Indian Institute of Technology Jammu

CSD001P5M **Linear Algebra** **Tutorial: 02**

1. Determine the inverse of the given matrix A using row reduction.

$$A = \begin{bmatrix} 2 & 1 & -1 \\ 0 & 2 & 1 \\ 5 & 2 & -3 \end{bmatrix}$$

2. Recall Proposition 5: if e is an elementary row-operation and E is the corresponding elementary matrix, then $e(A) = E(A)$. Illustrate with one example each for scaling and interchange operations (the minimum size of the matrices in your examples should be 3×3).

3. Prove Proposition 5 in the general case, i.e. for any row operation e and any matrix A. (NB: the three cases of scaling, replacement and interchange require separate proofs.)

4. Given an $m \times n$ matrix A and an $n \times k$ matrix B, the product $AB = [Av_1 \;\; Av_2 \;\; \cdots \;\; Av_k]$ in column form where $B = [v_1 \;\; v_2 \;\; \cdots \;\; v_k]$ in column form. Construct an example to illustrate this rule. The matrix A in your example should be at least 3×3 and B should be at least 3×2.

5. Suppose $AB = AC$, where B and C are $n \times k$ matrices and A is invertible. Show that $B = C$. Is this true, in general, when A is not invertible ? Justify your answer (proof if true, counter-example if false).

Problems on Groups

In all the problems below wherever G occurs, we shall consider $(G, \cdot)$ to be a group with respect to multiplicative operation "$\cdot$" unless otherwise stated.

6. Prove that identity element in any group is unique.

7. Prove that every element in any group has a unique inverse.

8. Let G be a group and $a, b, c \in G$. If $a \cdot c = b \cdot c$, then $a = b$. In particular, if $a \cdot c = c$,then a is the identity element.

9. (a) Let G be a finite abelian group of order n. Then prove that for any element $g \in G$, $g^n = e$, where e is the identity element of the group G and g^n denotes $g \cdot g \cdot \cdots \cdot g$ (n operation).

(b) By using the result of part 4(a), prove Fermat's Little Theorem, which states that:
Fermat's Little Theorem: If p is a prime number, then for any integer a, we have: $a^p \equiv a \pmod{p}$.

10. For $n \in \mathbb{N}$, the Euler's totient function $\phi(n)$ is defined as follows:

$$\phi(n) = |\{a \in \mathbb{Z} \;:\; 1 \le a \le n, \gcd(a,n) = 1\}|.$$

Prove the following:

(a) If $m, n \in \mathbb{N}$ such that $\gcd(m,n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.

(b) $\phi(p) = p - 1$, where p is a prime number.

(c) $\phi(p^k) = p^k \left(1 - \dfrac{1}{p}\right)$, where p is a prime number.

(d) $\phi(n) = n \prod_{p|n} \left(1 - \dfrac{1}{p}\right)$, where p is a prime divisor of n.

(e) Let p, q be primes and let $n = pq$, then prove that $\phi(n) = (p-1)(q-1)$.

11. Show that:

(a) $\mathbb{Z}_n := \{0, 1, 2, \cdots, n-1\}$ is an abelian group with respect to $+_n$ (addition modulo n).

(b) $\mathbb{Z}_n^* := \{1, 2, \cdots, n-1\}$ satisfies all the properties of an abelian group with respect to $\times_n$ (multiplication modulo n) except the inverse property.

(c) Multiplication (modulo n) distributes over addition (modulo n) in $\mathbb{Z}_n$.

12. (a) Consider the set $\mathbb{Z}^\times = \{a \in \mathbb{Z}_n \;:\; \gcd(a,n) = 1\}$. Prove that $\mathbb{Z}^\times$ forms an abelian group with respect to $\times_n$ (multiplication modulo n). What is the cardinality of the group $\mathbb{Z}^\times$?

(b) By using the results of 4(a) and 6(b), prove Euler's theorem, which states that:
Euler's Theorem: For $n \ge 2$ in $\mathbb{N}$ and any a in $\mathbb{Z}$ such that $\gcd(a,n) = 1$, we have:

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

[Note: Fermat's Little Theorem is immediate consequence of Part 7(b)]