October, 28, 2018

Algebra.

Elements of Set Theory.

Definition. We will define a **set** to be a group of objects (not necessarily ordered) with no duplicates.

Note that the objects in the sets can themselves be sets. We can describe a set by defining some property of objects in it. For example,

1. the set containing the positive integers from 1 to 5 is $\{\mathbf{1}, \mathbf{2}, \mathbf{3}, \mathbf{4}, \mathbf{5}\}$
2. the set of all natural integers, which we denote $\mathbb{N}$
3. the set of all integer numbers, which we denote $\mathbb{Z}$
4. the set of all rational numbers, $\frac{\boldsymbol{m}}{\boldsymbol{n}}$, $(\{\boldsymbol{m}, \boldsymbol{n}\} \in \mathbb{Z} \wedge \boldsymbol{n} \neq \mathbf{0})$, which we denote $\mathbb{Q}$
5. the set of all real numbers, which we denote $\mathbb{R}$
6. the set of all irrational numbers, which we denote **D**

If a set has finite number of objects, it is said to be finite. Otherwise, it is infinite. The number of elements, $\boldsymbol{n}$, in a finite set $\boldsymbol{A}$, is denoted $|\boldsymbol{A}| = \boldsymbol{n}$. If elements in the set can be counted by assigning a natural integer to each element, the set is called countable. The set that is not countable is called uncountable.

Exercise. Give examples of infinite, countable, uncountable sets.

If we wish to describe an infinite set, such as the set of even positive integers, we use what is called "set builder notation".

$$M = \{x : (x \in \mathbb{Z}) \wedge (x > 0) \wedge (x/2 \in \mathbb{Z})\}$$

This is read verbally as "the set of all x such that x is integer and greater than 0 and x divided by 2 is also integer". Another example,

$$F = \{n^2 - 4 : (n \in \mathbb{Z}) \wedge (0 \leq n \leq 19)\}$$

"F is the set of all numbers of the form $n^2 - 4$, such that n is a whole number in the range from 0 to 19 inclusive", where the colon ":" is read "such that".

If x is a member of a set M, we will use notation $x \in M$, if y is not a member of a set M we will write $y \notin M$. For example statement "$0 \leq x \leq 1$ " can be written as $x \in [0,1]$. Another example: If $x > 3$ and $x < 5$, so $x \in (-\infty, 5[\cap]3, +\infty) \Leftrightarrow x \in]3,5[$.

Exercise. Find the set of all values of x for which the following expression makes sense: $\sqrt{25 - x^2} = \frac{4}{x-2}$.

The algebra of sets.

An **algebraic structure** (algebra) is formed by a set of objects supplemented by a set of operations, which act on the elements of this set and obey certain algebraic laws. Typical example of an algebra are binary operations of addition and multiplication on a set of real, or integer numbers, which combine two elements to produce a third. These operations obey certain laws, such as commutative, associative, and distributive. Another example would be a set of all possible rotations of a solid body, with multiplication defined as combination of two consecutive rotations (Lie algebra, it is associative, but not commutative). The algebra of sets is an algebraic structure consisting of operations on sets (the elements of the set of sets).

Definition. An identity element (or neutral element) with respect to a binary operation on a set is an element of that set, which leaves other elements unchanged when combined with them. An identity with respect to binary addition is called an additive identity (often denoted as 0) and an identity in the case of multiplication a multiplicative identity (often denoted as 1).

Definition. The **empty set** (or **null set**) is the set which contains no objects and is denoted {}, or by the symbol ∅.

Definition. The **universal set** I (the Universe of discourse) is the set which contains all objects of any nature, and of which all other sets are subsets.

In the algebra of sets, the empty set and the universal set play roles of the additive and the multiplicative identity, respectively.

Definition. The set A is said to be a **subset** of the set B if there is no element in A that is not also in B. It is denoted by $A \subset B$, or $B \supset A$.

Exercise. Let A be a finite set, with the number of elements $|A| = n$. How many different subsets does A have (including the empty subset and A itself)?

Comparing sets.

If both statement $A \subset B$ and $B \subset A$ hold, then sets A and B are equal, $A = B$. In this case sets A and B contain exactly the same elements. The relation $A \subset B$ has some similarities with the $a \leq b$ relation between the real numbers. In particular, the following set comparison rules hold:

1. $A \subset A$
2. If $A \subset B$ and $B \subset A$ then $A = B$
3. If $A \subset B$ and $B \subset C$ then $B \subset C$
4. $\emptyset \subset A$ for any set A
5. $A \subset$ I for any set A

The difference between the order relation $A \subset B$ between sets and the $\leq$ relation between real numbers is that for numbers either $a \leq b$, or $a \geq b$ always holds, while this is not necessarily the case for sets order relation.

Definition. The **union** of two sets A and B is the set of elements, which are in A **or** in B **or** in both. It is denoted by $A \cup B$ and is read 'A union B'.

Definition. The **intersection** of two sets A and B is the set of elements, which are in A **and** in B. It is denoted by $A \cap B$ and is read 'A union B'.

We can associate the union with the "logical sum" of sets A and B,

$A \cup B = A + B$,

and the intersection with the "logical product",

$A \cap B = A \cdot B$.

Using these definitions, it can be easily verified that these operations satisfy the following rules.

6. $A + B = B + A$
7. $A \cdot B = B \cdot A$
8. $A + (B + C) = (A + B) + C$
9. $A \cdot (B \cdot C) = (A \cdot B) \cdot C$
10. $A + A = A$
11. $A \cdot A = A$
12. $A \cdot (B + C) = (A \cdot B + A \cdot C)$
13. $A + (B \cdot C) = (A + B) \cdot (A + C)$
14. $A + \varnothing = A$
15. $A \cdot I = A$
16. $A + \mathrm{I} = I$
17. $A \cdot \varnothing = \varnothing$
18. $A \subset B$ is equivalent to either of the two, $A + B = B$, or $A \cdot B = A$

Definition. The **complement** of set A in I is the set A', which consists of all objects in I which are not in A.

The operation of obtaining a complement A' has no analogs in the algebra of numbers, and possesses the following properties.

19. $A + A' = I$
20. $A \cdot \mathrm{A}' = \varnothing$
21. $\varnothing' = I$
22. $I' = \varnothing$
23. $A'' = A$
24. $(A \subset B) \Leftrightarrow (B' \subset A')$
25. $(A + B)' = A' \cdot B'$
26. $(A \cdot B)' = A' + B'$

These 26 laws of the algebra of sets possess an interesting duality symmetry: if we interchange $\subset$ and $\supset$, $+$ and $\cdot$, and $\varnothing$ and I, the same set of rules is obtained. Each of the 26 relations transforms in some other of these relations.

Exercise. Verify the above stated duality.

It is also remarkable from the point of view of the axiomatic constructions that all the above 26 laws, as well as all other theorems of set algebra can be deduced from the following three equation adopted as axioms, much like the Euclidian geometry.

1. $A + B = B + A$
2. $A + (B + C) = (A + B) + C$
3. $(A' + B')' + (A' + B)' = A$

The operations $A \cdot B$ and $A \subset B$ are then defined by: $A \cdot B = (A' + B')'$ and $A \subset B$ means that $A + B = B$.

Exercise. Verify that all 26 rules of the set algebra can be obtained from the three axioms stated above.

Example. An algebraic structure satisfying all laws of the algebra of sets is provided by a set of eight numbers, {1,2,3,5,6,10,15,30}, where addition is identified with obtaining the least common multiple, multiplication with the greatest common divisor, $m \subset n$ to mean "m is a factor of n", and $n' = 30/n$,

- $m + n \equiv LCM(n, m)$
- $m \cdot n \equiv GCD(n, m)$
- $m \subset n \equiv (n = 0 mod(m))$
- $n' \equiv 30/n$.

Exercise. Verify that thus obtained algebra satisfies all rules of set algebra.

We observe that laws of the algebra of sets look similar to the laws of propositional logic and predicate calculus, if we identify

$A \cap B = A \cdot B$, with conjunction (AND), A∧B

$A \cup B = A + B$, with disjunction (OR), A∨B

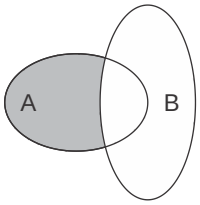
A' with negation (NOT), $\sim A$

$A \supset B$ with $A \Rightarrow B$, $A \subset B$ with $A \Leftarrow B$.

This is because any subset of a universal set can be defined using a predicate.

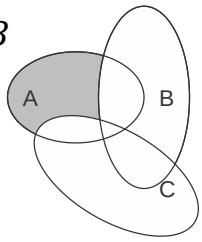
Definition. For two sets A, B, their difference $A - B$ (sometimes notation $A\backslash B$ is used instead of $A - B$) is defined by,

$$A - B \ = \ \{x\colon (x \in A) \wedge (x \notin B)\} = A \cap B'$$



The following properties can be shown to hold (consider Venn diagrams),

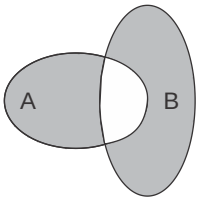
$A - (B \cup C) = \ (A - B) - C$, but in general, $A - (B - C) \neq (A \cup C) - B$



Definition. The symmetric difference of two sets is,

$$A \triangle B = (A - B) \cup (B - A)$$

This operation is commutative and associative,



$$A \triangle B = B \triangle A$$

$$(A \triangle B) \triangle C = A \triangle (B \triangle C)$$

Definition. For a set A, the characteristic function χ_A is defined as follows,

$$\chi_A(x) = \begin{cases} 1, if \ x \in A \\ 0, if \ x \ \notin A \end{cases}$$

Exercise. Show that χ_A has following properties

$$\chi_A = 1 - \chi_{A'}$$

$$\chi_{A \cap B} = \chi_A \, \chi_B$$

$\chi_{A \cup B} = 1 - \chi_{A' \cap B'} = 1 - \chi_{A'} \, \chi_{B'} = 1 - (1 - \chi_A)(1 - \chi_B) = \chi_A + \chi_B - \chi_A \chi_B$

Exercise. Write a formula for $\chi_{A \cup B \cup C}$; $\chi_{A \cup B \cup C \cup D}$.

Recap: Elements of number theory. Eucleadean algorithm and greatest common divisor.

Theorem 1 (division representation).

$$\forall a, b \in \mathbb{Z}, b > 0, \exists q, r \in \mathbb{Z}, 0 \leq r < b: a = bq + r$$

Proof. If a is a multiple of b, then $\exists q \in \mathbb{Z}, r = 0 : a = bq = bq + r$. Otherwise, if $a > 0$, then $\exists q > 0 \in \mathbb{Z} : bq < a < b(q+1)$, and $\exists r = a - bq \in \mathbb{Z} : 0 < r < b$. If $a < 0$, then $\exists q < 0 \in \mathbb{Z} : b(q-1) < a < bq$, and $\exists r = a - b(q-1) \in \mathbb{Z} : 0 < r < b$, which completes the proof.

Definition. A number $d \in \mathbb{Z}$ is a common divisor of two integer numbers $a, b \in \mathbb{Z}$, if $\exists n, m \in \mathbb{Z}: a = nd, b = md$.

A set of all positive common divisors of the two numbers $a, b \in \mathbb{Z}$ is limited because these divisors are smaller than the magnitude of the larger of the two numbers. The greatest of the divisors, d, is called the greatest common divisor (gcd) and denoted $d = (a, b)$.

Definition. Two integers $a, b \in \mathbb{Z}$, are called relatively prime if they have no common divisor larger than 1, i. e. $(a, b) = 1$.

Theorem 2. $\forall a, b, q, r \in \mathbb{Z}, (a = bq + r) \Rightarrow \big((a, b) = (b, r)\big)$

Proof. Indeed, if d is a common divisor of $a, b \in \mathbb{Z}$, then $\exists n, m \in \mathbb{Z}: a = nd, b = md \Rightarrow r = a - bq = (n - mq)d$. Therefore, d is also a common divisor of b and $r = a - bq$. Conversely, if d' is a common divisor of b and $r = a - bq$, then $\exists n', m' \in \mathbb{Z}: b = m'd', a - bq = n'd' \Rightarrow a = (n' + m'q)d'$, so d' is a common divisor of b and a. Hence, the statement of the theorem is valid for any divisor of a, b, and for gcd in particular.

Corollary 1 (Eucleadean algorithm). In order to find the greatest common divisor $d = (a, b)$, one proceeds iteratively performing successive divisions,

$$a = bq + r, (a, b) = (b, r)$$

$$b = rq_1 + r_1, (b, r) = (r, r_1),$$

$$r = r_1 q_2 + r_2, (r, r_1) = (r_1, r_2),$$

$$r_1 = r_2 q_3 + r_3, (r_1, r_2) = (r_2, r_3), \dots, r_{n-1} = r_n q_{n+1}$$

$$b > r_1 > r_2 > r_3 > \cdots r_n > 0 \Rightarrow \exists d \leq b, d = r_n = (a, b)$$

The last positive remainder, r_n, in the sequence $\{r_k\}$ is (a, b), the gcd of the numbers a and b. Indeed, the Eucleadean algorithm ensures that

$$(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_{n-1}, r_n) = (r_n, 0) = r_n = d$$

Examples.

a. $(385,105) = (105,70) = (70,35) = (35,0) = 35$
b. $(513,304) = (304,209) = (209,95) = (95,19) = (19,0) = 19$

Continued fraction representation. Using the Eucleadean algorithm, one can develop a continued fraction representation for rational numbers,

$$\frac{a}{b} = q + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\dots + \cfrac{1}{q_n + \cfrac{1}{q_{n+1}}}}}}$$

This is accomplished by successive substitution, which gives,

$$\frac{a}{b} = q + \frac{r}{b} = q + \frac{1}{\frac{b}{r}}, \frac{b}{r} = q_1 + \frac{r_1}{r} = q_1 + \frac{1}{\frac{r}{r_1}}, \frac{r}{r_1} = q_2 + \frac{1}{\frac{r_1}{r_2}}, \dots, \frac{r_{n-1}}{r_n} = q_{n+1}.$$

Exercise. Show the continued fraction representations for $\frac{385}{105}, \frac{513}{304}, \frac{105}{385}, \frac{304}{513}$.

Example. $\frac{105}{385} = \frac{1}{\frac{385}{105}} = \frac{1}{3+\frac{1}{\frac{105}{70}}} = \frac{1}{3+\frac{1}{1+\frac{1}{\frac{70}{35}}}} = \frac{1}{3+\frac{1}{1+\frac{1}{2}}}$.

Corollary 2 (Diophantian equation). $(d = (a, b)) \Rightarrow (\exists\, k, l \in \mathbb{Z} : d = ka + lb)$

Proof. Consider the sequence of remainders in the Eucleadean algorithm, $r = a - bq\,, r_1 = b - rq_1, r_2 = r - r_1q_2,\ r_3 = r_1\ - r_2q_3, \ldots, r_n = r_{n-2} - r_{n-1}q_n$. Indeed, the successive substitution gives, $r = a - bq\,, r_1 = b - (a - bq\,)q_1 = k_1a + l_1b, r_2 = r - (k_1a + l_1b)q_2 = k_2a + l_2b, , \ldots, r_n = r_{n-2} - (k_{n-1}a + l_{n-1}b)q_n = k_na + l_nb = d = (a, b)$.

It follows that if d is a common divisor of a and b, then equation $ax + by = d$, called the Diophantian equation, has solution for integer $x, y \in \mathbb{Z}$.

Exercise. Find the representation $d = ka + lb$ for the pairs (385,105) and (513,304) considered in the above examples.

Recap: Elements of number theory. Modular arithmetics.

Definition. For $a, b, n \in \mathbb{Z}$, the congruence relation, $a \equiv b \bmod n$, denotes that, $a - b$ is a multiple of n, or, $\exists q \in \mathbb{Z}, a = nq + b$.

All integers congruent to a given number $r \in \mathbb{Z}$ with respect to a division by $n \in \mathbb{Z}$ form congruence classes, $[r]_n$. For example, for $n = 3$,

$$[0]_3 = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$$

$$[1]_3 = \{\ldots, -2, 1, 4, 7, \ldots\}$$

$$[2]_3 = \{\ldots, -1, 2, 5, 8, \ldots\}$$

$$[3]_3 = \{\ldots, -6, -3, 0, 3, 6, \ldots\} = [0]_3$$

There are exactly n congruence classes mod n, forming set Z_n. In the above example $n = 3$, the set of equivalence classes is $Z_3 = \{[0]_3, [1]_3, [2]_3\}$. For general n, the set is $Z_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$, because $[n]_n = [0]_n$.

One can define addition and multiplication in Z_n in the usual way,

$$[a]_n + [b]_n = [a + b]_n$$

$$[a]_n \cdot [b]_n = [a \cdot b]_n$$

$$([a]_n)^p = [a^p]_n, p \in \mathbb{N}$$

Here the last relation for power follows from the definition of multiplication.

Exercise. Check that so defined operations do not depend on the choice of representatives a, b in each equivalence class.

Exercise. Check that so defined operations of addition and multiplication satisfy all the usual rules: associativity, commutativity, distributivity.

In general, however, it is impossible to define division in the usual way: for example, $[2]_6 \cdot [3]_6 = [6]_6 = [0]_6$, but one cannot divide both sides by $[3]_6$ to obtain $[2]_6 = [0]_6$. In other words, for general n an element $[a]_n$ of Z_n could give $[0]_n$ upon multiplication by some of the elements in Z_n and therefore would not have properties of an algebraic inverse, so there may exist elements in Z_n which do not have inverse. In practice, this means that if we try to define an inverse element, $[r^{-1}]_n$, to an element $[r]_n$ employing the usual relation, $[r]_n \cdot [r^{-1}]_n = [1]_n$, there might be no element $[r^{-1}]_n$ in class Z_n satisfying this equation. However, it is possible to define the inverse for some special values of r and n. The corresponding classes $[r]_n$ are called invertible in Z_n.

Definition. The congruence class $[r]_n \in Z_n$ is called invertible in Z_n, if there exists a class $[r^{-1}]_n \in Z_n$, such that $[r]_n \cdot [r^{-1}]_n = [1]_n$.

Theorem. Congruence class $[r]_n \in Z_n$ is invertible in Z_n, if and only if r and n are mutually prime, $(r, n) = 1$. Or, $\forall [r]_n, (\exists [r^{-1}]_n \in Z_n) \Leftrightarrow \big((r, n) = 1\big)$.

To find the inverse of $[a] \in Z_n$, we have to solve the equation, $ax + ny = 1$, which can be done using Eucleadean algorithm. Then, $ax \equiv 1 \bmod n$, and $[a]^{-1} = [x]$.

Examples.

3 is invertible mod 10, i. e. in Z_{10}, because $[3]_{10} \cdot [7]_{10} = [21]_{10} = [1]_{10}$, but is not invertible mod 9, i. e. in Z_9, because$[3]_9 \cdot [3]_9 = [0]_9$.

7 is invertible in Z_{15}: $[7]_{15} \cdot [13]_{15} = [91]_{15} = [1]_{15}$, but is not invertible in Z_{14}: $[7]_{14} \cdot [2]_{14} = [14]_{14} = [0]_{14}$.