Math 223
Assignment 5: Examples of Groups

Quinn Neumiiller

November 3, 2013

Question 1b. Show that a and $b^{-1}ab$ have the same order.
Claim: $|a| = |b^{-1}ab|$

Proof. Let $|a| = m$, $|b^{-1}ab| = n$
$a^m = e, (b^{-1}ab)^n = e$
$(b^{-1}ab)^n = e$
$b^{-1}a^n b = e$
$a^n = e$ Since the order of a^m must be the least such exponent, $m \leq n$.
Alternatively,
$a^m = e$
$b^{-1}(a^m) = b^{-1}(e)$
$(b^{-1}a^m) = b^{-1}$
$b(b^{-1}a^m) = b(b^{-1})$
$ba^m b^{-1} = e$ Since the order of $b^{-1}a^n b$ must be the least such exponent, $n \leq m$.
Since, $m \leq n$ and $n \leq m$ then $m = n$. $\square$

Question 1c. Show that ab and ba have the same order.
Claim: $|ab| = |ba|$

Proof. Let $|ab| = m$, $|ba| = n$
$(ab)^m = e$
$a(ba)^{(m-1)}b = e$
$(a^{-1})(a(ba)^{(m-1)}b) = (a^{-1})(e)$
$(ba)^{(m-1)}b = a^{-1}$
$(a)((ba)^{(m-1)}b) = (a)a^{-1}$
$(ba)^{(m-1)}(ab) = e$
$(ba)^m = e$ Since the order of ba must be the least such exponent, $n \leq m$.
Alternatively,
$(ba)^n = e$
$b(ab)^{(n-1)}a = e$
$(b^{-1})(b(ab)^{(n-1)}a) = b^{-1}e$
$(ab)^{(n-1)}a = b^{-1}e$
$(b)((ab)^{(n-1)}a) = (b)b^{-1}e$

$(ab)^{(n-1)}(ab) = e$
$(ab)^n = e$ Since the order of ab must be the least such exponent, $m \leq n$.
Since, $m \leq n$ and $n \leq m$ then $m = n$, giving $|ab| = |ba|$ □

Question 2. Claim: $m = |a| = |b|$

Proof. $bx = a \bmod n$
$b^{-1}(bx) = b^{-1}a \bmod n$
$x = b^{-1}a \bmod n$
We need to verify that b has an inverse in $\mathbb{Z}_n$.
There is an element $e \in \langle b \rangle$, which is the mth element of $\langle b \rangle$ such that $bm \equiv e \bmod n$.
m is the inverse, due to this.
Therefore $x = ma \bmod n$, and $a \in \langle b \rangle$.
if $a \in \langle b \rangle$, then $\forall i \in \langle a \rangle : i \in \langle b \rangle$, so $\langle a \rangle \subseteq \langle b \rangle$.
Finally, since $\langle a \rangle \subseteq \langle b \rangle$, and the size of $\langle a \rangle$ equals the size of $\langle b \rangle$, $\langle a \rangle = \langle b \rangle$.
□