Math 113 — Problem Set 4 — William Guss

(P28. 37) *Suppose that * is an associative and commutative binary operation on a set S. Show that $H = \{a \in S \mid a * a = a\}$ is closed under *.*

Proof. We need show for every $(a, b) \in H \times H$, $a*b \in H$. Clearly $a*b \in S$, we claim that $(a*b)*(a*b) \in H$. Essentially $(a*b)*(a*b) = (a*b)*(b*a)$ by commutativity. Then $(a*b)*(b*a) = a*(b*b)*a = a*b*a$ by associativity and idempotents of b. Finally $a * b * a = b * a * a = b * (a * a) = b * a = a * b$ by commutativity, associativity, and commutativity again. Therefore $a * b$ is idemopotent and in H, so H is closed under $*$. ☐

(P34. 4) *Determine whether or not ϕ is an isomorphism between $\langle \mathbb{Z}, + \rangle$ and $\langle \mathbb{Z}, + \rangle$ when $\phi(n) = n + 1, n \in \mathbb{Z}$.*
Claim. The mapping is not an isomorphism.

Proof. We will show that despite the bijection of ϕ, it is not a homomorphism. We first show that $\phi : \mathbb{Z} \to \mathbb{Z}$ is bijective. Clearly for ever $n \in \mathbb{Z}$, $\phi^{pre}(n) = n + (-1) \in \mathbb{Z}$ so the map is surjective. Next, the map is injective since every successor of an integer is unique by Piano's axioms. Hence ϕ is a bijection. But consider $\phi(n + m) = (n + m) + 1 = (n + 1) + m \neq (n + 1) + (m + 1) = \phi(n) + \phi(m)$, therefore the mapping is not a homomorphism. This completes the proof of the claim. ☐

(P34. 6) *Determine whether or not ϕ is an isomorphism between $\langle \mathbb{Q}, \cdot \rangle$ and $\langle \mathbb{Q}, \cdot \rangle$ when $\phi(x) = x^2$ for $x \in \mathbb{Q}$.*
Claim. The mapping is not an isomorphism.

Proof. We need only show that ϕ is not a bijection. If ϕ is an isomorphism then it is in an invertible mapping. Therefore take $\phi^{-1}(2) = \sqrt{2} \notin \mathbb{Q}$. This is a contradiction to the surjection of the inverse, therefore ϕ is not an isomorphism. ☐

(P28. 7) *Determine whether or not ϕ is an isomorphism between $\langle \mathbb{R}, \cdot \rangle$ and $\langle \mathbb{R}, \cdot \rangle$ where $\phi(x) = x^3$.*
Claim. The mapping *is* an isomorphism.

Proof. We first show the bijection. Clearly if $y \neq x$ then without loss of generality $y > x$ and $\phi(y) > \phi(x)$ by the monotonicity of x^3, (to see this, observe that the mapping preserves sign and if $(y - x) > 0$ then $(y - x)^3 > 0$), so the mapping is injective. For surjection, take $a \in \mathbb{R}$ and observe that $a^{1/3} \in \mathbb{R}$, by the completeness of $\mathbb{R}$ (take the sequence $x_1 = a$, $x_n = \frac{1}{n}\left[(n-1)x_{n-1} + \frac{a}{x_{n-1}^3}\right]$, and see its cauchyness, then reverse Newton's method to see that the 3rd power exponentiation of the limit tends to a.) So the mapping is bijective.

Now $\phi(ab) = (ab)^3 = a^3b^3 = \phi(a)\phi(b)$ and the mapping is a homormorphism by the distributive power law.

This completes the proof. ☐

(P45. 9) *Show that the group $\langle U, \cdot \rangle$ is not isomorphic to either $\langle \mathbb{R}, + \rangle$ and $\langle \mathbb{R}, \cdot \rangle$.*

Proof. Since all sets have the same cardinality, it must only be that $\langle U, \cdot \rangle$ does not share structural properties with either of the real groups. It suffices to show that $\langle U, \cdot \rangle \not\simeq \langle \mathbb{R}, \cdot \rangle$, since $\langle \mathbb{R}, \cdot \rangle \simeq \langle \mathbb{R}, + \rangle$ and isomorphisms form an equivalence relation on families of groups.

Structurally, take any $z \in U$ so that $\theta = Arg(z)$, then $\theta / 2\pi \in \mathbb{R}$ so $Arg(z^{n2\pi/\theta}) = n2\pi$ and so $z^{n2\pi/\theta} = 1$ for all $n \in \mathbb{N}$. It is not the case that for every $x \in \mathbb{R}$ there is are $a, r \in \mathbb{R}$ so that $x^{\phi(r)} = a$ where $\phi(r)$ is a set so that $p, q \in \phi(r) \implies p - q = nr \wedge p, q > 0$ for some $n \in \mathbb{Z}$. Take $x = 2, x^{r>0}$ increases monotonically :(. Since this cyclicity property is not common, there could not be a homormorphism, and so the groups are not isomorphic. □

(P46. 13) *Determine if the set S of $n \times n$ matrices with no zero diagonal enteries is a group under matrix multiplication.*
Claim. The set S is not a group.

Proof. Consider the multiplication following two elements in S,

$$\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

So the set is not even closed under multiplication. □

(P46. 17) *Determine if the set S of $n \times n$ upper triangular matrices with determinant 1 under matrix multiplication is a group.*
Claim. The set S is a group.

Proof. From linear algebra we know that a matrix is invertible if and only if it has determinant $D \neq 0$. Therefore every member of S is a full rank matrix. We now show that S is closed under matrix multiplication by the determinant laws from linear algebra. If $A, B \in S$ then $det(AB) = det(A)det(B) = 1$ so AB is invertible and thereby upper triangular. It follows that AB is closed under multiplication. From the chapter we know the set of invertible $n \times n$ matrices is the general linear group. Since invertibility if and only if determinant non-zero, it follows that S is a sub-group, inheriting associativity of multiplication from $GL(\mathbb{R}^n)$. □

(P49. 37) *Let G be a group and let $a, bc \in G$. Show that if $a * b * c = e$ then $b * c * a = e$.*

Proof. If $a * b * c = e$ then $a = c^{-1}b^{-1}$, $c = b^{-1}a^{-1}$ and $b = a^{-1} * c^{-1}$. Then $a * b * c * (c * b * a)^{-1} = a*b*c*a^{-1}*b^{-1}*c^{-1}$. Then by $a*b*c = e$ we have $a*b*c*a^{-1}*b^{-1}*c^{-1} = c^{-1}*b^{-1}*a^{-1}*a^{-1}*b^{-1}*c^{-1} = a*b*b^{-1}*a^{-1}*b^{-1}*c^{-1} = a*a^{-1}*b^{-1}*c^{-1} = a*b*c*b^{-1}*c^{-1} = b^{-1}*c^{-1}$ so $c*b*a^{-1} = b^{-1}*c^{-1} = a^{-1}*b^{-1}*c^{-1}$ so $a^{-1} = a$ without loss of generality, and $b*c*a = b*c*b*c = a^{-1}*b*c = a*b*c = e$. This completes the proof. □