11^{th} Annual Johns Hopkins Math Tournament
Sunday, April 11, 2010
Explorations Unlimited Round-Introduction to Group Theory

1. Introduction

Often times in mathematics, a particular set of objects is not as important as what the objects do when subjected to various operations. For example, there is nothing particularly interesting about the integers, $\mathbb{Z}$, until we are allowed to act on them with addition, multiplication, and so on. In group theory, rather than studying specific objects such as numbers, we study what happens when these objects are allowed to interact through operations, such as addition. As we'll see, the operations that we use can tell us a whole lot more about the structure of certain sets than the objects themselves. In this round, we will explore some of the very basic aspects of group theory.

2. Basic Definitions

A **group** is a set G together with an operation $\circ$ that combines two elements, a and b in G to form another element $a \circ b$ (called a binary operation). The set and the operation, written together as $(G, \circ)$ must satisfy the following four axioms:

(1) Closure: if a and b are in G, then $a \circ b$ must be in G as well.
(2) Associativity: if a, b, and c are in G, then $(a \circ b) \circ c = a \circ (b \circ c)$.
(3) Identity: there is an element e in G such that if a is any element in G, then $a \circ e = e \circ a = a$. We call e the identity.
(4) Inverses: if a is any element in G, then there is some element b in G such that $a \circ b = b \circ a = e$, where e is the identity from axiom 3. We call b the inverse of a and write $b = a^{-1}$ (this does *not* necessarily mean $\frac{1}{a}$, it is just the notation used).

So what is an example of a group? Perhaps the simplest example is the integers, $\mathbb{Z}$, under the operation of addition, $+$. Let's see why. From basic arithmetic, we know that if we add two integers, we get another integer, so axiom (1) holds. We also know from basic arithmetic that addition is an associative operation, so axiom (2) holds. For the identity, the number 0 of course does the trick ($a + 0 = a$ for any integer a). Finally, since the operation is addition, we are looking for *additive* inverses. Well, we know that if a is any integer, if we add $-a$, we get 0. Since we can always find a $-a$ for any integer a, we have inverses. Hence $\mathbb{Z}$ satisfies all of the group axioms.

Q1) [2 points] We can also regard the rational numbers, $\mathbb{Q}$, as a group under addition. If q is any rational number, what is its inverse? What is the identity element?

Let's look at an example where the operation is not addition. Consider the real numbers, $\mathbb{R}$. Of course, the real numbers form a group under addition in the same way that $\mathbb{Z}$ and $\mathbb{Q}$ do, but let's try multiplication. Again from elementary arithmetic, we know that we can multiply any two real numbers and we still get a real number, and we know that multiplication is associative. How about the identity? We are looking for a real number so that if we multiply by the identity, we get back the original. The number 1 immediately comes to mind, and that's it. Inverses are only slightly trickier. First, remember that we need *multiplicative* inverses, so we need some number b such that $ab = 1$. You should immediately want to divide both sides by a and declare that $b = \frac{1}{a}$ is the inverse we want. And you would be right except for one little caveat: a can't be 0. Alright, no problem. We simply say that the real numbers with 0 omitted, written $\mathbb{R} \setminus \{0\}$ or $\mathbb{R}^{\times}$, form a group under multiplication. And you should have little trouble seeing that $\mathbb{Q}$ works in exactly the same way under multiplication (remember, we have to get rid of 0).

Q2) [3 points] Consider the integers with 0 omitted, written $\mathbb{Z} \setminus \{0\}$. Does $\mathbb{Z} \setminus \{0\}$ form a group under multiplication? Why or why not? [Hint: There is only one axiom that might cause problems.]

Before we continue, here is one more definition. An **abelian group** is a group that is commutative. That is, a group is abelian if $a \circ b = b \circ a$ for all a, and b in the group. If G is a group, the **center** of the group, written $Z(G)$, is the set of all of the elements in G that commute with all the other elements. Notice that in an abelian group, since every element commutes with every other element, $Z(G) = G$. For example, $\mathbb{Z}$ under addition is an abelian group because addition is commutative, i.e. $a+b = b+a$ for all integers a and b. It follows that $Z(\mathbb{Z}) = \mathbb{Z}$.

Q3) [4 points] Is $\mathbb{Q}$ under addition an abelian group? What is its center? Is $\mathbb{R} \setminus \{0\}$ under multiplication an abelian group? What is its center?

3. Symmetric Groups

Now we'll introduce an extremely important group whose elements are not numbers. Let's say we have a set of objects, call it X (the objects might be numbers, pens, Hopkins students, and so on). A permutation of the objects is simply a rearrangement. For example, if we have a list of numbers written 1 2 3, then some examples of permutations are (1 3 2) and (2 3 1). Notice that we didn't change the objects or how many objects there were, we simply changed the order.

Now, given some set of objects X, the **symmetric group** on X is written S_X and consists of all possible permutations of the objects of X. That is, the elements of S_X are the permutations of the objects, *not* the objects themselves. We will always deal with the case when X is a set of integers. Now, if n is a positive integer (1,2,3 and so on), S_n is called the **symmetric group of degree** n and consists of all permutations of the set $\{1, 2, \ldots, n\}$. That is, all of the ways to write the numbers 1, 2, ..., n in a list.

Q4) [6 points] Write out all of the elements of S_3. In other words, write all possible permutations of the set $\{1, 2, 3\}$, listing the numbers in order inside brackets. For example, $\{1, 2, 3\}$. [Hint: There are 6 permutations.]

So how big is the symmetric group of degree n? Perhaps you've already suspected a pattern, but let's make it clear. Suppose we have S_3. We saw above that S_3 has 6 elements. Why? Well let's say that we want to list a permutation $\{- \ - \ -\}$. How many numbers can go in the first spot? Clearly, we have free choice and we can pick either 1, 2, or 3. In other words, there are 3 choices. In the second spot, we can pick from among either of the remaining 2 objects, and in the third sport, we're stuck with 1 remaining object. Hence there are $3 \cdot 2 \cdot 1 = 6$ possible permutations. Of course, we can do the same thing for any S_n; we have n choices for the first spot, $n-1$ for the second spot, $n-2$ for the third, and so on. Hence S_n has $n \cdot n-1 \cdots 2 \cdot 1 = n!$ elements.

Now, let's see why S_n is a group. First of all, we need an operation. The appropriate operation will actually be "composition of permutations." This means that we will take one permutation, and then permute the objects again. That is, we rearrange a rearrangement! To do this, we have to come up with notation. Let's assume that we're working in S_5, the permutations of the numbers 1-5, just for an example (it's the same for the other S_n).

We'll use something called cycle notation, which describes the permutation with sets of parentheses. We start with a number in our collection (typically 1 but it doesn't really matter). Next to that number, we write where we're sending it. For example, if 1 is being sent to 3, we write $(1\,3\cdots)$. Then, we write where 3 is going; say it goes to 5. Then we write $(1\,3\,5\cdots)$. Now, let's suppose that 5 gets sent to 1. Since 1 was used at the start, we see that the permutation has "cycled" back to the beginning, hence the name. In this case, we close the parentheses, and start the next cycle. So we would have (1 3 5). Next, we'll see what happens to 2, since that's the smallest number we haven't used yet. Suppose that 2 gets sent to 4. Then we write $(2\,4\cdots)$. And since this is S_5, 4 is the last number left and it gets sent back to 2. Then the desired cycle would just be (2 4). So the whole thing is (1 3 5)(2 4).

Of course, we can also use a cycle to tell us what's going on. Let's say we've got a permutation (2 3)(1 4 5) in cycle notation. This tells us that 1 goes to 4, 2 goes to 3, 3 goes to 2, 4 goes to 5, and 5 goes to 1. Or, we can write

$$1 \mapsto 4 \qquad 2 \mapsto 3 \qquad 3 \mapsto 2 \qquad 4 \mapsto 5 \qquad 5 \mapsto 1.$$

WARNING: It might be tempting to say that (1 2 4 3) and (4 3 1 2) are different permutations (say in S_4) but this is not the case. Remember, these are permutations so just rotating all the objects doesn't change anything. In other words two permutations are different if and only if the order of the numbers in them is different. So (1 2 3), (2 3 1), and (3 1 2) are all the same permutation in S_3 because the order of the numbers is the same; all we did was move them over.

Q5) [7 points] Consider the permutation which sends 5 to the first spot, 3 to the second spot, 7 to the third spot, 4 to the fourth spot, 1 to the fifth spot, 6 to the sixth spot, and 2 to the final spot. Write out this permutation using the parentheses notation above. Now consider the new permutation (2 1 3 4). Using the $\mapsto$ notation above, write where 1, 2, 3, and 4 are sent. To make grading easier, start with 1 like we did above.

Now we can discuss "composing" permutations. Suppose σ and τ represent two arbitrary permutations. Then to compute the composition $\sigma \circ \tau = \sigma\tau$, we must first look at how τ acts on a number, and then how σ acts on that new number. Suppose, for example, that $\sigma = (1\,5\,2\,4\,3)$ and $\tau = (3\,4\,1\,2\,5)$. How do we compute

$\sigma\tau = (1\,5\,2\,4\,3)(3\,4\,1\,2\,5)$? First, we look at what happens to 1. The τ permutation takes $1 \mapsto 2$. Now, we must see what σ does to 2: it takes $2 \mapsto 4$. Hence the composition takes $1 \mapsto 4$. Since 4 is the end result, we now start over with 4. That is, what does τ do to 4? We see that $4 \mapsto 1$ under τ, and then that $1 \mapsto 5$ under σ. Hence $4 \mapsto 5$. Now we go back to τ again and look at what happens to 5; it goes to 3 so $5 \mapsto 3$. Under σ, $3 \mapsto 1$. Therefore, we are right back where we started, so we have $(1\,4\,5)$. We can now stop this cycle and start a new one. The next smallest number we haven't used yet is 2 so let's start there. We notice that $2 \mapsto 5$ under τ and then $5 \mapsto 2$ under σ. So nothing happens at all! That is, we're left with (2). The last number that we haven't used yet is 3, and it's easy to check that $3 \mapsto 4 \mapsto 3$. So this cycle doesn't go anywhere either. That is, it's just (3). Hence if we write the whole composition together, we find that $\sigma\tau = (1\,4\,5)(2)(3)$.

Q6) [7 points] Compute the composition $(2\,1\,7\,6\,5\,3\,4)(3\,6\,1\,2\,7\,5\,4)(4\,7\,3\,1\,5\,2\,6)$ in S_7. Please begin with 1. [Hint: First compute $(3\,6\,1\,2\,7\,5\,4)(4\,7\,3\,1\,5\,2\,6)$ and then multiply on the left by $(2\,1\,7\,6\,5\,3\,4)$.]

Now that we've got an operation, let's finish defining the group structure of S_n. Closure of the operation is obvious, since permuting a set of n objects, and then re-permuting that set still gives us a permutation of n obejcts. Function composition is always an associative operation so that gives the second axiom. The identity permutation is simply the one that keeps every object where it is ($1 \mapsto 1$, $2 \mapsto 2$,..., $n \mapsto n$). Finding an inverse is easy, too: simply reverse the order of the permutation. For example, the inverse of $(4\,2\,3\,1)$ is $(1\,3\,2\,4)$ (you can check this if you like).

Q7) [7 points] Compute the inverse of your answer from Q6.

Q8) [6 points] Compute $(3\,4\,2\,1)(4\,1\,3\,2)$ and $(4\,1\,3\,2)(3\,4\,2\,1)$. Is S_4 abelian?

Q9) [10 points] An m-cycle is a cycle with m elements (for example, $(1\,2\cdots m)$ is an m-cycle). If $m \leq n$, find the number of m-cycles in S_n. [Hint: Count the number of ways to form an m-cycle and divide by the number of equivalent representations. The WARNING before Q5 will help with this.]

4. Subgroups

If we have a group G with some operation $\circ$, then subsets of G might behave nicely, too. A subset H of G is called a **subgroup** of G if it is also a group under $\circ$. For example, $\mathbb{Z}$ is a subgroup of $\mathbb{Q}$ under $+$, and $\mathbb{Q} \setminus \{0\}$ is a subgroup of $\mathbb{R} \setminus \{0\}$ under multiplication. If H is a subgroup of G, we write $H \leq G$. This does *not* mean H is less than or equal to G, it means that H is a subgroup of G. We will always use $\leq$ to mean "is a subgroup of" unless you are told otherwise.

Q10) [4 points] Find a non-trivial *proper* subgroup of S_3. [Hint: Start with the identity permutation, call it i, and then find some others that make all the axioms hold. In particular, if you compose any two permutations, you must get back one in your subgroup and everything must have an inverse.]

You might wonder if there is an easy way to test whether or not a subset of a group is a subgroup. As a matter of fact, there is a simple criterion: suppose G is a group and H is a subset of G. Then H is a subgroup of G if and only if H is not empty, and whenever a and b are in H, $a \circ b^{-1}$ is also in H.

Q11) [5 points] Let $4\mathbb{Z} = \{\ldots, -8, -4, 0, 4, 8, \ldots\}$ denote all integers that are divisible by 4. Use the subgroup test to determine if $4\mathbb{Z}$ is a subgroup of $\mathbb{Z}$ under addition.

The **order** of a group is the number of elements in the group, and is written $|G|$. For example, as we saw in the last section, $|S_n| = n!$. Of course, as we saw with $\mathbb{Z}$, the order of a group does not have to be finite (in fact, as $\mathbb{R}$ shows, it doesn't even have to be countable!). While it's a little bit harder to say things when the order of a group is infinite, as we will see in the next section, the order of a finite group can tell us a lot.

Q12) [4 points] Let $\sigma = (1\,3\,2)$ in S_3, and let $\langle\sigma\rangle = \{(1\,3\,2), (1\,3\,2)(1\,3\,2), (1\,3\,2)(1\,3\,2)(1\,3\,2), \ldots\}$. Find the order of the subgroup $\langle\sigma\rangle$ inside S_3. [Hint: It's finite.]

The last problem introduced a new way to form a subgroup. Let's say we have some group G, and a is some element in G. Instead of having a act on some other element b, let's make a act on itself. In other words, $a \circ a$. But why stop here? We can keep going to get $a \circ a \circ a$, $a \circ a \circ a \circ a$, and so on. Let's write $a_{(n)} = a \circ a \circ \cdots \circ a$, where a acts on itself n times. In the case where n is negative, we just mean the inverse of a acting on itself n times. Then $\langle a\rangle = \{\ldots, a_{(-2)}, a_{(-1)}, a_{(0)}, a_{(1)}, a_{(2)}, \ldots\}$ is called the **cyclic subgroup** generated by a. So $\langle a\rangle$ is

actually a subgroup of G.

Now, if G is a group with finite order, i.e. a finite number of elements, then $\langle a \rangle$ is also a subgroup with finite order. Now let's say that $a_{(n)}$ is equal to the identity for some n. In other words, if we have a act on itself n times, we reach the identity, which we'll call 1. That is, $a_{(n)} = 1$. Then n is called the **order** of a and we write $|a| = n$. This may seem to conflict with our earlier definition but as a matter of fact, $|\langle a \rangle| = |a|$. That is, the order of the subgroup generated by a is the same as the order of a as an element. So the definitions agree!

Q13) [3 points] What is the order of $(1\,2)$ as an element in S_2?

5. Lagrange's Theorem

In the last section, we suggested that the order of a finite group tells us something, so let's investigate that here. Let $H \leq G$ be a subgroup of an arbitrary group G and let a be any element in G. Then the **left coset** of H in G is $aH = \{ah \mid h \text{ in } H\}$. This means that we take the element a and we multiply on the right by every element in H. For example, above you saw the coset $4\mathbb{Z} = \{4z \mid z \text{ is an integer}\} = \{\ldots, -4, 0, 4, \ldots\}$. Remember, the element a appears on the left, and the elements of H appear on the right; since H and G might not be abelian, we can't move them to the other side. Of course, if the group has an addition operation, then the coset is defined by $a+H$.

Q14) [3 points] Let $H = \langle \sigma \rangle$ be the subgroup of S_3 generated by $(1\,3\,2)$ that you saw in Q12. List the elements of the left coset $(1\,2\,3)H$.

Now let's do something with these left cosets. If G is a group and H is a subgroup, write G/H to denote the set of *all* left cosets of H in G. This means that instead of using just one a in G, we go through every a in G. For example, let's take $G = \mathbb{Z}$ and $H = 3\mathbb{Z}$. Just what exactly is the quotient group $\mathbb{Z}/3\mathbb{Z}$? If we follow the definition, it's all elements of the form $z + 3\mathbb{Z}$, where z is an integer (remember, we're adding because that's the operation on $\mathbb{Z}$). Hence

$$\mathbb{Z}/3\mathbb{Z} = 3\mathbb{Z}, 1 + 3\mathbb{Z}, -1 + 3\mathbb{Z}, \ldots$$

As a matter of fact, as we will see below, there is some redundancy here but for now, just see how to write out the members of a quotient group.

Can we add and multiply cosets? Yes we can, but we have to be careful. However, all of the examples we pick here will work well so you won't have to worry about where problems arise. If we have a subgroup $H \leq G$, and two elements a and b in G, then we multiply cosets by $aH \circ bH = (a \circ b)H$, or add them as $(a+H) \circ (b+H) = (a \circ b)+H$. Again, it depends on the operation of the group. Speaking of groups, can we make G/H into a group? Yes and in fact, we already started to. We just presented the operation (adding/multiplying cosets) and we know it's associative. So we're left with identities and inverses. But these are easy, too. The identity is simply $1 \cdot H = H$ or $0+H = H$ (depending on the operation) and the inverse is simply $a^{-1}H$ or $-a+H$. So that's it, G/H is a group!

Q15) [5 points] What happens if a is already an element of H? In other words, compute aH if a is already in H.

Q16) [7 points] Let $H \leq G$ be a subgroup of G so that multiplication "works." Show that if n is any integer, then $(aH)_{(n)} = a_{(n)}H$ in the quotient group G/H, where a is any element in G.

Now we need an important property of cosets. A **partition** of a set is a way to split the set so that none of the pieces have any elements in common and when we put all of the pieces back together, we get the original set. Cosets are useful because they partition a group. Let's see an example of why this works. Let's look at $4\mathbb{Z}$ (under addition) and see how these cosets partition $\mathbb{Z}$. Let's start with 0, because that's easy. We have that

$$0 + 4\mathbb{Z} = \{\ldots, 0-4, 0+0, 0+4, \ldots\} = \{\ldots, -4, 0, 4, \ldots\} = 4\mathbb{Z}$$

In other words, it's the original. Let's go to 1 now:

$$1 + 4\mathbb{Z} = \{\ldots, 1-4, 1+0, 1+4, \ldots\} = \{\ldots, -3, 1, 5, \ldots\}$$

Now 2:

$$2 + 4\mathbb{Z} = \{\ldots, 2-4, 2+0, 2+4, \ldots\} = \{\ldots, -2, 2, 6, \ldots\}$$

And then 3:

$$3 + 4\mathbb{Z} = \{\ldots, 3-4, 3+0, 3+4, \ldots\} = \{\ldots, -1, 3, 7, \ldots\}$$

Now, if we try to add 4, then we see that we end up exactly where we started, i.e.

$$4 + 4\mathbb{Z} = 4\mathbb{Z}$$

You should now see that if we try adding 5, 6, 7,... and even -1, -2, -3,... we're still going to get the same things we already have. In other words, $4\mathbb{Z}, 1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}, 3 + 4\mathbb{Z}$ completely partition $\mathbb{Z}$ (observe that none of them have any elements in common and together, they cover every integer).

Now we are ready for the main result. Although it isn't always easy to find subgroups of a given group, there is a very easy property that all subgroups have. Suppose G is a group with finite order. Then of course any subgroup must have finite order as well. But in fact, the order of the subgroup must divide the order of the original group. This is Lagrange's Theorem.

Q17) [15 points] Lagrange's Theorem: If G is a finite group and H is a subgroup of G, then the order of H divides the order of G. Let $|H| = n$ and let the number of left cosets of H in G equal k.

(1) Find a function whose domain is H and whose range is aH for any *fixed* a in G. [Hint: This is easy!]
(2) A function f is called one-one if $f(x) = f(y)$ implies $x = y$. Show that your function from part 1 is one-one. [Hint: If your answer from part 1 is not one-one, you've got the wrong function!]
(3) Parts 1 and 2 showed that your function is something called a bijection. Bijections preserve size. What can you say about the order of H and aH?
(4) Since G is partitioned into k disjoint subsets each of which has cardinality n, $|G| = kn$. Conclude from part 3 that $|H| = \frac{|G|}{k}$.

Q18) [10 points] If G is a finite group and a is in G, show that the order of a divides the order of G. [Hint: Remember that $|a| = |\langle a \rangle|$.] Prove that $x_{(|G|)} = 1$ for all x in G.

Q19) [10 points] Recall that a group is cyclic if it can be generated by a single element, i.e. $G = \langle a \rangle$. Prove that if $|G| = p$ where p is any prime number, then G must be cyclic. [Hint: Use the fact that any cyclic groups of the same order are the same.]

6. Homomorphisms

Just like we can have functions between sets of numbers, we can also have functions between groups. However, not all functions are useful. Specifically, we need to look at functions that preserve group structure. Let $(G, \circ)$ and $(H, \cdot)$ be any two groups. Then a function $f : G \to H$ such that $f(a \circ b) = f(a) \cdot f(b)$ for all a and b in G is called a **homomorphism**. In other words, if we do an operation in the domain, then once we apply the function f, the operation is still preserved in the range. Let's look at some examples of functions that are homomorphisms. First, let's consider the groups $\mathbb{R}$ under addition and $\mathbb{R}_{>0}$ under multiplication (this means all of the real numers bigger than 0). Let $f(x) = e^x$. Is this a homomorphism? Let a and b be any two real numbers. Then $f(a+b) = e^{a+b}$. But if we remember our rules for multiplying exponents, this is really the same thing as $e^a \cdot e^b$. But then each of these is really the same thing as $f(a) \cdot f(b)$. So $f(a + b) = f(a) \cdot f(b)$, which means that f is indeed a homomorphism.

Q20) [5 points] Let $f : G \to H$ be a homomorphism. Prove that $f(a_{(n)}) = (f(a))_{(n)}$ for any positive integer n, where a is in G.

Q21) [7 points] Let G be an abelian group. Prove that $f(a) \cdot f(b) = f(b) \cdot f(a)$ for any a and b in G.

Now we will deal with a very special type of homomorphism. If $f : G \to H$ is a homomorphism that has H as its range and is also one-one, then we call f an **isomorphism**. In other words, an isomorphism is a homomorphism that is also a bijection. These are really nice because they actually show that G and H are the same! When we say "the same", we mean that the groups have the same structure (of course, the elements and the operation may be different). Determining when two groups are isomorphic is really important because it makes it easier to study complicated groups. If we show that some new and weird group is isomorphic to some group that we already have a lot of experience with, then it's easier to study. In fact, we have already seen an example of an isomorphism. The homomorphism $f(x) = e^x$ from above, between $\mathbb{R}$ (addition) and $\mathbb{R}_{>0}$ (multiplication) is actually an isomorphism because the function e^x is a bijection. If a group G is isomorphic to a group H, we write $G \cong H$.

Let's introduce some new terms. The **image** of a homomorphism is its range; it's wherever the function goes. So for the function e^x above, the image is all positive real numbers. The **kernel** is all of the stuff in the *domain*

that gets sent to the identity in the *range*. So for e^x, since the identity in $\mathbb{R}_{>0}$ under multiplication is 1, we need to find all of the elements in the range that get sent to 1. But of course we know that $e^x = 1$ only if $x = 0$, so the kernel is 0.

We will conclude our brief introduction to groups with a very powerful theorem. Sometimes, it's hard to actually construct an isomorphism. So instead, we look for a way to cheat a little bit-instead of actually finding an isomorphism, we look for just an ordinary homomorphism with certain properties.

Let's say we have a homomorphism with domain G and image (or range) H. Now, let's say that the kernel of this homomorphism is the set K. In other words, if k is in K, then $f(k)$ is the identity of H. Then the **First Isomorphism Theorem** says that $G/K \cong H$. In other words, the quotient group of the kernel in G is isomorphic to the image (range). Let's do an example.

Let G be the real numbers $\mathbb{R}$ under $+$ and let $f(x) = e^{2\pi ix}$, where $i = \sqrt{-1}$ (this is isn't nearly as weird as it looks; if you go on to take complex analysis, this comes up all the time). As x goes through the real numbers, $f(x)$ goes around the unit circle, which we'll call S^1 (don't worry if you don't immediately see this; you can take our word for it that it's true). In other words, the unit circle, S^1, is the image of f. So what's the kernel of f? We need to find all of the x such that $f(x) = 1$, because 1 is the identity in this case. In other words, we need $e^{2\pi ix} = 1$. Again, you can take our word for it, this happens whenever $2\pi ix$ is a multiple of $2\pi i$. But since we've already got a $2\pi i$ in the expression, we just need x to be an integer. So that's easy, the kernel of f is simply $\mathbb{Z}$, the integers! So now let's go back and see what the isomorphism theorem tells us: $G = \mathbb{R}$, the kernel $K = \mathbb{Z}$, and the image $H = S^1$, the unit circle. So if we put it together, the first isomorphism theorem tells us that $\mathbb{R}/\mathbb{Z} \cong S^1$. This is a rather fascinating result, don't you think?

Q22) [10 points] Prove the first isomorphism theorem by following the steps below.

(1) Let $\pi : G \to G/K$ be defined by $\pi(a) = aK$ where a is in G. In other words, π takes any element in G to its coset in K. Let $f : G \to H$ be any homomorphism with image (range) H. Now, define a function $\theta : G/K \to H$ by $\theta(aK) = f(a)$. Check θ is a homomorphism. In other words, check that $\theta((aK)(bK)) = \theta(aK)\theta(bK)$ where a and b are in G.
(2) Show that the kernel of θ is K. [Hint: Recall $\theta(aK) = f(a) = 1$. Then where must a be? Now use Q15.]
(3) What is the image of θ? It follows that θ is a bijection and a homomorphism between G/K and H, so the result follows.