M403 - Final Exam Review - Definitions - Examples & Counter examples

binary operation: is a function $f: S \times S \to S$.

example: f = sum on the reals, integers, rationals.

counter example: f = substraction on intergers,
$f: \mathbb{N} \times \mathbb{N} \to \mathbb{R}$; $f(n_1, n_2) = \sqrt[n_1]{n_2}$.

associativity: of a binary operation (a b.o. is said to be asso.) If $\forall a, b, c \in S$: $(a * b) * c = a*(b * c)$.

example: trivial. (reals addition).

counter example: ?

commutativity: of a binary operation (a b.o. is said to be commutative) If $\forall a, b \in S$: $a * b = b * a$

example: sum. on reals

counter example: matrix multiplication.

identity element: of a group. $\exists e \in G : \forall g \in G$: $g * e = e * g$.

example: $0 \in \mathbb{R}$.

counter example:

inverses: of groups. $\forall g \in G : \exists g^{-1} \in G$: $g * g^{-1} = g^{-1} * g$.

example:

counter example.

group: A set G together with a binary operation $*: G \times G \to G$ is a group if:

(i) $*$ is associative: $\forall g_1, g_2, g_3 \in G$. $(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$

(ii) existence of identity: $\exists e \in G : \forall g \in G$. $e * g = g * e = g$.

(iii) existence of inverses: $\forall g \in G : \exists g^{-1} \in G$: $g * g^{-1} = g^{-1} * g = e$

example: $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Z}, +)$ ...

counterexample: $(\mathbb{N}, -)$

subgroup: A set $H \subseteq G$, where G is a group is a subgroup if H is itself a group. to test for subgroup check for two conditions
(i) H is closed under $*$, (ii) H is closed under inverses: If $h \in H \Rightarrow h^{-1} \in$

Example : $Gl_n(\mathbb{R}) \leq M_n(\mathbb{R})$.
Counterexample : $\{1,2\} \subseteq (\mathbb{Z}, +)$.

Equivalence Relation : Given a set S. A relation R is a subset of the cartesian product $S \times S$, i.e., $R \subseteq S \times S$.
An equivalence relation is a relation that satisfies
(i) Reflexivity : $\forall s \in S \Rightarrow s \sim s$
(ii) Symmetry $\forall s_1, s_2 \in S \Rightarrow s_1 \sim s_2 \Rightarrow s_2 \sim s_1$
(iii) transitivity $\forall s_1, s_2, s_3 \in S$: $s_1 \sim s_2$ & $s_2 \sim s_3 \Rightarrow s_1 \sim s_3$
Example : Any relation with equality should work
Counterexample :

Cosets : G a group, $H \leq G$, the left cosets are the equivalence classes of the relation : $\forall g_1, g_2 \in G$. $g_1 \sim_H g_2 \Leftrightarrow g_1^{-1} g_2 \in H$.
$gH = \{gh \mid h \in H\}$. for a given $g \in G$. SAME with right cosets.

Example :

Counterexample :

Lagrange theorem : $[G:H] \cdot |H| = |G|$.

Consequence : $H \leq G \Rightarrow |H| \mid |G|$

Order of an element : is the smallest positive integer n s.t. $x^n = e$ denoted by $\theta(x) = n$. ; $1 \leq j < n$ s.t. $x^j \neq e$.

Group homomorphism : A function $f: G_1 \to G_2$, where G_1, G_2 are groups is called a homomorphism if $\forall g_1, g_2 \in G_1$: $f(g_1 g_2) = f(g_1) f(g_2)$.
Example : $f: \mathbb{R}^+ \to \mathbb{R}$: $f(x) = \log(x)$. $(\mathbb{R}^+, \cdot) \mapsto (\mathbb{R}, +)$.
Counterexample : (look at exam 1). Also, from an abelian group to a non-abelian group.

Isomorphism is a bijective homomorphism.
Example : $\{\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \mid x \in \mathbb{R}\} \mapsto (\mathbb{R}, +)$ given by $f(\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}) = x$.
Counterexample : $D_4 \to \mathbb{Z}_4$, there is no possible iso since $|D_4| = 8$, $|\mathbb{Z}_4| = 4$.

M403 - Final Exam Review - Definitions - Examples & Counterexamples (2

Centralizer: Let $S \subseteq G$, G a group. The centralizer of S in G is
$C_G(S) = \{g \in G \mid gs = sg \ \forall s \in S\}$. NOTE that if $S = \{x\}$, in which case
$C_G(x) = \{g \in G \mid gx = xg\}$ is the centralizer of x (a single element).
NOTE also that if $S = G$, then
$C_G(G) = \{g \in G \mid gh = hg \ \forall h \in G\} = Z(G)$, this is the center of G

Examples: $Z(GL_n(\mathbb{R})) = \{\lambda Id \mid \lambda \in \mathbb{R} \setminus \{0\}\}$.

Counterexamples:

Conjugacy Class: Let $x \in G$, G a group. The conjugacy class of x in G
$C_x = C(x) = \{gxg^{-1} \mid g \in G\}$.

Examples:

Counterexamples:

Facts: $G = Z(G) \iff G$ is abelian.
$G/Z(G)$ is cyclic $\Rightarrow G$ is abelian.

Class formula $\quad |C_x| = \dfrac{|G|}{|C_G(x)|} = [G : C_G(x)]$

$$|G| = \sum_{\substack{x \text{ in} \\ d.c.c.}} |C_x| = |Z(G)| + \sum_{\substack{x \text{ in } d \\ n.c.c.}} \frac{|G|}{|C_G(x)|} > 1.$$

Let G be a group. Define $\sim$ on G by $g_1 \sim g_2 \iff \exists x \in G$ s
$g_1 = x g_2 x^{-1}$. Then $\sim$ is an equivalence relation.

Reflexivity: Let $g_1 \in G$. Then $g_1 = e g_1 e^{-1} \Rightarrow g_1 \sim g_1$.

Symmetry: Let $g_1, g_2 \in G$. Suppose $g_1 \sim g_2 \iff g_1 = x g_2 x^{-1}$ for some
$\iff x^{-1} g_1 x = g_2$. Take $y = x^{-1}$. Then $g_2 = y g_1 y^{-1} \iff g_2 \sim g_1$.

Transitivity: Let $g_1, g_2, g_3 \in G$. Suppose $g_1 \sim g_2 \wedge g_2 \sim g_3$. Then
$g_1 = x g_2 x^{-1}$ for some $x \in G$; $\wedge$ $g_2 = y g_3 y^{-1}$ for some $y \in G$ $\Rightarrow$ $g_1 = x(y g_3 y^{-1})x^{-1} = (xy) g_3 (xy)^{-1}$
Let $z = xy$. Then $g_1 = z g_3 z^{-1} \iff g_1 \sim g$

$[x] = \{g \in G : x \sim g\} = \{g \in G : x = gyg^{-1}$ for some g$\} = \{g \in G : g^{-1}x \ldots$ $g^{-1}x$

he subgroup generated by a set of elements S, denoted by $\langle S \rangle$ is

$$\langle S \rangle = \bigcap_{\substack{H \leq G \\ H \supseteq S}} H$$

Examples: $D_4 = \langle \{H, R_1\} \rangle$; $Q_8 = \langle \{x, y\} \rangle$.

ounterexamples:

ormal subgroups: A subgroup H of a group G is called normal and
noted $H \trianglelefteq G$ if: $\forall g \in G : \forall h \in H.\ ghg^{-1} \in H$.

aracterization: T.F.C.A.E.
(i) $H \trianglelefteq G$. (ii) $\forall g \in G : gHg^{-1} = H$. (iii) $\forall g \in G : gH = Hg$ (iv) every left
et of H corresponds to a right coset

: $A_n \trianglelefteq S_n$.

E:

ct: $[G:H] = 2 \Rightarrow H$ is normal.

otient Groups: $H \trianglelefteq G$: $G/H = \{gH \mid g \in G\}$. only b/c H is normal,
$G/H, \circ)$ is a group: $(g_1H) \circ (g_2H) = g_1 g_2 H$.
$\Rightarrow g_1 h_1 g_2 h_2 =$

amples. $G/Z(G)$. $(Z(G) \trianglelefteq G)$. $G/\ker(\varphi)$, φ a homo.

nterexamples:

damental theorem on group homomorphisms: Let $G \xrightarrow{\alpha} G_1$, a homomor. onto.

$$\begin{tikzcd} G \arrow[r, "\alpha"] \arrow[d, "\pi"'] & G_1 \\ G/\ker(\alpha) \arrow[ur, dashed, "\varphi"'] & \end{tikzcd}$$

$\exists!\ \varphi$ s.t. $\varphi \circ \pi = \alpha$. If α is not onto, then use $\mathrm{img}(\alpha)$, wich we know is a subgroup and hence a group.

$\cong G_1$.
$\alpha)$

ct Products: Let G_1, G_2 be groups. Define $G_1 \times G_2 = (G_1, G_2) = \{(g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2\}$.
n $((G_1, G_2), \circ)$ is a group where
: $(G_1; G_2) \times (G_1, G_2) \mapsto G_1 \times G_2 : (g_1, g_2) \circ (g_1', g_2') = (g_1 \cdot g_1', g_2 \cdot g_2')$.

$W_1, W_2 \leq V$. $W_1 \cap W_2 = \{\vec{0}\}$, $W_1 + W_2 = V \Rightarrow V = W_1 \oplus W_2$.

: $H, K \trianglelefteq G$. $H \cap K = \{e\}$; $H \cdot K = G$ (group operation) $\Rightarrow G \cong H \times K$.
$hk \leftarrow (h, k)$

M403 - Final Exam Review - Definitions - Examples & Counterexamples (3)

Simple groups: A group G is called simple if its only normal subgroups are one $\{e\}$ and G itself. $\frac{G}{N}$, G is like a prime number in that it can only be "divided" (mod out) by $1 = \{e\}$ and itself.

Example: A_n, $n \geq 5$. $\mathbb{Z}/p$, cyclic group of prime order

Counter example: $\mathbb{Z}/4$. contains $\mathbb{Z}_2 \trianglelefteq \mathbb{Z}/4$. In general $\mathbb{Z}/n$, n not prime

theorem: Let p be a prime, G a group of finite order and $p \mid G \Rightarrow \exists x \in G : \theta(x) = p$.

Example: $\mathbb{Z}/4$, $2 \mid \mathbb{Z}/4 \Rightarrow \exists x \in \mathbb{Z}/4$ s.t. $\theta(x) = 2$.

Counterexample:

$Aut(G) = \{ f : G \to G \mid f \text{ is an isomorphism} \}$ is a group.

$(Aut(G), \text{function composition})$

$Inn(G) = \{ f_g : G \to G \mid f_g(x) = gxg^{-1} \}$.
Given $g \in G$.

Example:

Counter example:

field: Ring in which every element is invertible w.r.t. mul... distribution la...

Ring $(R, +, \cdot)$ ... $(R, +)$ is an abelian group,
↳ associative

if $\exists 1 \in R$ s.t. $1 \cdot r = r \cdot 1 = 1 \Rightarrow R$ has unity.

A set $(R, +, \cdot)$ is called a ring if:

1) $(R, +)$ is an abelian group.
2) $\cdot$ is associative.
3) $\forall r_1, r_2, r_3 \in R$: $r_1 \cdot (r_2 + r_3) = (r_1 \cdot r_2) + (r_1 \cdot r_3)$
$(r_1 + r_2) \cdot r_3 = (r_1 \cdot r_3) + (r_2 \cdot r_3)$

If $\exists 1 \in R : \forall r \in R: 1 \cdot r = r \cdot 1 = r \Rightarrow R$ is a ring with unity.

If $\cdot$ is commutative is called an abelian Ring (commutative).

field is a commutative Ring in which every non-zero element is invertible w.r.t. $\cdot$.

roup actions on a set.

G-set on a group acts on a set S if $\exists$ a function

$G \times S \mapsto S$, $(g, s) \mapsto g \cdot s$ s.t.

(1) $\forall s \in S$: $e \cdot s = s$.

(2) $\forall g_1, g_2 \in G$: $\forall s \in S$: $g_1 \cdot (g_2 \cdot s) = (g_1 g_2) \cdot s$.

$s \in S$. the orbit of S is:

$G \cdot s = \{ g \cdot s \mid g \in G \}$.

e stabilizer of s is: $C_G(s) = \{ g \in G \mid g \cdot s = s \}$.

$$|G \cdot s| = \frac{|G|}{|C_G(s)|} \qquad \left(|C_x| = \frac{|G|}{|C_G(x)|} : \text{where the action is conjugation. } G \times G \to G \quad (g_1, g) = g_1 g g_1^{-1} \right)$$

ylow THM: (1) $p^k \| |G| \Rightarrow \exists P \leq G$ s.t. $|P| = p^k$.

$p^k \| |G| \Leftrightarrow p^k \mid |G|$ and $p^{k+1} \nmid |G|$.

If P, Q are p-sylow groups, then $\exists x \in G$: $xPx^{-1} = Q$.