Notes on my portion of CC 2 (Algebra)

SB (Subhasundar Bandyopadhyay)
Deptt. of Mathematics, GGDC

Books that are to be followed:

1. Higher Algebra (Abstract and Linear) - S. K. Mapa
2. Higher Algebra (Classical) - S. K. Mapa
3. Advanced Higher Algebra - J. G. Chakravorty & P. R. Ghosh
4. Linear Algebra - K. Hoffman & R. Kunze
5. Elementary Number Theory - D. M. Burton

The portion of the syllabus we start with is:

[Unit-2 • Well-ordering property of positive integers, Principles of Mathematical induction, division algorithm, divisibility and Euclidean algorithm. Prime numbers and their properties, Euclid's theorem. Congruence relation between integers. Fundamental Theorem of Arithmetic. Chinese remainder theorem. Arithmetic functions, some arithmetic functions such as ϕ, τ, σ and their properties.]

But before that I think, it would be better to start with this portion:

[Unit-2 • Relation: equivalence relation & partition, partial order relation, poset, linear order relation]. as this portion is familiar to you in your H.S. course.

1. Relation (Definition): Let $S \neq \phi$ (null set). If $R \subset S \times S$ then R is said to be a relation on S.

Example 1.1: Let $S = \{a, b, c\}$. ~~Here $S \times S = \{\phi, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, S\}$~~

~~$R = \{(a, a)$~~

Here $S \times S = \{(a,a), (a,b), (a,c), (b,a), (b,b), (b,c), (c,a), (c,b), (c,c)\}$

$R = \{(a,a), (b,b), (b,a), (a,b)\}$ is a relation on S.

Note 1 : We use the notation $\mathbb{N}$ and $\mathbb{Z}$ for the set of all positive integers or natural numbers and the set of all integers respectively.

Note 2 : Let $o(S) = n$ ($o(S)$ is the number of elements in S). Then $o(S \times S) = n^2$. So, number of subsets of $S \times S$ is 2^{n^2}. So we can define a relation on S for each subset of $S \times S$. So, we can define 2^{n^2} relation on S. ϕ is called the null relation and $S \times S$ is called the universal relation on S.

Note 3 Let R be a relation on S. If $(a,b) \in R$ then a is said to be related to b and is expressed by the symbol aRb. If $(a,b) \notin R$ then a is said to be not related to b and is expressed by $a \not R b$.

Example 2 : Let R be a subset of $\mathbb{Z} \times \mathbb{Z}$ given by $R = \{(x,y) \in \mathbb{Z} \times \mathbb{Z} : x+y \text{ is even}\}$. Then R is a relation on $\mathbb{Z}$

Here $1R3$ but $2 \not R 3$

Example 3 : Let R be a subset of $\mathbb{Z} \times \mathbb{Z}$ given by. $R = \{(x,y) \in \mathbb{Z} \times \mathbb{Z} : x-y \text{ is divisible by } 3\}$. R is a relation on $\mathbb{Z}$. $5R2$ but $5 \not R 3$

1.1. Equivalence relation (Definition) : Let $S \neq \phi$ and R be a relation on S.

The relation R is said to be

(i) reflexive if aRa for all $a \in S$

(ii) ~~symmetric~~ symmetric if $aRb \Rightarrow bRa$ for $a, b \in S$

(iii) transitive if $aRb, bRc \Rightarrow aRc$ for $a, b, c \in S$.

R is said to be an equivalence relation on S if R is reflexive, symmetric and transitive

Examples : 1. A relation R on $\mathbb{Z}$ is defined by aRb if and only if $a-b$ is divisible by 5 i.e., $R = \{(x,y) \in \mathbb{Z}\times\mathbb{Z} : x-y \text{ is divisible by } 5\}$. Examine if R is an equivalence relation on $\mathbb{Z}$

Solution : Let $a \in \mathbb{Z}$. Then $a-a = 0 = 0.5$. So $a-a$ is divisible by 5. So, aRa $\forall a \in \mathbb{Z}$ ($\forall$ means for all). So R is reflexive.

Let $a, b \in \mathbb{Z}$ and aRb. Then $a-b$ is divisible by 5. So, $\exists$ ($\exists$ means there exists) an integer k such that $a-b = 5k$. So, $b-a = 5(-k)$ and $-k \in \mathbb{Z}$. So, $b-a$ is divisible by 5. So, bRa. Hence, R is symmetric.

Let $a, b, c \in \mathbb{Z}$ and aRb and bRc. So, $\exists$ $k_1, k_2 \in \mathbb{Z}$ such that $a-b = 5k_1$, $b-c = 5k_2$.

So, $a-c = a-b+b-c = 5k_1 + 5k_2 = 5(k_1+k_2) = 5k$ where $k = k_1+k_2 \in \mathbb{Z}$. So, $a-c$ is divisible by 5. So, aRc. Hence R is transitive. Hence R is an equivalence relation on $\mathbb{Z}$.

Home work : HW1 : Let m be a fixed positive integer. Show that ~~R = {(x,y) : x-y is divisible by m}~~ $R = \{(x,y) \in \mathbb{Z}\times\mathbb{Z} : x-y \text{ is divisible by } m\}$ is an equivalence relation

Note : R in HW1 is called the relation of congruence (mod m)

HW2 : Let $R = \{(x,y) \in \mathbb{Z}\times\mathbb{Z} : xy > 0\}$. Examine R is (i) reflexive, (ii) symmetric and (iii) transitive.

1.2 Equivalence classes (Definition) : Let R be an equivalence relation on a non-empty set S. ~~The~~ Let $a \in S$. The subset $\{x \in S : xRa\}$ of S is said to be equivalance class of a and denoted by $\bar{a}$ or $cl(a)$. So,

$cl(a) = \{x \in S : xRa\}$ is the equivalence class of a.

$cl(a) \neq \phi$ as $a \in cl(a)$

For example, in Example 1 of Page-3,

$$cl(0) = \{0, \pm 5, \pm 10, \cdots\}$$

<u>Theorem 1.2.1</u> Let R be an equivalence relation on a non-empty set S. and $a, b \in S$. Then $cl(a) = cl(b)$ if and only if aRb

[Note: If p, q be two statements then p if and only if q means $p \Leftrightarrow q$ i.e., $p \Rightarrow q$ and $q \Rightarrow p$

So, $cl(a) = cl(b)$ (statement p) $\Rightarrow aRb$ and

aRb (statement q) $\Rightarrow cl(a) = cl(b)$.]

Proof: Let $cl(a) = cl(b)$. Let $x \in cl(a) = cl(b)$

So, xRa and xRb. So, aRx and xRb as R is symmetric.

So, aRb as R is transitive.

Conversely, let aRb. Let $x \in cl(a)$

$\Rightarrow xRa$ and as aRb. So xRb as R is transitive.

So, $x \in cl(b) \Rightarrow cl(a) \subset cl(b)$

Similarly, $cl(b) \subset cl(a)$. So, $cl(a) = cl(b)$

Hence $cl(a) = cl(b)$ if and only if aRb