Abstract Algebra

Homework 3: 3.15, 3.16, 1, 4.20, 4.21

Kenny Roffo

Due February 13 (Late)

3.15: Let G be a nonempty set and let $*$ be an associative binary operation on G. Assume that both the left and right cancellation laws hold in $(G, *)$. Assume moreover that G is finite. Show that $(G, *)$ is a group.

Proof: To show $(G, *)$ is a group, we must show that $(G, *)$ has an identity, and inverses. We will first show the existence of the identity element:

Since G is finite, G has some number of elements, n, each denoted x_i. Consider an element, x_1, and the corresponding list of elements of G, $x_1, x_1 * x_1, x_1 * x_2, ..., x_1 * x_n$, which has $n + 1$ elements. Since every member of this list is an element of G, and there are more elements in the list than elements in G, it follows that there must exist some x_j such that $x_1 * x_j = x_1$. Now assume $\exists x_t$ such that $x_j * x_t \neq x_t$. This is true if and only if $x_1 * x_j * x_t \neq x_1 * x_t \iff x_1 * x_t \neq x_1 * x_t$, which is obviously false. Therefore it must be the case that $\forall x_i \in G$, $x_j * x_i = x_i$. Likewise, assume $\exists x_t$ such that $x_t * x_j \neq x_t$. This is true if and only if $x_t * x_j * x_1 \neq x_t * x_1 \iff x_t * x_1 = x_t * x_1$, which is false. Thus it must be the case that $\forall x_i \in G$, $x_i * x_j = x_i$. Therefore, there exists an element, x_j, such that $x_i * x_j = x_j * x_i = x_i$, $\forall x_i \in G$. Thus $(G, *)$ has an identity element.

We must now show that G has inverses. Let x_i be an arbitrary element of G. Then the list $x_i, x_i * x_i, ..., x_i^n$ contains $n + 1$ elements. Since G has only n elements, two elements of the list must be equal, $x_i^s = x_i^t = x_i^t * e$, where s¿t. Using the cancellation laws, this expression simplifies to $x_i * x_i^{s-t-1} = x_i^{s-t} = x_i = e$, which implies by definition that $x_i^{s-t-1} = x_i^{-1}$. Therefore, for every $x_i \in G$, $\exists x_i^1$.

Therefore, all of the group axioms are satisfied by $(G, *)$, so $(G, *)$ is a group.

3.16: Consider the nonegative integers under multiplication. multiplication is an associative binary operator on the set, and the cancellation laws hold, but though 1 is the identity, inverses do not exist for all elements. Consider 2, which has inverse 1/2. 1/2 is not a nonnegative integer, so the inverse for 2 is not in the set. Therefore the nonegative integers under multiplication do not form a group.

1: Find a group, G, with $(x*y)^{-1} \neq x^{-1}*y^{-1}\ \forall x, y \in G$:

Consider the group $GL(2,\mathbb{R})$ under matrix multiplication. Let $x = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$ and $y = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$. Then $x^{-1} = \begin{pmatrix} -1 & 1 \\ 2 & -1 \end{pmatrix}$ and $y^{-1} = \begin{pmatrix} -1 & 2 \\ 1 & -1 \end{pmatrix}$. We see $x*y = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix}$. Taking the inverse we have $(x*y)^{-1} = \begin{pmatrix} 5 & -3 \\ -3 & 2 \end{pmatrix}$. Also $x^{-1}*y^{-1} = \begin{pmatrix} -1 & 1 \\ 2 & -1 \end{pmatrix} \cdot \begin{pmatrix} -1 & 2 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 2 & -3 \\ -3 & 5 \end{pmatrix}$. Notice that $(x*y)^{-1} \neq x^{-1}*y^{-1}$, so we have found a group such that it is not the case for all elements x, y in the group that $(x*y)^{-1} = x^{-1}*y^{-1}$.

4.20: Let G be a group and let $a \in G$. An element $b \in G$ is called a *conjugate*of a if there exists an element $x \in G$ such that $b = xax^{-1}$. Show that any conjugate of a has the same order as a.

Let $a, b, y \in G$ such that $a = wbw^{-1}$. Then b is a conjugate of a. Let $r = o(a)$. We must show $o(wbw^{-1}) = r$. First we will show that for some x, y in any group, $(yxy^{-1})^m = yx^my^{-1} = e$ for all $m > 0$ by mathematical induction.

Let $P(n)$ be the statement $(yxy^{-1})^m = yx^my^{-1}$. $P(1)$ is true since $(yxy^{-1})^1 = yxy^{-1}$ and $yx^1y^{-1} = yxy^{-1}$, and $yxy^{-1} = yxy^{-1}$. Let $k \geq 1$, and assume $P(k)$ is true. That is, assume $(yxy^{-1})^k = yx^ky^{-1}$. We see $(yxy^{-1})^{k+1} = (yxy^{-1})^k(yxy^{-1}) = (yx^ky^{-1})(yxy^{-1}) = yx^ky^{-1}yxy^{-1} = yx^kxy^{-1} = yx^{k+1}y^{-1}$. That is, $(yxy^{-1})^{k+1} = yx^{k+1}y^{-1}$, thus $P(k)$ implies $P(k+1)$. Therefore $P(n)$ is true for all $n \geq 1$. Thus for all integers $m > 0$, $(yxy^{-1})^m = yx^my^{-1} = e$.

Now that the above equality has been proven, we have that $(wbw^{-1})^r = wb^rw^{-1} = wew^{-1} = e$. Thus, $o(wbw^{-1}) \leq r$. Now let $z = wbw^{-1}$. Then $b = w^{-1}zw$, and letting $t = w^{-1}$, $b = tzt^{-1}$, thus b is a conjugate of z. Therefore, $o(b) \leq o(z) = o(wbw^{-1}) = o(a) = r \leq o(b)$. Thus $o(wbw^{-1} = r)$, so a conjugate of a has the same order as a.

4.21: Show that for any two elements x, y of any group G, $o(xy) = o(yx)$:

Proof: For this proof we will consider two cases:

Case 1: Assume $o(xy) = \infty$. Assume for the sake of contradiction $o(yx) \neq \inf$. Then $\exists n \in \mathbb{Z}$ such that $o(yx) = n$. Then $(yx)(yx)(yx)..(\text{n times})..(yx) = e$. Multiplying both sides by x on the left, we have $x(yx)(yx)(yx)..(\text{n times})..(yx) = x*e = x$, and by associativity $(xy)(xy)(xy)..(\text{n times})..(xy)x = x$. Applying the right cancellation law, this implies $(xy)(xy)(xy)..(\text{n times})..(xy) = e$. But this implies $o(xy) = n$, which contradicts our assumption that $o(xy) = \infty$. Therefore if $o(xy) = \infty$ then it must be the case that

Case 2: Assume $o(xy) = n$ for some $n \in \mathbb{Z}$. Then $(xy)(xy)(xy)..(\text{n times})..(xy) = e$. Multiplying by y on the left to both sides syields $y(xy)(xy)(xy)..(\text{n times})..(xy) = y$, and by associativity, $(yx)(yx)(yx)$..(n times)..$(yx)y = y$. By the right cancellation law, we have $(yx)(yx)(yx)$..(n times)..$(yx) = e$ Thus it follows that $(yx)^n = e$. If we can show no integer $k < n$ exists such that $(yx)^k = e$, then we will have $o(yx) = n$. For the sake of contradiction, assume such a k exists. Then $(yx)(yx)(yx)$..(k times)..$(yx) = e$. Multiplying both sides by x on the left, we have $x(yx)(yx)(yx)$..(k times)..$(yx) = x * e = x$, and by associativity $(xy)(xy)(xy)$..(k times)..$(xy)x = x$. Applying the right cancellation law, this implies $(xy)(xy)(xy)$..(k times)..$(xy) = e$. But this implies $o(xy) = k$, which contradicts our assumption that $o(xy) = n$. Therefore no such $k < n$ exists, so $o(yx) = n$.

We have shown that given $x, y \in G$, $o(xy) = o(yx)$.