E0 219 Linear Algebra and Applications / August-December 2016

(ME, MSc. Ph. D. Programmes)

Download from : http://www.math.iisc.ernet.in/patil/courses/courses/Current Courses/...

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 ; 11:00–12:30 **Venue:** CSA, Lecture Hall (Room No. 117)

Corrections by : **Nikhil Gupta** (nikhil.gupta@csa.iisc.ernet.in ; **Lab No.: 303**) /
Vineet Nair (vineetn90@gmail.com ; **Lab No.: 303**) /
Rahul Gupta (rahul.gupta@csa.iisc.ernet.in ; **Lab No.: 224**) /
Sayantan Mukherjee (meghanamande@gmail.com ; **Lab No.: 253**) /
Palash Dey (palash@csa.iisc.ernet.in ; **Lab No.: 301 , 333 , 335**)

Midterms : 1-st Midterm : Saturday, September 17, 2016; 15:00 – 17:00 **2-nd Midterm :** Saturday, October 22, 2016; 15:00 – 17:00

Final Examination : December ??, 2016, 09:00 – -12:00

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

Range of Marks for Grades (Total 100 Marks)						
	Grade S	**Grade A**	**Grade B**	**Grade C**	**Grade D**	**Grade F**
Marks-Range	> 90	76 — 90	61 — 75	46 — 60	35 — 45	< 35

	Grade A$^+$	**Grade A**	**Grade B**$^+$	**Grade B**	**Grade C**	**Grade D**	**Grade F**
Marks-Range	> 90	81 — 90	71 — 80	61 — 70	51 — 60	40 — 50	< 40

Supplement 1

Basic Algebraic Concepts

We shall use the following standard notations for some frequently occurring sets :

$\mathbb{N} = \{0,1,2,3,\ldots\}$ set of natural numbers,

$\mathbb{N}^* = \{1,2,3,\ldots\}$ set of positive natural numbers,

$\mathbb{N}_n = \{x \in \mathbb{N} \mid x \leq n\} = \{0,1,\ldots,n\}$, $\mathbb{N}_n^* = \{x \in \mathbb{N}^* \mid x \leq n\} = \{1,\ldots,n\}$ $(n \in \mathbb{N})$,

$\mathbb{Z} = \{0,1,-1,2,-2,3,-3,\ldots\}$ set of integers,

$\mathbb{Q} = \left\{\frac{a}{b} = a/b \mid a,b \in \mathbb{Z}, b \neq 0\right\}$ set of rational numbers,

$\mathbb{R}$ set of real numbers,

$\mathbb{R}^\times = \{x \in \mathbb{R} \mid x \neq 0\}$ set of non-zero real numbers,

$\mathbb{R}_+ = \{x \in \mathbb{R} \mid x \geq 0\}$ set of non-negative real numbers,

$\mathbb{R}_- = \{x \in \mathbb{R} \mid x \leq 0\}$ set of non-positive real numbers,

$\mathbb{R}_+^\times = \{x \in \mathbb{R} \mid x > 0\}$ set of positive real numbers,

$\mathbb{C} = \{x + \mathrm{i}y \mid x,y \in \mathbb{R}\}$ set of complex numbers,

$\mathbb{C}^\times = \{z \in \mathbb{C} \mid z \neq 0\}$ set of non-zero complex numbers.

We assume that the reader is familiar with the standard arithmetical operations and the elementary computational rules for these number systems.

S1.1 (The Natural numbers — Peano's axioms) The theory of the set of natural numbers $\mathbb{N}$ from the *Peano's axioms*, which were set out first by G. Peano (1858– 1939) in 1889. The induction axiom[1] is the basis of the *principle of mathematical induction*. Proofs by induction are very common in mathematics and are undoubtedly familiar to the reader.

Using induction axiom one can construct the canonical or natural or usual order[2] $\leq$ on $\mathbb{N}$. One often use the Minimum Principle (also known as Well ordering Principle for $\mathbb{N}$, which states that : *Every non-empty subset M of $\mathbb{N}$ contains a least element,* i. e. , *there exists an element $m_0 \in M$ such that $m_0 \leq m$ for all $m \in M$. In particular, the canonical order on $\mathbb{N}$ is a total order.*

[1] **Induction axiom :** 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 $M = \mathbb{N}$.

[2] A relation on a set A is called an order if it is reflexive, antisymmetric and transitive.

Further, one can define the binary operations addition, multiplication and exponentiation and derive the entire arithmetic on $\mathbb{N}$. The natural order $\leq$ on $\mathbb{N}$ is compatible with the standard addition and multiplication:

For all $a,b,c \in \mathbb{N}$

(i) (Monotony of addition) $a \leq b$, implies that $a+c \leq b+c$.

(ii) (Monotony of multiplication) $a \leq b$, implies that $ac \leq bc$.

However, the standard order $\leq$ on the set of integers $\mathbb{Z}$ is not a well order, since for example, $\mathbb{Z}$ itself has no smallest element.

S1.2 (Arithmetic) In this supplement, we describe the structure of the commutative and regular monoid $\mathbb{N}^* = (\mathbb{N}^*, \cdot)$ of positive integers with the usual multiplication as binary operation.

(a) (Prime numbers) A positive integer $m \in \mathbb{N}^*$ is called irreducible or prime or a prime number if $m \neq 1$ and if m and 1 are the only divisors of m in $\mathbb{N}^*$. We denote the subset of prime numbers in $\mathbb{N}^*$ by $\mathbb{P}$.

An integer $m > 1$ is reducible or composite, i.e., not irreducible, if and only if there exist integers a, b such that $1 < a, b < m$ and $m = ab$. Note that *the smallest divisor > 1 of an integer $m > 1$ is necessarily irreducible.* The following famous theorem has a very simple proof:

(Euclid) *The set $\mathbb{P}$ of prime numbers is infinite.*

(The infinite strictly increasing sequence $p_n, n \in \mathbb{N}^*$, of prime numbers starts with $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, p_5 = 11, \ldots$. This sequence is still a big mystery. It is easy to show that the sequence $p_{n+1} - p_n$, $n \in \mathbb{N}^*$, of prime number gaps is unbounded. It is still open if there are infinitely many $n \in \mathbb{N}^*$ with $p_{n+1} - p_n = 2$. (The conjectured answer to this so-called twin prime problem is "yes".) However, recently (2013) Y. Zhang proved the following theorem: *The sequence $p_{n+1} - p_n$, $n \in \mathbb{N}^*$, does not converge to ∞*, i. e., there exists an $N \in \mathbb{N}$ with $p_{n+1} - p_n \leq N$ for infinitely many $n \in \mathbb{N}^*$. (Zhang proved this for $N = 70,000,000$. Meanwhile this bound is improved, for example by $N = 600$ (J. Maynard 2013).) In this connection the prime number function $\pi(x)$ plays an important role. By definition, for a positive real number x, $\pi(x)$ is the number of primes $\leq x$. For instance, $\pi(p_n) = n$.)

(b) (Division with remainder) 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.

(c) (Euclidean Algorithm) Let $a, b \in \mathbb{N}^*$ with $a > b$. We put $r_0 := a$ and $r_1 := b$ and consider the following system of equations obtained by repeated division with remainder:

$$\begin{array}{rll}
r_0 = q_1 r_1 + r_2\,, & \quad 0 < r_2 < r_1\,; \\
r_1 = q_2 r_2 + r_3\,, & \quad 0 < r_3 < r_2\,; \\
\cdots\cdots\cdots\cdots & \cdots\cdots\cdots\cdots \\
r_i = q_{i+1} r_{i+1} + r_{i+2}\,, & \quad 0 < r_{i+2} < r_{i+1}\,; \\
\cdots\cdots\cdots\cdots & \cdots\cdots\cdots\cdots \\
r_{k-1} = q_k r_k + r_{k+1}\,, & \quad 0 < r_{k+1} < r_k\,; \\
r_k = q_{k+1} r_{k+1}\,. &
\end{array}$$

The algorithm stops when $r_{k+2} = 0$, i. e. when $r_{k+1} \mid r_k$. This happens because the sequence $r_0 > r_1 > r_2 > \cdots$ of the non-negative remainders is strictly decreasing. Moreover, the successive pairs r_{i-1}, r_i and r_i, r_{i+1}, $i = 1, \ldots, k$, obviously have the same common divisors. Therefore

$$\gcd(a,b) = \gcd(r_0, r_1) = \cdots = \gcd(r_k, r_{k+1}) = r_{k+1}\,.$$

The equations of the algorithm also allow to construct coefficients $s, t \in \mathbb{Z}$ with $\gcd(a,b) = r_{k+1} = sa + tb$. For this, define s_i, t_i, $i = 0, \ldots, k+1$, recursively by

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

Then, by induction on i, one proves $r_i = s_i a + t_i b$, $i = 0, \ldots, k+1$. In particular,

$$\gcd(a,b) = r_{k+1} = s_{k+1} a + t_{k+1} b\,.$$

(We illustrate the above algorithm by the following example: Let $a := 40631$ and $b := 13571$. The Euclidean algorithm supplies

$$40631 = 2 \cdot 13571 + 13489\,,\ 13571 = 1 \cdot 13489 + 82\,,\ 13489 = 164 \cdot 82 + 41\,,\ 82 = 2 \cdot 41\,.$$

So we have $k=3$, and the integers s_i, t_i, $i=0,\ldots,4$, are computed in the following table:

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

Therefore $41=\gcd(40631,13571)=165\cdot 40631-494\cdot 13571$.

Two integers $a,b\in\mathbb{Z}$ are called coprime or relatively prime if $\gcd(a,b)=1$. *A prime number $p\in\mathbb{P}$ and an integer $a\in\mathbb{Z}$ are coprime if and only if p does not divide a.*

(d) (Bezout's Lemma) Let $a,b\in\mathbb{Z}$ be relatively prime integers. Then there exist integers $s,t\in\mathbb{Z}$ with $sa+tb=1$.

An important property of coprime numbers is described in the following lemma:

(e) (Euclid's Lemma) *Let $a,b,c\in\mathbb{Z}$ with $\gcd(a,b)=1$. If $a\,|\,bc$ then $a\,|\,c$. In particular, if a prime number $p\in\mathbb{P}$ divides the product bc, then it divides at least one of the factors b or c.*

(f) (Fundamental Theorem of Arithmetic)[3] *Every positive integer $m\in\mathbb{N}^*$ is a product of (not necessarily distinct) irreducible numbers $p_1,\ldots,p_r\in\mathbb{P}$ which are uniquely determined by m up to order.*

(Proposition 14 of Book IX of Euclid's "Elements" embodies the result which later became known as the Fundamental Theorem of Arithmetic. The existence is proved by induction and uniqueness statement is a direct consequence of Euclid's Lemma. The Fundamental Theorem of Arithmetic allows to define canonical representations of integers and also of rationals. Altogether, the Fundamental Theorem of Arithmetic allows a lucid description of the structure of the multiplicative monoids $\mathbb{N}^*$, $\mathbb{Z}^*$ and the multiplicative group $\mathbb{Q}^\times$. The prime numbers are the atoms to build up these structures.)

S1.3 (Euler's φ-function) For arbitrary integers $m,n,q\in\mathbb{Z}$, one has $\gcd(n,m)=\gcd(n+qm,m)$, since the pair n,m and the pair $n+qm,m$ have the same set of common divisors. In particular, n,m are coprime if and only if $n+qm,m$ are coprime.— Now, let $m\in\mathbb{N}^*$. Since, by division with remainder (cf. S1.?? (a)), there exists a (unique) $q\in\mathbb{Z}$ with $0\le n+qm<m$ one overviews all integers that are coprime to m if one only knows the integers n with $0\le n<m$ that are coprime to m. The number of these integers is denoted by $\varphi(m)$. The function $\varphi:\mathbb{N}^*\to\mathbb{N}^*$, $m\mapsto\varphi(m)$, is called Euler's φ-function or the totient function. It is $\varphi(1)=1$, $\varphi(2)=1$, $\varphi(3)=2$, $\varphi(4)=2$, $\varphi(5)=4$, $\varphi(6)=2$, etc. $\varphi(m)$ is also the number of positive integers n with $0<n\le m$ and $\gcd(m,n)=1$. In particular, $\varphi(p)=p-1$ for a prime number p. More generally, $\varphi(p^\alpha)=p^{\alpha-1}(p-1)=p^\alpha(1-\frac{1}{p})$ for $p\in\mathbb{P}$, $\alpha\in\mathbb{N}^*$, since the positive integers $\le p^\alpha$ that are *not* coprime to p^α are the multiples rp, $r=1,\ldots,p^{\alpha-1}$, of p.

(a) For every positive integer m one has, $m=\sum_{d|m}\varphi(d)$.

(b) (Euler's Formula) For every $m\in\mathbb{N}^*$ one has $\varphi(m)=m\cdot\displaystyle\prod_{p\in\mathbb{P},\,p\,|\,m}\left(1-\frac{1}{p}\right)$.

S1.4 (Periodic sequences) Let $(x_i)=(x_i)_{i\in\mathbb{N}}$ be an arbitrary sequence. A pair $(t,s)\in\mathbb{N}\times\mathbb{N}^*$ is called a pair of periodicity for (x_i) if $x_{i+s}=x_i$ for all $i\ge t$. In this case, t is called a preperiod length and s a period length of (x_i). (x_i) is called periodic if such a pair of periodicity exists, otherwise (x_i) is called aperiodic. Now, assume that (x_i) is periodic. Show that there exists a unique pair of periodicity $(\ell,k)\in\mathbb{N}\times\mathbb{N}^*$ with the following property: $(t,s)\in\mathbb{N}\times\mathbb{N}^*$ is a pair of periodicity for (x_i) if and only if $t\ge\ell$ and $s=mk$ for some $m\in\mathbb{N}^*$. (**Hint :** The submonoid of periods of the sequence (x_i) fulfills the assumptions for N in Exercise 2 above. — The smallest pair of periodicity (ℓ,k) is called the pair of periodicity per

[3] The Fundamental Theorem of Arithmetic does not seem to have been stated explicitly in Euclid's elements, although some of the propositions in book VII and/or IX are almost equivalent to it. Its first clear formulation with proof seems to have been given by Gauss in *Disquisitiones arithmeticae* § 16 (Leipzig, Fleischer, 1801). It was, of course, familiar to earlier mathematicians; but Gauss was the first to develop arithmetic as a systematic science.

se or the periodicity type of the sequence (x_i). Its first component ℓ is called the (minimal) preperiod length and the second component k the (minimal) period length of (x_i). The finite subsequences $(x_0,\ldots,x_{\ell-1})$ and $(x_\ell,\ldots,x_{\ell+k-1})$ of length ℓ and k, respectively, are called the (minimal) preperiod resp. the (minimal) period of (x_i). If $\ell=0$, then (x_i) is called purely periodic. If $k=1$, the sequence (x_i) is called stationary with limit x if x is its period (of length 1). The constant sequences are the sequences of periodicity type $(0,1)$. By definition, aperiodic sequences have the periodicity type $(\infty,0)$. — If x is an element of a group then the sequence $(x^i)_{i\in\mathbb{N}}$ of its powers has period length $\operatorname{ord} x$ and is purely periodic if $\operatorname{ord} x>0$.)

S1.5 For every subgroup H of $(\mathbb{Z},+)$, there exists a unique natural number $n\in\mathbb{N}$ such that $H=\mathbb{Z}n:=\{an\mid a\in\mathbb{Z}\}$. For $m_1,\ldots,m_n\in\mathbb{N}^*$, we have $\mathbb{Z}m_1+\cdots+\mathbb{Z}m_n=\mathbb{Z}\gcd(m_1,\ldots m_n)$ and $\mathbb{Z}m_1\cap\cdots\cap\mathbb{Z}m_n=\mathbb{Z}\operatorname{lcm}(m_1,\ldots m_n)$.

S1.6 (Congruence modulo[4] n) Let $n\in\mathbb{N}$, $n\neq 0$ be a fixed natural number. For arbitrary $a,b\in\mathbb{Z}$, we write $a\equiv_n b \bmod n$ (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.

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 two binary operations $(\mathbb{Z}_n,+_n,\cdot_n)$ is a commutative ring (with identity).

S1.7 Let M,N be two jugs of capacities m resp. n liters with coprime $m,n\in\mathbb{N}^*$. Then, from a tank which contains at least $m+n-1$ liters of water, one can draw precisely x liters for every $x\in\mathbb{N}$ with $0\le x<m+n$. (**Hint :** If M contains $y\in\mathbb{N}$ liters and is filled up with the content of the full jug N (where the content of M is poured back into the tank every time M is full), then the new content of M represents the residue class of $y+n$ in $\mathbf{Z}_m=\mathbb{Z}/\mathbb{Z}m$. Now use Theorem **??**. For example, if $m=11$, $n=7$, one obtains this way, starting with the empty jug M, successively 0, 7, 3, 10, 6, 2, 9, 5, 1, 8, 4, 0,… liters. Interchanging the roles of M and N one obtains 0, 4, 1, 5, 2, 6, 3, 0,… liters.)

S1.8 (Fibonacci-sequence) The recursively defined sequence $F=(F_n)_{n\in\mathbb{N}}$ with $F_0=0$, $F_1=1$, $F_n=F_{n-1}+F_{n-2}$, $n\ge 2$, is called the Fibonacci-sequence and F_n is called the n-th Fibonacci-number. The first terms of the Fibonacci-sequence are $0,1,1,2,3,5,8,13,21,34,55,89,144,233,\ldots$.

(a) For every natural number $m\ge 2$, the sequence $F\,(\bmod\, m)$ of least nonnegative residues of the terms F_n modulo m, is purely periodic.
(**Hint :** For example, $F\,(\bmod\,5)=(\overline{0,1,1,2,3,0,3,3,1,4,0,4,4,3,2,0,2,2,4,1};0,1,1,\ldots)$ This is a natural consequence of (1) Modulo m, there are m^2 possible pairs of residues, and hence some pair of consecutive terms of $F\,(\bmod\, m)$ must repeat, and (2) Any pair of consecutive terms of $F\,(\bmod\, m)$ determines the entire sequence both forward and backward.)

(b) Let $m\in\mathbb{N}$, $m\ge 2$ and let $\pi(m)$ denote the period of the sequence $F\,(\bmod\, m)$. Then $\pi(m)=\min\{k\in\mathbb{N}^+\mid F_k\equiv 0\,(\bmod\, m)\text{ and }F_{k+1}\equiv 1\,(\bmod\, m)\}$. For $m=2,3,4,5,6,7,8,9,10,\ldots$, the values of $\pi(m)$ are $3,8,6,20,24,16,12,24,60,\ldots$. For $m>2$, $\pi(m)$ is even. (**Remark :** Matrix interpretation of $\pi(m)$: Let $U=\begin{pmatrix}0&1\\1&1\end{pmatrix}$. Then $U^n=\begin{pmatrix}F_{n-1}&F_n\\F_n&F_{n+1}\end{pmatrix}$ and $\pi(m)$ is the least integer k such that $U^k=\begin{pmatrix}1&0\\0&1\end{pmatrix}$, i. e. $\pi(m)=$ the order of U in the group $\mathrm{GL}_2(\mathbb{Z}_m)$.)

(c) For $m,n\in\mathbb{N}^+$, $\pi(\operatorname{lcm}(m,n))=\operatorname{lcm}(\pi(m),\pi(n))$ and hence, if $n\,|\,m$, then $\pi(n)\,|\,\pi(m)$.

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

(d) If $m = p_1^{\nu_1} \cdots p_r^{\nu_r}$ is the prime factorization of m, then $\pi(m) = \mathrm{lcm}(\pi(p_1^{\nu_1}), \ldots, \pi(p_r^{\nu_r})$.

(e) For a prime number p, let t be the largest integer such that $\pi(p^t) = \pi(p)$, then $\pi(p^\nu) = p^{\nu-1}\pi(p)$ for all $\nu \geq t$. (**Remark :** So far, no prime p has been found for which $\pi(p^2) = \pi(p)$. *It is an open problem whether any such primes exist.* If any do exist, they are called Wall-Sun-Sun Primes. So, for every prime that we know of, the formula $\pi(p^\nu) = p^{\nu-1}\pi(p)$ holds.)

S1.9 For an element a of a set M with the binary operation $*$, the map $\lambda_a : M \to M$, $x \mapsto a * x$ is called the left translation of M by a. Similarly, the map $\rho_a : M \to M$, $x \mapsto x * a$, is called the right translation of M by a. The following conditions are equivalent:
(i) The operation $*$ is associative.
(ii) $\lambda_a \circ \lambda_b = \lambda_{a*b}$ for all $a, b \in M$.
(iii) $\rho_a \circ \rho_b = \rho_{b*a}$ for all $a, b \in M$.
(iv) λ_a and ρ_b commute (i. e. $\lambda_a \circ \rho_b = \rho_b \circ \lambda_a$) for all $a, b \in M$.
Moreover, an element $e \in M$ is a neutral element for $*$ if and only if $\lambda_e = \rho_e = \mathrm{id}_M$. Furthermore, $\lambda_a = \rho_a$ for all $a \in M$ if and only if M is commutative.

S1.10 A set M with binary operation $*$ is called a semigroup if the binary operation $*$ is associative. A semigroup $(M, *)$ whose binary operation has a neutral ement is called a monoid. The neutral element of a monoid M is usually denoted by e_M or — for multiplicative monoids by 1_M or — for additive monoids — by 0_M.

A semigroup $(M, *)$ is regular if and only if for every element $a \in M$ the left translation $\lambda_a : x \mapsto a * x$ and the right translation $\rho_a : x \mapsto x * a$ of M are injective. More generally, we define: an element a of a semigroup M is called regular if both the left translation λ_a *and* the right translation ρ_a of M are injective.

Regular elements can be cancelled in the following sense: If $a \in M$ is regular and if $a * b = a * c$ or if $b * a = c * a$, then $b = c$. The set $M^* := \{ a \in M \mid a \text{ regular in } M \}$ of regular elements of M is obviously a subsemigroup of M (since compositions of injective maps are injective).

A semigroup M is regular if and only if $M^* = M$.

Note that *in a regular monoid the neutral element $e \in M$ is the only idempotent element* because, from an equation $a^2 = a = a e$, one obtains the equality $a = e$ by canceling a. It follows that a subsemigroup N of a regular monoid M which is a monoid has necessarily the same neutral element as M. Hence it is a submonoid of M.

S1.11 (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 $-x$). *Invertible elements in a monoid M are always regular*

Let $M^\times := \{x \in M \mid x \text{ is invertible } \}$ be the set of all invertible elements of M. Then $M^\times \subseteq M^*$and
(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 submonoid of M in which every element is invertible, i. e. , 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!). For monoids M, N, determine the group of invertible elements in the product monoid $M \times N$ (in terms of the groups $M^\times$ and $N^\times$).

S1.12 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 λ_a and the right translation ρ_a of M are bijective.
(iii) The left translation λ_a of M is bijective.
(iv) The right translation map ρ_a of M is bijective.
(v) The left translation λ_a and the right translation ρ_a of M are surjective.

(b) Give an example of a monoid M with an element $x_0 \in m$ such that λ_{x_0} is surjective, but x_0 is not invertible. (**Hint :** In the monoid $\mathbb{N}^{\mathbb{N}}$, define the map φ by $\varphi(0) := 0$, $\varphi(n) := n-1$ if $n \geq 1$, and the map ψ by $n \mapsto n+1$. Then $\varphi\psi = \mathrm{id}_{\mathbb{N}}$, and the element $\psi \in \mathbb{N}^{\mathbb{N}}$ has infinitely many left inverses in $\mathbb{N}^{\mathbb{N}}$. In particular, ψ is not invertible.)

S1.13 Let X be any set and let $\mathfrak{P}(X) := \{A \mid A \text{ is a subset of } X\}$ be the *power set of* X.

(a) 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.

(b) 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 $(\mathfrak{P}(X), \triangle)$?

(c) (*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 :
(i) $e_{A \cap B} = e_A e_B$, (ii) $e_{A \cup B} = e_A + e_B - e_A e_B$, (iii) $e_{A \smallsetminus B} = e_A(1 - e_B)$.
In particular, $e_{X \setminus A} = 1 - e_A$ and $e_{A \triangle B} = e_A + e_B - 2e_A e_B$.

(d) 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).)

S1.14 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 $b \neq b^{-1}$.

S1.15 Let G be a non-empty semigroup. The following statements are equivalent:
(i) G is a group.
(ii) For arbitrary $a, b \in G$ the equations $ax = b$ and $ya = b$ are uniquely solvable in G, i. e. all the translations λ_a and ρ_a, $a \in G$, are bijective.
(iii) For arbitrary $a, b \in G$ the equations $ax = b$ and $ya = b$ are solvable in G, i. e. all the translations λ_a and ρ_a, $a \in G$, are surjective.

S1.16 Let M be a semigroup with the following two properties: (1) For all $a \in M$, the left translations λ_a of M are surjective. (2) There exists at least one $b \in M$ such that the right translation ρ_b is surjective. Show that M is a group.

S1.17 Let A and B be two subsets of a finite group G. If $\#A + \#B > \#G$, then show that $G = AB := \{ab \mid a \in A \text{ and } b \in B\}$. (**Hint :** For $x \in G$, let $A_x := \{a^{-1}x \mid a \in A\}$. Use the Pigenhole principle (see Footnote 1) to conclude that $\#A_x = \#A$ and hence $A_x \cap B \neq \emptyset$ for every $x \in G$.)

S1.18 **(a)** Which of the following subsets are subgroups of the multiplicative group $\mathbb{Z}_{31}^\times$:

$$H_1 := \{\overline{1}, \overline{3}, \overline{6}, \overline{9}, \overline{18}, \overline{21}\}\,, \quad H_2 := \{\overline{1}, \overline{2}, \overline{4}, \overline{8}, \overline{16}\}\,.$$

(**Remark :** Note that H_2 is the submonoid of the powers $\overline{2}^k$, $k \in \mathbb{N}$, of $\overline{2}$. The sequence $\overline{2}^k$, $k \in \mathbb{N}$, is periodic with period 5, since $\overline{2}^5 = \overline{1}$. This proves that H_2 is a subgroup. More generally, see Exercise 1.3.)

(b) Which of the following subsets are subgroups of the multiplicative group $\mathbb{Z}_{29}^\times$:

$$H_1 := \{\overline{1}, \overline{12}, \overline{17}, \overline{28}\}\,, \quad H_2 := \{\overline{1}, \overline{2}, \overline{4}, \overline{8}, \overline{16}, \overline{20}, \overline{24}\}\,.$$