Homework # 2 Math 3340 Spring 2021

Due at the end of the day 25 Feb 2021, at midnight.

Please submit your completed homework via gradescope on canvas. I encourage you to work with your classmates on this homework (except for the journal entries!) When you submit your work, please **list your collaborators**. (Your grade will not be affected.) Even if you work in a group, you should write up your solutions **yourself**! You should include all computational details, and proofs should be carefully written with full details. As always, please write **neatly and legibly** (feel free to use LaTeX to write up your solutions, if you wish!).

Journal entry. There is no journal entry this week.

Exercises.

1. Let G be a group. Prove that if $x^2 = e$ for all $x \in G$, then G is Abelian.
2. Let G be a group. Recall that if $g \in G$, then $o(g)$ denotes the order of g. Show that, for all $a, b, g \in G$,
   (a) $o(e) = 1$,
   (b) $o(ab) = o(ba)$,
   (c) $o(a^{-1}) = o(a)$, and
   (d) $o(gag^{-1}) = o(a)$.
3. Let $G = GL(2, \mathbb{Q})$, and let $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, and $B = \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix}$. Show that A and B have finite order, and find their orders. Then show that AB does not have finite order. This shows that AB can have infinite order even if A and B have finite order.
4. For each group S_n, where $1 \leq n \leq 10$, what is the largest order of an element of S_n?
5. Let G be a group.
   (a) If $|G| = 3$, show that G is Abelian.
   (b) If $|G| = 4$, show that G is Abelian.
   (c) If $|G| = 5$, show that G is Abelian.
   (d) Find a group of order 6 which is not Abelian.
6. Let G be a finite group with an even number of elements. Show that the number of elements of order 2 is odd (and so, at least one exists).

7. In this problem, we find the elements of $\mathbb{Z}_n$ which have a multiplicative inverse, that is for which $[a]_n$ can we solve $[a]_n[x]_n = [1]_n$. Let's define

$$\mathbb{Z}_n^\times := \{[a]_n \in \mathbb{Z}_n \mid \text{there exists an integer } x \text{ with } [a]_n[x]_n = [1]_n\}$$

   (a) Let $a \in Z$. Show that $\langle a \rangle := \{ka \mid k \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$. If $a, b \in \mathbb{Z}$, show that $\langle a, b \rangle := \{ma + nb \mid m, n \in \mathbb{Z}\}$ is also a subgroup of $\mathbb{Z}$.

   (b) Let $I \subset \mathbb{Z}$ be a non-zero subgroup (that is, there exists at least one non-zero element in I). Prove that there exists a positive integer g such that $a \in I$ if and only if $g|a$.

   (c) If $a, b \in \mathbb{Z}$ are two integers, let g be their greatest common divisor (gcd, often written $\mathrm{gcd}(a, b)$, or even (a, b)). Show that $\langle a, b \rangle = \langle g \rangle$.

   (d) If $a, b \in \mathbb{Z}$ are two nonnegative integers, and $g = \mathrm{gcd}(a, b)$, then show that there exists $x, y \in \mathbb{Z}$ such that $g = xa + yb$.

   (e) Suppose that $a = 8, b = 3$, therefore $g = \mathrm{gcd}(a, b) = 1$. Find $x, y \in \mathbb{Z}$ such that $8x+3y = 1$. Recall that nonzero integers a and b and called relatively prime if $\mathrm{gcd}(a, b) = 1$.

   (f) Fix a positive integer n. Prove that

$$\mathbb{Z}_n^\times = \{[a]_n \in \mathbb{Z}_n \mid \; a \text{ and } n \text{ are relatively prime}\}.$$