MATH3100 Dr. Smith Test # 2, Friday March 5, 2024. 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.

1. Let G be a group. Prove two of the following statements; you may prove all three for extra credit.

a. Let $x \in G$, prove that the inverse of x in G is unique.

Solution. Suppose that $\hat{x}$ is an inverse of x. Then:

$$\begin{aligned} x \cdot \hat{x} &= e \\ x^{-1} \cdot x \cdot \hat{x} &= x^{-1} \cdot e \\ e \cdot \hat{x} &= x^{-1} \\ \hat{x} &= x^{-1}. \end{aligned}$$

□

b. Prove that if x, y and z are elements of G, then

$$(xyz)^{-1} = z^{-1}y^{-1}x^{-1}.$$

Solution.

$$\begin{aligned} (xyz) \cdot (xyz)^{-1} &= e \\ x^{-1} \cdot (xyz) \cdot (xyz)^{-1} &= x^{-1} \cdot e \\ (x^{-1} \cdot x)(yz) \cdot (xyz)^{-1} &= x^{-1} \\ eyz \cdot (xyz)^{-1} &= x^{-1} \\ yz \cdot (xyz)^{-1} &= x^{-1}. \end{aligned}$$

Continuing similarly,

$$\begin{aligned} yz \cdot (xyz)^{-1} &= x^{-1} \\ y^{-1}yz \cdot (xyz)^{-1} &= y^{-1}x^{-1} \\ z \cdot (xyz)^{-1} &= y^{-1}x^{-1} \\ z^{-1}z \cdot (xyz)^{-1} &= z^{-1}y^{-1}x^{-1} \\ (xyz)^{-1} &= z^{-1}y^{-1}x^{-1}. \end{aligned}$$

□

c. If $F : G \to G$ is a homomorphism, then F maps the identity into itself. (I.e.: $F(e) = e$.)

Solution. since F is a homomorphism we have,

$$\begin{aligned} F(e \cdot e) &= F(e) \cdot F(e) \\ F(e) &= F(e) \cdot F(e) \\ (F(e))^{-1} \cdot F(e) &= (F(e))^{-1} \cdot F(e) \cdot F(e) \\ e &= e \cdot F(e) \\ e &= F(e). \end{aligned}$$

□

2. Consider the multiplication operator for $\mathbb{Z}_{10}$.

a. Construct the multiplication table for $(\mathbb{Z}_{10}, \cdot_{10})$.

Solution. [Note that I picked 10 so that the multiplication modulo 10 is easy: you just do standard multiplication and keep the rightmost integer in the answer.]

	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

□

b. Argue that the set $\{1, 3, 7, 9\}$ with the operator $\cdot_{10}$ is a subgroup of $\mathbb{Z}_{10}$.

Solution. Multiplication table for $\{1, 3, 7, 9\}$:

	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

1. Associativity follows from the associativity of the original operation in $\mathbb{Z}_{10}$.

2. The above table verifies closure.

3. Since the set $\{1, 3, 7, 9\}$ contains 1 and since that's the identity, then $\{1, 3, 7, 9\}$ contains the identity.

4. Since 1 is in each row and column of the table, we see that each element has an inverse. □

3. Prove that $\sqrt[3]{9}$ is irrational.

Proof. [Solution]

Method 1: Assume that the theorem is not true and that $\sqrt[3]{9} = \frac{a}{b}$ where each of a and b is a positive integer. Then, by the Fundamental Theorem of Arithmetic, each of a and b is uniquely represented by 3 to a power times a product of primes that does not include 3:

$$\begin{aligned} a &= 3^n Q \\ b &= 3^k P. \end{aligned}$$

Where n and k are non-negative integers and 3 divides neither Q nor P. Then:

$$\begin{aligned} \sqrt[3]{9} &= \frac{a}{b} \\ 9b^3 &= a^3 \\ a^3 &= 3^{3n} Q^3 \\ b^3 &= 3^{3k} P^3 \\ 9 \cdot 3^{3k} P^3 &= 3^{3n} Q^3 \\ 3^{3k+2} P^3 &= 3^{3n} Q^3. \end{aligned}$$

By the Fundamental Theorem, this implies that $3k+1 = 3n$ which in turn tells us that 3 divides 2 and this is a contradiction because $3 > 2$. So our original assumption was false and $\sqrt[3]{9}$ is irrational.

Method 2: Assume that the theorem is not true and that $\sqrt[3]{9} = \frac{a}{b}$ where each of a and b is a positive integer and a and b are relatively prime (i.e. $\frac{a}{b}$ is in lowest terms). Then,

$$\begin{aligned} \sqrt[3]{9} &= \frac{a}{b} \\ 9b^3 &= a^3. \end{aligned}$$

Since the prime number 3 divides the left side of the equation, it must also divide the right side. And since 3 is prime, it must divide one of the factors of the expression a^3; so there is an integer q so that $a = 3q$. Then:

$$\begin{aligned} 9b^3 &= a^3 \\ 9b^3 &= (3q)^3 \\ 9b^3 &= 27q^3 \\ b^3 &= 3q^3. \end{aligned}$$

Since the prime number 3 divides the right side of the equation, it must also divide the left side. And since 3 is prime, it must divide one of the factors of the expression b^3; so there is an integer q' so that $b = 3q'$. But then a and b have the common factor of 3 and so are not relatively prime. This contradicts the fact that our original choice of a and b were relatively prime. □

4. Prove that if x and n are relatively prime then $[x]_n$ has a multiplicative inverse in $\mathbb{Z}_n$.

Solution. Since x and n are relatively prime, then my theorem there exist integers p and q so that:

$$1 = np + xq.$$

So we have

$$\begin{aligned} np &= 1 - xq \\ [xq]_n &= [1]_n \\ [x]_n[q]_n &= [1]_n. \end{aligned}$$

So $[x]_n$ has a multiplicative inverse. □

5. Prove that the multiplication operator $\otimes$ on $\mathbb{Z}_n$ is well defined. $\big[$Where $[x]_n \otimes [y]_n = [xy]_n.\big]$

Solution. I'll use the notation that $x \sim a$ means that $n|(a-x)$; so $x \sim a$ means $[x]_n = [a]_n$. Suppose that $x \sim a$ and $y \sim b$. Then there are integers q and p so that

$$\begin{aligned} a-x &= nq \\ b-y &= np \\ a &= nq+x \\ b &= np+y. \end{aligned}$$

Then to prove well defined we need to see if $ab \sim xy$, so:

$$\begin{aligned} ab-xy &= (nq+x)(np+y)-xy \\ ab-xy &= (n^2qp+npx+nqy+xy)-xy \\ &= (n^2qp+npx+nqy) \\ &= n(nqp+px+qy). \end{aligned}$$

Therefore $n|(ab-xy)$ and $ab \sim xy$. □

6. Let α be the following permutation on the set $\{1,2,3,4,5,6\}$:

$$\alpha = (1356).$$

a.) Calculate α^n for all $n > 0$.

Solution.

$$\begin{aligned} \alpha &= (1356) \\ \alpha^2 &= (1356)(1356) = (15)(36) \\ \alpha^3 = \alpha \cdot \alpha^2 &= (1356)(15)(36) = (1653) \\ \alpha^4 = \alpha \cdot \alpha^3 &= (1356)(1653) = (1)(2)(3)(4) = e \end{aligned}$$

□

b.) Argue that $\{a^n\}_{n>0}$ is a subgroup of the group of permutations on the set $\{1, 2, 3, 4, 5, 6\}$.

Solution. 1. Associativity follows since we have a subset of a group with the same operation.

2. Closure follows since:

$$\alpha^n \cdot \alpha^m = \alpha^{(n+m) \mod 4}$$

3. The identity is in the set since

$$\alpha^4 = e$$

4. Each element has an inverse

$$\begin{array}{ll} \alpha^3 & \text{is the inverse of } \alpha \\ \alpha^2 & \text{is the inverse of } \alpha^2 \end{array}$$

We can also see that it's a subgroup from the multiplication table:

	$e = \alpha^4$	α	α^2	α^3
e	e	α	α^2	α^3
α	α	α^2	α^3	e
α^2	α^2	α^3	e	α
α^3	α^3	e	α	α^2

□

Extra Credit. Suppose that $F : Z_n \to Z_\ell$ so that $F([x]_n) = [ax + b]_\ell$. Then, if $\ell | an$, then F is well defined .