

## 16 Chapter: Polynomial Rings

GAP will allow you to set up polynomial rings. For example the following GAP commands create the polynomial ring  $P1 = \mathbf{Z}_7[x]$ :

```
gap> R1:= Integers mod 7;
GF(7)
gap> P1:= PolynomialRing(R1);
GF(7)[x_1]
```

Suppose we want to factor the polynomial  $x^2 - 2 \in \mathbf{Z}_7[x]$ . Recall from Chapter 12 of this manual that the nonzero elements in  $\mathbf{Z}_7$  are denoted in GAP by powers of  $Z(7)$  where  $Z(7)$  denotes a generator of the cyclic group of nonzero elements:

```
gap> Elements(R1);
[ 0*Z(7), Z(7)^0, Z(7), Z(7)^2, Z(7)^3, Z(7)^4, Z(7)^5]
```

To see what integer  $Z(7)$  represents (mod 7) type:

```
gap> Int(Z(7));
3
```

The command:

```
gap> x:= X(R1, "x");
x
```

creates the indeterminate  $x$  over the ring  $R1$ . We can now set up a polynomial in the ring  $P1$  and factor it:

```
gap> g:= x^2-2;
x^2+Z(7)^5
gap> Factors(g);
[ x+Z(7), x+Z(7)^4 ]
```

Note that even though we entered the polynomial as  $x^2 - 2$ , GAP echoed the polynomial  $x^2 + Z(7)^5$ . But  $Z(7)^5 = 3^5 = 5 = -2$ . So  $x^2 + Z(7)^5 = x^2 - 2$ . Notice the above GAP output tells us the factors of  $x^2 - 2$  over  $\mathbf{Z}_7$  are  $x + Z(7) = x + 3$  and  $x + Z(7)^4 = x + 4$ .

As a second example, the following are the GAP commands and output used to find the factors of  $x^2 - 2$  over  $\mathbf{Z}_{11}$ .

```
gap> R2:= Integers mod 11;
GF(11)
gap> y:= X(R2, "y");
y
gap> h:= y^2-2;
```

```

y^2+Z(11)^6
gap> Factors(h);
[ y^2+Z(11)^6 ]

```

Note that  $Z(11) = 2 \pmod{7}$  and  $Z(11)^6 = -2$ :

```

gap> Int(Z(11));
2
gap> Int(-Z(11)^6);
2

```

Thus GAP echoes  $y^2 - 2$  with  $y^2 + Z(11)^6$ . As expected,  $x^2 - 2$  factors into linear factors in  $Z_7$  because 2 is a square in  $Z_7$ , but  $x^2 - 2$  does not factor in  $Z_{11}$  since 2 is not a square in  $Z_{11}$ .

GAP will also factor polynomials over the rationals. For example the following factors  $f(x) = x^2 - 1 \in \mathbf{Q}[x]$ :

```

gap> R:= Rationals;
Rationals
gap> z:= X(R, "z");
z
gap> f:= z^2-1;
z^2-1
gap> Factors(f);
[ z-1, z+1 ]

```

If you do not need to know the factors of a polynomial but only whether or not it is irreducible, you can use the `IsIrreducible` command:

```

gap> IsIrreducible(x^2-2);
false
gap> IsIrreducible(y^2-2);
true
gap> IsIrreducible(z^2-1);
false

```

### Exercises

16.1 Use GAP to factor  $x^{p-1} - 1$  in  $\mathbf{Z}_p[x]$  for  $p = 3, 5, 7$  and 11.

16.2 Using Exercise 16.1, make a conjecture about the factors of  $x^{p-1} - 1$  in  $\mathbf{Z}_p[x]$  for any prime  $p$ .

16.3 Find three monic irreducible polynomials in  $\mathbf{Z}_3[x]$  of degree three and three of degree four.

16.4 For the polynomials found in Exercise 16.3 use GAP to determine if these polynomials are irreducible over the rational numbers. (Treat the coefficient 2 mod 3 in a polynomial over  $\mathbf{Z}_3$ , for example, as the coefficient 2 in a polynomial over the rational numbers.)

16.5 Repeat Exercises 16.3 and 16.4 for the field  $\mathbf{Z}_5$ .

16.6 What do you think the irreducibility of a polynomial in  $\mathbf{Z}_p$  for  $p$  a prime tells you about the same polynomial over the rational numbers?