# Amalgamated Worksheet \# 5 

Induction Workshop

May 6, 2013

## 1 Induction warmup

Problem 1: (Sum of the first $n$ integers) Prove by induction that

$$
1+2+\cdots+n=\frac{1}{2} n(n+1) .
$$

Solution: The base case $n=1$ is clear, as $1=\frac{1}{2} \cdot 1 \cdot(1+1)$.
Suppose that $1+2+\cdots+n=\frac{1}{2} n(n+1)$. Then

$$
\begin{aligned}
1+2+\cdots+n+(n+1) & =\frac{1}{2} n(n+1)+(n+1) \\
& =\frac{1}{2}(n(n+1)+2(n+1)) \\
& =\frac{1}{2}((n+2)(n+1))
\end{aligned}
$$

Problem 2: (Geometric series) Prove by induction that

$$
1+r+r^{2}+\cdots+r^{n}=\frac{1-r^{(n+1)}}{1-r}
$$

where $r \neq 1$
Solution: The base case $n=0$ is immediate, as $1=\left(1-r^{0+1}\right) /(1-r)$, so long as $r \neq 1$.

Suppose that $1+r+\cdots+r^{n}=\left(1-r^{n+1}\right) /(1-r)$. We add to both sides and simplify

$$
\begin{aligned}
1+r+\cdots+r^{n}+r^{n+1} & =\frac{1-r^{n+1}}{1-r}+r^{n+1} \\
& =\frac{1-r^{n+1}+r^{n+1}(1-r)}{1-r} \\
& =\frac{1-r^{n+2}}{1-r}
\end{aligned}
$$

Remark: One usually thinks of this more conceptually in the following way: if $x=1+$ $r+\cdots+r^{n}$, then $r x=r+r^{2}+\cdots+r^{n+1}$, and $r x-x=r^{n+1}-1$ and $x=\left(r^{n+1}-1\right) /(r-1)$.

Problem 3: Correction - show that $4^{n}+5$ is divisible by 3
Solution: If $n=0$ we get $4^{0}+5=6$, which is divisible by 3 .
Now suppose that $4^{n}+5$ is divisible by 3 . Then

$$
\begin{aligned}
4^{n+1}+5 & =4 \cdot 4^{n}+4 \cdot 5-3 \dot{5} \\
& =4\left(4^{n}+5\right)-15
\end{aligned}
$$

which is a difference of integers which are divisible by 3 , hence is itself divisible by 3 . This completes the induction.

Remark: Previously, the exercise was stated with a minus instead of a plus: show that $4^{n}-5$ is divisible by 3 . This is false, since for example it fails when $n=1,2$ etc. While I was thinking about this, I realized that the $a_{n}=4^{n}-5$ has some cool properties. Try proving the following for fun (in order of increasing difficulty) for each $n>0: a_{n}$ is even, 5 does not divide $a_{n}, 3$ does not divide $a_{n}$, and finally $\operatorname{gcd}\left(a_{n}, a_{n+1}\right)=1$.

Problem 4: Show that $4^{n}+15 n-1$ is divisible by 9 for all $n$.
Solution: The base case works: 9 divides $4+15-1=18$.
Suppose that 9 divides $A=4^{n}+15 n-1$. Then of course 9 divides

$$
\begin{aligned}
4\left(4^{n}+15 n-1\right) & =4^{n+1}+60 n-4 \\
& =4^{n+1}+15 n-1+45 n-3+15-15 \\
& =\left(4^{n+1}+15(n+1)-1\right)+45 n-18
\end{aligned}
$$

since also 9 divides $45 n-18$, the result follows.
Remark: In light of the correction to Problem 3, here is another solution. Notice that $15 n-6=3(5 n-2)$ is divisible by 3 as is $4^{n}+5$ (see Problem 3). Hence, their sum is also divisible by 3

$$
\left(4^{n}+5\right)+(15 n-6)=4^{n}+15 n-1
$$

which is the desired conclusion.

Problem 5: Prove that $n!>2^{n}$ for all $n \geq 4$

Solution: If $n=4$, then $4!=24>2^{4}=16$.
Suppose for induction that $n!>2^{n}$ for some $n \geq 4$. Then $(n+1)>2$, which in conjunction with the supposed inequality says that $(n+1) n!>2 \cdot 2^{n}$, i.e. $(n+1)!>$ $2^{n+1}$ as desired.

Problem 6: Let $a$ and $b$ be two distinct integers and $n$ any positive integer. Prove that $a^{n}-b^{n}$ is divisible by $(a-b)$.

Solution: The identity in the hint allows one to use induction. The case $n=1$ is clear.

For induction, suppose that $(a-b)$ divides $a^{n}-b^{n}$. Then we see that $a-b$ divides both $\left(a^{n}+b^{n}\right)(a-b)$ and $\left(a^{n}-b^{n}\right)(a+b)$. According to the hint, we have that $(a-b)$ divides $2\left(a^{n+1}-b^{n+1}\right)=\left[\left(a^{n}+b^{n}\right)(a-b)+\left(a^{n}-b^{n}\right)(a+b)\right]$. Now if $(a-b)$ is odd, we are done, as we can divide a factor of 2 from the equation

$$
(a-b) d=2\left(a^{n+1}-b^{n+1}\right)
$$

to show that $a-b$ divides $a^{n+1}-b^{n+1}$. On the other hand, if $(a-b)$ is even, then also $a+b$ and $a^{n}+b^{n}$ are even. [Write $b=a+2 k$, then $a+b=2 a+2 k$ and $a^{n}+b^{n}=a^{n}+a^{n}+n a^{n-1} 2+\cdots+2^{n}=2 a^{n}+2\left(n a^{n}+\cdots+2^{n-1}\right)$.] Therefore the hint can be re-written as

$$
a^{n+1}-b^{n+1}=\left(\frac{a^{n}+b^{n}}{2}\right)(a-b)+\left(a^{n}-b^{n}\right)\left(\frac{a+b}{2}\right)=\alpha(a-b)+\left(a^{n}-b^{n}\right) \beta
$$

and for the same reasons as before, $(a-b)$ divides the right hand side.
Hint: Use the identity

$$
\left(a^{n+1}-b^{n+1}\right)=\frac{1}{2}\left(\left(a^{n}+b^{n}\right)(a-b)+\left(a^{n}-b^{n}\right)(a+b)\right) .
$$

## 2 Induction on steroids

### 2.1 Peyam Tabrizian

## Problem 1:

Show by induction on $n$ that the determinant of an upper-triangular $n \times n$ matrix $A$ equals to the product of its diagonal entries.

Base case: If $n=1$, then any $1 \times 1$ upper-triangular matrix $A$ is of the form $\left[a_{11}\right]$, and then:

$$
\operatorname{det}(A)=a_{11}=\prod_{i=1}^{1} a_{i i}
$$

Induction step: Suppose the result holds for any $n \times n$ upper-triangular matrix, and let $A$ be an $(n+1) \times(n+1)$ upper-triangular matrix, of the form:

$$
A=\left[\begin{array}{cccc}
a_{11} & \star & \cdots & \star \\
0 & a_{22} & \star & \star \\
0 & 0 & \ddots & \vdots \\
0 & \cdots & \cdots & a_{(n+1)(n+1)}
\end{array}\right]
$$

Now expanding $\operatorname{det}(A)$ along the first column of $A$, we get:

$$
\operatorname{det}(A)=a_{11} A=a_{11} \operatorname{det}\left[\begin{array}{cccc}
a_{22} & \star & \cdots & \star \\
0 & a_{33} & \star & \star \\
0 & 0 & \ddots & \vdots \\
0 & \cdots & \cdots & a_{(n+1)(n+1)}
\end{array}\right]=a_{11} \operatorname{det}(B)
$$

where:

$$
B=\left[\begin{array}{cccc}
a_{22} & \star & \cdots & \star \\
0 & a_{33} & \star & \star \\
0 & 0 & \ddots & \vdots \\
0 & \cdots & \cdots & a_{(n+1)(n+1)}
\end{array}\right]
$$

However, $B$ is an $n \times n$ upper-triangular matrix, so by induction hypothesis, we have:

$$
\operatorname{det}(B)=a_{22} \cdots a_{(n+1)(n+1)}
$$

And therefore:

$$
\operatorname{det}(A)=a_{11} \operatorname{det}(B)=a_{11}\left(a_{22} \cdots a_{(n+1)(n+1)}\right)=a_{11} \cdots a_{(n+1)(n+1)}=\prod_{i=1}^{n+1} a_{i i}
$$

Hence, by induction, we're done

[^0]Note: See the footnote below for another cool way of doing this, without induction. Thank you Dan Sparks for suggesting this alternate approach! ${ }^{2}$

## Problem 2:

If $\mathbb{F}=\mathbb{C}$, show that the determinant of a linear operator $T$ equals to the product of its eigenvalues, including multiplicities

Note: You may use the fact that the determinant of $T$ equals to the determinant of $\mathcal{M}(T)$, which is independent of the basis of $V$ that you choose for $\mathcal{M}(T)^{3}$.

By Schur's theorem (Theorem 5.13), there exists a basis $\left(v_{1}, \cdots, v_{n}\right)$ of $V$ such that the matrix $\mathcal{M}(T)$ with respect to that basis is upper-triangular.
Moreover, by Prop 5.18, the entries on the diagonal $\mathcal{M}(T)$ are the eigenvalues of $T$ (including multiplicities), that is:

$$
\mathcal{M}(T)=\left[\begin{array}{ccc}
\lambda_{1} & \cdots & \star \\
0 & \ddots & \vdots \\
0 & \cdots & \lambda_{n}
\end{array}\right]
$$

(where the $\lambda_{i}$ are not necessarily distinct)

[^1]First of all, there's only one permutation $\sigma$ with the property that $\sigma(i) \geq i$, namely the identity map (Proof: Use contradiction and the pigeonhole priciple)!

This means that for any $\sigma$ other than the identity map, we have at least one $i$ such that $\sigma(i)<i$. However, since $A$ is upper-triangular, we get $a_{\sigma(i) i}=0$ for this $i$, which means that for any $\sigma$ other than the identity, we get $\operatorname{sign}(\sigma) a_{\sigma(1) 1} \cdots a_{\sigma(n) n}=0$. On the other hand, for for $\sigma=$ identity (which has sign 1), we get $\operatorname{sign}(\sigma) a_{\sigma(1) 1} \cdots a_{\sigma(n) n}=a_{11} \cdots a_{n n}$.

Since any $\sigma \in S_{n}$ is either not the identity or the identity, using the definition of the determinant, we get $\operatorname{det}(A)=a_{11} \cdots a_{n n}$
${ }^{3}$ In case you're curious, here's a proof of this fact: In Math 54 , you $\operatorname{define} \operatorname{det}(T)$ to be $\operatorname{det}(\mathcal{M}(T))$ with respect to any basis of $V$. So all you have to show is that this definition makes sense, i.e. that is independent of the choice of basis. So suppose $\mathcal{M}(T)$ and $\mathcal{M}^{\prime}(T)$ are the matrices of $T$ with respect to two different bases of $V$. We want to show $\operatorname{det}(\mathcal{M}(T))=\operatorname{det}\left(\mathcal{M}^{\prime}(T)\right)$.

But, by Theorem 10.3, we have $\mathcal{M}(T)=P \mathcal{M}^{\prime}(T) P^{-1}$ for some invertible matrix $P$. But then you can show, using Math 54 -techniques, that $\operatorname{det}(A B)=\operatorname{det}(A) \operatorname{det}(B)$, and so $\operatorname{det}(\mathcal{M}(T))=$ $\operatorname{det}\left(P \mathcal{M}^{\prime}(T) P^{-1}\right)=\operatorname{det}(P) \operatorname{det}\left(\mathcal{M}^{\prime}(T)\right) \frac{1}{\operatorname{det}(P)}=\operatorname{det}\left(\mathcal{M}^{\prime}(T)\right)$, which is what you wanted to show

However, since $\mathcal{M}(T)$ is upper-triangular by Problem 1, we have:

$$
\operatorname{det}(\mathcal{M}(T))=\lambda_{1} \cdots \lambda_{n}
$$

And hence, by the note above, we get:

$$
\operatorname{det}(T)=\operatorname{det}(\mathcal{M}(T))=\lambda_{1} \cdots \lambda_{n}=\prod_{i=1}^{n} \lambda_{i}
$$

That is, $\operatorname{det}(T)$ is the product of the eigenvalues of $T$ (counting multiplicities)

## Problem 3:

(a) Do there exist linear operators $S$ and $T \in \mathcal{L}(V)$ such that $T S-S T=I$ ?

NO, because if there were such linear operators $S$ and $T$, then we would have:

$$
\begin{aligned}
\operatorname{Tr}(T S-S T) & =\operatorname{Tr}(I) \\
\operatorname{Tr}(T S)-\operatorname{Tr}(S T) & =n \\
\operatorname{Tr}(T S)-\operatorname{Tr}(T S) & =n \\
0 & =n
\end{aligned}
$$

Where $n$ is $\operatorname{dim}(V)$, and we get a contradiction ${ }^{4} \Rightarrow \Leftarrow$
(b) Is there a $3 \times 3$ matrix $A$ with $A^{2}=-I$ ?

In general NO, because if $\mathbb{F}=\mathbb{R}$ and if there were such a matrix $A$, then we would have:

$$
\operatorname{det}\left(A^{2}\right)=(\operatorname{det}(A))^{2} \geq 0
$$

Yet, on the other hand:

$$
\operatorname{det}\left(A^{2}\right)=\operatorname{det}(-I)=-1<0
$$

[^2]Which is a contradiction $\Rightarrow \Leftarrow$
But if $\mathbb{F}=\mathbb{C}$, then YES, because the following matrix satisfies $A^{2}=-I$ :

$$
A=\left[\begin{array}{lll}
i & 0 & 0 \\
0 & i & 0 \\
0 & 0 & i
\end{array}\right]
$$

## Problem 4:

Without using any integrals, calculate the volume of the ellipsoid

$$
E=\left\{(x, y, z) \in \mathbb{R}^{3} \left\lvert\, \frac{x^{2}}{a^{2}}+\frac{y^{2}}{b^{2}}+\frac{z^{2}}{c^{2}} \leq 1\right.\right\}
$$

Where $a, b, c$ are nonnegative real numbers.

Define the following linear transformation $T \in \mathcal{L}\left(\mathbb{R}^{3}\right)$ by $^{5}$

$$
\begin{aligned}
& T(1,0,0)=(a, 0,0) \\
& T(0,1,0)=(0, b, 0) \\
& T(0,0,1)=(0,0, c)
\end{aligned}
$$

Then by the linear extension lemma, there exists such a linear transformation $T$, and moreover, you can check that $T(B)=E$, where $B$ is the unit ball in $\mathbb{R}^{3}$.

Moreover, we have:

$$
\mathcal{M}(T)=\left[\begin{array}{lll}
a & 0 & 0 \\
0 & b & 0 \\
0 & 0 & c
\end{array}\right]
$$

And so $\operatorname{det}(T)=\operatorname{det}(\mathcal{M}(T))=a b c$.
Finally, we use the cool formula:

$$
\operatorname{Vol}(T(B))=\operatorname{det}(T) \operatorname{Vol}(B)
$$

[^3]to conclude:
$$
\operatorname{Vol}(E)=\operatorname{Vol}(T(B))=\operatorname{det}(T) \operatorname{Vol}(B)=a b c \frac{4}{3} \pi(1)^{3}=\frac{4 \pi}{3} a b c
$$

TA-DAAA!!!

### 2.2 Daniel Sparks

Preliminary: If $a, b$ are natural numbers at least 1 , then we say $a$ divides $b$, and we write $a \mid b$, if there exists a third natural number $d$ such that $b=d a$. You may use the following facts:

- If $m \mid n$ and $m^{\prime} \mid n^{\prime}$, then $m m^{\prime} \mid n n^{\prime}$.
- If $(a b) \mid c$ then $a \mid c$.
- If $p$ is prime, and $p \mid(m n)$ then $p \mid m$ or $p \mid n$.

You may also find useful the formulas

- (Geometric series) $\frac{x^{r}-1}{x-1}=x^{r-1}+x^{r-2}+\cdots+1$.
- (Difference of squares) $\left(a^{2}-b^{2}\right)=(a-b)(a+b)$.

Part 1: Prove that $3 \cdot 2^{n+2}$ divides $\left(5^{2^{n}}-1\right)$ for all $n \geq 1$.
Solution: The base case $n=1$ is clear: $3 \cdot 2^{1+2}=3 \cdot 8=24$ which equals (and therefore, of course, divides) the integer $\left(5^{2^{1}}-1\right)$.

Now suppose the result is true for $n$. That is, suppose that

$$
3 \cdot 2^{n+2} \mid\left(5^{2^{n}}-1\right)
$$

Write $5^{2^{n+1}}-1=5^{2 \cdot 2^{n}}-1=\left(5^{2^{n}}\right)^{2}-1=\left(5^{2^{n}}-1\right)\left(5^{2^{n}}+1\right)$ via the difference of squares formula $\left(a^{2}-b^{2}\right)=(a-b)(a+b)$. Now, since $5^{2^{n}}$ and 1 are both odd numbers, their sum $5^{2^{n}}+1$ is even, i.e. divisible by 2 . Combining this with the inductive hypothesis completes the induction:
$3 \cdot 2^{n+2} \mid\left(5^{2^{n}}-1\right)$ and $2\left|\left(5^{2^{n}}+1\right) \Rightarrow\left(3 \cdot 2^{n+2} \cdot 2\right)\right|\left(\left(5^{2^{n}}-1\right)\left(5^{2^{n}}+1\right)\right)=5^{2^{n+1}}-1$
Rewriting this, we have $3 \cdot 2^{n+3} \mid\left(5^{2^{n+1}}-1\right)$, completing the induction.
Part 2: Let $p$ be a prime, and let $n, a, b$ be natural numbers at least 1. Prove that if $p^{n} \mid(a b)$, and $p \nmid b$, then $p^{n} \mid a$.

Solution: The induction is on $n$. The base case, $n=1$, is exactly the hint which you can take for granted: $p|a b \Rightarrow p| a$ or $p \mid b$. Since the latter disjunct cannot be true (we suppose $b$ is not divisible by $p$ ) then the former must be: $p=p^{1}$ divides $a$.

So suppose the result is true for $n$, and suppose that $p^{n+1} \mid a b$ with $b$ not divisible by $p$. Then in particular $p^{n} \mid a b$ with $b$ not divisible by $p$, so the inductive hypothesis implies that $p^{n} \mid a$. We can write $a=p^{n} d^{\prime}$. Now write out our supposition and divide by $p^{n}$ :

$$
\begin{aligned}
\left(p^{n+1}\right)(d) & =(a)(b) \\
\left(p^{n+1}\right)(d) & =\left(p^{n} d^{\prime}\right)(b) \\
p d & =d^{\prime} b
\end{aligned}
$$

Thus, $p \mid d^{\prime} b$. The given hint now says that $p \mid d^{\prime}$ or $b$, but since it cannot divide $b$ by hypothesis, $p \mid d^{\prime}$. Since $p^{n}$ divides $p^{n}$ and $p$ divides $d^{\prime}$, we see that $p^{n+1}=\left(p^{n}\right)(p)$ divides $p^{n} d^{\prime}=a$ completing the induction.

Part 3: Prove that $2^{n+2}$ divides $\left(7^{2^{n}-1}+7^{2^{n}-2}+\cdots+7+1\right)$ for $n \geq 1$. Suggestion: Try making this into a statement more like the one in Problem 1.

Solution: Let's write $S=\left(7^{2^{n}-1}+7^{2^{n}-2}+\cdots+7+1\right)$. First observe that $2^{n+2}$ divides $S$ if and only if $6 \cdot 2^{n+2}=3 \cdot 2^{n+3}$ divides $6 S=(7-1) S$. In other words $6 \cdot 2^{n+2} \cdot d=6 S$ for some $d$ if and only if $2^{n+2} \cdot d^{\prime}=S$ for some $d^{\prime}$. (In fact one can take $d=d^{\prime}$.)

So we aim to show that $3 \cdot 2^{n+3}$ divides

$$
(7-1) S=(7-1)\left(7^{n^{2}-1}+7^{n^{2}-2}+\cdots+7+1\right)=\left(7^{2^{n}}-1\right)
$$

This is exactly like Problem 1. For induction, the base case $n=1$ is clear: $3 \cdot 2^{4}=48$ divides $48=7^{2^{1}}-1$. So suppose the result is true for $n$. Then we factor

$$
7^{2^{n+1}}-1=\left(7^{2^{n}}+1\right)\left(7^{2^{n}}-1\right)
$$

Since $7^{2^{n}}$ is odd, $2 \mid\left(7^{2^{n}}+1\right)$. Combining this with the inductive hypothesis, namely $3 \cdot 2^{n+3} \mid\left(7^{2^{n}}-1\right)$, we see that $3 \cdot 2^{n+4} \mid\left(7^{2^{n+1}}-1\right)$.

## 3 Mohammad Safdari

Let $A, B$ be self adjoint operators on a finite dimensional inner product space $V$ such that $A B=B A$. Prove, by induction on $\operatorname{dim} V$, that there exists an orthonormal basis of $V$ whose elements are eigenvectors for both $A$ and $B$.

Solution: First, I will show you what I consider to be the easier proof, and then show you how to modify it to use induction. Since $A$ is self-adjoint, whether $\mathbf{F}=\mathbf{R}$ or $\mathbf{C}$,
$A$ admits an orthonormal basis of eigenvectors. In particular, there is a Jordan style orthogonal decomposition $V=\bigoplus_{\lambda} V_{\lambda}$ where $\lambda$ ranges over the distinct eigenvalues of $A$ and $V_{\lambda}=\operatorname{Null}(A-\lambda I)$. Notice that $V_{\lambda}$ is $B$ invariant: if $A v=\lambda v$ then $A B v=$ $B A v=B(\lambda v)=\lambda(B v)$, which is exactly what it means for $B v \in V_{\lambda}=\operatorname{Null}(A-\lambda I)$. We will prove in the next paragraph that $\left.B\right|_{V_{\lambda}}$ is self-adjoint. Hence we may take, for each $\lambda$, and orthonormal eigenbasis of $V_{\lambda}$ for $\left.B\right|_{V_{\lambda}}$. Call this basis $\beta_{\lambda}=\left(b_{1}^{\lambda}, \cdots, b_{e_{\lambda}}^{\lambda}\right)$. Since each $b_{i}^{\lambda} \in V_{\lambda}$, the basis $\beta_{\lambda}$ is an eigenbasis for each of $A, B$ on $V_{\lambda}$. Upon concatenating the bases into one basis $\bigcup \beta_{\lambda}=\left(b_{1}^{\lambda_{1}}, \cdots, B_{e_{\lambda_{r}}}^{\lambda_{r}}\right)$. The vectors are each of unit length and are each eigenvectors of both $A, B$. By construction, $b_{j}^{\lambda_{i}} \perp b_{\ell}^{\lambda_{k}}$ if $i=k$. On the other hand, since $V=\bigoplus_{\lambda} V_{\lambda}$ is an orthogonal direct sum, we see that $b_{j}^{\lambda_{i}} \perp b_{\ell}^{\lambda_{k}}$ when $i \neq k$ as well.

The loose string is this: Let $U$ be an invariant subspace of a self-adjoint operator $T$. Then $\left.T\right|_{U}$ is also self-adjoint, where we take as inner product on $U$ the restriction of $\langle\cdot, \cdot \cdot\rangle: V \times V \rightarrow \mathbf{F}$. More generally, $\left(\left.T\right|_{U}\right)^{*}=\left.\left(T^{*}\right)\right|_{U}$. To see this, write for any $v, w \in U$

$$
\left\langle\left(\left.T\right|_{U}\right) v, w\right\rangle=\langle T v, w\rangle=\left\langle v, T^{*} w\right\rangle=\left\langle v,\left(T^{*}\right)_{U} w\right\rangle
$$

which verifies that $\left(T^{*}\right)_{U}$ satisfies the definition of the adjoint of $\left.T\right|_{U}$, i.e. $\left(\left.T\right|_{U}\right)^{*}=$ $\left.\left(T^{*}\right)\right|_{U}$. In particular, if $T$ is self-adjoint then $\left(\left.T\right|_{U}\right)^{*}=\left.\left(T^{*}\right)\right|_{U}=\left.T\right|_{U}$ as well.

Remark: Now, the only way I have imagined getting induction into the picture is, after obtaining the orthogonal decomposition $V=\bigoplus_{\lambda} V_{\lambda}$, consider two cases: either some $V_{\lambda}=V$ or not. In the case that $V_{\lambda}=V$, we see that every vector is an eigenvector for $A$. Hence any orthonormal eigenbasis of $B$ will do the trick (notice we don't even need $A B=B A$ in this case). On the other hand, suppose that no $V_{\lambda}=V$. Then each $V_{\lambda}$ has strictly smaller dimension than $V$, and so we can apply the inductive hypothesis to the pair of operators $\left.A\right|_{V_{\lambda}},\left.B\right|_{V_{\lambda}}$ on $V_{\lambda}$. This yields orthonormal simultaneous eigenbases on each $V_{\lambda}$ which may be concatenated as above.

## 4 Lisha Li

There are 20 people in a room, each with either a blue or red hat on their head. Each person can clearly see the hat on everyone elses head, but cannot see their own. In fact 8 people have blue hats and 12 have red. The game is played in rounds, and in each round the people who know the color of their hats raise their hands. The game proceeds this way an exhausting number of rounds and no one raises their hands.

Then a child wanders into the room and exclaims a blue hat! Eight rounds later all eight people with blue hats raise their hands.

1. Explain why this happened. i.e. show that if there were k blue hats all k people would raise their hands in the k-th round.
2. What do you expect to happen in the 9th round?
3. Everyone in the room already knew that there was at least one person had a blue hat, since everyone could see at least seven blue hats. Then why did the childs exclamation have any effect?

## Solution:

1. Proof by induction. Base case: Suppose $\mathrm{k}=1$. The person with the blue hat sees only red hats, and is not sure if there is a blue hat $(k=1)$ or not $(k=0)$. With knowledge that a blue hat exists, the sole blue hat knows that $\mathrm{k}=1$ and raises their hand.

Suppose that for $\mathrm{k}=\mathrm{n}$, n people raise their hand on the nth round. Consider the case for $\mathrm{k}=\mathrm{n}+1$. Each person with a blue hat sees n blue hats, and must gure out if there are n blue hats or $\mathrm{n}+1$ blue hats. Assuming themselves to have red hats, they watch a game which should have $\mathrm{k}=\mathrm{n}$ blue hats. After n rounds, when n players dont raise their hands, by the inductive hypothesis, this player knows this is a game with $n+1$ blue hats, and raises their hand the next round. This holds for every player with a blue hat, and so all raise their hands at the same time.

Therefore, after k rounds, k players raise their hand, for k 1 .
2. In the 9th round, the remaining players raise their hand, knowing they have red hats. As they saw 8 blue hats, they had been thinking either there are 8 blue hats, or I am wearing a blue hat!. Knowing there to be 8 blue hats induces knowledge that this player is wearing a red hat.
3. The issue here is common knowledge: $A, B$ have knowledge about fact $F$ if $A$ knows $F, A$ knows that $B$ knows $F, A$ knows that $B$ knows that $A$ knows $F$, ... To see why common knowledge is relevant, consider the case where there are exactly 3 blue hats on $A, B, C$. $A$ knows that $B$ and $C$ have blue hats. $A$ even knows that $B$ knows that $C$ has a blue hat and vice versa. But $A$ does not know that $B$ knows that $C$ has a blue hat. This is because $A$ does not know that she has a blue hat, since she only sees 2 blue hats. So now she has no way of reasoning that if there were only two blue hats then $B$ and $C$ would raise their hands on the second round - since as far as she knows $B$ doesnt know that $C$ knows that he has a blue hat and $C$ doesnt know that $B$ knows that she has a blue hat. So the induction does not work.

When the child says there is a blue hat, it becomes common knowledge that there is a blue hat. i.e. $A$ knows that $B$ knows that $C$ knows that ... that $A$ knows that there is at least one blue hat. Now the induction can go through.


[^0]:    ${ }^{1}$ where in general, $\prod_{i=1}^{n} a_{i i}$ is defined to be $a_{11} \cdots a_{n n}$

[^1]:    ${ }^{2}$ For this, we'll use the definition $\operatorname{det}(A)=\sum_{\sigma \in S_{n}} \operatorname{sign}(\sigma) a_{\sigma(1) 1} \cdots a_{\sigma(n) n}$ given on page 229. $S_{n}$ is just the set of permutations/bijective functions from $\{1, \cdots, n\}$ to itself.

[^2]:    ${ }^{4}$ unless $V=\{0\}$, but don't worry about this case

[^3]:    ${ }^{5}$ You can obtain this guess if you draw the unit ball in $\mathbb{R}^{3}$ and the ellipsoid $E$, and 'match' the principal axes

