HW 1

HW 1

5.

Suppose otherwise. Let $e = [1]$; then e is the identity element because for all $k \in \mathbb{Z}$ we have $e * [k] = [1] * [k] = [1 * k] = [k]$. Let $x = [0]$ and $x^{-1} = [k]$ for some $k \in \mathbb{Z}$, which exists because of the existence of inverses in a group. By the uniqueness of identities in groups we have $[1] = e = x * x^{-1} = [0] * [k] = [0 * k] = [0]$, which means $0 \sim 1$, which means n divides 1, which is not true for $n > 1$.

7.

Let $f(l)$ be the fractional part of l. We have $f(l) = l - [l] \geq 0$ because $[l] \leq l$ by definition. We have $f(l) = l - [l] < 1$ because otherwise, $[l] + 1$ would be an integer less than l. Hence $x * y \in G$.

Commutativity: for all $x, y \in G$ we have $x * y = x + y - [x + y] = y + x - [y + x] = y * x$.

Lemma: $f(l) = r \iff r \in R$ and there exists an integer t such that $r + t = l$. $\implies$ follows because we can take $t = [l]$. $\impliedby$ follows because $f(l) = l - t = r$ where the first equality holds because t cannot be increased (since we have $l - (t + 1) = r - 1 < 0$).

For associativity we will show that for $a, b, c \in G$ we have $a * (b * c) = f(a + b + c)$; the proof that $(a * b) * c = a + b + c - [a + b + c]$ is similar, and then we have $a * (b * c) = (a * b) * c$.

By our lemma, $a * (b * c) = f(a + b + c) \iff$ there exists an integer t such that $a + b + c = t + a * (b * c)$.

14.

I'll write the powers of the elements, represented as integers modulo 36.

$1; o(1) = 1$

$-1, 1; o(-1) = 2$

$5, 25, 17, 13, 29, 1; o(5) = 6$

$13, 25, 1; o(13) = 3$

$-13, 25, -1, 13, -25, 1; o(-13) = 6$

$17, 1; o(17) = 1$

22.

For all positive integers k we have $(g^{-1}xg)^k = g^{-1}xgg^{-1}xg \dots g^{-1}xg = g^{-1}x^k g$. In particular for $k = n$ we have $(g^{-1}xg)^k = g^{-1}x^k g = g^{-1}g = 1$, hence $o(g^{-1}xg) \leq 1$. Suppose $o(g^{-1}xg) = k$ with $k < n$; then we have $g^{-1}x^k g = 1 \implies x^k g = g \implies x^k = gg^{-1} = 1$, contradicting that n is the least positive integer such that $x^n = 1$.

31.

For every $g \in t(G)$ create an edge from g to g^{-1}; since G does not contain elements which are their own inverses, each edge points to a different element. Since we have $(g^{-1})^{-1} = g$ this forms a set of bidirectional edges, meaning that $|t(G)|$ is even. Hence $|G - t(G)|$ is even, and since $e \notin t(G)$ it has at least two elements. Let x be such an element with $x \neq e$. We have $x = x^{-1} \implies x^2 = 1$. Since $x \neq e, o(x) = 2$.

32.

Suppose otherwise, and let $x^a = x^b$ with $a < b$ be two equal elements from the list, and let $t = b - a$. We have $t \leq n - 1$ since $b \leq n, 0 \leq a$. Then $x^t = x^{b-a} = x^b(x^a)^{-1} = x^b(x^b)^{-1} = 1$, contradicting the fact that n is the least positive integer such that $x^n = 1$.

Suppose $t = |x| > |G|$; then $x^0, x^1, \dots x^{t-1}$ are all distinct elements of G, hence $|G| \geq |\{x^0, x^1, \dots x^{t-1}\}| = t > |G|$, a contradiction.

35.

Let x^k be such an integer power, and let $k = qn+r$ where $0 \leq r < n$. We have $x^k = x^{qn+r} = (x^n)^q + x^r = 1^q x^r = x^r$ as required.