Kris Harper
MATH 20700
October 6, 2008

Homework 1

Problem 1. *If r and s are rational numbers such that $r+s$ and rs are integers, must r and s be integers?* Yes.

Proof. Let $r, s \in \mathbb{Q}$. Then $r = a/b$ and $s = c/d$ where $a, b, c, d \in \mathbb{Z}$, $b, d \neq 0$ and $(a, b) = (c, d) = 1$. Then $rs = ab/cd$ and $r + s = (ad + bc)/bd$. Since $rs, r + s \in \mathbb{Z}$ we know that $bd \mid ac$. Thus either $b = 1$ or there exists some prime, p, such that $p \mid b$ and $p \mid ac$. Note that either $p \mid a$ or $p \mid c$, but since $(a, b) = 1$ we see that $p \mid c$. The same can be said for another prime, q, such that either $d = 1$ or $q \mid d$ and $q \mid a$. Note also that $bd \mid (ad + bc)$ and so $p \mid (ad + bc)$. But also, $p \mid bc$ and $p \nmid ad$. Since p doesn't divide one term of the sum, but divides the sum, it must be the case that $p = 1$. The same can be said for $q = 1$. Thus $b = d = 1$ and r and s are integers. □

Problem 2. *Show that, for $n \geq 2$,*

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$$

is never an integer.

Proof. Let $n \geq 2$. Note that the sum

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$$

can be written as

$$\frac{\sum_{k=1}^{n} \frac{n!}{k}}{n!}$$

Note that there exists an integer p such that $2^p \leq n < 2^{p+1}$. Let the highest power of 2 that divides $n!$ be q. Each term in the above sum in the numerator consists of $n!$ divided by some integer $1 \leq k \leq n$. Thus the lowest power of 2 which divides any of the terms in the numerator is $(q - p)$ which occurs when $k = 2^p$. Every other term will be divisible by 2^{q-p+1} and so the highest power of 2 dividing the sum is $(q - p)$. For $n \geq 2$ we have $p \geq 1$ and so the numerator must have a lower power of 2 dividing it than the denominator. Thus the original sum cannot be an integer since 2 is prime. □

Problem 3. *Show that, if $n \geq 2$, the integer $n! = n(n-1)(n-2)\ldots 2 \cdot 1$ is never a perfect square.*

Lemma 1. *The number of factors of a perfect square is odd.*

Proof. Let k be a positive integer and consider some factor of k, a. Then we know $a \mid k$ and so there exists some positive integer b such that $ab = k$. An element such as b will exist for every factor of k and a and b will always be distinct, unless k is a perfect square. In this case there exists some factor of k, c such that $c^2 = k$. Thus, if k is not a perfect square, then factors of k can be paired distinctly, so k has even number of factors. If k is a perfect square then the factors of k can be paired distinctly, save for one pair, which makes an odd number of factors. □

Proof. Note that $n!$ must have an even number of factors. Then by Lemma 1 it must not be a perfect square. □

Problem 4. *Suppose $f : \mathbb{R} \to \mathbb{R}$ is a function such that $|f(x) - f(y)| = |x - y|$ for all real numbers x, y. What can you say about f?*

Letting $y = 0$ we see that $|f(x) - f(0)| = |x|$. From here we have $f(x) = \pm x \pm f(0)$. Thus f is a continuous, differentiable, linear function.

Problem 5. *Show that there does not exist an equilateral triangle in the plane whose vertices are lattice points. Find those regular polygons in the plane whose vertices are lattice points.*

Proof. Let us briefly use the complex plane. Suppose that we already have two lattice points, u and w. We show that a third point, z, must not be a lattice point. Given the three points u, w, z, the centroid of the triangle formed by them is

$$x = \frac{u + w + z}{3}.$$

Given this and the two points u and w we want the condition each of u w and z are a distance L from the center, x, and are separated by an angle of $2\pi/3$. Thus

$$u - x = L \exp(\alpha)$$

$$z - x = L \exp\left(\alpha - \frac{2\pi}{3}\right)$$

and

$$w - x = L \exp\left(\alpha + \frac{2\pi}{3}\right)$$

for some angle α. This implies that $(u - x)(w - x) = (z - x)^2$ which after substituting for x and expanding gives us

$$u^2 + w^2 + z^2 = uw + uz + wz.$$

Using the quadratic formula to solve for z we end up with

$$z = \frac{u + w \pm i\sqrt{3}(u - w)}{2}.$$

Thus, since u and w have integer values for both their real an imaginary parts, we see that z must have an irrational value for one of its coordinates. □

All regular polygons with four or more sides have interior angles greater than or equal to $\pi/2$ and less than π. Since the only angle greater than or equal to $\pi/2$ and less than π with rational values for both sine and cosine is $\pi/2$, we know that the square is the only possible regular polygon with lattice coordinates.

**** Problem 1.** *For a group $(G, \circ)$ show the following:*
1) Left inverses exist and are also right inverses.
2) Left identity is also right identity.
3) Left solvability is also right solvability.
4) Inverses are unique.
5) Identity is unique.

Proof. 1) To show that left inverses exist, use the solvability axiom with the identity element. For all $a \in G$ there exists $x \in G$ such that $x \circ a = e$. Thus, $x = a^{-1}$ serves as the left inverse of a. To show that left inverses are also right inverses, consider $a^{-1} \circ a = e$ and $\left(a^{-1}\right)^{-1} \circ a^{-1} = e$. With the associative property these imply

$$\left(a^{-1}\right)^{-1} = \left(a^{-1}\right)^{-1} \circ e = \left(a^{-1}\right)^{-1} \circ \left(a^{-1} \circ a\right) = \left(\left(a^{-1}\right)^{-1} \circ a^{-1}\right) \circ a = e \circ a = a$$

which then means that $a^{-1} \circ a = a \circ a^{-1} = e$.

2) For the identity we use the previous property noting that for all $a \in G$ we have $a^{-1} \circ a = a \circ a^{-1} = e$. Then with the associative property we have

$$a = e \circ a = \left(a^{-1} \circ a\right) \circ a = \left(a \circ a^{-1}\right) \circ a = a \circ \left(a^{-1} \circ a\right) = a \circ e$$

which means $e \circ a = a \circ e = a$ and so left identities are also right identities.

3) For solvability we use both of the previous properties. Note that if G is solvable then for all $a, b \in G$ there exists $x \in G$ such that $x \circ a = b$. Then $x^{-1} \circ x \circ a = x^{-1} \circ b$ and so $a = x^{-1} \circ b$. Then $a \circ b^{-1} = x^{-1} \circ b \circ b^{-1} = x^{-1}$. Therefore $a \circ b^{-1} \circ x = x^{-1} \circ x = e$ and $a \circ b^{-1} \circ x \circ b = b$. Thus, for all $a, b \in G$ there exists $y \in G$ such that $a \circ y = b$.

4) To show inverses are unique, consider an element $a \in G$ and two inverses of a, a_1^{-1} and a_2^{-1}. Then using the associativity axiom and the fact that left inverses and identities are also right, we have

$$a_1^{-1} = a_1^{-1} \circ e = a_1^{-1} \circ (a \circ a_2^{-1}) = (a_1^{-1} \circ a) \circ a_2^{-1} = e \circ a_2^{-1} = a_2^{-1}.$$

Thus $a_1^{-1} = a_2^{-1}$.

5) To show that the identity, e, is unique, consider two identities, e_1 and e_1. Then, because left identities are also right, we have

$$e_1 = e_1 \circ e_2 = e_2 \circ e_1 = e_2.$$

Thus, e is unique. □

**** Problem 2.** *If $f, g \in \mathcal{S}(A)$, then $g \circ f, f \circ g \in \mathcal{S}(A)$.*

Proof. Let $f, g \in \mathcal{S}(A)$. Then $f : A \to A$ and $g : A \to A$ are bijections. Consider two elements $a, b \in A$ such that $g(f(a)) = g(f(b))$. We know g is injective so $f(a)$ must equal $f(b)$. And since f is injective $a = b$. Thus $g \circ f$ is injective. Now consider some element $c \in A$. We know g is surjective so there exists some $b \in A$ such that $g(b) = c$. Also, f is surjective so there exists some element $a \in A$ such that $f(a) = b$. Then $g(f(a)) = c$ so for all $c \in A$ there exists $a \in A$ such that $g \circ f(a) = c$. Thus $g \circ f$ is surjective. Therefore, $g \circ f$ is a bijection and is in $\mathcal{S}(A)$. A similar proof holds for $f \circ g$. □

**** Problem 3.** *Show that $(\mathcal{S}(A), \circ)$ is a group.*

Proof. Let $f, g, h \in \mathcal{S}(A)$ and $a \in A$. Then consider

$$(h \circ g) \circ f(a) = h \circ g(f(a)) = h(g(f(a))) = h(g \circ f(a)) = h \circ (g \circ f)(a)$$

which shows that $\circ$ is associative.

Consider the function I where $I(a) = a$ for all $a \in A$. This function is bijective and is thus in $\mathcal{S}(A)$. Then for all $f \in \mathcal{S}(A)$ we have $I \circ f(a) = I(f(a)) = f(a)$. Thus I serves as a left identity for $\circ$.

To show solvability we consider two functions $f, g \in \mathcal{S}(A)$ and we wish to find a function $h \in \mathcal{S}(A)$ such that $h \circ f = g$. Choose $h : A \to A$ such that $h(f(a)) = a$ for all $a \in A$. Now consider two elements, $a, b \in A$ such that $h(f(a)) = h(f(b))$. Then $a = b$ and so $f(a) = f(b)$. Thus h is injective. Next we see that for all $a \in A$, $h(f(a)) = a$ and so h is surjective. Thus, h is a bijection and so $h \in \mathcal{S}(A)$. Thus, $\mathcal{S}(A)$ is solvable. Since all the axioms are met, $(\mathcal{S}(A), \circ)$ is a group. □

**** Problem 4.** *Show that the Dihedral Group D_{2n} on a regular n-gon is the set $\{I, r, r^2, \ldots, r^{n-1}, f, rf, r^2f, \ldots, r^{n-1}f\}$ endowed with composition of transformations. Also show that $r^n = I$, $f^2 = I$ and $rf = fr^\alpha$ for some value of alpha. Find alpha.*

Proof. We know that D_{2n} is the group of symmetries of a regular n-gon. The transformation, I, corresponds to doing nothing to the n-gon. This is the identity function of the group. The transformation, r, rotates the n-gon counterclockwise by $360/n$ degrees. This corresponds to the rotation which moves each vertex one spot counterclockwise. Doing this twice, that is, performing the r^2 transformation, rotates the n-gon counterclockwise by $2(360/n)$ degrees. Doing this n times corresponds to rotating it $n(360/n) = 360$

degrees, which is the same as doing nothing. This shows that $r^n = I$ and that the elements $r, r^2, \ldots r^{n-1}$ are all in D_{2n}.

The function, f, reflects the n-gon about an axis of symmetry connecting one vertex to its opposite vertex, for n even, or from one vertex to the midpoint of the opposite side, for n odd. If we reflect the n-gon about any of these axes of symmetry and then reflect back on the same one, we will have the original orientation. Thus $f^2 = I$. Also, performing r on the n-gon rotates which vertex corresponds to the axis of symmetry. Thus, f reflects about one axis of symmetry and rf reflects about another. To reflect about each axis of symmetry we must perform all possible rotations, which we just showed were $r, r^2, \ldots, r^{n-1}$. Thus $f, fr, fr^2, \ldots, fr^{n-1}$ are all elements of D_{2n}. Finally, note that if we rotate the n-gon k spots counterclockwise and then reflect about an axis of symmetry, then reflect back, we must rotate the remaining $n - k$ spots counterclockwise to end up where we started. Thus $r^k f = fr^{n-k}$ for $0 \leq k \leq n$. In particular, we have $rf = fr^{n-1}$. □