MATH 207: Homework #9

Jesse Farmer

01 December 2003

1. *Find* $Aut D_{2n}$ *and* $Aut S_n$.

   Let $\varphi : D_{2n} \to D_{2n}$ be an automorphism. We automatically have, then, $\varphi(I) = I$ and for any $x \in D_{2n}, \varphi(x^{-1}) = \varphi(x)^{-1}$. Moreover, we see that if the order of an element x is n then the order of $\varphi(x)$ is also n.

   First we consider only the subgroup of rotations, specifically $\varphi(r)$. An element is a generator of this subgroup if and only if it has order n, but an automorphism preserves order. Therefore an automorphism must send r to another generator. Trivially, if an element r^k is a generator then the properties of an automorphism are preserved. Therefore any automorphism of D_{2n} sends r to some generator of the rotational subgroup.

   We now consider f, the flip element. As each flip is of order two, sending f to any of $f, \ldots, fr^{n-1}$. As it is impossible to have more automorphisms here, these are all the automorphisms.

   As for the symmetric group, I haven't the slightest.

2. *Find* $Aut\mathbb{Q}(\sqrt{2})$.

   Let $\varphi : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ be an automorphism and $a, b \in \mathbb{Q}$. If $x_0 \in \mathbb{Q}$ we know that $\varphi(x_0) = x_0$, so, for any $a + b\sqrt{2} = y_0 \in \mathbb{Q}(\sqrt{2})$ we have $\varphi(y_0) = a + b\varphi(\sqrt{2})$

   Notice that $2 = \varphi(2) = \varphi(\sqrt{2}\sqrt{2}) = \varphi(\sqrt{2})\varphi(\sqrt{2}) = \varphi(\sqrt{2})^2$. Thus $\varphi(\sqrt{2}) = \pm\sqrt{2}$ and the only two automorphisms on $\mathbb{Q}(\sqrt{2})$ are $\varphi(a + b\sqrt{2}) = a + b\sqrt{2}$ and $\varphi(a + b\sqrt{2}) = a - b\sqrt{2}$.

3. *Find* $Aut\mathbb{R}$.

   Any automorphism φ on $\mathbb{R}$ must fix $\mathbb{Q}$. Consider $a \in \mathbb{R}, a > 0$. Then there exists a $b \in \mathbb{R}$ such that $b^2 = a$ and $\varphi(a) = \varphi(b^2) = \varphi(b)^2 > 0$. Next, $a < b \Rightarrow \varphi(b - a) > 0 \Rightarrow \varphi(a) < \varphi(b)$.

   Let $y \in \mathbb{R}\backslash\mathbb{Q}$. Assume for contradiction that $y < \varphi(y)$. There exists $r \in \mathbb{Q}$ such that $y < r = \varphi(r) < \varphi(y)$. But then $\varphi(y) < \varphi(r)$ by the fact that φ is increasing, a contradiction.

Likewise, assume for contradiction that $\varphi(y) < y$. There exists $r \in \mathbb{Q}$ such that $\varphi(y) < \varphi(r) = r < y$. But then $\varphi(r) < \varphi(y)$ by the fact that φ is increasing, a contradiction.

Therefore $\varphi(x) = x$ for all $x \in \mathbb{R}$.

4. *Given $r \in \mathbb{Q}$ and $|r|_p = 1$ find $k \in \mathbb{Z}$ such that $|r - k|_p \leq \frac{1}{p^m}$ for $m \in \mathbb{N}$.*

   Let $r = \frac{a}{b}$. We need to find $k \in \mathbb{Z}$ such that $|\frac{a}{b} - k|_p \leq \frac{1}{p^m}$. We know that $p \not| b$, so $|b|_p = 1$. Hence we need to find k such that $|\frac{a}{b} - k|_p = |\frac{a-bk}{b}|_p = \frac{|a-bk|_p}{|b|_p} = |a - bk|_p \leq \frac{1}{p^m}$ for any $m \in \mathbb{N}$.

   First consider $a \cong kb(\text{mod p})$. For $k = 0, \ldots, p-1$ we see this forms a reduced residue system, and thus that there exists a k which satisfies the above congruence. For each $n = 0, \ldots, m-1$ we then have m solutions. Iterating this for each n, that is, for each $a \cong kb(\text{mod p}^n)$, we arrive at a reduced residue system with one less solution than the previous. Therefore, there is one integer such that $|a - bk|_p \leq \frac{1}{p^m}$ which we find by repeating this process.

5. *Find a sequence in $\mathbb{Q}$ which is Cauchy but does not converge under the p-adic norm.*

   Choose $a_n = \sum_{k=1}^{n} p^k$. Assuming $n > m$ without a loss of generality, we have $|a_n - a_m|_p = \frac{1}{p^{n+1}}$, so (a_n) is Cauchy. Assume (a_n) converges, then for every $\epsilon > 0$ there exists $N \in \mathbb{N}$ such that $n \geq N \Rightarrow |a_n - L|_p < \epsilon$. If $p \not| L$ then $|a_n - L|_p = 1$ for all n and we are done, so assume $p|L$ and write L in base-p. Even if L is rational we can do this, since the numerator and denominator are integers and they can certainly be written in base-p. Moreover, we can split apart the sum of the denominator to get a sum of rational numbers times a prime power. $|a_n - \sum_{k=1}^{m} b_k p^k|_p = |\sum_{k=1}^{n} c_k p^k|_p = max_{1 \leq k \leq n}\{|c_k p^k|_p\} > 0$. Therefore we can pick an $\epsilon > 0$ (anything smaller than this number) for which any N will fail, i.e., this sequence does not converge.

6. *Let $V \subset X'$ be an open set. Show that $f : X \to X'$ is continuous if $f^{-1}(V)$ is open.*

   Let $x_0 \in X$ be arbitrary and $\epsilon > 0$ be fixed. $B_\epsilon(f(x_o))$ is open, so $f^{-1}(B_\epsilon(f(x_o))$ is also open by hypothesis. Since $f(x_0) \in B_\epsilon(f(x_0))$ we have that $x_0 \in f^{-1}(B_\epsilon(f(x_o))$, and hence that there exists $\delta > 0$ such that $B_\delta(x_0) \subset f^{-1}(B_\epsilon(f(x_o))$.

   If $\rho(x, x_0) < \delta$ then $x \in B_\delta(x_0)$ and, moreover, $x \in f^{-1}(B_\epsilon(f(x_o))$. Therefore, $f(x) \in B_\epsilon(f(x_o))$, or, $\rho(f(x), f(x_0)) < \epsilon$. That is, f is continuous.

7. *Let $V \subset X'$ be a closed set. Show that $f : X \to X'$ is continuous if $f^{-1}(V)$ is closed.*

   Let $f^{-1}(V)$ be closed.

   Claim: $f^{-1}(V^c) = f^{-1}(V)^c$

   Proof:
   $$\begin{aligned} x \in f^{-1}(V^c) &\Leftrightarrow f(x) \in V^c \\ &\Leftrightarrow f(x) \notin V \\ &\Leftrightarrow x \notin f^{-1}(V) \\ &\Leftrightarrow x \in f^{-1}(V)^c \end{aligned}$$

   Then $f^{-1}(V)^c = f^{-1}(V^c)$ is open. By the previous problem, this correspondence between open sets and their preimage impluies f is continuous.

8. (a) *Show that the set of all homeomorphisms between a set and itself is a group under composition.*

We know that the set of all bijections from a set to itself forms a group under composition, so all we must show is that composition preserves continuity. We will denote the set of all homeomorphisms from X to itself as $\mathbb{H}$.

Let $f, g \in \mathbb{H}$. f is continuous at every point in X, so it is certainly continuous at $g(a)$. Then, there exists a $\delta_1 > 0$ such that for all $y \in X, \rho(y, g(a)) < \delta_1 \Rightarrow \rho(f(y), f(g(a))) < \epsilon$ for all $\epsilon > 0$. In particular, $y = g(x)$. Moreover, for some $delta > 0$ we have $\rho(x, a) < \delta \Rightarrow \rho(g(x), g(a)) < \epsilon$ for all $\epsilon > 0$.

That is, for all $\epsilon > 0$ there exists $\delta > 0$ such that $\rho(x, a) < \delta \Rightarrow \rho(g(x), g(a)) < \delta_1 \Rightarrow \rho(f(g(x)), f(g(a))) < \epsilon$.

As we already have that the inverses are continuous, we now have that their composition is, too. Therefore composition preserves continuity and the set of all homeomorphisms from a set to itself forms a group under composition.

(b) *Show that the set of all isometries between a set and itself is a group under composition.*

Let f, g be isometries. Since g is a bijection from a set to itself, we have that there exist x, y for any a, b such that $g(x) = a$ and $g(y) = b$. Then $\rho((f \circ g)(x), (f \circ g)(y)) = \rho(f(a), f(b)) = \rho(g(x), g(y)) = \rho(x, y)$. Therefore the composition of isometries is also an isometry, and, as above, we inherit all the other properties of the group of bijections from a set to itself.