Introduction to Algebra Tutorial Sheet 5 Comments Handout

27/11/18

1 Introduction

Please hand in the solutions for the following exercises on Sheet 6 next week: Q1(a)(b)(c)(d), Q3, Q4(c)(d), Q7(c), Q8.

2 Comments on solutions to Sheet 5

2.1 Questin 3

Most people wrote a variation of the following proof:

Proof. Fix $g, h \in G$. Then

$$g^2h = eh = h = he = hg^2$$

so G is abelian. □

The issue here is that this only shows that squares in G commute with all other elements. We need to show that *all* elements of G commute with all other elements of G. In other words, we need to show that for all $g, h \in G$ we have $gh = hg$. Here is the full solution:

Proof. Fix $g, h \in G$. We need to show that $gh = hg$. First observe that we have:

$$(gh)^{-1}(gh)^{-1} = ((gh)^2)^{-1} = e^{-1} = e$$

Now, starting with

$$(gh)(gh)^{-1} = e$$

we may multiply on the right by $(gh)^{-1}$ to get

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

which simplifies down to

$$gh = h^{-1}g^{-1}$$

But note that since $g^2 = e$ and $h^2 = e$, we must have that $g = g^{-1}$ and $h = h^{-1}$ so that $gh = hg$ as required. □

2.2 Question 5

The issue with this question was mostly forgetting what the precise definition of order is. Note that I marked some people 'wrong' even if part of the question was correctly answered as the important part wasn't really addressed. Let's recall the definition of the order of an element:

Definition. Let G be a group and $g \in G$ an element. We say that g has **finite order** if there exists $n \in \mathbb{N}$ such that $g^n = e$. If $o \in \mathbb{N}$ is the least natural number such that $g^o = e$ the **order** of g. If g does not have finite order then we say that g has **infinite order**.

Now, the first mistake people made in this question was forgetting the case of infinite order. If g has infinite order then one also needs to prove that g^{-1} also has infinite order.

The second mistake that people made was writing the following "proof" (or a variation thereof):

Proof. Suppose that $g \in G$ has order n. Then

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

so g^{-1} has order n. □

The issue here is that we have not shown that n is the *least positive integer* such that $(g^{-1})^n = e$. At this stage it is not yet clear that there doesn't exist another $m \in \mathbb{N}$ such that $m \leq n$ and $(g^{-1})^m = e$. Let us now give a full solution to the problem:

Proof. Assume that g has infinite order. Suppose that g^{-1} has finite order. Then we may choose $n \in \mathbb{N}$ such that $(g^{-1})^n = e$. But then

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

By taking inverses on both sides, we see that $g^n = e$ as well. But this contradicts the assumption that g has infinite order so we must have that g^{-1} has infinite order as well.

Now assume that g has finite order, say $n \in \mathbb{N}$ so that $g^n = e$ and n is the least such positive integer. First observe that we have

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

so we must necessarily have that the order of g^{-1} divides n. Suppose, for a contradiction, that the order of g^{-1}, say m, is strictly smaller than n. We then have that

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

But this contradicts the fact that n is the order of g as we have found $m < n$ such that $g^m = n$. We must therefore have that n is the smallest positive integer such that $(g^{-1})^n = e$ and is thus the order of g^{-1}. Hence g and g^{-1} have the same order. □