MAU22C00 Lecture 24

John Stalker

Trinity College Dublin

Homomorphisms

Suppose (A,f) is a semigroup, $B \subseteq A$, and $f(x,y) \in B$ whenever $x \in B$ and $y \in B$, i.e. that (B,g) is a subsemigroup of (A,f), where g is the restriction of f to B^2.

Let h be the inclusion function from B to A, i.e. the domain of h is B and $h(x) = x$ for all $x \in B$.

Then

$$f(h(x),h(y)) = h(g(x,y))$$

for all $x \in B$ and $y \in B$.

More generally, if (A,f) and (B,g) are semigroups and h is a function from B to A such that $f(h(x),h(y)) = h(g(x,y))$ for all $x \in B$ and $y \in B$ then we say that h is a semigroup homomorphism from (B,g) to (A,f).

If h is an invertible function we say that it is a semigroup isomorphism. If also $B = A$ and $g = f$ then we say that h is a semigroup automorphism of (A,f)

The semigroup automorphisms of (A,f) form a group.

Homomorphisms, continued

We can define monoid homomorphisms similarly. In addition to $f(h(x), h(y)) = h(g(x, y))$ we need to require that $h(j)$ is the identity for A, where j is the identity in B.

If h is an invertible function we say that it is a monoid isomorphism. Monoid automorphisms are defined as isomorphisms from a monoid to itself. These form a group.

We can define group homomorphisms similarly. In addition to $f(h(x), h(y)) = h(g(x, y))$ we could require that $h(j)$ is the identity for A, where j is the identity in B and that $h(y)$ is the inverse to $h(x)$ whenever y is the inverse of x.

It turns out those conditions are redundant. They follow from $f(h(x), h(y)) = h(g(x, y))$

If h is an invertible function we say that it is a group isomorphism. Again, we define group automorphisms as isomorphisms from a group to itself. These form a group.

Examples

The length function is a monoid homomorphism from the monoid of lists of members of C, with concatenation as the operation, to the natural numbers, with addition as the operation.

In other words, the empty list is of length zero and the length of the concatenation of two lists is the sum of their lengths.

Let A be the natural numbers and f the maximum operation. Let B be the set of Boolean values T and F and g the $\wedge$ operation. Define h from B to A by $h(T) = 0$ and $h(F) = 1$. Then h is a monoid homomorphism.

In other words, $h(T) = 0$ and $\max(h(p), h(q)) = h(p \wedge q)$. There are four possible values for (p, q) so you can check this.

Suppose (A, f) is a semigroup, B is the set of lists all of whose items are members of A, and g is the concatenation relation. Let h be the function which takes a list and computes its "product". This h is a semigroup homomorphism.

More examples

There is a monoid homomorphism from $(N, +)$ to the bicyclic semigroup given by $h(m) = (m, 0)$.

This is just the fact that the product, in the bicyclic semigroup, of $(m, 0)$ and $(n, 0)$ is $(m + n, 0)$, as mentioned previously.

Similarly, $h(m) = (0, m)$ is a monoid homomorphism.

There is a monoid homomorphism from $(N, \max)$ to the bicyclic semigroup given by $h(m) = (m, m)$.

This is true because the product in the bicyclic semigroup of (m, m) and (n, n) is $(\max(m, n), \max(m, n))$.

Last time I mentioned that the group of automorphisms of the Wumpus graph and the group of symmetries of a regular dodecahedron both have 120 elements. In fact there is an isomorphism from one group to the other.

An isomorphism

You can label the vertices of a dodecahedron such that the faces are $(1,2,3,4,5)$, $(1,5,6,7,8)$, $(2,1,8,9,10)$, $(3,2,10,11,12)$, $(4,3,12,13,14)$, $(5,4,14,15,6)$, $(7,6,15,16,17)$, $(8,7,17,18,9)$, $(10,9,18,19,11)$, $(12,11,19,20,13)$, $(14,13,20,16,15)$, and $(17,16,20,19,18)$.

There is then an edge between vertices i and j on the dodecahedron if and only if there is edge between vertices i and j on the graph.

So every symmetry of the dodecahedron gives a graph automorphism.

It's less obvious, but true, that every graph automorphism comes from a symmetry of the dodecahedron.

People often refer to groups as being "the same" when they really mean "isomorphic".

The power function

Let P be the set of positive natural numbers, i.e. $P = N \setminus \{0\}$. Then $(P, +)$ is a subsemigroup, but not submonoid, of $(N, +)$.

Suppose (A, f) is a semigroup and $x \in A$. Let h be the function which takes an $n \in P$ and gives you the "product" of n copies of x.

We saw earlier that all products give the same value, so we're justified in talking about *the* product.

h is a semigroup homomorphism.

$h(n)$ is called the n'th "power" of x. It's often written as x^n.

This terminology and notation is fine when f is really a product, but can be confusing when it's not.

It has some of the properties you would expect, e.g.

$$x^m x^n = x^{m+n}, \quad (x^m)^n = x^{m \cdot n}.$$

but $(xy)^n = x^n y^n$ is false in general.

Homomorphisms and equivalence relations

Suppose (A,f) and (B,g) are semigroups and h is a semigroup homomorphism from (A,f) to (B,g).

In other words,

$$g(h(x),h(y)) = h(f(x,y))$$

for all x and y in A.

Define a relation R on A by $(x,y) \in R$ if and only if $h(x) = h(y)$.

R is an equivalence relation. In fact for this we don't even need the fact that h is a homomorphism.

- R is reflexive, i.e. if $x \in A$ then $(x,x) \in R$, i.e. $h(x) = h(x)$.
- R is transitive, i.e. if $x \in A$, $y \in A$ and $z \in A$ and $(x,y) \in R$ and $(y,z) \in R$ then $(x,z) \in R$, i.e. if $h(x) = h(y)$ and $h(y) = h(z)$ then $h(x) = h(z)$.
- R is symmetric, i.e. if $x \in A$ and $y \in A$ and $(x,y) \in R$ then $(y,x) \in R$, i.e. if $h(x) = h(y)$ and $h(y) = h(x)$.

Homomorphisms and equivalence relations

Recall that $g(h(x),h(y)) = h(f(x,y))$ for all x and y in A and $(x,y) \in R$ if and only if $h(x) = h(y)$.

Suppose $(u,x) \in R$ and $(v,y) \in R$, i.e. that $h(u) = h(x)$ and $h(v) = h(y)$.

Then $g(h(u),h(v)) = g(h(x),h(y))$, so $h(f(u,v)) = h(f(x,y))$.

In other words $(f(u,v),f(x,y)) \in R$.

So $(u,x) \in R$ and $(v,y) \in R$ imply $(f(u,v),f(x,y)) \in R$.

We just constructed an equivalence relation from a semigroup homomorphism. We can also construct a semigroup homomorphism from an equivalence relation.

Quotients

Suppose (A,f) is a semigroup and R is a relation on A such that $(u,x) \in R$ and $(v,y) \in R$ imply $(f(u,v),f(x,y)) \in R$.

Then there is a semigroup (B,g) and a surjective function h from A to B such that h is a semigroup homomorphism from (A,f) to (B,g).

The members of B are the equivalence classes for the relation R and h is the function which takes a member of A to the equivalence class to which it belongs.

h is a homomorphism so

$$g(h(x),h(y)) = h(f(x,y)).$$

For any $C \in B$ and $D \in B$ there are $x \in A$ and $y \in A$ such that $x \in C$ and $y \in D$ so this equation tells us $g(C,D)$ must be the equivalence class of $f(x,y)$.

The problem is to show that this is genuinely a function, i.e. that the equivalence class doesn't depend on which $x \in C$ and $y \in D$ are chosen. This is where we need the fact that $(u,x) \in R$ and $(v,y) \in R$ imply $(f(u,v),f(x,y)) \in R$.

Quotients, continued

The semigroup (B, g) constructed in this way is called the quotient of the semigroup (A, f) by the relation R.

If i is an identity for (A, f) then $h(i)$ is an identity for (B, g).

So (B, g) is a monoid if (A, f) is.

If y is an inverse for x then $h(y)$ is an inverse for $h(x)$.

Every member of B is $h(x)$ for some $x \in A$, so if every member of A is invertible then so is every member of B.

In other words, (B, g) is a group if (A, f) is.

(B, g) may be a group even if (A, f) isn't.