Department of Mathematics, University of Toronto
MAT224H1F - Linear Algebra II
Fall 2013

Problem Set 1 Solutions

1. (a) Find the number $x \in \{0,1,2,3,4,5,6\}$ such that $x = 3^{-1}$ in $\mathbb{Z}_7$.

   (b) Express the complex number $\frac{(2i+1)(i^3+i+1)}{1-i}$ in the form $a+bi$, with $a, b \in \mathbb{R}$.

Solution.

(a) By definition of multiplicative inverses, the x we are looking for satisfies $3x = 1$ in $\mathbb{Z}_7$. We know from class that $\mathbb{Z}_7$ is a field, so exactly one such x exists. The easiest way to find it is to start multiplying 3 by each element of $\{0,1,2,3,4,5,6\}$ until we find one that works. All the computations are done mod 7:

$$\begin{aligned} 3*0 &= 0 \neq 1 \\ 3*1 &= 3 \neq 1 \\ 3*2 &= 6 \neq 1 \\ 3*3 &= 9 = 2 \neq 1 \\ 3*4 &= 12 = 5 \neq 1 \\ 3*5 &= 15 = 1 \end{aligned}$$

So $5 = 3^{-1}$ in $\mathbb{Z}_7$.

(b) Start by simplifying the numerator. Note that $i^3 = i^2 \cdot i = (-1) \cdot i = -i$.

$$(2i+1)(i^3+i+1) = (2i+1)(-i+i+1) = 2i+1.$$

The easiest way to simplify a fraction in $\mathbb{C}$ is to multiply the numerator and denominator by the conjugate of the denominator, then simplify, remembering that $i^2 = -1$.

$$\begin{aligned} \frac{(2i+1)(i^3+i+1)}{1-i} &= \frac{2i+1}{1-i} \\ &= \frac{2i+1}{1-i}\left(\frac{1+i}{1+i}\right) \\ &= \frac{2i+1+2i^2+i}{1-i+i-i^2} \\ &= \frac{-1+3i}{2} \\ &= \frac{-1}{2} + \frac{3}{2}i \end{aligned}$$

2. Recall that if p is a prime, then for any n, $\mathbb{Z}_p^n = \{ (x_1, \ldots, x_n) : x_1, \ldots, x_n \in \mathbb{Z}_p \}$ is a vector space over $\mathbb{Z}_p$ with pointwise addition and scalar multiplication mod p.

   (a) Consider the subspace $S = \operatorname{span}\{ (1,1,1), (2,3,4) \}$ of $\mathbb{Z}_5^3$. Does the vector $(0,1,0)$ belong to S? Does the vector $(3,1,4)$ belong to S?

   (b) Find a basis for the subspace $S = \operatorname{span}\{ (2,1,0,2), (1,0,1,4), (0,1,3,4) \}$ of $\mathbb{Z}_5^4$.

Solution.

(a) The vector $(0,1,0)$ is in S if and only if we can find $a, b \in \mathbb{Z}_5$ such that $a(1,1,1) + b(2,3,4) = (0,1,0)$, with the computations done mod 5. This equation is an abbreviated way of writing a system of three equations in the unknowns a, b:

$$\begin{aligned} a + 2b &= 0 \\ a + 3b &= 1 \\ a + 4b &= 0 \end{aligned}$$

Any of the usual methods for solving such a system will work, as long as we remember to make the computations mod 5. We use an augmented matrix and row-reduce:

$$\begin{bmatrix} 1 & 2 & | & 0 \\ 1 & 3 & | & 1 \\ 1 & 4 & | & 0 \end{bmatrix} \to \begin{bmatrix} 1 & 2 & | & 0 \\ 0 & 1 & | & 1 \\ 0 & 2 & | & 0 \end{bmatrix}.$$

From this partially row-reduced form we see that we must have $2b = 0$ and $b = 1$. There is no $b \in \mathbb{Z}_5$ satisfying both of these equations, so $(0,1,0) \notin S$.

For the vector $(3,1,4)$, we repeat the above process of forming an augmented matrix and row-reducing:

$$\begin{aligned} \begin{bmatrix} 1 & 2 & | & 3 \\ 1 & 3 & | & 1 \\ 1 & 4 & | & 4 \end{bmatrix} &\to \begin{bmatrix} 1 & 2 & | & 3 \\ 0 & 1 & | & -2 \\ 0 & 2 & | & 1 \end{bmatrix} \\ &\to \begin{bmatrix} 1 & 0 & | & 2 \\ 0 & 1 & | & -2 \\ 0 & 1 & | & 2^{-1} \end{bmatrix} \end{aligned}$$

From this row-reduced matrix we see that there is a solution if and only if $-2 = 2^{-1}$ in $\mathbb{Z}_5$. Calculating mod 5, we have $-2 = 3$, and $3 \cdot 2 = 6 = 1$, so $3 = 2^{-1}$. Thus $(2,3)$ is a solution to our system of equations, and $(3,1,4) = 2(1,1,1) + 3(2,3,4) \in S$.

(b) In MAT223 you saw how to solve a problem like this over the field $\mathbb{R}$, and the same technique works here - we just need to remember to calculate mod 5. We form a matrix whose columns are the vectors in the given spanning set, then we row-reduce. The columns of the original matrix corresponding to the columns of the row-reduced matrix with leading 1's will form a basis for S.

$$\begin{bmatrix} 2 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 3 \\ 2 & 4 & 4 \end{bmatrix} \to \begin{bmatrix} 0 & 1 & -2 \\ 1 & 0 & 1 \\ 0 & 1 & 3 \\ 0 & 4 & 2 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 1 & 3 \\ 1 & 0 & 1 \\ 0 & 1 & 3 \\ 0 & 4 & 2 \end{bmatrix}$$

$$\to \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 3 \\ 0 & 2 & 1 \\ 0 & 0 & 0 \end{bmatrix}$$

$$\to \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 3 \\ 0 & 0 & -5 \\ 0 & 0 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 3 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

We see that the first two columns have leading 1's, so a basis for S is $\{ (2,1,0,2), (1,0,1,4) \}$.

3. (a) Consider the subspace $S = \operatorname{span}\{(1,2,3,4),(4,5,6,2),(2,5,1,1),(0,4,1,0)\}$ of $\mathbb{Z}_7^4$. Find the dimension of S.

   (b) Consider the subspace $S = \operatorname{span}\{(i,0,1),(1,i,-1),(i,i-1,-1)\}$ of $\mathbb{C}^3$. Find the dimension of S.

Solution.

Recall from MAT223 that to solve questions of this kind over $\mathbb{R}$, we can put the given spanning vectors as the columns of a matrix and row-reduce. The number of columns with leading 1's will be the dimension of the subspace S. The same technique works here, except that now we do our calculations in other fields ($\mathbb{Z}_7$ for part (a), $\mathbb{C}$ for part (b)).

(a) We follow the description above, remembering as we row-reduce that all calculations are done in $\mathbb{Z}_7$.

$$\begin{bmatrix}1&4&2&0\\2&5&5&4\\3&6&1&1\\4&2&1&0\end{bmatrix} \to \begin{bmatrix}1&4&2&0\\7&25&15&4\\7&22&9&1\\7&14&7&0\end{bmatrix}$$
$$= \begin{bmatrix}1&4&2&0\\0&4&1&4\\0&1&2&1\\0&0&0&0\end{bmatrix}$$
$$\to \begin{bmatrix}1&4&2&0\\0&4&1&4\\0&4&8&4\\0&0&0&0\end{bmatrix}$$
$$= \begin{bmatrix}1&4&2&0\\0&4&1&4\\0&4&1&4\\0&0&0&0\end{bmatrix}$$
$$\to \begin{bmatrix}1&4&2&0\\0&8&2&8\\0&0&0&0\\0&0&0&0\end{bmatrix}$$
$$= \begin{bmatrix}1&4&2&0\\0&1&2&1\\0&0&0&0\\0&0&0&0\end{bmatrix}$$

We see that there are two leading 1's, so $\dim(S) = 2$.

(b) We again follow the description from above, this time doing the row-reduction calculations in $\mathbb{C}$.

$$\begin{bmatrix}i&1&i\\0&i&i-1\\1&-1&-1\end{bmatrix} \to \begin{bmatrix}-1&i&-1\\0&1&1+i\\1&-1&-1\end{bmatrix}$$
$$\to \begin{bmatrix}-1&i&-1\\0&1&i+1\\0&i-1&-2\end{bmatrix}$$
$$\to \begin{bmatrix}1&-i&1\\0&1&i+1\\0&0&0\end{bmatrix}$$

Here the last line was obtained by subtracting $(i-1)$ times the second row from the third row. We see that there are two leading 1's, so $\dim(S) = 2$.

4. Let $T : P_2(\mathbb{C}) \to P_3(\mathbb{C})$ be defined by $T(p(x)) = (x+i)(p(x+i))$.

   (a) Show that T is linear.

   (b) Let $\alpha = \left\{ 1, x, x^2 \right\}$ and $\beta = \left\{ 1, x, x^2, x^3 \right\}$ be bases for $P_2(\mathbb{C})$ and $P_3(\mathbb{C})$, respectively. Compute $[T]_\alpha^\beta$.

   (c) Find a basis for $\operatorname{im}(T)$ and find a basis for $\ker(T)$.

Solution.

(a) Let $p(x) = a_2x^2 + a_1x + a_0$, and $q(x) = b_2x^2 + b_1x + b_0$, and let $r, s \in \mathbb{C}$. As we saw in class, it suffices to check

$$T(rp(x) + sq(x)) = rT(p(x)) + sT(q(x)).$$

We compute:

$$\begin{aligned}
T(rp(x) + sq(x)) &= T((ra_2 + sb_2)x^2 + (ra_1 + sb_1)x + (ra_0 + sb_0)) \\
&= (x+i)\left((ra_2 + sb_2)(x+i)^2 + (ra_1 + sb_1)(x+i) + (ra_0 + sb_0)\right) \\
&= (x+i)\left(ra_2(x+i)^2 + ra_1(x+i) + ra_0 + sb_2(x+i)^2 + sb_1(x+i) + sb_0\right) \\
&= r(x+i)(a_2(x+i)^2 + a_1(x+i) + a_0) + s(x+i)(b_2(x+i)^2 + b_1(x+i) + b_0) \\
&= rT(a_2x^2 + a_1x + a_0) + sT(b_2x^2 + b_1x + b_0) \\
&= rT(p(x)) + sT(q(x))
\end{aligned}$$

This proves that T is linear.

(b) Recall that the function $1 \in \alpha$ is the function $1(x) = 1$ for all $x \in \mathbb{C}$. We thus have $1(x+i) = 1$ as well. We compute:

$$\begin{aligned}
T(1) &= (x+i)1 \\
&= x + i \\
&= i \cdot 1 + 1 \cdot x + 0 \cdot x^2 + 0 \cdot x^3 \\
T(x) &= (x+i)(x+i) \\
&= (x+i)^2 \\
&= x^2 + 2ix + i^2 \\
&= (-1) \cdot 1 + (2i) \cdot x + 1 \cdot x^2 + 0 \cdot x^3 \\
T(x^2) &= (x+i)(x+i)^2 \\
&= (x+i)^3 \\
&= x^3 + 2ix^2 - x + ix^2 + 2i^2x - i \\
&= (-i) \cdot 1 + (-3) \cdot x + (3i) \cdot x^2 + 1 \cdot x^3
\end{aligned}$$

We have expressed each $T(v)$, for $v \in \alpha$, in terms of the basis β. The coefficients then give us the columns of $[T]_\alpha^\beta$. Remember that the order matters, so the first entry of the first column will be the coefficient of 1 in $T(1)$. We thus have:

$$[T]_\alpha^\beta = \begin{bmatrix} i & -1 & -i \\ 1 & 2i & -3 \\ 0 & 1 & 3i \\ 0 & 0 & 1 \end{bmatrix}.$$

(c) Starting from $[T]_\alpha^\beta$, we row-reduce:

$$\begin{bmatrix} i & -1 & -i \\ 1 & 2i & -3 \\ 0 & 1 & 3i \\ 0 & 0 & 1 \end{bmatrix} \to \begin{bmatrix} i & -1 & 0 \\ 1 & 2i & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\to \begin{bmatrix} i & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\to \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

From this we see that all three columns have leading 1's. This tells us that the columns of the original matrix form a basis for $\operatorname{im}([T]_\alpha^\beta)$. We know from class that the vectors in $P_3(\mathbb{C})$ whose coordinates with respect to β are the columns of $[T]_\alpha^\beta$ then form a basis for $\operatorname{im}(T)$. That is, a basis for $\operatorname{im}(T)$ is:

$$\left\{ x + i, x^2 + 2i - 1, x^3 + 3ix^2 - 3x - i \right\}.$$

We also see from the row-reduced matrix that the null space of $[T]_\alpha^\beta$ is trivial. As we saw in class, this means that $\ker(T) = \{ 0 \}$ as well. This means that $\ker(T)$ has dimension 0; a basis for $\ker(T)$ is therefore $\emptyset$, the set with no elements.

5. Let $T : \mathbb{R}^2 \to \mathbb{R}^3$ be the linear transformation whose matrix with respect to the bases $\alpha = \{ (1,1), (1,-1) \}$ of $\mathbb{R}^2$ and $\beta = \{ (1,0,1), (2,2,0), (0,-1,1) \}$ of $\mathbb{R}^3$ is:

$$[T]_\alpha^\beta = \begin{bmatrix} 1 & 1 \\ 0 & -1 \\ 4 & 2 \end{bmatrix}.$$

Find $T(x,y)$ for all $(x,y) \in \mathbb{R}^2$.

Solution.

For any $(x,y) \in \mathbb{R}^2$, we can write $[(x,y)]_\alpha = (a,b)$, where $(x,y) = a(1,1) + b(1,-1)$. To find a, b we solve the system of equations $x = a+b$, $y = a-b$ to find $a = \frac{x+y}{2}$ and $b = \frac{x-y}{2}$. We then have

$$\begin{aligned} [T(x,y)]_\beta &= [T]_\alpha^\beta [(x,y)]_\alpha \\ &= \begin{bmatrix} 1 & 1 \\ 0 & -1 \\ 4 & 2 \end{bmatrix} \begin{bmatrix} \frac{x+y}{2} \\ \frac{x-y}{2} \end{bmatrix} \\ &= \left(\frac{x+y}{2} + \frac{x-y}{2}, -\frac{x-y}{2}, 4\frac{x+y}{2} + 2\frac{x-y}{2} \right) \\ &= \left(x, \frac{y-x}{2}, 3x+y \right) \end{aligned}$$

Thus for any $(x,y) \in \mathbb{R}^2$,

$$\begin{aligned} T(x,y) &= x(1,0,1) + \frac{y-x}{2}(2,2,0) + (3x+y)(0,-1,1) \\ &= (x,0,x) + (y-x, y-x, 0) + (0, -3x-y, 3x+y) \\ &= (y, -4x-2y, 4x+y) \end{aligned}$$

6. Let $T : \mathbb{R}^3 \to \mathbb{R}^3$ be defined by

$$T(x, y, z) = (2x - y - z, x + 3y + 2z, y)$$

Find $[T]_\alpha^\beta$, where $\alpha = \{ (0,1,1), (1,1,0), (1,0,1) \}$ and $\beta = \{ (2,-1,1), (1,1,1), (0,0,1) \}$.

Solution.

We first find the first column, which will be the sequence of numbers v such that $[T(0,1,1)]_\beta = v$. Straightforward computation gives

$$T(0,1,1) = (-2,5,1).$$

We need to write $(-2,5,1) = a(2,-1,1) + b(1,1,1) + c(0,0,1)$. This gives a system of equations:

$$\begin{aligned} 2a + b &= -2 \\ -a + b &= 5 \\ a + b + c &= 1 \end{aligned}$$

Solving this system of equations, we obtain $a = -\frac{7}{3}, b = \frac{8}{3}, c = \frac{2}{3}$. The first column of $[T]_\alpha^\beta$ will therefore be $\begin{bmatrix} -\frac{7}{3} \\ \frac{8}{3} \\ \frac{2}{3} \end{bmatrix}$.

Next, we have $T(1,1,0) = (1,4,1)$, and solving $(1,4,1) = a(2,-1,1) + b(1,1,1) + c(0,0,1)$ gives $a = -1, b = 3, c = -1$.

Finally, $T(1,0,1) = (1,3,0)$, and solving $(1,3,0) = a(2,-1,1) + b(1,1,1) + c(0,0,1)$ gives $a = -\frac{2}{3}, b = \frac{7}{3}, c = -\frac{5}{3}$.

Therefore, the matrix $[T]_\alpha^\beta$ is

$$[T]_\alpha^\beta = \begin{bmatrix} -\frac{7}{3} & -1 & -\frac{2}{3} \\ \frac{8}{3} & 3 & \frac{7}{3} \\ \frac{2}{3} & -1 & -\frac{5}{3} \end{bmatrix}.$$

7. (a) Prove that $\mathbb{Z}_{10}$ (with the operations of addition and multiplication modulo 10) is not a field. *Hint:* Find a non-zero element of $\mathbb{Z}_{10}$ which does not have a multiplicative inverse.

   (b) Prove that if $n \in \mathbb{N}$ is not prime, then $\mathbb{Z}_n$ is not a field. *Hint:* Write $n = k \cdot m$, where $k, m > 1$ and $k, m < n$. The element $k \in Z_n$ is non-zero - show that it does not have a multiplicative inverse by considering the meaning of the equation $k \cdot a = 1$ in $\mathbb{Z}_n$.

Solution.

(a) We will show that $2 \in \mathbb{Z}_{10}$ does not have a multiplicative inverse. We know that $2 \neq 0$ in $\mathbb{Z}_{10}$, so this will suffice to show that $\mathbb{Z}_{10}$ is not a field. The easiest way to prove there is no inverse for 2 is to simply compute $2 \cdot x \pmod{10}$ for each $x \in \{0, 1, \ldots, 9\}$, and see that we never get the value 1.

$$\begin{aligned}
2 \cdot 0 &= 0 \neq 1 \\
2 \cdot 1 &= 2 \neq 1 \\
2 \cdot 2 &= 4 \neq 1 \\
2 \cdot 3 &= 6 \neq 1 \\
2 \cdot 4 &= 8 \neq 1 \\
2 \cdot 5 = 10 &= 0 \neq 1 \\
2 \cdot 6 = 12 &= 2 \neq 1 \\
2 \cdot 7 = 14 &= 4 \neq 1 \\
2 \cdot 8 = 16 &= 6 \neq 1 \\
2 \cdot 9 = 18 &= 8 \neq 1
\end{aligned}$$

An alternate solution would be to solve part (b) first, then observe that $10 = 2 \cdot 5$ is not prime.

(b) As suggested by the hint, use the fact that n is not prime to write $n = k \cdot m$, where $k, m > 1$. Notice that the conditions on k, m imply that $0 < k < n$, so k is not 0 in $\mathbb{Z}_n$. Suppose for a contradiction that k has a multiplicative inverse in $\mathbb{Z}_n$. Then there is some $a \in \{0, 1, \ldots, n-1\}$ such that $a \cdot k = 1$ in $\mathbb{Z}_n$. By definition, this equation means that there is some $l \in \mathbb{Z}$ such that $a \cdot k = 1 + l \cdot n$. Rearranging this equation, we get:

$$a \cdot k - l \cdot n = 1.$$

Again using that $n = k \cdot m$, we have:

$$a \cdot k - l \cdot k \cdot m = 1.$$

So

$$k(a - l \cdot m) = 1.$$

Here $a, l, n \in \mathbb{Z}$, so $a - l \cdot m \in \mathbb{Z}$ as well. This equation says that there is some integer r such that $k \cdot r = 1$. We chose $k > 1$, so this is impossible. Therefore k is a non-zero element of $\mathbb{Z}_n$ without a multiplicative inverse, so $\mathbb{Z}_n$ is not a field.

8. Let $T : M_{2\times2}(\mathbb{R}) \to M_{2\times2}(\mathbb{R})$ be defined by

$$T(A) = A - A^t.$$

(Recall that A^t is the transpose of A). Find the dimension of $\ker(T)$ and the dimension of $\operatorname{im}(T)$. You may assume without proof that T is linear.

Solution.

Let $\alpha = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \right\}$. This α is a basis for $M_{2\times2}(\mathbb{R})$, as you saw in MAT223. We compute:

$$\begin{aligned}
T\left(\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\right) &= \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \\
T\left(\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\right) &= \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = 1 \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} + (-1) \begin{bmatrix} 0 & 0 \\ -1 & 0 \end{bmatrix} \\
T\left(\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}\right) &= \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = (-1) \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} + 1 \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \\
T\left(\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}\right) &= \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}
\end{aligned}$$

Hence

$$[T]_\alpha^\alpha = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

This matrix row-reduces to

$$\begin{bmatrix} 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

There is one leading 1, so $\dim \operatorname{im}(T) = 1$, and $\dim \ker(T) = 3$.

9. Let V be a vector space over a field F, and let W_1, W_2 be subspaces of V. We say that V is the *direct sum* of W_1 and W_2, and write $V = W_1 \oplus W_2$, if $V = W_1 + W_2$ and $W_1 \cap W_2 = \{0\}$.

   Prove that $V = W_1 \oplus W_2$ if and only if for each $v \in V$ there are unique $w_1 \in W_1$ and $w_2 \in W_2$ such that $v = w_1 + w_2$.

   Solution.

   Assume $V = W_1 \oplus W_2$, and consider any $v \in V$. Part of the definition of $V = W_1 \oplus W_2$ is that $V = W_1 + W_2$, so $v \in W_1 + W_2$, i.e., there exist $w_1 \in W_1$ and $w_2 \in W_2$ such that $v = w_1 + w_2$. This shows existence, but we must still show uniqueness. Suppose that $w_1' \in W_1$ and $w_2' \in W_2$ are such that $v = w_1 + w_2 = w_1' + w_2'$. We must show that $w_1 = w_1'$ and $w_2 = w_2'$. We know that $w_1 + w_2 = w_1' + w_2'$, which we can rearrange as $w_1 - w_1' = w_2' - w_2$. Now W_1 is a subspace of V, and $w_1, w_1' \in W_1$, so $w_1 - w_1' \in W_1$. Similarly, $w_2' - w_2 \in W_2$, which is the same as saying $w_1 - w_1' \in W_2$. So $w_1 - w_1' \in W_1 \cap W_2$. By definition of $V = W_1 \oplus W_2$, we have $W_1 \cap W_2 = \{0\}$, so $w_1 - w_1' = 0$. That is, $w_1 = w_1'$. We already had $w_1 - w_1' = w_2' - w_2$, and we now know $w_1 - w_1' = 0$, so $w_2' - w_2 = 0$, and hence $w_2' = w_2$ as well. This proves uniqueness.

   Now assume that for each $v \in V$ there are unique $w_1 \in W_1$ and $w_2 \in W_2$ such that $v = w_1 + w_2$. Given any $v \in V$ we thus have $v \in W_1 + W_2$, so $V \subseteq W_1 + W_2$. The reverse containment is always true, so we conclude $V = W_1 + W_2$. We still need to show that $W_1 \cap W_2 = \{0\}$. Suppose that $v \in W_1 \cap W_2$. Let $w_1 = v$, and $w_2 = 0$. Then $w_1 \in W_1, w_2 \in W_2$, and $v = w_1 + w_2$. Let $w_1' = 0$ and $w_2' = v$. Then again, $w_1' \in W_1, w_2' \in W_2$, and $v = w_1' + w_2'$. By hypothesis there is a *unique* way of writing v as a sum of a vector in W_1 and a vector in W_2, so we must have $w_1 = w_1'$ and $w_2 = w_2'$. That is, $v = w_1 = w_1' = 0$, so $v = 0$. This proves that $W_1 \cap W_2 = \{0\}$, so $V = W_1 \oplus W_2$.