Some Solutions for Week 9 Homework

20. Suppose S is finite first and write $S = \{g_1, \ldots, g_n\}$. Let g be any element of S. Then by hypothesis $gg_1, \ldots, gg_n$ are n distinct elements of S, so that $S = \{gg_1, \ldots, gg_n\}$. In particular, for some g_i we have $g = gg_i$. Reindex if necessary so that $g = gg_1$. Then $gg_1 = (gg_1)g_1 = g(g_1^2)$, so that $g_1 = g_1^2$.

Now let g be any element in S and write $g_1 g = g'$. Then $g_1(g_1 g) = g_1 g'$. By associativity $g_1(g_1 g) = g_1^2 g = g_1 g$, so by left cancellation $g = g'$. In other words, $g_1 g = g$ for all $g \in S$. Similarly, if we write $gg_1 = g'$, then $gg_1 = gg_1^2 = g'g_1$ and $g = g'$, so that $gg_1 = g$ for all $g \in S$, too. This shows that g_1 is an identity element.

Again let g denote an element of S. As above, $S = \{gg_1, \ldots, gg_n\}$. In particular, $g_1 = gg_i$ for some index i. Then $g(g_i g) = (gg_i)g = g_1 g = g = gg_1$, so by cancellation $g_i g = g_1$, too. This shows that g_i is an inverse for g. Hence S is a group since there in an identity and every element has an inverse.

This is definitely not the case when S is infinite. For example, suppose S is the set of non-zero integers with the usual multiplication. This fits the hypotheses above, but it is not a group (no inverses). For another example, consider the non-zero even integers with the usual multiplication. This isn't a group since it doesn't even have an identity element.

22. Suppose G is a group such that $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$. Let $a, b \in G$. Then by Proposition 3.1.2 (one of our "little results") $(ba)^{-1} = a^{-1}b^{-1}$. We thus have $(ba)^{-1} = (ab)^{-1}$, and taking inverses of both sides (using another "little result") gives $ba = ab$. Thus, G is abelian.

Now suppose G is abelian and $a, b \in G$. Then $(ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1}$ by Proposition 3.1.2 and the hypothesis that G is abelian.

11. Let S be a set, $a \in S$ and $H = \{\sigma \in \mathrm{Sym}(S) \colon \sigma(a) = a\}$. Clearly H is not empty since the identity permutation is in H. Suppose $\sigma, \tau \in H$. Then $\tau^{-1}(a) = \tau^{-1}(\tau(a)) = a$, and so $\sigma(\tau^{-1}(a)) = \sigma(a) = a$. Thus $\sigma \circ \tau^{-1} \in H$. By Corollary 3.2.3, H is a subgroup.