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.

After some time with this book my opinion changed a bit in a worse direction due to an increasing number of typos that I have to deal with. $\subseteq$ and $\subset$ are often mixed up, I've encountered an exercise (2.30(c)), whose whole text is one big typo, and some others. On a brighter note, nothing seems to be as messed up as an unprovable exercise from the Lovett's book, and every typo is kinda handled by the context.

Some of the notation migrated from my previous endeavours in the maths. Some of the notation comes from the boot, notable examples of this notation are:

$\langle g \rangle$- a cyclic group that is generated by g

I might mix up isometry and isomorphy here and there, but it's pretty clear from context what exactly do I mean.

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

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

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

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

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.

2.2.2

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 $k \in Z$. 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.

2.2.3

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 suffested 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

$$a \to (\text{h * k = e}) \to c \to b \to c \to a \to (\text{h * k = e})$$

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 practially establishes the Identity axiom. The associative law is unchanged from the stadart 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

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

but they have fewer or different asiomx 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 $N = \{1, 2, 3, ...\}$ 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 $N_0 = \{0, 1, 2, 3, ...\}$ with the composition law being addition.

handled in part (a)

(c) $(Z, +)$

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 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) $(Z, *)$

Same as previous for the same reason.

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

If there's $m \in Z$, then there's $n_0, n_1 \in Z$ 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 associaativity. 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 binanry 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 a 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 do to 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 indentity, 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 $S_n : \omega \to \omega$

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

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 agenerator of G. Prove that g^k is a generator of G if and only uf $gcd(k, n) = 1$.

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 exits $j \in Z$ 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 vertiex 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 fillow that for each $i \in Z/pZ$, $i * 1 = i$, and thus i is our identity. Associativity of multiplication under Z implies our associativity.

From group theory we know that there's x such that $ax \equiv 1(modm)$ if and only if $gcd(a, m) = 1$. We then follow that for any given $i \in Z/pZ$ we've got that $gcd(i, p) = 1$ since p is prime, and thus there's $a \in Z/pZ$ such that $a * i = 1$. Thus we've got the inverse, and Z/pZ 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 Z/pZ, which implies that only multiple of q is its multiple, or 0, which implies that it's got no inverse and hence Z/pZ is not a group, as desired. If p is not a prime, however, then we've got that Z/pZ 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 didnt 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:

$$(Z/pZ)^*$$

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

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

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

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

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. We can scale with determinants here as well.

This group does not include all the isometries though, which is kinda interesting. Some isometries (e.g. $1, -1$ on diagonal) will not be included here. TODO: research this thing a bit more

(c) ...

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

General linear group is a set of invertible linear functions.

Special linear group is a set of matrices with 1 for the determinant.

2.3.8

Let $GL_2(R)$ be the general linear group. Prove or disprove that each of the following subsets of $GL_2(R)$ is a group. In the case of non-groups, indicate which of the group conditions fail.

(a)

$$\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(R) : a, b, c, d \in R, ad - bc = 2\}$$

Not a group, identity is not in there, and composition is not closed ($|AB| = |A||B| = 2 * 2 = 4$)

(b)

$$\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(R) : a, b, c, d \in R, ad - bc \in \{1, -1\}\}$$

Is a group, pretty sure that those describe the isometries.

(c)

$$\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(R) : a, b, c, d \in R, c = 0\}$$

Is a set of upper-triangulars, which are closed under composition, and contain the identity. Inverses of upper-triangular are also upper-triangular, thus we've got a group.

(d)

$$\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(R) : a, b, c, d \in R, d = 0\}$$

Does not contain the identity, and inverses arent present
(e)

$$\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(R) : a, b, c, d \in R, a = d = 1, c = 0\}$$

Pretty sure that this once is a group as well.

2.3.9

Let $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ be the group of quaternions. We clamed that the group law for Q is determined by

$$i^2 = j^k = k^2 = ijk = -1$$

Use there formulas to prove following formulas, which completely determine the group opetrations on Q:

We firstly follow that $(-1)^{-1} = -1$. Thus

$$i * i = -1$$

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

$$i^{-1} * i^{-1} = -1$$

$$i^{-1} = -1 * i$$

$$i^{-1} = -i$$

where the last part comes from the note that -1 commutes with eveything. We can follow that $k^{-1} = -k$ and $j^{-1} = -j$ by the same logic.

We follow now that

$$i * j = i * j * 1 = i * j * (k * -k) = (i * j * k) * -k = -1 * -k = k$$

$$j * k = 1 * j * k = (-i * i) * j * k = -i * -1 = i$$

$$k * i = 1 * k * i = -j * j * k * i = -j * (j * k) * i = -j * i * i = -j * -1 = j$$

we then follow that

$$-k = k^{-1} = (i * j)^{-1} = -j * -i = j * i$$

and so on for all the inverses.

2.3.10

Skip

2.3.11

Practically continue with the functions in the notes. Part (a) is handled

(b) If X is a finite set with n elements, Prove that $\mathcal{E}_X$ is a finite monoid and compute how many elements it has.

We follow that the number of functions is n^n, the rest is handled in the notes

(c) If $|X| \geq 3$, prove that $\mathcal{E}_X$ is not commutative, i.e. show that there are elements $\phi, \psi \in \mathcal{E}_X$ satisfying $\phi \circ \psi \neq \psi \circ \phi$.

We can map a portion of this set to $1, 2, 3$, and then get functions

$$\phi(x) = \begin{cases} 1 \to 2 \\ 2 \to 2 \\ 3 \to 2 \end{cases}$$

$$\psi(x) = \begin{cases} 1 \to 3 \\ 2 \to 3 \\ 3 \to 3 \end{cases}$$

which will suffice.

2.4 Group Homomorphism

2.4.1

Recall that two groups G_1, G_2 are said to be isomorphic if there is a bijective homomorphism

$$\phi : G_1 \to G_2$$

The fact that ϕ is bijective means that the inverse map $\phi^{-1} : G_2 \to G_1$ exists. Prove that ϕ_1 is a homomorphism from G_2 to G_1.

We essentially need to prove that

$$\phi^{-1}(h_1 * h_2) = \phi^{-1}(h_1) * \phi^{-1}(h_2)$$

for all $h_1, h_2 \in G_2$.

ϕ is a bijection, and thus for $h_1, h_2 \in G_2$ there are $g_1, g_2 \in G_1$ such that $\phi(g_1) = h_1, \phi(g_2) = h_2$. By the fact that ϕ is a bijection we also follow that $g_1 = \phi^{-1}(h_1), g_2 = \phi^{-1}(h_2)$. Thus we've got that

$$\phi^{-1}(h_1 * h_2) = \phi^{-1}(\phi(g_1) * \phi(g_2)) = \phi^{-1}(\phi(g_1 * g_2)) = g_1 * g_2 = \phi^{-1}(h_1) * \phi^{-1}(h_2)$$

as desired

2.4.2

Let G be a group, and consider the functiion

$$\phi : G \to G, \phi(g) = g^{-1}$$

(a) Prove that $\phi(\phi(g)) = g$ for all $g \in G$

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

(b) Prove that ϕ is a bijection.

We follow that for each $g \in G$ there's $g^{-1} \in G$, thus $\phi(g^{-1}) = g$, which implies that the range of ϕ is G.

We follow that if $g_1 \neg g_2$, then $g_1{}^{-1} \neq g_2{}^{-1}$, and thus ϕ is injective.

(c) Prove that ϕ is a group homomorphism if and ony if G is an abelian group.

Forward direction: We know that ϕ is bijective, and thus for all $h_1, h_2 \in G$ there are $g_1, g_2 \in G$ such that $\phi(g_1) = h_1, \phi(g_2) = h_2$. If G is a group homomorphism, then we follow that

$$h_1 * h_2 = \phi(g_1)\phi(g_2) = \phi(g_1 g_2) = (g_1 g_2)^{-1} = g_2{}^{-1} g_1{}^{-1} = h_2 * h_1$$

thus the group is abelian.

Reverse direction:

Let us keep assumptions about our variables. If G is abelian, then we follow that

$$h_2 * h_1 = g_2{}^{-1} g_1{}^{-1} = (g_1 g_2)^{-1} = \phi(g_1 g_2)$$

$$h_1 * h_2 = g_1{}^{-1} g_2{}^{-1} = \phi(g_1) * \phi(g_2)$$

Since G is abelian we follow that $h_1 h_2 = h_2 h_1$, and thus we can equate given equalities to get the desired result.

2.4.3

Skip

2.4.4

Let G_1 and G_2 be groups, and suppose that $\phi : G_1 \to G_2$ is an isomorphism

(a) Prove that if G_1 is finite, then G_2 is also finite, and that they satify $|G_1| =_c |G_2|$

Isomorphism is a bijection, thus sets have equal cardinality.

(b) Suppose that G_1 is abelian. Prove that G_2 is abelian

Let $g_1, g_2 \in G_2$. Since ϕ is a bijection we follow that there are $h_1, h_2 \in G_1$ such that $\phi(h_1) = g_1$ and $\phi(h_2) = g_2$. We follow that

$$g_1 g_2 = \phi(h_1)\phi(h_2) = \phi(h_1 h_2) = \phi(h_2 h_1) = \phi(h_2)\phi(h_1) = g_2 g_1$$

as desired.

The solution for the rest of this exercise practically copies the structure of part (a)

2.4.5

In this exericse, C_n is a cyclic group of order n, D_n is the nh dihedral group, and S_n is the nth symmetric group.

(a) Prove that C_2 and S_2 are isomorphic.

We follow that both C_2 and S_2 have 2 and $2! = 2$ elements respectively. Non-identity elements can interact with identity in a predictible way, or with themselves, where they've got an order of 2. This pretty much concludes the proof.

(b) Prove that D_3 is isomorphic to S_3.

We know that D_3 is a subgroup (although we haven't defined at this point what a subgroup is, it doesn't take a genius to guess) of S_3, with the same cardinality.

(c) Let $m \geq 3$. Prove that for every n, the groups C_m and S_n are not isomorphic.

If $m \neq n!$, then we follow that groups have different cardinalities, thus there's no bijection between the two, and thus no isomorphisms.

If $m = n!$, then we follow that since $m \geq 3$ that $n \geq 3$ as well. We follow that there are elements of S_n that map $(1, 2, 3)$ to $(1, 3, 2)$ and $(2, 1, 3)$ and the rest to identity. Composition of those elements is not commutative ($(2, 3, 1)$ and $(3, 1, 2)$ in forward and reverse respectively), and thus S_n is not abelian. C_n on the other hand is commutative, and thus we follow that they aren't isomorhic. This also proves that S_n is non-abelian for any $n \geq 3$.

(d) Prove that for every $n \geq 4$ the groups D_n and S_n aren't isomorphic

They dont have the same cardinalities.

(e) More generally, let $m \geq 4$, and let $n \geq 4$. Prove that the groups D_m and S_n aren't isomorphic.

We once again look at the case when $2m = n!$. We probably want to find some irregularities with orders of the elements here. We follow that if m is odd, then there is only 1 element of order 2 (f). If m is even, then we've got 3 such elements ($f, r^{m/2}, fr^{m/2}$). For S_n for $n \geq 4$ we follow that there are at least 6 of them (bijections that swap elements, there are $C(4, 2) = 6$ of them at least).

(f) The cyclic group C_8, the dihedral group D_4, and the quaternion group Q are non-abelian groups of order 8. Prove that they ren't isomorphic.

First of all, C_8 is abelian (as is any cyclic group for that matter). If we ignore that, then we can follow that there is one element of order 4 (2) in C_8, and there are 6 ($\pm i, \pm j, \pm k$) in Q. There are 3 elements of order 2 in D_4, but only one in C_8. Q has 1 element of order 2.

2.4.6

Skip

2.5 Subgroups, Cosets, and Lagrange's Theorem

Notes

Important definition from the exercises: *Let G be a group, and let $S \subseteq G$ be a subset of G. The subgroup of G generated by S, which we denote by $\langle S \rangle$, is the intersection of all of the subgroups of G that contains S; i.e.*

$$\langle S \rangle = \bigcap_{S \subseteq H \subseteq G : H \text{ is a subgroup of } G} H$$

Exercise proves that $\langle S \rangle$ is essentially a subgroup, where every element is a multiple of some combination (i.e. ordered list in non-abelian and multiset in abelian) of elements of S or their inverses, and also the smallest subgroup, that contains the entirety of S.

2.5.1

Let G be a group and let $g \in G$ be an element of order n, and let $k \geq 1$.

(a) Prove that g^k has order $n/gcd(n,k)$.

We follow that g is a generator for a cyclic group, in which multiples of g^k comprises a subgroup. Since g has order n we follow that $\langle g \rangle$ is a cyclic group of order n.

We know that $gcd(n,k)$ is the lowest number that is a positive sum of multiples of n and k respectively. Thus there are integers a, v such that

$$an + vk = gcd(n,k)$$

We then follow that

$$(g^n)^a * (g^k)^v = g^{gcd(n,k)}$$

order of g is n and thus

$$(g^n)^a * (g^k)^v = (e)^a * (g^k)^v = e * (g^k)^v = (g^k)^v = g^{gcd(n,k)}$$

We thus follow that multiples of $g^{gcd(n,k)}$ are in cyclic subgroup of g^k. There are exacltly $n/gcd(n,k)$ such elements.

Suppose that v is not a multiple of $gcd(n,k)$ and suppose that there's $j \in Z_+$ such that $(g^k)^j = g^{k*j} = g^v$. Since v is not a multiple of $gcd(n,k)$, it is not a multiple of k. Thus we follow that $k * j > n$. We thus conclude that there's a maximal $h \in Z_+$ such that

$$kj - hn = v$$

$$kj + (-h)n = v$$

thus we conclude that v is a multiple of $gcd(n, k)$, which is a contradiction.

(b) Use (a) to give a quick proof of Exercise 2.10, which says that $G = \langle g \rangle$ is a cyclic group of order n, then g^k generates G if and only if $gcd(n, k) = 1$

We follow that if g^k generates G, then $|\langle g^k \rangle| = n/gcd(n, k) = n$. Thus $gcd(n, k) = 1$. Reverse case is pretty much the same.

2.5.2

Let G be a cyclic group of order n, and let $d \geq 1$ be an integer.

(a) Prove that every subgroup of G is cyclic.

Since G is cyclic we follow that there's $g \in G$ that generates G.

Suppose that H is a subgroup of G. If $g \in H$, then $G = H$, and thus we're done. Thus suppose that $g \notin H$. We then follow that there is a lowest possible $i \in Z_+$ such that $g^i \in H$. We follow that every multiple of i is in H. Suppose that $k \in Z_+$ is not a multiple of i and such that $g^k \in H$. We follow that $gcd(k, i) < i$ since k is not a multiple of i. Thus we follow that there are $a, v \in Z$ such that

$$ak + vi = gcd(k, i)$$

and thus

$$g^{ak} + g^{vi} = g^{gcd(k,i)}$$

thus $g^{gcd(k,i)} \in H$, which implies that i is not the lowest element of Z_+ such that $g^i \in H$, which is a contradiction. Thus we conclude that multiples of i are the only elements of H, which implies that H is cyclic, as desired.

Important note: this argument also works for groups G, and so we can follow that any subgroup of any cyclic group is cyclic.

(b) If d divides n, prove that G has a unique subgroup of order d.

Let H_1 and H_2 be two subgroups of order d. We follow that for both of there are least elements i_1, i_2 of Z_+ such that $g^{i_1} \in H_1$ $g^{i_2} \in H_2$. Suppose that $i_1 \neq i_2$ and assume that $i_1 < i_2$. Previous arguments in (a) imply that g^{i_1} and g^{i_2} generate H_1 and H_2. We know also that H_1 is comrised entirely of powers of g^{i_1}. If $gcd(i_1, d) \neq i$, we follow that $gcd(i_1, d) < i$, and thus there are $a, v \in Z$ such that

$$(g^{i_1})^a * (g^d)^v = g^{gcd(i_1,d)}$$

$$(g^{i_1})^a * (e)^v = g^{gcd(i_1,d)}$$

$$(g^{i_1})^a = g^{gcd(i_1,d)}$$

We thus follow that $g^{gcd(i_1,d)} \in H_1$, and thus i_1 is not the lowest positive integer such that $g^{i_1} \in H$, which is a contradiction. We thus conclude that $gcd(i_1, d) = i_1$, and thus $i_1 | d$.

This implies that $|H_1| = |\langle g^{i_1} \rangle| = d/i_1$. Thus if $i_1 \neq i_2$ we follow that $|H_1| \neq |H_2|$, which is a contradiction. Thus we conclude that $i_1 = i_2$, and thus $H_1 = H_2$, as desired.

(c) If d does not divide n, prove that G does not have a subgroup of order d.

We follow that number of cosets of G of order d is a natural number, and thus Lagrange's Theorem implies that order of any subgroup of G divides n, as desired.

2.5.3

Let G be a group, and let $H \subseteq G$. Prove that H is a subgroup if and only if it has the following properties:

(1) $H \neq \emptyset$

(2) For every $h_1, h_2 \in H$, $h_1 * {h_2}^{-1} \in H$

Forward direction is covered by axioms.

Suppose that $H \neq \emptyset$ and for every $h_1, h_2 \in H$, $h_1 * {h_2}^{-1} \in H$. We follow that there's $h \in H$, and thus $h * h^{-1} = e \in H$. Thus we follow the identity axiom.

Suppose that $k \in H$. We follow that $k \in H$ and $e \in H$, thus $e * k^{-1} = k^{-1} \in H$. Thus we follow the inverse axiom.

Let $h_1, h_2 \in H$. We follow that ${h_2}^{-1} \in H$, and thus $h_1 * {h_2}^{-1\,-1} = h_1 * h_2 \in H$, thus giving us closure, which completes the definition of the subgroup, as desired.

2.5.4

Let G be a group, and let $H \subseteq G$ be a nonempty subset of G. Prove that H is a subgroup if and only if it has the following property:

For every $a \in H$, we have $H = \{ah : h \in H\}$

If H is a subgroup, then we follow that $a \in H$ implies that $a^{-1} \in H$, and thus for every $h \in H$ we follow that $a^{-1} h \in H$, and thus $h = e * h = aa^{-1} h \in \{ah : h \in H\}$, thus $H \subseteq \{ah : h \in H\}$. Reverse subset argument is trivial, and thus those two sets are equal, as desired.

qSuppose that for every $a \in H$ we have $H = \{ah : h \in H\}$. Let $b \in H$ be an arbitrary element. We follow that $ab \in \{ah : h \in H\} = H$. We thus follow that all $H = \{ab * h : h \in H\}$. Thus there's an element k of h such that $abk = a$, which implies that $bk = e$, and thus $k = b^{-1}$. Thus we conclude that $b^{-1} = k \in H$. Since b is arbitrary, we conclude that H contains inverses of its elements. Since $b^{-1} \in H$, we follow that

$$H = \{ah : h \in H\}$$

and thus $ab^{-1} \in H$, which implies that H is a subgroup, as desired.

2.5.5

This exercise generalizes the notion of the cyclic subgroup generated by an element of a group as described in Example 2.37. Let G be a group, and let $S \subseteq G$ be a subset of G.

The subgroup of G generated by S, which we denote by $\langle S \rangle$, is the intersection of all of the subgroups of G that contains S; i.e.

$$\langle S \rangle = \bigcap_{S \subseteq H \subseteq G : H \text{ is a subgroup of } G} H$$

We also note that the set of subgroups of G is a subset of $\mathcal{P}(G)$, and thus let us define

$$K = \{H \in \mathcal{P}(G) : H \text{ is a subgroup of } G \text{ and } S \subseteq H \subseteq G\}$$

which is a set and our original definition can be rewritten as

$$\langle S \rangle = \bigcap_{H \in K} H$$

(a) Prove that S is not an empty set.

We follow that S is a subset of G, $G \subseteq G$, and G is a subgroup of G, and thus

$$g \in K$$

Thus K is nonempty, which is also important, since there are no intersections of empty sets. We follow that every subgroup of G contains e, and thus $e \in \langle S \rangle$, as desired.

(b) Prove that $\langle S \rangle$ is a subgroup of G

Let $a, b \in \langle S \rangle$. We follow that every element of K contains a, b, and since every element of K is a subgroup that b^{-1} is also in every element of K. Thus ab^{-1} is also in every element of K, and thus $ab^{-1} \in S$, which implies that S is a subgroup, as desired.

(c) Suppose that L is a subgroup of G and that $S \subseteq L$. Prove that $\langle S \rangle \subseteq L$. (The whole text of this part of the exercise is one big typo)

We follow that $L \in K$, and thus $\langle S \rangle = \bigcap_{H \in K} H \subseteq L$ by definition.