My abstract algebra exercises

Evgeny Markin

2023

Contents

Chapter 1

Groups

1.1 Symmetries of a Regular Polygon

Content of this section was pretty much taken care of in a previous try at an abstract algebra coutse

1.2 Introduction to Groups

For the next 14 exercises decide whether or not hte given pair forms a group.

1.2.1

The pair $(N, +)$

No, since there are no inverses for nonzero elements

1.2.2

The pair $(Q \setminus \{-1\}, \star)$*, where* $a \star b = a + b + ab$

$$a \star (b \star c) = a \star (b + c + bc) = a + (b + c + bc) + ab + ac + abc$$

so associativity checks out.

We can follow that 0 is an identity, since

$$a \star 0 = a + 0 + a0 = a$$

Suppose that $a \in Q \setminus \{-1\}$. We follow that

$$a + b + ab = 0$$

$$b = -a(1 + b)$$

$$b/(1+b) = -a$$
$$-b/(1+b) = a$$

since $b \in Q \setminus \{-1\}$, we follow that $b = m/n$, and thus

$$-\frac{m/n}{1+m/n} = a$$
$$-\frac{m/n}{(n+m)/n} = a$$
$$-\frac{m}{n+m} = a$$

since $a \in Q \setminus \{-1\}$ we follow that $a = k/l$, and thus

$$-\frac{m}{n+m} = k/l$$
$$\frac{-m}{n+m} = \frac{k}{l}$$
$$\begin{cases} m = -k \\ n = l + k \end{cases}$$

thus we follow that as long as $n \neq 0$, a will have an inverse. $n = 0 \iff l = -k \iff a = -1$, and since $a \neq -1$, we conclude that any given element in the given set is an inverse, and thus the given set satisfies all the axioms of a group.

1.2.3

The pair $\langle Q \setminus \{0\}, / \rangle$

We follow that if $a \in lhs$, then $a = m/n$, and thus n/m is the inverse, thus every element got an inverse ($a \neq 0$, thus $m \neq 0$).

$$a/(b/c) = a/\frac{b}{c} = a\frac{c}{b} = \frac{ac}{b}$$
$$(a/b)/c = \frac{a}{b}/c = \frac{a}{b}\frac{1}{c} = \frac{a}{bc}$$

nonzero a, b, c ($\langle 1, 2, 3 \rangle$ should do the trick) will give us a concrete proof that / is not associative, which means that there's no group

1.2.4

The pair $\langle A, + \rangle$ *where* $A = \{x \in Q : |x| < 1\}$

Assuming that $|\star|$ means absolute value, we follow that + won't be a binary operation on A.

The rest of the exercises are left for better times

1.3 Properties of Group Elements

Notes

Order of a group is defined as cardinality of G, which is a functional and not a function. This is not that big of a deal, all things considered. Order of an element is a separate entity altogether, that is defined as a function from a set G, to an extended natural line with excluded 0 (i.e. $\omega \setminus 0 \cup \{\infty\}$), where we define order in the latter by obvious means.

1.3.1

Find the orders of $\overline{5}$ *and* $\overline{6}$ *in* $(Z/21Z, +)$

We follow that order of $\overline{5}$ is 21 and 7 for $\overline{6}$.

1.3.2

Find the orders of $\overline{21}$ *in* $Z/52$

It's' 13

1.3.3

Calculate the order of $\overline{285}$ *in the group* $Z/360Z$

$$(285 * 24)/360 = 19$$

thus the order is 19

1.3.4

Calculate the order of r^{16} *in* D_{24}

We follow that $|r| = 24$, and thus

$$|r^{16}| = \frac{24}{gcd(16, 24)} = \frac{24}{gcd(16, 24)} = 3$$

$$(r^{16})^3 = r^{48} = (r^{24})^2 = e^2 = e$$

1.3.11

Prove 1.2.12

The definition of powers in the book as not as rigorous, as one might want. We can rigorously a function $f_x : \omega \to G$ for an arbitrary group G and arbitrary $x \in G$ by setting

$$f_x(0) = e$$

and

$$f_x(n^+) = xf(n)$$

which will give us a proper function by recursive definition. Thus we can create a function from G to a set of functions, defined this way, and then can expand the domains to Z of resulting function by setting

$$f_x(-n) = f_{x^{-1}}(n)$$

to then get a function $\mathcal{P} : G \times Z \to G$, which we're gonna call the power function. That way we don't have to prove that the power function is indeed a function and all that nonsense.

Now we can follow that

$$\mathcal{P}(x, 0) = e$$

$$\mathcal{P}(x, n{+}1) = \mathcal{P}(x, n{+}1) = \mathcal{P}(x, n)n = \mathcal{P}(x, n{-}1)nn = n\,\mathcal{P}(x, n{-}1)n = nn\,\mathcal{P}(x, n{-}1) = \mathcal{P}(x, n{+}1)$$

and the same thing for negative numbers, which by induction will give us that

$$\mathcal{P}(x, n)x = x\,\mathcal{P}(x, n)$$

for arbitrary $x \in G$ and $n \in Z$.

Now we want to prove that

$$x^m x^n = x^{m+n}$$

with a functional notation, we want to prove that

$$\mathcal{P}(x, m)\,\mathcal{P}(x, n) = \mathcal{P}(x, m + n)$$

We firstly can follow that

$$\mathcal{P}(x, m)\,\mathcal{P}(x, 0) = \mathcal{P}(x, m)e = \mathcal{P}(x, m) = \mathcal{P}(x, m + 0)$$

then we follow that

$$\mathcal{P}(x, m)\,\mathcal{P}(x, n^+) = \mathcal{P}(x, m)x\,\mathcal{P}(x, n) = \mathcal{P}(x, m)\,\mathcal{P}(x, n)x = \mathcal{P}(x, m + n)x = \mathcal{P}(x, m + n^+)$$

and this will give us an inductive proof that $x^m x^n = x^{m+n}$ for arbitrary $m \in Z$ and $n \in \omega$. Some burocracy with regards to domains, maybe a trivial proof of the fact that $\mathcal{P}(x, m)x^{-1} = \mathcal{P}(x, m - 1)$ and whatnot will give us inductive proof for arbirtrary pairs of $m, n \in Z$. Same kind of reasoning (i.e. setting arbitrary m and then do the inductive proof over n) can be applied to the latter part of the theorem, which is gonna be as boring as this one.

1.3.18

Prove that $(Q, +)$ is not a cyclic group.

We can follow that $q \in Q$ is either positive, negative or zero. Thus q^n is either positive, negative or zero respectively for all $n \in \omega$, thus proving that no element of Q can be a generator, which means that Q has no generator.

1.3.19

Prove 1.3.5

1.3.5 states that $|x^{-1}| = |x|$. Let $n = |x|$. Assume that $|x| \in \omega$. If $|x^{-1}| = m \neq n$, then we follow that if $m < n$ then

$$x^n (x^{-1})^m = x^{n-m}$$

which gives us that either $|x| \neq n$ or that our properties of powers don't work, both of which are contraciction. Same logic (with some obvious handling of a case when $|x^{-1}| = \infty$) can be applied for $m > n$, thus giving us the desired conclusion for $|x| \in \omega$. If $|x| = \infty$ and $|x^{-1}| = n$ for $n \in \omega$ we follow practically the same thing: $x^n (x^{-1})^n$ is either not equal to e, or equal to it, both of which aren't good for not having contradictions.

1.3.23

Let $x \in G$ be an element of finite order n. Prove that $e, x, x^2, ..., x^n - 1$ are all distict. Deduce that $|x| \leq |G|$

The premise of the given exercise should be given as a proposition in the book. Don't put the theorems in exercises, it doesn't help anyone

If $0 < i < j < n$ are such that $x^i = x^j$, then $n - i \neq n - j$ but

$$e = x^n = x^{n-i} x^i$$

$$e = x^n = x^{n-j} x^j$$

and thus

$$e = x^{n-j} x^j = x^{n-j} x^i = x^{n-j+i}$$

since $i < j$ we follow that $-j + i < 0$ thus $n - j + i < n$ and therefore n is not an order of $|x|$, as desired.

1.3.29

Using a CAS find all the orders of all the elements in $GL_2(F_3)$

We can use

```
for i in GL(2, GF(3)):
    print(i.order())
```

in SAGE to ge the desired result

The rest of the exercises (or exercises similar to those given in a book) were taken care of previously in previous books

1.4 Concept of a Classification Theorem

Notes

An obvious remark: if G and H are finite, then $|G \oplus H| = |G \times H| = |G||H|$.

1.4.1

Find all orders of all elements in $Z_4 \oplus Z_2$

We can follow that

$$|\langle 0,0\rangle| = 1$$
$$|\langle 1,0\rangle| = 4$$
$$|\langle 2,0\rangle| = 2$$
$$|\langle 3,0\rangle| = 4$$
$$|\langle 0,1\rangle| = 2$$
$$|\langle 1,1\rangle| = 4$$
$$|\langle 2,1\rangle| = 2$$
$$|\langle 3,1\rangle| = 4$$

1.4.2

What is the largest order of an element in $Z_{75} \oplus Z_{100}$? Illustrate with a specific element

We follow that for $\langle x, y\rangle \in Z_{75} \oplus Z_{100}$ we've got that

$$|\langle x, y\rangle| = lcm(|x|, |y|)$$

we thus want to maximize the desired value of lcm. Both Z_{75} and Z_{100} are cyclic, and thus

$$|n| = \frac{75}{gcd(n, 75)}$$

for $n \in Z_{75}$ and it's simular for a Z_{100}. We thus want to maximize the function

$$lcm(75/gcd(n, 75), 100/gcd(m, 100))$$

fundamental theorem of arithmetics essentially states that eny given positive number greater than 2 can be destructed to a multiset of primes, whose product is gonna be that number. lcm in that matter presents some sort of a uniom of multisets, that are connected to a given number, and thus we can practically follow that we want n and m such that

$$n * m = lcm(75, 100)$$

since

$$75 = 3 * 5^2$$

and

$$100 = 2^2 * 5^2$$

let's take $n = 5^2 = 25$ so that $|n| = 3$ and let us take $m = 1$ so that $|m| = 2^2 * 5^2$. this way we'll have that

$$lcm(n, m) = 3 * 2^2 * 5^2 = 300$$

Since we were'nt required to present a proper proof that a given number is an absolute maximum, I'm gonna leave this exercisee at that.

1.4.3

Show that $Z_5 \oplus Z_2$ is cyclic

We follow that $|Z_5 \oplus Z_2| = 5 * 2 = 10$ and that

$$|\langle 1, 1\rangle| = 10$$

1.4.4

Show that $Z_4 \oplus Z_2$ is not cyclic

We've seen the orders of elements of those groups previously, and none of them are 8.

1.4.5

Skip

1.4.6

Let A and B be groups. Prove that the direct sum $A \oplus B$ is abelian of and only if A and B are both abelian

Let's start with reverse implication: if A and B are abelian, then

$$\langle a, b\rangle\langle c, d\rangle = \langle ac, bd\rangle = \langle ca, db\rangle = \langle c, d\rangle\langle a, b\rangle$$

for arbitatry blah-blah-blah and thus as desired.

If $A \oplus B$ is abelian, then assume that e is an identity for B and $a, b \in A$ are such that $ab \neq ba$. We follow then that $\langle ab, e\rangle \neq \langle ba, e\rangle$ but we've got that

$$\langle a, e\rangle\langle b, e\rangle = eangleab, e = \langle b, e\rangle\langle a, e\rangle$$

which contradicts. Thus we conclude that A is abelian, and the same can be followed by the same thread of logic for B and in general for arbitrary (but finite) direct sum of groups.

1.4.7

Let G and H be two finite groups. Prove that $G \oplus H$ is cyclic if and only if G and H are both cyclic with $gcd(|G|, |H|) = 1$

if G, H are cyclic and $gcd(|G|, |H|) = 1$, then we can take generators a, b of both groups to get

$$|\langle a, b\rangle| = lcm(|a|, |b|) = lcm(|G|, |H|) = |G||H|$$

thus making the direct sum cycic, as desired.

$G \oplus H$ is cyclic if and only if there's an element $\langle a, b\rangle \in G \oplus H$ such that

$$|\langle a, b\rangle| = |G \oplus H|$$

i.e.

$$|\langle a, b\rangle| = |G||H|$$

we know that $|\langle a, b\rangle| = lcm(|a|, |b|)$ and therefore $|\langle a, b\rangle| = |G||H|$ iff

$$lcm(|a|, |b|) = |G||H|$$

for all elements k of an arbitrary finite group K we've got that $|k| \leq |K|$ and thus if $|G|$ is not cycic, then $|a| < |G|$, and thus this equality won't hold. Same goes for $|H|$, thus we follow that both G, H are cyclic. We also follow that the equality won't hold if $gcd(|G|, |H|) \neq 1$, which gives the desired conclusion.

1.4.8

This one is trivial, skip.

1.4.9

Find all groups of order 5

Cyclic group is one of those.

If $|x| = 4$ then e, x, x^2, x^3 are all distinct. We follow that $|x^2| = 4/2 = 2$ and $|x^3| = 4$. We then follow that $x^{-1} = x^3$ and x^2 is an inverse of itself. Thus we follow that the last element k is an inverse of itself, and thus has order of 2. We then follow that if $xk = k$, then $x = e$, which is not the case. Thus $xk = x^n$, which means that $k = x^{n-1}$, which is also not the case, thus giving us a contradiction.

If $|x| = 3$ and the group is not cyclic, then $\langle e, x, x^2\rangle$ are all distinct. Let's name the other elements as a, b and thus we'll have a group $\{e, x, x^2, a, b\}$. We follow that $ax \neq x^2$ since that would imply that $a = x$. We also follow that $ax = a \Rightarrow x = e$, $ax = x \Rightarrow a = e$ and $ax = e \Rightarrow x^{-1} = a \Rightarrow a = x^2$, all of which are contradictions. Thus we conclude that $ax = b$. Same reasoning leads us to a conclusion that $bx = a$. Thus $bx^2 = ax = b$, and thus $bx^2 = b$, which implies that $x^2 = e$, which is a contradiction. Thus we conclude that there's no element of order 3.

If $|x| = 2$ and the group is not cyclic, then e, x are distinct. This means that we've got a group $\{e, x, a, b, c\}$. We follow from previous paragraph that there are no elements of order 3 or 4, which implies that $|x| = |a| = |b| = |c| = 2$. We now can follow that since all of the elements are equal to their inverses

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba$$

thus making the group abelian. We can also follow without loss of generality that $ab = e \Rightarrow a = b^{-1} \Rightarrow a = b$, which gives us a contradiction, thus proving that $ab \notin seta, b$. If $x = ab$, then $xc = abc$, therefore $x \neq abc$, and thus $abc \in \{a, b, c\}$. If $abc = a$, then $bc = e$ and therefore $b = c$, which is a contradiction. In general we follow that $abc \notin \{a, b, c\}$, and thus $abc = e$. This implies that $xc = e$, which is a contradiction. Thus we conclude that xc is cannot be equal to non of the elements, which implies that there's no element, whose order is equal to 2 and the group is not cyclic, as desired.

1.4.10

We consider groups of order 6. We know that Z_6 is a group of order 6. We now look for all the others. Let G be any group of order 6 that is not cyclic.

(a) Show that G cannot have an element of order 7 or higher

Order of an element of a group is less than the order of the group, in which it is located. There's an exercise that proves it.

(b) Show that G cannot have an element of order 5

If $|x| = 5$ then $G = \{e, x, x^2, x^3, x^4, a\}$, therefore $ax = x^n$, which gives us a countradiction.

(c) Show that G cannot have an element of order 4.

Let $G = \{e, x, x^2, x^3, a, b\}$. We follow that

$$xa = e \Rightarrow a = x^3$$

$$xa = x \Rightarrow a = e$$

$$xa = x^2 \Rightarrow a = x$$

$$xa = x^3 \Rightarrow a = x^2$$

$$xa = a \Rightarrow x = e$$

thus $xa = b$. We then follow for the same reason that $xb \notin \{e, x, x^2, x^3, b\}$, thus $xb = a$. Therefore $xa = xxb = x^2b = b$, thus $x^2 = e$, which gives us a contradiction.

(d) Show that the nonidentity elements of G have order 2 or 3

We follow that it's got to be either 2, 3, or 6. 6 is not an option since G is not cyclic.

(e) Conclude that there exist only two subgroups of order 6*. In particular, there exists one abelian group of order* 6 *(cyclic) and one nonabelian group of order* 6 *(*D_3 *is such a group)*

We follow that

$$|0| = 1, |1| = 6, |2| = 3, |3| = 2, |4| = 3, |5| = 6$$

for the cyclic group and

$$|e| = 1, |r| = 3, |r^2| = 3, |s| = 2, |sr| = 2, |sr^2| = 2$$

for the dihedral group.

We follow that order of all nonidentity elements cannot be equal to 3, since there are 5 of those and none of them are equal to their inverses.

If all of the orders are equal to 2