Math 620: Groups HW

Due on Monday, October 5, 2015

Boynton 10:00

Kailee Gray

Exercise 3.1.2: For each binary operation $*$ defined on a set below, determine whether or not $*$ gives a group structure on the set. If it is not a group, say which axioms fail to hold. (a) Define $*$ on $\mathbb{Z}$ by $a * b = ab$.

(closure) Multiplication of integers is closed, so for any $a, b \in \mathbb{Z}$ implies $a * b \in \mathbb{Z}$.

(associativity) Multiplication of integers is associative, so for any $a, b, c \in \mathbb{Z}$, $a * (b * c) = a(bc) = (ab)c = (a * b) * c$.

(identity) For any $a \in \mathbb{Z}$, $a \cdot 1 = a = 1 \cdot a$, so $a * 1 = a \cdot 1 = a = 1 \cdot a = 1 * a$.

(inverses) Consider any $a \in \mathbb{Z}$. If $a^{-1} \in \mathbb{Z}$, then $a * a^{-1} = 1 = a^{-1} * a$. Equivalently, $a^{-1} = \frac{1}{a}$. If $a = 0$, a^{-1} does not exist. Also, $\frac{1}{a} \in \mathbb{Z}$ only if $a = \pm 1$. Thus, not all elements in $\mathbb{Z}$ have an inverse element in $\mathbb{Z}$ under $*$ so $(\mathbb{Z}, *)$ is not a group.

(b) Define $*$ on $\mathbb{Z}$ by $a * b = \max\{a, b\}$.

(closure) For any $a, b \in \mathbb{Z}$, The image of $*$ is either a or b so $*$ is closed in $\mathbb{Z}$.

(associativity) Consider $a, b, c \in \mathbb{Z}$. Then, $a * (b * c) = \max\{a, \max\{b, c\}\} = \max\{a, b, c\} = \max\{\max\{a, b\}, c\} = (a * b) * c$.

(identity) Suppose there exists some $e \in \mathbb{Z}$ such that $e * a = a * e = a$ for any $a \in \mathbb{Z}$. Then, $\max\{a, e\} = a = \max\{e, a\}$. Since $e, 1 \in \mathbb{Z}$, $e - 1 \in \mathbb{Z}$, so if e is the identity, $\max\{e, e - 1\} = e - 1$. However, $\max\{e, e - 1\} = e$. Because $(\mathbb{Z}, *)$ does not contain an identity element, it not a group.

(inverses) Because $(\mathbb{Z}, *)$ does not contain an identity element, we cannot determine inverses of the elements in $(\mathbb{Z}, *)$.

(c) Define $*$ on $\mathbb{Z}$ by $a * b = a - b$.

(closure) For any $a, b \in \mathbb{Z}$, $a - b \in \mathbb{Z}$, so $a * b \in \mathbb{Z}$.

(associativity) Notice $1, 2, -3 \in \mathbb{Z}$. Then, $1 * (2 * -3) = 1 - (2 - (-3)) = -4$. However, $(1 * 2) * -3 = (1 - 2) - (-3) = 2$. Thus, $*$ is not associative and so $(\mathbb{Z}, *)$ is not a group.

(identity) Suppose there exists some $e \in \mathbb{Z}$ such that $e * a = a * e = a$ for any $a \in \mathbb{Z}$. Then, $e - a = a = a - e$ which implies $e = 2a$ and $e = 0$. However, $e \neq 0$ since $0 - a = -a$ and

$e \neq 2a$ since $a - 2a = -a$. So there is no identity under $*$. Thus, $(\mathbb{Z}, *)$ does not contain an identity element and is therefore not a group.

(inverses) Because $(\mathbb{Z}, *)$ does not contain an identity element, we cannot determine inverses of the elements in $(\mathbb{Z}, *)$.

(d) Define $*$ on $\mathbb{Z}$ by $a * b = |ab|$.

(closure) For any $a, b \in \mathbb{Z}$, $ab \in \mathbb{Z}$ so $|ab| \in \mathbb{Z}$. Thus, $a * b \in \mathbb{Z}$ so $\mathbb{Z}$ is closed under $*$.

(associativity) Consider $a, b, c \in \mathbb{Z}$. Then, $a * (b * c) = |a|bc|| = |abc| = ||ab|c| = (a * b) * c$.

(identity) Notice if $(\mathbb{Z}, *)$ contains an identity element, e, then since $-2 \in \mathbb{Z}$, $-2 * e$ must equal -2 and $e * -2$ must equal -2. However, $-2 * e = |-2e| \geq 0$ and $e * -2 = |e(-2)| \geq 0$, so $-2 * e$ can not equal -2 and $e * -2$ can not equal -2. Thus, $(\mathbb{Z}, *)$ does not contain an identity element and is therefore not a group.

(inverses) Because $(\mathbb{Z}, *)$ does not contain an identity element, we cannot determine inverses of the elements in $(\mathbb{Z}, *)$.

(e) Define $*$ on $\mathbb{R}^+$ by $a * b = ab$.

(closure) For any $a, b \in \mathbb{R}^+$, $ab \in \mathbb{R}^+$ so $a * b \in \mathbb{R}^+$. Thus $\mathbb{R}^+$ is closed under $*$.

(associativity) Consider $a, b, c \in \mathbb{R}^+$. Then, by associativity of multiplication in $\mathbb{R}$, $a * (b * c) = a(bc) = (ab)c = (a * b) * c$.

(identity) For any $a \in \mathbb{R}^+$, $a \cdot 1 = a = 1 \cdot a$ so $a * 1 = a = 1 * a$. Thus, 1 is the identity element in $(\mathbb{R}^+, *)$.

(inverses) For any $a \in \mathbb{R}^+$, since $a \neq 0$, $\frac{1}{a} \in \mathbb{R}^+$ and $\frac{1}{a} \cdot a = 1 = a \cdot \frac{1}{a}$. Thus, $\frac{1}{a} * a = 1 = a * \frac{1}{a}$ so $\frac{1}{a}$ is the inverse of any element in $\mathbb{R}^+$.

Hence, $(\mathbb{R}^+, *)$ defines a group.

(f) Define $*$ on $\mathbb{Q}$ by $a * b = ab$.

(closure) For any $a, b \in \mathbb{Q}$, $a = \frac{m_1}{n_1}, b = \frac{m_2}{n_2}$ for $m_1, n_1, m_2, n_2 \in \mathbb{Z}$ with $n_1, n_2 \neq 0$. Then, $ab = \frac{m_1}{n_1}\frac{m_2}{n_2} = \frac{m_1 m_2}{n_1 n_2}$. Since $m_1 m_2, n_1 n_2 \in \mathbb{Z}$ and $n_1 n_2 \neq 0$, $ab \in \mathbb{Q}$ so $a * b \in \mathbb{Q}$. Thus $\mathbb{Q}$ is closed under $*$.

(associativity) Consider $a, b, c \in \mathbb{Q}$. Then, by associativity of multiplication in $\mathbb{R}$, $a*(b*c) = a(bc) = (ab)c = (a*b)*c$.

(identity) Since $1 \in \mathbb{Q}$ and because for any $a \in \mathbb{Q}$, $a \cdot 1 = a = 1 \cdot a$ so $a * 1 = a = 1 * a$. Thus, 1 is the identity element in $(\mathbb{Q}, *)$.

(inverses) Note $0 \in \mathbb{Q}$. Suppose 0 has an inverse in $\mathbb{Q}$, a^{-1}. Then, $a^{-1} * 0 = 1 = 0 * a^{-1}$. However, $a^{-1} \cdot 0 = 0 = 0 \cdot a^{-1}$. Thus, 0 does not have an inverse in $\mathbb{Q}$. Notice for any $a \in \mathbb{Q}$ with $a \neq 0$, if $a = \frac{m}{n}$, $a^{-1} = \frac{n}{m}$ since $a * a^{-1} = a \cdot a^{-1} = 1 = a^{-1} \cdot a = a^{-1} * a$. However since 0 does not have an inverse, $(\mathbb{Q}, *)$ is not a group.

Exercise 3.1.9: Let $G = \{x \in \mathbb{R} \mid x > 0$ and $x \neq 1\}$. Define the operation $*$ on G by $a * b = a^{\ln b}$ for all $a, b \in G$. Prove that G is an abelian group under $*$.

(closure) For any $a, b \in G$, $b > 0, b \neq 1$ so $\ln b \neq 0$ and $\ln b > 0$ so $a^{\ln b} > 0$ and $a^{\ln b} \neq 1$. Thus $a * b = a^{\ln b} \in G$.

(associativity) Consider $a, b, c \in G$. Then, $a*(b*c) = a*(b^{\ln c}) = a^{\ln(b^{\ln c})}$. By properties of ln, $a^{\ln(b^{\ln c})} = a^{\ln c \ln b}$. Also, $(a*b)*c = (a^{\ln b})*c = (a^{\ln b})^{\ln c}$. Then, $(a^{\ln b})^{\ln c} = a^{\ln b \ln c} = a^{\ln c \ln b}$. Thus, $a * (b * c) = (a * b) * c$.

(identity) The identity in $(G, *)$ is the mathematical constant e: for any $a \in G$, $a * e = a^{\ln e} = a^1 = a$ and $e * a = e^{\ln a} = a$.

(inverses)

Claim: the inverse of any element $a \in G$, $a^{-1} = e^{(\ln a)^{-1}}$.

Proof. Since $a \in G$, $a > 0$ and $a \neq 1$. Then, $\ln a \neq 0$ and $\ln a > 0$. Thus, $(\ln a)^{-1} \in \mathbb{R}$ and $(\ln a)^{-1} > 0$ and so $e^{(\ln a)^{-1}} > 0$ and $e^{(\ln a)^{-1}} \neq 1$. Hence, $e^{(\ln a)^{-1}} \in G$. Additionally,

$$e^{(\ln a)^{-1}} * a = (e^{(\ln a)^{-1}})^{\ln a} = e^{(\ln a)^{-1} \ln a} = e^1 = e.$$

$$a * e^{(\ln a)^{-1}} = a^{1^{(\ln a)^{-1}}} = a^{(\ln a)^{-1}}.$$

$a^{(\ln a)^{-1}} = x$ for some $x \in G$. Then, $\ln(a^{(\ln a)^{-1}}) = \ln x$ and $(\ln a)^{-1}(\ln a) = 1$ implies $\ln x = 1$. Thus, $x = e$. $\square$

(commutativity) Notice for any $a, b \in G$, $a * b = a^{\ln b}$. From closure of $*$ shown above, $a * b = a^{\ln b} = x$ for some $x \in G$. Then, $\ln a^{\ln b} = \ln x$ and $\ln a^{\ln b} = (\ln b) \ln a = \ln a (\ln b) = \ln b^{\ln a}$. Thus, $\ln b^{\ln a} = \ln x$ so $x = b^{\ln a} = b * a$. Therefore, for any $a, b \in G$, $a * b = b * a$. Hence by definition 3.1.9 in Beachy, G is abelian.

Exercise 3.1.10: Show that the set $A = \{f_{m,b} : \mathbb{R} \to \mathbb{R} \mid m \neq 0$ and $f_{m,b}(x) = mx + b\}$ of affine functions from $\mathbb{R}$ to $\mathbb{R}$ forms a group under composition of functions.

(closure) For any $f_{m_1,b_1}, g_{m_2,b_2} \in A$ with $m_1, m_2 \neq 0$, $f_{m_1,b_1}(x) = m_1x + b_1$ and $g_{m_2,b_2}(x) = m_2x + b_2$. Then $f_{m_1,b_1} \circ g_{m_2,b_2} = f_{m_1,b_1}(g_{m_2,b_2}) = m_1 g_{m_2,b_2} + b_1 = m_1(m_2x + b_2) + b_1 = m_1m_2x + m_1b_2 + b_1$. Since $m_1, m_2 \neq 0$, $m_1m_2 \neq 0$, so $f_{m_1,b_1} \circ g_{m_2,b_2} \in A$.

(associativity) Consider $f_{m_1,b_1}, g_{m_2,b_2}, k_{m_3,b_3} \in A$. Then, $f_{m_1,b_1} \circ (g_{m_2,b_2} \circ k_{m_3,b_3}) = f_{m_1,b_1} \circ (g_{m_2,b_2}(k_{m_3,b_3})) = f_{m_1,b_1}(m_2(m_3x + b_3) + b_2) = m_1(m_2(m_3x + b_3) + b_2) + b_1$. By associativity, distributivity, and commutativity of multiplication and addition in $\mathbb{R}$ we can write $m_1(m_2(m_3x+b_3)+b_2)+b_1 = m_1m_2(m_3x+b_3)+m_1b_2+b_1 = m_1m_2(k_{m_3,b_3})+m_1b_2+b_1$. From above we know $f_{m_1,b_1} \circ g_{m_2,b_2} = m_1m_2x + m_1b_2 + b_1$, so $m_1m_2(k_{m_3,b_3}) + m_1b_2 + b_1 = (f_{m_1,b_1} \circ g_{m_2,b_2}) \circ k_{m_3,b_3}$. Thus, $f_{m_1,b_1} \circ (g_{m_2,b_2} \circ k_{m_3,b_3}) = (f_{m_1,b_1} \circ g_{m_2,b_2}) \circ k_{m_3,b_3}$.

(identity) The identity in $(A, \circ)$ is the function $I(x) = x$:
for any $f_{m,b} \in A$, $f_{m,b} \circ I = f_{m,b}(I(x)) = f_{m,b}(x)$ and $I \circ f_{m,b} = I(f_{m,b}(x)) = f_{m,b}(x)$.

(inverses)

Claim: the inverse of any element $f_{m,b} \in A$, $f^{-1}(x) = \dfrac{1}{m}x - \dfrac{b}{m}$.

Proof. Since $f_{m,b} \in A$, $m \neq 0$ and $m, b \in \mathbb{R}$. Therefore, $\frac{1}{m}, \frac{b}{m} \in \mathbb{R}$ and $\frac{1}{m} \neq 0$. Hence $f^{-1}(x) = \frac{1}{m}x - \frac{b}{m} \in A$. Additionally,

$$f_{m,b} \circ f^{-1} = f_{m,b}\left(\frac{1}{m}x - \frac{b}{m}\right) = m\left(\frac{1}{m}x - \frac{b}{m}\right) + b = x - b + b = x = I(x).$$

$$f^{-1} \circ f_{m,b} = f^{-1}(f_{m,b}(x)) = f^{-1}(mx + b) = \left(\frac{1}{m}(mx + b) - \frac{b}{m}\right) = x + \frac{b}{m} - \frac{b}{m} = x = I(x).$$

Therefore $(A, \circ)$ is a group. ∎

Exercise 3.1.17: Let G be a group. For $a, b \in G$, prove that $(ab)^n = a^n b^n$ for all $n \in \mathbb{Z}$ if and only if $ab = ba$.

Proof. Let G be any group and let e be the identity element of the group G.

($\Rightarrow$) Assume $(ab)^n = a^n b^n$ for all $n \in \mathbb{Z}$ and any $a, b \in G$. So, this equality most hold $n = 2$. Then, $(ab)^2 = a^2 b^2$ and so $abab = aabb$. Since $a, b \in G$, there exists $a^{-1}, b^{-1} \in G$ such that $aa^{-1} = a^{-1}a = e$ and $bb^{-1} = b^{-1}b = e$. Thus, $(ab)(ab) = (aa)(bb)$ implies $a^{-1}(ab)(ab)b^{-1} = a^{-1}(aa)(bb)b^{-1}$. G is associative, so we can write $(a^{-1}a)ba(bb^{-1}) = (a^{-1}a)ab(bb^{-1})$. Thus, $ebae = eabe$ and so $(eb)(ae) = (ea)(be)$. Since $eb = b, ae = a, ea = a, be = b$ we have $ba = ab$ for any $a, b \in G$. Thus, G is abelian.

($\Leftarrow$) Assume for any $a, b \in G$, $ab = ba$. Thus, G is abelian. Suppose $n > 0$. First, consider $n = 2$, then G is an abelian group, so we apply the associative and commutative properties of G to obtain $(ab)^2 = (ab)^2 = (ab)(ab) = a(ba)b = a(ab)b = (aa)(bb) = a^2 b^2$. So the given statement is true for $n = 2$. Assume $(ab)^k = a^k b^k$ for $1 < k < n$. Then, applying the commutative and associative properties of G, $(ab)^{k+1} = (ab)^k (ab) = a^k b^k ba = a^k b^{k+1} a = a^k a b^{k+1} = a^{k+1} b^{k+1}$. By the principle of induction, $(ab)^n = a^n b^n$ for $n > 0$.

Suppose $n < 0$ and let $m = -n$. Then, $m > 0$, so by our previous conclusion: $(an)^m = a^m b^m$. Then, by page 92 of Beachy, two elements of G are equal if and only if their inverses are equal, so we can write: $(ab)^{-m} = a^{-m} b^{-m}$. Thus, $(ab)^n = a^n b^n$ when $n < 0$.

Finally, suppose $n = 0$. Then, by extension of definition 3.1.4, given on the last paragraph of page 92 of Beachy, $(ab)^n = (ab)^0 = e$ and $a^n b^n = a^0 b^0 = ee = e$ so $(ab)^n = a^n b^n$ when $n = 0$. $\square$

Exercise 3.1.20: Let S be a nonempty finite set with a binary operation $*$ that satisfies the associative law. Show that S is a group if $a * b = a * c$ implies $b = c$ and $a * c = b * c$ implies $a = b$ for all $a, b, c \in S$. What can you say if S is infinite?

Proof. Assume S is a nonempty finite set with a binary operation $*$ such that $a * b = a * c$ implies $b = c$ and $a * c = b * c$ implies $a = b$ for all $a, b, c \in S$. For simplification, let's write $a * b = ab$ for the remainder of this proof. We will use proposition 3.1.8 to to show S is a group:

Consider $\varphi_a : S \to S$ such that $a \in S$ and $\varphi_a(x) = ax$. First show φ_a is a bijection:

Notice $|S| = |S|$ is finite, so by proposition 2.1.8, it suffices to show φ_a is one-to-one or onto. We will show φ_a is one-to-one. Consider any $b, c \in S$ and suppose $\varphi_a(b) = \varphi_a(c)$. Then, $ab = ac$. By assumption, this implies $b = c$. Thus, φ_a is one-to-one. Then, by proposition 2.1.8, φ_a is a bijection.

Consider any $b \in S$. Since φ_a is a bijection, there exists $x \in S$ such that $\varphi_a(x) = b$. Then, $ax = b$, as desired for part of proposition 3.1.20.

Next, consider $\varphi_a^{'} : S \to S$ by $\varphi_a^{'}(x) = xa$. Notice $|S| = |S|$ is finite, so by proposition 2.1.8, it suffices to show $\varphi_a^{'}$ is one-to-one or onto. We will show $\varphi_a^{'}$ is one-to-one. Consider any $b, c \in S$ and suppose $\varphi_a^{'}(b) = \varphi_a^{'}(c)$. Then, $ba = ca$. By assumption, this implies $b = c$. Thus, φ_a is one-to-one. Then, by proposition 2.1.8, $\varphi_a^{'}$ is a bijection.

Consider any $b \in S$. Since $\varphi_a^{'}$ is a bijection, there exists $x \in S$ such that $\varphi_a^{'}(x) = b$. Then, $xa = b$, as desired for part of proposition 3.1.20.

Thus, S is a nonempty set with an associative binary operation in which the equations $ax = b$ and $xa = b$ have solutions for all $a, b \in G$, so by proposition 3.1.8, S is a group.

$\square$

Exercise 3.1.22: Let G be a group. Prove that G is abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$.

Proof. ($\Rightarrow$) Assume G is an abelian group. Then consider any $a, b \in G$. Because G is a group there exists $a^{-1}, b^{-1} \in G$ From proposition 3.1.3 in Beachy, $(ab)^{-1} = b^{-1}a^{-1}$. Since G is abelian, $b^{-1}a^{-1} = a^{-1}b^{-1}$. Thus, for any $a, b \in G$, $(ab)^{-1} = a^{-1}b^{-1}$

($\Leftarrow$) Assume for any $a, b \in G$, $(ab)^{-1} = a^{-1}b^{-1}$. For any $a, b \in G$, $a^{-1}, b^{-1} \in G$ so $(ab)^{-1} = a^{-1}b^{-1}$ must be valid for a^{-1}, b^{-1}. From proposition 3.1.3, $(ab)^{-1} = b^{-1}a^{-1}$; thus $a^{-1}b^{-1} = b^{-1}a^{-1}$. Substituting a^{-1}, b^{-1}, we obtain $(a^{-1})^{-1}(b^{-1})^{-1} = (b^{-1})^{-1}(a^{-1})^{-1}$. From paragraph 1 on page 92 of Beachy, $(a^{-1})^{-1} = a, (b^{-1})^{-1} = b$. Thus, $ab = ba$ for any $a, b \in G$ and therefore G is abelian. □

Exercise 3.1.23: Let G be a group. Prove that if $x^2 = e$ for all $x \in G$, then G is abelian.

Proof. Assume $x^2 = e$ for all $x \in G$. Then, $x^{-1} \in G$ and $x^2x^{-1} = ex^{-1}$ implies $x = x^{-1}$ for any $x \in G$. Consider any $a, b \in G$. Then, $ab \in G$. Then, since $x = x^{-1}$ for any $x \in G$, $(ab)^{-1} = ab$. From prop osition 3.1.3, $(ab)^{-1} = b^{-1}a^{-1}$. Thus, $ab = b^{-1}a^{-1}$. Then, since $x = x^{-1}$ for any $x \in G$, $b^{-1} = b$ and $a^{-1} = a$ so $ab = b^{-1}a^{-1} = ba$ for any $a, b \in G$. Thus, G is abelian. □

Exercise 3.1.24: Show that if G is a finite group with an even number of elements, then there must exist an element $a \in G$ with $a \neq e$ such that $a^2 = e$.

Assume G is a finite group with an even number of elements. Then, $|G| = 2k$ for $k \geq 1$. Since G is a group, G must have an identity element, $e \in G$. Thus, there are $2k - 1$ elements in G that are not the identity element. Since G is a group, all elements in G have at most one inverse that is also in G. Since we have an odd number of elements not equal to e in G, by the pigeon hole principle, there must be at least one element in G which is its own inverse. Suppose $a \in G$ is an element that is its own inverse. Then $aa = e$ and so $a^2 = e$.