Homework on Section 6

Due Monday, Sep 23

This homework must be done individually. Remember to follow Math department's guidelines for homework. Please write your solutions neatly. Typesetting in LaTeX is appreciated and encouraged.

1. Let G be a group and let $g \in G$ be such that $|g^5| = 12$. What are the possibilities for $|g|$? If $|a^4| = 12$, then what are the possibilities for $|a|$?
2. Let G be a group and let $x, y \in G$ be such that $|xy|$ is finite. Show that $|xy| = |yx|$.
3. Let G be a group and let $x, y \in G$ be such that $|x| = m$ and $|y| = n$. Assume that x and y commute, i.e. $xy = yx$. Prove that $|xy|$ divides the least common multiple of m and n.
4. Let p be a prime and let n be a positive integer. Show that if x is an element of the group G such that $x^{p^n} = 1$ then $|x| = p^m$ for some $m \leq n$.
5. Let p be a prime number. Determine all subgroups of $\mathbb{Z}_p$. Justify your answer.
6. Recall the definition of the discrete logarithm $L_\alpha(\beta)$ from the handout. Show that the discrete logarithm satisfies the familiar property of the logarithmic function: $L_\alpha(\beta_1\beta_2) = L_\alpha(\beta_1) + L_\alpha(\beta_2)$