Abstract algebra

Thursday, 16. September 2021 13:20

Subgroup

Chain of inclusions of group

$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ under ordinary addition

integers rational real complex

a+b+c

1) $(a+b)+c = a+(b+c)$ Associativity
2) $a+e=a$ $e=0$ identity
3) $a+a^{-1}=0$ $a^{-1}=-a$ inverse.

$a+b$ add two integers compatible

Definition:
Let G be a group, H be a subset of G.

We say H is a subgroup of G if the multiplication and inverse make H into a group

H is a subset of G.
$H \times H \not\subset G$

Example: 1) G: integers. H. odd number. $H \subset G$.

$a, b \in H$, $a+b =$ even number $\notin H$ H is not a subgroup of G.

2). H: natural numbers.

$a, b \in H$ $a+b \in H$ $a + (a^{-1}) =$ identity $= 0$
$-a \notin H$.

Definition:
Let G be a group. S be a subset of G

S is closed under multiplication if whenever $a, b \in S$, the product of a, b is in S

S is closed under taking inverses if $\cdot\cdot$ $a \in S$, inverse of a is in S inversion

Example: even numbers (integers) is closed under multiplication and taking inverses

odd numbers is closed under taking inverses.

natural numbers is closed under addition.

Proposition: H be a non-empty subset of G.
H is a subgroup of G iff H is closed under multiplication and taking inverses.

identity of H = identity of G

inverse of $a \in H$ = inverse of $a \in G$ = a^{-1} in G

G is abelian $\Rightarrow$ H is abelian. $ab=ba$

Proof. $\Rightarrow$ clearly

$\Leftarrow$ 1) Associativity. $g, h, k \in H$ $H \subset G$ $g h k \in G$
$(gh)k = g(hk)$ $\Longleftarrow$ $(gh)k = g(hk)$

2) H contains an identity.

$a \in H$ H is closed under taking inverses. $a^{-1} \in H$

H is closed under multiplication. $a \cdot a^{-1} \in H$
$e \in H$

3). inverses $a \in H$, $a^{-1} \in H$.

H is a subgroup.

$\underline{a \in H \quad H \subset G \quad a \in G \quad a^{-1} \in G \quad a^{-1} \in H} \quad aa^{-1} = e$

$a \in H, b \in H \Leftrightarrow ab \in G \overset{G \text{ is abelian}}{\Longleftrightarrow} ab = ba \Leftrightarrow H$ is abelian. $\square$

Example: 1) set of even numbers is a subgroup of the set of integers under addition.

2). $M_{mn}(\mathbb{Z}) \subset M_{m,n}(\mathbb{Q}) \subset M_{m,n}(\mathbb{R}) \subset M_{mn}(\mathbb{C})$.

$+$,

3). $GL_n(\mathbb{Q}) \subset GL_n(\mathbb{R}) \subset GL_n(\mathbb{C})$

4). D_n: dihedral group $\Rightarrow D_3 = \{I, R, R^2, F_1, F_2, F_3\}$

$\{I, R, R^2\}$ closed under multiplication, taking inverses.

$\{I, F_i\}$ $i \in \{1, 2, 3\}$ .....

Are all subgroups? ✓

H contains R. R^2, I $\quad I, R, R^2$

$R \times R$

$R^2 \quad R^4 = R \quad I, R, R^2$.

H also contains F_i flip, F_1 $\quad RF_1 = F_3$. closed under multiplication

$F_1R = F_2$ $\quad D_3$

H contains two flip. $F_1 F_2$, R

$F_1^{-1} F_1 R = F_1^{-1} F_2 \Leftrightarrow R = F_1 F_2 \quad D_3$

Definition:- Lemma.

Let G be a group and $g \in G$ be an element of G

the cetralizer of G is $C_g = \{h \in G \mid hg = gh\}$ centre. isomorphism.

Then C_g is a subgroup of G. $\quad g^{-1}g = gg^{-1}$ Non-empty.

Proof: it is suffices to prove C_g is closed under multiplication and taking inverses.

1). $h, k \in C_g$ $\quad$ Need $hk \in C_g \Leftrightarrow (hk)g = g(hk)$

$(hk)g = h(kg)$ by associativity

$= h(gk)$ $\quad k \in C_g$

$= (hg)k$

$= (gh)k \quad h \in C_g$

G ~~abelian~~ commutative

$g \in G$.

$= (gh)k$ $\quad h = g$

$= g(hk)$

$\Rightarrow$). $h \in C_g$. Need $h^{-1} \subset C_g \Leftrightarrow h^{-1}g = gh^{-1}$.

$\Updownarrow$

$hg = gh$

$\Updownarrow$

$h^{-1}hg = h^{-1}gh$

$\Updownarrow$

$g = (h^{-1}g)h \leftrightarrow gh^{-1} = h^{-1}g$

$h \in G$. $hg = gh$

$C_g = G$.

G non-commu

$g \in G$

$h \cdot g = gh$

D_3. F_i $\quad F_i R \neq R F_i$

$\{I, F_i\}$ $\quad F_i \cdot F_i = F_i F_i$ $\quad I \cdot F_i = F_i I$

$\square$

Lemma: Let G be a finite group. H be a non-empty finite subset. closed under multiplication.

H is a subgroup of G.

order.

group $\to$ ring $\to$ field

Proof: it is suffices to prove H is closed under taking inverses.

Let $a \in H$. $a = e$ $\quad a^{-1} = e \in H$.

$a \neq e$ $\quad H \neq \{a, a^2, a^3, \dots\} \leftarrow a^k$

Finite field.

q prime.

$a^{\varphi(q)} = 1$ $\quad \varphi(q) = q-1$

$a \cdot a^{q-2} = 1$

$a!$

$m(a+b)$

$m.a.b \in G$.

H is closed under products $\Rightarrow$ H is closed under powers

H is finite $\quad a^m = a^n \quad m < n$

a^{n-1}

$a^{q-1} = 1$

$a^m \in H \quad a^m \in G$. $\quad a^m \in G$

$e = a^{-m}a^m = a^{-m} \cdot a^n = a^{n-m}$.

$a \neq e$, $n - m \neq 1$ $\quad k = n-m-1 > 0 \quad b = a^k \in H$.

F_q. $n = pq$

$\varphi(n) = 1$

$a^{pq} = 1$

$b \in H$

$\{b, b^2, \dots\}$

$b \cdot a = a^k \cdot a = a^{n-m-1} \cdot a = a^{n-m} = e$.

similarly: $ab = e$

b is a inverse of a. $b \in H$.

H is closed under taking inverses.

$\square$

Coset.

odd number is not a subgroup of integers G $\quad g \in G$.

even number is a subgroup of integers

odd + even numbers. = odd numbers

$g \cdot H$ = set $\leftarrow$ coset

干饭