MATH1050 Examples of proofs of statements with conclusion '... iff ...'

1. Consider the pair of statements (†), (‡) of the form below:

   (†) '*Let/suppose blih-blih-blih. Suppose blah-blah-blah. Then bleh-bleh-bleh.*'

   (‡) '*Let/suppose blih-blih-blih. Suppose bleh-bleh-bleh. Then blah-blah-blah.*'

   When want to state that both of (†), (‡) are to hold simultaneously, we may combine them into one statement of the form

   - '*Let/suppose blih-blih-blih. blah-blah-blah iff bleh-bleh-bleh.*'

   When one or both of '*blah-blah-blah*', '*bleh-bleh-bleh*' is very lengthy, we may write in this way:

   - '*Let/suppose blih-blih-blih. The following statements are logically equivalent:*
     (1) *Blah-blah-blah.*
     (2) *Bleh-bleh-bleh.*'

   The safest way for proving such a statement is to return to its original meaning: prove (†), (‡) separately.

   Below are some illustrations on the general format of proofs for such statements.

2. **Statement (a).**

   Suppose x, y are positive real numbers. Then $\dfrac{x+y}{2} = \sqrt{xy}$ iff $x = y$.

   Proof of Statement (a).

   Suppose x, y are positive real numbers. (Then $\sqrt{x}$, $\sqrt{y}$, $\sqrt{xy}$, $\sqrt{x} - \sqrt{y}$ are well-defined as real numbers.)

   - ['$\Leftarrow$-part'.]
     Suppose $x = y$.
     Then $\dfrac{x+y}{2} = \dfrac{2x}{2} = x$.
     Since x is positive, $\sqrt{x^2} = x$. Then $\sqrt{xy} = \sqrt{x^2} = x$.
     Hence $\dfrac{x+y}{2} = x = \sqrt{xy}$.
   - ['$\Rightarrow$-part'.]
     Suppose $\dfrac{x+y}{2} = \sqrt{xy}$.
     Since x, y are positive, we have $(\sqrt{x})^2 = x$ and $(\sqrt{y})^2 = y$. Also, $\sqrt{xy} = \sqrt{x}\sqrt{y}$.
     Then $(\sqrt{x})^2 + (\sqrt{y})^2 = x + y = 2\sqrt{xy} = 2\sqrt{x}\sqrt{y}$.
     Therefore $(\sqrt{x} - \sqrt{y})^2 = (\sqrt{x})^2 + (\sqrt{y})^2 - 2\sqrt{x}\sqrt{y} = 0$.
     Hence $\sqrt{x} - \sqrt{y} = 0$.
     Now we have $\sqrt{x} = \sqrt{y}$. Therefore $x = (\sqrt{x})^2 = (\sqrt{y})^2 = y$.

3. **Statement (b).**

   Let $\mathbf{x}$, $\mathbf{y}$ be non-zero vectors in the real n-dimensional space. The following statements are logically equivalent:
   (1) *There exist some real numbers κ, λ, not both zero, such that $\kappa\mathbf{x} + \lambda\mathbf{y} = \mathbf{0}$.*
   (2) $|\langle \mathbf{x}, \mathbf{y} \rangle| = \|\mathbf{x}\| \cdot \|\mathbf{y}\|$.

   Remark. $\langle \mathbf{x}, \mathbf{y} \rangle$ is the dot product of the vectors $\mathbf{x}$, $\mathbf{y}$. $\|\mathbf{x}\|$, $\|\mathbf{y}\|$ are the respective norms of the vectors $\mathbf{x}$, $\mathbf{y}$.

   Proof of Statement (b).

   Let $\mathbf{x}$, $\mathbf{y}$ be vectors in the real n-dimensional space.

   - ['(1)$\Rightarrow$(2)'?]
     Suppose there exist some real numbers κ, λ, not both zero, such that $\kappa\mathbf{x} + \lambda\mathbf{y} = \mathbf{0}$.
     Without loss of generality, suppose $\lambda \neq 0$. Then $\mathbf{y} = -\dfrac{\kappa}{\lambda}\mathbf{x}$. We have

     $$|\langle \mathbf{x}, \mathbf{y} \rangle| = |\langle \mathbf{x}, -\frac{\kappa}{\lambda}\mathbf{x} \rangle| = |-\frac{\kappa}{\lambda}\langle \mathbf{x}, \mathbf{x} \rangle| = \left|-\frac{\kappa}{\lambda}\right| \|\mathbf{x}\|^2 = \|\mathbf{x}\| \cdot \|-\frac{\kappa}{\lambda}\mathbf{x}\| = \|\mathbf{x}\| \cdot \|\mathbf{y}\|$$

   - ['(2)$\Rightarrow$(1)'?]
     Suppose $|\langle \mathbf{x}, \mathbf{y} \rangle| = \|\mathbf{x}\| \cdot \|\mathbf{y}\|$. Then $\langle \mathbf{x}, \mathbf{y} \rangle = \|\mathbf{x}\| \cdot \|\mathbf{y}\|$ or $\langle \mathbf{x}, \mathbf{y} \rangle = -\|\mathbf{x}\| \cdot \|\mathbf{y}\|$.

* (Case 1). Suppose $\langle \mathbf{x}, \mathbf{y} \rangle = \|\mathbf{x}\| \cdot \|\mathbf{y}\|$.
  Define $\kappa = \|\mathbf{y}\|$, $\lambda = -\|\mathbf{x}\|$. Since $\mathbf{x}$, $\mathbf{y}$ are non-zero vectors, κ, λ are non-zero real numbers.

$$\begin{array}{rcl} \|\kappa\mathbf{x} + \lambda\mathbf{y}\|^2 & = & \langle \kappa\mathbf{x} + \lambda\mathbf{y}, \kappa\mathbf{x} + \lambda\mathbf{y} \rangle \\ & = & \kappa^2 \langle \mathbf{x}, \mathbf{x} \rangle + \kappa\lambda \langle \mathbf{x}, \mathbf{y} \rangle + \lambda\kappa \langle \mathbf{y}, \mathbf{x} \rangle + \lambda^2 \langle \mathbf{y}, \mathbf{y} \rangle \\ & = & \kappa^2 \|\mathbf{x}\|^2 + 2\kappa\lambda \langle \mathbf{x}, \mathbf{y} \rangle + \lambda^2 \|\mathbf{y}\|^2 \\ & = & \kappa^2\lambda^2 + 2\kappa\lambda \|\mathbf{x}\| \cdot \|\mathbf{y}\| + \kappa^2\mu^2 \\ & = & \kappa^2\lambda^2 - 2\kappa^2\lambda^2 + \kappa^2\lambda^2 \\ & = & 0 \end{array}$$

  Then $\|\kappa\mathbf{x} + \lambda\mathbf{y}\| = 0$. Therefore $\kappa\mathbf{x} + \lambda\mathbf{y} = \mathbf{0}$.
* (Case 2). Suppose $\langle \mathbf{x}, \mathbf{y} \rangle = -\|\mathbf{x}\| \cdot \|\mathbf{y}\|$.
  Define $\kappa = \|\mathbf{y}\|$, $\lambda = \|\mathbf{x}\|$.
  Modifying the arguments in (Case 1), we also deduce that $\kappa\mathbf{x} + \lambda\mathbf{y} = \mathbf{0}$.

4. Here are some other examples of such statements in school mathematics.
   (α) *Let $\triangle ABC$ be a triangle. $\angle ACB$ is a right angle iff $AB^2 = AC^2 + BC^2$.*
   Remark. In this statement we have combined the two true statements known as **Pythagoras' Theorem** and the **Converse of Pythagoras' Theorem**.
   (β) *Let $\triangle ABC$ be a triangle.*
   $\angle ACB$ is a right angle iff AB passes through the centre of the circumcircle of $\triangle ABC$.
   (γ) *Let $f(z)$ be a polynomial with real/complex coefficients and indeterminate z, and c be a real/complex number. The polynomial $z - c$ is a factor of the polynomial $f(z)$ iff $f(c) = 0$.*
   Remark. Incorporated in this statement is the result known as the **Factor Theorem**.
   (δ) *Let $\{a_n\}_{n=0}^{\infty}$ be an infinite sequence of complex numbers. The statements below are logically equivalent:*
   (1) *$\{a_n\}_{n=0}^{\infty}$ is an arithmetic progression. (There exists some complex number d such that for any $n \in \mathbb{N}$, $a_n = a_0 + nd$.)*
   (2) *For any $n \in \mathbb{N}$, $a_{n+1} = \dfrac{a_n + a_{n+2}}{2}$.*

5. Many results in your *linear algebra* course are statements of this form. Here are some examples.
   (α) *Let $\mathbf{u}_1, \mathbf{u}_2, \cdots, \mathbf{u}_n \in \mathbb{R}^m$. The statements below are logically equivalent:*
   (1) *$\mathbf{u}_1, \mathbf{u}_2, \cdots, \mathbf{u}_n$ are linearly dependent.*
   (2) *One of $\mathbf{u}_1, \mathbf{u}_2, \cdots, \mathbf{u}_n$ is a linear combination of the others.*
   (β) *Let A be an $(n \times n)$-square matrix with real entries. The statements below are logically equivalent:*
   (1) *A is non-singular. (The zerovector is the only element of the null space of A.)*
   (2) *A is row-equivalent to the identity matrix I_n.*
   (3) *A is invertible.*
   (4) *For any $\mathbf{b} \in \mathbb{R}^n$, the system $A\mathbf{x} = \mathbf{b}$ has a unique solution.*
   (5) *The columns of A constitute a basis for $\mathbb{R}^n$.*
   (6) $\det(A) \neq 0$.

   Watch out how these results are proved in your *linear algebra* course.