Homework 7

Submission Instructions: You are responsible to read these instructions. Failure to submit correctly as described below will result in point deductions or loss of credit for entire problems. Submit these problems on Gradescope by Sunday, Mar. 17th, at 11:59pm. Each problem should be on a separate page (or pages). **You will need to scan a PDF of the assignment AND select the pages belonging to each problem when you submit on gradescope.**

1. Let G and H be groups.
   (a) Give an example where G and H are both cyclic, but $G \times H$ is not.
   (b) If $G \times H$ is a cyclic group, prove that G and H are both cyclic.
   (c) Recall that $\mathbb{R}^\times$ is the multiplicative group of units of $\mathbb{R}$. Define an explicit isomorphism $f : \mathbb{R}^\times \to \mathbb{R} \times \mathbb{Z}_2$.

   (a) Let $G = \mathbb{Z}_2 = H$. Then $G \times H$ is not cyclic.
   (b) Suppose $G \times H$ is cyclic, then there is some generator $(g, h) \in G \times H$. Then pick any $g' \in G$ and $h' \in H$. Then $(g', h') \in G \times H$ so there is some n such that $(g, h)^n = (g', h')$. But then, by definition $g^n = g'$ and $h^n = h'$, so G and H are both cyclic with generators g and h.
   Alternatively, one might argue that given any $g' \in G$, we can consider $(g', e_H) \in G \times H$. Then $(g^n, h^n) = (g', e_H)$ for some $n \in \mathbb{Z}$, so $g^n = g'$. Therefore, G is cyclic. A symmetric argument with $h' \in H$, considering (e_G, h'), proves H is cyclic.
   (c) Since $\mathbb{Z}_2 \cong \{\pm 1\}$, we can instead give an isomorphism $f : \mathbb{R}^\times \to \mathbb{R} \times \{\pm 1\}$. Define first $g : \mathbb{R}^\times \to (0, \infty) \times \{\pm 1\}$ by $g(x) = (|x|, x/|x|)$. Here, the operation on $(0, \infty) \times \{\pm 1\}$ is multiplication on both groups. Now we can use function $\log : ((0, \infty), \cdot) \to (\mathbb{R}, +)$. We know $\log(AB) = \log(A) + \log(B)$, so this is a group homomorphism. We can prove that $\log : (0, \infty) \to \mathbb{R}$ is an isomorphism using calculus: log is increasing, so it is injective, and is easily shown to be surjective.

2. Let $S^1 \subset \mathbb{C}$ be the unit circle; that is
$$S^1 = \{z \in \mathbb{C} \ : \ |z| = 1\}.$$
   (a) Prove that S^1 is a subgroup of $\mathbb{C}^\times$.
   (b) For every positive integer n, find an element of order n in S^1.
   (c) Find an element of infinite order in S^1.

   (a) Obviously $S^1 \subset \mathbb{C}^\times$, since $0 \notin S^1$. Given $x, y \in S^1$, $|xy| = |x||y| = 1$, so S^1 is closed for the product. Moreover, $1 \in S^1$, and $|x^{-1}| = |x|^{-1} = 1$, so S^1 is also closed for inverses. We conclude that S^1 is a subgroup of $\mathbb{C}^\times$.

(b) We will use Euler's formula for the next two parts, which says that for any $\theta \in \mathbb{R}$ we have

$$e^{\theta i} = \cos(\theta) + i\sin(\theta).$$

(This can be proved by plugging $x = \theta i$ into the Maclaurin series for e^x and expanding, noticing that the terms without an i give the Maclaurin series for $\cos(\theta)$ and the terms with an i give $i\sin(\theta)$.)

We know from trigonometry that any $x+iy \in S^1$ can be written as $\cos(\theta)+i\sin(\theta)$, so we can alternatively represent any point of S^1 by $e^{\theta i}$ for some θ. Now letting $\theta = \frac{2\pi}{n}$ gives an element of S^1 of order n for any $n > 0$.

(c) Choosing $\theta > 0$ so that $n\theta \neq 2\pi$ for any $n \in \mathbb{Z}$ will give an element of infinite order. For example, $\theta = 1$ works, since π is irrational.

3. Let R be a commutative ring, and consider the group $\mathrm{GL}_2(R)$ of units in the ring of 2×2 matrices $\mathrm{M}_2(R)$ with coefficients in R.

(a) Suppose that

$$A = \begin{bmatrix} a & c \\ b & d \end{bmatrix} \in \mathrm{M}_2(R)$$

and all the entries are in an ideal $I \subsetneq R$. Prove that A is not a unit.

(b) Prove that for any matrix

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{M}_2(R)$$

there is a matrix B such that

$$AB = BA = \det(A)I_2.$$

(c) (This is the hard problem) Prove that a matrix

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{M}_2(R)$$

is a unit in $\mathrm{M}_2(R)$ if and only if $\det(A)$ is a unit.

(a) Suppose that $a, b, c, d \in I$ and let

$$B = \begin{bmatrix} e & f \\ g & h \end{bmatrix} \in \mathrm{M}_2(R)$$

be an arbitrary matrix. Then:

$$AB = \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix}$$

Thus $ae+bg, cf+dh \in I$. As we assumed $I \subsetneq R$, these can never equal 1. Thus there does not exist an inverse matrix in $M_2(R)$.

(b) Consider the *adjugate matrix*:

$$B = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

A straightforward calculation shows this has the desired properties.

(c) If $u = \det(A)$ is a unit with inverse w and B is the adjugate matrix from the previous part then we have

$$\begin{bmatrix} w & 0 \\ 0 & w \end{bmatrix} \cdot B = A^{-1}.$$

If $\det(A)$ is not a unit, then $(\det(A)) \subsetneq R$ is a proper ideal. Suppose for contradiction that A is also invertible. Then by part (b) we have:

$$BAA^{-1} = \det(A)A^{-1}.$$

Every entry in A is $\pm$ an entry in B. Every entry in $B = \det(A)A^{-1}$ is contained in the proper ideal $(\det(A))$. Therefore, every entry in A is contained in $(\det(A))$ and so by part (a), the matrix A is not invertible.

4. Let p be a prime number and consider the field $\mathbb{Z}_p$.

(a) Show that a 2×2 matrix $A \in \mathrm{M}_2(\mathbb{Z}_p)$ is not a unit if and only if "the columns are linearly dependent."

(b) Show that the set of upper triangular invertible matrices in $\mathrm{GL}_2(\mathbb{Z}_p)$ forms a subgroup of order $p(p-1)^2$, which is non-abelian when $p \neq 2$.

(c) Compute the order of $\mathrm{GL}_2(\mathbb{Z}_p)$.

(d) Show that the diagonal invertible matrices form an abelian subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$ of order $(p-1)^2$.

(e) Find an abelian subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$ of order p. Make sure to show this is a subgroup.

(a) We use the previous problem. A matrix is invertible $\iff$ $\det(A) \neq 0 \in \mathbb{Z}_p$.
If $\det(A) = 0$ then

$$d\begin{bmatrix} a \\ c \end{bmatrix} - c\begin{bmatrix} b \\ d \end{bmatrix} = c\begin{bmatrix} a \\ b \end{bmatrix} - a\begin{bmatrix} b \\ d \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}.$$

If $A \neq 0_2$ then one of these is a non-trivial relation. If $A = 0_2$ then there are many non-trivial relations.

If there is a non-trivial relation on the columns of A, then we can write one column as a constant multiple of the other. So either:

$$A = \begin{bmatrix} a & \lambda a \\ c & \lambda c \end{bmatrix} \quad \text{or} \quad A = \begin{bmatrix} \lambda b & b \\ \lambda d & d \end{bmatrix}.$$

Both of these satisfy $\det(A) = 0$.

(b) The upper triangular matrices again must have nonzero entries on the diagonal (since the determinant is nonzero) but the upper right entry can be arbitrary. There are $(p-1)^2 p$ such matrices. The product of upper triangular matrices is upper triangular, the inverse of an upper triangular matrix is upper triangular, and the identity is upper triangular. For example,

$$\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}^{-1} = (ac)^{-1} \begin{bmatrix} c & -b \\ 0 & a \end{bmatrix}.$$

To see this is not abelian, just note that

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix} \neq \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

(c) For each nonzero first column, there are choices of a second column that make an invertible matrix – all columns except the p multiples of the first column. There are $p(p-1) = p^2 - 1$ choices for the first column, and $p(p-1) - (p-1) = p^2 - p$ for the second. There are $p^2(p-1)^2$ elements in $\mathrm{GL}_2(\mathbb{Z}_p)$.

(d) We need to have nonzero elements on the diagonal (or the determinant would be zero). There are $(p-1)^2$ of these. It's easy to check by direct computation that diagonal matrices commute with each other, the product of diagonal matrices is a diagonal matrix, and that the inverse of a diagonal matrix is diagonal. The identity matrix is a diagonal matrix.

(e) The upper triangular invertible matrices of the form

$$\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix},$$

where $a \in \mathbb{Z}_p$ can be any element, form an abelian subgroup with p elements, since

$$\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & ab \\ 0 & 1 \end{bmatrix}.$$

Note that this subgroup is then isomorphic to $\mathbb{Z}_p$.