Homework 4

Walker Bagley and Hayden Gilkinson

February 17, 2023

Section 6

1. $42 = q * 9 + r \Rightarrow q = 4, r = 6$

5. $32 : 32, 16, 8, 4, 2, 1$
   $24 : 24, 12, 8, 6, 4, 3, 2, 1$
   $gcd(32, 24) = 8$

11. Generators of $|G| = 60$: a^n where $n = 1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59$
    There are 16 generators

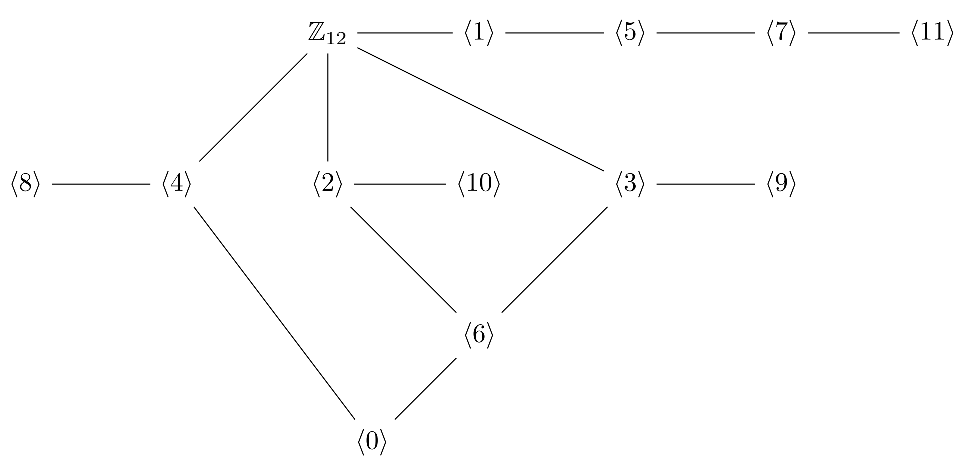
14. There are 4 automorphisms since there are 4 generators: $\langle 1\rangle, \langle 3\rangle, \langle 5\rangle, \langle 7\rangle$

15. There are 2 automorphisms since $\phi(n) = n$ or $\phi(n) = -n$

17. $\langle 25\rangle = \{25, 20, 15, 10, 5, 0\}$ so $|\langle 25\rangle| = 6$

20. $\left\langle \frac{(1+i)}{\sqrt{2}} \right\rangle = \left\{ \frac{(1+i)}{\sqrt{2}}, i, \frac{(i-1)}{\sqrt{2}}, -1, -\frac{(1+i)}{\sqrt{2}}, -i, -\frac{(i-1)}{\sqrt{2}}, 1 \right\}$ so $\left| \left\langle \frac{(1+i)}{\sqrt{2}} \right\rangle \right| = 8$

21. $\langle 1+i\rangle = \{1+i, 2i, 2i-2, -4, -4-4i, -8i...\}$ so $|\langle 1+i\rangle| = \infty$

22. 

25. Subgroups of $\mathbb{Z}_6$: $\langle 1\rangle, \langle 2\rangle, \langle 3\rangle, \langle 0\rangle$ which have orders of $6, 3, 2, 1$ respectively

30. An element $a \in G$ has order $n \in \mathbb{Z}^+$ if and only if n is the smallest n satisfying $a^n = e$

31. The greatest common divisor of two positive integers is the largest positive integer that divides both of them without remainder.

32. (a) True
    (b) False
    (c) False
    (d) False
    (e) True

(f) True

(g) False

(h) False

(i) True

(j) True

36. No examples because if a is a generator, then $x \in G$ can be defined as a^n for some $n \in \mathbb{Z}$. $a^n = (a^{-1})^{-n}$ so a^{-1} is also a generator. But these are the only two possible generators since all other elements can be expressed as a^n for some $n \in \mathbb{Z}$.

37. $G = \mathbb{Z}_{10} = \langle 1 \rangle = \langle 3 \rangle = \langle 7 \rangle = \langle 9 \rangle$

38. i and $-i$ both generate the group $U_4 = \{1, i, -1, -i\}$

42. For some cyclic group $G = \langle a \rangle$ with elements $g_1 = a^r$ and $g_2 = a^s$, then $g_1 g_2 = a^r a^s = a^{r+s} = a^{s+r} = a^s a^r = g_2 g_1$, so G is abelian.

44. *Proof.*

$$\begin{aligned}
&\text{Let } \phi : G \to G' \text{ be an isomorphism and } a \in G \text{ be a generator of } G \\
&\text{By the homomorphism property, we have } \phi(a^n) = (\phi(a))^n \\
&\text{Similarly, if } \psi : G \to G' \text{ is an isomorphism, } \psi(a^n) = (\psi(a))^n \\
&\text{Since } G \text{ is generated by } a\text{, then with the isomorphism, } G' \text{ is generated by } \phi(a) \\
&\text{So for any } x \in G,\ \phi(x) = (\phi(a))^n \text{ for some } n \in \mathbb{Z} \\
&\text{If } \phi(a) = \psi(a) \text{ then } (\phi(a))^n = (\psi(a))^n \text{ for all } n \in \mathbb{Z} \\
&\text{Thus, } \phi(x) = \psi(x) \text{ for all } x \in G
\end{aligned}$$

□

49. *Proof.*

$$\begin{aligned}
&\text{Consider } G = V \\
&\text{The only proper subgroups of } G \text{ are } \{e\}, \{e, a\}, \{e, b\}, \{e, c\} \\
&\text{It is easy to see that each subgroup has a generator, } e, a, b, c \text{ respectively} \\
&\text{However, we know that } G \text{ is not cyclic and therefore have a counterexample}
\end{aligned}$$

□