Name: ______________________

MAS 4301 – Exam 1

Throughout, $(G, \cdot, e)$ denotes a group. (We do not assume that G is abelian.)
I will not give credit without work or an explanation when asked for it.

Definitions State the following definitions.

(1) The *center* $Z(G)$ of G

$$Z(G) = \{x \in G : \forall y \in G, xy = yx\}$$

(2) The *order* of the element $g \in G$
is the least positive integer $n \in \mathbb{N}$ such that $g^n = e$. If no such $n \in \mathbb{N}$ exists, then g is said to have infinite order.

(3) Define $< g >$

$$< g >= \{g^n : n \in \mathbb{Z}\}.$$

(4) The group G is *cyclic* if
there is some $g \in G$ such that $G =< g >$.

(5) What does it mean for $\sigma \in S_n$ to be *even*?
if σ can be written as a product of an even number of transpositions.

Problems

(1) In S_5, let $\sigma = (3\ 4\ 5)$ and $\tau = (1\ 5)(2\ 3)$.
i) Compute $\sigma \circ \tau$.

$$\sigma \circ \tau = (1\ 3\ 2\ 4\ 5)$$

ii) Compute σ^{-1}.

$$\sigma^{-1} = (3\ 5\ 4)$$

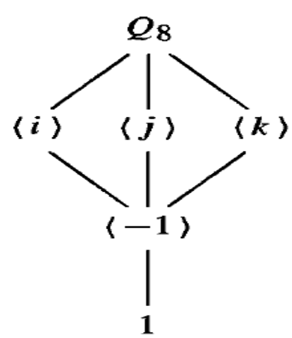
(2) List the elements in $U(9)$. Find the inverse of 2 in $U(9)$.

$$U(9) = \{1, 2, 4, 5, 7, 8\}. 2 \cdot 5 = 10 \cong 1 \bmod 9, 2^{-1} = 5.$$

(3) Let $G = U(10) = \{1, 3, 7, 9\}$. Is G cyclic? Explain.

$$< 3 >= \{3, 9, 7, 1\}. \text{ Yes, G is cyclic.}$$

(4) Draw the lattice of subgroups of Q_8.



(5) Draw the lattice of subgroups of $\mathbb{Z}_{15}$.

(6) In $\mathbb{Z}_{100}$ what is $|42|$? Explain.

First, we take $gcd(42, 100) = 2$. It follows that $< 2 >=< 42 >$ and so $|42| = \frac{100}{2} = 50$.

(7) Let $G =< x, y | x^7 = y^3 = e, xy = yx^2 >$.

(a) Write the following elements in the form yx^j for $1 \leq j \leq 6$. Show some work.

(i) $x^2y = x(yx^2) = yx^4$

(ii) $x^3y = x(x^2y) = yx^6$

(iii) $x^4y = yx^8 = yx$

(iv) $x^5y = yx^3$

(v) $x^6y = yx^5$

(b) Write xy^2 in the form y^2x^j for some $1 \leq j \leq 6$.

$$xy^2 = (xy)y = (yx^2)y = y(x^2y) = y(yx^4) = y^2x^4$$

(c) What is the order of xy?

$(xy)^2 = xy(xy) = x(yx)y = x(x^4y)y = x^5y^2$

$(xy)^3 = xy(x^5y^2) = x(x^6y)y^2 = x^7y^3 = e$

$< xy >= \{xy, x^5y, e\}$

$|xy| = 3.$

Proofs Let G be a group, $H \leq G$, and $g \in G$.

(1) Prove that the set gHg^{-1} is a subgroup of G.

Proof. Let $g \in G$ be fixed. By assumption, $H \leq G$ and so $e \in H$ and therefore

$$e = geg^{-1} \in gHg^{-1}$$

Next, let $x, y \in gHg^{-1}$. By definition, $x = gh_1g^{-1}$ and $y = gh_2g^{-1}$ for some $h_1, h_2 \in H$. Note that $y^{-1} = (gh_2g^{-1})^{-1} = gh_2^{-1}g^{-1}$. Therefore,

$$xy^{-1} = (gh_1g^{-1})(gh_2^{-1}g^{-1}) = g(h_1h_2^{-1})g^{-1}.$$

We know that $h_1h_2^{-1} \in H$ since they each belong to H and $H \leq G$.

Therefore, $xy^{-1} \in gHg^{-1}$ and we conclude that $gHg^{-1} \leq G$. $\square$

(2) Prove that $|H| = |gHg^{-1}|$. [Hint: bijection]

Proof. We define a map $\rho : H \to gHg^{-1}$ by mapping $h \in H$ to $\rho(h) = ghg^{-1}$ which belongs to gHg^{-1}. If $h_1 = h_2$, then $gh_1g^{-1} = gh_2g^{-1}$ from which it follows that ρ is well-defined.

Next, suppose that $\rho(h_1) = \rho(h_2)$. This means that $gh_1g^{-1} = gh_2g^{-1}$. By left and right cancellation, $h_1 = h_2$. This demonstrates that ρ is injective.

Finally, take $x \in gHg^{-1}$. Then $x = ghg^{-1}$ for some $h \in H$. But then $\rho(h) = ghg^{-1} = x$, and so ρ is surjective.

It follows that $\rho : H \to gHg^{-1}$ is a bijection and thus $|H| = |gHg^{-1}|$. $\square$

(3) Suppose that $xy = yx^5$. Prove, using induction, that $x^n y = yx^{5n}$ for all natural numbers $n \in \mathbb{N}$.

Proof. **(Base Case)**. Let $n = 1$. Then $x^1 y = xy = yx^5 = yx^{5n}$.

(Inductive Case). Suppose that for $n \in \mathbb{N}$, $x^n y = yx^5 n$. Then

$$x^{n+1}y = (xx^n)y = x(yx^{5n}) = (xy)x^{5n} = (yx^5)x^{5n} = yx^{5+5n} = yx^{5(n+1)}.$$

Therefore, the statement is true for $n + 1$.

By the Principles of Mathematical Induction, the statement is true for all $n \in \mathbb{N}$. $\square$