# Lecture 3. Algebra

We have learnt about sets and numbers. One of the main things we learn about numbers are operations such as $+, \times$. We will find many number systems useful. First we need a standard way to thing when two items are equal.

**Definition.** Let $A$ be a non-empty set. A relation $R$ is a subset of $A \times A$ $(= \{(a,b) \mid a \in A, b \in A\})$

Example: All functions $f: A \to A$ can be considered to be relations. Consider $\{(a,b) \mid f(a) = b\}$. This is a relation with an additional requirement that $a_1 = a_2 \Rightarrow f(a_1) = f(a_2)$ (well-defined)

- If $(a,b) \in R \subset A \times A$, we say $aRb$ – $a$ is related to $b$.
- Often we use $a \sim b$ for $\sim$ is a relation.
- We refer to $\sim$ as a binary relation on $A$

**Def (Equivalence Relation).** A binary relation $\sim$ on $A$ is called an equivalence relation on $A$ if

1. $a \sim a$ for all $a \in A$ (reflexive)
2. if $a \sim b$ then $b \sim a$ (symmetric)
3. if $a \sim b$ and $b \sim c$ then $a \sim c$. (transitive).

All these conditions hold for all the '$=$' relations we have defined so far.

- Works for $\mathbb{N}$?
- $A \times B$: $(a_1, b_1) = (a_2, b_2)$ if $a_1 = a_2, b_1 = b_2$. Works?
- $A, B$ sets: $A = B$ if $A \subset B$ and $B \subset A$. Works? (Binary relation on $\mathcal{P}(X)$) — power set of universal set

**Def.** A binary operation on $A$ is a function from $A \times A \to A$.
We use symbols such as $+, \cdot, *, \times, \cdot, \oplus, \otimes$ to denote binary ops. (nothing!)

An algebraic system (my term) will consist of a set and one or more such operations satisfying certain axioms (rules).

- In general we can also have operations such as
  $* : A \times B \to B$ or $A \times B \to A$
- Algebraic systems satisfy one or more of the following axioms

① Associative law: $a*(b*c) = (a*b)*c$
② Commutative law: $a*b = b*a$
③ Existence of identity: $I*b = b*I = b$
④ Existence of inverse: For all $a$, there is a $a^{-1}$ s.t. $a*a^{-1} = a^{-1}*a = I$.
⑤ Distributive laws: Given 2 operations $\oplus, *$
$$a*(b \oplus c) = (a*b) \oplus (a*c)$$

⑥ Order relations: Other than an equality relation we can have an $<$ satisfying

- one of $a = b$, $a < b$ or $a > b$: TRICHOTOMY
- $a < b$ and $b < c \Rightarrow a < c$
- if $a < b$ then $a + c < b + c$ for any $c$
- Variations: $a < b$, $c > 0$ then $ac < bc$
  eg.

- Completely ordered sets / partially ordered sets. (posets (we will study them later)).

$\mathbb{N}$: $+, \times$

$+$: Associative ✓
commutative ✓
identity. ✗ (but $\mathbb{N}_0$ has)

$\times$: Associative ✓
mult ✓
identity: yes. $1$
inverse: No $2^{-1} = ?$ Not in $\mathbb{N}$.

Distributive ✓
order ✓

Note: Multiplicative inverse allows for division, inverse of multiplication additive inverse is subtraction.
When operation is $+ \to$ we use $0, -$
$\times \to$ $1, a^{-1}$ or $\div$

**Thm** (Well ordering Principle). Let $S$ be a non-empty subset of $\mathbb{N}$. Then $S$ has a least element; ie, there is an $x \in S$ s.t. $x \leq n$ for all $n \in S$.

- WOP – Also for $\mathbb{N}_0$.

**Proof:** Let $P = \mathbb{N} \setminus S = \{n \in \mathbb{N} \mid n \notin S\}$

We claim $P = \mathbb{N}$ so $S$ has to be empty, so its a contradiction. Assume $S$ has no least element.

- This proof is an example of proof by contradiction. We begin with a statement $P$, and show it leads to a statement of the form $Q$ and NOT $Q$. This is not allowed. (why?).

The proof is by induction.
Clearly $1 \in P$. Otherwise it would be the least element. Let $k \in P$.
Now $2 \in P$. Otherwise it would be least
Carry on in this fashion and suppose we reach $k \in P$.
Then we claim $k+1 \in P$. Otherwise $k+1 \in S$, $1, 2, \ldots, k-1, k \notin S$, so $k+1$ is least element of $S$.
So $P = \mathbb{N}$ and thus $S = \phi$. $\rightarrow\leftarrow$ symbol for contradiction
$\square$.

**Remark:** From the argument above, we see the following. "stronger form" of induction.

**Prop:** (PMI - stronger form). Let $S \subseteq \mathbb{N}$ s.t.
(1) $1 \in S$
(2) $1, 2, 3, \ldots, k \in S \Rightarrow k+1 \in S$.
Then $S = \mathbb{N}$.

**Proof:** It's obvious from PMI

$P \Rightarrow Q$ and $Q \Rightarrow P$.

**Remark:** In fact PMI (both forms) and WOP are equivalent. mean same thing.

- $\mathbb{N}$. $a, b \in \mathbb{N}$, $a + b \in \mathbb{N}$.
- $\mathbb{N} \cup \{0\}$ has $0$ but no $-$
- multiplication is there
- No inverses but we can divide and do reverse process partially.

$\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$ ↑ has $-, 0$.

**Def.** (Division) We say $d \mid n$ ($d$ divides $n$ / $d$ is a divisor of $n$) if there is an integer $m$ s.t. $n = d \times m$. (factor)

**Thm** (Division algorithm) Given $n, m \in \mathbb{N}$, there are numbers $q$ and $r$ s.t. $n = mq + r$ and
either $r = 0$ or $0 < r < m$.

**Proof:** Let $S = \{n - mq \in \mathbb{N} \mid q \in \mathbb{N}_0\}$.
$S \neq \phi$ since $n \in S$.
By WOP, it has a least element, say $r$.
Then $n = mq + r$.
Now $r = 0$ or $r \neq 0$.
If $r > 0$ then claim $r < m$. If not, so $r = m + r'$, and $r' < r$.
Then $n = mq + m + r'$
$= m(q+1) + r'$. $\rightarrow\leftarrow$ to $r$ being least in $S$.
So $n = mq + r$, where $r = 0$ or $0 < r < m$. $\square$

**Examples:** ① Say $n = 5$ $m = 7$, $S = \{5\}$ $r = 5$; $5 = 0 \cdot 7 + 5$
② $n = 17$ $m = 5$ → Calculation: find $\min(S)$.
OR
$17 - 5 = 12$
$12 - 5 = 7$
$7 - 5 = 2 < 5$ so is remainder.

$n = 17$ $m = 5$

| $r$ | $q$ |
|---|---|
| 17 | 0 |
| 12 | 1 |
| 7 | 2 |
| $r$ 2 | 3 $q$ |
| $-3$ ← stop if it becomes $< 0$. | |

Assuming you know how to subtract, you can teach a computer to divide.

Ex. Show WOP $\Rightarrow$ PMI.
($P \Rightarrow Q$ is same as IF $P$ THEN $Q$).