

# My abstract algebra exercises

Evgeny (Gene) Markin

2024

# Contents

<b>1</b>	<b>A Potpourri of Preliminary Topics</b>	<b>3</b>
<b>2</b>	<b>Groups - Part 1</b>	<b>4</b>
2.1	Introduction to Groups . . . . .	4
2.1.1	. . . . .	4
2.1.2	. . . . .	4
2.1.3	. . . . .	4
2.1.4	. . . . .	5
2.2	Abstract Groups . . . . .	5
2.2.1	. . . . .	5
2.2.2	. . . . .	6
2.2.3	. . . . .	8
2.2.4	. . . . .	8
2.2.5	. . . . .	10
2.3	Interesting Examples of Groups . . . . .	10
2.3.1	. . . . .	11
2.3.2	. . . . .	12
2.3.3	. . . . .	12
2.3.4	. . . . .	12
2.3.5	. . . . .	12
2.3.6	. . . . .	13
2.3.7	. . . . .	13

# 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.

Some of the notation was migrated from my previous endeavours in the maths.

## 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 until stated otherwise since it's most convenient 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  $\{1, 2, \dots, n\}$  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 exactly the factorial of the cardinality of the underlying set.

### 2.1.3

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

I'm pretty sure that we've proven that rigorously in the set theory course. If not, then the proof comes from contradiction and the 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  $\phi : S \rightarrow S$  such that  $\phi$  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  $\phi : S \rightarrow S$  such that  $\phi$  is surjective but not bijective

We can set  $S = \omega$  and

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

### 2.1.4

*This one involves drawing and is pretty trivial; skip*

## 2.2 Abstract Groups

### 2.2.1

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

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

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

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

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

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

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

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

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.

### 2.2.2

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  $k \in \mathbb{Z}$ . 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  $G = \mathbb{Z}/5$ ) 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:

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

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.  $l = \text{lcm}(m, n)$ ). 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  $l = \text{lcm}(m, n)$  is divided by both  $m$  and  $n$  we follow that  $g^m h^n$ 's order divides  $l$ .

If there's  $k \leq \text{lcm}(m, n)$  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  $k < \text{lcm}(m, n)$ , thus  $h^{nk}$ 's order is a multiple of both  $m$  and  $n$ .  $h^{nk}$  cannot be 1, and its order must be then  $\text{lcm}(m, n)$  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  $k = \text{lcm}(m, n)$ , as desired.



## 2.2.3

Definition 2.6 says that a group is a set  $G$  with a composition law satisfying three axioms. In particular, it says that there's an identity element  $e \in G$  that works on both sides and that every element  $g \in G$  has an inverse that works on both sides. Suppose that we weaken the requirements to specify that the identity and inverse work only on one side. In other words, we suppose that  $G$  is a set with a composition law satisfying the following weaker axioms:

(a) (Right-Identity Axiom) There is an element  $e \in G$  so that  $g * e = g$  for all  $g \in G$

(b) (Right-Inverse Axiom) For all  $g \in G$  there is an element  $h \in G$  so that  $g * h = e$

(c) (Associative Law)  $(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$  for all  $g_1, g_2, g_3 \in G$ .

Prove that  $G$  is a group.

We're gonna start with establishing the inverse axiom for  $G$ , as suggested in the hint to the exercise. Suppose that for  $g \in G$  there's  $h \in G$  such that

$$g * h = e$$

we also follow that for  $h$  there's an element  $k$  such that  $h * k = e$  by the same axiom. We thus follow that

$$h * g = h * g * e = h * g * h * k = h * (g * h) * k = h * e * k = (h * e) * k = h * k = e$$

where we use justification of

$$a \rightarrow (h * k = e) \rightarrow c \rightarrow b \rightarrow c \rightarrow a \rightarrow (h * k = e)$$

in our equalities (given axioms are presented by letters). Thus we've got that  $h * g = e = g * h$  (i.e. normal inverse axiom)

Now suppose that  $g \in G$ . We follow that

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

which practically establishes the Identity axiom. The associative law is unchanged from the standard definition of the group, and thus we're following that  $G$  is indeed a group, as desired.

## 2.2.4

There are other sorts of algebraic structures that are similar to groups in that they are sets  $S$  that have a composition law

$$S \times S \rightarrow S, (s_1, s_2) \rightarrow s_1 * s_2$$

but they have fewer or different axioms than a group. In this exercise we explore two of these structures.

*The set  $S$  with its composition law is a monoid if it has an identity element  $e \in S$  and satisfies the associative law, but elements are not required to have inverses.*

*The set  $S$  with its composition law is a semigroup if its composition law is associative, but it need not have an identity element or inverses.*

i.e. monoid satisfies associative and identity, semigroup satisfies associative, and group satisfies all of them. Hence we've got nested classes of structures:

semigroup  $\subseteq$  monoid  $\subseteq$  group

*For each of the following sets  $S$  and composition laws  $*$  determine if  $(S, *)$  is a group, a monoid, or a semigroup.*

(a) *The set of natural numbers  $N = \{1, 2, 3, \dots\}$  with the composition law being addition.*

I usually do include 0 into the set of naturals, but in this particular case it seems that we don't do it.

In this particular case we follow that  $N$  has associativity with  $+$ , rigorous proof of which comes from the construction of the naturals. In the course of the set theory I've gone through that proof, but I'm pretty sure that it's not required here.

If we don't include 0 into  $N$ , then we don't have an identity in  $N$ , which can be proven by defining order  $>$  on  $N$  and proceeding from there (which was also handled in the course on set theory). Hence it is only a semigroup. If we include it, however, then we get an identity, and thus this set becomes a monoid.

We can also state that it's not got identities.

(b) *The set of extended natural numbers  $N_0 = \{0, 1, 2, 3, \dots\}$  with the composition law being addition.*

handled in part (a)

(c)  $(\mathbb{Z}, +)$

We can follow that it's a superset of  $N$ , which gets its inverses ( $a^{-1} = -a$ ) and hence becomes a full-blown group.

(d)  $(N, *)$

We follow that it's associative, has the identity 1, and hence is at least a monoid. It's not got multiplicative inverses (because that would be  $\mathbb{Q}_+$ ), and hence is not a group.

(e)  $(N_0, *)$

Same as previous, 0 does not change associativity and identities. Is not a group for the same reason as the previous case.

(f)  $(\mathbb{Z}, *)$

Same as previous for the same reason.

(g) *The set of integers  $\mathbb{Z}$  with the composition law  $m * n = \max\{m, n\}$*

If there's  $m \in \mathbb{Z}$ , then there's  $n_0, n_1 \in \mathbb{Z}$  such that

$$n_0 < m < n_1$$

and hence

$$n_0 * m = n_0, n_1 * m = m$$

and hence we follow that there's no identity.

We follow that

$$(n * m) * k = \max\{\max\{n, m\}, k\} = \max\{n, m, k\} = \max\{n, \max\{m, k\}\} = n * (m * k)$$

hence we've got associativity. Thus the given structure is a semigroup.

(h) *The set of naturals  $N$  with the composition law  $m * n = \max\{m, n\}$*

It's got associativity and hence this thing is a semigroup. We can follow that  $1 \leq m$  for all  $m \in N$ , and thus  $\max\{1, m\} = m$ . Thus we follow that we also have a monoid. Inverses are not present, and thus it's not a group.

(i) *The set of naturals  $N$  with the composition law  $m * n = \min\{m, n\}$*

We've got associativity. If  $m \in N$ , then there's  $n \in N$  such that  $n > m$ , and thus  $\min\{m, n\} = m$ , which means that there's no identity, and hence this thing is only a semigroup.

(j) *The set of naturals  $N$  with the composition law  $m * n = mn^2$*

We follow that

$$(m * n) * k = (mn^2) * k = mn^2k^2$$

$$m * (n * k) = m * nk^2 = mn^2k^4$$

setting  $m, n, k$  to primes we can follow that  $(m * n) * k \neq m * (n * k)$ , which implies that this thing is neither a group, a monoid, nor a semigroup.

## 2.2.5

*Look up magmas, Moufang loops, quandles, and matroids*

Magma is just a set with a binary function. There are some discussions about closure, but as long as the thing provided with a set is a binary function, it's a magma.

TODO: look up the rest

## 2.3 Interesting Examples of Groups

### Notes

Although I'm pretty sure that the collection of groups is a proper class (i.e. not a set), I don't have a proof for that. I'll try to change it now.

Empty sets cannot be groups since they've gotta have an element (identity).

Although we can try to do something with cardinals and whatnot, we know that for any set  $S$  there's an injection to the set  $S^S$ . We then follow that there's a subset of bijections in  $S^S$ . We then follow that this subset of bijections is a group (permutations), and hence we conclude that for each set there's a group, and thus a collection of groups is a proper class, as desired.

We can also skip all this stuff, and state singleton of any set  $S$  is a trivial group under projection. Trivial group (if I'm not mistaken) is a group that's got only an identity in it.

Permutation Group practically states that a set of bijections over a set constitutes a group under composition. There are no further restrictions, which is pretty neat.

Matrix group leads us to an interesting idea, which is also bleeding into dihedral groups: as long as a subset of the set of bijections is closed under composition, includes inverses, and includes an identity, given subset is a group (associativity is a property of composition). Can we lose some restrictions though?

Suppose that there's a set of bijections over a set and it is closed under composition. If a set is finite, then we can follow that the set of pairs of bijections is larger than the set of bijections, hence there's got to be a pair

$$S \circ C = S$$

or something like that, which would imply that  $C$  is an identity. If the set is infinite, then this proof will not do. Finality of the set does not imply the existence of inverses:  $\{C, e\}$  will be closed under composition, will have an identity, and will not have inverses.

Given a set of nonzero naturals  $N$ , for each  $n \in N$  we can have  $S_n : \omega \rightarrow \omega$

$$S_n(x) = x + n$$

For each  $n, m \in N$  we've got that

$$(S_n \circ S_m)(x) = S_n(x + m) = x + m + n = S_{m+n}(x)$$

which gives us a set of bijections, that is closed under a composition, does not include an identity ( $0 \notin N$  by our restriction), and no element has an inverse.

Thus we conclude that if a set of bijections is finite and is a singleton, then it's a group. If it's not a singleton and is finite, then it's a monoid (i.e. associativity and identity). If it's not finite, then it's just a semigroup (i.e. associativity exclusively).

We can't have a group of functions, where the set is not a singleton and domain and range of the function are distinct, since two functions are supposed to compose. We can't have non-bijections be present, since we've got to have both left-hand side and right-hand side inverses of any given element.

### 2.3.1

*Let  $G$  be a finite cyclic group of order  $n$ , and let  $g$  be a generator of  $G$ . Prove that  $g^k$  is a generator of  $G$  if and only if  $\gcd(k, n) = 1$ .*

Suppose that  $g^k$  is a generator of  $G$ . If  $k = 1$ , then we follow that  $\gcd(k, n) = \gcd(1, n) = 1$ , thus assume that  $k \neq 1$ .

We follow that there's  $m \in \omega$  such that  $m \neq 0$  and

$$(g^k)^m = g^{km} = g$$

thus

$$g^{km-1} = e$$

and hence we follow that  $km - 1$  is multiple of order of  $G$ . Thus there exists  $j \in Z$  such that  $km - 1 = jn$ . Thus  $km - jn = 1$ , which implies that  $\gcd(k, n) = 1$ , as desired.

Every implication in the forward direction is pretty much a biconditional (not exactly though, we need to add some quantifiers to the mix), so it works in the reverse direction as well.

Also, we haven't gone into a proof that  $\gcd(m, n) = l$  if and only if  $l$  is the lowest positive number such that there exist  $i, j \in Z$  such that

$$mi + jn = l$$

but we've essentially proven the result for  $\gcd(m, n) = 1$  in 1.35

### 2.3.2

*Skip*

### 2.3.3

*Prove that the Dihedral group  $D_n$ , as described in Example 2.22, has exactly  $2n$  elements*

We can follow that there are  $n$  vertices, and each of them gotta go to one of the other  $n$  spaces. There are  $n$  ways to put the first vertex into any of those places. Whenever we put the first vertex  $n$  into some place, there are 2 places where the second vertex can go, so now we're down to  $2n$  possible positions. Whenever we put the second vertex down, positions of the rest are determined, and hence we can follow that there are total of  $2n$  possible positions, as desired.

### 2.3.4

*(a) Let  $Q^*$  be the set of non-zero rational numbers, with the group law being multiplication. Prove that  $Q^*$  is a group.*

We follow that  $1 * q = q$ , and hence we've got an identity. If  $q \in Q^* \Rightarrow q \neq 0 \wedge q \in Q$ , then we follow that  $1/q$  exists, and thus there's  $q^{-1}$  such that  $qq^{-1} = 1$ . Multiplication's associativity does not require a proof (or can be provided, but in this course it is assumed), and thus we conclude that  $Q^*$  is a group (moreover, an abelian group), as desired.

### 2.3.5

*(b) Let  $p$  be a prime number. Prove that the set of non-zero elements of  $Z/pZ$  is a group using multiplication as the group law*

We follow that for each  $i \in \mathbb{Z}/p\mathbb{Z}$ ,  $i * 1 = i$ , and thus  $i$  is our identity. Associativity of multiplication under  $\mathbb{Z}$  implies our associativity.

From group theory we know that there's  $x$  such that  $ax \equiv 1 \pmod{m}$  if and only if  $\gcd(a, m) = 1$ . We then follow that for any given  $i \in \mathbb{Z}/p\mathbb{Z}$  we've got that  $\gcd(i, p) = 1$  since  $p$  is prime, and thus there's  $a \in \mathbb{Z}/p\mathbb{Z}$  such that  $a * i = 1$ . Thus we've got the inverse, and  $\mathbb{Z}/p\mathbb{Z}$  is a group under multiplication, as desired.

We can probably also prove the other direction if we want. If  $p$  is not 1 and is not a prime, then there's a divisor  $q$  of  $p$  in  $\mathbb{Z}/p\mathbb{Z}$ , which implies that only multiple of  $q$  is its multiple, or 0, which implies that it's got no inverse and hence  $\mathbb{Z}/p\mathbb{Z}$  is not a group, as desired. If  $p$  is not a prime, however, then we've got that  $\mathbb{Z}/p\mathbb{Z}$  is a trivial group. We can probably reword this thing so it becomes a theorem, but I'm too lazy to do this.

(c) Heck, I've proven this already and I didn't even read this section

(d) blah blah blah

Got pretty much the same proof as part (a). The only thing of note is that we've got new notation:

$$(\mathbb{Z}/p\mathbb{Z})^*$$

which is a group under multiplication of numbers relatively prime to  $p$ .

### 2.3.6

Let  $C$  be the set of complex numbers, that is, the (... a crude definition of complex numbers)

(a) We make  $C$  into ...

It's a group under addition, yes. Proof is trivial

(b)  $C^* = C \setminus \{0\}$  is a group under multiplication.

Yes it is. Multiplicative inverse is kinda whacky in complex numbers, let me find it:

$$\frac{1}{a+bi} = \frac{(a-bi)}{(a+bi)(a-bi)} = \frac{(a-bi)}{a^2-b^2i^2} = \frac{(a-bi)}{a^2-b^2*(-1)} = \frac{(a-bi)}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i$$

which I would never ever find on my own, if I wouldn't start a complex analysis course at some time in the past (probably should look into it not, this thing looks pretty fun)

### 2.3.7

(a) Let

$$GL_2(R) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in R, ad - bc \neq 0 \right\}$$

be the indicated set of 2-by-2 matrices, with composition law being matrix multiplication. Prove that  $GL_2(R)$  is a group.

It's a set of bijections, that is closed under composition (see linear algebra course), each element is invertible by the restriction, and has identity, thus it's a group. We can also

scale this thing to complex numbers, and we can also increase dimensions of the underlying sets and substitute restriction from the determinant-based to just being invertible (which are equivalent).

(b) Let

$$SL_2(R) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in R, ad - bc = 1 \right\}$$

be the indicated set of 2-by-2 matrices, with composition law being matrix multiplication. Prove that  $SL_2(R)$  is a group.

Same logic as before,

(c) ...

Pretty much is solved by my discussion in previous points. A thing to remember though:

**General** linear group is a set of invertible linear functions.

**Special** linear group is a set of isometries. Not sure if it applies only to euclidean inner product, but the canonical version is euclidean.