MATH 4010/6010 Exam 1 Solutions
C. McCrory, March 1, 2009

1. Define an isomorphism $\mathbb{Z}_{10}^\times \to \mathbb{Z}_4$, and check that it is an isomorphism.

The group $\mathbb{Z}_{10}^\times$ is the set of units of the commutative ring $\mathbb{Z}_{10}$ with group operation given by multiplication in this ring. So $\mathbb{Z}_{10}^\times = \{1, 3, 7, 9\}$, an abelian group with identity $e = 1$, and multiplication given by $3{\cdot}3 = 9$, $3{\cdot}7 = 1$, $3{\cdot}9 = 7$, $7{\cdot}7 = 9$, $7{\cdot}9 = 3$, $9{\cdot}9 = 1$. Thus the element 3 has order 4, and $\mathbb{Z}_{10}^\times = \langle 3\rangle$, the cyclic group generated by 3, and so $3^m = 3^n$ if and only if $m \equiv n \pmod 4$. If we define $\phi : \mathbb{Z}_{10}^\times \to \mathbb{Z}_4$ by $\phi(3^n) = n \pmod 4$, then ϕ is a bijection, and $\phi(3^m 3^n) = \phi(3^{m+n}) = m + n \pmod 4 = (m \pmod 4) + (n \pmod 4) = \phi(3^m) + \phi(3^n)$, and so ϕ is a homomorphism. Therefore ϕ is an isomorphism.

(An alternate proof is to check directly that the bijection $\phi : \mathbb{Z}_{10}^\times \to \mathbb{Z}_4$, $\phi(1) = 0$, $\phi(3) = 1$, $\phi(7) = 3$, $\phi(9) = 2$ is a homomorphism.)

2. Let G be a group, and let $a \in G$. Define a function $\phi : G \to G$ by

$$\phi(g) = aga^{-1}.$$

Prove that ϕ is an isomorphism.

First we show that ϕ is a homomorphism:

$$\phi(g)\phi(h) = (aga^{-1})(aha^{-1}) = (ag)(a^{-1}a)(ha^{-1}) = (ag)e(ha^{-1}) = a(gh)a^{-1} = \phi(gh).$$

Next we show ϕ is bijective by constructing an inverse. Let $\psi(g) = a^{-1}ga$. Then

$$\psi(\phi(g)) = a^{-1}(aga^{-1})a = (a^{-1}a)g(a^{-1}a) = ege = g,$$

$$\phi(\psi(g)) = a(a^{-1}ga)a^{-1} = (aa^{-1})g(aa^{-1}) = ege = g.$$

3. Let G be the group of matrices

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

in $GL(2, \mathbb{R})$ such that $c = 0$. Let H be the subgroup of G consisting of matrices M with $c = 0$ and $a = 1$. Prove that H is a normal subgroup of G, and that the quotient group G/H is isomorphic to $\mathbb{R}^\times$.

First we check that G is a group:

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\begin{pmatrix} s & t \\ 0 & v \end{pmatrix} = \begin{pmatrix} as & at + bv \\ 0 & dv \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}^{-1} = \frac{1}{ad}\begin{pmatrix} d & -b \\ 0 & a \end{pmatrix}$$

H is a subgroup:

$$\begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix}\begin{pmatrix} 1 & t \\ 0 & v \end{pmatrix} = \begin{pmatrix} 1 & t+bv \\ 0 & dv \end{pmatrix}$$

$$\begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -b/d \\ 0 & 1/d \end{pmatrix}$$

Now define $\phi : G \to \mathbb{R}^\times$ by

$$\phi\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = a$$

We have $a \in \mathbb{R}^\times = \mathbb{R} \setminus \{0\}$ since

$$\det\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = ad \neq 0.$$

The function ϕ is a homomorphism:

$$\phi\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\begin{pmatrix} s & t \\ 0 & v \end{pmatrix}\right) = \phi\begin{pmatrix} as & at+bv \\ 0 & dv \end{pmatrix} = as = \phi\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\phi\begin{pmatrix} s & t \\ 0 & v \end{pmatrix}$$

The homomorphism ϕ is surjective, for if $a \in \mathbb{R}^\times$, then

$$a = \phi\begin{pmatrix} a & 1 \\ 0 & 1 \end{pmatrix}$$

By the definition of ϕ we have $\ker\phi = H$, so H is a normal subgroup of G. By the Fundamental Homomorphism Theorem, G/H is isomorphic to $\mathbb{R}^\times$.

4. How many elements of the symmetric group S_5 are conjugate to the element $(1\,2\,3)$? Explain your reasoning.

Two permutations $\sigma, \tau \in S_n$ are conjugate if and only if they have the same cycle type. So $\sigma \in S_5$ is conjugate to $(1\,2\,3)$ if and only if σ is a cycle of length 3. The number of symbols $(a\,b\,c)$ with $a, b, c \in \{1, 2, 3, 4, 5\}$ is $5 \cdot 4 \cdot 3 = 60$. But there are three symbols $(a\,b\,c)$, $(b\,c\,a)$, $(c\,a\,b)$ representing each cycle of length three, so the number of permutations σ conjugate to $(1\,2\,3)$ is $60/3 = 20$.

5. Prove: Let p be a prime and let m be a positive integer. If a group of order p^m acts on a set with n elements, and p does not divide n, then the action has a fixed point.

We prove this statement by contradiction. Suppose the group G of order p^m acts without fixed points on the set S, and p does not divide $n = \#(S)$. For each element $s \in S$ we have $|G| = \#(\mathcal{O}_s)|G_s|$, where $\mathcal{O}_s$ is the orbit of s and G_s is the stabilizer of s. Thus $\#(\mathcal{O}_s)$ divides $|G| = p^m$ for all $s \in S$. The divisors of p^m are $1, p, p^2, \ldots, p^m$. The element s is a fixed point of the action if and only if $\#(\mathcal{O}_s) = 1$. Since we have assumed there are no fixed points, we conclude that $\#(\mathcal{O}_s) \in \{p, p^2, \ldots, p^m\}$, and so p divides $\#(\mathcal{O}_s)$ for all $s \in S$. But S is the disjoint union of the orbits, so $n = \#(S)$ is a sum of integers that are divisible by p. Therefore p divides n, which is a contradiction.