Test #2 Math 5310/6310.
November 1, 2019.

Make sure to show all your work. You may not receive full credit if the accompanying work is incomplete or incorrect. If you do scratch work, make sure to indicate scratch work - I will not take off points for errors in the scratch work if it is so labeled and will assume that the scratch work is not part of the final answer/proof. Do five of the following six problems; you may do all six for extra credit.

Section I - Theorems.

Problem 1. Suppose G and H are groups and $\varphi : G \to H$ is an onto homomorphism. Let K be the kernel of φ. Prove that the function $\psi : G/K \to H$ defined by $\psi(Kg) = \varphi(g)$ is well defined and is a homomorphism.

Proof. First we prove the function is well defined. So suppose $Kx = Ky$, then

$$\begin{aligned} Kx &= Ky \\ Kxy^{-1} &= K \\ xy^{-1} &\in K \\ \varphi(xy^{-1}) &= e_H \quad \text{since } xy^{-1} \in ker(\varphi) \\ \varphi(x)\varphi(y^{-1}) &= e_H \\ \varphi(x)(\varphi(y))^{-1} &= e_H \\ \varphi(x) &= \varphi(y). \end{aligned}$$

So the function is well defined. Next we prove that ψ a homomorphism.

$$\begin{aligned} \psi(Kx \cdot Ky) &= \psi(Kxy) \\ &= \varphi(xy) \\ &= \varphi(x)\varphi(y) \\ &= \psi(Kx)\psi(Ky). \end{aligned}$$

□

Problem 2. Consider $(\mathbb{Z}_n, \cdot_n)$ the set $\mathbb{Z}_n$ with $\mod n$ multiplication. Prove that if k and n are relatively prime, then $[k]_n$ has a multiplicative inverse.

Proof. Since k and n are relatively prime there exists integers a and b so that

$$\begin{aligned} 1 &= ka + nb \\ ka &= 1 - nb \\ [ka]_n &= [1 - nb]_n \\ [k]_n[a]_n &= [1]_n - [n]_n[b]_n \\ &= [1]_n - [0]_n[b]_n \\ &= [1]_n. \end{aligned}$$

So $[a]_n$ is the inverse of $[k]_n$.

$\square$

Section II - Exercises.

Problem 3. Consider $(\mathbb{Z}_8, \cdot_8)$.

a. List all the elements of $(\mathbb{Z}_8, \cdot_8)$ that have multiplicative inverses and construct the multiplication table for them.

Solution. The elements are $\{[1]_8, [3]_8, [5]_8, [7]_8\}$.

Multiplication table:

	$[1]_8$	$[3]_8$	$[5]_8$	$[7]_8$
$[1]_8$	$[1]_8$	$[3]_8$	$[5]_8$	$[7]_8$
$[3]_8$	$[3]_8$	$[1]_8$	$[7]_8$	$[5]_8$
$[5]_8$	$[5]_8$	$[7]_8$	$[1]_8$	$[3]_8$
$[7]_8$	$[7]_8$	$[5]_8$	$[3]_8$	$[1]_8$

$\square$

b. Argue, based on the table constructed in part (a), that these elements form a group with the operation $\cdot_8$.

Solution. Associativity follows from the associativity of the usual multiplication. From the chart we have closure: two element multiply together to give another element in the set; we have an identity $[1]_8$ and the identity appears in each row and column (symmetrically), so each element has an inverse. So it's a group. $\square$

Problem 4. Let $G = (\mathbb{Z}_{72}, +_{72})$ and $H = (\mathbb{Z}_8, +_8)$ and let $\varphi : G \to H$ be defined by

$$\varphi([m]_{72}) = [5m]_8.$$

Let $K = \ker(\varphi)$.

a. List the elements of K.

Solution.

$$\begin{aligned} K &= \{[8m]_{72} \mid m \in \mathbb{N}\} \\ &= \{[0]_{72}, [8]_{72}, [16]_{72}, [24]_{72}, [32]_{72}, [40]_{72}, [48]_{72}, [56]_{72}, [64]_{72}\} \end{aligned}$$

□

b. Give a generator of G/K.

Solution.

$$\text{generator} = K +_{72} [1]_{72}$$

□

c. Calculate $|G/K|$ the number of elements of G/K.

Solution.

$$[8m]_{72} = \frac{|G|}{|H|} = \frac{72}{9} = 8$$

□

Problem 5. Consider S_6 the permutation group on six elements

a. Find a subgroup of that S_6 is isomorphic to $(\mathbb{Z}_5, +_5)$. List the elements of each of these groups and indicate an isomorphism. (It is not necessary to prove that it is an isomorphism.)

Solution.

$$\begin{array}{rcl} S_6 & & \mathbb{Z}_5 \\ (12345) & \to & [1]_5 \\ (13524) & \to & [2]_5 \\ (14253) & \to & [3]_5 \\ (15432) & \to & [4]_5 \\ e & \to & [0]_5 \end{array}$$

□

b. Consider the subgroup of S_6 generated by the permutations (123) and (456). Show that every element of this subgroup has order 3. (And therefore is not cyclic.)

Solution. Since $\alpha = (123)$ and $\beta = (456)$ are disjoint cycles they commute. So an arbitrary element g generated by α and β has the form

$$g = \alpha^k \beta^\ell.$$

Observe that either triple has order 3 in S_6:

$$\begin{array}{rcl} \alpha & = & (123) \\ \alpha^2 & = & (132) \\ \alpha^3 & = & e \end{array}$$

and similarly for β.

So then:

$$\begin{array}{rcl} g^3 & = & (\alpha^k \beta^\ell)^3 \\ & = & (\alpha^k)^3 (\beta^\ell)^3 \\ & = & \alpha^{3k} \beta^{3\ell} \\ & = & (\alpha^3)^k (\beta^3)^\ell \\ & = & e \cdot e = e. \end{array}$$

□

Problem 6. Prove that for each positive integer n that $5^{4n} - 1$ is divisible by 8. [Hint: $5^4 = 625$.]

Proof. We prove the theorem by induction. First for $n = 1$;

$$5^4 - 1 \quad = \quad 624 = 78 \cdot 8.$$

Our induction hypothesis is that there is an integer q so that $5^{4n} - 1 = 8q$; this implies that $5^{4n} = 8q + 1$. So:

$$\begin{aligned} 5^{4(n+1)} - 1 &= 5^{4n+4} - 1 \\ &= 5^{4n} \cdot 5^4 - 1 \\ &= (8q + 1) \cdot 5^4 - 1 \\ &= 8q \cdot 5^4 + 5^4 - 1 \\ &= 8q \cdot 5^4 + 78 \cdot 8 \\ &= 8(q \cdot 5^4 + 78). \end{aligned}$$

Which shows that $5^{4(n+1)} - 1$ is divisible by 8 and this completes the proof by induction. $\square$