SUMMER SEMINAR: ANALYSIS
Preliminary Concepts

Monoids, Groups, Rings, Integral Domains and Fields

Def: Let S be a non-empty set and let $*$ be an associative binary operator on S. If there exists an element $e \in S$ so that

$$\forall x \in S \left(x * e = e * x = x \right)$$

then $\langle S, *, e \rangle$ is a called a **monoid** and e is called an **identity element** for $*$ on S.

Thm: Identity elements of monoids are unique. I.e. if e_1 and e_2 are both identity elements of a monoid S, then $e_1 = e_2$.

Def: Let $\langle S, *, e \rangle$ be a monoid. If the following holds:

$$\forall x \in S \left(\exists y \in S \left(x * y = e \right) \right)$$

then $\langle S, *, e \rangle$ is called a **group** and for each such y, it is called an **operational inverse** of x.

Thm: Operational inverses are unique for each element in a group. I.e. If y_1 and y_2 are both operational inverses of an element x, then $y_1 = y_2$.

Def: If in a group S, the following holds:

$$\forall x, y \in S \ (x * y = y * x)$$

then S is called a **commutative** group (also alternatively an **Abelian** group).

Def: We say $\langle S, +, \times, 1 \rangle$ is a **ring** if

1) $\langle S, + \rangle$ is a commutative group.
2) $\langle S, \times, 1 \rangle$ is a multiplicative monoid.
3) $\forall a, b, c \in S \left(\left(a \times (b + c) = (a \times b) + (a \times c) \right) \wedge \left((b + c) \times a = (b \times a) + (c \times a) \right) \right)$

Def: If $\forall x, y \in S \ (x \times y = y \times x)$ then S is called a **commutative ring**.

Def: A group or ring is said to be **trivial** if and only if $S = \{e\}$ where e is the operational identity for both $+$ and $\times$.

Def: For any non-trivial ring S, elements $a, b \in S$ are called **zero-divisors** of S if:

$$(a \neq 0) \wedge (b \neq 0) \wedge (a \times b = 0).$$

Def: A non-trivial commutative ring $\langle S, +, \times, 0, 1 \rangle$ is called an **integral domain** if it contains no zero-divisors.

Thm: If S is an integral domain then $\forall x, y \in S, \left(\frac{(x \times y = 0)}{(x = 0) \vee (y = 0)} \right)$.

Def: A non-trivial commutative ring $\langle S, + \ \times, 0, 1\rangle$ is called a **field** if every non-zero element has a multiplicative inverse, i.e.

$$\forall x \in S \left(\frac{x \neq 0}{\exists y \in S \ (x \times y = 1)}\right)$$

Thm: Multiplicative inverses are unique. I.e. if z_1 and z_2 are both inverses of an element x then $z_1 = z_2$.

Thm:

(1) All fields are integral domains.
(2) $\mathbb{N}$ is an additive and multiplicative monoid.
(3) $\mathbb{Z}$ is an integral domain.
(4) $\mathbb{Q}$ and $\mathbb{R}$ are fields.

Integer Intervals and Correspondent Sets

Def: For $a, b \in \mathbb{Z}$, $a..b \coloneqq \{n \in \mathbb{Z} \mid a \leq n \leq b\}$. This is the **integer interval** from a to b.

Note that:

(1) $a..a = \{a\}$.
(2) $a..b = \{\ \}$ when $b < a$. In particular $1..0 = \{\ \}$.

Def: Two sets, A and B are said to be **correspondent** if there exists a bijection from one to the other and we write $A \simeq B$.

Thm:

(1) If there exists an injection from A into B and an injection from B into A, then $A \simeq B$.
(2) If there exists a surjection from A onto B and a surjection from B onto A, then $A \simeq B$.

Thm: Correspondence of sets is an equivalence relation on $\mathrm{Pwr}(\mathcal{U})$. I.e.:

(1) $\forall S \subseteq \mathcal{U} \ (S \simeq S)$.
(2) $\forall S, T \subseteq \mathcal{U} \left(\frac{S \simeq T}{T \simeq S}\right)$.
(3) $\forall S, T, W \subseteq \mathcal{U} \left(\frac{(S \simeq T) \wedge (T \simeq W)}{S \simeq W}\right)$.

Thm:

(1) $\mathbb{N} \simeq \mathbb{Z} \simeq \mathbb{Q}$.
(2) $\mathbb{Q} \not\simeq \mathbb{R}$.

Thm: Suppose S and T are both algebraic structures (of some type H). If S and T are H-isomorphic, then S and T are correspondent (as sets).

Finiteness, Infiniteness, Cardinality, Countability and Denumeration

Def: A set A is said to be **finite**, $Fnt(A)$, If there exists an integer $n \geq 0$ where $A \simeq 1..n$. Note that if $n = 0$, then A is empty. In any case, the **cardinality** of A, written $|A|$ (or $\nu(A)$), is defined to be n. Symbolically:

$$Fnt(A) :\Leftrightarrow \exists n \in \mathbb{N}\ (A \simeq 1..n)$$
$$Fnt(A) \Rightarrow (|A| \coloneqq n)$$

Def: Any set A that is not finite is said to be **infinite**, $\cancel{Fnt}(A)$.

Def: Let $\mathcal{F}$ be the set of all finite sets. I.e.: $\mathcal{F} \coloneqq \{A \subseteq \mathcal{U} \mid Fnt(A)\}$. Note then $Fnt(A) \Leftrightarrow (A \in \mathcal{F})$.

Thm: $\forall n \in \mathbb{N}\ (|1..n| = n)$. Moreover $\forall a, b \in \mathbb{Z}, \left(|a..b| = \begin{cases} b - a + 1, & \text{if } a \leq b \\ 0, & \text{if } b < a \end{cases}\right)$.

Def: If there exists a surjective function from $\mathbb{N}$ onto a set A, then A is called a **countable** set, $Cntbl(A)$. If A is also infinite, then A is said to be **countably infinite**.

Def: A function ϕ that is a bijection from either the integer interval $1..n$ for some $n \in \mathbb{N}$ or from $\mathbb{N}$ itself to a set A, then ϕ is called a **denumeration** of A.

Thm: There exists a denumeration for every countable set. (Countable sets are therefore often called **denumerable** sets.)

Thm:

(1) $\mathbb{N}, \mathbb{Z}$ *and* $\mathbb{Q}$ are countably infinite.
(2) $\mathbb{R}$ is infinite but not countable.
(3) $|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| < |\mathbb{R}|$.
(4) $\forall A \subseteq \mathcal{U} \left(\dfrac{|A| < |\mathbb{N}|}{Fnt(A)}\right)$ (double line)
(5) $\forall A \subseteq \mathcal{U} \left(\dfrac{\cancel{Fnt}(A) \wedge Cntbl(A)}{A \simeq \mathbb{N}}\right)$ (double line)

Thm: Every infinite set includes a countably infinite subset.

Thm [Galileo]: If there exists an injective function that is not surjective from a set into itself, then A is infinite. Symbolically:

$$\left(\frac{\exists \phi \in Fnct(A, A)\ \left(Inj(\phi) \wedge \cancel{Srj}(\phi)\right)}{\cancel{Fnt}(A)}\right)$$

Thm:

(1) $\forall A, B \subseteq \mathcal{U} \left(\dfrac{|A| = |B|}{|\mathrm{Pwr}(A)| = |\mathrm{Pwr}(B)|}\right)$. (double line)
(2) $\forall A, B \subseteq \mathcal{U} \left(\dfrac{A \simeq B}{|A| = |B|}\right)$ (double line)
(3) $\forall A \subseteq \mathcal{U} \left(|A| < |\mathrm{Pwr}(A)|\right)$.

Thm: $\mathrm{Pwr}(\mathbb{Q}) \simeq \mathbb{R}$.

Order and Density

Def: A partially ordered set $\langle S, \precsim \rangle$ is said to be a (**linearly**) **ordered set** if

$$\forall a, b \in S \left((a \precsim b) \vee (b \precsim a) \right).$$

Def: We say a linearly ordered set S with more than 1 element is (**order-wise**) **dense** in a linearly ordered set T if

$$(S \subseteq T) \wedge \left(\forall x, y \in T \left(\frac{(x \prec y)}{\exists z \in S \left(x \prec z \prec y \right)} \right) \right)$$

where $x \prec y$ is the strict order corresponding to $\precsim$. We write $Dns(S, T)$.

Def: Any set A that is dense in itself is called an (**order-wise**) **dense set,** $Dns(A)$.

Thm:

1) Both $\mathbb{Q}$ and $\mathbb{R}$ are (order-wise) dense sets.
2) $\mathbb{Q}$ is (order-wise) dense in $\mathbb{R}$.
3) $\mathbb{Z}$ is not (order-wise) dense. (e.g. there is no integer between 0 and 1.)

Thm: $\forall S, T \subseteq \mathcal{U}$:

(1) If S is (order-wise) dense in T, then $|\mathbb{N}| \leq |S| \leq |T|$.

(2) $\left(\frac{\exists S \subseteq T \left(Dns(S, T) \right)}{Dns(T)} \right)$.

(3) $\left(\frac{(S \subseteq T) \wedge \cancel{Dns}(T)}{\cancel{Dns}(S)} \right)$.

Thm:

(1) All dense sets are infinite.

(2) All infinite fields are dense.

Thm:

(1) If S is a linearly ordered field and ϕ is a field-isomorphism from S to T, then T is linearly ordered.

(2) All dense sets include a subset that is order-isomorphic to $\mathbb{Q}$.

(3) All infinite fields T include a dense subset S (in S and T) that is field-isomorphic to $\mathbb{Q}$.

Note: The set of irrational real numbers, $\mathbb{I}$, is not a field (since it has neither an additive nor a multiplicative identity). It is however an ordered, dense subset of $\mathbb{R}$. Its **arithmetic closure** (i.e. the smallest field containing $\mathbb{I}$) is $\mathbb{R}$.

Thm:

(1) $\forall x, y \in \mathbb{Q} \left((x < y) \Rightarrow \exists \alpha \in \mathbb{I} \left(x < \alpha < y \right) \right)$.

(2) $\forall \alpha, \beta \in \mathbb{I} \left((\alpha < \beta) \Rightarrow \exists x \in \mathbb{Q} \left(\alpha < x < \beta \right) \right)$.