Russ Johnson
Problem Set #4
March 12, 2013

(4)
(a) Show that U_{22} is cyclic.

The congruence class [7] is a generator of U_{22} and therefore U_{22} is cyclic.

$$U_{22} = \langle[7]\rangle = \{[7], [5], [13], [3], [21], [15], [17], [9], [19], [1]\}.$$

(b) Find all the generators of U_{22}. Explain how you know that each element is a generator.

We know that U_{22} is a group and therefore is closed under its operation. Therefore, by finding an element in U_{22} with the same order as U_{22}, we are guaranteed that this is a generator of U_{22}. The order of U_{22} is 10 and from part (a) we already have the generator [7] with order 10. From Theorem 21.3 part (ii) we know that the order of $[7]^k$ for some positive integer k is equal to $\dfrac{10}{gcd(k,10)}$. Therefore, when k and 10 are coprime, we know that the order of $[7]^k$ is 10 and is a generator of U_{22}. And so, the generators of U_{22} are $[7]^3 = [13]$, $[7]^7 = [17]$, and $[7]^9 = [19]$.

(5) Let $A = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}$.
(a) Find $|A|$ and $|B|$.

We note that $\langle A\rangle = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\}$ and $\langle B\rangle = \left\{ \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\}$. And so, $|A| = |B| = 2$.
(b) Determine $|AB|$. Does your answer surprise you? Explain.

First of all,

$$AB = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix},$$

$$AB^2 = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix},$$

and

$$AB^3 = \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix}.$$

From this we see that

$$\langle AB\rangle = \left\{ \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} | a \in \mathbb{N} \right\}.$$

And so, AB has infinite order. This answer is somewhat surprising, but by multiplying A and B we obtain a matrix that is not in $\langle A\rangle$ or $\langle B\rangle$ and so we cannot expect it to be finite.

(9) Prove Theorem 21.5.

Proof. Let $G = \langle a\rangle$ be an infinite cyclic group with identity e, and let $b \neq e$ be an element in G. Let $m, n \in \mathbb{Z}^+$ such that

$$b^m = b^n. \tag{1}$$

The element a is the generator of G and therefore there must exist some positive integer k such that

$$a^k = b. \tag{2}$$

Raising both sides of equation (2) to the power of m we obtain

$$a^{km} = b^m. \tag{3}$$

Raising both sides of equation (2) to the power of n we obtain

$$a^{kn} = b^n. \tag{4}$$

From equations (1), (3), and (4) we know that

$$a^{kn} = a^{km}. \tag{5}$$

The element a has infinite order and so from (5) we know that

$$kn = km. \tag{6}$$

Applying the Group Cancellation Rule to (6) we obtain

$$n = m.$$

In conclusion, we have shown that if $b^m = b^n$ for some positive integer powers m and n, then $m = n$. The contrapositive of this is that all integer powers of b are distinct. And so by proving this fact we have shown that $\langle b\rangle$ is an infinite cyclic group. The fact that $\langle b\rangle$, is a cyclic group comes from the Theorem 21.1 and the unique powers proof means that b has infinite order. □

(18) Let G be a group and let $a, b \in G$ with $|a| = b$ and $|b| = m$.
(a) Is it necessarily true that $|ab| = mn$?
(b) If $ab = ba$, is it necessarily true that $|ab| = mn$?

This counter-example works for parts (a) and (b). The congruence classes

[7] and [7] are both in U_{22}. We have already shown that [7] has an order of 10 and U_{22} also has an order of 10. It is impossible for an element in U_{22} to have an order of 100, which is greater than the order of the group and so it is not necessarily true that $|ab| = mn$ when the elements commute.

(c) Prove that if $ab = ba$ and $gcd(m, n) = 1$, then the order of ab is mn.

Proof. First of all we have must show that ab has finite order. We know that $ab = ba$ and so

$$(ab)^{nm} = a^{nm}b^{nm} = (a^n)^m(b^m)^n = e^m e^n = e.$$

From this we see that ab does have finite order. Let q be the order of ab. From Theorem 21.2 (ii) we know that $q|nm$. From Theorem 21.2 (i) we know that

$$(ab)^q = e. \tag{7}$$

Raising both sides of equation (7) to the power of m we obtain

$$(ab)^{qm} = a^{qm}b^{qm} = a^{qm}e^q = a^{qm} = e.$$

From this and Theorem 21.2 (ii) we know that $n|qm$ and because m and n are coprime $n|q$. Raising both sides of equation (7) to the power of n we obtain

$$(ab)^{qn} = a^{qn}b^{qn} = e^q b^{qn} = b^{qn} = e.$$

From this and Theorem 21.2 (ii) we know that $m|qn$ and because m and n are coprime $m|q$. Because $n|q$, $m|q$ and m and n are coprime we can conclude that $mn|q$. We have already shown that $q|mn$, and so we can conclude that $mn = q$. In other words, the order of ab is equal to the product of the orders of a and b. $\square$

(2) Let n be an integer with $n \geq 3$.
(a) If n is even, show that the center of D_n is not trivial. Then find all of the elements in $Z(D_n)$.
(b) If n is odd, find all elements in $Z(D_n)$.
Let R be the smallest rotation in D_n and let r be any reflection in D_n. We know that any element of D_n can be written as a power of R or r times a power of R. In other words

$$D_n = \{R^k | 0 \leq k < n\} \cup \{rR^k | 0 \leq k < n\}.$$

We are looking for elements in D_n that commute with all other elements in D_n. In other words, $x \in D_n$ is in the center of D_n if and only if $ax = xa$ for all $a \in D_n$.

Assume that p be an integer such that $0 \leq p < n$ and rR^p is in the center of D_n. We will prove that this leads to a contradiction. Because rR^p is in the center of D_n

$$(rR^p)R^k = R^k(rR^p) \tag{8}$$

for all $k \in \mathbb{Z}$ such that $0 \leq k < n$. Applying the associative property to (8) we obtain

$$(rR^p)R^k = (R^k r)R^p \tag{9}$$

Next we substitute $R^k r$ with rR^{-k} coming from the presentation of D_n

$$(rR^p)R^k = (rR^{-k})R^p. \tag{10}$$

Next we apply the associative property to (10) to obtain

$$(rR^p)R^k = r(R^{-k}R^p). \tag{11}$$

Next we commute the rotations on the right side of (11) to obtain

$$(rR^p)R^k = r(R^p R^{-k}). \tag{12}$$

Next we apply the associative property to (12) to obtain

$$(rR^p)R^k = (rR^p)R^{-k}. \tag{13}$$

Finally we apply the group cancellation law to (13) and arrive at

$$R^k = R^{-k}.$$

The inverse of a rotation is not always the rotation itself, except when we are working with $n \leq 2$. Since we are working with $n \geq 3$ we can conclude that there is no such integer p such that rR^p is in the center of D_n when $n \geq 3$.

Next we assume that p is an integer such that $0 \leq p < n$ and R^p is in the center of D_n. Because R^p is in the center of D_n,

$$R^p R^k = R^k R^p$$

and

$$R^p(rR^k) = (rR^k)R^p$$

for all $k \in \mathbb{Z}$ such that $0 \leq k < n$. The first equation is true for any p, because rotations commute with each other. For the second equation we first apply the associative property to the right side of the equation to obtain

$$R^p(rR^k) = r(R^k R^p). \tag{14}$$

Next we apply the knowledge that rotations commute with one other to the right side of equation (14) to obtain

$$R^p(rR^k) = r(R^p R^k). \tag{15}$$

Applying the associative property to the right side of (15), we obtain

$$R^p(rR^k) = (rR^p)R^k. \tag{16}$$

Next we substitute rR^p with $R^{-p}r$ coming from the presentation of D_n

$$R^p(rR^k) = (R^{-p}r)R^k. \tag{17}$$

We then apply the associative property to (17) to obtain

$$R^p(rR^k) = R^{-p}(rR^k). \tag{18}$$

Finally, applying the group cancellation law to (18) we arrive at

$$R^p = R^{-p}.$$

This is true when $p = 0$ regardless of whether n is even or odd. In this case, $R^0 = R^{-0} = I$. The other case when this is possible is when $p = n/2$. When n is odd $n/2$ is not an integer, but when n is even $n/2$ is an integer.

In conclusion, when n is odd $Z(D_n) = \{I\}$ and when n is even $Z(D_n) = \{I, R^{n/2}\}$.

(10) Let n be an integer greater than 2. Prove that the center of S_n is $\{I\}$, where I is the identity permutation in S_n.

Proof. We know from its definition that the identity I of S_n commutes with all elements of this group and so $I \in Z(S_n)$. Now we will prove that there is no other element in the center of S_n. Let $p \in S_n$ not equal to the identity of S_n. Because p is not the identity, we know that there exist distinct points i and j such that $p(i) = j$. Because $n \geq 3$, there exists some $q \in S_n$ such that $q(j) = k$ and $q(k) = j$ with $k \neq i$ and $k \neq j$ and fixes everything else. The permutation q fixes the point i and so q^{-1} must also fix i. And so,

$$qpq^{-1}(i) = qp(i) = q(j) = k.$$

If the permutation p commuted with all other elements in S_n, we would have

$$qpq^{-1}(i) = qq^{-1}p(i) = j.$$

Since we know that $k \neq j$, we can conclude that the permutation p does not commute with all other elements in S_n. The only condition that we placed on the permutation p was that it is not the identity, and so the only element in $Z(S_n)$ is I. $\square$

(12) When is the cycle $(a_1a_2 \cdots a_k)$ in S_n even and when is it odd?

Conjecture. When k is an even integer such that $k \geq 1$ the cycle $(a_1a_2 \cdots a_k)$ in S_n is odd and when k is an odd integer such that $k \geq 1$ the cycle $(a_1a_2 \cdots a_k)$ in S_n is even.

Proof. Let $k = 2$. The cycle (a_1a_2) is itself a single transposition and therefore is odd. From this we have our base step for a proof by induction. Next assume that k is even and $(a_1a_2 \cdots a_k)$ is an odd cycle. We will prove that $(a_1a_2 \cdots a_ka_{k+1}a_{k+2})$ is an odd cycle. Because $(a_1a_2 \cdots a_k)$ is an odd cycle, we also know that its factorization $(a_1a_k)(a_1a_{k-1}) \cdots (a_1a_2)$ is made up of an odd number of transpositions. The cycle $(a_1a_2 \cdots a_ka_{k+1}a_{k+2})$ can be decomposed as $(a_1a_{k+2})(a_1a_{k+1})(a_1a_k)(a_1a_{k-1}) \cdots (a_1a_2)$ which has contains exactly two more transpositions than $(a_1a_k)(a_1a_{k-1}) \cdots (a_1a_2)$ and therefore $(a_1a_2 \cdots a_ka_{k+1}a_{k+2})$ is an odd cycle. By induction we have shown that if k is a positive even integer then the cycle $(a_1a_2 \cdots a_k)$ is odd.

Next we let $k = 1$. This gives us the identity which we know to be an even cycle. From this we have our base step for a proof by induction. Next assume that k is odd and $(a_1a_2 \cdots a_k)$ is an even cycle. We will prove that $(a_1a_2 \cdots a_ka_{k+1}a_{k+2})$ is an even cycle. Because $(a_1a_2 \cdots a_k)$ is an even cycle, we also know that its factorization $(a_1a_k)(a_1a_{k-1}) \cdots (a_1a_2)$ is made up of an even number of transpositions. The cycle $(a_1a_2 \cdots a_ka_{k+1}a_{k+2})$ can be decomposed as $(a_1a_{k+2})(a_1a_{k+1})(a_1a_k)(a_1a_{k-1}) \cdots (a_1a_2)$ which has contains exactly two more transpositions than $(a_1a_k)(a_1a_{k-1}) \cdots (a_1a_2)$ and therefore $(a_1a_2 \cdots a_ka_{k+1}a_{k+2})$ is an even cycle. By induction we have shown that if k is a positive odd integer then the cycle $(a_1a_2 \cdots a_k)$ is even.

$\square$