all of these products as in calculus, but we can equally well omit it.
  - If $I \cap J \neq \emptyset$, then $e_I e_J = 0$.
  - If $I \cap J = \emptyset$, then $e_I e_J = \operatorname{sgn}(\sigma) e_{I \cup J}$.
    - σ is the permutation that puts it into ascending order.
  - Extend multiplication in an R-linear way and check that $\mathcal{A}$ is actually a ring. This can be proven via

Figure 8.7: Proving that sets with related structure are isomorphic to $F_R(S)/I$.

  - Then $\Lambda(Re_1 \oplus \cdots \oplus Re_n)$ is a free R-module with the e_I as basis.

- Second approach: Induction.
  - Let $M = Re_1 \oplus Re_2 \oplus \cdots \oplus Re_n$.
  - We assume that we have already proven the case $N = Re_2 \oplus \cdots \oplus Re_n$.
  - Let $\Lambda(N) = A$ be an R-algebra.
  - We wish to construct $B = A \oplus eA$.
  - Let $\sigma : A \to A$ be defined by $\sigma(n) = -n$ for all $n \in N$. Then σ is a ring homomorphism and $\sigma^2(a) = a$.
  - It follows that $ea = \sigma(a)e$.
  - We have that
    $$(a + be)(c + de) = ac + (ad + b\sigma(c))e$$
    and this is the ring structure.
  - Problem: Show that B is a ring when $\sigma : A \to A$ is a ring homomorphism satisfying $\sigma^2 = \mathrm{id}$.
- We have that $\Lambda(M) = \bigoplus_{k \geq 0} \Lambda^k(M)$.
  - Thus, $\mathrm{rank}(M) = n$ where $\Lambda^k(M) = 0$ for all $k > n$.
- Corollary of the universal property: Given $L : M \to N$ an R-module homomorphism, then there is a unique R-algebra homomorphism called $\Lambda(L)$ such that the following diagram commutes. *picture*
- What does $\Lambda^k(M)$ mean?
  - It is an R-module spanned by e_I, where the cardinality of I is k. This is a bad definition, though.
  - Better: R-submodule of $\Lambda(R)$ generated by $v_1, \ldots, v_k$ where all $v_i \in M$.
- Let $\Lambda(M) = \bigoplus_{k \geq 0} \Lambda^k(M)$. Given $L : M \to N$, we get R-module homomorphisms called $\Lambda^k(L) : \Lambda^k(M) \to \Lambda^k(N)$ and $\Lambda(L)(\alpha_0 + \alpha_1 + \cdots) = \alpha_0 + L(\alpha_1) + \Lambda^2(L)(\alpha_2) + \cdots$.
- Now assume that $\mathrm{rank}(M) = \mathrm{rank}(N) = n$ and $L : M \to N$ is an R-module homomorphism. Then $\Lambda^n(L) : \Lambda^n(M) \to \Lambda^n(N)$. This is also called the determinant of L.
- Now assume that $M = N$. We have a map from a space to itself?? Suppose ω is a basis element of $\Lambda^n(M)$. Then $\Lambda^n(L)\omega = \alpha\omega$. There exists such an $\alpha \in R$.
  - Then $\Lambda^n(L)(a\omega) = a\alpha\omega = \alpha(a\omega)$ for all $a \in R$ and $\Lambda^n(L)\eta = \alpha\eta$ for all $\eta \in \Lambda^n(M)$.
  - Let $\det(L) \in R$. Then $\Lambda^n(L)\eta = (\det(L))\eta$ for all $\eta \in \Lambda^n(M)$.
- On the formula for the inverse in terms of adjoint matrices.
  - We have $\Lambda^{n-1}(L) : \Lambda^{n-1}(M) \to \Lambda^{n-1}(M)$.
- Characteristic polynomial: M is an R-module.
  - We have $R[\lambda]$ as the polynomial ring in one variable.
  - $M[\lambda] = M \oplus M \oplus \cdots$ implies that $(m_0, m_1, \ldots)$ is $m_0 + m_1\lambda + m_2\lambda^2 + \cdots$ is an $R[\lambda]$-module.
  - Let $L : M \to N$ be an R-module. Then $L_e : M[\lambda] \to N[\lambda]$ is an $R[\lambda]$-module homomorphism.
  - Take $M = N$ to be a free R-module of rank n.
  - Then $\sum_i m_i\lambda^n$ maps to $\sum_i L(m_i)\lambda^i$.
  - It follows that $M[\lambda]$ and $R[\lambda]$...
  - We have $\lambda : M[\lambda] \to M[\lambda]$ and $\lambda(m\lambda^i) = m\lambda^{i+1}$. Take $\det(\lambda - L_e) = \det_L(\lambda) \in R[\lambda]$ a monic polynomial of degree n.
  - Then $\lambda^n - \mathrm{tr}(L)\lambda^{n-1} + \cdots + (-1)^n \deg(L)$.

- We have $R[\lambda]$ and $\mathrm{End}_R(M)$. Send $\lambda \mapsto L$. This is evaluation at L. We also send $c \mapsto c$ for all $c \in R$.
- Cayley-Hamilton theorem: $L : M \to M$ is an R-module homomorphism and L is free of rank n implies that $\det_L(L) = 0$.
- We'll get an eighth week summary next Monday.
- Next week: A bit of number theory and a bit of geometry. It's up to us whether we come or not. Nori just wants to enjoy himself. None of the content will be on the exam.

8.8 Chapter 10: Introduction to Module Theory

From Dummit and Foote (2004).

Section 10.4: Tensor Products of Modules

2/26:

- Goal: Study the **tensor product** of two modules over a (not necessarily commutative) ring.
- What is the tensor product?
  - The construction of a module $M \otimes N$ in which we can take the "product" mn of elements $m \in M$ and $n \in N$.
- The general construction is quite complex, so we start with a special case: Extending scalars/changing base.
- **Extension** (of a ring): A ring S related to the original ring R via a ring homomorphism $f : R \to S$ and with the special property that any module on which R acts is acted upon by $f(R)$.
- **Restriction of scalars**: The R-module N constructed from the S-module N by defining the ring action from $f(R)$ onto N, where $f : R \to S$.
- Thus, it is possible in general to restrict an S-module to an R-module.
- However, it is *impossible* in general to do the opposite, that is, to extend an R-module to an S-module.
- Examples.
  - $\mathbb{Z}$ is a $\mathbb{Z}$-module, but not a $\mathbb{Q}$-module.
    - Suppose (contradiction): $\mathbb{Z}$ is a $\mathbb{Q}$-module. Consider the element $z = 1/2 \cdot 1 \in \mathbb{Z}$. Then since
    $$1 = 1 \cdot 1 = \left(\frac{1}{2} + \frac{1}{2}\right) \cdot 1 = \frac{1}{2} \cdot 1 + \frac{1}{2} \cdot 1 = z + z = 2z$$
    there is a $z \in \mathbb{Z}$ such that $2z = 1$. But by definition, no such element exists, a contradiction.
  - However, $\mathbb{Z} \hookrightarrow \mathbb{Q}$.
  - Dummit and Foote (2004) similarly proves that the $\mathbb{Z}$-module $\mathbb{Z}/2\mathbb{Z}$ cannot be embedded into any $\mathbb{Q}$-module.
- **Embedding**: A natural injection.
  - For example, $\mathbb{Z} \hookrightarrow \mathbb{Q}$ is an embedding.
- We now construct (for a general R-module N) the S-module that is the "best possible" target in which to try to embed N.
  - Said module determines *all* possible R-module homomorphisms of N into S-modules.
  - In particular, it determines when N is contained in an S-module (see Corollary 10.9).

  - Example: As per the above, this construction will give us $\mathbb{Q}$ when $R = \mathbb{Z}$ and $S = \mathbb{Q}$.

- **Tensor product** (of S and N over R): The quotient group formed from the free $\mathbb{Z}$-module $S \times N$ (a free abelian group) and its subgroup H generated by all elements of the form

$$(s_1 + s_2, n) - (s_1, n) - (s_2, n) \qquad (s, n_1 + n_2) - (s, n_1) - (s, n_2) \qquad (sr, n) - (s, rn)$$

  for $s, s_1, s_2 \in S$, $n, n_2, n_2 \in N$, and $r \in R$, where rn in the rightmost element above refers to the R-module structure already defined on N. *Denoted by* $\boldsymbol{S \otimes_R N}$, $\boldsymbol{S \otimes N}$.

  - "Free $\mathbb{Z}$-module $S \times N$:" We mean the collection of all finite commuting sums of elements of the form (s_i, n_i), where $s_i \in S$ and $n_i \in N$.
  - We denote the coset containing (s, n) in $S \otimes_R N$ by $s \otimes n$.

- The quotient definition forces the relations

$$(s_1 + s_2) \otimes n = s \otimes n + s_2 \otimes n \qquad s \otimes (n_1 + n_2) = s \otimes n_1 + s \otimes n_2 \qquad sr \otimes n = s \otimes rn$$

- **Tensor**: An element of $S \otimes_R N$.

  - "Tensors can be written (non-uniquely in general) as finite sums of 'simple tensors' of the form $s \otimes n$ with $s \in S$, $n \in N$" (Dummit & Foote, 2004, p. 360).

- The tensor product $S \otimes_R N$ is naturally a left S-module under the action defined by

$$s\left(\sum_{\text{finite}} s_i \otimes n_i\right) = \sum_{\text{finite}} (ss_i) \otimes n_i$$

  - Dummit and Foote (2004) proves that this expression is well-defined.
  - Dummit and Foote (2004) performs a rote axiom check.

- **Left S-module obtained by extension of scalars from the left R-module N**: The module $S \otimes_R N$.

- There is a natural map $\iota : N \to S \otimes_R N$ defined by $n \mapsto 1 \otimes n$.

  - ι is an R-module homomorphism: $1 \otimes rn = r \otimes n = r(1 \otimes n)$.
  - ι is *not* injective in general: Since we pass to a quotient group.

- Since ι need not be injective, we have constructed a natural relation between N and $S \otimes_R N$ but we have not asserted that $S \otimes_R N$ contain an isomorphic copy of N.

  - In the domain of homomorphisms, though, the fact that the relations we used to construct H and hence $S \otimes_R N$ were the *minimal* ones needed for $S \otimes_R N$ to be a module at all, it is save to assume that $S \otimes_R N$ is the "best possible" S-module to serve as the target for an R-module homomorphism from N.
  - More precisely, we know this is the best possible one because any other R-module homomorphism from N factors through this one. In other words, Φ below contains all information given by φ.

- What is described above is the **universal property** (for the tensor product), stated as follows.

  Theorem 10.8. Let R be a subring of S, let N be a left R-module, and let $\iota : N \to S \otimes_R N$ be the R-module homomorphism defined by $\iota(n) = 1 \otimes n$. Suppose that L is any left S-module (hence also an R-module) and that $\varphi : N \to L$ is an R-module homomorphism from N to L. Then there is a unique S-module homomorphism $\Phi : S \otimes_R N \to L$ such that φ factors through Φ, i.e., $\varphi = \Phi \circ \iota$ and the following diagram commutes. Conversely, if $\Phi : S \otimes_R N \to L$ is an S-module homomorphism, then $\varphi = \Phi \circ \iota$ is an R-module homomorphism from N to L.

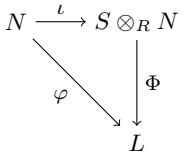

Figure 8.8: Universal property of the tensor product.

Proof. Given. □

- Conditions on when it is possible to map N injectively into some S-module, i.e., when some S-module contains an isomorphic copy of N.

  Corollary 10.9. Let $\iota : N \to S \otimes_R N$ be the R-module homomorphism in Theorem 10.8. Then $N/\ker \iota$ is the unique largest quotient of N that can be embedded in any S-module. In particular, N can be embedded as an R-submodule of some left S-module if and only if ι is injective (in which case N is isomorphic to the R-submodule $\iota(N)$ of the S-module $S \otimes_R N$).

  Proof. Given. □

- Examples.
  1. $R \otimes_R N \cong N$.
     - Takeaway: Extending scalars from R to R does not change the module.
     - Proof: Take $\varphi = \mathrm{id} : N \to N$ and $S = R$ in Theorem 10.8; then $\iota = \Phi^{-1}$ are isomorphisms.
     - Particular example: If A is any abelian group, then $\mathbb{Z} \otimes_{\mathbb{Z}} A \cong A$.
  2. More on the $\mathbb{Z}, \mathbb{Q}$ example from above.
  3. Extension of scalars for free modules.
  4. Extension of scalars for vector spaces.
  5. Induced modules for finite groups.
- Return to examples 2-5 later.
- We now explore the general tensor product construction, i.e, module 1 need not be a ring $S \supset R$.
- First: Two observations about the previous construction.
  1. The construction of $S \otimes_R N$ as an abelian group (i.e., before we put the module structure on it) only required quotienting out the elements given in the definition. This quotienting, in turn, only required S to be a *right* R-module and N to be a left R-module.
     - In a similar way, we shall construct an abelian group $M \otimes_R N$ for any *right* R-module M and any *left* R-module N.
  2. The S-module structure on $S \otimes_R N$ required only a *left* R-module structure on S and the "compatibility relation"
     $$s'(sr) = (s's)r$$
     for all $s, s' \in S$, $r \in R$ between the left S-module structure and the right R-module structure on S.
     - We shall also treat the module structure of $M \otimes_R N$ second.
- **Tensor product** (of M and N over R): The quotient group formed from the free $\mathbb{Z}$-module on the set $M \times N$ divided by the subgroup generated by all elements of the form
  $$(m_1 + m_2, n) - (m_1, n) - (m_2, n) \qquad (m, n_1 + n_2) - (m, n_1) - (m, n_2) \qquad (mr, n) - (m, rn)$$
  for $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$, and $r \in R$, where N is a left R-module and M is a right R-module. *Denoted by* $\boldsymbol{M \otimes_R N}$, $\boldsymbol{M \otimes N}$.

- **Tensor**: An element of $M \otimes_R N$.
- **Simple tensor**: A coset $m \otimes n$ of an element $(m, n) \in M \otimes_R N$.
- We have the same module-like relations as above, and statement about non-unique decomposition into simple tensors.
- Points of care.
  - $m \otimes n = m' \otimes n'$ is possible even if $m \neq m'$ or $n \neq n'$.
    - Thus, we must exercise care when referring to elements and defining maps based on m, n; such a map is only well-defined if it can be shown to be independent of the particular choice of $m \otimes n$ as a coset representative.
  - When M, N, R may not be clear from context.
- ***R*-balanced** (map): A map $\varphi : M \times N \to L$ satisfying

$$\varphi(m_1 + m_2, n) = \varphi(m_1, n) + \varphi(m_2, n) \quad \varphi(m, n_1, n_2) = \varphi(m, n_1) + \varphi(m, n_2) \quad \varphi(m, rn) = \varphi(mr, n)$$

  for all $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$, and $r \in R$, where M is a right R-module, N is a left R-module, and L is an additive abelian group. *Also known as* **middle linear with respect to *R***.
  - The prototypical R-balanced map is $\iota : M \times N \to M \otimes_R N$ defined by $\iota(m, n) = m \otimes n$. We can check all necessary axioms (Dummit and Foote (2004) do this).
- We now prove the more general universal property of the tensor product (with respect to balanced maps).

  Theorem 10.10. Suppose R is a ring, M is a right R-module, and N is a left R-module. Let $M \otimes_R N$ be the tensor product of M and N over R, and let $\iota : M \times N \to M \otimes_R N$ be the R-balanced map defined above.

  1. If $\Phi : M \otimes_R N \to L$ is any group homomorphism from $M \otimes_R N$ to an abelian group L, then the composite map $\varphi = \Phi \circ \iota$ is an R-balanced map from $M \times N \to L$.
  2. Conversely, suppose L is an abelian group and $\varphi : M \times N \to L$ is any R-balanced map. Then there is a unique group homomorphism $\Phi : M \otimes_R N \to L$ such that φ factors through ι, i.e., $\varphi = \Phi \circ \iota$ as above.

  Equivalently, the correspondence $\varphi \leftrightarrow \Phi$ in the commutative diagram

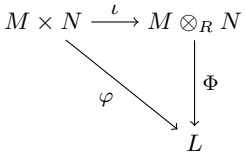

  Figure 8.9: Universal property of the general tensor product.

  establishes a bijection between the R-balanced maps $\varphi : M \times N \to L$ and the group homomorphisms $\Phi : M \otimes_R N \to L$.

  Proof. Given. □
- Characterizing the tensor product as an abelian group.

  Corollary 10.11. Suppose D is an abelian group and $\iota' : M \times N \to D$ is an R-balanced map such that...

(i) The image of ι' generates D as an abelian group;

(ii) Every R-balanced map defined on $M \times N$ factors through ι' as in Theorem 10.10.

Then there is an isomorphism $f : M \otimes_R N \to D$ of abelian groups with $\iota' = f \circ \iota$.

Proof. Given. □

- We now give $M \otimes_R N$ a module structure.
- **(S, R)-bimodule**: An abelian group M such that M is a left S-module, a right R-module, and $s(mr) = (sm)r$ for all $s \in S$, $r \in R$, and $m \in M$, where R, S are rings.
- Examples of (S, R)-bimodules. Return to later.
- **Standard** (R-module structure on M): The (R, R)-bimodule structure on M defined by letting the left and right R-actions coincide, i.e., $mr = rm$ for all $m \in M$ and $r \in R$, where M is a left (or right) R module over the commutative ring R.
- The tensor product $M \otimes_R N$ is naturally a left S-module under the action defined by

$$s\left(\sum_{\text{finite}} m_i \otimes n_i\right) = \sum_{\text{finite}} (sm_i) \otimes n_i$$

provided that N is a left R-module and M is an (S, R)-bimodule.

  - Proving well-definedness can be done with either analogous calculations to the above, or Theorem 10.10 (return to later).

- An important special case of the above general construction: R is commutative and $S = R$.
  - This is often the only case considered in works on tensor products!
- ***R*-bilinear** (map): A map $\varphi : M \times N \to L$ that is R-linear in each factor, that is

$$\varphi(r_1 m_1 + r_2 m_2, n) = r_1\varphi(m_1, n) + r_2\varphi(m_2, n) \qquad \varphi(m, r_1 n_1 + r_2 n_2) = r_1\varphi(m, n_1) + r_2\varphi(m, n_2)$$

for all $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$, and $r \in R$, where R is a commutative ring and M, N, L are R-modules. *Also known as* **2-multilinear**.

  - The prototypical R-bilinear map is $\iota : M \times N \to M \otimes_R N$, where $M \otimes_R N$ is an R-module and R is a commutative ring.

- Characterizing R-bilinear maps.

Corollary 10.12. Suppose R is a commutative ring. Let M, N be two left R-modules and let $M \otimes_R N$ be the tensor product of M and N over R, where M is given the standard R-module structure. Then $M \otimes_R N$ is a left R-module with

$$r(m \otimes n) = (rm) \otimes n = (mr) \otimes n = m \otimes (rn)$$

and the map $\iota : M \times N \to M \otimes_R N$ with $\iota(m, n) = m \otimes n$ is an R-bilinear map. If L is any left R-module, then there is a bijection between the R-bilinear maps $\varphi : M \times N \to L$ and the R-module homomorphisms $\Phi : M \otimes_R N \to L$ where the correspondence between φ and Φ is given by the following commutative diagram in Figure 8.9.

Proof. Given. □

- Examples of tensor products (return to later).

- For the rest of the section, we establish some basic properties of the tensor product.
- Applying Theorem 10.10 to establish the existence of homomorphisms.

  Theorem 10.13 (The "Tensor Product" of Two Homomorphisms)**.** Let M, M' be right R-modules, let N, N' be left R-modules, and suppose $\varphi : M \to M'$ and $\psi : N \to N'$ are R-module homomorphisms.

  1. There is a unique group homomorphism $\varphi \otimes \psi : M \otimes_R N \to M' \otimes_R N'$ such that
  $$(\varphi \otimes \psi)(m \otimes n) = \varphi(m) \otimes \psi(n)$$
  for all $m \in M$, $n \in N$.
  2. If M, M' are also (S, R)-bimodules for some ring S and φ is also an S-module homomorphism, then $\varphi \otimes \psi$ is a homomorphism of left S-modules. In particular, if R is commutative, then $\varphi \otimes \psi$ is always an R-module homomorphism for the standard R-module structures.
  3. If $\lambda : M' \to M''$ and $\mu : N' \to N''$ are R-module homomorphisms, then
  $$(\lambda \otimes \mu) \circ (\varphi \otimes \psi) = (\lambda \circ \varphi) \otimes (\mu \circ \psi)$$

  Proof. Given. □

- Defining n-fold tensor products.

  Theorem 10.14 (Associativity of the Tensor Product)**.** Suppose M is a right R-module, N is an (R, T)-bimodule, and L is a left T-module. Then there is a unique isomorphism
  $$(M \otimes_R N) \otimes_T L \cong M \otimes_R (N \otimes_T L)$$
  of abelian groups such that $(m \otimes n) \otimes l \mapsto m \otimes (n \otimes l)$. If M is an (S, R)-bimodule, then this is an isomorphism of S-modules.

  Proof. Given. □

  Corollary 10.15. Suppose R is commutative and M, N, L are R-modules. Then
  $$(M \otimes N) \otimes L \cong M \otimes (N \otimes L)$$
  as R-modules for the standard R-module structures on M, N, L.

- **Multilinear** (map): A map $\varphi : M_1 \times \cdots \times M_n \to L$ that is an R-module homomorphism in each component when the other component entries are kept constant, that is, for each $i \in \{1, \ldots, n\}$,
$$\phi(m_1, \ldots, rm_i + r'm_i', \ldots, m_n) = r\varphi(m_1, \ldots, m_i, \ldots, m_n) + r'\varphi(m_1, \ldots, m_i', \ldots, m_n)$$
for all $m_i, m_i' \in M_i$ and $r, r' \in R$, where R is a commutative ring and $M_1, \ldots, M_n, L$ are R-modules under the respective standard R-module structures. *Also known as* ***n*-multilinear over *R***. *Also known as* ***n*-multilinear form on *V***.
- **Trilinear** (map): A 3-multilinear map.
- The universal property of the tensor product of n modules.

  Corollary 10.16. Let R be a commutative ring and let $M_1, \ldots, M_n, L$ be R-modules. Let $M_1 \otimes \cdots \otimes M_n$ denote any bracketing of the tensor product of these modules, and let $\iota : M_1 \times \cdots \times M_n \to M_1 \otimes \cdots \otimes M_n$ be the map defined by
  $$(m_1, \ldots, m_n) \mapsto m_1 \otimes \cdots \otimes m_n$$
  Then...

1. For every R-module homomorphism $\Phi : M_1 \otimes \cdots \otimes M_n \to L$, the map $\varphi = \Phi \circ \iota$ is n-multilinear from $M_1 \times \cdots \times M_n \to L$;
2. If $\varphi : M_1 \times \cdots \times M_n \to L$ is an n-multilinear map, then there is a unique R-module homomorphism $\Phi : M_1 \otimes \cdots \otimes M_n \to L$ such that $\varphi = \Phi \circ \iota$.

Hence there is a bijection between the n-multilinear maps $\varphi : M_1 \times \cdots \times M_n \to L$ and the R-module homomorphisms $\Phi : M_1 \otimes \cdots \otimes M_n \to L$ with respect to which the following diagram commutes.

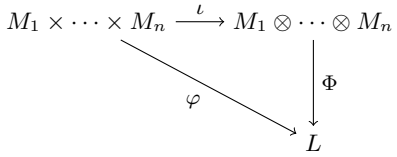

Figure 8.10: Universal property of the n-fold tensor product.

Proof. We may prove this from first principles analogously to the above. Alternatively, we can invoke Theorem 10.14 and Corollary 10.15 to obtain the n-fold tensor product unambiguously and then applying Theorem 10.10 and Corollary 10.12 repeatedly. □

- A sufficient condition for $M_1 \subset M$ an R-submodule to imply that $M_1 \otimes_R N \subset M \otimes_R N$ as an R-submodule.

  Theorem 10.17 (Tensor Products of Direct Sums)**.** Let M, M' be right R-modules and let N, N' be left R-modules. Then there are unique group isomorphisms

  $$(M \oplus M') \otimes_R N \cong (M \otimes_R N) \oplus (M' \otimes_R N) \qquad M \otimes_R (N \oplus N') \cong (M \otimes_R N) \oplus (M \otimes_R N')$$

  such that $(m, m') \otimes n \mapsto (m \otimes n, m' \otimes n)$ and $m \otimes (n, n') \mapsto (m \otimes n, m \otimes n')$, respectively. If M, M' are also (S, R)-bimodules, then these are isomorphisms of left S-modules. In particular, if R is commutative, these are isomorphisms of R-modules.

  Proof. Given. □

- Tensor products commute with direct sums: The generalization of the result; in particular, the statement

  $$M \otimes \left(\bigoplus_{i \in I} N_i \right) \cong \bigoplus_{i \in I} (M \otimes N_i)$$

- Applying the above back to the extension of scalars case.

  Corollary 10.18 (Extension of Scalars for Free Modules)**.** The module obtained from the free R-module $N \cong R^n$ by extension of scalars from R to S is the free S-module S^n, i.e.,

  $$S \otimes_R R^n \cong S^n$$

  as left S-modules.

  Proof. Given. □

- The tensor product of two free modules of arbitrary rank over a commutative ring is free. Finite case:

  Corollary 10.19. Let R be a commutative ring and let $M \cong R^s$ and $N \cong R^t$ be free R-modules with bases $m_1, \ldots, m_s$ and $n_1, \ldots, n_t$, respectively. Then $M \otimes_R N$ is a free R-module of rank st with basis $m_i \otimes n_j$ $(1 \leq i \leq s,\, 1 \leq j \leq t)$, i.e.,

  $$R^s \otimes_R R^t \cong R^{st}$$

Proof. Given. □

- Commutativity of the tensor product.

  Proposition 10.20. Suppose R is a commutative ring and M, N are left R-modules under the standard R-module structures. Then there is a unique R-module isomorphism

  $$M \otimes_R N \cong N \otimes_R M$$

  mapping $m \otimes n \mapsto n \otimes m$.

  Proof. Given. □

- Note that it is not true in general that $M = N$ implies $a \otimes b = b \otimes a$ for all $a, b \in M$.
  - Such **symmetric tensors** are the object of Section 11.6.
- The tensor product of R-algebras is again an R-algebra.

  Proposition 10.21. Let R be a commutative ring, and let A, B be R-algebras. Then the multiplication $(a \otimes b)(a' \otimes b') = aa' \otimes bb'$ is well-defined and makes $A \otimes_R B$ into an R-algebra.

  Proof. Given. □

- An example is given to tie a lot of things together.

8.9 Chapter 11: Vector Spaces

From Dummit and Foote (2004).

Section 11.4: Determinants

2/27:

- We will primarily apply the theory of determinants to vector spaces over a field, but it takes no extra effort to develop it over arbitrary commutative rings, so we will do that.
- In this section, let R be an arbitrary commutative ring and $V_1, \ldots, V_n, V, W$ be R-modules.
- **Alternating** (n-multilinear function): An n-multilinear function $\varphi : V_1 \times \cdots \times V_n \to W$ such that $\varphi(v_1, \ldots, v_n) = 0$ whenever $v_i = v_{i+1}$ for some $i \in \{1, \ldots, n-1\}$.
- **Symmetric** (n-multilinear function): An n-multilinear function $\varphi : V_1 \times \cdots \times V_n \to W$ such that interchanging v_i and v_j for any $i, j \in (v_1, \ldots, v_n)$ does not alter the value of φ on this n-tuple.
- Example: The dot product on $V = \mathbb{R}^m$ is a bilinear form (here, $R = \mathbb{R}$).
- Properties of alternating functions.

  Proposition 11.22. Let φ be an n-multilinear alternating function on V. Then...

  1. $\varphi(v_1, \ldots, v_{i-1}, v_{i+1}, v_i, v_{i+2}, \ldots, v_n) = -\varphi(v_1, \ldots, v_n)$ for any $i \in \{1, \ldots, n-1\}$, i.e., the value of φ on an n-tuple is negated if two adjacent components are interchanged.
  2. For each $\sigma \in S_n$, $\varphi(v_{\sigma(1)}, \ldots, v_{\sigma(n)}) = \operatorname{sgn}(\sigma)\varphi(v_1, \ldots, v_n)$, where $\operatorname{sgn}(\sigma)$ is the sign of the permutation σ.
  3. If $v_i = v_j$ for any pair of distinct $i, j \in \{1, \ldots, n\}$, then $\varphi(v_1, \ldots, v_n) = 0$.
  4. If v_i is replaced by $v_i + \alpha v_j$ in $(v_1, \ldots, v_n)$ for any $j \neq i$ and any $\alpha \in R$, the value of φ on this n-tuple is not changed.

Proof. Given. □

- Relating $\varphi(w)$ to $\varphi(v)$ when we have w in terms of v.

  Proposition 11.23. Assume φ is an n-multilinear alternating function on V and that for some $v_1, \ldots, v_n, w_1, \ldots, w_n \in V$ and some $\alpha_{ij} \in R$, we have

  $$\begin{aligned} w_1 &= \alpha_{11}v_1 + \cdots + \alpha_{n1}v_n \\ &\vdots \\ w_n &= \alpha_{1n}v_1 + \cdots + \alpha_{nn}v_n \end{aligned}$$

  Note that we have purposely written the indices of the α_{ij} in "column format" so that it is easier to relate this proposition to the determinant of column vectors introduced momentarily. Then

  $$\varphi(w_1, \ldots, w_n) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma)\alpha_{\sigma(1)1} \cdots \alpha_{\sigma(n)n}\varphi(v_1, \ldots, v_n)$$

  Proof. Given. □

- ***n* × *n* determinant function**: Any function from $M_{n\times n}(R) \to R$ that satisfies the following two axioms. *Denoted by* **det**. *Constraints*

  (i) det is an n-multilinear alternating form on R^n $(= V)$, where the n-tuples are the n columns of the matrices in $M_{n\times n}(R)$.

  (ii) $\det(I) = 1$, where I is the $n \times n$ identity matrix.

- We will sometimes denote $\det A$ by $\det(A_1, \ldots, A_n)$, where $A_1, \ldots, A_n$ are the columns of A.

- Uniqueness and computability of the determinant.

  Theorem 11.24. There is a unique $n \times n$ determinant function on R and it can be computed for any $n \times n$ matrix (α_{ij}) by the formula

  $$\det(\alpha_{ij}) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma)\alpha_{\sigma(1)1} \cdots \alpha_{\sigma(n)n}$$

  Proof. Given. □

- Determinant of the transpose.

  Corollary 11.25. The determinant is an n-multilinear function on the rows of $M_{n\times n}(R)$ and for any $n \times n$ matrix A, $\det A = \det(A^t)$, where A^t is the transpose of A.

  Proof. Given. □

- An unusual form of Cramer's Rule.

  Theorem 11.26 (Cramer's Rule)**.** If $A_1, \ldots, A_n$ are the columns of an $n \times n$ matrix A and $B = \beta_1 A_1 + \cdots + \beta_n A_n$ for some $\beta_1, \ldots, \beta_n \in R$, then

  $$\beta_i \det A = \det(A_1, \ldots, A_{i-1}, B, A_{i+1}, \ldots, A_n)$$

  Proof. This follows immediately from Proposition 11.22(4) and the multilinearity of the determinant. □

- Determinant of a singular matrix.

Corollary 11.27. If R is an integral domain, then $\det A = 0$ for $A \in M_n(R)$ iff the columns of A are R-linearly dependent as elements of the free R-module of rank n. Also, $\det A = 0$ iff the rows of A are R-linearly dependent.

Proof. Given. □

- Determinant of the product is the product of the determinants.

  Theorem 11.28. For matrices $A, B \in M_{n\times n}(R)$, $\det AB = (\det A)(\det B)$.

  Proof. Given. □

- **Minor** (of a matrix): The $n-1 \times n-1$ matrix obtained from an $n \times n$ matrix $A = (\alpha_{ij})$ by deleting its i^{th} row and j^{th} column. *Denoted by* $\boldsymbol{A_{ij}}$.
- **Cofactor** (of a matrix): An element of the form $(-1)^{i+j} \det(A_{ij}) \in R$.
- An alternate method of computing the determinant.

  Theorem 11.29 (The Cofactor Expansion Formula Along the i^{th} Row)**.** If $A = (\alpha_{ij})$ is an $n\times n$ matrix, then the determinant of A can be computed from the following formula for each fixed $i \in \{1, \ldots, n\}$.

$$\det A = (-1)^{i+1}\alpha_{i1} \det A_{i1} + \cdots + (-1)^{i+n}\alpha_{in} \det A_{in}$$

  Proof. Given. □

- Computing A^{-1} using cofactors.

  Theorem 11.30 (Cofactor Formula for the Inverse of a Matrix)**.** Let $A = (\alpha_{ij})$ be an $n \times n$ matrix and let B be the transpose of its matrix of cofactors, i.e., $B = (\beta_{ij})$, where $\beta_{ij} = (-1)^{i+j} \det A_{ji}$ $(1 \le i, j \le n)$. Then $AB = BA = (\det A)I$. Moreover, $\det A$ is a unit in R iff A is a unit in $M_{n\times n}(R)$; in this case, the matrix

$$\frac{1}{\det A} B$$

  is the inverse of A.

  Proof. Given. □

Section 11.5: Tensor Algebras, Symmetric and Exterior Algebras

- In this section, R denotes any commutative ring, and we assume that each R-module possesses the standard R-module structure.
- We will primarily be interested in the special case $R = F$, but the basic constructions hold in general.
- How is the tensor product a ring, and how is it different from a ring?
  - In the tensor product, we can form "products" $m_1 m_2 = m_1 \otimes m_2$ of two elements in M. However, this does not make M an M-module since $m_1 m_2 \notin M$.
  - Can we make it more like a ring, though? We can, using tensor algebras.
- $\boldsymbol{\mathcal{T}^k(M)}$: The k-fold tensor product of the R-module M, where $k \ge 1$. *Given by*

$$\mathcal{T}^k(M) = \underbrace{M \otimes_R \cdots \otimes_R M}_{k \text{ times}}$$

- $\boldsymbol{\mathcal{T}^0(M)}$: The ring R, where M is an R-module.

- ***k*-tensor**: An element of $\mathcal{T}^k(M)$.
- **Tensor algebra** (of a module): The set of all finite linear combinations of k-tensors over M a module for $k \geq 0$. *Denoted by* $\boldsymbol{\mathcal{T}(M)}$. *Given by*

$$\mathcal{T}(M) = \bigoplus_{k=0}^{\infty} \mathcal{T}^k(M) = R \oplus \mathcal{T}^1(M) \oplus \mathcal{T}^2(M) \oplus \cdots$$

  - This is a ring containing M that is "universal" with respect to rings containing M, meaning that...??
  - We identify $M \cong \mathcal{T}^1(M)$ so that M is an R-submodule of $\mathcal{T}(M)$.
- We now justify the name, "tensor *algebra*."

  Theorem 11.31. If M is any R-module over the commutative ring R, then...

  1. $\mathcal{T}(M)$ is an R-algebra containing M with multiplication defined by mapping

$$(m_1 \otimes \cdots \otimes m_i)(m_1' \otimes \cdots \otimes m_j') = m_1 \otimes \cdots \otimes m_i \otimes m_1' \otimes \cdots \otimes m_j'$$

     and extended to sums via the distributive laws. With respect to this multiplication,

$$\mathcal{T}^i(M)\mathcal{T}^j(M) \subset \mathcal{T}^{i+j}(M)$$

  2. (Universal Property) If A is any R-algebra and $\varphi : M \to A$ is an R-module homomorphism, then there is a unique R-algebra homomorphism $\Phi : \mathcal{T}(M) \to A$ such that $\Phi|_M = \varphi$.

  Proof. Given. □
- Basis for $\mathcal{T}^k(V)$ over F.

  Proposition 11.32. Let V be a finite dimensional vector space over the field F with basis $\mathcal{B} = \{v_1, \ldots, v_n\}$. Then the k-tensors

$$v_{i_1} \otimes \cdots \otimes v_{i_k}$$

  with $v_{i_j} \in \mathcal{B}$ are a vector space basis of $\mathcal{T}^k(V)$ over F (with the understanding that the basis vector is the element $1 \in F$ when $k = 0$). In particular, $\dim(\mathcal{T}^k(V)) = n^k$.

  Proof. Given. □
- Theorem 11.31 and Proposition 11.32: $\mathcal{T}(V)$ can be regarded as a **noncommutative polynomial algebra** over F in the (noncommuting) variables $v_1, \ldots, v_n$.
  - A linear combinations of the basis vectors in Proposition 11.32 is just like a multivariable polynomial in the variables $v_1, \ldots, v_n$, i.e., an element of $F[v_1, \ldots, v_n]$.

2/28:
  - Recall that an analogous result holds for finitely generated free modules over any commutative ring (see Corollary 10.19).
- Examples (return to later).
- **Graded** (ring): A ring S that is the direct sum of additive subgroups $S_0, S_1, \ldots$ such that $S_i S_j \subset S_{i+j}$ for all $i, j \geq 0$.
- **Homogeneous element** (of degree $\boldsymbol{k}$ of a graded ring): An element of S_k.
- **Homogeneous component** (of S of degree k): The subgroup S_k.

- **Graded ideal**: An ideal I of a graded ring S for which
$$I = \bigoplus_{k=0}^{\infty} (I \cap S_k)$$
  - Alternate condition: Whenever a sum $i_{k_1} + \cdots + i_{k_n}$ of homogeneous elements with distinct degrees $k_1, \ldots, k_n$ is in I, each of the individual summands is in I.
  - An ideal is a graded ideal iff it can be generated by homogeneous polynomials.
  - Not every ideal of a graded ring is a graded ideal.
- **Graded ring homomorphism**: A ring homomorphism $\varphi : S \to T$ that respects the grading structures on S and T, i.e., $\varphi(S_k) \subset T_k$ for all $k \in \mathbb{Z}_{\geq 0}$.
- Since $S_0 S_0 \subset S_0$ in a graded ring, S_0 is a subring of S and S is a S_0-module.
  - If $S_0 \subset Z(S)$, then S is an S_0-algebra.
- Examples.
  1. The second equation in Theorem 11.31(1) implies that the tensor algebra is a graded ring.
  2. $R[X_1, \ldots, X_n]$.
- Quotients of graded rings by graded ideals are graded.

  Proposition 11.33. Let S be a graded ring, let I be a graded ideal in S, and let $I_k = I \cap S_k$ for all $k \geq 0$. Then S/I is naturally a graded ring whose homogeneous component of degree k is isomorphic to S_k/I_k.

  Proof. Given. □
- Symmetric algebras.
  - Return to later.
- Exterior algebras.
- **Exterior algebra** (of a module): The R-algebra obtained from the R-module M by taking the quotient of the tensor algebra $\mathcal{T}(M)$ by the ideal $\mathcal{A}(M)$ generated by all elements of the form $m \otimes m$ for $m \in M$. *Denoted by* $\boldsymbol{\Lambda(M)}$. *Given by*
$$\Lambda(M) = \mathcal{T}(M)/\mathcal{A}(M)$$
  - The image of $m_1 \otimes \cdots \otimes m_k \in \mathcal{T}(M)$ in $\Lambda(M)$ is denoted by $m_1 \wedge \cdots \wedge m_k$.
- Note that $\mathcal{A}(M)$ is a graded ideal.
- Thus, by Proposition 11.33, $\Lambda(M)$ is graded.
- $\boldsymbol{k^{\text{th}}}$ **exterior power** (of a module): The R-module equal to the k^{th} homogeneous component of the graded ring $\Lambda(M)$. *Denoted by* $\boldsymbol{\Lambda^k(M)}$. *Given by*
$$\Lambda^k(M) = \mathcal{T}^k(M)/\mathcal{A}^k(M)$$
  - We again let $R = \Lambda^0(M)$ and $M = \Lambda^1(M)$; hence, M is an R-submodule of the R-algebra $\Lambda(M)$.
- **Wedge product**: The multiplication in the exterior algebra. *Also known as* **exterior product**. *Given by*
$$(m_1 \wedge \cdots \wedge m_i) \wedge (m'_1 \wedge \cdots \wedge m'_j) = m_1 \wedge \cdots \wedge m_i \wedge m'_1 \wedge \cdots \wedge m'_j$$
  - This multiplication is alternating (by the definition of the quotient) in the sense that $m_1 \wedge \cdots \wedge m_k = 0$ if $m_i = m_{i+1}$ for any $1 \leq i < k$.

– Multiplication is also anticommutative for all $m, m' \in M$:

$$\begin{aligned} 0 &= (m+m') \wedge (m+m') \\ &= (m \wedge m) + (m \wedge m') + (m' \wedge m) + (m' \wedge m') \\ &= 0 + (m \wedge m') + (m' \wedge m) + 0 \\ m \wedge m' &= -m' \wedge m \end{aligned}$$

■ The anticommutativity does not extend to arbitrary products, though, i.e., we need not have $ab = -ba$ for all $a, b \in \Lambda(M)$.

- Basic properties of the exterior algebra.

Theorem 11.36. Let M be an R-module over the commutative ring R and let $\Lambda(M)$ be its exterior algebra.

1. The k^{th} exterior power $\Lambda^k(M)$ of M is equal to $M \otimes \cdots \otimes M$ (k times) modulo the submodule generated by all elements of the form $m_1 \otimes \cdots \otimes m_k$ where $m_i = m_j$ for some $i \neq j$. In particular, $m_1 \wedge \cdots \wedge m_k = 0$ if $m_i = m_j$ for some $i \neq j$.
2. (Universal Property for Alternating Multilinear Maps) If $\varphi : M \times \cdots \times M \to N$ is an alternating k-multilinear map, then there is a unique R-module homomorphism $\Phi : \Lambda^k(M) \to N$ such that $\varphi = \Phi \circ \iota$, where $\iota : M \times \cdots \times M \to \Lambda^k(M)$ is the map defined by

$$(m_1, \ldots, m_k) \mapsto m_1 \wedge \cdots \wedge m_k$$

Proof. Given. □

- Examples.

1. If V is a one-dimensional vector space over F with basis $\{v\}$, then

$$\Lambda(V) = F \oplus V \oplus 0 \oplus 0 \oplus \cdots$$

– By definition, $\Lambda^k(V)$ consists of all finite sums of elements of the form

$$\alpha_1 v \wedge \cdots \wedge \alpha_k v = \alpha_1 \cdots \alpha_k (v \wedge \cdots \wedge v)$$

for $\alpha_1, \ldots, \alpha_k \in F$.

– Since $v \wedge v = 0$,

$$\Lambda^0(V) = F \qquad \Lambda^1(V) = V \qquad \Lambda^i(V) = 0 \ (i \geq 2)$$

implying the original result.

2. If V is a two-dimensional vector space over F with basis $\{v, v'\}$, then

$$\Lambda(V) = F \oplus V \oplus F(v \wedge v') \oplus 0 \oplus 0 \oplus \cdots$$

– As before, $\Lambda^0(V) = F$ and $\Lambda^1(V) = V$.

– For $\Lambda^2(V)$, an arbitrary element of is a sum of elements of the form

$$\begin{aligned} (av + bv') \wedge (cv + dv') &= ac(v \wedge v) + ad(v \wedge v') + bc(v' \wedge v) + bd(v' \wedge v') \\ &= (ad - bc) v \wedge v' \end{aligned}$$

– Proving the $v \wedge v' \neq 0$.

■ We know that $\Lambda^2(V) = \mathcal{T}^2(V)/\mathcal{A}^2(V)$.

■ By Proposition 11.16, $\mathcal{T}^2(V)$ is a 4-dimensional vector space with basis $\{v \otimes v, v \otimes v', v' \otimes v, v' \otimes v'\}$.

- Note that another valid basis of $\mathcal{T}^2(V)$ is $\{v \otimes v, v \otimes v' + v' \otimes v, v' \otimes v', v \otimes v'\}$ since we can easily regenerate the original from it.
- This alternate basis is of interest since $\mathcal{A}^2(V)$ consists of all of the 2-tensors in the ideal generated by the tensors

$$(av + bv') \otimes (av + bv') = a^2(v \otimes v) + ab(v \otimes v' + v' \otimes v) + b^2(v' \otimes v')$$

- It follows that $\mathcal{A}^2(V)$ is contained in the 3-dimensional subspace of $\mathcal{T}^2(V)$ having $\{v \otimes v, v \otimes v' + v' \otimes v, v' \otimes v'\}$ as basis.
- In particular, since $v \otimes v' \notin \mathcal{A}^2(V)$, we know that $v \wedge v' \neq 0$ in $\Lambda^2(V)$.
- In fact, it follows that $\Lambda^2(V) \cong F(v \wedge v')$.

– We have $\Lambda^i(V) = 0$ $(i \geq 3)$ since in such an i-fold wedge product, either v or v' must appear more than once, making the entire wedge product equal to 0 by definition.

– These last four results together imply the original one.

- Unlike the tensor and symmetric algebras, $\Lambda^k(V)$ is finite-dimensional for V finite dimensional.

Corollary 11.37. Let V be a finite dimensional vector space over the field F with basis $\mathcal{B} = \{v_1, \ldots, v_n\}$. Then the vectors $v_{i_1} \wedge \cdots \wedge v_{i_k}$ $(1 \leq i_1 \leq \cdots \leq i_k \leq n)$ form a basis of $\Lambda^k(V)$, and $\Lambda^k(V) = 0$ when $k > n$ (when $k = 0$, the basis vector is the element $1 \in F$). In particular,

$$\dim_F(\Lambda^k(V)) = \binom{n}{k}$$

Proof. Given. □

- The results in Corollary 11.37 are true for any *free* R-module of rank n.
- Example.

– Return to later.

- This concludes our direct treatment of exterior algebras.
- We now move on to homomorphisms of tensor algebras.

– There's some stuff on symmetric algebras in here that I should return to later.

- Every R-module homomorphism $\varphi : M \to N$ induces a map on the k^{th} tensor power defined by

$$\mathcal{T}^k(\varphi) : m_1 \otimes \cdots \otimes m_k \mapsto \varphi(m_1) \otimes \cdots \otimes \varphi(m_k)$$

- This map sends the generators of $\mathcal{A}(M)$ to themselves.

– Example: We send $m \otimes m$ to $\varphi(m) \otimes \varphi(m)$, another element of the form $n \otimes n$.

- Thus, φ also induces an R-module homomorphism on the quotient defined by

$$\Lambda^k(\varphi) : \Lambda^k(M) \to \Lambda^k(N)$$

– Since this map is also a ring homomorphism, it is a graded R-algebra homomorphism.

- The case where $M = V$ an n-dimensional vector space over F and $\varphi : V \to V$.

– Let $v_1, \ldots, v_n$ be a basis of V.

– Corollary 11.37: $\Lambda^n(\varphi)$ maps the 1-dimensional vector space $\Lambda^n(V)$ to itself. In particular,

$$\Lambda^n(\varphi)(v_1 \wedge \cdots \wedge v_n) = \varphi(v_1) \wedge \cdots \wedge \varphi(v_n) = D(\varphi)v_1 \wedge \cdots \wedge v_n$$

for some $D(\varphi) \in F$.

- Characterizing $D(\varphi)$.

  Proposition 11.38. If φ is an endomorphism on an n-dimensional vector space V, then $\Lambda^n(\varphi)(w) = \det(\varphi)w$ for all $w \in \Lambda^n(V)$.

  Proof. Let A be an arbitrary $n \times n$ matrix over F. Defining the associated endomorphism φ gives a map $D : M_{n\times n}(F) \to F$ defined by $D(A) = D(\varphi)$. Confirming that this map D satisfies the three axioms for a determinant function in Section 11.4, the uniqueness statement of Theorem 11.24 yields the desired result. □

- The map $\Lambda^k(\varphi)$ induced by φ injective need not remain injective.

8.10 Chapter 12: Modules over Principal Ideal Domains

From Dummit and Foote (2004).

Section 12.2: The Rational Canonical Form

2/21:

- As stated previously, we apply the results of Section 12.1 to $F[X]$-modules herein.
- Let V be a finite dimensional vector space over F of dimension N. Let (V, T) be an $F[X]$-module.
- Since V is finite dimensional, it is finitely generated as an F-module and hence also as an $F[X]$-module.
- If V were free, it would be isomorphic to a direct sum of copies of $F[X]$ (by Theorem 12.5(1)) and hence be infinite dimensional.
  - Thus, V is a torsion $F[X]$-module.
  - Theorem 12.5(3): V is isomorphic to the direct sum of cyclic, torsion $F[X]$-modules.
  - This decomposition will allow us to choose a basis for V with respect to which the matrix representation for the linear transformation T is in a specific simple form.
- **Rational canonical form** (of a matrix): The form obtained when we use the invariant factor decomposition of the relevant vector space.
- **Jordan canonical form** (of a matrix): The form obtained when we use the elementary divisor decomposition (and when F contains all the eigenvalues of T).
- Theorem 12.9 ensures that the RCF and JCF are unique, justifying the labeling of them as *canonical*.
- An application of canonical forms: Classifying distinct linear transformations.
  - Two matrices that represent the same linear transformation (hence are similar) have the same RCF and JCF.
  - This is another instance of the structure of the space being acted upon (e.g., the invariant factor decomposition of V) providing information on the algebraic objects (e.g., linear transformations) which are acting.
- **Representation Theory of Groups**: The special case of algebraic objects acting on spaces concerning groups acting on vector spaces.
- **Eigenvalues**, **eigenvectors**, **eigenspaces**, and the **determinant** are defined for linear transformations and analogously for matrices.
- Properties of eigenvalues.

  Proposition 12.12. TFAE.

1. λ is an eigenvalue of T.
2. $\lambda I - T$ is a singular linear transformation of V.
3. $\det(\lambda I - T) = 0$.

Proof. Given. □

- **Characteristic polynomial** (of a linear transformation): The polynomial defined as follows, where T is the linear transformation in question. *Denoted by* $\boldsymbol{c_T(X)}$. *Given by*

$$c_T(X) = \det(XI - T)$$

  - Defined similarly for matrices A.
  - A monic polynomial of degree $\dim V$.
  - The eigenvalues are the roots.

- **Minimal polynomial** (of of a linear transformation): The unique monic polynomial which generates the ideal $\mathrm{Ann}(V)$ in $F[X]$. *Denoted by* $\boldsymbol{m_T(X)}$.
  - Defined similarly for matrices A.
  - We know that such a polynomial exists by Theorem 12.5(3).
  - Exercise 12.2.5: The degree of the minimal polynomial is at most n^2.

- **Cayley-Hamilton Theorem**: The minimal polynomial for T is a divisor of the characteristic polynomial for T.
  - Thus, the degree of the minimal polynomial is at most n.

- We now build up to the **rational canonical form**.

- Introduction.
  - Theorem 12.5: There exists an isomorphism

$$V \cong F[X]/(a_1(X)) \oplus \cdots \oplus F[X]/(a_m(X)) \tag{12.1}$$

  - The invariant factors a_i are only determined up to units, but since $F[X]^\times = F - \{0\}$, we can make the a_i unique by requiring them to be monic.
  - Theorem 12.5(3) asserts that $(a_m(X)) = \mathrm{Ann}(V)$.

- The minimal polynomial and the invariant factors.

  Proposition 12.13. The minimal polynomial $m_T(X)$ is the largest invariant factor of V. All of the invariant factors of V divide $m_T(X)$.

- We now build up to calculating the minimal polynomial of T and the other invariant factors.

- Choosing a basis for each of the summands in Equation 12.1.
  - Recall that the action of T on V is equivalent to the action of X on each summand.
  - Recall also (from the Example following Proposition 11.1) that $1, \bar{X}, \bar{X}^2, \ldots, \bar{X}^{k-1}$ gives a basis of $F[X]/(a(X))$, where $a(X) = X^k + b_{k-1}X^{k-1} + \cdots + b_0$.

– With respect to this basis, the linear transformation $T = l_X$ acts via

$$\begin{aligned} 1 &\mapsto \bar{X} \\ \bar{X} &\mapsto \bar{X}^2 \\ \bar{X}^2 &\mapsto \bar{X}^3 \\ &\vdots \\ \bar{X}^{k-2} &\mapsto \bar{X}^{k-1} \\ \bar{X}^{k-1} &\mapsto \bar{X}^k = -b_0 - b_1\bar{X} - \cdots - b_{k-1}\bar{X}^{k-1} \end{aligned}$$

■ The last equality holds since $a(\bar{X}) = 0$ in $F[X]/(a(X))$.

– With respect to this basis, the matrix for multiplication by X is called the **companion matrix** of $a(X)$.

– Applying this procedure to each of the cyclic modules on the right side of Equation 12.1 under an appropriate basis yields the **direct sum** of the companion matrices for the invariant factors as the matrix of T.

– Note that this matrix is uniquely determined by the invariant factors of the $F[X]$-module V. These invariant factors, in turn, uniquely determine V up to isomorphism by Theorem 12.9.

- **First subdiagonal**: The set of entries in a matrix which lie directly below a diagonal entry. *Also known as* **subdiagonal**.
- **Companion matrix** (of a polynomial): The $k \times k$ matrix, pertaining to the polynomial $a(X) = X^k + b_{k-1}X^{k-1} + \cdots + b_0$, which consists of 1's down the first subdiagonal, $-b_0, \ldots, -b_{k-1}$ down the last column, and zeros elsewhere. *Denoted by* $\boldsymbol{\mathcal{C}_{a(X)}}$. *Given by*

$$\mathcal{C}_{a(X)} = \begin{pmatrix} 0 & 0 & \cdots & \cdots & \cdots & -b_0 \\ 1 & 0 & \cdots & \cdots & \cdots & -b_1 \\ 0 & 1 & \cdots & \cdots & \cdots & -b_2 \\ 0 & 0 & \ddots & & & \vdots \\ \vdots & \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & \cdots & 1 & -b_{k-1} \end{pmatrix}$$

- **Direct sum** (of matrices): The block diagonal matrix consisting of the component matrices.
  – See the RCF example below.
- **Rational canonical form** (of a matrix): A matrix that is the direct sum of companion matrices for monic polynomials $a_1(X), \ldots, a_M(X)$ of degree at least one with $a_1(X) \mid a_2(X) \mid \cdots \mid a_m(X)$. *Also known as* **RCF**. *Given by*

$$\begin{pmatrix} \mathcal{C}_{a_1(X)} & & & \\ & \mathcal{C}_{a_2(X)} & & \\ & & \ddots & \\ & & & \mathcal{C}_{a_m(X)} \end{pmatrix}$$

- **Invariant factors** (of the RCF): The polynomials a_i in the above definition.
- Definition of a **block diagonal** matrix.
- **Rational canonical form** (of a linear transformation): The matrix representing T which is in rational canonical form.
- Dummit and Foote (2004) proves that the rational canonical form is unique by means of running the generation process in reverse.

Theorem 12.14 (Rational Canonical Form for Linear Transformations)**.** Let V be a finite dimensional vector space over the field F, and let T be a linear transformation of V.

1. There is a basis for V with respect to which the matrix for T is in rational canonical form, i.e., is a block diagonal matrix whose diagonal blocks are the companion matrices for monic polynomials $a_1(X), \ldots, a_m(X)$ of degree at least one with $a_1(X) \mid a_2(X) \mid \cdots \mid a_m(X)$.
2. The rational canonical from for T is unique.

- Why the *rational* canonical form?
  - "Rational" refers to the fact that this canonical form is calculated entirely within the field F and exists for any linear transformation T.
  - This is not the case for the JCF, which only exists if the field F contains the eigenvalues for T.
- Similar matrices, modules, and the RCF.

Theorem 12.15. Let S and T be linear transformations of V. Then TFAE.

1. S and T are similar linear transformations.
2. The $F[X]$-modules obtained from V via S and via T are isomorphic $F[X]$-modules.
3. S and T have the same rational canonical form.

Proof. Given. □

- Observation: Any $n \times n$ matrix A with entries in F arises as the matrix for some linear transformation T of an n-dimensional vector space.
- This observation allows us to restate Theorems 12.14-12.15 in the language of matrices.

Theorem 12.16 (Rational Canonical Form for Matrices)**.** Let A be an $n \times n$ matrix over the field F.

1. The matrix A is similar to a matrix in rational canonical form, i.e., there is an invertible $n \times n$ matrix P over F such that $P^{-1}AP$ is a block diagonal matrix whose diagonal blocks are the companion matrices for monic polynomials $a_1(X), \ldots, a_m(X)$ of degree at least one with $a_1(X) \mid a_2(X) \mid \cdots \mid a_m(X)$.
2. The rational canonical from for A is unique.

Theorem 12.17. Let A, B be $n \times n$ matrices over the field F. Then A, B are similar iff A, B have the same RCF.

- **Invariant factors** (of a matrix): The invariant factors of the matrix's RCF.
- RCF and similarity questions for A do not depend on which field contains the entries of A.

Corollary 12.18. Let A, B be two $n \times n$ matrices over a field F, and suppose F is a subfield of the field K.

1. The rational canonical form of A is the same whether it is computed over K or over F. The minimal and characteristic polynomials and the invariant factors of A are the same whether A is considered as a matrix over F or as a matrix over K.
2. The matrices A, B are similar over K iff they are similar over F, i.e., there exists an invertible $n \times n$ matrix P with entries from K such that $B = P^{-1}AP$ iff there exists an (in general different) invertible $n \times n$ matrix Q with entries from F such that $B = Q^{-1}AQ$.

Proof. Given. □

- Takeaways from Corollary 12.18.
  - The RCF for A is an $n \times n$ matrix with entries in the smallest field containing the entries of A.
  - Further explanation of the word *rational*: The RCF is the same matrix even if we allow conjugation of A by nonsingular matrices whose entries come from larger fields.
- Characteristic polynomials and invariant factors.

Lemma 12.19. Let $a(X) \in F[X]$ be any monic polynomial.

1. The characteristic polynomial of the companion matrix of $a(X)$ is $a(X)$.
2. If M is the block diagonal matrix

$$M = \begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_k \end{pmatrix}$$

given by the direct sum of matrices $A_1, \ldots, A_k$, then the characteristic polynomial of M is the product of the characteristic polynomials of $A_1, \ldots, A_k$.

Proof. See the exercises. □

Proposition 12.20. Let A be an $n \times n$ matrix over the field F.

1. The characteristic polynomial of A is the product of all the invariant factors of A.
2. (The Cayley-Hamilton Theorem) The minimal polynomial of A divides the characteristic polynomial of A.
3. The characteristic polynomial of A divides some power of the minimal polynomial of A. In particular, these polynomials have the same roots, not counting multiplicities.

Proof. Given. □

- The relations in Proposition 12.20 are frequently useful in determining the invariant factors of A, particularly for $\deg(A)$ small.
- **Elementary row and column operations**: The following three operations, where A is an $n \times n$ matrix over the field F and $XI - A$ is an $n \times n$ matrix with entries in $F[X]$. *Given by*

(i) Interchanging two rows or columns.

(ii) Adding a multiple (in $F[X]$) of one row or column to another.

(iii) Multiplying any row or column by a unit in $F[X]$, i.e., by a nonzero element in F.

- **Smith Normal Form** (of a matrix): The following form of the $n \times n$ matrix $XI - A$ with entries from $F[X]$, where $a_1, \ldots, a_m$ are the invariant factors of A. *Given by*

$$\begin{pmatrix} 1 & & & & & & & \\ & \ddots & & & & & & \\ & & 1 & & & & & \\ & & & a_1(X) & & & & \\ & & & & a_2(X) & & & \\ & & & & & \ddots & & \\ & & & & & & a_m(X) & \end{pmatrix}$$

- Computing the invariant factors in general.

  Theorem 12.21. Let A be an $n \times n$ matrix over the field F. Using the three elementary row and column operations above, the $n \times n$ matrix $XI - A$ is with entries in $F[X]$ can be put into Smith Normal Form.

- Dummit and Foote (2004) provides algorithms for computing the invariant factor decomposition and the RCF. Return to later.

Exercises

5. Prove directly from the fact that the collection of all linear transformations of an n-dimensional vector space V over F to itself form a vector space over F of dimension n^2 that the minimal polynomial of a linear transformation T has degree at most n^2.