Math 620: Subgroup HW

Due on Monday, October 12, 2015

Boynton 10:00

Kailee Gray

Exercise 3.2.4: Show that $\{(1), (12)(34), (13)(24), (14)(23)\}$ is a subgroup of S_4.

Let $G = \{(1), (12)(34), (13)(24), (14)(23)\}$. Notice that G and S_4 are finite sets. G contains only permutations of $\{1, 2, 3, 4\}$ and S_4 contains all possible permutations of $\{1, 2, 3, 4\}$ so G is a subset of S_4. From proposition 3.1.6 we know S_4 is a group under the operation of composition of functions. Thus, by corollary 3.2.4, it suffices to show for any $a, b \in G$, $a \circ b \in G$. Since $|G| = 4$, we will verify this property holds by calculating every possible composition in G:

$\circ$	(1)	(12)(34)	(13)(24)	(14)(23)
(1)	(1)	(12)(34)	(13)(24)	(14)(23)
(12)(34)	(12)(34)	(1)	(14)(23)	(13)(24)
(13)(24)	(13)(24)	(14)(23)	(1)	(12)(34)
(14)(23)	(14)(23)	(13)(24)	(12)(34)	(1)

The table above shows the composition of any two elements in G is contained in G. Thus, G is a subgroup of S_4.

Exercise 3.2.11: Let S be a set, and let a be a fixed element of S. Show that $\{\sigma \in \mathbf{Sym}(S) |\ \sigma(a) = a\}$ is a subgroup of $\mathbf{Sym}(S)$.

Let $H = \{\sigma \in \text{Sym}(S) |\ \sigma(a) = a\}$. Then, by definition of H, for any $\sigma \in H$, $\sigma \in \text{Sym}(S)$, so $H \subseteq \text{Sym}(S)$. Consider any $\sigma, \tau \in H$. Then, $\sigma(a) = a$ and $\tau(a) = a$. By definition 2.3.1, a function σ is a permutation of S if σ is one-to-one and onto. Therefore, σ and τ are well-defined, one-to-one, and onto. Then, $\sigma\tau(a) = \sigma(\tau(a)) = \sigma(a) = a$ implies $\sigma\tau \in H$ for any $\sigma, \tau \in H$. Also if $\tau(a) = a$, $\tau^{-1}(a) = a$ which implies $\tau^{-1} \in H$. We know $\sigma\tau \in H$ for any $\sigma, \tau \in H$; so since $\sigma, \tau^{-1} \in H$, $\sigma\tau^{-1} \in H$.

Notice $\delta = (1) \in \text{Sym}(S)$. Also, since $\delta(a) = a$, $\delta \in H$. So, $H \neq \emptyset$. Thus, for any $\sigma, \tau \in H$, $\sigma\tau^{-1} \in H$. By corollary 3.2.3, H is a subgroup of $\text{Sym}(S)$.

Exercise 3.2.15: Prove that any cyclic group is abelian.

Proof. Let G be any cyclic group. By definition 3.2.5, there exists some $a \in G$ such that $\langle a \rangle = G$. So, for any $x, y \in G$, $x = a^{n_1}$ and $y = a^{n_2}$ for some $n_1, n_2 \in \mathbb{Z}$. Then, $xy = a^{n_1}a^{n_2}$. By definition 3.1.4', $a^{n_1}a^{n_2} = a^{n_1+n_2}$. Then, addition in $\mathbb{Z}$ is commutative, so $n_1 + n_2 = n_2 + n_1$. Therefore, $xy = a^{n_2+n_1} = a^{n_2}a^{n_1} = yx$. For any $x, y \in G$ we have $xy = yx$; hence G is abelian. □

Exercise 3.2.17: Prove that the intersection of any collection of subgroups of a group is again a subgroup.

Proof. Let G be a group with identity element e. Consider some collection of subgroups of G, indexed in no particular order by $k \in K$. Then consider $L = \bigcap_K H_k$. $H_k \subseteq G$ for all k so $\bigcap_K H_k \subseteq G$. Notice $L \neq \emptyset$ since all subsets of G must contain e. If $L = \{e\}$, then L is trivially a subgroup, so consider $a, b \in L$. Then $a, b \in H_k$ for all k. Since all $H_k \leq G$, $ab \in H_k$ for all k which implies $ab \in L$. Also, if $a \in H_k$ for all k, H_k are groups, so $a^{-1} \in H_k$ for all k. Thus, $a^{-1} \in L$. Thus, by proposition 3.2.2, L is a subgroup of G. □

Exercise 3.2.19: Let G be a group and let $a \in G$. The set $C(a) = \{x \in G \mid xa = ax\}$ of all elements of G that commute with a is called the centralizer of a.

(a) Show that $C(a)$ is a subgroup of G.

Proof. Let G be a group and let $a \in G$. Define the set $C(a) = \{x \in G \mid xa = ax\}$. Notice for all $x \in C(a)$, $x \in G$, so $C(a) \subseteq G$. Also, G is a group so G contains an identity element e, and for any $a \in G$, $ea = a = ea$. Thus, $e \in C(a)$. Consider any $x \in C(a)$. Then, $xa = ax$. Since $x \in C(a)$, $x \in G$, so there exists $x^{-1} \in G$ such that $x^{-1}x = e$. $xa = ax$ implies $x^{-1}xax^{-1} = x^{-1}axx^{-1}$. Thus, $eax^{-1} = x^{-1}ae$, so $ax^{-1} = x^{-1}a$ implies $x^{-1} \in C(a)$. Finally, consider any $x, y \in C(a)$. Then, $xa = ax$ and $ya = ay$. If $ya = ay$, then $xya = xay$. But, $xa = ax$, so $xya = axy$. Thus, $x, y \in C(a)$. By proposition 3.2.2, $C(a) \leq G$.

□

(b) Show that $\langle a \rangle \subseteq C(a)$.

Proof. Consider some $x \in \langle a \rangle$. Then, $x = a^n$ for some $n \in \mathbb{Z}$. Notice $ax = aa^n = a^{1+n} = a^{n+1} = a^n a = xa$. Thus, $x \in C(a)$. □

(c) Compute $C(a)$ if $G = S_3$ and $a = (123)$. Note, $S_3 = \{(1), (123), (132), (23), (13), (12)\}$. Since (1) is the identity element of S_3, $(1)(123) = (123)(1)$ implies $(1) \in C(a)$. Also, any element commutes with itself, so $(123) \in C(a)$. We will compose all remaining elements of S_3 with (123) to check for commutativity:

	(132)	(23)	(13)	(12)
permutation from top row $\circ\,(123)$	(1)	(12)	(23)	(13)
$(123)\,\circ$ **permutation from top row**	(1)	(13)	(12)	(23)

Thus, $C((123)) = \{(1), (123), (132)\} = \langle (123) \rangle$.

(d) Compute $C(a)$ if $G = S_3$ and $a = (12)$. Since (1) is the identity element of S_3, $(1)(12) = (12)(1)$ implies $(1) \in C(a)$. Also, any element commutes with itself, so $(12) \in C(a)$. We will compose all remaining elements of S_3 with (12) to check for commutativity:

	(132)	(23)	(13)	(123)
permutation from top row $\circ\,(12)$	(13)	(123)	(132)	(23)
$(12)\,\circ$ **permutation from top row**	(23)	(132)	(123)	(13)

Thus, $C((12)) = \{(1), (12)\}$.

Exercise 3.2.21: Let G be a group. The set $Z(G) = \{x \in G \mid xg = gx$ for all $g \in G\}$ is called the center of G. (a) Show that $Z(G)$ is a subgroup of G.

Proof. Note $e \in Z(G)$ since $eg = ge$ for all $g \in G$. Also, all $x \in Z(G) \in G$ by defintion of $Z(G)$ so $Z(G) \subseteq G$. Consider any $x, y \in Z(G)$. Then, for all $g \in G$, $xg = gx$ and $yg = gy$. If $yg = gy$, $xyg = xgy$. Since $xg = gx$ we have $xyg = gxy$. Thus, $xy \in Z(G)$. Since $x \in G$, $x^{-1} \in G$ such that $x^{-1}x = e = xx^{-1}$. Then, if $x \in Z(G)$, $xg = gx$ for all $g \in G$. Equivalently, $x^{-1}xgx^{-1} = x^{-1}gxx^{-1}$ and $egx^{-1} = x^{-1}ge$. So, $gx^{-1} = x^{-1}g$ implies $x^{-1} \in Z(G)$ for any $x \in Z(G)$. By proposition 3.2.2, $Z(G)$ is a subgroup of G. □

(b)Show that $Z(G) = \bigcap_{a\in G} C(a)$.

Proof. **(show $Z(G) \subseteq \bigcap_{a\in G} C(a)$)** Consider any $x \in Z(G)$. Then, for all $g \in G$, $xg = gx$. Equivalently for all $a \in G$, $xa = ax$. Thus, $x \in C(a)$ for all $a \in G$ so $x \in \bigcap_{a\in G} C(a)$.
(show $Z(G) \supseteq \bigcap_{a\in G} C(a)$) Consider any $x \in \bigcap_{a\in G} C(a)$. Then, for all $a \in G$, $x \in C(a)$. So, for all $a \in G$, $xa = ax$. Equivalently, for all $g \in G$, $xg = gx$ so $x \in Z(G)$. □

(c) Compute the center of S_3. Consider the multiplication table of S_3:

$\circ$	(1)	(12)	(13)	(23)	(123)	(132)
(1)	(1)	(12)	(13)	(23)	(123)	(132)
(12)	(12)	(1)	(132)	(123)	(23)	(13)
(13)	(13)	(123)	(1)	(132)	(12)	(23)
(23)	(23)	(132)	(123)	(1)	(13)	(12)
(123)	(123)	(13)	(23)	(12)	(132)	(1)
(132)	(132)	(23)	(12)	(123)	(1)	(123)

By inspection, $Z(G) = \{(1)\}$. Also note that $C(123) \cap C(12) = \{(1)\}$ so $Z(G) = \{(1)\}$ also follows from exercise 3.2.19 parts c, d.

Exercise 3.2.23: Let G be a cyclic group, and let a, b be elements of G such that neither $a = x^2$ nor $b = x^2$ has a solution in G. Show that $ab = x^2$ does have a solution in G.

Proof. Let G be a cyclic group, and let a, b be elements of G such that neither $a = x^2$ nor $b = x^2$ has a solution in G. Since G is cyclic, $G = \langle g \rangle$ for some $g \in G$ and so $a, b \in G$ imply $a = g^n$ and $b = g^m$ for some $n, m \in \mathbb{Z}$. If m or n are even, then $m = 2k$ or $n = 2l$ for $k, l \in \mathbb{Z}$. Then, $a = g^{2k} = (g^k)^2$ and $b = g^{2l} = (g^l)^2$. But $a \neq x^2$ and $b \neq x^2$ for any $x \in G$, so m, n must be odd. Also, G is a group so we can write $ab = g^{m+n}$. Then, since m, n are odd, $m + n$ is even so $\frac{m+n}{2} \in \mathbb{Z}$ which implies $g^{\frac{m+n}{2}} \in G$. We can write $ab = (g^{\frac{m+n}{2}})^2$. Thus, $ab = x^2$ has a solution in G, namely $g^{\frac{m+n}{2}}$. □

Exercise 3.2.24: Let G be a group with $a, b \in G$. (a) Show that $o(a^{-1}) = o(a)$.

Proof. Let G be a group with $a \in G$. Consider $o(a) < \infty$ and suppose $o(a) = n$ for $n \in \mathbb{Z}^+$. Then, by definition 3.2.7, $a^n = e$ and n is the smallest such positive integer. Since G is a group, $a^{-1} \in G$ and $(a^{-1})^n = a^{-n} \in G$. If $a^n = e$, then $a^n a^{-n} = ea^{-n}$. By exponential laws of groups, $a^n a^{-n} = a^{n-n} = a^0 = e$. Thus, $ea^{-n} = a^{-n} = e$. Again, by the exponential laws of groups $a^{-n} = (a^{-1})^n$. Hence, $(a^{-1})^n = e$. Now, suppose there is $m \in \mathbb{Z}^+, m < n$ such that $(a^{-1})^m = e$. Then, following a similar argument as above, $(a^{-1})^m = e$ implies $a^{-m}a^m = ea^m$ which implies $e = a^m$. The order of a is n, so the existence of such an $m < n$ contradicts the definition of order of a. Thus, when $o(a) < \infty$, $o(a^{-1}) = n = o(a)$. Next, suppose $o(a) = \infty$. Then, there does not exists a $k \in \mathbb{Z}^+$ such that $a^k = e$. If $o(a^{-1}) \neq \infty$, then there exists some $k \in \mathbb{Z}^+$ such that $(a^{-1})^k = e$ where k is the smallest such integer. But from the first part of the proof we know this implies $a^k = e$ which contradicts our assumption that $o(a) = \infty$. Thus, if $o(a) = \infty$, $o(a^{-1}) = \infty$. □

(b) Show that $o(ab) = o(ba)$.

Proof. Let G be a group with $a, b \in G$. First, consider $o(ab) < \infty$. Then, suppose $o(ab) = n$ for $n \in \mathbb{Z}^+$. Then, by definition 3.2.7, $(ab)^n = e$ and n is the smallest such positive integer. By part (a), $o(ab) = n$ implies $o((ab)^{-1}) = n$. So, $(ab)^{-n} = e$. We will manipulate $(ab)^n = e$ using the listed properties of groups to obtain our desired result:

$$
\begin{array}{ccc}
(ab)^n & = e & \\
(ab)(ab)\cdots(ab) & = e & \text{by exponential laws of groups} \\
a(ba)(ba)\cdots(ba)b & = e & \text{by associative property} \\
a(ba)^{n-1}b & = e & \\
a(ba)^{n-1}ba & = ea & \text{multiply on the right by a} \\
a^{-1}a(ba)^{n-1}ba & = a^{-1}ea & \text{multiply on the left by } a^{-1} \\
(a^{-1}a)(ba)^{n-1}(ba) & = (a^{-1}e)a & \text{by associative property} \\
(e)(ba)^{n-1}(ba) & = (a^{-1})a & \text{definition of identity and inverse elements} \\
(e(ba)^{n-1})(ba) & = e & \text{definition of inverse elements, associativity} \\
(ba)^{n-1}(ba) & = e & \text{definition of identity element} \\
(ba)^n & = e & \text{definition of identity element .}
\end{array}
$$

The above implies that for any $n \in \mathbb{Z}^+$, if $(ab)^n = e$, then $(ba)^n = e$. So, if there exists some $k \in \mathbb{Z}^+$ with $k \leq n$ and $(ba)^k = e$, then $(ab)^k = e$. This contradicts our assumption that $o(ab) = n$, since n must be the smallest positive integer with $(ab)^n = e$. Thus, n is the smallest positive integer such that $(ba)^n = e$ so $o(ba) = n$.

If $o(ab) = \infty$, then there is no integer $n \in \mathbb{Z}^+$ such that $(ab)^n = e$. If $o(ba) \neq \infty$, there there exists some integer $k \in \mathbb{Z}^+$ such that $(ba)^k = e$. From above, if $(ba)^k = e$, then $(ab)^k = e$ which contradicts our assumption that $o(ab) = \infty$. Thus, if $o(ab) = \infty$, then $o(ba) = \infty$. Hence, $o(ab) = o(ba)$. $\square$

(c) Show that $o(aba^{-1}) = o(b)$.

Proof. Let G be a group with $a, b \in G$. Then, $a^{-1}, e \in G$ such that $a^{-1}a = e$ and $aba^{-1} \in G$. By associative property we can write, $aba^{-1} = (ab)a^{-1}$. If two elements of G are equal, their orders must be equal so, $o(aba^{-1}) = o((ab)a^{-1})$. Then, $ab, a^{-1} \in G$, so by part (b), $o((ab)a^{-1})) = o(a^{-1}(ab))$. By associativity, $a^{-1}(ab) = (a^{-1}a)b = eb = b$. Since $a^{-1}(ab) = b$ and $o((ab)a^{-1})) = o(a^{-1}(ab))$, $o((ab)a^{-1})) = o(b)$. Thus, $o(aba^{-1}) = o(b)$ for any $a, b \in G$.

$\square$

Exercise 3.2.26: Let G be a group with $a, b \in G$. Assume that $o(a)$ and $o(b)$ are finite and relatively prime, and that $ab = ba$. Show that $o(ab) = o(a)o(b)$.

Proof. Let G be a group with $a, b \in G$. Without loss of generality, assume $a, b \neq e$. Assume that $o(a)$ and $o(b)$ are finite and relatively prime, and that $ab = ba$. Then, G is abelian. If $o(a)$ and $o(b)$ are finite and relatively prime, $o(a) = p$ and $o(b) = q$ for some $p, q \in \mathbb{Z}^+$ such that $\gcd(p, q) = 1$. Then, p, q are the smallest positive integers such that $a^p = e$ and $b^q = e$. Since G is abelian, by exercise 17 in section 3.1, $(ab)^{pq} = a^{pq}b^{pq}$. Applying the exponential laws of groups, we obtain $a^{pq}b^{pq} = (a^p)^q(b^q)^p = e^q e^p = e$. Thus, $(ab)^{pq} = e$. Suppose $o(ab) \neq pq$ and $o(ab) = k$ where $k \in \mathbb{Z}^+$, $k < pq$ and $(ab)^k = e$. By proposition 3.2.8 (b), $(ab)^{pq} = e$ implies $o(ab) \mid pq$ and so $k \mid pq$. Because p and q are relatively prime, the only divisors of pq are $\pm 1, \pm p, \pm q, and \pm pq$. Since $k \in \mathbb{Z}^+$, $k > 0$, $k \neq pq$, so $k = 1, p, q$. We will consider all these cases:

($k = 1$) If $k = 1$, $(ab)^1 = ab = e$. Then, $a^{-1} = b$ and $a = b^{-1}$. From part (a) of exercise 3.2.24, $o(a^{-1}) = o(a)$. Since $a^{-1} = b$, $o(a^{-1}) = o(b)$ which implies $o(a) = o(b)$. So, $p = q$. Then, $\gcd(p, q) = p = q \neq 1$ as assumed. Hence, $k \neq 1$.

($k = p$) If $k = p$, $(ab)^p = e$. By exercise 3.1.17, $(ab)^p = a^p b^p = e$. Since $o(a) = p$, $a^p = e$, so $a^p b^p = e$ implies $a^p b^p = a^p$. Thus, $b^p = e$. If $p > q$, by proposition 3.2.8(b), $q \mid p$. But, p and q are relatively prime, $q \not\mid p$ and so $p < q$. But, $p \not< q$ since q is the smallest integer such that $b^q = e$. Hence, $k \neq p$.

($k = q$) If $k = q$, $(ab)^q = e$. By exercise 3.1.17, $(ab)^q = a^q b^q = e$. Since $o(b) = q$, $b^q = e$, so $a^q b^q = e$ implies $a^q b^q = b^q$. Thus, $a^q = e$. If $q > p$, by proposition 3.2.8(b), $p \mid q$. But, p and q are relatively prime, $p \not\mid q$ and so $q < p$. But, $p \not< q$ since q is the smallest integer such that $b^q = e$. Hence, $k \neq p$.

Thus, pq is the smallest integer such that $(ab)^{pq} = e$ and $o(ab) = pq = o(a)o(b)$.

$\square$