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 $\sim$ be a equivalence relation on real numbers: for real numbers a, b let $a \sim b$ if $b - a$ is an integer. This is reflexive as 0 is an integer, and transitive as the sum of two integers is an integer.

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 $x * y \in R$.

Lemma 1: for a positive real number a we have $[a] + 1 = [a + 1]$. Proof: $[a] + 1 \leq a + 1$ by adding 1 to both sides of the inequality $[a] \leq a$. Suppose there is an integer $t > [a] + 1$ which satisfies $t \leq a + 1$; then because the difference of two distinct integers is at least 1, $[a] + 2 \leq t \leq a + 1$ which means $[a] + 1 \leq a$, contradicting the definition of $[a]$.

Lemma 2: for a positive real number a and a positive integer k we have $[a] + k = [a + k]$ by induction on k.

Lemma 3: for two positive reals a, b we have $a \sim b \implies f(a) = f(b)$. Proof: WLOG $b = a + k$ for a positive integer k, then $f(b) = f(a + k) = a + k - [a + k] = a + k - ([a] + k) = a - [a] = f(a)$.

Lemma 4: for a positive real $a, f(a) \sim a$. Proof: their difference is an integer by the defition of f.

Identity: 0 is the identity since for all $x \in G, 0 * x = f(x + 0) = f(x) = x$.

Inverse: let $x \in G$; then $1 - x \in G$ and their group product is $f(1 - x + x) = f(1) = 0$.

Commutativity: for $x, y \in G$ we have $x + y = y + x$ hence $f(x + y) = f(y + x)$.

Associativity: for $x, y, z \in G$ we have $x*(y*z) \sim x*(y+z) \sim x+(y+z) = (x+y)+z \sim (x*y)+z \sim (x*y)*z$.

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 $(g^{-1}xg)^k = g^{-1}x^kg$ by induction on k, with inductive step $(g^{-1}xg)^{k+1} = (g^{-1}xg)^k(g^{-1}xg) = g^{-1}x^kgg^{-1}xg = g^{-1}x^kxg = g^{-1}x^{k+1}g$ and base case $k = 1$.

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

We have $o(ab) = o(a^{-1}aba) = o(ba)$.

31.

For every $g \in t(G)$ create an edge from g to g^{-1}; since $t(G)$ 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 $x^0, x^1, \ldots x^{t-1}$ are all distinct elements of G, hence $|G| \geq |\{x^0, x^1, \ldots x^{t-1}\}| = t > |G|$, a contradiction.

35.

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