Seminar Nr1 – 916

Algebra

→ the study of algebraic structures

$$(\underbrace{S}_{\text{set}}, \underbrace{*, \cdot, \ldots}_{\text{operations}})$$

- $*$ (binary) operation on a set S $\Leftrightarrow$ $*: S \times S \to S$, $(x, y) \mapsto x * y$

  → internal law

- If $*$ operation on S and $A \subseteq S$, then:

  A <u>stable part</u> of S if: $\forall x, y \in A: x * y \in A$

<u>Ex.</u> of algebraic structures: monoids, groups, rings, fields
(+ vector spaces)

Def: $(G, *)$ group if:

- $*$ is an operation: $\forall x, y \in G : x * y \in G$
- associativity: $\forall x, y, z \in G : (x * y) * z = x * (y * z)$

Semigroup

- neutral element: $\exists e \in G \ \forall x \in G : x * e = e * x = x$

monoid

Semigroup (monoid)

- invertibility: $\forall x \in G \ \exists x' \in G : x * x' = x' * x = e$

(+ Commutativity: $\forall x, y \in G : x * y = y * x$)

$\hookrightarrow$ abelian group

3. Decide which ones of the numerical sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are groups together with the usual addition or multiplication.

Sol.:

	$\mathbb{N}$	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}$	$\mathbb{C}$
$+$	No	Yes	Yes	Yes	Yes
$\cdot$	No	No	No	No	No

5. Let "$*$" be the operation defined on $\mathbb{N}$ by $x * y = \text{g.c.d.}(x, y)$.

(i) Prove that $(\mathbb{N}, *)$ is a commutative monoid.

(ii) Show that $D_n = \{x \in \mathbb{N} \mid x/n\}$ ($n \in \mathbb{N}^*$) is a stable subset of $(\mathbb{N}, *)$ and $(D_n, *)$ is a commutative monoid.

$x \mid n \iff n \vdots x$

(iii) Fill in the table of the operation "$*$" on D_6.

(You can use the fact that $\gcd(\gcd(x,y), z) = \gcd(x, \gcd(y,z))$) ($\star$)

Sol.:

(i) $\forall x, y \in \mathbb{N}$: $\gcd(x,y) \in \mathbb{N} \Rightarrow *$ operation on $\mathbb{N}$

Associativity is proven by ($\star$)

If e is a neutral element
$\gcd(x, e) = x \Rightarrow x \mid e \Rightarrow e = x$

We check that $e = 0$.

$\forall x \in \mathbb{N}: \quad \gcd(x, 0) = x$

$\forall x, y \in \mathbb{N}: \quad x * y = \gcd(x, y) = \gcd(y, x) = y * x$

<u>Remark</u>: $n \in \mathbb{N}, \quad n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$

$\forall p$ prime we define $v_p(n) =$ the power of p in the factorization of n

in our case: $v_{p_1}(n) = \alpha_1, \ldots, v_{p_n}(n) = \alpha_n$

$\forall p \neq p_1, \ldots, p_n: \quad v_p(n) = 0$

- $v_p(ab) = v_p(a) + v_p(b)$

$v_p(a+b) \geq \min(v_p(a), v_p(b))$

$v_p(\gcd(a, b)) = \min(v_p(a), v_p(b))$

(ii) $(D_n, *)$ stable subset of $(\mathbb{N}, *)$?

$\forall x, y \in D_n: \quad \gcd(x, y) \overset{?}{\in} D_n$

We know $x \mid n$, $y \mid n$, we want to show that $\gcd(x, y) \mid n$

$$\left[\begin{array}{l} \text{if } a \mid b \text{ and } b \mid c \Rightarrow a \mid c\ ? \\ \left.\begin{array}{l} a \mid b \Rightarrow b = a \cdot k,\ k \in \mathbb{Z} \\ b \mid c \Rightarrow c = b \cdot m,\ m \in \mathbb{Z} \end{array}\right\} \Rightarrow c = a \underbrace{km}_{\in \mathbb{Z}} \Rightarrow a \mid c \end{array}\right]$$

$\gcd(x,y) \mid x,\ x \mid n \Rightarrow \gcd(x,y) \mid n \Rightarrow$

$\Rightarrow \gcd(x,y) \in D_n \Rightarrow (D_n, \ast)$ stable part

$(D_n, \ast)$ commutative monoid ?

The associativity and commutativity are inherited from $(\mathbb{N}, \ast)$

$0 \notin D_n \Rightarrow$ we need to look for another neutral element.

We can see that $\forall x \in D_n$:

$$x \ast n = n \ast x = \gcd(x, n) \overset{x \mid n}{=} x$$

$\Rightarrow n$ is the neutral element in $(D_n, \ast)$

(iii) $D_6 = \{1, 2, 3, 6\}$

$\ast$	1	2	3	6
1	1	1	1	1
2	1	2	1	2
3	1	1	3	3
6	1	2	3	6

7. Let $(G, \cdot)$ be a group. Show that:
(i) G is abelian $\Longleftrightarrow \forall x, y \in G$, $(xy)^2 = x^2y^2$.
(ii) If $x^2 = 1$ for every $x \in G$, then G is abelian.

Sol.: (i) "$\Rightarrow$" $\forall x, y \in G$: $(xy)^2 = x\underbrace{yx}_{=xy}y = x^2y^2$

"$\Leftarrow$" $(xy)^2 = xyxy = x^2y^2$

$x^{-1} \mid xyxy = x^2y^2 \mid \cdot y^{-1}$

$\Rightarrow yx = xy \Rightarrow G$ abelian

(ii) Let $x, y \in G \Rightarrow (xy)^2 = 1$
$x^2 = y^2 = 1$ $\Bigg\} \Rightarrow (xy)^2 = x^2y^2 \Rightarrow$
$\overset{(i)}{\Rightarrow}$ G abelian