MATH 257: Homework #2

Jesse Farmer

13 October 2004

1. *Prove that for all $n > 1$ that $\mathbb{Z}/n\mathbb{Z}$ is not a group under multiplication.*

   $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ is a ring with $1 \neq 0$ if $n > 1$, so for all $a \in \mathbb{Z}/n\mathbb{Z}$,

   $$0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a \Rightarrow 0 \cdot a = 0$$

   Hence there cannot exist a multiplicative inverse for 0, and therefore $(\mathbb{Z}/n\mathbb{Z}, \cdot)$ is never a group if $n > 1$.

2. *If a, b are commuting elements of a group G, prove that $(ab)^n = a^n b^n$ for all $n \in \mathbb{Z}$.*

   This is obviously true for $n = 1$, so assume it is true for $n = k \in \mathbb{N}$, then

   $$(ab)^{k+1} = (ab)^k (ab) = a^k b^k ab = a^k ab^k b = a^{k+1} b^{k+1}$$

   To show this for all $k \in \mathbb{Z}$, consider $(ab)^{-n}$. If a and b are commuting elements then $a^{-1}b^{-1} = (ba)^{-1} = (ab)^{-1} = b^{-1}a^{-1}$, so a^{-1}, b^{-1} are also commuting elements. Therefore $(ab)^{-1} = a^{-1}b^{-1}$. Assume the statement is true for $n = k$, then

   $$(ab)^{-(k+1)} = (ab)^{-k}(ab)^{-1} = a^{-k}b^{-k}a^{-1}b^{-1} = a^{-k}a^{-1}b^{-k}b^{-1} = a^{-(k+1)}b^{-(k+1)}$$

   Therefore if a, b are commuting elements then $(ab)^n = a^n b^n$ for all $n \in \mathbb{Z}$.

3. *Prove that if $x^2 = 1$ for all $x \in G$ then G is an Abelian group.*

   If $x^2 = 1$ for all $x \in G$ then $x = x^{-1}$ for all $x \in G$. Let $x, y \in G$ be arbitrary, then

   $$xy = (xy)^{-1} = y^{-1}x^{-1} = yx$$

4. *Show that an element has order 2 in S_n if and only if its cycle decomposition is a product of commuting 2-cycles.*

   This problem is a special case of the next problem where $p = 2$.

5. *Let p be a prime. Show that an element has order p in S_n if and only if its cycle decomposition is a product of commuting p-cycles. Show that this need not be the case if p is not prime.*

   It is important in this problem to note that if a cycle has length one it is omitted from the "cycle" decomposition. Therefore there is never a case where the length of a "cycle" is 1.

If $\pi \in S_n$ is the product of commuting p-cycles then obviously the order of p, the least common multiple of the lengths of the cycles, is p. Let $c_1, c_2, \dots, c_k$ be the cycles into which π is decomposed, $l_1, l_2, \dots, l_k$ their respective lengths, and assume π has an order of p. Then

$$p = \operatorname{lcm}(l_1, \dots, l_k) = \min\{d : l_i \mid d, i = 1, 2, \dots, k\}$$

Since each $l_i \mid p$, $l_i = 1$ or $l_i = p$. As was stated before the case where $l_i = 1$ is ruled out by our notation, and therefore $l_i = p$.

To show that p must be prime, take $p = 6$. Then there are permutations of order 6 in S_5 (e.g., $(123)(45)$) even though it is impossible to create a single cycle of order 6.

6. *If $\varphi : G \to H$ is a group isomorphism show that $|\varphi(x)| = |x|$ for all $x \in G$. Deduce that any two isomorphic groups have the same number of elements of order n for each $n \in \mathbb{N}$. Is this true if φ is only assumed to be a homomorphism?*

   Inductively it is clear that $\varphi(x^n) = \varphi(x)^n$ for $n \in \mathbb{Z}$. Let $|x| = n$ and $|\varphi(x)| = j$, $n, j > 0$. Then

   $$\varphi(x^j) = \varphi(x)^j = 1 = \varphi(1) = \varphi(x^n)$$

   By the injectivity of φ, $x^j = x^n$, which implies $x^{n-j} = 1$. Since neither n nor j is 0, and by hypothesis n is the smallest non-zero number such that $x^n = 1$, it must be the case that $n - j = 0$, i.e., $n = j$.

   Define $G_n = \{x \in G \mid |x| = n\}$ and H_n similarly. $\varphi(G_n) = H_n$ since, for every element $h \in H_n$ there exists an element $g \in G$ such that $\varphi(g) = h$. However, from above, $|g| = |h| = n$, and therefore $g \in G_n$. For the same reason, every element of G_n is sent to an element of H_n. Since φ is also injective it follows that $\varphi|_{G_n} : G_n \to H_n$ is a bijection, and hence G_n and H_n have the same cardinality.

   This need not be the case if φ is only assumed to be a homomorphism. The map $\varphi(x) = e_H$ is a non-bijective homomorphism, and $|\varphi(x)| \neq |x|$ for all $x \in G$ unless G is the trivial group.

7. *Prove that $(\mathbb{R}^\times, \cdot) \not\cong (\mathbb{C}^\times, \cdot)$.*

   Assume for contradiction that $\varphi : (\mathbb{C}^\times, \cdot) \to (\mathbb{R}^\times, \cdot)$ is a group isomorphism. There exists a $k \in \mathbb{R}^\times$ such that $\varphi(i) = k$. However,

   $$1 = \varphi(1) = \varphi(i^4) = k^4$$

   and therefore $\varphi(i) = -1$ since φ is a bijection and $\varphi(1) = 1$. Then

   $$-1 = \varphi(-1) = \varphi(i^2) = (-1)^2 = 1$$

   This is a contradiction, and therefore no such φ can exist.

8. *Prove that $(\mathbb{Z}, +) \not\cong (\mathbb{Q}, +)$.*

   Let $\varphi : \mathbb{Z} \to \mathbb{Q}$ be a group isomorphism. Then, since every element of $\mathbb{Z}$ is generated by 1, we can write $n = \epsilon_1 + \epsilon_2 + \cdots + \epsilon_k$ where $\epsilon_i = \pm 1$. Then $\varphi(n) = \sum_{i=1}^k \varphi(\epsilon_i) = \sum_{i=1}^k \pm\varphi(1)$, i.e., every element of the image set must be generated by $\varphi(1)$. This is clearly not the case ($(\mathbb{Q}, +)$ is not cyclic – indeed, it is not even finitely generated), and so no such isomorphism can exist.

   To show that that $(\mathbb{Q}, +)$ is not cyclic, assume it is generated by some element $\frac{p}{q} \in \mathbb{Q}$. Then $\left\langle \frac{p}{q} \right\rangle = \{k\frac{p}{q} \mid k \in \mathbb{Z}\}$. Clearly $\frac{p'}{q} \in \mathbb{Q}$ is not in this set, where p' is an integer which is not divided by p.

9. *For the following show that the specified subset is not a subgroup of the given group:*

   (a) *The set of 2-cycles of S_n for $n \geq 3$.*
   The identity is a 1-cycle and therefore not contained in this set.

   (b) *The set of reflections in D_{2n} for $n \geq 3$.*
   The identity is not a reflection.

   (c) *For $n > 1$ a composite integer and G a group with an element of order n, the set $H = \{x \in G \mid |x| = n\} \cup \{1\}$.*
   Write $n = ab$ for $a, b \neq 1$. Assume H is a subgroup of G, then since $x \in H$ by hypothesis, $x^a \in H$. However, $(x^a)^b = x^{ab} = 1$, and $b < n$, so the order of x^a is less than n, a contradiction. Therefore H cannot be a subgroup of G.

   (d) *The set of odd integers and 0 in $\mathbb{Z}$.*
   The set is not closed under addition since the sum of two odd integers is never odd.

   (e) *The set of real numbers whose square is a rational number (under addition).*
   Let p, q be primes with $p \neq q$. Assume for contradiction that $\sqrt{pq} \in \mathbb{Q}$, i.e., there exist m, n with $(m, n) = 1$ such that $\sqrt{pq} = \frac{m}{n}$. Then $n^2 pq = m^2$ and $p \mid m$, so write $m = pk$ for some $k \in \mathbb{Z}$. This yields $n^2 pq = p^2 k^2 \Rightarrow n^2 q = k^2 p$. Since $p \nmid q$, this also implies $p \mid n$, i.e., $(m, n) \geq p$, a contradiction. Therefore $\sqrt{pq} \notin \mathbb{Q}$ for p, q prime and $p \neq q$.

   Let p, q be primes as above. Then certainly $\left(\sqrt{p}\right)^2$ and $\left(\sqrt{q}\right)^2$ are rational. However

   $$(\sqrt{p} + \sqrt{q})^2 = p + 2\sqrt{pq} + q$$

   This is rational only if $\sqrt{pq} \in \mathbb{Q}$, which as was shown above is never the case. Hence this set is not closed under addition.

10. *Prove that G cannot have a subgroup H with $|H| = |G| - 1$, and $|G| > 2$.*

    If $|H| = |G| - 1$ then there must be one and only one element contained in G that is not contained in H. Call this element g. Take $x, y \in H$, $x \neq 1$, and write $y = x^{-1}g \neq g$. Then $xy = g \notin H$, so H is not closed under the group operation and therefore cannot be a subgroup of G.

11. *Let $H_1 \leq H_2 \leq \cdots$ be an ascending chain of subgroups of G. Prove that $\bigcup_{i=1}^{\infty} H_i$ is a subgroup of G.*

    Let $h \in \bigcup_{i=1}^{\infty} H_i$. Then there exists a $k \in \mathbb{N}$ such that $h \in H_k$. Since H_k is by hypothesis a group, $k^{-1} \in H_k \subset \bigcup_{i=1}^{\infty} H_i$.

    Similarly, let $h_1, h_2 \in \bigcup_{i=1}^{\infty} H_i$. Then there exist i, j such that $H_i \subset H_j$ and $h_1 \in H_i$, $h_2 \in H_j$. Since this implies $h_2 \in H_j$ then, since H_j is by hypothesis a group, $h_1 h_2 \in H_j \subset \bigcup_{i=1}^{\infty} H_i$. Therefore $\bigcup_{i=1}^{\infty} H_i$ is a group.

12. *Let G be a group and for fixed $g \in G$ define a map from G to G*

    $$\varphi_g(h) = ghg^{-1}$$

    (a) *Prove that φ_g is an isomorphism of G.*
    Let $\varphi_g^{-1}(h) = g^{-1}hg$, then

    $$\varphi_g(\varphi_g^{-1}(h)) = g(g^{-1}hg)g^{-1} = (gg^{-1})h(gg^{-1}) = h$$

and

$$\varphi_g^{-1}(\varphi_g(h)) = g^{-1}(ghg^{-1})g = (g^{-1}g)h(g^{-1}g) = h$$

Therefore φ_g is a bijection. Moreover, let $h_1, h_2 \in G$,

$$\varphi_g(h_1h_2) = g(h_1h_2)g^{-1} = (gh_1)g^{-1}g(h_2g^{-1}) = (gh_1g^{-1})(gh_2g^{-1}) = \varphi_g(h_1)\varphi_g(h_2)$$

so φ_g is a homomorphism.

(b) *Prove that $\psi : G \to Aut(G)$ defined by $\psi(g) = \varphi_g$ is a homomorphism.*
Let $h, g_1, g_2 \in G$, then

$$\varphi_{g_1g_2}(h) = (g_1g_2)h(g_1g_2)^{-1} = g_1(g_2hg_2^{-1})g_1^{-1} = g_1\varphi_{g_2}(h)g_1^{-1} = (\varphi_{g_1} \circ \varphi_{g_2})(h)$$

Therefore $\psi(g_1g_2) = \psi(g_1) \circ \psi(g_2)$, i.e., $\psi : (G, \cdot) \to (\mathrm{Aut}(G), \circ)$ is a group homomorphism.

13. *Let G be a group and H be a subgroup of G. Define*

$$X = \{gHg^{-1} \mid g \in G\}$$

(a) *Prove that $N_G(H) = \{g \in G \mid gHg^{-1} \subset H\}$ is a subgroup of G.*
First, $N_G(H) \neq \emptyset$ since $1 \in N_G(H)$. Let $g \in N_G(H)$. For every $h \in H$ there exists an $h' \in H$ such that $ghg^{-1} = h'$. Hence, $g^{-1}h'g = h \in H$, i.e., $g^{-1} \in N_G(H)$. Similarly, let $g_1, g_2 \in N_G(H)$. Then for every $h \in H$ there exist h', h'' such that $g_1hg_1^{-1} = h'$ and $g_2gg_2^{-1} = h''$, hence

$$g_1g_2hg_2^{-1}g_1^{-1} = g_1h'g_1^{-1} = h'' \in H$$

Therefore $N_G(H)$ is a subgroup of G.

(b) *Prove that the map $\pi : G \to Sym(X)$ defined by $\pi(g) = \phi_g$, where $\phi_g(H') = gH'g^{-1}$ for $H' \in X$, is a homomorphism.*
Let $h, g_1, g_2 \in G$ be arbitrary, then

$$\phi_{g_1g_2}(H') = g_1g_2H'g_2^{-1}g_1^{-1} = g_1(g_2H'g_2^{-1})g_1^{-1} = g_1\phi_{g_2}(H')g_1^{-1} = (\phi_{g_1} \circ \phi_{g_2})(H')$$

and therefore $\pi(g_1g_2) = \pi(g_1) \circ \pi(g_2)$, i.e., $\pi : (G, \cdot) \to (\mathrm{Sym(X)}, \circ)$ is a group homomorphism.

14. *Let G be a group and $g \in G$. Prove that if $|g| < \infty$ then $g^i = g^j$ if and only if $i \equiv j \pmod{|g|}$, and that if $|g| = \infty$ then $g^i = g^j$ if and only if $i = j$.*

In general, since $|g|$ is the smallest integer n such that $g^n = e$ it follows that if $g^k = 1$ then $|g| \mid k$, i.e., k must be some multiple of the order of g. Assume g is of finite order, then $g^i = g^j$ if and only if $g^{i-j} = e$, which is true if and only if $|g| \mid (i - j)$, i.e., $i \equiv j \pmod{|g|}$.

If g is of infinite order then there exists no non-zero integer n such that $g^n = e$, so $g^{i-j} = e$ if and only if $i - j = 0$, i.e., $i = j$.