

Def If G is a group, $H \subset G$ is a subgroup of G
we define $a \equiv b \pmod H$ if $a = bh$ for some $h \in H$

(1) $a = a \cdot 1$ ($1 \in H$)

(2) $a = bh \Rightarrow ah^{-1} = b$ ($h^{-1} \in H$ since H is a group)

(3) $a = bh_1, b = ch_2$ then $a = ch_2h_1$, ($h_2h_1 \in H$ since H is a group.)

This is an equivalence relation and the equivalence classes are called cosets

Def let H be a subgroup of G , for every $a \in G$
 $aH := \{ah, h \in H\}$ is called ^{a left} ~~the~~ coset of
 H in G .

with respect to above equivalence relation we

have $aH = [a]$

note $1H = H$

Remark let aH, bH be two left cosets of H in G

Then we have a bijective map $aH \rightarrow bH$

$ah \rightarrow bh$.

(well defined)

(one to one) $f(ah_1) = f(ah_2) \Rightarrow bh_1 = bh_2 \Rightarrow h_1 = h_2 \Rightarrow ah_1 = ah_2$

(onto) if $bh \in bH$ then $f(ah) = bh$.

Thm So the order of the subgroup divides the order of the group.

Def Let G be a group, H a subgroup the set of cosets of H in G is denoted by G/H and called Quotient set of G by H .

$$G/H = \{ aH \mid a \in G \}$$

The index of H in G is $[G:H] := |G/H|$ if it's finite

Def Let $a \in G$, G group The order of a in G is

$$\text{ord}(a) = \begin{cases} \min \{ n \in \mathbb{Z}_+ \mid a^n = 1 \} & , \text{ if this min is finite} \\ \infty & , \text{ otherwise} \end{cases}$$

Corollary Let G be a finite group, $a \in G$ then the order of a divides the order of G

pf: $\langle a \rangle \mid |G|$ but $\langle a \rangle = \{ a^n \mid n \in \mathbb{Z} \}$ if $|\langle a \rangle| = m$

then we write $n = d \cdot m + r$, $0 \leq r \leq m-1$

$$a^n = a^{dm+r} = a^r \Rightarrow \langle a \rangle = \{ 1, a, \dots, a^{\text{ord}(a)-1} \}$$

those numbers are different since if $a^{r_1} = a^{r_2}$ and $0 \leq r_1 < r_2 < \text{ord}(a)$ then $a^{r_1-r_2} = 1$ also

$0 \leq r_2 - r_1 < \text{ord}(a)$, by def of $\text{ord}(a)$

$r_2 - r_1 = 0$ so $r_2 = r_1$ so $\text{ord}(a) \mid |G|$

Corollary $a^{|G|} = 1$

Proof $\text{ord}(a) \mid |G| \Rightarrow |G| = \text{ord}(a) \cdot d, d \in \mathbb{Z}_+$
 ~~$a^{|G|}$~~ $a^{|G|} = a^{\text{ord}(a) \cdot d} = (a^{\text{ord}(a)})^d = (1)^d = 1$

Corollary G finite group, $|G| = p$ then the only subgroups of G are $\{1\}$ and G itself furthermore G is cyclic

~~Def~~ If G is a group, H a subgroup of G

~~H~~ and define $(aH) \cdot (bH) = abH$

This is a valid definition if it's independent of representatives, thus we need $bH = b'H$

and $aH = a'H \Rightarrow abH = a'b'H$

take $a=1, a'=h \in H, b \in G, b'=b$ so we want $abH = a'b'H$ that is $bH = hbH$ so $\exists h' \in H$ s.t. $bh' = hb$ i.e. $h' = b^{-1}hb$.

Condition: $\forall h \in H, b \in G : bhb^{-1} \in H$.

so we have a chance of ~~satisfying~~ the definition being valid 😊

Def Let G be a group, H a subgroup of G

H is called a Normal subgroup of G if

$$a h a^{-1} \in H, \forall a \in G, \forall h \in H.$$

Ex If G is abelian then all subgroups are normal

Ex $\{1\}, G$ are normal subgroups of G (trivial)

Ex $G = S_3, H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\}$, H is not normal

$$\text{since } \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \notin H$$

Proposition Let G be a group, H normal subgroup of G then G/H is group under the operation

$$(aH)(bH) = abH$$

Proof Let $a, a', b, b' \in G$ s.t. $aH = a'H, bH = b'H$

i.e. $a = a'h$ for some $h \in H$, $b = b'h'$ for some $h' \in H$

$$\text{so } ab = (a'h)(b'h') = a' b' \underbrace{(h')^{-1} h}_{h''} b' h'$$

$$= a' b' h'' h' \text{ but since } h'' h' \in H \Rightarrow abH = a' b' H.$$

Associativity is inherited from G

Identity is H , inverse of aH is $a^{-1}H$.

Def Let G, H be groups a homomorphism $f: G \rightarrow H$ is a map with $f(ab) = f(a)f(b)$

Ex $f: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}, +)$

$$n \rightarrow kn, \text{ for } k \in \mathbb{Z}$$

Remark Let $f: G \rightarrow H$ be a group homomorphism and e is the identity of G , e' is the identity of H then $f(e) = e'$, $f(a^{-1}) = f(a)^{-1}$, $\forall a \in G$

Remark if $f: G \rightarrow H$, $g: H \rightarrow L$ are group homomorphisms then $g \circ f: G \rightarrow L$ is a group homomorphism.

Def Let $f: G \rightarrow H$ be a group homomorphism the kernel of f is $\ker(f) = \{a \in G \mid f(a) = 1\} \subset G$ and $\text{Im}(f) = \{f(a) \mid a \in G\} \subset H$

Lemma (1) $\text{Im}(f)$ is a subgroup of H

(2) $\ker(f)$ is a normal subgroup of G

Note Normal subgroups are kernels of a homomorphism

Def An isomorphism is a bijective homomorphism

Remark If f is an isomorphism then f^{-1} is an isomorphism

[Def] G and H are isomorphic if there exist an isomorphism $f: G \rightarrow H$. Denoted by $G \cong H$

[Remark] The class of isomorphisms is an equivalence class. ☺

[Note] If $f: G \rightarrow H$ is a homomorphism then $\text{Im}(f)$ is a subgroup of H so we can think of f as a surjective group homomorphism $f: G \rightarrow \text{Im}(f)$

[Lemma] If $f: G \rightarrow H$ is a group homomorphism then f is injective $\Leftrightarrow \ker(f) = \{1\}$.

[Ex] If $f: M \rightarrow N$ is a bijection then

$$g: S(M) \rightarrow S(N), \sigma \rightarrow f \circ \sigma \circ f^{-1}$$

is an isomorphism, since

$$g(\sigma \tau) = f \circ \sigma \circ \tau \circ f^{-1} = f \circ \sigma \circ f^{-1} \circ f \circ \tau \circ f^{-1} = g(\sigma) g(\tau)$$

and its inverse $g^{-1}: S(N) \rightarrow S(M)$ $\sigma \rightarrow f \circ \sigma^{-1} \circ f^{-1}$ is a function. If M finite $S(M) \cong S_{|M|}$

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ \sigma \downarrow & & \downarrow f \circ \sigma \circ f^{-1} \\ M & \xrightarrow{f} & N \end{array}$$

[Lemma] Let G be a group, N normal subgroup of G . Then the canonical projection (Natural map) $\pi: G \rightarrow G/N, g \rightarrow gN$ is a surjective group homomorphism with kernel N

Thm There exist an isomorphism $\bar{f}: G/\ker(f) \rightarrow H$ such that $f = \bar{f} \circ \pi$ that is $H \cong G/\ker(f)$.

we want $f = \bar{f} \circ \pi$, $f(a) = \bar{f}(\pi(a)) = \bar{f}(aK)$

so define $\bar{f}(aK) := f(a)$

$aK = bK \Rightarrow a = bk, k \in K$ so

$$f(a) = f(bk) = f(b)f(k) = f(b)$$

so it's well defined and it's easy to check it's an isomorphism. 😊

