E0 219 Linear Algebra and Applications / August-December 2011

(ME, MSc. Ph. D. Programmes)

Tel : +91-(0)80-2293 2239/(Maths Dept. 3212) **E-mails :** dppatil@csa.iisc.ernet.in / patil@math.iisc.ernet.in

Lectures : Monday and Wednesday ; 11:30–13:00 **Venue:** CSA, Lecture Hall (Room No. 117)

Corrections by : **Jasine Babu** (jasinekb@gmail.com) / **Nitin Singh** (nitin@math.iisc.ernet.in) / **Amulya Ratna Swain** (amulya@csa.iisc.ernet.in) / **Meghana Mande** (meghanamande@gmail.com) / **Achintya Kundu** (achintya.ece@gmail.com)

1-st Midterm : Saturday, September 17, 2011; 10:30 -12:30 **2-nd Midterm :** Saturday, October 22, 2011; 10:30 -12:30
Final Examination : December ??, 2011, 10:00 -13:00

Evaluation Weightage : Assignments : 20% **Midterms (Two) :** 30% **Final Examination :** 50%

1. Basic Algebraic Concepts

Submit a solution of the $*$-Exercise ONLY

Due Date : Monday, 15-08-2011 (Before the Class)

1.1 Let $G \subseteq \mathbb{Z}$ be a subset of integers which contains at least one positive integer and at least one negative integer. Suppose that G is closed under the usual addition in $\mathbb{Z}$ i.e. $a+b \in G$ whenever $a, b \in G$. Prove that $(G,+)$ is a group. (**Hint :** Use Test-Exercise T1.1 (f) 1).)

1.2 For $a, b \in \mathbb{R}$, let $f_{a,b} : \mathbb{R} \to \mathbb{R}$ be the function defined by $f_{a,b}(x) := ax + b$, $x \in \mathbb{R}$. Then $G := \{f_{a,b} \mid a, b \in \mathbb{R}, a \neq 0\}$ with the composition as a binary operation is not a commutative group. (**Remark :** This group G is called the affine group of $\mathbb{R}$ and is usually denoted by $\mathrm{Aff}(1,\mathbb{R})$; Its elements are called the affine linear maps.)

1.3 **(a)** Let G be a finite group with the identity element e. Suppose that $\#G = n$ and $(a_1, \ldots, a_n) \in G^n = G \times \cdots \times G$ (n-times). Then there exist r, s with $0 \leq r < s \leq n$ such that $a_{r+1} \cdots a_s = e$. (**Hint :** The $n+1$ products $a_1 \cdots a_s$, $s = 0, \ldots, n$, cannot be pairwise distinct.)

(b) For any given $a_1, \ldots, a_n \in \mathbb{Z}$, $n \in \mathbb{N}^+$, show that there exist r, s with $0 \leq r < s \leq n$ such that $a_{r+1} + \cdots + a_s$ is divisible by n. (**Hint :** Consider $a_1, \ldots, a_n$ in the group $(\mathbb{Z}_n, +_n)$ and apply part a).)

1.4 Let M be a (multiplicative)) monoid.

(a) Show that for an element $a \in M$, the following statements are equivalent:

(i) a is invertible in M, i. e. $a \in M^\times$.

(ii) The left translation map $\lambda_a : M \to M$, $x \mapsto ax$ is bijective.

(iii) The right translation map $\rho_a : M \to M$, $x \mapsto xa$ is bijective.

(b) Show that M is a group if and only if every equation of the form $ax = b$ with $a, b \in M$ has a solution in M.

***1.5** Let $n \in \mathbb{N}^*$. Show that:

(a) A residue class $[k]_n \in \mathbb{Z}_n$, $k \in \mathbb{Z}$, is invertible in the multiplicative monoid $(\mathbb{Z}_n, \cdot)$ if and only if $\gcd(k,n) = 1$, i. e. $(\mathbb{Z}_n, \cdot_n)^\times = \{[k]_n \mid \gcd(k,n) = 1\}$. In particular, the unit group $(\mathbb{Z}_n)^\times$ is a group of order $\varphi(n)$, where φ is the *Euler's totient* function. (**Hint :** Use the **Bezout's Lemma**: *If a and b are positive natural numbers, then there exist integers s and t with $\gcd(a,b) = sa + tb$. —In particular, if a and b are relatively prime positive natural numbers, then there exist integers s and t with $1 = sa + tb$.*) Compute the inverse of $[69]_{100}$ in $\mathbb{Z}_{100}$.

(b) $(\mathbb{Z}_n, +_n, \cdot_n)$ is a field if and only if n is a prime number.

On the other side one can see auxiliary results and (simple) test-exercises.

Auxiliary Results/Test-Exercises

T1.1 (Relations, Order, Equivalence relations and Quotient sets) Let X be a set.

(a) (Relations) A relation on X is a subset of the cartesian product $X \times X$. Instead of "$(x,y) \in R$ we usually write xRy." We need to consider relations with additional properties.

Let X be a set and let $R \subseteq X \times X$ be a relation on X. Then

1) R is called reflexive if for all $x \in X$, xRx.

2) R is called symmetric if for all $x, y \in X$, from xRy, it follows that yRx.

3) R is called anti-symmetric if for all $x, y \in X$, from xRy and yRx, it follows that $x = y$.

4) R is called transitive if for all $x, y, z \in X$,from xRy and yRz, it follows that xRz.

5) R is called complete if for all $x, y \in X$ either xRy or yRx.

We usually denote relations on a set X by the symbols $=$, $\sim$, $\approx$, $\equiv$, $\simeq$, $\subseteq$, $\preceq$, $\leq$ and so on.

(b) (Order Relations) A relation on a set is called an order (relation) if it is reflexive, anti-symmetric and transitive. A complete order relation is called a total or linear order.

Order relations are often denoted by the symbol $\leq$. We also write $y \geq x$ for $x \leq y$; and $x < y$ if $x \leq y$ and $x \neq y$. A set X with a (fixed) order $\leq$ is called an ordered set and is denoted by the pair $(X, \leq)$.

(c) Let $(X, \leq)$ be an ordered set. For a subset $Y \subseteq X$, an element $y_0 \in Y$ is called a smallest (respectively, biggest) element of Y if for all $y \in Y$, we have $y_0 \leq y$ (respectively, $y \leq y_0$).

If at all Y has a smallest (respectively, biggest) element, then it is uniquely determined (since $\leq$ is anti-symmetric) and is usually denoted by $\min Y$ (respectively, $\max Y$) and also called the minimum (respectively, maximum) of Y.

(d) (Well Order) A total order on a set X is called a well order if every non-empty subset of X has a smallest element.

(e) (Equivalence relations and Quotient Sets) A relation on a set X is called an equivalence relation if it is reflexive, symmetric and transitive.

Let X be a set and let $\sim$ be an equivalence relation on X. Two elements $x, y \in X$ are called equivalent under $\sim$ if $x \sim y$ (and hence $y \sim x$ also). For $x \in X$, the subset $\{y \in X \mid x \sim y\}$ of X is called the equivalence class of x under $\sim$ and is usually denoted by $[x]_\sim$ or just by $[x]$ or $\bar{x}$.
(1) For every $x \in X$, $x \in [x]$. In particular, $[x] \neq \emptyset$ and $X = \cup_{x \in X}[x]$. (2) For all $x, y \in X$, the following statements are equivalent: (i) $[x] = [y]$. (ii) $[x] \cap [y] \neq \emptyset$. (iii) $x \sim y$.

The set of equivalence classes $X/\sim := \{[x] \mid x \in X\}$ is called the quotient set of the relation $\sim$ on X. The natural map $q : X \to X/\sim$ which maps every element $x \in X$ maps to its equivalence class $[x]$ is clearly surjective and is called the canonical projection or quotient map of the equivalence relation $\sim$ on X. Its fibres are precisely the equivalence classes. One also says that $X/\sim$ is obtained by identifying the equivalent element with respect to $\sim$. An element in an equivalence class is called representative of its equivalence class. If we choose exactly one representative from each equivalence class, then together they form a complete representative system or fundamental domain for the quotient set $X/\sim$. For example:
(1) On every set X "equality" is an equivalence relation, its equivalence classes are singletons $\{x\}$, $x \in X$. This is the only equivalence relation which is also an order on X.

(f) 1) (Law of well order) The standard order $\leq$, i. e. the subset $\{(m,n) \mid n - m \in \mathbb{N}\} \subseteq \mathbb{N} \times \mathbb{N}$ is a well order on $\mathbb{N}$. This is equivalent to the principle of mathematical induction[1] (which is a part of the definition on $\mathbb{N}$). However, the standard order $\leq$ on the set of integers $\mathbb{Z}$ is not a well order,

[1] **Principle of mathematical induction:** If M is a subset of $\mathbb{N}$ such that $0 \in M$ and for all $m \in M$, $m+1$ also belongs to M, then $M = \mathbb{N}$.

since for example, $\mathbb{Z}$ itself has no smallest element. The standard order $\leq$ on $\mathbb{N}$ is compatible with the standard addition and multiplication:
(i) (Monotony of addition) For all $a,b,c \in \mathbb{N}$, from $a \leq b$, it follows that $a+c \leq b+c$.
(ii) (Monotony of multiplication) For all $a,b,c \in \mathbb{N}$, from $a \leq b$, it follows that $ac \leq bc$.
The Well Ordering principle states that: *If X is a non-empty set, then there exists a well-order on X.* The main advantage of the well-ordering principle is that it enables us to extend the principle of mathematical induction to any well-ordered set. This is known as the principle of transfinite induction.

2) On the power set $\mathfrak{P}(X)$ of a set X, the inclusion relation $\subseteq$ is an order which is in general not a total order; if X has at least two elements x,y, then neither $\{x\} \subseteq \{y\}$ nor $\{y\} \subseteq \{x\}$.

3) The divisibility is a reflexive and transitive relation on $\mathbb{Z}$ which is neither symmetric nor anti-symmetric. For example, 3 divides 6, but 6 is not a divisor of 3. Moreover, 3 and -3 divide each other. However, on $\mathbb{N}$ the divisibility is an order, but not a total order.

4) (Congruence modulo[2] n) Let $n \in \mathbb{N}$, $n \neq 0$ be a fixed natural number. For arbitrary $a,b \in \mathbb{Z}$, we put $a \equiv_n b \bmod n$ (and read a is congruent to b modulo n) if n divides $a-b$ (equivalently, a and b have the same remainders (between 0 and $n-1$) on division by n). Then $\equiv_n$ is an equivalence relation on $\mathbb{Z}$. there are exactly n equivalence classes under $\equiv_n$, so-called the residue classes modulo n. the set of residue classes (quotient set under $\equiv_n$) is denoted by $\mathbb{Z}_n$; the numbers $0,1,\ldots,n-1$ form a complete representative system for $\equiv_n$. In the case $n=2$, the residue class $\overline{0} = [0]$ is the set of all even integers and the residue class $\overline{1} = [1]$ is the set of odd integers.

(g) 1) Every complete order is reflexive and hence in the definition of total order one may drop reflexivity.

2) In the definition of well order one may drop completeness.

3) For a relation $\sim$ on a set X, show that: (i) If $\sim$ is symmetric and complete, then $\sim$ be the whole order $X \times X$. (ii) If $\sim$ is reflexive, symmetric and anti-symmetric, then $\sim$ must be the equality order $\Delta_X := \{(x,x) \mid x \in X\}$.

4) The relation $\sim$ on $\mathbb{Z}$ defined by $a \sim b$ if $a = b \neq 0$ is not reflexive, but is symmetric and transitive. The relation $\approx$ on $\mathbb{Z}$ defined by $a \approx b$ if $|a-b| < 2$ is not transitive, but is reflexive and symmetric.

5) The set $\mathbb{Z}$ with the usual order $\leq$ is totally ordered but not well-ordered (since the subset of negative integers has no smallest element). However, each of the following order (where by definition $a < b$ if a is to the left of b) is a well-order:
(i) $0,1,-1,2,-2,3,-3,\ldots,n,-n,\ldots$; (ii) $0,1,3,5,7,\ldots,2,4,6,8,\ldots,-1,-2,-3,-4,\ldots$;
(iii) $0,3,4,5,6,\ldots,-1,-2,-3,-4,\ldots,1,2.$

T1.2 (a) (Division algorithm) Let a and b be integers with $b \neq 0$. Then there exist unique integers q and r such that $a = qb + r$, with $0 \leq r < |b|$. The integers q and r are called the quotient and remainder of a on division by b, respectively.

(b) (Euclidean algorithm) The existence and a rapid computation of the $\gcd(a,b)$ is proved by the following Euclidean algorithm:
Put $r_0 := a$ and $r_1 := b$ and use the division algorithm repeatedly to write the equations:

$$\begin{aligned} r_0 &= q_1 r_1 + r_2, && 0 < r_2 < r_1; \\ r_1 &= q_2 r_2 + r_3, && 0 < r_3 < r_2; \\ \cdots & \quad \cdots \quad \cdots \\ r_{k-1} &= q_k r_k + r_{k+1}, && 0 < r_{k+1} < r_k; \\ r_k &= q_{k+1} r_{k+1}. \end{aligned}$$

This process terminates after finitely many steps, since $r_1 > r_1 > \cdots > r_k > r_{k+1}$. Then $\gcd(a,b) = r_{k+1}$. Parallel to the Euclidean algorithm one can represent the remainder r_i in the form $r_i = s_i a + t_i b$ with $s_i, t_i \in \mathbb{Z}$. In particular, $r_{k+1} = s_{k+1} a + t_{k+1} b$ with $s_{k+1}, t_{k+1} \in \mathbb{Z}$. This can be done by recursively by defining:

$$\begin{aligned} s_0 &= 1, \quad t_0 = 0 \qquad s_1 = 0 \quad t_1 = 1 \\ s_{i+1} &= s_{i-1} - q_i s_i \qquad t_{i+1} = t_{i-1} - q_i t_i, \qquad i = 1, \ldots k. \end{aligned}$$

[2] First time this relation is systematically studied by C. F. Gauss in his *Disquisitiones arithmeticae* (1801).

Then:
$$a = r_0 = s_0a + t_0b, \qquad b = r_1 = s_1a + t_1b$$
$$r_{i+1} = r_{i-1} - q_ir_i = s_{i-1}a + t_{i-1}b = -q_is_ia - q_it_ib = s_{i+1}a + t_{i+1}b\,, \qquad i = 1, \ldots k.$$

This proves Bezout's lemma which is stated in Exercise 1.5. We illustrate this algorithm by the following example: $a := 36667$ and $b = 12247$. Then:
$$\begin{aligned} 36667 &= 2 \times 12247 + 12173;\\ 12247 &= 1 \times 12173 + 74;\\ 12173 &= 164 \times 74 + 37\\ 74 &= 2 \times 37. \end{aligned}$$

Therefore $\gcd(36667, 12247) = 37$. Further,

i	0	1	2	3	4
q_i		2	1	164	2
s_i	1	0	1	-1	165
t_i	0	1	-2	3	-494

Therefore $37 = \gcd(36667, 12247) = 165 \times 36667 - 494 \times 12247$.

T1.3 (The unit group of a monoid) Let M be a (multiplicative) monoid. An element $x \in M$ is called invertible if there exists $x' \in M$ such that $x'x = e = xx'$. In this case the inverse x' is uniquely determined by x and is denoted by x^{-1} (in the additive notation by $-x$). Let $M^\times$ denote the set of all invertible elements of M.

1) $e \in M^\times$.

2) If $x, y \in M^\times$, then $xy \in M^\times$ and $(xy)^{-1} = y^{-1}x^{-1}$.

3) $M^\times$ is a group under the induced binary operation of M.

4) M is a group if and only if $M = M^\times$.

– The group $M^\times$ is called the group of invertible elements of M or the unit group of M. For example, in a field K with respect to multiplication the unit group is $K^\times = K \setminus \{0\}$. For the monoid $(X^X, \circ)$ of the set of all maps of a set X into itself, the unit group is $(X^X)^\times = \mathfrak{S}(X)$ the set of all permutations of X (proof!).

T1.4 (Addition modulo n and multiplication modulo n) Let $n \in \mathbb{N}^+$ be a non-zero natural number. On the quotient set $\mathbb{Z}_n := \{[0]_n, [1]_n, \ldots, [n-1]_n\}$ of the congruence modulo n, the binary operations $+_n$ addition modulo n and $\cdot_n$ multiplication modulo n are defined by $[a]_n +_n [b]_n := [a+b]_n$ and $[a]_n \cdot_n [b]_n := [a \cdot b]_n$, respectively. With these binary operations $(\mathbb{Z}_n, +_n, \cdot_n)$ is a commutative ring (with identity).

T1.5 (Power set of a set) Let X be any set and let $\mathfrak{P}(X)$ denote the power set of X, i. e. $\mathfrak{P}(X) := \{A \mid A \text{ is a subset of } X\}$.

1) The union $\cup$ and intersection $\cap$ are associate and commutative binary operations on $\mathfrak{P}(X)$. What are the neutral elements for these binary operations? In the case $X \neq \emptyset$, neither $(\mathfrak{P}(X), \cup)$ nor $(\mathfrak{P}(X), \cap)$ is a group.

2) On $\mathfrak{P}(X)$ the symmetric difference $\triangle$ is a binary operation, in fact $(\mathfrak{P}(X), \triangle)$ is a group. What is the inverse of $Y \in \mathfrak{P}(X)$ in the group $(\mathfrak{P}(X), \triangle)$?

3) (Indicator functions) For $A \in \mathfrak{P}(X)$, let $e_A : X \to \{0, 1\}$, $e_A(x) = 1$ if $x \in A$ and $e_A(x) = 0$ if $x \notin A$, denote the indicator function of A. For $A, B \in \mathfrak{P}(X)$, prove that : $e_{A\cap B} = e_Ae_B\,, \quad e_{A\cup B} = e_A + e_B - e_Ae_B\,, \quad e_{A\setminus B} = e_A(1 - e_B)$. In particular, $e_{X\setminus A} = 1 - e_A$ and $e_{A\triangle B} = e_A + e_B - 2e_Ae_B$.

4) The map $e : \mathfrak{P}(X) \to \{0, 1\}^X$ defined by $A \mapsto e_A$ is bijective. (**Remark :** One can use this bijective map and part (3) to prove (2).)

T1.6 There are natural examples of non-associative binary operations. For example, on the set $\mathbb{N}$ of natural numbers the exponentiation $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $(m, n) \mapsto m^n$ is a non-associative binary operation on $\mathbb{N}$. The difference $\mathbb{Z} \times Z \to \mathbb{Z}$, $(m, n) \to m - n$ and the division $\mathbb{Q}^\times \times \mathbb{Q}^\times \to \mathbb{Q}^\times$, $(x, y) \mapsto x/y$ are also non-associative binary operations. More generally, if G is a group, then $G \times G \to G$, $(a, b) \mapsto ab^{-1}$ is a non-associative binary operation if there is at least one element $b \in G$ with $b \neq b^{-1}$.