1 Mathematical Prerequisites

1.1 Linear Algebra

1.1.1 Vector Space

Definition 1.1 (Vector Space): A vector space $\mathbb{V}$ over a field $\mathbb{F}$ is a an non-empty set together with two binary operations($*$,$\otimes$) that satisfy the following axioms.
1. If $\boldsymbol{v} \in \mathbb{V}$ and $\boldsymbol{w} \in \mathbb{V}$ then $\boldsymbol{v} * \boldsymbol{w} \in \mathbb{V}$
2. If $\boldsymbol{v} \in \mathbb{V}$ and $a \in \mathbb{F}$ then $a \otimes \boldsymbol{v} \in \mathbb{V}$
3. For every $\boldsymbol{v}$ $\exists$ $\boldsymbol{p}$ such that $\boldsymbol{v} * \boldsymbol{p} = \boldsymbol{e}$
4. For very vector space $\mathbb{V}$, $\exists$ $\boldsymbol{e}$ such that $\boldsymbol{v} * \boldsymbol{i} = \boldsymbol{e} * \boldsymbol{v} = \boldsymbol{v}$

Now this idea of vector space seems to do nothing with our high school idea of vectors. Before going into this question I would like improve our notation of vectors into more physicists like. So from now on we'll denote a vector by $|a\rangle$ and if I were to write all these axioms in one line the best I can write is $\alpha|u\rangle + \beta|v\rangle = |w\rangle$ where $|w\rangle \in V$.

Exercise 1.1: Write 5 examples of vector spaces.

Exercise 1.2: Check whether the following set forms a vector space or not?
1. $\mathbb{R}$ over $\mathbb{C}$
2. $\mathbb{C}$ over $\mathbb{R}$
3. Set of all matricies with zero trace over $\mathbb{R}$
4. Set of all matricies with zero determinent over $\mathbb{R}$

Definition 1.2 (Subspace): Let V be a vector space over a field F and U be a subset of V then U is called a subspace if U is also a vector space over field F.

Example 1.1: Think of $\mathbb{R}$ over $\mathbb{Q}$ and $\mathbb{Q}$ over $\mathbb{Q}$. Write a formal proof.

Definition 1.3 (Linear Dependence): Let $\mathbb{V}$ be a set such that $\{|v_1\rangle, |v_2\rangle, ..., |v_n\rangle\}$ is subset of $\mathbb{V}$ then vectors are said to be linearly independent only if $\sum_j a_j |v_j\rangle = 0$ only if all a_j are zero.

Now clearly as you can see from the definition that you cannot write any linearly independent vector as a sum of other vectors in the space then if I take all the linearly independent vectors and make a set out of them then they form something we call as **basis**. Now take an example

Example 1.2: Say I have three vectors $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ then these three are linearly independent. Check.

Solution: Now if denote them as $|e_1\rangle, |e_2\rangle, |e_3\rangle$ respectively by definition of vector space another vector $|v\rangle$ can be given as $|v\rangle = c_1|e_1\rangle + c_2|e_2\rangle + c_3|e_3\rangle$ where c_1, c_2 and $c_3 \in \mathbb{R}$. Now by varing a,b and c we can have any vector in the $\mathbb{R}^3$ ■

Now I thing I should formalise the above ideas

Definition 1.4 (Basis): Let V be a vector space over F. A subset B of V is called a basis for V if B is linearly independent over F and every element of V is a linear combination of elements of B.

Theorem 1.1.1.1: If $\{|u_1\rangle, |u_2\rangle, ..., |u_n\rangle\}$ and $\{|v_1\rangle, |v_2\rangle, ..., |v_n\rangle\}$ represents the basis of some vector space V then $m = n$.

Definition 1.5 (Dimensions): The number of elements in a basis set is called its dimensions.

Now so far I have discussed a lot concepts which doesn't appear that frequently in the my day to day QM but now I should define something that is key to the idea of QM, i.e. **inner product**.

Definition 1.6: An inner product is a map from the vector space $\mathbb{V}$ to a field $\mathbb{F}$ defined as $(.,.) : \mathbb{V} \times \mathbb{V} \mapsto F$ following some properties given below
1. $(.,.)$ is linear in second argument as $\left(|u\rangle, \sum_i \lambda_i |v_i\rangle\right) = \sum_i \lambda_i (|u\rangle, |v_i\rangle)$
2. $(|u\rangle, |w\rangle) = (|w\rangle, |u\rangle)^*$
3. $(|u\rangle, |u\rangle) \geq 0$

Now a vector space with an inner product attached to it is called **an inner product space**. But before I talk about more on inner product I would introduce something that we call as **Dual Space**.
So as defined above we have inner product relates a vector with a complex number. So I have a functional f such that $f(|v\rangle)$ is a complex number. Let us think it through little more now see the following properites of a functional

1. Linearity in second argument: $f(\alpha|u\rangle + \beta|v\rangle) = \alpha f(|u\rangle) + \beta f(|v\rangle)$
2. $(f + g)|u\rangle = f(|u\rangle) + g(|u\rangle)$
3. $g() = af(|u\rangle)$ is also a linear functional.

Now from argument 2 and 3, one may say that set of all linear functional forms a vector space. which indeed they do and hence they are called **dual space**. Now I would like make a distinction between elements of our vector space and the dual space. Please note that elements of the vector space,in our case are functions or row matrices and dual space elements are functional. Now we would *assume that there is a one to one correspondence between elements of dual space and our vector space*. I would like denote a functional as $f() \equiv \langle f|$. Now I would like to formally introduce an inner product widely used in QM $\langle i|j\rangle = \delta_{ij}$ for finite dimensional vector spaces we may represent our quantum states as row matrices and for case of infinite dimensional vector spaces definitely we have functions. For $\langle i|j\rangle = 0$ then two states are said to be **orthogonal** and one also define a set of **orthonormal** vectors as $\langle i|i\rangle = \lambda_i^2$ then we may define a new set of vectors as $|e_i\rangle \equiv \frac{|i\rangle}{\lambda_i}$

1.1.2 Linear Operators

So we defined *a **function** as rule which connects two numbers* and then we defined *a **functional**, which connects a vector and a number* now we want a new kind of "thing" which connects a vector and a vector. One can define any such rule but one we are interested in is given as

$$F(|u\rangle) = a|u\rangle \tag{1}$$

and this what an operator does. So I shall give a formal definition of an operator.

Definition 1.7 (Operator): An operator is a map between two vector spaces and sometimes possibly the same vector space. $\mathcal{O} : V \mapsto W$

For our case we would restrict ourselves to with the same vector space. a special class among these operators is **Linear Operators**. We should give a formal definition of Linear Operators

Definition 1.8 (Linear Operators): A linear operator is defined as the following

$$\mathcal{O}(\alpha|u\rangle + \beta|v\rangle) = \alpha\mathcal{O}|u\rangle + \beta\mathcal{O}|v\rangle \tag{2}$$

Alright now I should define few rules of the game
Two operators say A and B are said to be equal only if $A|u\rangle = B|u\rangle \forall |u\rangle \in \mathbb{V}$. Next for addition and multiplication of operators I define $C = AB$ and $D = A + B$, then I may have,

$$C(\alpha|u\rangle + \beta|v\rangle) = \alpha AB|u\rangle + \beta AB|v\rangle \tag{3}$$

$$D(\alpha|u\rangle + \beta|v\rangle) = \alpha(A + B)|u\rangle + \beta(A + B)|v\rangle \tag{4}$$

Clearly one may observe that both C and D themselves are linear operators and they follow all the rules like numbers except for commuting. For now I'll just introduce a quantity which we call as commutation relation as

Definition 1.9 (Commutator): A commutator of A and B is defined as

$$[A, B] = AB - BA \tag{5}$$

and on the same grounds an opposite of it **anti-commutator**

Definition 1.10: Anti-Commutator An anti-commutator of A and B is defined as

$$\{A, B\} = AB + BA \tag{6}$$

wait for a couple of more topics after I'll really get you to calculate these and I should also give you a couple of them which will remain use full to you for rest of your life. Now defining product of two operator one can go ahead and define operator power to something.

Definition 1.11 (Power of an Operator): An operator rasied to power m is defined as $\mathcal{O}^m|u\rangle = \mathcal{O}$..m times..$\mathcal{O}|u\rangle$

And now one would like wonder what this means [sin(A)] where A is an operator or e^A thanks to the taylor series we have the following relations

$$e^A = \sum_{n=0}^{\infty} \left(\frac{A^n}{n!} \right) \tag{7}$$

and similarly one can define $\sin(A)$ and $\cos(A)$.

Exercise 1.3: What these following things means mathematically, where A is an operator.
1. $\sin(A)$
2. $\cos(A)$
3. $\tanh(A)$

Now I should present a difficulty we have with operators which you would encounter while doing QM

Example 1.3: Say we have x,y $\in \mathbb{R}$, then we'll have

$$e^{x+y} = e^x e^y \tag{8}$$

but this doesn't hold for A,B such that A and B are operators. I should show this (Professor Vidhyadhiraja, asked me this question during one of our meetings) we have $e^{A+B} = 1 + \frac{A+B}{1} + \frac{(A+B)^2}{2!} + ...$ and for $e^A e^B = \left(1 + \frac{A}{1!} + \frac{A^2}{2!} + ...\right)\left(1 + \frac{B}{1!} + \frac{B^2}{2!} + ...\right)$ now in the second expansion we'll have terms containing BA which are clearly not there in first expansion. So clearly $e^{A+B} \neq e^A e^B$

Now the next question is how to fix this ? We have a nice formula called **Baker-Campbell-Hausdorff Formula**

Theorem 1.1.2.1 (Baker-Campbell-Hausdorff Formula):

$$e^X e^Y = e^Z \tag{9}$$

where Z is given as following

$$Z = X + Y + \frac{1}{2}[X, Y] + \frac{1}{12}[X, [X, Y]] - \frac{1}{12}[Y, [X, Y]] + ... \tag{10}$$

here both X,Y are non-commutative in the Lie Algebra of a Lie Group.

Exercise 1.4: Prove the Baker-Campbell-Hausdorff Formula.

Now one last thing in the algebra of operators is how operators act on dual space. Suppose we have $\langle v|$ then $\langle v|\mathcal{O} \equiv \langle v|\mathcal{O}|u\rangle$ for some $|u\rangle$.

Remark: We have $A|u\rangle = a|u\rangle$ but

$$\langle u|A \neq \langle u|a \tag{11}$$

on the other hand for some vector $|u\rangle$ $(A|u\rangle)^\dagger = \langle u|A^\dagger = \langle u|a^*$

1.1.3 Matrix Representation and Outer Product

Now I would like to introduce a new concept which is very important in QM, i.e. matrix representation of operators. So let us say we have a vector space $\mathbb{V}$ and a basis $\{|e_1\rangle, |e_2\rangle, ..., |e_n\rangle\}$ then any vector $|u\rangle$ and $|v\rangle$ can be written as $|u\rangle = \sum_i u_i|e_i\rangle$ and $|v\rangle = \sum_j v_j|e_j\rangle$ respectively. Now suppose we have an operator $\mathcal{O} : \mathbb{V} \mapsto \mathbb{V}$ and suppose $\mathcal{O}|u\rangle = |v\rangle$ then we can write $\mathcal{O}|u\rangle = \sum_{ij} \mathcal{O}_{ij} u_i|e_i\rangle = \sum_j v_j|e_j\rangle$ now by using einstein summation convention we have

$$\mathcal{O}_{ij} u_i = v_j \tag{12}$$

and hence we have $\mathcal{O}_{ij}$ is a matrix. Now one can also determine the matrix element as

$$\mathcal{O}_{ij} = \langle e_i|\mathcal{O}|e_j\rangle \tag{13}$$

Now I define something called as **outer product** which is defined as

Definition 1.12 (Outer Product): An outer product of two vectors $|u\rangle$ and $|v\rangle$ is defined as $|u\rangle\langle v| = \mathcal{O}$ where $\mathcal{O}_{ij} = u_i^* v_j$

Exercise 1.5: Prove that $|u\rangle\langle v|$ is an linear operator.

Exercise 1.6: Write following operators in matrix form
1. $\mathcal{O}|0\rangle = |0\rangle$ and $\mathcal{O}|1\rangle = |1\rangle$
2. $\mathcal{O}|0\rangle = |1\rangle$ and $\mathcal{O}|1\rangle = |0\rangle$
3. $\mathcal{O}|0\rangle = \iota|1\rangle$ and $\mathcal{O}|1\rangle = -\iota|0\rangle$
4. $\mathcal{O}|0\rangle = |0\rangle$ and $\mathcal{O}|1\rangle = -|1\rangle$

the solution of the above lead to 4 unique matrices called as **Pauli Matrices**, which are

$$\mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{14}$$

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{15}$$

$$\sigma_y = \begin{pmatrix} 0 & -\iota \\ \iota & 0 \end{pmatrix} \tag{16}$$

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{17}$$

Now the next question would be to write the rules of algebra for matrices.
1. Say I define, $C = A + B$,then in some basis the matrix elements of C are given as $\langle i|C|j\rangle = \langle i|A|j\rangle + \langle i|B|j\rangle$
2. Now let us define, $C = AB$ then the matrix element of the matix C can be given as $\langle i|C|j\rangle = \sum_k \langle i|A|k\rangle\langle k|B|j\rangle$
3. Now division is not so generally defined but I'll try to define it so for some matrices A and B, a matrix C is defined as $C = AB^{-1}$

This one may call as division but this calls upon for us to define this A^{-1} called inverse of A but I won't describe the method to compute inverse of a matrix. The only condition I will put forward is $\det(A) \neq 0$.

1.2 Some Special Operators

I would like to make a point on the fact that it may so happen that $A_l^{-1}A = E$ and $\mathbb{A}_r^{-1} = E$ and it may so happen $\mathbb{A}_l^{-1} \neq 1$ and $A_r^{-1}A \neq 1$. Here $A_l^{\{-1\}}$ and $A_r^{\{-1\}}$ are called left and right inverse respectively. But there is an important theorem that I should tell here

Theorem 1.2.1: If for a given operator A both $A_l^{\{-1\}}$ and $A_r^{\{-1\}}$ exits then $A_l^{\{-1\}} = A_r^{\{-1\}}$ and this pair is unique.

Exercise 1.7: Prove the above theorem.

Now that I have proved for a nice class of operators which have the property $A_{\{l\}}^{\{-1\}} = A_{\{r\}}^{\{-1\}}$ and the pair is unique then I may say that $A_l^{\{-1\}} = A_r^{\{-1\}} = A^{\{-1\}}$ and such operators are called **Invertible**. newpage

Exercise 1.8: Prove that $(AB)^{\{-1\}} = B^{\{-1\}}A^{\{-1\}}$ if both $A^{\{-1\}}$ and $B^{\{-1\}}$ exits.

Now suppose you have the scalar product defined as following

$$\langle a|X|b\rangle = \overline{\langle b|A|a\rangle} \tag{18}$$

Then I may write $X = A^\dagger$, $A^\dagger$ is called **adjoint of A**.

Exercise 1.9: Prove the following results
1. $(AB)^\dagger = B^\dagger A^{\{\dagger\}}$
2. $(A + B)^\dagger = A^\dagger + B^\dagger$

Now there is a special class of operators **Hermitian Operators** defined as $A^\dagger = A$ and another important class of operators are **Unitary Operators** defined as $\mathbb{U}^\dagger = U^\dagger U = \mathbb{I}$. Unitary Operators have this wonderful property that they preserve norm, these two operators are something that you'll encounter your whole life as a physicist.

Theorem 1.2.2: If U is unitary then U is supposed to preserve the norm of a vector.

Proof: Let $|u\rangle$ be a vector the its norm will be

$$\|a\| = \langle a|a\rangle \tag{19}$$

Let

$$|b\rangle = U|a\rangle \tag{20}$$

Then

$$\langle b|b\rangle = \langle a|U^\dagger U|a\rangle = \langle a|a\rangle \tag{21}$$

■

Now I'll introduce another important class of operators called **projection operators**. Suppose we have a vector space S spanned the the given set of vectors $\{|1\rangle, |2\rangle, |3\rangle, ..., |n\rangle\}$ say $|u\rangle \in$

S. Let S_1 be the vector space spanned by $\{|1\rangle\}$ then I want the projection of $|u\rangle$ on S_e. For a second I would like you to just remember your high school physics where you might have been asked to find how much of a vector is along some given vector which is precisely is your dot product and if you want to construct the vector then you'll just multiply the references vector by the scalar one got. Here we also have a mechanism and that mechanism is written as **Projection Operator**. For a vector $|\psi\rangle$ a projection operator $\hat{P}$ defined as $\hat{P} \equiv |u\rangle\langle u|$ will project $|\psi\rangle$ into a subspace spanned by $|u\rangle$. Here are some properties of projection operators
1. $\hat{P}^2 = \hat{P}$
2. $\hat{P}^\dagger = \hat{P}$

1.3 Eigenvalues and Eigenkets

Definition 1.13 (Eigenvalue and Eigenvectors): Given an operator A acting on a vector space V, then there may or may not exists a vector such that

$$A|u\rangle = a|u\rangle \tag{22}$$

such vector $|u\rangle$ is called its **eigenvector** and a is called its **eigenvalue**.

Hermitian operators play a particularly important role in physics, especially in wave phenomena and in quantum mechanics. This is the reason that compels us to examine in greater detail the properties of Hermitian operators.

Theorem 1.3.1: All the eigenvalues of an Hermitian operator are real.

Proof: Let H be an operator and $|u\rangle$ be its eigenket then

$$H|u\rangle = a|u\rangle \tag{23}$$

$$H^{\{\dagger\}}|u\rangle = a^*|u\rangle \tag{24}$$

Subtracting the above equation

$$(0)|u\rangle = \left(a - a^{\{*\}}\right)|u\rangle \tag{25}$$

For the above condition to satisfy $a = a^*$ ∎

So in the above proof we were able to show that eigenvalues of Hermitian Operators are real. Probably now one would like to convince himself that why hermitian operators represent experiments but I should tell you that non-hermitian QM is also equally flourishing and real eigenvalues have nothing to do with it. Now other important thing which I would like to prove is orthognality of different eigenkets.

Theorem 1.3.2: Two eigenkets corresponding to different eigenvalue are orthogonal to each other.

Proof: Let H be an operator and $|1\rangle$ be its eigenket then

$$\langle 2|H|1\}\rangle = a\langle 2||1\rangle \tag{26}$$

$$\langle 1|H|2\rangle = b\langle 1||2\rangle \tag{27}$$

Subtracting the above equation, and as $\langle 1|H|2\rangle = \langle 2|H|1\rangle$

$$0 = (a - b)\ \texttt{bra}\{2\}\ \texttt{ket}\{1\} \tag{28}$$

Therefore $\langle 2|1\rangle = 0$ ■

but clearly this proof will not work if $a = b$ or to say that we have degeneracy. Now we may want to extend the proof to degenerate case as well.

Exercise 1.10: Extend the above proof for degenerate case as well.

Theorem 1.3.3 (Spectral Decomposition): Any normal operator M on a vector space V is diagonal with respect to some orthonormal basis for V . Conversely, any diagonalizable operator is normal.

Proof: Someday later..... ■

This theorem enables us to decompose any hermitian operators into some basis in which it is diagonal

$$H = \sum_i \lambda_i |i\rangle\langle i| \tag{29}$$