Homework #2 Solutions

14. Suppose that G is a group with the following property: for any $a, b, c \in G$, $ab = ca$ implies $b = c$. Let $x, y \in G$. Set $a = x^{-1}$, $b = xy$ and $c = yx$. Then

$$ab = x^{-1}(xy) = (x^{-1}x)y = ey = y = ye = y(xx^{-1}) = (yx)x^{-1} = ca.$$

By our hypothesis, we must have $xy = b = c = yx$. Since x and y were arbitrary, we conclude that G is abelian.

16. Let G be a group and let $a, b \in G$. Using the associativity property of groups we have

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$$

and

$$(b^{-1}a^{-1})(ab) = b(aa^{-1})b^{-1} = beb^{-1} = bb^{-1} = e.$$

Since inverses are unique, we must have $(ab)^{-1} = b^{-1}a^{-1}$.

Note: In class I showed that any one-sided inverse in a group is automatically a two-sided inverse. Therefore, any *one* of the above inequalities also establishes the result.

20. We will prove by induction that if G is a group, $n \in \mathbb{Z}^+$ and $a_1, a_2, \ldots, a_n \in G$ then

$$(a_1 a_2 \cdots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \cdots a_2^{-1} a_1^{-1}.$$

There is nothing to prove if $n = 1$. So, assume that the result holds for some $n \geq 1$. Let $a_1, a_2, \ldots, a_{n+1} \in G$. Then, according to the previous problem and the inductive hypothesis we have

$$(a_1 a_2 \cdots a_n a_{n+1})^{-1} = ((a_1 a_2 \cdots a_n)(a_{n+1}))^{-1} = a_{n+1}^{-1}(a_1 a_2 \cdots a_n)^{-1} = a_{n+1}^{-1} a_n^{-1} \cdots a_2^{-1} a_1^{-1}$$

which shows that the result holds for $n+1$ any time it holds for $n \geq 1$. By induction, the result holds for all $n \geq 1$.

32. In D_n, for any flip f we have $f^{-1} = f$. Since $frf = r^{-1}$ and $(frf^{-1})^n = fr^n f^{-1}$ (proven in class) we have

$$(frf)^n = fr^n f$$

and so

$$fr^n = fr^n e = fr^n(ff) = (fr^n f)f = (frf)^n f = r^{-n} f.$$

a. In D_4, $r^4 = e$ for any rotation r. Therefore

$$fr^{-2}fr^5 = fr^{-2}fr = fr^{-2}r^{-1}f = fr^{-3}f = frf = r^{-1} = r^3 = r^3 f^0.$$

b. In D_5, $r^5 = e$ for any rotation r. Therefore

$$r^{-3}fr^4fr^{-2} = r^{-3}fr^4r^2f = r^{-3}frf = r^{-3}r^{-1}f^2 = r^{-4}e = r = rf^0.$$

c. In D_6, $r^6 = e$ for any rotation r. Therefore

$$fr^5fr^{-2}f = fr^5(fr^{-2}f) = fr^5(frf)^{-2} = fr^5(r^{-1})^{-2} = fr^7 = fr = r^{-1}f = r^5f$$

36. Let G be a group and let

$$S = \{g \in G \mid g \neq e, g^5 = e\}.$$

We are asked to show that $|S|$ is a multiple of 4. Let $g \in S$. We show first that $|g| = 5$. Since $g \neq e$ and $g^5 = e$ it is clear that $2 \leq |g| \leq 5$. We need to show that $g^2, g^3, g^4 \neq e$. Let n be any of 2,3 or 4. Then $n \in U(5)$ so there is an $m \in U(5)$ so that $nm \bmod 5 = 1$. That is, $nm = 5q + 1$ for some $q \in \mathbb{Z}$. If $g^n = e$ then, raising both sides to the mth power, we obtain

$$e = e^m = g^{nm} = g^{5q+1} = (g^5)^q g = e^q g = eg = g$$

which is impossible. Thus $g, g^2, g^3, g^4 \neq e$ and so $|g| = 5$.

We now claim that for $g, h \in S$, if $h^r \in \{g, g^2, g^3, g^4\}$ for some $1 \leq r \leq 4$, then $\{h, h^2, h^3, h^4\} = \{g, g^2, g^3, g^4\}$. If $h^r \in \{g, g^2, g^3, g^4\}$ then $h^r = g^s$ for some $s \in U(5)$. If $t \in U(5)$ then, since $U(5)$ is a group, there is a $u \in U(5)$ so that $t = ru \bmod 5$. If $v = sr \bmod 5 \in U(5)$ then

$$h^t = h^{ru} = (h^r)^u = (g^s)^u = g^{su} = g^v$$

and so $h^t \in \{g, g^2, g^3, g^4\}$. This proves that $\{h, h^2, h^3, h^4\} \subset \{g, g^2, g^3, g^4\}$. On the other hand, since $h^r = g^s$, we have $g^s \in \{h, h^2, h^3, h^4\}$, so by what we have already shown it follows that $\{g, g^2, g^3, g^4\} \subset \{h, h^2, h^3, h^4\}$, and so $\{h, h^2, h^3, h^4\} = \{g, g^2, g^3, g^4\}$ as claimed.

We now count S. If $S = \emptyset$ then $|S| = 0$ and we're done. Otherwise, choose $g \in S$. Since $|g| = 5$, $g^i \neq e$ for $i = 2, 3, 4$, and the elements g, g^2, g^3, g^4 are all distinct. Also $(g^i)^5 = (g^5)^i = e^i = e$. It follows that g, g^2, g^3, g^4 are distinct elements of S. Moreover, the preceding paragraph shows that two sets of the form $\{g, g^2, g^3, g^4\}$, $\{h, h^2, h^3, h^4\}$ for $g, h \in S$ are either disjoint or equal. Therefore the sets g, g^2, g^3, g^4 partition S into a collection of subsets, each with size 4. It follows that the size of S is a multiple of 4.