Math 581 Problem Set 9

1. Let m and n be relatively prime positive integers.
(a) Prove that $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ as RINGS. (Hint: First Isomorphism Theorem)

Proof: Define $\varphi\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ by $\varphi(x) = ([x]_m, [x]_n)$. It is clear this is a hormormophism. Let $([a]_m, [b]_n) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Since $\gcd(m, n) = 1$, there exists $s, t \in \mathbb{Z}$ so that $ms + nt = 1$. Multiply both sides by $a - b$ and set $x = a + (b - a)ms = b + (a - b)nt$. Then $\varphi(x) = ([a]_m, [b]_n)$ and so φ is surjective. It is clear that $mn\mathbb{Z} \subset \ker \varphi$. If $a \in \ker \varphi$, then $[a]_m = [0]_m$ and $[a]_n = [0]_n$, i.e., $m|a$ and $n|a$. Thus, $mn|a$ and so $a \in mn\mathbb{Z}$. Thus, using the first isomorphism theorem we have the result. ■

(b) Show by example that part (a) may be false if m and n are not assumed to be relatively prime.

Let $m = n = 2$. Observe that $\mathbb{Z}/4\mathbb{Z}$ is a cyclic group of order 4 where $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ has no elements of order 4.

(c) Prove that if one has rings R and S and $R \cong S$ as rings, then $R^\times \cong S^\times$ as groups under multiplication, i.e., the units in the rings are isomorphic as groups.

Proof: We already have a homomorphism between them since $R \cong S$ as rings, so we only need to show the map is a bijection. However, we showed last term that $u \in R$ is a unit if and only if $\varphi(u)$ is a unit. Thus, φ must be a bijection between $R^\times$ and $S^\times$ as well. ■

(d) Prove that if R and S are rings, then $(R \times S)^\times \cong R^\times \times S^\times$ as groups under multiplication.

Proof: This just boils down to writing down what each thing is. Note that

$$(R \times S)^\times = \{(a, b) \in R \times S : \text{there exists } (c, d) \in R \times S \text{ so that } (a, b)(c, d) = (1, 1)\}$$

and

$$R^\times \times S^\times = \{(a, b) \in R \times S : a \in R^\times, b \in S^\times\}.$$

From this the result follows. ■

(e) Use part (d) to conclude that $(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$.

Proof: Apply part (d) to conclude that

$$(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})^\times$$

and parts (a) and (c) to conclude

$$(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/mn\mathbb{Z})^\times.$$

Combining these we have the result. ■

(f) Now let $m = p$ and $n = q$ for some primes p and q. Prove that the order of the group $(\mathbb{Z}/pq\mathbb{Z})^\times$ is $(p-1)(q-1)$.

Proof: We know that $(\mathbb{Z}/p\mathbb{Z})^\times$ has $p-1$ elements for any prime p and that $|G \times H| = |G||H|$. Part (e) now gives the result. ■

(g) Prove that if $\gcd(a, pq) = 1$, then $a^{(p-1)(q-1)} \equiv 1 (\bmod\, pq)$.

Proof: Since $\gcd(a, pq) = 1$ we have that $a \in (\mathbb{Z}/pq\mathbb{Z})^\times$. Since this group has order $(p-1)(q-1)$, we get that $a^{(p-1)(q-1)} = e_G$. Translated into a congruence statement, this reads $a^{(p-1)(q-1)} \equiv 1(\bmod\, pq)$. ■

2. Let N be a subgroup of G such that $[G : N] = 2$. Prove that N is a normal subgroup of G.

Proof: Since $[G : N] = 2$ there are only two distinct cosets, either right or left. One of them will be eN (just choose e as the representative for whatever coset it is in) and label the other one gN. So in particular, $g \notin N$. Similarly, we have that the right cosets are Ne and Ng. We know that $G = eN \bigsqcup gN = Ne \bigsqcup Ng$. It is clear that $eN = Ne$ since they are both just N as sets. Thus, it must be that $gN = Ng$. Since all the left cosets are equal to the right cosets we have that N is normal in G. ■

3. Show that every element in $\mathbb{Q}/\mathbb{Z}$ has finite order. (Recall you showed last homework that there are infinitely many elements in $\mathbb{Q}/\mathbb{Z}$.)

Proof: Let $\frac{r}{s} + \mathbb{Z}$ be an element in $\mathbb{Q}/\mathbb{Z}$. Observe that if we add this element to itself s times we get $r + \mathbb{Z}$. However, $r \in \mathbb{Z}$ so we have $s(\frac{r}{s} + \mathbb{Z}) = 0 + \mathbb{Z}$.

Thus, every element of $\mathbb{Q}/\mathbb{Z}$ has finite order. ■

4. Let p be an odd prime.
(a) Show that $a^2 \equiv b^2 (\bmod p)$ if and only if $a \equiv b (\bmod p)$ or $a \equiv -b (\bmod p)$.

Proof: Observe that $a^2 - b^2 = (a-b)(a+b)$. Thus, if $a^2 \equiv b^2 (\bmod p)$ then we know $p|(a-b)(a+b)$. Since p is prime, $p|(a-b)$ or $p|(a+b)$, as claimed. ■

(b) Show that $\varphi : (\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ defined by $\varphi(a) = a^2$ is a group homomorphism whose image is a subgroup H of index 2. (Hint: Use part (a) to determine the kernel of φ and use the first isomorphism theorem.)

Proof: Let $a, b \in (\mathbb{Z}/p\mathbb{Z})^\times$. We have $\varphi(ab) = (ab)^2 = a^2 b^2 = \varphi(a)\varphi(b)$ where we have used that $(\mathbb{Z}/p\mathbb{Z})^\times$ is an abelian group. Thus, φ is a homomorphism. Let H be the image of φ. The first isomorphism theorem gives us that $(\mathbb{Z}/p\mathbb{Z})^\times / \ker\varphi \cong H$. Therefore, if we can calculate the order of $\ker\varphi$ we will be able to calculate the order of H and hence the index of H in $(\mathbb{Z}/p\mathbb{Z})^\times$. Suppose $a \in \ker\varphi$. Then we have $a^2 \equiv 1 (\bmod p)$. Using part (a) this shows that $a = 1$ or $a = p-1$. Thus, $|\ker\varphi| = 2$. Hence, $|H| = (p-1)/2$. Now we see that $[(\mathbb{Z}/p\mathbb{Z})^\times : H] = \frac{(p-1)}{\frac{(p-1)}{2}} = 2$ as claimed. ■

(c) Define $\psi : (\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}$ by

$$\psi(a) = \begin{cases} +1, & \text{if } a \text{ is a square in } \mathbb{Z}/p\mathbb{Z} \\ -1, & \text{otherwise.} \end{cases}$$

Prove that ψ is a group homomorphism. (Hint: Consider the quotient group $(\mathbb{Z}/p\mathbb{Z})^\times / H$.)

Proof: Note that $(\mathbb{Z}/p\mathbb{Z})^\times$ is an abelian group so all subgroups are normal. In particular, the H in part (b) is normal. Thus, $(\mathbb{Z}/p\mathbb{Z})^\times/H$ is a group of order 2. Any group of order 2 must necessarily be isomorphic to the group $\{\pm 1\}$. We proved in class that the natural map $G \to G/N$ given by $g \mapsto gN$ is a surjective homomorphism. Applying this to our situation, we need only show that ψ is this natural map. Recall that H consists of all of the squares. Therefore, $gH = H$ if and only if g is a square. Therefore, the map ψ is the correct map as it takes squares to the identity $1H$ and nonsquares to the nonidentity element $-1H$. Therefore, ψ is a homomorphism. ■

(d) Conclude that if neither a nor b is a square in $\mathbb{Z}/p\mathbb{Z}$, then their product ab is a square in $\mathbb{Z}/p\mathbb{Z}$. (We used this result last term when showing there was a polynomial that was irreducible but reducible modulo every prime p.)

Proof: Suppose neither a or b is a square in $\mathbb{Z}/p\mathbb{Z}$. In particular, this means neither can be 0 so they both lie in $(\mathbb{Z}/p\mathbb{Z})^\times$. Applying ψ to ab we obtain $\psi(ab) = \psi(a)\psi(b) = (-1)(-1) = 1$. Thus, ab must be a square. ■

5. If N is a normal subgroup of G and if every element of N and G/N has finite order, prove that every element of G has finite order.

Proof: Let $g \in G$. We wish to show that there exists $N \in \mathbb{N}$ so that $g^N = e_G$. Consider the coset gN. Since every element in G/N has finite order, there exists $n \in \mathbb{N}$ so that $g^n N = (gN)^n = eN$, i.e., $g^n \in N$. Now we use the fact that every element in N has finite order, so there exists $m \in \mathbb{N}$ so that $(g^n)^m = e_G$, i.e., $g^{mn} = e_G$. Thus g has finite order. ■

6. Let $G = \mathbb{R} \times \mathbb{R}$.
(a) Show that $N = \{(x, y) | x = -y\}$ is a normal subgroup of G.

Proof: Note that $(0, 0) \in N$ so N is not empty. Let (a, b) and (c, d) be in N. Observe that $(a, b)+(c, d) = (a+c, b+d)$ and $a+c = -b-d = -(b+d)$ since $a = -b$ and $c = -d$. So N is closed under addition. Note that $(-x, -y) \in N$ if (x, y) is in N since $x = -y$ is equivalent to $-x = -(-y)$. Thus N is a subgroup. To see it is normal, just observe that $\mathbb{R} \times \mathbb{R}$ is abelian so all subgroups are normal. ■

(b) Describe the quotient group G/N.

Observe first that the coset $(0, 0) + N = N$ is just the line $y = -x$. Let $(a, b) \in \mathbb{R} \times \mathbb{R}$. We wish to describe the coset $(a, b) + N$. If we think of this in terms of elements, we are just taking each point on the line $y = -x$ and adding (a, b) to it. Geometrically, this amounts to shifting the line to the line $y = a+b-x$. Therefore, the group G/N consists of lines with slope -1.

7. Prove that $\mathbb{R}^\times/\langle -1, 1\rangle \cong \mathbb{R}_{>0}$ where $\mathbb{R}_{>0}$ is the group of positive real numbers.

Proof: Observe that $\mathbb{R}^\times$ and $\mathbb{R}_{>0}$ are both groups under multiplication with identity $e = 1$. Define $\varphi : \mathbb{R}^\times \to \mathbb{R}_{>0}$ by $\varphi(x) = |x|$. It is clear that this is a homomorphism as $\varphi(xy) = |xy| = |x||y| = \varphi(x)\varphi(y)$. To see it is surjective, let $x \in \mathbb{R}_{>0}$. Then $|x| = x$ and so $\varphi(x) = x$. The first isomorphism theorem now gives that $\mathbb{R}^\times/\ker\varphi \cong \mathbb{R}_{>0}$. It is clear that $\{\pm 1\} \subset \ker\varphi$ since each has absolute value 1. Since these are the only real numbers with absolute value 1, we have the reverse containment as well. Thus, $\mathbb{R}^\times/\{\pm 1\} \cong \mathbb{R}_{>0}$. ■

8. Let G be the set of all matrices of the form

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

where $a, b, c \in \mathbb{Q}$.

(a) Show that G is a group under matrix multiplication.

Proof: Note that each matrix in this set has nonzero determinant, so is a subset of $\mathrm{GL}_2(\mathbb{R})$. Thus we need only show it is a subgroup to show it is in fact a group. First observe that the identity matrix is in G so G is nonempty. Let $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}$ be in G. Observe that

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+d & e+af+b \\ 0 & 1 & c+f \\ 0 & 0 & 1 \end{pmatrix} \in G$$

since $\mathbb{Q}$ is closed under addition and multiplication. Thus, G is closed under matrix multiplication. The inverse of $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$ is given by $\begin{pmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}$ which is clearly still in G. Thus, G is a subgroup of $\mathrm{GL}_2(\mathbb{R})$ and hence a group itself. ■

(b) Find the center $Z(G)$ of G and show it is isomorphic to $\mathbb{Q}$.

Proof: Recall the center of the group is the set of elements that commute with everything. Reversing the order of the multiplication above we get

$$\begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+d & b+dc+e \\ 0 & 1 & c+f \\ 0 & 0 & 1 \end{pmatrix}.$$

Therefore, for $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$ to be in $Z(G)$, we must have $a = c = 0$. Therefore,

$$Z(G) = \left\{ \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : b \in \mathbb{Q} \right\}.$$

Define a map $\varphi : Z(G) \to \mathbb{Q}$ by $\begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mapsto b$. It is not difficult to check this is an isomorphism. ■

(c) Show that $G/Z(G) \cong \mathbb{Q} \times \mathbb{Q}$.

Proof: Define $\varphi : G \to \mathbb{Q} \times \mathbb{Q}$ by $\varphi\left(\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}\right) = (a, c)$. Note that this map is clearly surjective. To see it is a homomorphism, observe that

$$\begin{aligned}
\varphi\left(\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}\right) &= \varphi\left(\begin{pmatrix} 1 & a+d & e+af+b \\ 0 & 1 & c+f \\ 0 & 0 & 1 \end{pmatrix}\right) \\
&= (a+d, c+f) \\
&= (a, c) + (d, f) \\
&= \varphi\left(\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}\right) + \varphi\left(\begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}\right).
\end{aligned}$$

It is not difficult to see that $\ker \varphi = Z(G)$, and so the first isomorphism theorem gives the result. ■