The Theoretical Minimum

Quantum Mechanics - Solutions

L03E01

M. Bivert

April 5, 2023

Exercise 1. *Prove the following: If a vector space in N-dimensional, an orthonormal basis of N vectors can be constructed from the eigenvectors of a Hermitian operator.*

We're here asked to prove a portion of an important theorem. I'm going to be somehow thorough in doing so, but to save space, I'll assume familiarity with linear algebra, up to diagonalization. Let's start with some background.

This exercise is about proving one part of what the authors call the *Fundamental theorem*, also often called in the literature the *(real) Spectral theorem*. So far, we've been working more or less explicitly in finite-dimensional spaces, but this result in particular has a notorious analogue in infinite-dimensional Hilbert spaces, called the *Spectral theorem*[1].

Now, I'm *not* going to prove the the infinite dimension version here. There's a good reason why quantum mechanics courses often start with spins: they don't require the generalized results, which demands heavy mathematical machinery (a copious amount of functional analysis, and in some formulation at least, the Lebesgue integral, hence portions of measure theory). You may want to refer to F. Schuller YouTube lectures on quantum mechanics[2] for a thorough development.

Finally, I'm going to use a mathematically inclined approach here (definitions/theorems/proofs), and as we won't need it, I won't be using the bra-ket notation.

To fix things, here's the theorem we're going to prove (I'll slightly restate it with minor adjustments later on):

Theorem 1. *Let $H : V \to V$ be a Hermitian operator on a finite-dimensional vector space V, equipped with an inner-product*[3]*.*

$$\boxed{\textit{Then, the eigenvectors of } H \textit{ form an orthonormal basis}}$$

Saying it otherwise, it means that a matrix representation M_H of H is diagonalizable, and that two eigenvectors associated with distinct eigenvalues are orthogonal.

For clarity, let's recall a few definitions.

Definition 1. *Let $L : V \to V$ be a linear operator on a vector space V over a field $\mathbb{F}$. We say that a non-zero $\boldsymbol{p} \in U$ is an eigenvector for L, with associated eigenvalue $\lambda \in \mathbb{F}$ whenever:*

$$L(\boldsymbol{p}) = \lambda \boldsymbol{p}$$

Remark 1. *As this can be a source of confusion later on, note that the definition of eigenvector/eigenvalue does not depend on the diagonalizability of L.*

[1] See `https://ncatlab.org/nlab/show/spectral+theorem` and `https://en.wikipedia.org/wiki/Spectral_theorem`

[2] `https://www.youtube.com/watch?v=GbqA9Xn_iMO&list=PLPH7f_7ZlzxQVx5jRjbfRGEzWY_upS5K6`; see also the lectures notes (.pdf) made by a student (Simon Rea): `https://drive.google.com/file/d/1nchF1fRGSY3R3rP1QmjUg7fe28tAS428/view`

[3] Remember, we need it to be able to talk about orthogonality.

Remark 2. *Note also that while eigenvectors must be non-zero, no such restrictions are imposed on the eigenvalues.*

Definition 2. *Two vectors $\boldsymbol{p}$ and $\boldsymbol{q}$ from a vector space V over a field $\mathbb{F}$ equipped with an inner product $\langle .,. \rangle$ are said to be orthogonal (with respect to the inner-product) whenever:*

$$\boxed{\langle \boldsymbol{p}, \boldsymbol{q} \rangle = 0_{\mathbb{F}}}$$

The following lemma will be of great use later on. Don't let yourself be discouraged by the length of the proof: it can literally be be shorten to just a few lines, but I'm going to be very precise, hence very explicit, as to make the otherwise simple underlying mathematical constructions as clear as I can.

Lemma 1. *A linear operator $L : V \to V$ on a $n \in \mathbb{N}$ dimensional vector space V over the complex numbers has at least one eigenvalue.*

Proof. Let's take a $\boldsymbol{v} \in V$. We assume V is not trivial, that is, V isn't reduced to its zero vector $\mathbf{0}_V$, and so we can always choose $\boldsymbol{v} \neq \mathbf{0}_V$[4].

Consider the following set of $n+1$ vectors:

$$\{\boldsymbol{v}, L(\boldsymbol{v}), L^2(\boldsymbol{v}), \ldots, L^n(\boldsymbol{v})\}$$

where:

$$L^0 := \mathrm{id}_V; \qquad L^i := \underbrace{L \circ L \circ \ldots \circ L}_{i \in \mathbb{N} \text{ times}}$$

It's a set of $n+1$ vectors, but the space is n dimensional, so its vectors are *not* all linearly independent. This means there's a set of $(\alpha_0, \alpha_1, \ldots, \alpha_n) \in \mathbb{C}^n$ which are not all zero, such that:

$$\sum_{i=0}^{n} \alpha_i L^i(\boldsymbol{v}) = \mathbf{0}_V \tag{1}$$

Here's the "subtle" part. You remember what a polynomial is right, something like:

$$x^2 - 2x + 1$$

You know it's customary to then consider this a function of a single variable x, which for instance, can range through the reals:

$$L : \begin{pmatrix} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & x^2 - 2x + 1 \end{pmatrix}$$

This allows you to graph the polynomial and so forth:

[4]Note that if V is trivial, because an eigenvalue is always associated to a non-zero vector, there are no eigenvalues/eigenvectors, and the result is trivial.

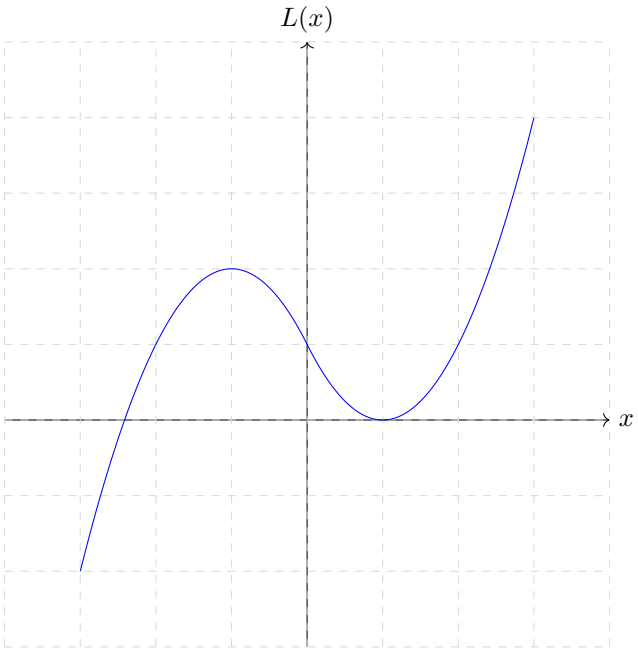

Figure 1: $L(x) = x^2 - 2x + 1$

But that's kindergarten polynomials. The more "correct" polynomials are *not* functions of a real variable. Rather, we say that $L(x)$ or L is a polynomial of a single variable/indeterminate[5] x, where x stands for an abstract symbol.

The reason is that, when you say that x is a real number (or a complex number, or whatever), you tacitly assume that you can for instance add, subtract or multiply various occurrences of x, but when mathematicians study polynomials, they want to do so without requiring additional (mathematical) structure on x.

Hence, x is just a placeholder, an abstract symbol.

The set of polynomials of a single variable X with coefficient in a field $\mathbb{F}$ is denoted $\mathbb{F}[X]$. For instance, $\mathbb{C}[f]$ is the set of all polynomials with complex coefficient of a single variable f, say, $P(f) = (3 + 2i)f^3 + 5f \in \mathbb{C}[f]$.

Now you'd tell me, wait a minute: if I have a $P(X) = X^2 - 2X + 1$, am I not then adding a polynomial $X^2 - 2X$ with an element from the field, 1?

Well, you'd be somehow right: the notation *is* ambiguous, in part inherited from the habits of kindergarten polynomials, in part because the context often makes things clear, and perhaps most importantly, because a truly unambiguous notation is unpractically verbose. Actually, $X^2 - 2X + 1$ is a shortcut notation for $X^2 - 2X^1 + 1X^0$. So no: all the $+$ here are between polynomials.

What does this mean that the $+$ are between polynomials? Well, most often when you encounter $\mathbb{F}[X]$, it's actually a shortcut for $(\mathbb{F}[X], +_{\mathbb{F}[X]}, \cdot_{\mathbb{F}[X]})$, which is a *ring*[6] *of polynomials of a single indeterminate over a field*[7] $\mathbb{F}$. This means that mathematicians have defined a way This means that $X^2 - 2X + 1$ is actually a shortcut for:

$$1._{\mathbb{F}[X]}X^2 +_{\mathbb{F}[X]} (-2)._{\mathbb{F}[X]}X^1 +_{\mathbb{F}[X]} (1)._{\mathbb{F}[X]}X^0$$

Awful, right? Hence why we often use ambiguous notations and reasonable syntactical shortcuts.

[5] `https://en.wikipedia.org/wiki/Indeterminate_(variable)`

[6] `https://en.wikipedia.org/wiki/Ring_(mathematics)`. Note that there is no notion of subtraction in a ring: the minus signs actually are part of the coefficients.

[7] `ttps://en.wikipedia.org/wiki/Field_(mathematics)`

The main takeaway though is that mathematicians have defined a set of precise rules (addition, scalar multiplication, exponentiation of an indeterminate), and that by cleverly combining such rules and only such rules, they have obtain a bunch of interesting results, and we want to use one of them in particular.

Let's get back to our equation (1); let me add some parenthesis for clarity:

$$\sum_{i=0}^{n} \left(\alpha_i L^i(\boldsymbol{v})\right) = \mathbf{0}_V$$

Our goal is to transform this expression so that it involves a polynomial in $\mathbb{C}[L]$[8].

Let's start by pulling out the $\boldsymbol{v}$ on the left-hand side as such:

$$\left(\underbrace{\sum_{i=0}^{n} \alpha_i L^i}_{=:P(L)} \right) (\boldsymbol{v}) = \mathbf{0}_V$$

What's P ? It's a function which takes a linear operator on V and returns ... A polynomial? But then, we don't know how to evaluate a polynomial on a vector $\boldsymbol{v} \in V$ so there's an problem somewhere.

P actually returns a new *linear operator on* V:

$$P : \begin{pmatrix} (V \to V) & \to & (V \to V) \\ L & \mapsto & \sum_{i=0}^{n} \alpha_i L^i \end{pmatrix}$$

But this means that while in (1) the $\sum$ was a sum of complex numbers, it's now a sum of functions, and that $\alpha_i L_i$ went from a multiplication between complex numbers to a scalar multiplication on a function.

The natural way, that is, the simplest consistent way, to do so, is to define them pointwise[9] for two functions $f, g : X \to Y$, we define $(f + g) : X \to Y$ by:

$$(\forall x \in X),\ (f + g)(x) := f(x) + g(x)$$

The process is similar for scalar multiplication:

$$(\forall x \in X), (\forall y \in Y),\ (yf)(e) := yf(e)$$

We *equip* the space of (linear) functions (on V) with additional laws. All in all, P is well defined[10], and that we can indeed pull the $\boldsymbol{v}$ out.

How then can we go from such a weird "meta" function P to a polynomial? Well, as we stated earlier, polynomials are defined by a set of specific rules: addition, scalar multiplication, and exponentiation of the indeterminate.

But if you look closely:

- Our point-wise addition has the same property as the additions on polynomial (symmetric, existence of inverse elements, neutral element, etc.)
- Similarly for our scalar multiplication;
- And our rules of exponentiation on function by repeated application also follows the rules of exponentiation for an indeterminate variable.

[8] Remember, this means a polynomial of a single variable L, with coefficient in $\mathbb{C}$.

[9] `https://en.wikipedia.org/wiki/Pointwise`

[10] Meaning, the laws we introduce on functions are consistent with the results we would otherwise get without using them; you can check this out if you want

This mean that if we squint a little, if we only look at the expression $P(L)$ as having nothing but those properties, then it behaves exactly as a polynomial. Hence, for all intents and purposes, it "is" a polynomial, and we can manipulate it as such.
So we can apply the fundamental theorem of algebra[11], we know that we can always factorize polynomials with complex coefficient as such:

$$(\exists (c, \lambda_1, \ldots, \lambda_n) \in \mathbb{C}^{n+1}, c \neq 0),\ P(L) = c\prod_{i=0}^{n}(L - \lambda_i)$$

But don't we have a problem here? L is an abstract symbol, and we're "subtracting" it a scalar? Well, there are a few implicit elements:

$$P(L) = c\prod_{i=0}^{n}(L^1 + (-\lambda_i)L^0)$$

Let's replace this new expression for $P(L)$ in our previous equation, which we can do essentially re-using our previous argument: the rules (addition, scalar multiplication, etc.) to manipulate polynomials are "locally" consistent with the rules to manipulate our (linear) functions:

$$\left(c\prod_{i=0}^{n}(L^1 - \lambda_i L^0)\right)(\boldsymbol{v}) = \mathbf{0}_V$$

Note that L^0 becomes the identity function, and by using the previous point-wise operations, we can reduce it to:

$$c\prod_{i=0}^{n}(L(\boldsymbol{v}) - \lambda_i \mathrm{id}_V(\boldsymbol{v})) = c\prod_{i=0}^{n}(L(\boldsymbol{v}) - \lambda_i \boldsymbol{v}) = \mathbf{0}_V$$

Now, $c \neq 0$ by the fundamental theorem of algebra. So we must have:

$$\prod_{i=0}^{n}(L(\boldsymbol{v}) - \lambda_i \boldsymbol{v}) = \mathbf{0}_V$$

Which implies that there's at least a λ_j for which

$$L(\boldsymbol{v}) - \lambda_j \boldsymbol{v} = \mathbf{0}_V \Leftrightarrow L(\boldsymbol{v}) = \lambda_j \boldsymbol{v}$$

But we've selected $\boldsymbol{v}$ to be non-zero: λ_j is then an eigenvalue λ_j associated to the eigenvector $\boldsymbol{v}$.

□

OK; let me adjust the fundamental theorem a little bit, and let's prove it.

Theorem 2. *Let $H : V \to V$ be a Hermitian operator on a finite, n-dimensional vector space V, equipped with an inner-product $\langle ., . \rangle$.*

Then, the eigenvectors of H form an orthogonal basis of V, and the associated eigenvalues are real.

Saying it otherwise, it means that a matrix representation M_H of H is diagonalizable, and that two eigenvectors associated with distinct eigenvalues are orthogonal.

Proof. I'm assuming that this is clear for you that the eigenvectors associated to the eigenvalues of a diagonalizable matrix makes a basis for the vector space. Again, refer to a linear algebra course for more.

Furthermore, you can refer to the book for a proof of orthogonality of the eigenvectors associated to distinct eigenvalues[12].

Note that I've included a mention to characterize the eigenvalues as real numbers: there's already a proof in the book, but it comes with almost no effort with the present proof, so I've included it anyway.

Remains then to prove that the matrix representation M_H of H is diagonalizable (and that the eigenvalues are real). Let's prove this by induction on the dimension of the vector space. If you're not familiar with proofs by induction, the idea is as follow:

[11] `https://en.wikipedia.org/wiki/Fundamental_theorem_of_algebra`

[12] I'm not doing it here, as I've avoided the bra-ket notation, and this would force me to talk about dual spaces, and so on.

- Prove that the result is true, say, for $n = 1$;
- Then, prove that if the result is true for $n = k$, then the result must be true for $n = k + 1$.
- If the two previous points hold, then you can combine them: if the first point hold then by applying the second point, the result must be true $n = 1 + 1 = 2$. But then by applying the second point again, it must be true that the result holds for $n = 2 + 1 = 3$.
- And so on: the result is true $\forall n \in \mathbb{N}\backslash\{0\}$.

$\boxed{n = 1}$ Then, H is reduced to a 1×1 matrix, containing a single element h. This is trivially diagonal already, and because H is assumed to be Hermitian, the only eigenvalue $h = h^*$ is real.

$\boxed{\text{Induction}}$ Assume the result holds for any Hermitian operator $H : W \to W$ on a k-dimensional vector space W over $\mathbb{C}$.

Let V be a $k + 1$-dimensional vector space over $\mathbb{C}$. By our previous lemma, $H : V \to V$ must have at least one eigenvalue $\lambda \in \mathbb{C}$ associated to an eigenvector $\boldsymbol{v} \in V$.

Pick $\{\boldsymbol{v}_1, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_{k+1}\} \subset V$ so that $\{\boldsymbol{v}, \boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_{k+1}\}$ is an (ordered) basis of V[13].

Apply the Gram-Schmidt procedure[14] to extract from it an (ordered) orthonormal basis $\{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_{k+1}\}$ of V; note that by construction:

$$\boldsymbol{b}_1 = \frac{\boldsymbol{v}}{\|\boldsymbol{v}\|}$$

That's to say, $\boldsymbol{b}_1$ is still an eigenvector for λ[15].

Now we're trying to understand what's the matrix representation D_H of H, in this orthonormal basis. If you've taken the blue pill, you know how to "read" a matrix:

$$D_H = \begin{pmatrix} \begin{pmatrix} | \\ H(\boldsymbol{b}_1) \\ | \end{pmatrix} & \begin{pmatrix} | \\ H(\boldsymbol{b}_2) \\ | \end{pmatrix} & \ldots & \begin{pmatrix} | \\ H(\boldsymbol{b}_{k+1}) \\ | \end{pmatrix} \end{pmatrix}$$

OK; let's start by what we know: $\boldsymbol{b}_1$ is an eigenvector for H associated to λ, meaning:

$$H(\boldsymbol{b_1}) = \lambda \boldsymbol{b}_1 = \lambda \boldsymbol{b}_1 + \sum_{i=2}^{k+1} 0 \times \boldsymbol{e}_i = \begin{pmatrix} \lambda \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Rewrite D_H accordingly, and break it into blocks:

$$D_H = \begin{pmatrix} \lambda & \begin{pmatrix} | \\ H(\boldsymbol{b}_2) \\ | \end{pmatrix} & \ldots & \begin{pmatrix} | \\ H(\boldsymbol{b}_{k+1}) \\ | \end{pmatrix} \\ 0 & & & \\ \vdots & & & \\ 0 & & & \end{pmatrix} = \left(\begin{array}{c|c} \lambda & A \\ \hline 0 & \\ \vdots & C \\ 0 & \end{array}\right)$$

Where A is a $1 \times k$ matrix (a row vector), and C a $k \times k$ matrix. But then H is Hermitian, which means its matrix representation obeys:

$$D_H = (D_H^T)^* = D_H^\dagger$$

[13] Start with $W = \{\boldsymbol{v}\}$, and progressively augment it with elements of V so that all elements in W are linearly independent. If we can't select such elements no more, this mean we've got a basis. Ordering naturally follows from the iteration steps.

[14] `https://en.wikipedia.org/wiki/Gram%E2%80%93Schmidt_process`

[15] $H(\boldsymbol{b}_1) = H(\boldsymbol{v}/\|\boldsymbol{v}\|)$, by linearity of H, this is equal to $\frac{1}{\|\boldsymbol{v}\|} H(\boldsymbol{v})$. But $\boldsymbol{v}$ is an eigenvector for an eigenvalue λ, so this is equal to $\frac{\lambda}{\|v\|}\boldsymbol{v} = \lambda \frac{\boldsymbol{v}}{\|\boldsymbol{v}\|} = \lambda \boldsymbol{b_1}$

This implies first that $\lambda = \lambda^*$, i.e λ is real, and we'll see shortly, can be considered an eigenvalue, as we can transform D_H in a diagonal matrix with λ on the diagonal.

Second, $A^\dagger = (0\ 0\ \dots\ 0) = A$, i.e:

$$\left(\begin{array}{c|ccc} \lambda & 0 & \dots & 0 \\ \hline 0 & & & \\ \vdots & & C & \\ 0 & & & \end{array}\right)$$

Third, $C = C^\dagger$. But then, C is a $k \times k$ Hermitian matrix, corresponding to a Hermitian operator in a k-dimensional vector space. Using the induction assumption, it is diagonalizable, with real valued eigenvalues. Hence D_H is diagonalizable, and all its eigenvalues are real.

□