

GROUP THEORY, SUMMER 2025

ANON

CONTENTS

1. Introduction	1
2. Groups and Homomorphism	1
2.1. Semigroups \oplus Groups	1
2.2. Homomorphisms	3
3. The Isomorphism Theorems	3
3.1. Subgroups	3
3.2. Lagrange's Theorem	3
3.3. Cyclic Subgroups	3
3.4. Normal Subgroups	3
3.5. Quotient Subgroups	3
3.6. The Isomorphism Theorems	3
3.7. Correspondence Theorem	3
3.8. Direct Product	3
References	3

1. Introduction

Theoretical problems primarily from [1].
Computational problems primarily from [2]. See the url in the bibtex to find the actual uploads of the homework.

2. Groups and Homomorphism

2.1. Semigroups \oplus Groups.

Problem 1. (1.23) If G is a group and $a_1, a_2, \dots, a_n \in G$, then

$$(a_1 a_2 \cdots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \cdots a_1^{-1}.$$

Conclude that if $n \geq 0$, then

$$(a^{-1})^n = (a^n)^{-1}.$$

Proof. Let $P(n)$:

$$(a_1 a_2 \cdots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \cdots a_1^{-1}, \quad n \in \mathbb{N}$$

$P(1)$: $(a_1)^{-1} = a_1^{-1}$ is true.

Assume $P(k)$: $(a_1 \cdots a_k)^{-1} = a_k^{-1} \cdots a_1^{-1}$.

Then

$$(a_1 \cdots a_{k+1})^{-1} = a_{k+1}^{-1} (a_1 \cdots a_k)^{-1} = a_{k+1}^{-1} a_k^{-1} \cdots a_1^{-1}$$

Thus $P(n)$ is true for all $n \in \mathbb{N}$.

Now, if $n \geq 0$, let $a_1 = a_2 = \dots = a_n = a$

Then, we get $(a^n)^{-1} = (a^{-1})^n$ □

Problem 2. (1.26) A group in which $x^2 = e$ for every x must be abelian.

Proof. $x, y \in G \implies x^2 y^2 = e \implies xy = x^{-1} y^{-1}$

Now, $(xy)(yx)^{-1} = (xy)(x^{-1} y^{-1}) = (xy)(xy) = e \implies xy = yx$ □

Problem 3. (1.27)

(i) Let G be a finite abelian group containing no elements $a \neq e$ with $a^2 = e$. Evaluate

$$a_1 a_2 \cdots a_n,$$

where a_1, a_2, \dots, a_n is a list, with no repetitions, of all the elements of G .

(ii) Prove Wilson's Theorem: If p is prime, then

$$(p-1)! \equiv -1 \pmod{p}.$$

Proof. (i) Claim: $a_1 \dots a_n = e$

For n being odd, $\forall a_i \in G, \exists a_i^{-1} \in G, i \in \{1, \dots, n\}$. As the group is abelian and finite so only one element say $a_k \in G, k \in \{1, \dots, n\}$ remains. Now it is clear that $a_k = a_k^{-1} \implies a_k = e$ is the only possibility.

Thus, $a_1 \dots a_n = e$

For n being even, as each element is distinct and each of their inverse is unique, so we get, for $e \in G, \exists a_k \in G, k \in \{1, \dots, n\}$ such that $ea_k = e \implies a_k = e$ but e is unique so there is no group with order even satisfying the given conditions.

Or we can use **Cauchy's theorem**, Let G be a finite group and p be a prime. If p divides the order of G , then G has a non identity element of order p . If $|G|$ was even then Cauchy's theorem implies that there is a non identity element of order 2 which contradicts the hypothesis.

(ii) We have $U(p) = \{1, 2, \dots, p-1\}$. $U(p)$ is a finite abelian group. Now, each element of $U(p)$ has an inverse. $|U(p)|$ is even so there is a non identity element of order 2.

For some $x \in U(p), x^2 = 1 \implies x = x^{-1} \implies x = 1, -1 (= p-1) \implies x^{-1} = -1 (= p-1), 1$.

Strategy: Using the idea of $ab^{-1} = e \implies a = b$ along with the given information which is not there for no reason. $x^2 = e \implies x = x^{-1}$ so we can definitely try leveraging this property.

Strategy: For P3 (i) Let's start with small cases???. For Z_n when n is odd, the evaluation yields 0, when n is even, the evaluation yields 1, 2, 3, ... The even case also seems to have an element whose order is 2 which violates the condition. The odd case doesn't. So the naive conjecture seems that the evaluation would yield the identity element.

As, we already know for a group with order even, eventually after pairing and cancellation, $1 \cdot y = 1 \implies y = -1 = p - 1$.

$1 \cdot 2 \cdots (p - 1) = 1 \cdot (p - 1)$ Thus,

$$(p - 1)! = p - 1 = -1$$

□ We ignore the repeated use of $\equiv (\text{mod } p)$ as it is clear that we are working in $\text{mod } p$ environment due to the way $U(p)$ is defined.

2.2. Homomorphisms.

3. The Isomorphism Theorems

3.1. Subgroups.

3.2. Lagrange's Theorem.

3.3. Cyclic Subgroups.

3.4. Normal Subgroups.

3.5. Quotient Subgroups.

3.6. The Isomorphism Theorems.

3.7. Correspondence Theorem.

3.8. Direct Product.

REFERENCES

- [1] Joseph J. Rotman, *An Introduction to the Theory of Groups*, 4th ed., Graduate Texts in Mathematics, Springer New York, NY, 1995. Originally published by Allyn & Bacon, 1965, 1973 and 1984.
- [2] Han-Bom Moon, *Homework*, 2014. MATH 3005.