Linear Algebra Quiz - 1
Course Instructor : Prof. R. Vittal Rao
Date : 28 August, 2010 **Duration** : 12:00 pm - 12:20 pm

1. Find all solutions to the equation

$$x^2 - 10x + 16 = 0$$

in (i) $\mathbb{F}_2$ (ii) $\mathbb{F}_5$ (iii) $\mathbb{F}_8$

Solution:

$$x^2 - 10x + 16 = 0$$
$$x^2 - 8x - 2x + 16 = 0$$
$$(x-2)(x-8) = 0$$
$$\text{In } \mathbb{F}_2 \Rightarrow x.x = 0$$
$$x = 0 \text{ is the solution}$$
$$\text{In } \mathbb{F}_5 \Rightarrow x^2 + 1 = 0$$
$$\text{It can be verified that } x = 2 \text{ and } x = 3 \text{ are solutions}$$
$$\text{In } \mathbb{F}_8 \Rightarrow x^2 - 2x = 0$$
$$\text{It can be verified that } x = 0, x = 2, x = 4 \text{ and } x = 6 \text{ are solutions}$$

2. Let K be a set of numbers. Let $K(\sqrt{3})$ be the set of all real numbers of the form $\alpha + \beta\sqrt{3}$, where $\alpha, \beta \in K$.
   (a) Is $K(\sqrt{3})$ a field when $K = \mathbb{Z}$?
   (b) Is $K(\sqrt{3})$ a field when $K = \mathbb{N}$?
   (c) Give an example of a set K so that $K(\sqrt{3})$ becomes a field.

   Solution:

   (a) No.
   Observe that the additive identity is $0 = (0)+(0)\sqrt{3}$ and the multiplicative identity is $1 = (1) + (0)\sqrt{3}$. In a field, the multiplicative inverse exists for all non-zero elements. Suppose this is true, and $\mathbb{Z}(\sqrt{3})$ is a field. Then, for every non-zero $a + b\sqrt{3}$, there exists $c + d\sqrt{3}$ such that

$$(a + b\sqrt{3})(c + d\sqrt{3}) = 1$$
$$c + d\sqrt{3} = \frac{1}{a + b\sqrt{3}}$$
$$= \frac{a - b\sqrt{3}}{a^2 - 3b^2}$$
$$= \left(\frac{a}{a^2 - 3b^2}\right) + \left(\frac{b}{a^2 - 3b^2}\right)\sqrt{3}$$
$$\Rightarrow c = \frac{a}{a^2 - 3b^2} \ , \ d = \frac{b}{a^2 - 3b^2} \qquad (1)$$

For $a = b = 1$, we see that $c = d = -1/2 \notin \mathbb{Z}$. This violates the closure law for fields. Hence $\mathbb{Z}(\sqrt{3})$ is not a field

(b) No.
It is easy to see that the additive inverse of an element does not exist in $\mathbb{N}(\sqrt{3})$.

(c) Example 1: $\mathbb{R}$, $\mathbb{C}$
Notice that $\mathbb{R}(\sqrt{3}) = \mathbb{R}$. It is easy to show that $\mathbb{R}$ is a field. The same applies to $\mathbb{C}$.

Example 2: $\mathbb{Q}$
The basic laws for addition, multiplication and distributivity can be easily verified.
We need to show that the multiplicative inverse exists for every non-zero element $a+b\sqrt{3}$. In equation (1), we see that $\forall a, b \in \mathbb{Q}$, $\frac{a}{a^2-3b^2}, \frac{b}{a^2-3b^2} \in \mathbb{Q}$. (Note that $\forall a, b \in \mathbb{Q}, a \neq 0$ or $b \neq 0$, we have $a^2 - 3b^2 \neq 0$.) Hence, it follows that the multiplicative inverse exists. It follows that $\mathbb{Q}(\sqrt{3})$ is a field.

Example 3: $\mathbb{F}_p$, where p is a prime number.
$\mathbb{F}_p$ is an integral domain when p is prime. If it can be shown that every non-zero element in $\mathbb{F}_p$ has a multiplicative inverse, then it follows that $\mathbb{F}_p$ is a field. Let $0 \neq a \in \mathbb{F}_p$. Consider $a, a^2, a^3, \ldots$. Since $\mathbb{F}_p$ has finitely many elements, we must have $a^m = a^n$ for some $m < n$. Then $a^m - a^n = 0 = a^m(1 - a^{n-m})$. Since $\mathbb{F}_p$ is an integral domain, $ab = 0 \Rightarrow a = 0$ or $b = 0$. Since $a^m \neq 0$ (why??), we get $1 = a^{n-m} = aa^{n-m-1}$, and we have a multiplicative inverse for a. Thus, it follows that every element in $\mathbb{F}_p$ has a multiplicative inverse, and hence it is a field.
It follows from the above that, whenever $a^2 - 3b^2 \neq 0$, we have $\frac{a}{a^2-3b^2} \in \mathbb{F}_p$ and $\frac{b}{a^2-3b^2} \in \mathbb{F}_p$ and hence every element in $\mathbb{F}_p(\sqrt{3})$ has a multiplicative inverse. Thus, it follows that $\mathbb{F}_p(\sqrt{3})$ is a field. If $a^2 - 3b^2 = 0$, this means $a^2 = 3b^2 \Rightarrow a = \sqrt{3}b \Rightarrow \sqrt{3}$ exists in $\mathbb{F}_p \Rightarrow \mathbb{F}_p(\sqrt{3}) = \mathbb{F}_p$ which we know to be a field.

3. Let $A = \begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix}$

(a) Is A diagonalizable over the field of integers, $\mathbb{Z}$?

(b) Does the answer change if we consider the above matrix over
i)$\mathbb{Q}$, ii) $\mathbb{F}_5$

Solution: Suppose $\exists P$ (invertible) s.t.

$$P^{-1}AP = D = \begin{bmatrix} d_1 & 0 \\ 0 & d_2 \end{bmatrix}$$
$$P^{-1}A^2P = D^2$$
$$\text{We get } A^2 = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = 2I$$
$$\Rightarrow P^{-1}2IP = D^2$$
$$\Rightarrow d_1^2 = 2; d_2^2 = 2$$

It can seen that $d_1, d_2 \notin \mathbb{Z}$ or $\mathbb{Q}$. Hence the matrix A is not diagonalizable over $\mathbb{Z}$ or $\mathbb{Q}$.

In $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$, we cannot find a d_1 such that $d_1^2 = 2$ (Note: Take *modulo* 5 after addition and multiplication operations). Hence the matrix A is not diagonalizable over $\mathbb{F}_5$.

4. Prove that the equation $x^2 = 0$ has a unique solution in $\mathbb{F}_n$, where $n = pq$, p and q are distinct primes.
(Hint: If a prime p divides a product of integers $a \times b$, then p divides a or b, or both)

   Solution: The equation $x^2 = 0$ in $\mathbb{F}_n$ can be re-written as $x^2 \equiv 0(mod\ n)$. Hence, $n|x^2$ (i.e., n divides x^2). Therefore, $pq|x^2 \Rightarrow p|x.x \Rightarrow p|x$ (a property of prime numbers). Similarly, $q|x.x \Rightarrow q|x$.

   So, $x = 0$ is the only integer solution in the range $\{0, 1, ..., n-1\}$ to $x^2 \equiv 0(mod\ n)$.

5. Let $A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$

   (a) Is A diagonalizable over the field of rational numbers, $\mathbb{Q}$?

   (b) Does the answer change if we consider the above matrix over
   i)$\mathbb{R}$, ii) $\mathbb{F}_7$

   Solution: Suppose $\exists P$ (invertible) s.t.

$$P^{-1}AP = D = \begin{bmatrix} d_1 & 0 \\ 0 & d_2 \end{bmatrix}$$
$$P^{-1}A^2P = D^2$$
$$\text{We get } A^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = 2I$$
$$\Rightarrow P^{-1}(-I)P = D^2$$
$$\Rightarrow d_1^2 = -1; d_2^2 = -1$$

It can seen that $d_1, d_2 \notin \mathbb{Q}$ or $\mathbb{R}$ or $\mathbb{F}_7$. Hence the matrix A is not diagonalizable over $\mathbb{Q}$ or $\mathbb{R}$.

In $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$, we cannot find a d_1 such that $d_1^2 = -1(mod\ 7) = 6$ (Note: Take *modulo* 7 after addition and multiplication operations). Hence the matrix A is not diagonalizable over $\mathbb{F}_7$.

6. Find all solutions to the equation

$$x^2 - 7x + 12 = 0$$

in (i) $\mathbb{F}_2$ (ii) $\mathbb{F}_5$ (iii) $\mathbb{F}_6$

Solution:

$$x^2 - 7x + 12 = 0$$
$$\text{In } \mathbb{F}_2 \Rightarrow x^2 - x = 0$$
$$x = 0 \text{ and } x = 1 \text{ are the solutions}$$
$$\text{In } \mathbb{F}_5 \Rightarrow x^2 - 2x + 2 = 0$$
$$\text{It can be verified that } x = 3 \text{ and } x = 4 \text{ are solutions.}$$
$$\text{In } \mathbb{F}_6 \Rightarrow x^2 - x = 0$$
$$\text{It can be verified that } x = 0, x = 1, x = 3 \text{ and } x = 4 \text{ are solutions.}$$

7. Let $A = \begin{bmatrix} 0 & -2 \\ 2 & 0 \end{bmatrix}$

   (a) Is A diagonalizable over the field of rational numbers, $\mathbb{Q}$?

   (b) Does the answer change if we consider the above matrix over
   i)$\mathbb{R}$, ii) $\mathbb{F}_7$

Solution: Suppose $\exists P$ (invertible) s.t.

$$P^{-1}AP = D = \begin{bmatrix} d_1 & 0 \\ 0 & d_2 \end{bmatrix}$$
$$P^{-1}A^2P = D^2$$
$$\text{We get } A^2 = \begin{bmatrix} -4 & 0 \\ 0 & -4 \end{bmatrix} = -4I$$
$$\Rightarrow P^{-1}(-4I)P = D^2$$
$$\Rightarrow d_1^2 = -4; d_2^2 = -4$$

It can seen that $d_1, d_2 \notin \mathbb{Q}$ or $\mathbb{R}$. Hence the matrix A is not diagonalizable over $\mathbb{Q}$ or $\mathbb{R}$.

In $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$, we cannot find a d_1 such that $d_1^2 = -4(mod\ 7) = 3$ (Note: Take *modulo* 7 after addition and multiplication operations). Hence the matrix A is not diagonalizable over $\mathbb{F}_7$.

8. Let $K(\sqrt{2})$ be the set of all real numbers of the form $\alpha+\beta\sqrt{2}$, where $\alpha, \beta \in K$.

   (a) Is $K(\sqrt{2})$ a field when $K = \mathbb{Z}$?

   (b) Is $K(\sqrt{2})$ a field when $K = \mathbb{N}$?

   (c) Give an example of a set K so that $K(\sqrt{2})$ becomes a field.

   Solution:
   The solution is similar to the solution for Question 2.

9. Let $A = \begin{bmatrix} 0 & 4 \\ 3 & 0 \end{bmatrix}$

   (a) Is A diagonalizable over the field of integers, $\mathbb{Z}$?

   (b) Does the answer change if we consider the above matrix over
   i)$\mathbb{Q}$, ii) $\mathbb{F}_7$

   Solution: Suppose $\exists P$ (invertible) s.t.

$$P^{-1}AP = D = \begin{bmatrix} d_1 & 0 \\ 0 & d_2 \end{bmatrix}$$
$$P^{-1}A^2P = D^2$$
$$\text{We get } A^2 = \begin{bmatrix} 12 & 0 \\ 0 & 12 \end{bmatrix} = 12I$$
$$\Rightarrow P^{-1}(12I)P = D^2$$
$$\Rightarrow d_1^2 = 12; d_2^2 = 12$$

   It can seen that $d_1, d_2 \notin \mathbb{Z}$ or $\mathbb{Q}$. Hence the matrix A is not diagonalizable over $\mathbb{Z}$ or $\mathbb{Q}$.

   In $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$, we cannot find a d_1 such that $d_1^2 = 12(mod\ 7) = 5$ (Note: Take *modulo* 7 after addition and multiplication operations). Hence the matrix A is not diagonalizable over $\mathbb{F}_7$.

10. Consider the set of integers $\mathbb{Z}$ with "addition" operation $\oplus$ and "multiplication" operation $\otimes$. Define

$$x \oplus y = x + y - 1, \quad x \otimes y = x + y - xy.$$

   - Determine the additive identity and also the multiplicative identity, if one exists.
   - Show that $(\mathbb{Z}, \oplus, \otimes)$ is an integral domain.
     (Error in Quiz-1: Show that $(\mathbb{Z}, \oplus, \otimes)$ is not an integral domain.)

   Solution:

- Let e be the additive identity. Then

$$x \oplus e = e \oplus x = x + e - 1 = x$$

The above must be true for all $x \in \mathbb{Z}$. So, $e - 1 = 0 \Rightarrow e = 1$. So, when $e = 1$, $x \oplus e = e \oplus x = x, \forall x \in \mathbb{Z}$.

Let the multipliative identity be u. Then $x \otimes u = u \otimes x = x$ must be true $\forall x \in \mathbb{Z}$. So, on solving $x + u - xu = x$ we get $u(1-x) = 0$. So, $u(1-x) = 0$ must hold for all $x \in \mathbb{Z}$ which implies $u = 0$.

- Let $x \otimes y = e = 1$ (1 is the "zero element"). Therefore, $x \otimes y = x + y - xy = 1$. On rearranging we get $(1 - x)(1 - y) = 0$. Hence, $x = 1$ or $y = 1$. So the product of "non-zero" elements is "non-zero." The other properties of an integral domain can be easily verified to hold true for $(\mathbb{Z}, \oplus, \otimes)$.

11. Find all solutions to the equation

$$x^2 - 9x + 18 = 0$$

in (i) $\mathbb{F}_2$ (ii) $\mathbb{F}_5$ (iii) $\mathbb{F}_8$

Solution:

$$x^2 - 9x + 18 = 0$$
$$\text{In } \mathbb{F}_2 \Rightarrow x^2 - x = 0$$
$$x = 0 \text{ and } x = 1 \text{ are the solutions}$$
$$\text{In } \mathbb{F}_5 \Rightarrow x^2 - 4x + 3 = 0$$
$$\text{It can be verified that } x = 1, x = 3 \text{ are solutions.}$$
$$\text{In } \mathbb{F}_8 \Rightarrow x^2 - x + 2 = 0$$
$$\text{It can be verified that } x = 3, x = 6 \text{ are solutions.}$$

12. Let G be the set of matrices of the form $\begin{pmatrix} a & a \\ a & a \end{pmatrix}$, where $a \in \mathbb{Q}$, the set of rational numbers

- We know that any integral domain S has the following property:
  The product of any two non zero elements is non zero.
  Does this property hold for G?
- Determine the multiplicative identity of G.
- Does every non-zero element of G have a multiplicative inverse? If yes, find it.

Solution: Let $p = \begin{pmatrix} a & a \\ a & a \end{pmatrix}$ and $q = \begin{pmatrix} b & b \\ b & b \end{pmatrix}$ where $p, q \in S$.

$$p \times q = 0 \Rightarrow \begin{pmatrix} a & a \\ a & a \end{pmatrix} \begin{pmatrix} b & b \\ b & b \end{pmatrix} = 0 \tag{2}$$

$$\Rightarrow \begin{pmatrix} 2ab & 2ab \\ 2ab & 2ab \end{pmatrix} = 0 \tag{3}$$

$$\Rightarrow ab = 0 \tag{4}$$

Since $a, b \in \mathbb{Q}$ and $\mathbb{Q}$ is an integral domain, we have that S satisfies the above mentioned property of integral domain.

Let $\begin{pmatrix} e & e \\ e & e \end{pmatrix}$ be the multiplicative identity. It can be shown $\begin{pmatrix} 0.5 & 0.5 \\ 0.5 & 0.5 \end{pmatrix}$ is the multiplicative identity.

Similarly, it can be shown $\begin{pmatrix} \frac{1}{4a} & \frac{1}{4a} \\ \frac{1}{4a} & \frac{1}{4a} \end{pmatrix}$ is the multiplicative inverse of any non-zero element of the set S.