Solutions to Homework #4

1. Saracino, Section 4, Problem 4.5: Let G be a group, and let $x \in G$ be an element of order 18. Find the orders of $x^2, x^3, x^4, x^5, x^{12}$.

Solution. By Theorem 4.4(iii), we have $o(x^m) = 18/d$, where $d = (m, 18)$, for each $m \in \mathbb{Z}$. [Remember that (m, n), also denoted $\gcd(m, n)$, is the greatest common divisor of m and n.] We have

$$(2, 18) = 2, \quad (3, 18) = 3, \quad (4, 18) = 2, \quad (5, 18) = 1, \quad (12, 18) = 6,$$

so Theorem 4.4(iii) gives

$$\boxed{o(x^2) = 9, \quad o(x^3) = 6, \quad o(x^4) = 9, \quad o(x^5) = 18, \quad o(x^{12}) = 3}$$

---

2. Saracino, Section 4, Problem 4.6: List all the elements of $(C_{45}, \oplus)$ that are of order 15. As always, justify your answer.

Solution. We know 1 is a generator for C_{45}, and any $n \in C_{45}$ has order $o(n) = 45/(n, 45)$ by Theorem 4.4(iii). Thus, we are looking for all those $n \in C_{45}$ for which $(n, 45) = 3$.
Since 45 has prime factorization $3^2 \cdot 5$, this means we are looking for all integers n from 0 to 44 that are divisible by 3 but *not* by 9 or 5. Listing *all* the multiples of 3 between 0 and 44 gives:

$$0, 3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42.$$

Discarding the multiples of 5 and the multiples of 9, this means the answer to the question is:

$$\boxed{3, 6, 12, 21, 24, 33, 39, 42}$$

are the elements of C_{45} of order 15.

---

3. Saracino, Section 4, Problem 4.10(a): Let $G = \{1, 2, 3, 4, 5, 6\}$ and define an operation $\odot$ on G by $a \odot b = \overline{ab}$, the remainder of $ab \pmod 7$. For instance, $2 \odot 4 = \overline{8} = 1$, and $5 \odot 6 = \overline{30} = 2$. Prove that $(G, \odot)$ is a group.

Proof. **Bin Op**: Given $a, b \in G$, neither a nor b is divisible by 7, so ab is also not divisible by 7, since 7 is prime. Thus, $a \odot b = \overline{ab} \neq 0$, since $ab \not\equiv 0 \pmod 7$. Since remainders mod 7 are between 0 and 6, and this one is not 0, we have $a \odot b \in G$.

Assoc: First, observe that for any integers $x, y \in \mathbb{Z}$, we have $x \equiv \overline{x} \pmod 7$, and hence by HW 3, Problem 6, we have $\overline{\overline{x}y} = \overline{xy}$.

We now use this fact to prove associativity. Given $a, b, c \in G$, we have

$$(a \odot b) \odot c = \overline{(\overline{ab})c} = \overline{(ab)c} = \overline{a(bc)} = \overline{a(\overline{bc})} = a \odot (b \odot c),$$

where the second and fourth equalities are by the observation about $\overline{\overline{x}y} = \overline{xy}$.

Identity. Let $e = 1 \in G$. Then for any $a \in G$, we have $a \odot e = \overline{a1} = \overline{a} = a$, since $1 \leq a \leq 6$, so the remainder of a mod 7 is a itself. Similarly, $e \odot a = \overline{1a} = \overline{a} = a$.

Inverses. Observe the following computations:

$$1 \odot 1 = 1, \quad 2 \odot 4 = 4 \odot 2 = \overline{8} = 1, \quad 3 \odot 5 = 5 \odot 3 = \overline{15} = 1, \quad 6 \odot 6 = \overline{36} = 1.$$

Thus, each of the elements of G has an inverse; the above list shows $1^{-1} = 1$, $2^{-1} = 4$, $3^{-1} = 5$, $4^{-1} = 2$, $5^{-1} = 3$, and $6^{-1} = 6$. QED

---

4. Saracino, Section 4, Problem 4.10(b): Is the group $(G, \odot)$ above cyclic? Prove or disprove.

Answer/Proof. $\boxed{\text{YES}}$ In particular, we claim 3 is a generator for G. To verify this, we compute:

$$3^0 = 1, \quad 3^1 = 3, \quad 3^2 = 3 \odot 3 = 2, \quad 3^3 = 3 \odot 2 = 6, \quad 3^4 = 3 \odot 6 = 4, \quad 3^5 = 3 \odot 4 = 5.$$

Thus, every element of G is 3^n for some n, so $\langle 3 \rangle = G$, i.e., 3 is indeed a generator of G. QED

[**Note**: 5 is also a generator; that is, $G = \langle 5 \rangle$. No other element of G is a generator, though.]

5. Saracino, Section 4, Problem 4.20: Let G be a group and $a \in G$. We say an element $b \in G$ is a *conjugate* of a if there exists $x \in G$ such that $b = xax^{-1}$. Show that any conjugate of a has the same order as a.

Proof. Given $a, x \in G$, let $b = xax^{-1}$. Let $S = \{n \geq 1 : a^n = e\}$ and $T = \{n \geq 1 : b^n = e\}$. We claim that $S = T$.
To show $S \subseteq T$: Given $n \in S$, then by HW 3, Problem 7, $b^n = (xax^{-1})^n = xa^n x^{-1} = xex^{-1} = e$, and therefore $n \in T$.
To show $T \subseteq S$: First note that $a = x^{-1}bx$, and that $x = (x^{-1})^{-1}$. So given $n \in T$, we have $a^n = (x^{-1}bx)^n = x^{-1}b^n x = x^{-1}ex = e$, and hence $n \in S$.
We have shown our claim that $S = T$. If $S = T = \varnothing$, then a and b are both of infinite order, so $o(a) = o(b)$. On the other hand, if $S = T$ is nonempty, then since $o(a)$ is the smallest element of S and $o(b)$ is the smallest element of $T = S$, we have $o(a) = o(b)$. QED

[**Note 1**: A common mistake on this problem is to say that $(xax^{-1})^n = x^n a^n x^{-n}$. This is **FALSE**.]

[**Note 2**: Another common mistake on this problem is to assume that a has finite order. (E.g., "Let $n = o(a)$," and then treating n like it's a number. You can't make that assumption, because the problem didn't say that you could. So you need to prove it BOTH in the case that $o(a) < \infty$ AND in the case that $o(a) = \infty$.]

---

6. Saracino, Section 4, Problem 4.21: Let G be a group and $x, y \in G$. Prove that $o(xy) = o(yx)$.

Proof 1. Let $S = \{n \geq 1 : (xy)^n = e\}$ and $T = \{n \geq 1 : (yx)^n = e\}$.
Lemma. $S = T$.
Proof of Lemma. ($\subseteq$): Given $n \in S$, we have $(xy)^n = e$, so $(xy)^{n-1} = (xy)^{-1} = y^{-1}x^{-1}$. Thus,

$$(yx)^n = yxyx \cdots yx = y(xy \cdots xy)x = y(xy)^{n-1}x = y(y^{-1}x^{-1})x = ee = e,$$

and hence $n \in T$.
($\supseteq$): Similar. QED Lemma

Having shown that $S = T$: If $S = T = \varnothing$, then $o(xy) = \infty = o(yx)$. Or, if $S = T \neq \varnothing$, then since $o(xy)$ is the smallest element of S and $o(yx)$ is the smallest element of $T = S$, we have $o(xy) = o(yx)$. QED

Proof 2. Note $yx = y(xy)y^{-1}$ is a conjugate of xy. Thus, $o(xy) = o(yx)$ by Problem 4.20. QED

[**Note**: The "dot-dot-dot" part of the proof of the Lemma (in Proof 1 above) means that we really should have done induction on n to prove that $(yx)^n = y(xy)^{n-1}x$ for every $n \geq 1$.]