Homework #4 Solutions

p 67, #8. In $U(14)$ we have

$$\begin{aligned}
3^2 \bmod 14 &= 9\\
3^3 \bmod 14 &= 27 \bmod 14 = 13\\
3^4 \bmod 14 &= 3\cdot 13 \bmod 14 = 39 \bmod 14 = 11\\
3^5 \bmod 14 &= 3\cdot 11 \bmod 14 = 33 \bmod 14 = 5\\
3^6 \bmod 15 &= 3\cdot 5 \bmod 14 = 15 \bmod 14 = 1
\end{aligned}$$

and

$$\begin{aligned}
5^2 \bmod 14 &= 25 \bmod 14 = 11\\
5^3 \bmod 14 &= 5\cdot 11 \bmod 14 = 55 \bmod 14 = 13\\
5^4 \bmod 14 &= 5\cdot 13 \bmod 14 = 65 \bmod 14 = 9\\
5^5 \bmod 14 &= 5\cdot 9 \bmod 14 = 45 \bmod 14 = 3\\
5^6 \bmod 15 &= 5\cdot 3 \bmod 14 = 15 \bmod 14 = 1.
\end{aligned}$$

Hence $\langle 3\rangle = \langle 5\rangle = \{1, 3, 5, 9, 11, 13\} = U(14)$.

p 68, # 16.

Lemma 1. *Let G, $x \in G$ and $k \in \mathbb{Z}$. Then*

$$C(x) \leq C(x^k).$$

Proof. If $y \in C(x)$ then $x = yxy^{-1}$ so that $x^k = (yxy^{-1})^k = yx^ky^{-1}$ (the latter equality was proven in class) and hence $y \in C(x^k)$. □

If we apply the lemma with $x = a$, $k = -1$ we have

$$C(a) \leq C(a^{-1})$$

while if we take $x = a^{-1}$ we get

$$C(a^{-1}) \leq C((a^{-1})^{-1}) = C(a).$$

proving that $C(a) = C(a^{-1})$.

p 68, # 24. We will prove the following more general fact.

Proposition 1. *Let G be a group, $a \in G$ and suppose $|a| = n$. If $(k, n) = 1$ then*

$$C(a) = C(a^k).$$

Proof. Taking $x = a$ in the lemma of the preceding problem immediately gives

$$C(a) \leq C(a^k).$$

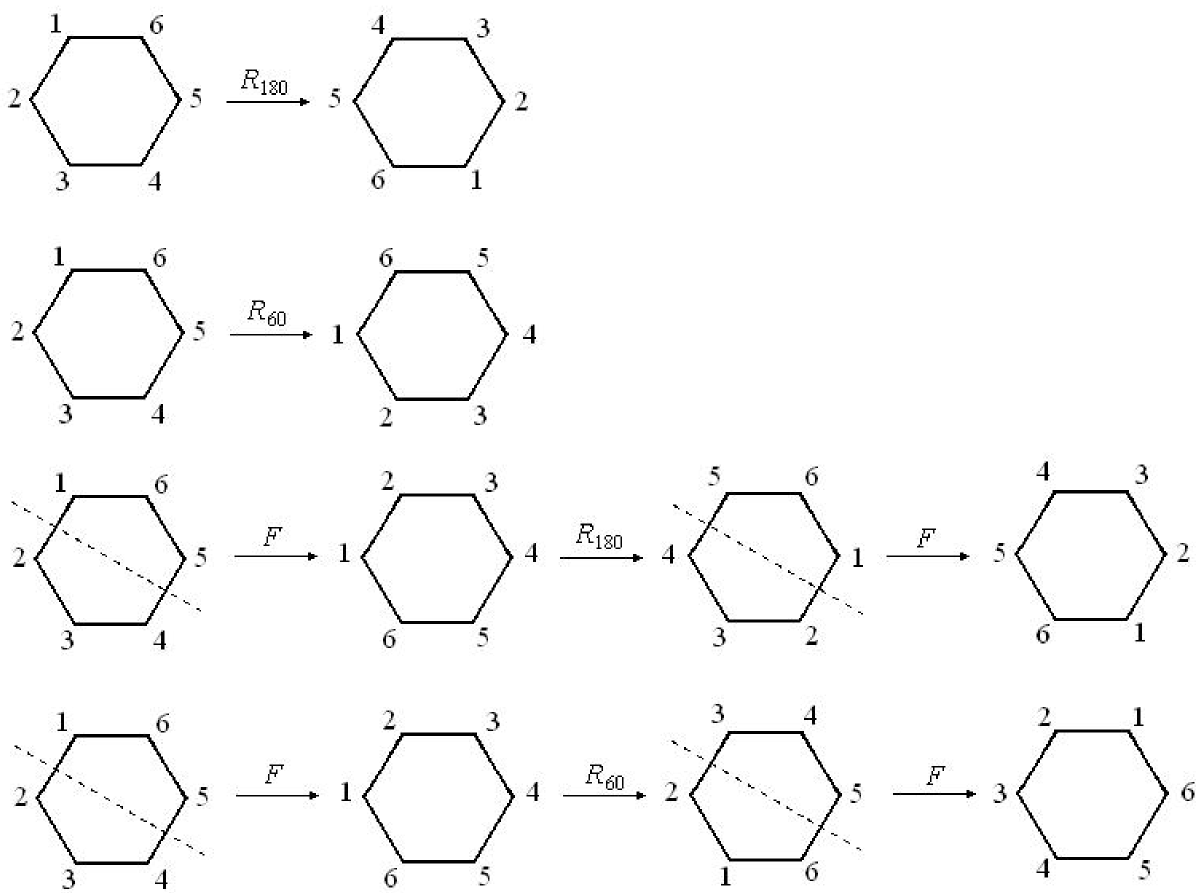
We must establish the reverse inclusion. Since $(k, n) = 1$, we know that there is an $m \in \mathbb{Z}$ so that $mk \bmod n = 1$. Since $|a| = n$, this means that $a^{mk} = a^1 = 1$ (proven in previous homework). The lemma above thus implies

$$C(a^k) \leq C((a^k)^m) = C(a^{mk}) = C(a)$$

which finishes the proof. □

The first part of the problem follows immediately by taking $n = 5$, $k = 3$.

As for the second part, consider the group D_6. The element $R_{60} \in D_6$ (counterclockwise rotation of the hexagon by 60^o) has order 6 and $R_{60}^3 = R_{180}$. If F denotes the flip of the hexagon across the line $y = -x/\sqrt{3}$ then the illustration below shows that $FR_{60}F \neq R_{60}$ but $FR_{180}F = R_{180}$. Hence $F \in C(R_{180})$ but $F \notin C(R_{60})$ and so $C(R_{60}) \neq C(R_{180}) = C(R_{60}^3)$.



p 69, # 34. We simply compute the cyclic subgroups generated by each element in $U(15) =$

$\{1, 2, 4, 7, 8, 11, 13, 14\}$. We find

$$\begin{aligned}
\langle 1\rangle &= \{1\}\\
\langle 2\rangle &= \{1, 2, 4, 8\}\\
\langle 4\rangle &= \{1, 4\}\\
\langle 7\rangle &= \{1, 7, 4, 13\}\\
\langle 8\rangle &= \{1, 8, 4, 2\}\\
\langle 11\rangle &= \{1, 11\}\\
\langle 13\rangle &= \{1, 13, 4, 7\}\\
\langle 14\rangle &= \{1, 14\}
\end{aligned}$$

so that the 6 cyclic subgroups are

$$\begin{aligned}
&\langle 1\rangle\\
&\langle 2\rangle = \langle 8\rangle\\
&\langle 7\rangle = \langle 13\rangle\\
&\langle 4\rangle\\
&\langle 11\rangle\\
&\langle 14\rangle.
\end{aligned}$$

p 70, # 42. It is easy to verify that as elements of $U(40)$ we have $|11| = |29| = 2$ and $11 \cdot 29 \bmod 40 = 39$. Since $U(40)$ is abelian, (the solution to) Exercise # 10 shows that

$$\{1, 11, 29, 39\}$$

is a subgroup of $U(40)$ of order 4. It is noncyclic because none of its elements have order 4.

p 82, # 2. If $|x| = n$ then Corollary 2 of Theorem 4.2 tells us that

$$\langle x\rangle = \langle x^i\rangle$$

if and only if $(i, n) = 1$. Since $\langle x\rangle = \{e, x, x^2, \ldots, x^{n-1}\}$ (Theorem 4.1), we see that the set of generators of $\langle x\rangle$ is

$$\{x^i \mid i \in U(n)\}.$$

Since $U(6) = \{1, 5\}$, the only generators of $\langle a\rangle$ are a and a^5. Since $U(8) = \{1, 3, 5, 7\}$, the generators of $\langle b\rangle$ are b, b^3, b^5 and b^7. Finally, since $U(20) = \{1, 3, 7, 9, 11, 13, 17, 19\}$, the generators of $\langle c\rangle$ are $c, c^3, c^7, c^9, c^{11}, c^{13}, c^{17}$ and c^{19}.

p 82, # 8. We use Theorem 4.2, which states that if $|a| = n$ then

$$|a^k| = \frac{n}{(n, k)}.$$

(a) Since $(3,15) = (6,15) = (9,15) = (12,15) = 3$ we see that

$$|a^3| = |a^6| = |a^9| = |a^{12}| = \frac{15}{3} = 5.$$

(b) Since $(5,15) = (10,15) = 5$ we see that

$$|a^5| = |a^{10}| = \frac{15}{5} = 3.$$

(c) Since $(2,15) = (4,15) = (8,15) = (14,15) = 1$ we see that

$$|a^2| = |a^4| = |a^8| = |a^{14}| = \frac{15}{1} = 15.$$

p 83, # 18. Let $G = \langle a \rangle$ and suppose that G has an element of infinite order. Then G must be infinite and so a must have infinite order as well, by Theorem 4.1. Let $x \in G$ have finite order. Then $x = a^k$ for some $k \in \mathbb{Z}$ and there is some $n \in \mathbb{Z}^+$ so that $a^0 = e = x^n = a^{kn}$. Since a has infinite order, Theorem 4.1 tells us that we must have $kn = 0$. Since $n \neq 0$, it must be the case that $k = 0$. That is, $x = a^0 = e$. So, the identity is the only element of G with finite order.

p 83, # 28. Suppose a has infinite order and that $\langle a^i \rangle = \langle a^j \rangle$. Then $a^i \in \langle a^j \rangle$ so that $a^i = (a^j)^k = a^{jk}$ for some k. Likewise, $a^j \in \langle a^i \rangle$ so that $a^j = (a^i)^l = a^{il}$ for some l. Since a has infinite order, Theorem 4.1 tells us that $i = jk$ and $j = il$. Substituting the second equation into the second yields $i = ikl$ or $i(1 - kl) = 0$. This can only happen if $i = 0$ or $kl = 1$. In the first case we have $i = \pm j = 0$, and in the second we have $k = \pm 1$ so that $i = \pm j$ as well.

p 84, # 46. If $|x| = 40$, then according to Theorem 4.2

$$|x^k| = \frac{40}{(k, 40)}.$$

Thus, x^k has order 10 if and only if $(k, 40) = 4$. Theorem 4.1 implies that we may restrict to $0 \leq k < 40$ and it is easy to check that the values of k in this range that satisfy $(k, 40) = 4$ are 4, 12, 28 and 36. Thus, the elements of $\langle x \rangle$ of order 10 are

$$x^4, x^{12}, x^{28}, x^{36}.$$

p 85, # 54. Let $H = \langle a \rangle \cap \langle b \rangle$. Since $H \leq \langle a \rangle$ the Fundamental Theorem of Cyclic Groups implies $|H|$ divides $|a|$. The same reasoning shows that $|H|$ divides $|b|$ as well. Therefore $|H|$ divides $(|a|, |b|) = 1$, i.e. $|H| = 1$. Since the identity is a member of any group, it must be the case that it is the only member of H. That is, $\langle a \rangle \cap \langle b \rangle = H = \{e\}$