Group theory → Definition, order, infinite group where every element is of finite order.

definition of cyclic group, subgroup of a cyclic group.

proof that $(\mathbb{Q}, +)$ is not cyclic where

Contradiction

$$(\mathbb{Q},+) = \langle p/q \rangle$$

$$G = \{na : n \in \mathbb{Z}\} = \langle a \rangle$$

$$\therefore \frac{p}{2q} = n \cdot p/q$$

$\therefore n = 1/2$ but $n$ is integer so contradiction

Proof that $(\mathbb{R},+)$ is cyclic or not.

→ Subgroup of a cyclic group is cyclic.

As $(\mathbb{Q},+)$ is not cyclic so $(\mathbb{R},+)$ is not cyclic.

Proof of Lagrange's theorem, normal subgroup definition, example.

Q. Let $H$ and $K$ be two normal subgroup of a group $G$ if $H \cap K = \{e\}$ then show that $ab = ba$ $\forall$ $a \in H$ and $b \in K$.

Let $a \in H$, $b \in k$

$\underline{aba^{-1}b^{-1}} \in H \cap k = \{e\}$.

$$aba^{-1}(b^{-1}b) = eb = b$$

$$\Rightarrow aba^{-1}a = ba$$

$$\Rightarrow aba^{-1}a = ba$$

$$= \boxed{ab = ba}$$

$\Rightarrow$

we need to show $aba^{-1}b^{-1} \in H \cap k$.

$\therefore$ Let $a \in H$, $b \in k \subseteq G$

$a \in H \rightarrow b^{-1} \in k$

$aba^{-1} \in k$

$aba^{-1}b^{-1}$

For $G$ if ~~ab=ab~~ $a = a^{-1}$ $\forall a \in G$ then $ab = ba$.

Let $a, b \in G$ then $a = a^{-1}$, $b = b^{-1}$

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba.$$

Let $G$ be a group then for every non identity element of $G$ is of order 2. then $G$ is commutative.

Centre of group, quotient group, isomorphism.

~~[illegible]~~

Ring

$\boxed{\text{Boolean ring}}$

$a^2 = a$, $a \to$ idempotent element.

If every element of ring is idempotent then that ring becomes boolean ring.

$\mathbb{Z}_2$ is a boolean ring.

$(P(X), \Delta, \cap) \to$ ~~[illegible]~~ boolean ring.

$A + B = A \Delta B$

$AB = A \cap B$

$|P(x)| = 2^n$

$A = B, \; A^2 = A \cap A = A$

## Characteristics of a ring

Let $(R, +, \cdot)$ be a ring

$\exists n \in N, \; na = 0 \;\; \forall a \in R$

$Ch(R) = n$

$Z_n = \{[0], \ldots [n-1]\}$

$n[a] = [0] \;\; \forall [a] \in Z_n$

If a ring does not have characteristis then it is ring of zero characteristic

e.g. $(Z, +, \cdot)$.

~~Characteri~~

Characteristic of a boolean ring is always 2.

Every boolean ring is commutative.

$a^2 = a$

Let $a \in B$

$-a \in B$

$\therefore a^2 = a$

$(-a)^2 = -a$

$\Rightarrow (-a)(-a) = a^2$

$a^2 = a$

$\therefore a = -a$

$2 \quad a =$

$\Rightarrow 2a = 0$

$\therefore ch(B) = 2.$

Every boolean ring is commutative.

We have to show $ab = ba$.

$(a+b)^2 = a^2 + ab + ba + b^2$

$(a+b)^2 = a+b$

$\Rightarrow a^2 + ab + ba + b^2 = a+b$

$\Rightarrow a + ab + ba + b = a + b$

$\Rightarrow ab = -ba$

$\Rightarrow ab = (-b)a$

$\Rightarrow ab = ba$

Characteristic

As, $2b = 0$

$\Rightarrow b = -b$

Liked

Prime no | $p > 1$

2 is the only even integer which is prime.

For $n \geq 2$, every $n$ can be split into prime factors.

# Prove no of primes is infinite.

If possible no of primes are finite.

$P_1 \; P_2, \ldots P_n$

$n = P_1 P_2 \cdots P_n + 1 \geq 2$

$P_i \mid n = P_1 P_2 \ldots P_n + 1$

$f(n) = n^2 + n + 13 \quad n \in \mathbb{N}$

is not prime.

$f(n) = n^3 - 1 = (n-1)(n^2+n+1)$

$1 \mid n^3 - 1$

$n^2+n+1 > 1$

$\therefore n - 1 = 1$

$\Rightarrow n = 2$

Fermat's little theorem

If $p \to$ prime no then $a^{p-1} \equiv 1 \pmod{p}$

~~Agg~~

Again $a^p \equiv a \pmod{p}$.

$$p(n) = \begin{cases} m < n \\ \end{cases}$$

For any integer $n$, $\frac{n^7}{7} + \frac{n^3}{3} + \frac{11n}{21}$ is an integer

$$\Rightarrow \frac{n+7r}{7} + \frac{n+3t}{3} + \frac{11n}{21}$$

$a^7 \equiv a \pmod{7} = a^7 - a = 7r \Rightarrow a^7 = a + 7r$

$a^3 \equiv a \pmod{3} \Rightarrow a^3 - a = 3t \Rightarrow a^3 = a + 3t.$