Russ Johnson
Problem Set #4
March 10, 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 $\langle b\langle$ is an infinite cyclic group. The fact that $\langle b\langle$, 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 for an element in U_{22} to have an order of 100, which is greater than the order of the group.

(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. By 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. □

(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 $Z(D_n)$.

(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.

(12) When is the cycle $(a_1 a_2 \cdots a_k)$ in S_n even and when is it odd?
When k is an even integer greater than or equal to zero