MATH 210A

Name: Quin Darcy
Instructor: Dr. Shannon

Due Date: 9/11/19
Assignment: Homework 2

1. Assume $(G, \star)$ is a group, $a \in G$, $o(a) = n$, $m \in \mathbb{Z}^+$, and $d = (m.n)$.

   (a) Prove that $o(a^m) = o(a^d)$.

   Proof. Let $y = o(a^m)$ and $t = o(a^d)$. Then in order to show that $y = t$, we must show that $t \mid y$ and $y \mid t$. Since $d = (m, n)$, then there exists $\alpha, \beta \in \mathbb{Z}$ such that $d = \alpha m + \beta n$. Thus,

   $$t = o(a^d) = o(a^{\alpha m + \beta n}) = o(a^{\alpha m} \star a^{\beta n}) = o(a^{\alpha m} \star (a^n)^\beta) = o(a^{\alpha m} \star e^\beta) = o(a^{\alpha m}).$$

   Hence, $(a^{\alpha m})^t = e$. This can be rearranged to say $(a^m)^{\alpha t} = e$. Additionally, we also have that $(a^m)^y = e$. Thus, $(a^m)^y = (a^m)^{\alpha t}$. Thus, $(a^m)^{y - \alpha t} = e$. Since y is the smallest number such that $(a^m)^y = e$ and $y - \alpha t < y$, then $y - \alpha t = 0$. Thus, $y = \alpha t$. This implies that $t \mid y$. In the case that $\alpha < 0$, then since $(a^m)^{y + \alpha t} = e$, then $y + \alpha t < y$ would still imply that $y + \alpha t = 0$ and thus $y = -\alpha t$. So we still have that $t \mid y$.

   Since $d = (m, n)$, then $d \mid m$ and thus there exists some $k \in \mathbb{Z}$ such that $m = kd$. Thus, we have that $(a^d)^t = e$ and $(a^m)^y = (a^{kd})^y = (a^d)^{ky} = e$. Hence, $(a^d)^t = (a^d)^{ky}$. Multiplying both sides by $(a^d)^{-ky}$ yields $(a^d)^{t - ky} = e$. Since $t - ky < t$, then $t - ky = 0$. Thus, $t = ky$ which implies $y \mid t$. Thus, we have that $t \mid y$ and $y \mid t$. Thus, $t = y$. Therefore, $o(a^m) = o(a^d)$. □

   (b) Prove that $\langle a^m \rangle = \langle a^d \rangle$.

   Proof. Let $p \in \langle a^d \rangle$. Then for some $k \in \mathbb{Z}$, $p = (a^d)^k$. Note that in part (a) we showed that $a^d = a^{\alpha m}$ for some $\alpha \in \mathbb{Z}$. So then $(a^d)^k = (a^{\alpha m})^k = (a^m)^{\alpha k}$. Since $\alpha k \in \mathbb{Z}$, then $(a^m)^{\alpha k} \in \langle a^m \rangle$. Thus, $p \in \langle a^m \rangle$. Thus, $\langle a^d \rangle \subseteq \langle a^m \rangle$.

   Now let $p \in \langle a^m \rangle$. Then for some $k \in \mathbb{Z}$, $p = (a^m)^k$. However, since $d \mid m$, then for some $q \in \mathbb{Z}$, we have that $m = qd$. Thus, $(a^m)^k = (a^{qd})^k = (a^d)^{kq}$. Since $kq \in \mathbb{Z}$, then $(a^d)^{kq} \in \langle a^d \rangle$. Thus, $p \in \langle a^d \rangle$. Thus, $\langle a^m \rangle \subseteq \langle a^d \rangle$. Therefore, $\langle a^m \rangle = \langle a^d \rangle$. □

2. Assume that $(G, \star)$ is a cyclic group, $G = \langle a \rangle$, $(H, \star)$ is a subgroup of $(G, \star)$, and $H \neq \{e\}$.

   (a) Prove that $H = \langle a^k \rangle$, where k is the smallest positive integer such that $a^k \in H$.

   Proof. We are given that $(H, \star)$ is a subgroup of $(G, \star)$ and that $a^k \in H$. It follows from the definition of subgroup that H is closed under $\star$. So then let $g \in \langle a^k \rangle$. Then for some $m \in \mathbb{Z}$, $g = a^{mk}$. Since a^{mk} is the result of applying $\star$ on a^k m-many times with itself, then $a^{mk} \in H$ by the closure of H under $\star$. Thus, $g \in H$. Thus, $\langle a^k \rangle \subseteq H$.

Let $h \in H$. Since $H \subseteq G = \langle a \rangle$, then $h \in \langle a \rangle$ and so for some $m \in \mathbb{Z}$, $h = a^m$. Since k is the smallest positive integer such that $a^k \in H$, then $k \leq m$. Moreover, by the division algorithm, there exists $q, r \in \mathbb{Z}$, with $0 \leq r < k$ such that $m = qk + r$. Thus, $a^m = a^{qk+r} = a^{qk}a^r$. Assume that $r \neq 0$, then since $r < k$, it follows that $a^r \notin H$. Now consider

$$a^m = a^{qk}a^r = (a^k)^q a^r \Leftrightarrow (a^k)^{-q}a^m = a^r.$$

Since $(a^k)^q \in H$ and H is a subgroup, then $(a^k)^{-q} \in H$. Thus, a^r is the 'product' of two elements of H, namely $(a^k)^{-q}$ and a^m. Thus, $a^r \in H$. This is a contradiction. Thus, $r = 0$ and $a^m = a^{kq} = (a^k)^q$, which implies $a^m \in \langle a^k \rangle$. Thus, $h \in \langle a^k \rangle$. Thus, $H \subseteq \langle a^k \rangle$. Therefore, $H = \langle a^k \rangle$. □

(b) G/H is cyclic (since G is cyclic). Assume $[G\colon H] = t$. Prove that $t = k$.

Proof. If $[G\colon H] = t$, then there are t many distinct right (or left) cosets of H in G. Now consider the following cosets of H in G

$$\begin{aligned} H &= \{a^k, a^{2k}, a^{3k}, \ldots, e\} \\ Ha &= \{a^{k+1}, a^{2k+1}, a^{3k+1}, \ldots, a\} \\ Ha^2 &= \{a^{k+2}, a^{2k+2}, a^{3k+2}, \ldots, a^2\} \\ &\vdots \\ Ha^{k-1} &= \{a^{2k-1}, a^{3k-1}, a^{4k-1}, \ldots, a^{k-1}\} \end{aligned}$$

Clearly, there are k many of these cosets. Now we want to show that this set of cosets forms a partition on G. If we can show this, then it would imply that the list above is equal to G/H and that $t = k$.

First, let $A = \{H, Ha, Ha^2, \ldots, Ha^{k-1}\}$. To show that A forms a partition on G, we will take two arbitrary elements of A, call them Ha^i and Ha^j, and show that if $i = j$, then $Ha^i = Ha^j$ and if $i \neq j$, then $Ha^i \cap Ha^j = \varnothing$. The first case follows immediately, for if $i = j$, then $Ha^i = Ha^i = Ha^j$.

Now assume that $i \neq j$. Let $a^s \in Ha^i \cap Ha^j$. Then we have that $a^s \in Ha^i$. Thus, $a^s = a^{lk+i}$, for some $0 \leq l < k$. Similarly, $a^s \in Ha^j$. Thus, $a^s = a^{mk+j}$, for some $0 \leq m < k$. Thus, $a^{lk+i} = a^{mk+j}$, which can be written as $a^{lk} \star a^i = a^{mk} \star a^j$. Since $0 \leq i, j < k$ and $i \neq j$, then $a^i \neq a^j$. Moreover, because $0 \leq l, m < k$, then if $l = m$ this would imply that $a^{mk} \star a^i = a^{mk} \star a^j$ and thus $a^i = a^j$ which is a contradiction. Thus, if $l \neq m$, then $a^{lk} \neq a^{mk}$. Thus, $a^{lk+i} \neq a^{mk+j}$, which is a contradiction. Thus, $a^s \notin Ha^i \cap Ha^j$. Therefore, $Ha^i \cap Ha^j = \varnothing$ and the elements of A are mutually disjoint.

Now we must show that $G = \cup A$. Clearly, $\cup A \subseteq G$ since A contains, as its elements, subsets of G. Let $a^y \in G$. Then either $0 \leq y < k$, or $k \leq y < o(a)$. If $0 \leq y < k$, then $a^y \in Ha^y \in A$ and thus $a^y \in \cup A$. If $k \leq y < o(a)$, then $y = nk + m$ for some $m, n \in \mathbb{Z}^+$ such that $m < k$ and $nk + m < o(a)$. Thus, $a^y = a^{nk+m} = (a^k)^n \star a^m \in Ha^m$. Thus, $a^y \in \cup A$ and hence $G \subseteq \cup A$. Therefore, $G = \cup A$ and A forms a partition on G. Thus, $A = G/H$ and $[G\colon H] = k$. □

3. Assume that $(G, \star)$ is a group. $Z(G) = \{a \in G \mid \forall g \in G \colon a \star g = g \star a\}$, and if $x \in G$, then $N(x) = \{y \in G \mid y \star x = x \star y\}$. Prove that $Z(G) \subseteq_g G$, and that $a \in Z(G)$ iff $N(a) = G$.

Proof. To prove that $Z(G) \subseteq_g G$, we must show, by the corollary on pg.4, that $Z(G) \neq \varnothing$ and $a \star b^{-1} \in Z(G)$ whenever $a, b \in Z(G)$. We can see that $e \in Z(G)$ since for all $g \in G$, $e \star g = g = g \star e$. Thus, $Z(G) \neq \varnothing$. Now let $a, b \in Z(G)$. Then since $a \in Z(G)$, it follows that $\forall g \in G$, $a \star g = g \star a$ and since $b^{-1} \in G$, then $a \star b^{-1} = b^{-1} \star a$. Similarly, since $b \in Z(G)$, then $b \star g = g \star b$. Multiplying both sides on the left by b^{-1} we get that $g = b^{-1} \star g \star b$. Then multiplying both sides on the right by b^{-1}, we get $g \star b^{-1} = b^{-1} \star g$. Thus, $b^{-1} \in Z(G)$. Finally, letting $g \in G$ and using all the previous equalities we obtain

$$\begin{aligned}(a \star b^{-1}) \star g &= a \star (b^{-1} \star g) \\ &= a \star (g \star b^{-1}) \\ &= (a \star g) \star b^{-1} \\ &= (g \star a) \star b^{-1} \\ &= g \star (a \star b^{-1}).\end{aligned}$$

Thus, $a \star b^{-1} \in Z(G)$. Thus, $Z(G) \subseteq_g G$.

Assume $a \in Z(G)$. Then $a \star g = g \star a$ for all $g \in G$. Thus, the set of all elements which commute with a is every element of G. Hence, $N(a) = G$. Now assume $N(a) = G$. Then $a \star g = g \star a$ for all $g \in G$. Thus, $a \in Z(G)$. Therefore, $a \in Z(G)$ iff $N(a) = G$. $\square$

4. Assume that $(G, \star)$ is a group, $H \subseteq_g G$, $a \in G$, and $aHa^{-1} = \{a \star h \star a^{-1} \colon h \in H\}$.

   (a) Prove that $H \lhd G$ iff for all $g \in G$, $gHg^{-1} = H$, iff for all $g \in G$, $Hg = gH$.

   Proof. ($\Rightarrow$) Assume $H \lhd G$. Then by definition, for all $g \in G$ and for all $h \in H$, $g \star h \star g^{-1} \in H$. We want to show that this implies that for all $g \in G$, $gHg^{-1} = H$. First, we will show that for any $g \in G$, $gHg^{-1} \subseteq H$. Let $g \in G$ and let $a \in gHg^{-1}$. Then for some $h' \in H$, $a = g \star h' \star g^{-1}$. However, by assumption we have that for all $g \in G$ and all $h \in H$, $g \star h \star g^{-1} \in H$. Thus, $a = g \star h' \star g^{-1} \in H$. Hence $gHg^{-1} \subseteq H$. Now we want to show that for any $g \in G$, $H \subseteq gHg^{-1}$. Let $g \in G$ and let $h' \in H$. Then by assumption, $g^{-1} \star h' \star g \in H$, since $g^{-1} \star h' \star g = (g^{-1}) \star h' \star (g^{-1})^{-1}$. Thus, if we let $h \in H$ such that $h = g^{-1} \star h' \star g$, then $h' = g \star h \star g^{-1}$. Thus, $h' \in gHg^{-1}$. Hence, $H \subseteq gHg^{-1}$. Therefore, for all $g \in G$, $gHg^{-1} = H$.

   ($\Rightarrow$) Assume that for all $g \in G$, $gHg^{-1} = H$. We want to show that this implies that for all $g \in G$, $Hg = gH$. First, we will show that for all $g \in G$, $Hg \subseteq gH$. Let $g \in G$ and let $a \in Hg$. Then $a = h' \star g$, for some $h' \in H$. Since $h' \in H$, then our assumption implies that for some $h \in H$, $h' = g \star h \star g^{-1}$. Thus, multiplying both sides on the right by g, we obtain $h' \star g = g \star h$ and since $a = h' \star g$, then $a = g \star h$. Thus, $a \in gH$. Hence, $Hg \subseteq gH$. Now let $a \in gH$. Then for some $h' \in H$, $a = g \star h'$. Thus, $a \star g^{-1} = h' \in H$. Thus, $a = (a \star g^{-1}) \star g \in Hg$. Hence, $gH \subseteq Hg$. Therefore, for all $g \in G$, $Hg = gH$.

($\Rightarrow$) Assume that for all $g \in G$, $Hg = gH$. We want to show that this implies that $H \triangleleft G$. Thus, we need to show that for all $g \in G$ and for all $h \in H$, $g \star h \star g^{-1} \in H$. Let $g \in G$ and $h \in H$. Then for some $h' \in H$, we have that $g \star h = h' \star g$. Multiplying both sides by g^{-1}, we obtain that $g \star h \star g^{-1} = h' \in H$. Thus, for all $g \in G$ and for all $h \in H$, $g \star h \star g^{-1} \in H$. Therefore, $H \triangleleft G$. $\square$

(b) Prove that aHa^{-1} is a subgroup of G, and prove that $o(aHa^{-1}) = o(H)$.

Proof. To prove $aHa^{-1} \subseteq_g G$, we must show that $aHa^{-1} \neq \varnothing$ and we must show that $x \star y^{-1} \in aHa^{-1}$ whenever $x, y \in aHa^{-1}$. We know that $e \in H$, and since $a \star e \star a^{-1} = e$, then $e \in aHa^{-1}$. Thus, $aHa^{-1} \neq \varnothing$. Now let $x, y \in aHa^{-1}$. Then for some $h_1, h_2 \in H$, we have that $x = a \star h_1 \star a^{-1}$ and $y = a \star h_2 \star a^{-1}$. Note that $y^{-1} = a \star h_2^{-1} \star a^{-1}$. Thus,

$$\begin{aligned} x \star y^{-1} &= (a \star h_1 \star a^{-1}) \star (a \star h_2^{-1} \star a^{-1}) \\ &= a \star h_1 \star (a^{-1} \star a) \star h_2^{-1} \star a^{-1} \\ &= a \star (h_1 \star h_2^{-1}) \star a^{-1}. \end{aligned}$$

Since $h_1 \star h_2^{-1} \in H$, then $a \star (h_1 \star h_2^{-1}) \star a^{-1} \in aHa^{-1}$. Thus, $x \star y^{-1} \in aHa^{-1}$. Therefore, $aHa^{-1} \subseteq_g G$.

To prove that $o(aHa^{-1}) = o(H)$, we will show that there exists a bijective map from aHa^{-1} to H. Let $f \colon aHa^{-1} \to H$ be a map defined as

$$f(x) = a^{-1} \star x \star a$$

for all $x \in aHa^{-1}$. To show that this map is 1-1, let $x_1, x_2 \in aHa^{-1}$ such that $f(x_1) = f(x_2)$. Then we need to show that this implies $x_1 = x_2$. Since $x_1, x_2 \in aHa^{-1}$, then for some $h_1, h_2 \in H$, we have that $x_1 = a \star h_1 \star a^{-1}$ and that $x_2 = a \star h_2 \star a^{-1}$. It follows from the definition of f that

$$\begin{aligned} f(x_1) &= f(a \star h_1 \star a^{-1}) \\ &= a^{-1} \star (a \star h_1 \star a^{-1}) \star a \\ &= (a^{-1} \star a) \star h_1 \star (a^{-1} \star a) \\ &= e \star h_1 \star e \\ &= h_1. \end{aligned}$$

Similarly,

$$\begin{aligned} f(x_2) &= f(a \star h_2 \star a^{-1}) \\ &= a^{-1} \star (a \star h_2 \star a^{-1}) \star a \\ &= (a^{-1} \star a) \star h_2 \star (a^{-1} \star a) \\ &= e \star h_2 \star e \\ &= h_2. \end{aligned}$$

Thus, $f(x_1) = f(x_2)$ implies that $h_1 = h_2$. Multiplying both sides on the right by a and both sides on the left by a^{-1}, We get that $a \star h_1 \star a^{-1} = a \star h_2 \star a^{-1}$. Hence, $x_1 = x_2$ and f is thereby injective.

To prove that f is surjective, we must show that for all $h \in H$, there exists some $x \in aHa^{-1}$, such that $f(x) = h$. Let $h \in H$. Then let $x = a \star h \star a^{-1}$. Clearly, $x \in aHa^{-1}$, and we also find that $f(x) = f(a \star h \star a^{-1}) = h$. Hence, f is surjective. Thus, f is a bijective map from aHa^{-1} to H. Therefore, $o(aHa^{-1}) = o(H)$. □

(c) Assume that H is the only subgroup of G whose order is $o(H)$. Prove that $H \triangleleft G$.

Proof. From the previous result, we have that for any $a \in G$, $aHa^{-1} \subseteq_g G$ and that $o(aHa^{-1}) = o(H)$. Thus, it follows that $H = aHa^{-1}$. Moreover, from the result obtained in 4.(a), this implies that $H \triangleleft G$. □

5. Assume that $(G, \star)$ is a group, $H \subseteq_g G$, and that $[G : H] = 2$. Prove that $H \triangleleft G$.

Proof. Let $a \in G$. Then $a \in H$ or $a \notin H$. If $a \in H$, then $aH \subseteq H$ since for any $x \in aH$, we have that $x = a \star h$, where both $a, h \in H$ and so $a \in H$. Similarly, for any $h \in H$, we have that $h = a \star (a^{-1} \star h)$ and thus, $x \in aH$. Thus, $H \subseteq aH$. Hence, $aH = H = Ha$. If $a \notin H$, then $a \in G - H$. Thus, $aH = G - H = Ha$. Thus, for any $a \in G$, $Ha = aH$. Therefore, $H \triangleleft G$. □

6. Assume that $(G, \star)$ is a group, $(H, \star)$ is a subgroup of G, and R is defined on G by aRb iff $a \star b^{-1} \in H$. Recall that R is an equivalence relation on G.

(a) If $G = S_4$, and $H = \{(1), (12), (34), (12)(34)\}$, prove that R is not a congruence relation.

Proof. Consider the elements (13) and (132). Note that $(132)^{-1} = (123)$ and so $(13) \star (123) = (12)$. Thus, $(13) \star (132)^{-1} \in H$ and so $(13)R(132)$. Next, consider the elements (14) and (142). Note that $(142)^{-1} = (124)$. Thus, $(14) \star (124) = (12)$. Thus, $(14) \star (142)^{-1} \in H$. Thus, $(14)R(142)$. Lastly, consider the products $(13) \star (14) = (143)$ and $(132) \star (142) = (14) \star (23)$. Also note that $((14) \star (23))^{-1} = (14) \star (23)$. Thus, $(143) \star (14) \star (23) = (132)$. We see that $(132) \notin H$. Thus, it is not true that for all $a, b, c, d \in G$, aRb and cRd implies $(a \star c)R(b \star d)$. Therefore, R is not a congruence relation. □

(b) Prove that if $H \triangleleft G$, then R is a congruence relation.

Proof. Assume that $H \triangleleft G$. Then for $a, b, c, d \in G$, assume aRb and cRd. Then we have that $a \star b^{-1} \in H$ and $c \star d^{-1} \in H$. We want to show that $(a \star c) \star (b \star d)^{-1} \in H$. We see that $(a \star c) \star (b \star d)^{-1} = a \star (c \star d^{-1}) \star b^{-1}$. Additionally, since $c \star d^{-1} \in H$, let $h = c \star d^{-1}$. Then we have

$$\begin{aligned} a \star h \star b^{-1} &= (a \star h \star b^{-1}) \star (b \star a^{-1}) \star (a \star b^{-1})^{-1} \\ &= (a \star h \star a^{-1}) \star (b \star a^{-1}). \end{aligned}$$

Since H is normal, then $aHa^{-1} = H$ and so $a \star h \star a^{-1} \in H$. Moreover, since $a \star b^{-1} \in H$, then $(a \star b^{-1})^{-1} = (b \star a^{-1}) \in H$. Thus, $(a \star h \star a^{-1}) \star (b \star a^{-1}) \in H$. Hence,

$$a \star h \star b^{-1} = a \star (c \star d^{-1}) \star b^{-1} = (a \star c) \star (b \star d)^{-1} \in H.$$

Thus, aRb and cRd implies $(a \star c)R(b \star d)$, for all $a, b, c, d \in G$. Therefore, R is a congruence relation. $\square$