MATH 3030, Abstract Algebra
FALL 2012
Toby Kenney
Homework Sheet 1
Due: Wednesday 26th September: 3:30 PM

Basic Questions

1. *Which of the binary operations in the following table are (a) Commutative (b) Associative?*

(i)

	a	b	c	d
a	a	b	c	c
b	a	b	c	c
c	c	c	c	c
d	c	c	c	d

(ii)

	a	b	c
a	c	a	c
b	a	b	a
c	c	a	c

(iii)

	a	b	c
a	b	b	c
b	c	c	a
c	a	a	b

(iv)

	a	b	c
a	b	c	c
b	c	a	a
c	a	b	b

(a) (ii) is the only commutative operation. To be a commutative operation, the multiplication table must be a symmetric matrix.

(b) (i) For the products $(x * y) * z$ and $x * (y * z)$, if any of x, y, or z is c, then both answers must be c, so we only need to consider cases when none of x, y, and z are c. Similarly, if any of x, y, or z is d, then either they are all d, in which case associativity holds, or both answers are c. Therefore, we are left considering cases when x, y and z are all a or b, in which case, both answers are z. So this is associative.

(ii)

x	y	z	$(x * y) * z$	$x * (y * z)$
a	a	a	c	c
a	a	b	a	c
a	a	c	c	c
a	b	a	c	c
a	b	b	a	a
a	b	c	c	c
a	c	a	c	c
a	c	b	a	c
a	c	c	c	c
b	a	a	c	a
b	a	b	a	a
b	a	c	c	a
b	b	a	a	a
b	b	b	b	b
b	b	c	a	a
b	c	a	c	a
b	c	b	a	a
b	c	c	c	a
c	a	a	c	c
c	a	b	a	c
c	a	c	c	c
c	b	a	c	c
c	b	b	a	a
c	b	c	c	c
c	c	a	c	c
c	c	b	a	c
c	c	c	c	c

(iii)

x	y	z	$(x*y)*z$	$x*(y*z)$
a	a	a	b	c
a	a	b	c	b
a	a	c	c	c
a	b	a	c	c
a	b	b	a	a
a	b	c	c	b
a	c	a	a	b
a	c	b	a	b
a	c	c	a	b
b	a	a	a	c
b	a	b	a	c
b	a	c	c	a
b	b	a	a	a
b	b	b	a	a
b	b	c	b	c
b	c	a	b	c
b	c	b	b	c
b	c	c	c	c
c	a	a	b	a
c	a	b	b	a
c	a	c	c	b
c	b	a	b	b
c	b	b	b	b
c	b	c	c	a
c	c	a	c	a
c	c	b	c	a
c	c	c	a	a

(iv) This is isomorphic to (iii), so it is not associative.

2. *Which of the following produce well-defined binary operations? Justify your answers.*

   (a) $*$ on the complex numbers defined by $a*b$ is the solution to $x^2+ax+b=0$.

   This is not well-defined because the equation has two solutions.

   (b) $*$ on the non-negative integers given by $a*b$ is the number of digits that a and b have in common (written in decimal).

   This is not very clearly defined — do we ignore leading zeros? Do the common digits need to be in the same position?

   If we assume that leading zeros are ignored, even if there are non-leading zeros in the corresponding position of the other number and that digits have to be in corresponding positions, then this is a well-defined binary operation.

(c) $*$ on the set of circles in the plane where $c_1 * c_2$ is the smallest circle which is tangent to both c_1 and c_2.

This is not well-defined — if c_1 and c_2 are the same circle (or are tangent to each other) then there is no smallest circle tangent to both of them.

(d) $*$ on the set of intervals $[a, b]$ in the real numbers given by $[a, b] * [c, d] = \{xy | x \in [a, b], y \in [c, d]\}$.

This is well-defined. It is clear from the definition that the set in question is uniquely defined for each pair of intervals. The difficulty is in showing that it is an interval. However, this can be checked by case analysis on the signs of a, b, c, and d.

3. *Which pairs of the binary operations in Question 1 are isomorphic? Give an isomorphism if one exists and explain why one cannot exist if one does not exist.*

(i) has 4 elements while the others have 3, so (i) cannot be isomorphic to any of the others.

The columns in (ii) contain only two different elements, while those in (iii) and (iv) contain all three, so (ii) cannot be isomorphic to any of the others.

(iii) and (iv) are isomorphic via the isomorphism:

a	c
b	b
c	a

[It is easy to see that this must be the isomorphism by counting solutions to $x^2 = y$ for each y.]

4. *Which of the following binary operations are groups? Justify your answers.*

(i)

	a	b	c	d	e
a	a	b	c	d	e
b	b	d	a	e	c
c	c	e	d	b	a
d	d	a	e	c	b
e	e	c	b	a	d

(ii)

	a	b	c	d	e
a	a	b	c	d	e
b	b	a	e	c	d
c	c	d	a	e	b
d	d	e	b	a	c
e	e	c	d	b	a

(iii)

	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	a	e	f	c	d
c	c	f	a	e	d	b
d	d	e	f	a	b	c
e	e	d	b	c	f	a
f	f	c	d	b	a	e

(iv)

	a	b	c	d
a	a	b	c	d
b	b	b	d	d
c	c	d	c	d
d	d	d	d	d

(v)

	a	b	c
a	a	b	c
b	c	a	b
c	b	c	a

(iv)

	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

(i) is not associative. For example, $(b*b)*b = d*b = a$ while $b*(b*b) = b*d = e$. It does however have an identity element a, and each element has both a left and a right inverse, but these inverses are not the same. [This also implies non-associativity, as we will see later.]

(ii) is also not associative. For example, $(b*c)*d = e*d = b$ while $b*(c*d) = b*e = d$. It does however have an identity element a, and every element is its own inverse.

(iii) is a group.

(iv) is associative, and has an identity element a, but no element except a has an inverse.

(v) does not have an identity element. It is also not associative, e.g. $(b*a)*a = c*a = b$ while $b*(a*a) = b*a = c$.

(vi) is a group.

Standard Questions

5. *Let $*$ and $.$ be two binary operations on a set S, with the same identity element 1. Suppose further that $(a*b).(c*d) = (a.c)*(b.d)$ for any a, b, c and d in S. Prove that $*$ and $.$ are the same operation, and further that this operation is commutative and associative. [Hint: consider $(a.1)*(1.b)$ and $(1.b)*(a.1)$.]*

   By considering $(a.1)*(1.b)$, we get $a*b = (a.1)*(1.b) = (a*1).(1*b) = a.b$. This shows that $*$ and $.$ are the same operation. By considering $(1.b)*(a.1)$, we get $b*a = (1.b)*(a.1) = (1*a).(b*1) = a.b$. This shows that the operation is commutative. Finally, $(a*b)*c = (a*b).c = (a*b).(1*c) = (a.1)*(b.c) = a*(b.c) = a*(b*c)$, so the operation is associative.

6. *Show that the isomorphism relation between sets with a binary operation is an equivalence relation.*

   The identity function is clearly an isomorphism from a set to itself, so the relation is reflexive. If ϕ is an isomorphism from $(X,.)$ to $(Y,*)$, then as ϕ is a bijection, there is a function $Y \xrightarrow{\phi^{-1}} X$ where $\phi^{-1}(y)$ is the unique $x \in X$ such that $\phi(x) = y$. This will be an isomorphism from $(Y,*)$ to $(X,.)$ we just need to show that $\phi^{-1}(ab) = \phi^{-1}(a)\phi^{-1}(b)$. However, we know that $\phi^{-1}(ab)$ is the unique solution to $\phi(\phi^{-1}(ab)) = ab$, and that $\phi(\phi^{-1}(a)\phi^{-1}(b)) = \phi(\phi^{-1}(a))\phi(\phi^{-1}(b)) = ab$, so by uniqueness they

must be equal. Finally, if $(X,.) \xrightarrow{\phi} (Y,*)$ and $(Y,*) \xrightarrow{\theta} (Z,\#)$ are isomorphisms, then the composite $\theta \circ \phi$ given by $\theta \circ \phi(x) = \theta(\phi(x))$ is an isomorphism from $(X,.)$ to $(Z,\#)$. It is clearly a bijection, so we just need to show that $\theta \circ \phi(xy) = \theta \circ \phi(x)\theta \circ \phi(y)$. However, we have that $\theta \circ \phi(xy) = \theta(\phi(xy)) = \theta(\phi(x) * \phi(y)) = \theta \circ \phi(x)\#\theta \circ \phi(y)$, so it is an isomorphism.

7. *Let G be a finite group with identity e, and let x be an element of G. Show that there is some number n such that $x^n = e$.*

   Consider the set $\{e, x, x^2, x^3, \ldots\}$ of all powers of x in G. Since G is finite, these elements cannot all be different, so we must have $x^i = x^j$ for two distinct i and j. Suppose, without loss of generality, that $i < j$, and suppose that i is as small as possible. Then multiplying by the inverse of x, we have that $x^{-1}x^i = x^{-1}x^j$, so that $x^{i-1} = x^{j-1}$. This contradicts minimality unless $i = 0$, so we must have that $i = 0$, i.e. $x^j = e$.

8. *For a fixed element a of a group G, show that the map ϕ given by $\phi(x) = axa^{-1}$ is an isomorphism from G to itself.*

   We need to show that ϕ is a bijection, and that $\phi(xy) = \phi(x)\phi(y)$. However $\phi(x)\phi(y) = axa^{-1}aya^{-1} = axya^{-1}$. For the bijection part, we have the function $\theta(x) = a^{-1}xa$. Now $\theta \circ \phi$ and $\phi \circ \theta$ are both the identity function, so ϕ is a bijection and an isomorphism.

Bonus Questions

9. *How many associative binary operations are there on a 3-element set?*

   We consider the different operations up to isomorphism and duality (transposing the table). We get the following:

   Operations with an attracting element:

	a	b	c
a	a	c	c
b	c	b	c
c	c	c	c

   6 isomorphisms

	a	b	c
a	a	b	c
b	b	b	c
c	c	c	c

   6 isomorphisms

	a	b	c
a	a	b	c
b	a	b	c
c	c	c	c

3 isomorphisms times 2 duality

	a	b	c
a	c	c	c
b	c	c	c
c	c	c	c

3 isomorphisms

	a	b	c
a	a	b	c
b	b	c	c
c	c	c	c

6 isomorphisms

	a	b	c
a	a	b	c
b	b	a	c
c	c	c	c

6 isomorphisms

	a	b	c
a	a	c	c
b	c	c	c
c	c	c	c

6 isomorphisms

	a	b	c
a	b	b	c
b	b	b	c
c	c	c	c

6 isomorphisms

	a	b	c
a	b	c	c
b	c	c	c
c	c	c	c

6 isomorphisms

Operations with an identity but no attracting element

	a	b	c
a	a	b	c
b	b	b	c
c	c	b	c

3 isomorphisms times 2 dualities

	a	b	c
a	a	b	c
b	b	c	b
c	c	b	c

6 isomorphisms

	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

3 isomorphisms

Other operations:

	a	b	c
a	a	c	c
b	b	b	b
c	c	c	c

6 isomorphisms times 2 dualities

	a	b	c
a	a	b	c
b	a	b	c
c	a	b	c

2 dualities

	a	b	c
a	b	a	a
b	a	b	b
c	a	b	b

6 isomorphisms

	a	b	c
a	b	c	b
b	c	b	c
c	b	c	b

6 isomorphisms

Adding these all up, we get a total of 92 associative operations.

10. *Let S be a set with an associative binary operation $*$ such that for every element $x \in S$, there is a unique element x' such that $x*x'*x = x$. Prove that S is a group under $*$.*

First note that $x*(x'*x*x')*x = (x*x'*x)*x'*x = x*x'*x = x$, so by uniqueness, we get that $x'*x*x' = x'$. Therefore $(x')' = x$.

Recall that an element x is idempotent if $x*x = x$. Suppose a and b are idempotent elements, and let $x = (a*b)'$. We have that $(a*b)*(b*x)*(a*b) = a*b*x*a*b = a*b$, so by uniqueness, we get that $x = b*x$, and similarly, $x = x*a$. Now since $x' = a*b$, we get $x = x*a*b*x = x*x$, so x is idempotent. Furthermore, since $x*x*x = x*x = x$, uniqueness again gives that $x = x' = a*b$. Thus $a*b$ is also idempotent. Now also $a*b*a*a*b = a*b*a*b = a*b$, so we also get $a = x$, and similarly, $b = x$, so we must have $a = b$. Since a and b were arbitrary idempotents, this means that there is at most one idempotent e in S. On the other hand, for any $x \in S$, $(x*x')*(x*x') = (x*x'*x)*x' = x*x'$, so $x*x'$ is idempotent and must equal e. Similarly $x'*x = e$, so we have $e*x = x*x'*x = x$ and $x*e = x*x'*x = x$, so e is an identity element, and x' is the inverse of x, so we have shown that S is a group.