Tensor Products and the Minkowski Embedding
Math 129 Presentation
2sday February 22, 2022

Zach Halberstam and Eliot Hodges

1. Introduction

In this presentation, we will introduce tensor products of modules over a ring and their connections to algebraic number theory. Specifically, we will use tensor products to explain why there exists a "choice free" Minkowski embedding.

2. Basic Definitions

We'll begin by introducing tensor products of vector spaces, as these are a little more user-friendly. We present two definitions and use the second to introduce tensor products of modules over a ring. Throughout take K to be a field and R a ring.

Definition 2.1. Let V and W be K-vector spaces. If V and W have $\{v_1, \dots, v_n\}$ and $\{w_1, \dots, w_m\}$ as bases respectively, then define $V \otimes W$ to be the K-vector space with basis $\{v_i \otimes w_j \mid 1 \leq i \leq n, 1 \leq j \leq m\}$. For any $v \in V$ and $w \in W$ with $v = \sum a_i v_i$ and $w = \sum b_j w_j$, we define $v \otimes w$ in the natural way:

$$v \otimes w = \sum a_i b_j v_i \otimes w_j$$

Such an element is called a *pure tensor*; any element of $V \otimes W$ may be expressed as a sum of pure tensors. The minimal number of pure tensors needed to express an element of $V \otimes W$ as a sum of pure tensors is called the *rank* of the element.

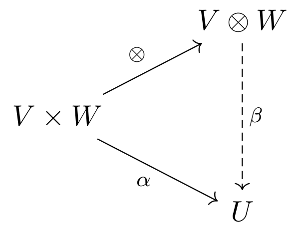
This definition is particularly nice in that it is concrete and easy to understand and use immediately. Moreover, we know immediately that $\dim(V \otimes W) = mn$. The drawbacks of this definition are: (1) it obscures the fact that the tensor product defines a *functor* from the product of the category of K-vector spaces with itself, to itself

$$\otimes : (Vect_K) \times (Vect_K) \to (Vect_K);$$

(2) it relies on choosing bases for V and W. While this in and of itself is not ideal (indeed, it would be ironic if, in explaining how to arrive at a choice-free version of the Minkowski embedding, we made lots of arbitrary choices on the way), this definition will completely break down if we try to generalize it to modules over a ring, since not every module has a basis.

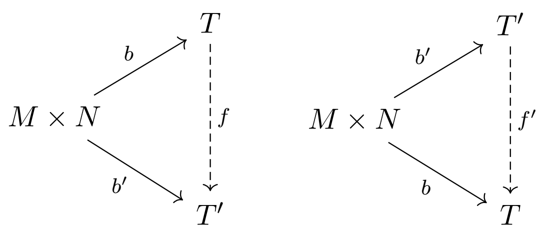
Thus, we present the following definition of tensor products:

Definition 2.2. Let V and W be K-vector spaces. The *tensor product* $V \otimes W$ is a K-vector space equipped with a bilinear map $\otimes : V \times W \to V \otimes W$ such that for any vector space U and bilinear map $\alpha : V \times W \to U$ there exists a unique linear map $\beta : V \otimes W$ such that $\alpha = \otimes \circ \beta$ and the following diagram commutes:

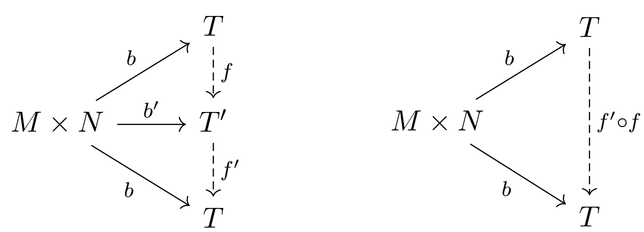


We see below that any two objects T and T' satisfying the above are the same up to isomorphism, implying the tensor product is unique.

Exercise 2.3. We prove the above claim. Specifically, if T and T' are two R-modules with respective bilinear maps $b : M \times N \to T$ and $b' : M \times N \to T'$ satisfying the desired mapping property, we claim that $T \cong T'$. By the universal mapping property, we have the following diagrams:



We combine these diagrams into one



and apply the universal mapping property to $f' \circ f$. Namely, there is a unique linear map from $T \to T$ making the diagram above (on the right) commute. The identity works, implying that $f' \circ f = \mathrm{id}_T$. A similar trick can be used to show that $f \circ f' = \mathrm{id}_{T'}$. This implies that $T \cong T'$, as desired. $\square$

Example 2.4. Finally, we illustrate how, given two R-modules M and N, one may construct their tensor product $M \otimes N$. By the above, we know that this construction gives us *the* tensor product of M and N. Begin by letting U be the free R-module generated by the symbols $a \otimes b$ for $a \in M$ and $b \in N$ (i.e. U is the module consisting of all finite R-linear combinations of the symbols $a \otimes b$, where a and b range over all elements of M and N respectively). This module is *huge*, but luckily we do not need to deal with it for very long. Let U_0 be the subspace generated by elements of the form

$$(ra) \otimes b - r(a \otimes b); \quad a \otimes (rb) - r(a \otimes b);$$

$$(a+a')\otimes b - a\otimes b - a'\otimes b; \quad a\otimes(b+b') - a\otimes b - a\otimes b'.$$

We claim that $M \otimes N$ is just the quotient module U/U_0. As an exercise, you should check that this is true (or at least justify it to yourself).

To do:

(1) Generalize all of this to modules over a ring.

(2) Given two R-modules M and N, show how to construct their tensor product. (See page 7 of this article by Keith Conrad or the second definition in the Auroux-Harris document. If using the Auroux-Harris source, will need to generalize to R-modules, which should be the same but things might be different? Not sure.)

(3) Give some interesting examples of tensors of R-modules specifically. E.g. tensors of free modules will behave just like vector spaces, but things get freaky when you add torsion: $\mathbb{Z}_2 \otimes \mathbb{Z}_3 = \{0\}$ as a $\mathbb{Z}$-module.

3. Some Commutative Algebra

In this section, we state but do not prove some important results from commutative algebra, while also introducing the requisite definitions.

Recall the definition of an algebra over a ring—an algebra over a ring is simply an R-module A that is also endowed with a ring structure, where scalars commute with everything. Thus, when $R = K$ is a field, an algebra is just a vector space that is also a ring. Examples include the algebra of $n \times n$ matrices with entries in R, $M_n(R)$; $R[X]$; RG a group ring; $\mathbb{H}$ the quaternions (as an $\mathbb{R}$-algebra, $\mathbb{H}$ is *not* an algebra over $\mathbb{C}$, since then scalars do not commute with everything). From here on out, we will only deal with algebras over a field K.

Definition 3.1. Let A be a K-algebra. An A-module V is *simple* if it is nonzero and it does not have any other A-submodules other than 0 and itself.

Definition 3.2. An A-module V is called *semisimple* if it is the direct sum of simple submodules. In other words, V is semisimple if there exist simple submodules $S_i \subset V$ (for $i \in I$, an index set) such that

$$V = \bigoplus_{i\in I} S_i.$$

Definition 3.3. A K-algebra A is *semisimple* if it is semisimple as an A-module.

Now, we state the Artin-Wedderburn theorem and one of its corollaries:

Theorem 3.4 (Artin-Wedderburn Theorem)**.** *Let K be a field and A a semisimple K-algebra. Then, there exist positive integers r and $n_1, \ldots, n_r$, as well as division algebras $D_1, \ldots, D_r$ over K such that*

$$A \cong M_{n_1}(D_1) \times \ldots \times M_{n_r}(D_r).$$

Conversely, each K-algebra of the form $M_{n_1}(D_1)\times\ldots\times M_{n_r}(D_r)$ is semisimple.

Corollary 3.5. *Let $f \in \mathbb{R}[X]$ be of the form $f = f_1\cdots f_r \cdot g_1\cdots g_s$ for pairwise coprime irreducible polynomials $f_i, g_j \in \mathbb{R}[X]$, where the f_i's are the degree 1 polynomials in the factorization of f and the g_j's have degree 2. Then, the Artin-Wedderburn decomposition of $\mathbb{R}[X]/(f)$ is*

$$\mathbb{R}[X]/(f) \cong \mathbb{R}\times\ldots\times\mathbb{R}\times\mathbb{C}\times\ldots\times\mathbb{C} = \mathbb{R}^r \times \mathbb{C}^s.$$

To do:

(1) This section should be finished; just need to check it over.

4. Connections to Fields

To do:

(1) This entire section.

5. The Minkowski Embedding

We begin by recalling *the Minkowski embedding* of a a number field into Euclidean space. Given a number field $K/\mathbb{Q}$ of degree n, recall that we may take a primitive element θ such that $K = \mathbb{Q}[\theta]$. Letting $f \in \mathbb{Q}[X]$ be the (monic) irreducible polynomial of θ, we recall that f factors over $\mathbb{R}$ as the product of r linear factors with real roots times a product of s quadratic factors each having genuinely complex (and therefore conjugate) numbers as roots. Thus, the roots of f (conjugates of θ) are as follows:

$$\theta_1, \theta_2, \ldots, \theta_r \in \mathbb{R}$$

and

$$\{\theta_{r+1}, \theta_{r+2} = \overline{\theta_{r+1}}\}, \{\theta_{r+3}, \theta_{r+4} = \overline{\theta_{r+3}}\}, \ldots, \{\theta_{r+2s-1}, \theta_{r+2s} = \overline{\theta_{r+2s-1}}\} \in \mathbb{C}.$$

The corresponding n homomorphisms into $\mathbb{C}$ give us r embeddings of K into $\mathbb{R}$ and s pairs of conjugate, nonreal embeddings into $\mathbb{C}$. Choosing one embedding for each of the s pairs of conjugate embeddings, we get an injective homomorphism called the *fundamental embedding* or *Minkowski embedding* of K into Euclidean space. Namely, if $\sigma_1, \ldots, \sigma_r$ are the r real embeddings, and if $\gamma_1, \ldots, \gamma_s$ are our selected s complex ones, ι is the map

$$\iota : K \hookrightarrow E := \mathbb{R}^r \times \mathbb{C}^s \cong \mathbb{R}^n$$

given by

$$\iota(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_r(\alpha), \gamma_1(\alpha), \ldots, \gamma_s(\alpha)).$$

While this definition of the Minkowski embedding is completely fine, it is possible to formulate it without making arbitrary choices, which is preferable. The vocabulary for doing so is that of tensor products.

With notation as above, consider $K = \mathbb{Q}[\theta] \cong \mathbb{Q}[X]/(f)$ and $\mathbb{R}$ as $\mathbb{Q}$-vector spaces. Let $f = f_1\cdots f_r g_1\cdots g_s$ be the factorization of f over $\mathbb{R}$ into r linear factors $f_1, \ldots, f_r$ and s quadratic factors $g_1, \ldots, g_s$. Take their tensor product over $\mathbb{Q}$: $\mathbb{Q}[\theta] \otimes_{\mathbb{Q}} \mathbb{R}$. (From here on out, we will blur the line use $\mathbb{Q}[\theta]$ and $\mathbb{Q}[X]/(f)$ interchangeably.) We claim that this is an algebra over $\mathbb{R}$ and that it is in fact isomorphic to $\mathbb{R}[X]/(f)$. Note that the multiplication structure on $\mathbb{Q}[\theta] \otimes_{\mathbb{Q}} \mathbb{R}$ is just componentwise multiplication (so $a \otimes b \cdot c \otimes d = ac \otimes bd$). Moreover, $\mathbb{Q}[\theta] \otimes_{\mathbb{Q}} \mathbb{R}$ is an $\mathbb{R}$-algebra via the $\mathbb{R}$-action given by $r \cdot (p(x) \otimes s) := p(x) \otimes rs$. We leave it as an exercise to check this detail. Basically, in taking the $\mathbb{Q}$-tensor product of $\mathbb{Q}[X]/(f)$ with $\mathbb{R}$, we are extending our ring of scalars to $\mathbb{R}$. Because $\mathbb{Q}[\theta]$ is a subfield of $\mathbb{C}$, it makes intuitive sense that this might be possible; the proposition below shows that it is:

Proposition 5.1. *$\mathbb{Q}[X]/(f) \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}[X]/(f)$ as $\mathbb{R}$-algebras.*

Proof. Let $\phi : \mathbb{Q}[X]/(f) \otimes_{\mathbb{Q}} \mathbb{R} \to \mathbb{R}[X]/(f)$ be the map defined by taking $p(x) \otimes r \mapsto rp(x)$ and extending linearly, where $p(x) \in \mathbb{Q}[X]/(f)$ and where $r \in \mathbb{R}$. Clearly, ϕ is well-defined because if $p - q \in (f)$, then $rp - rq \in (f)$ (where (f) is considered as an ideal of $\mathbb{R}[X]$ in this case). It is also easy to check that ϕ is indeed an $\mathbb{R}$-algebra homomorphism; for the sake of brevity we omit these details. It remains to show that this map is invertible. Let $\psi : \mathbb{R}[X]/(f) \to \mathbb{Q}[X]/(f) \otimes_{\mathbb{Q}} \mathbb{R}$ be given by

$$f(x) := a_n x^n + \ldots + a_1 x + a_0 \mapsto 1 \otimes a_0 + x \otimes a_1 + \ldots + x^n \otimes a_n.$$

Again, we leave it to the reader to check that this is an $\mathbb{R}$-algebra homomorphism. However, it is not immediate that this is a well-defined map, and we must check this. If $p - q = gf$, where $p, q, g \in \mathbb{R}[X]$, then we may "translate" this expression into one with tensors via the map given above. We are left with something that looks like

$$1 \otimes (a_0 - b_0) + \ldots + x^k \otimes (a_k - b_k) = (1 \otimes c_0 + \ldots + x^m \otimes c_m)(1 \otimes d_0 + \ldots + x^n \otimes d_n),$$

where the a's, b's, c's and d's correspond to p, q, g and f respectively (remark that we may not have as many b's as a's, since p and q do not necessarily have the same degree; the above is just a notational convenience). Note that in the above, the d's are all in $\mathbb{Q}$, so

$$1 \otimes d_0 + \ldots + x^n \otimes d_n = f(x) \otimes 1 = 0 \otimes 1 = 0,$$

implying the images of p and q under ψ are equal. We should also check that if a polynomial in $\mathbb{R}[X]/(f)$ is of the form $rp(x)$ for $p \in \mathbb{Q}[X]/(f)$ and $r \in \mathbb{R}$, then $\psi(rp(x)) = p(x) \otimes r$. This is not difficult to see:

$$\begin{aligned} rc_0 + rc_1 x + \ldots + rc_{n-1} x^{n-1} &\mapsto 1 \otimes rc_0 + \ldots + x^n \otimes rc_{n-1} \\ &= c_0 \otimes r + \ldots + c_{n-1} x^{n-1} \otimes r = p(x) \otimes r, \end{aligned}$$

where the second to last equality is a consequence of the fact that we may move rationals in between the coordinates of the tensors. Thus, we have that ψ is a well-defined homomorphism of $\mathbb{R}$-algebras, and, moreover, it is the inverse of ϕ:

$$\psi(\phi(p(x) \otimes r)) = \psi(rp(x)) = p(x) \otimes r,$$

and

$$\begin{aligned}\phi(\psi(c_0 + c_1 x + \ldots + c_{n-1}x^{n-1})) &= \phi(1 \otimes c_0 + x \otimes c_1 + \ldots + x^{n-1} \otimes c_{n-1}) \\ &= c_0 + c_1 x + \ldots + c_{n-1}x^{n-1}.\end{aligned}$$

The desired isomorphism follows. □

Now, armed with the commutative algebra we recalled in section 3, we note that the Artin-Wedderburn Theorem and its corollaries imply that

$$K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}[X]/(f) \cong \mathbb{R}^r \times \mathbb{C}^s.$$

This gives us a canonical embedding of $K = \mathbb{Q}[\theta]$ into $\mathbb{E} = \mathbb{R}^r \times \mathbb{C}^s$, and importantly, this version of the Minkowski embedding was derived without making arbitrary choices, which is exactly what we wanted.[1] To do:

(1) Choice-free Minkowski embedding

[1]Another way to see the second isomorphism in the above is to use the Chinese Remainder Theorem.