# MTH 343 Homework 3

Philip Warton

May 4, 2020

## Problem 1 (4.4.23)

Let $a, b \in G$.

### (a)

Prove that the order of $a$ is the same as the order of $-a$.

*Proof.* Denote the order of $a$ as $p \in \mathbb{N} : a^p = e$. Operate with $-a^p$ and we have

$$\begin{aligned} a^p &= e \\ a^p(-a^p) &= e(-a^p) \\ a^{p-1}(e)(-a^{p-1}) &= -a^p \\ &\vdots \\ e &= -a^p \end{aligned}$$

Suppose there was another $p_0 \in \mathbb{N} : p_0 < p$ and $-a^{p_0} = e$. Then by a similar argument we have

$$-a^{p_0} = e \Rightarrow e = a^{p_0}$$

Which would mean that $p_0$ would be the order of $a$ (contradcition). So $p$ is the smallest natural number such that $-a^p = e$ and must be the order of $-a$. □

### (b)

For every $g \in G, |a| = |g^{-1}ag|$.

*Proof.* □

### (c)

## Problem 2 (4.4.29)

Prove that $\forall n \in \mathbb{N} : n > 2$, $\mathbb{Z}_n$ has an even number of generators.

*Proof.* Let $n \in \mathbb{N}$ such that $n > 2$, and let $a \in \mathbb{Z}_n$ such that $\langle a \rangle = \mathbb{Z}_n$. We want to show that $\langle a \rangle = \mathbb{Z}_n \Rightarrow \langle -a \rangle = \mathbb{Z}_n$. Let $p \in \mathbb{Z}_n$, then $\exists m_p \in \mathbb{N}$ such that $(m_p)a = p$. Since $-a \in \mathbb{Z}_n$, there exists $m_{-a} \in \mathbb{N}$ such that $(m_{-a})a = -a$. If we take this equation and add $(m_{-a})(-a)$ then we have

$$\begin{aligned} (m_{-a})a &= -a \\ (m_{-a})a + (m_{-a})(-a) &= -a + (m_{-a})(-a) \\ 0 &= -a + (m_{-a})(-a) \\ a &= a + (-a) + (m_{-a})(-a) \\ a &= (m_{-a})(-a) \end{aligned}$$

This shows that $\exists m_{-a} \in \mathbb{N} : m_{-a}(-a) = a$. Now we can rewrite $(m_p)a = p$ as $(m_p)(m_{-a}(-a)) = (m_p)(m_{-a})(-a) = p$. Which means that $\forall p \in \mathbb{Z}_n, \exists m_p, m_{-a} \in \mathbb{N} : (m_p)(m_{-a})(-a) = p$, so we say that $-a$ is a generator for $\mathbb{Z}_n$ and $\langle -a \rangle = \mathbb{Z}_n$.

For every generator $a \in \mathbb{Z}_n : \langle a \rangle = \mathbb{Z}_n$, $\langle -a \rangle = \mathbb{Z}_n$. Suppose that $a = -a$, then $a + a = -a + a = 0$. This means that either $a = 0$ or that $2a \equiv 0$ and therefore $a|n$. If $a = 0$ then $\langle a \rangle = \{0\}$ and $a$ is not a generator of $\mathbb{Z}_n$. If $2a = n$ and $a$ is coprime to $n$ then $n = 2$ and $a = 1$, which contradicts our assumption that $n > 2$. So we conclude that for all generators $a \in \mathbb{Z}_n$, $a \neq -a$. Since both elements generate the group, we have some number of disjoint pairs of generators, so the set of generators must have an even cardinality as it can be partitioned into sets of two elements. □

# Problem 2 (4.4.)

$f'(x) = \frac{d}{dx} f(x)$