

## 15 Chapter: Ring Homomorphisms

The map,  $f$  from  $\mathbf{Z}_{10}$  to  $\mathbf{Z}_{10}$  given by  $f(x) = 2x$  is not a ring homomorphism. But the map  $g$  from  $\mathbf{Z}_{10}$  to  $\mathbf{Z}_{10}$  given by  $g(x) = 5x$  is a ring homomorphism. (Convince yourself that these statements are true!) In this chapter we will investigate the question: Given a fixed  $n$ , for which  $m$  is the map  $f : \mathbf{Z}_n \rightarrow \mathbf{Z}_n$  given by  $f(x) = mx$  a ring homomorphism? Similarly, when is the map  $f : \mathbf{Z}_n \rightarrow \mathbf{Z}_n$  given by  $f(x) = x^m$  a ring homomorphism? Recall that any **group** homomorphism from  $\mathbf{Z}_n$  to  $\mathbf{Z}_n$  is completely determined by the image of  $1 \bmod n$ . Since a ring homomorphism is also a group homomorphism, the image of any ring homomorphism from  $\mathbf{Z}_n$  to  $\mathbf{Z}_n$  is also completely determined by the image of  $1 \bmod n$ .

Consider the following example in GAP:

```
gap> R:= Integers mod 10;
(Integers mod 10)
gap> e:= Elements(R);
[ZmodnZObj(0,10), ZmodnZObj(1,10), ZmodnZObj(2,10),
ZmodnZObj(3,10), ZmodnZObj(4,10), ZmodnZObj(5,10),
ZmodnZObj(6,10), ZmodnZObj(7,10), ZmodnZObj(8,10),
ZmodnZObj(9,10)]
gap> h:= x -> e[6]*x;
function(x) ... end
gap> f:= MappingByFunction(R,R,h);
GeneralMappingByFunction( (Integers mod 10), (Integers mod
10), function(x)...end)
gap> IsRingHomomorphism(f);
true
```

The above output tells us the map  $f$  from  $\mathbf{Z}_{10}$  to  $\mathbf{Z}_{10}$  given by  $f(x) = 5x$  is a ring homomorphism. The above command `h:= x -> e[6]*x;` creates a function that takes an element and multiplies it by  $5 \bmod 10$ . ( $5 \bmod 10$  is the sixth element in the list of elements of  $R$ .) The above command `f:= MappingByFunction(R,R,h);` creates this map. In general, the command is `MappingByFunction( <domain>, <range>, <function>)`. Now we can use `<ctl>-p` to redefine  $h$  and  $f$  and test for other homomorphisms:

```
gap> h:= x -> e[1]*x;
function(x) ... end
gap> f:= MappingByFunction(R,R,h);
GeneralMappingByFunction( (Integers mod 10), (Integers mod
10), function(x)...end)
gap> IsRingHomomorphism(f);
true
gap> h:= x -> e[2]*x;
function(x) ... end
gap> f:= MappingByFunction(R,R,h);
```

```

GeneralMappingByFunction( (Integers mod 10), (Integers mod
10), function(x)...end)
gap> IsRingHomomorphism(f);
true
gap> h:= x -> e[3]*x;
function(x) ... end
gap> f:= MappingByFunction(R,R,h);
GeneralMappingByFunction( (Integers mod 10), (Integers mod
10), function(x)...end)
gap> IsRingHomomorphism(f);
false

```

We could continue testing all 10 possible cases for homomorphisms. Since the above steps are repetitive, it may be better to write a short program that will make GAP test all the cases. The subroutine “ringHoms” contains a function that takes as input a positive integer  $n$ . Fetch this subroutine from the manual web site. The output is a list of  $m$  such that  $f : \mathbf{Z}_n \rightarrow \mathbf{Z}_n$  given by  $f(x) = mx \bmod n$  is a ring homomorphism. (Thanks to Russell Blyth for providing this function.) See the end of this chapter for a print out of this function.

```

gap> Read("ringHoms");
gap> ringHoms(10);
The map f: Z_10 -> Z_10 given by f(x)=mx is a homomorphism for m=[ 0, 1, 5, 6 ]

```

Thus  $f : \mathbf{Z}_n \rightarrow \mathbf{Z}_n$  given by  $f(x) = mx \bmod n$  is a ring homomorphism if and only if  $m = 0, 1, 5$  or  $6$ .

### Exercises

15.1 Using GAP determine for which  $m \leq 15$  the map  $f : \mathbf{Z}_{15} \rightarrow \mathbf{Z}_{15}$  given by  $f(x) = mx \bmod 15$  is a ring homomorphism.

15.2 Repeat Exercise 15.1 for the rings  $\mathbf{Z}_{25}$ ,  $\mathbf{Z}_{20}$ ,  $\mathbf{Z}_{30}$  and  $\mathbf{Z}_{40}$ .

15.3 Make a conjecture that describes for which  $m$  the map  $f : \mathbf{Z}_n \rightarrow \mathbf{Z}_n$  given by  $f(x) = mx \bmod n$  is a ring homomorphism.

15.4 Prove your conjecture in Exercise 15.3.

15.5 Make a conjecture that describes for which  $k$  the map  $f : \mathbf{Z}_m \rightarrow \mathbf{Z}_n$  given by  $f(x) = kx \bmod n$  is a ring homomorphism. (The GAP commands that you used in Exercises 15.1 and 15.2 will not work here. Instead of using GAP, think about what conditions on  $k$  will be necessary to make  $f$  a ring homomorphism.)

15.6 Using GAP determine for which  $m \leq 15$  the map  $f : \mathbf{Z}_{15} \rightarrow \mathbf{Z}_{15}$  given by  $f(x) = x^m \bmod 15$  is a ring homomorphism. You may want to write a program in GAP by modifying the program “ringHoms”.

15.7 Using your program from Exercise 15.6, repeat Exercise 15.6 for the rings  $\mathbf{Z}_{25}$ ,  $\mathbf{Z}_{20}$ ,  $\mathbf{Z}_{30}$  and  $\mathbf{Z}_{40}$ .

15.8 Make a conjecture that describes for which  $m$  the map  $f : \mathbf{Z}_n \rightarrow \mathbf{Z}_n$  given by  $f(x) = x^m \pmod n$  is a ring homomorphism.

### Appendix for Chapter 15

The following is the file “ringHoms” which is used in this chapter. (Thanks to Russell Blyth for providing this function.)

```
ringHoms := function(n)
local R,e,h,f,l,j;
R := Integers mod n;
e := Elements(R);
l := [];
Print("The map f: Z_", n, " -> Z_", n, " given by f(x)=mx is a homomorphism for m=");
for j in [1..Size(e)] do
  h := x -> e[j]*x;
  f := MappingByFunction(R,R,h);
  if IsRingHomomorphism(f) then
    Append(l,[Int(e[j])]);
  fi;
od;
return l;
end;
```