MATH 436: Homework I.
Due in class on Friday, Sep 19

1. Fix a set S. Let $P(S)$ denote the power set of S, i.e., $P(S) = \{A | A \subseteq S\}$.
(a) Check that $P(S)$ is an Abelian monoid under the operation $\cap$, where $A_1 \cap A_2$ is the intersection of the subsets A_1 and A_2. What is the identity element for the monoid $(P(S), \cap)$? Does this monoid have the cancellation property?
(b) Check that $P(S)$ is an Abelian monoid under the operation $\cup$, where $A_1 \cup A_2$ is the union of the subsets A_1 and A_2. What is the identity element for the monoid $(P(S), \cap)$? Does this monoid have the cancellation property?
(c) Show that the monoids $(P(S), \cap)$ and $(P(S), \cup)$ are isomorphic, i.e., that there is a bijection f between them such that $f(A \cap B) = f(A) \cup f(B)$ and such that f matches the two identity elements.

2. Let $M(\mathbb{N}) = \{f : \mathbb{N} \to \mathbb{N}\}$ be the monoid of all functions with domain and codomain equal to the natural numbers $\mathbb{N} = \{0, 1, 2, \dots\}$. Recall the monoid operation is that of composition of functions. Consider $\Theta \in M(\mathbb{N})$ defined by $\Theta(n) = 2n$ for all $n \in \mathbb{N}$. Explain why Θ has infinitely many left inverses but no right inverse in $M(\mathbb{N})$. Furthermore find an element $\Psi \in M(\mathbb{N})$ which has neither a left inverse nor a right inverse.

3. Let * be a binary product on a set S which is not necessarily associative. Given elements $a_1, a_2, \dots, a_n$, a meaningful product is an interpretation of $a_1 * a_2 * \cdots * a_n$ as a sequence of binary (pairwise) multiplications. Thus for example among the meaningful products of a sequence of 4 elements are: $(a_1 * a_2) * (a_3 * a_4)$ and $a_1 * ((a_2 * a_3) * a_4)$ among others.
(a) Make a list of all the possible meaningful products for $a_1 * a_2 * a_3 * a_4$.
(b) If we let C_n be the number of meaningful products for a string of length n, then show that $C_1 = C_2 = 1, C_3 = 2$ and that generally $C_n = \sum_{j=1}^{n-1} C_j C_{n-j}$ for $n \geq 2$. Does this formula give a value of C_4 which agrees with your answer in (a)? The numbers C_n are called **Catalan numbers**. (There is a closed form expression for them in terms of binomial coefficients.)

4. Let $\mathbb{Z}$ be the group of integers under addition. It was shown in class that all subgroups of $\mathbb{Z}$ are of the form $(d) = \{\dots, -3d, -2d, -d, 0, d, 2d, 3d, \dots\}$ for some integer $d \geq 0$. Recall for integers s, t we say s divides t if $\frac{t}{s}$ is an integer.
(i) Given m, n nonzero elements of $\mathbb{Z}$ let $S(m, n) = \{am + bn | a, b \in \mathbb{Z}\}$. Show that $S(m, n)$ is a subgroup of $\mathbb{Z}$ which contains m and n.

(ii) It follows from (i) that $S(m, n) = (d)$ for some integer $d \geq 1$. Show that d divides m and n. Then, using that $d \in S(m, n)$ show that in fact, d is the greatest common divisor of m and n, i.e., that any other common divisor of m and n must also divide d.
(iii) Explain how parts (i) and (ii) show that in general if m, n are nonzero integers then we may find integers a and b such that $gcd(m, n) = am + bn$.

5. Fix a group G (which could be infinite).
(a) Show that the inversion map $A : G \to G$ given by $A(g) = g^{-1}$ is an **anti − automorphism** i.e., a bijection which has the property that $A(xy) = A(y)A(x)$.
(b) Give an example of a group G and a subgroup H of G such that the partition of G into left cosets of H is different from the partition of G into right cosets of H.
(c) Let $G/H = \{gH | g \in G\}$ denote the set of left cosets of H in G and let $H \backslash G = \{Hg | g \in G\}$ denote the set of right cosets of H in G. Construct a bijection between G/H and $H \backslash G$. Thus these sets have the same cardinality and the index $|G : H|$ is independent of whether we use left cosets or right cosets in its definition. (Note: Your proof should work even when $|G : H|$ is infinite!)

6. Show that if $x^2 = e$ for all $x \in G$ then the group G must be Abelian. (Recall $x^2 = x * x$)

7. Suppose $\mathbb{A}, \mathbb{B}$ and $\mathbb{C}$ are $n \times n$ real matrices with $\mathbb{A}\mathbb{B} = \mathbb{A}\mathbb{C}$ and $det(\mathbb{A}) \neq 0$. Explain why we may then conclude $\mathbb{B} = \mathbb{C}$. On the other hand, when $det(\mathbb{A}) = 0$ explain why we can find **distinct** $n \times n$ matrices $\mathbb{B}$ and $\mathbb{C}$ such that $\mathbb{A}\mathbb{B} = \mathbb{A}\mathbb{C}$.

8. Let $\mathbb{Q} = \{\frac{m}{n} | m, n \in \mathbb{Z}, n \neq 0\}$ be the group of rational numbers under addition. Show that the Abelian group $(\mathbb{Q}, +)$ is not finitely generated as a group.