CSU Math 366

Homework 3

Due Friday, February 14 at the beginning of class

Reading. Chapter 4

Remark. Make grammatically correct sentences by adding in just a few English words.

Problems.

1. (a) Watch the YouTube video https://www.youtube.com/watch?v=JUzYl1TYMcU, and then use the Euclidean Algorithm (described within) to compute $\gcd(63, 141)$, the *greatest common divisor* of 63 and 141.

   Spoiler alert: You should get $\gcd(63, 141) = 3$.

   (b) Watch the YouTube video https://www.youtube.com/watch?v=6KmhCKxFWOs, and then use the extended Euclidean Algorithm (described within) to find integers $s, t \in \mathbb{Z}$ such that $63s + 141t = \gcd(63, 141) = 3$.

   Remark: I understand the Euclidean takes some getting-used-to, so if you come to office hours or ask me after class then I will show you how to do this problem! (In fact, this is the case for all problems.) Don't think of this as a random homework problem that you can safely skip — the Euclidean algorithm is fundamental for abstract algebra.

2. Recall that $\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z} \text{ with } b \neq 0\}$ is the set of all *rational numbers*, and that $\mathbb{Q}^*$ is the set of all rational numbers excluding 0. That is, $\mathbb{Q}^*$ is the set of all fractions of the form $\frac{a}{b}$ with $b \neq 0$ and with $a \neq 0$. Show that $(\mathbb{Q}^*, \cdot)$ is a group (under multiplication) by verifying the definition on page 13 of our class notes.

   Hint: Do this as follows.

   - *First, to show that multiplication is a binary operation on $\mathbb{Q}^*$, you will show that given $\frac{a}{b}, \frac{a'}{b'} \in \mathbb{Q}^*$, their product $\frac{a}{b} \cdot \frac{a'}{b'}$ is also in $\mathbb{Q}^*$. Is this product necessarily nonzero?*
   - *Then, to show there is an identity, you will identify which element is the identity, and then show that this element satisfies the defining property of an identity.*
   - *Then, to show there are inverses, you will take an arbitrary element $\frac{a}{b} \in \mathbb{Q}^*$, identify its inverse, and then show that this element satisfies the defining property of an inverse.*
   - *Then, to show associativity, you can simply write "Finally, note that multiplication is associative on $\mathbb{Q}^*$" — no need to write anything more!*

   Conclude by saying "Hence $(\mathbb{Q}^*, \cdot)$ is a group." Remember to use grammatically correct sentences at each step!

3. Let G be a group, let $g \in G$, and let $n \geq 1$ be a positive integer. Show that $(g^{-1})^n$ is the inverse of g^n. In other words, show that $(g^n)^{-1} = (g^{-1})^n$.

   Hint: Your proof could look like the following.
   "Note that

   $$g^n(g^{-1})^n = \underbrace{gg\cdots g}_{n\ times}\underbrace{g^{-1}g^{-1}\cdots g^{-1}}_{n\ times} = \ldots$$

   and

   $$(g^{-1})^n g^n = \underbrace{g^{-1}g^{-1}\cdots g^{-1}}_{n\ times}\underbrace{gg\cdots g}_{n\ times} = \ldots.$$

   Hence by the definition of an inverse, we have shown that ...."
   Your task is to show all the work and to complete all the steps in the missing blanks!

   Remark: Since the above homework problem shows that $(g^n)^{-1} = (g^{-1})^n$, we may safely denote both elements by the common symbol g^{-n}.

4. Let G be a group, and let $a \in G$. Show that $\langle a \rangle$ is a subgroup of G by using the One-Step Subgroup Test.

   Hint: On Wednesday, Feb 5, we showed that $\langle a \rangle$ is a subgroup of G using the Two-Step Subgroup test. On Friday, Feb 7, we showed that $\langle a \rangle$ is a subgroup of G using the One-Step Subgroup test, even though this isn't written up in our class notes. I am asking you to re-do this proof from Friday in class. Neither proof is "better" than the other — you can often prove something in multiple ways!