Math 4720 & 5210 # Homework #1 **Due: Fri., Aug. 27^{th}, 2021**

#1 Establishing Order Find the order and inverse of each of the following elements:

(a) Find the order and inverse of $(4,7)$ in $\mathbb{Z}_5 \times \mathbb{Z}_{12}$. Also, what is the order of the group $\mathbb{Z}_5 \times \mathbb{Z}_{12}$?

Note: $\mathbb{Z}_n$ is a group under addition modulo n. You should be adding.

(b) Find the order and inverse of $(4,7)$ in $(\mathbb{Z}_5)^\times \times (\mathbb{Z}_{12})^\times$. Also, what is the order of the group $(\mathbb{Z}_5)^\times \times (\mathbb{Z}_{12})^\times$?

Note: $(\mathbb{Z}_n)^\times = U(\mathbb{Z}_n) = \{x \in \mathbb{Z}_n \mid \gcd(x,n) = 1\}$ (Gallian calls this $U(n)$) is the group of units of $\mathbb{Z}_n$. This is a group under multiplication modulo n. For example: $(\mathbb{Z}_{12})^\times = \{1,5,7,11\}$. You should be multiplying.

(c) Find the order and inverse of $\begin{bmatrix}1 & 2\\ 3 & 9\end{bmatrix}$ in $(\mathbb{Z}_{10})^{2\times 2}$. Also, what is the order of the group $(\mathbb{Z}_{10})^{2\times 2}$?

Note: $(\mathbb{Z}_m)^{n\times n}$ is a group under (matrix) addition with entries added modulo m. You should be adding.

(d) Find the order and inverse of $\begin{bmatrix}1 & 2\\ 3 & 9\end{bmatrix}$ in $\mathrm{GL}_2(\mathbb{Z}_{10})$.

Note: $\mathrm{GL}_2(\mathbb{Z}_{10}) = ((\mathbb{Z}_m)^{n\times n})^\times = \{A \in (\mathbb{Z}_m)^{n\times n} \mid \det(A) \in (\mathbb{Z}_m)^\times\}$ is a group under (matrix) multiplication with entries computed modulo m. You should be multiplying.

Suggestion: Even working mod 10, computing the order of this matrix can be tedious (doable but tedious). You might want to use some technology. For example, you could go to my SAGE sandbox[1] and make SAGE do the heavy lifting. The following code creates a matrix A in $(\mathbb{Z}_{10})^{2\times 2}$. Then it prints both A and A^2:

```
A = matrix(IntegerModRing(10),[[1,2],[3,4]])
pretty_print("A = ", A)
pretty_print("A^2 = ", A^2)
```

(e) **[Grad Problem:]** What is the order of the group $\mathrm{GL}_2(\mathbb{Z}_2)$? How about $\mathrm{GL}_2(\mathbb{Z}_{10})$? Then use the following boxed fact and these answers to find the order of $\mathrm{GL}_2(\mathbb{Z}_{10})$.

> When $\mathbb{Z}_n$ is a field (i.e., when n is prime), finding the order of $\mathrm{GL}_2(\mathbb{Z}_n)$ is relatively easy using some linear algebra. When n is the product of distinct primes, we can then use the following:[n]
> Suppose k and ℓ are relatively prime. Then $\mathbb{Z}_{k\ell} \cong \mathbb{Z}_k \times \mathbb{Z}_\ell$ (as rings). Next, as rings we get $(\mathbb{Z}_{k\ell})^{2\times 2} \cong (\mathbb{Z}_k)^{2\times 2} \times (\mathbb{Z}_\ell)^{2\times 2}$. It then follows, for their group of units, $\mathrm{GL}_2(\mathbb{Z}_{k\ell}) \cong \mathrm{GL}_2(\mathbb{Z}_k) \times \mathrm{GL}_2(\mathbb{Z}_\ell)$.
>
> [n]Juncheol Han's paper "The general linear group over a ring", Bulletin of the Korean Mathematical Society, Vol. 43, No. 3 (2006).

#2 Cyclical Issues Draw a subgroup lattice for $\mathbb{Z}_{99}$. Then make a table listing possible element orders and how many elements there are of each of those orders. Finally, list all elements of order 9 in $\mathbb{Z}_{99}$.

#3 Progressive Abstract Algebra – Intersectionality For each i in some index set I, let H_i be a subgroup of G. Prove that $\displaystyle\bigcap_{i\in I} H_i$ is a subgroup of G.

Note: Recall that $x \in \displaystyle\bigcap_{i\in I} H_i$ if and only if for every $i \in I$, we have $x \in H_i$.

#4 Lemprob Wardsback Let $\varphi : G_1 \to G_2$ be a homomorphism between two groups. Let K be a subgroup of G_2. Prove that $\varphi^{-1}(K)$ is a subgroup of G_1.

Note: $\varphi^{-1}(K) = \{x \in G_1 \mid \varphi(x) \in K\}$ is the *inverse image* (or *preimage*) of K. $\quad x \in \varphi^{-1}(K)$ iff $\varphi(x) \in K$

Warning: Given some $x \in G_2$, "$\varphi^{-1}(x)$" is nonsense. The mapping φ may not be invertible, so φ^{-1} may not be defined *on elements*. On the other hand, $\varphi^{-1}(S)$ *always* makes sense for any subset, S, of the codomain.

#5 You're free cheesybread! You're free! Use the universal property to show that each $x \in X$ is an element of infinite order in the free group $F(X)$. In particular, if X is a non-empty set of generators, we have that $F(X)$ is an infinite group.

[Grad Problem:] Next, suppose $X = \{a,b,c\}$. Show that $ab^{-3}a^2c$ has infinite order in $F(X)$.

Note: Actually, *all* non-identity elements are of infinite order in $F(X)$.

[1]https://billcookmath.com/sage/linear_algebra/