My abstract algebra exercises

Evgeny (Gene) Markin

2024

Contents

Preface

This is another yet another attempt at making any progress with abstract algebra, this time with 'Abstract Algebra: An Integrated Approach' by Joseph H. Silverman. I really hope that it works out this time.

So far, it's been most pleasurable journey. This book embodies all the things, that I like in the mathematics books: lots of rigor and a bit of lightheartedness, that really lights it up.

Chapter 1

A Potpourri of Preliminary Topics

All of the topics, discussed in this chapter I know already; skip

Chapter 2

Groups - Part 1

Notes

I'm gonna use the symbol $*$ as the generic group function and e as an identity untill stated otherwise since it's most convinient to me. Sometimes I'll omit $*$ whenever it's clear what's going on. Also, sometimes I omit parenthesis, but given that we've got associativity, we can omit them without problems. For rigorousness' sake, I'll define it to mean left-associative (i.e. $a * b * c = (a * b) * c$).

2.1 Introduction to Groups

2.1.1

By substituting shapes for numbers we get a trivial exercise

2.1.2

Let n be a positive integer, and let S_n be the group of permutations of the set $\{1, 2, ..., n\}$ as described in Example 2.19. Prove that S_n is a finite group, and give a formula for the order of S_n.

From the combinatorics we know that the number of permutations is exacly the factorial of the cardinality of the underlying set.

2.1.3

(a) Let S be a finite set, and let $\phi : S \to S$ be a function. Prove that the injectivity, surjectivity, and bijectivity of this function are equivatent

I'm pretty sure that we've proven that rigorously in the set theory course. If not, then the proof comes from contradiction and theh cardinality of the codomain of, which proves

that injectivity and surjectivity are equivalent, and bijectivity comes from definition.

(b) Give an example of an infinite set S and a function $\phi : S \to S$ such that ϕ is injective but not surjective

We can let $S = \omega$, $\phi(x) = 2x$, which gives us range of even numbers.

(c) Give an example of an infinite set S and a function $\phi : S \to S$ such that ϕ is surjjective but nnot bijective

We can set $S = \omega$ and

$$\phi(x) = \begin{cases} x = 0 \to 1 \\ x - 1 \text{ otherwise} \end{cases}$$

2.1.4

This one involves drawing and is pretty trivial; skip

2.2 Abstract Groups

Let G be a group. In this exercise you will prove the remaining parts of Proposition 2.9. Be sure to justify each step using the group axioms or by reference to a previously proven fact

(a) G has exactly one identity element.

Suppose that e_1 and e_2 both satisfy identity axiom. We follow that both of them are in G and thus

$$e_1 = e_1 e_2 = e_2 e_1 = e_2$$

which comes directly from the Identity Axiom.

(b) $g, h \in G \Rightarrow (g * h)^{-1} = h^{-1} g^{-1}$

We follow that

$$(g * h)^{-1}(g * h) = e$$

by definition of identity. Thus

$$(g * h)^{-1}(g * h) * h^{-1} = eh^{-1}$$

$$(g * h)^{-1}(g * h) * h^{-1} g^{-1} = eh^{-1} g^{-1}$$

by the fact that $*$ is a binary function. Thus

$$(g * h)^{-1} g * (h * h^{-1}) * g^{-1} = eh^{-1} g^{-1}$$

$$(g * h)^{-1} g * g^{-1} = eh^{-1} g^{-1}$$

$$(g * h)^{-1}(g * g^{-1}) = eh^{-1} g^{-1}$$

$$(g * h)^{-1} = eh^{-1} g^{-1}$$

by associative laws, and then we've got that

$$(g * h)^{-1} = h^{-1} g^{-1}$$

by the identity axiom, as desired

(c) $g \in G \Rightarrow (g^{-1})^{-1} = g$

We follow that

$$(g^{-1})^{-1} * (g^{-1}) = e$$

by the inverse axiom. Thus

$$(g^{-1})^{-1} * (g^{-1}) * g = e * g$$

$$(g^{-1})^{-1} * (g^{-1}) * g = g$$

by identity and properties of functions. Thus

$$(g^{-1})^{-1} * ((g^{-1}) * g) = g$$

$$(g^{-1})^{-1} * e = g$$

$$(g^{-1})^{-1} = g$$

by associativity and so on, as desired.

2.2.1

Let G be a group, let $g, h \in G$, and suppose that g has order n and that h has order m.

(a) If G is an abelian group and if $gcd(m, n) = 1$, prove that the order of gh is mn.

Firstly, I want to follow a couple of things:

If order of g is m, and order of g^{-1} is not $n < m$, then

$$e = e * e = g^m (g^{-1})^n = g^{m-n} = e$$

which is a contradiction. Similar case holds for $n > m$. Thus if order of g is n, then order of g^{-1} is also n.

We also follow that if g has finite order n, then $(g^k)^n = (g^n)^k = e$, and thus g^k has finite order for any $k \in Z$. Moreover, since $(g^k)^n = e$ we follow that g^k's order divides n.

We also follow that if g has finite order n, then

$$g * g^{n-1} = e$$

$$g^{n-1} = g^{-1}$$

Now back to our exercise. We follow that

$$(gh)^{mn} = g^{mn} h^{mn} = (g^n)^m (h^m)^n = e^m e^n = e$$

where we can split it this way since G is abelian. Thus we follow that order of gh is finite and divides mn.

Suppose that the order of gh is k. We follow that $k \leq mn$ since it divides mn.

$$(gh)^k = e$$

thus

$$(gh)^k = g^k h^k = e$$

if $g^k \neq e$, then we follow that $h^k = (g^k)^{-1} \neq e$, thus $h^k = (g^{-1})^k = (g^{n-1})^k$. Thus we follow that h^k is a multiple of g, and thus its order divides order of g m. Since h^k is both multiple of g and h, we follow that its order divides both m and n, and since $gcd(m, n) = 1$, we follow that its order is 1. Thus $h^k = e$, which is a contradiction.

Thus we conclude that $g^k = e$. For h^k we've got a similar case. Thus we follow that k divides both m and n, and thus it's either 1 or mn. If $k = 1$, then we follow that $g = h^{-1}$, and thus $gcd(m, n) = 1$ implies that the order of both g and h cannot be anything other than 1, and thus $k = mn = 1$. If $k \neq 1$, then we follow that $k = mn$, as desired.

(b) Give an example showing that (a) need not be true of we allow $gcd(m, n) > 1$

We can have some group where order of g is $n > 1$ (for example $g = 1$ in $G = Z/5$) and set $h = g^{-1}$, for which we'll have that order of gh is 1.

(c) Give an example of a nonabelian group showing that (a) need not be true even if we retain the requirement that $gcd(m, n) = 1$.

A dihedral group of a triangle with $g = r$ and $h = f$ will do. We'll have that order of rf is 2:

$$(rf)^2 = (rfrf) = f^{-1} rrf = e$$

with order of g being 2 and order of h being 3

(d) Again assume that G is an abelian group, and let $l = mn/gcd(m, n)$ (i.e. $l = lcm(m, n)$). Prove that G has an element of order l.

We follow that n divides order of g^m. We also follow that m divides order of h^n. Since $l = lcm(m, n)$ is divided by both m and n we follow that $g^m h^n$'s order divides l.

If there's $k \leq lcm(m, n)$ such that

$$(g^m h^n)^k = e$$

then we follow that

$$g^{mk} h^{nk} = e$$

Here we're gonna employ a more generalized version of an argument in part (a): If $g^{mk} \neq e$, then $k < lcm(m, n)$, thus h^n's order is a multiple of both m and n. h^{nk} cannot be 1, and its order must be then $lcm(m, n)$ or 1, and it can be neither, thus we've got a contradiction. Thus we conclude that $g^{mk} = h^{nk} = 1$, which implies that k divides both m and n, which implies that $k = lcm(m, n)$, as desired.

2.2.2

TODO