

Exploring Abstract Algebra with Computer Software

PREP Workshop 2004

Section 13: Extension Fields

Consider the polynomial $g(x) = x^3 - x \in \mathbf{Z}_3[x]$. If we factor this polynomial in $\mathbf{Z}_3[x]$ we get $x(x+1)(x-1)(x^2+1)(x^2+x-1)(x^2-x-1)$:

```
gap> x:= X(GF(3),"x");
x
gap> Factors(x^9-x);
[ x, Z(3)^0+x, -Z(3)^0+x, Z(3)^0+x^2, -Z(3)^0+x+x^2, -Z(3)^0-x+x^2 ]
```

The above shows that $x^9 - x$ does not factor into linear factors over $GF(3)$. Alternatively you can have GAP list just the degrees of the factors of $x^9 - x$:

```
gap> factors:= Factors(x^9-x);;
gap> List(factors, DegreeOfLaurentPolynomial);
[ 1, 1, 1, 2, 2, 2 ]
```

This shows $x^9 - x$ factors over $GF(3)$ into 3 irreducible polynomials of degree one and 3 irreducible polynomials of degree 2. Let α denote a zero of an irreducible factor of $g(x)$ of degree 2. If we adjoin α to \mathbf{Z}_3 we get a field with 9 elements. There is only one field (up to isomorphism) of order p^n for each prime p and each positive integer n . The field of order p^n for p a prime is denoted in GAP by $GF(p^n)$. To see if $g(x)$ splits over this larger field use the command `Factors(P,g)` where `P` is the polynomial ring over this larger field and `g` is the polynomial. Notice that $x(x^{3^2-1} - 1)$ splits into linear factors over $GF(9)$:

```
gap> polyring:= PolynomialRing(GF(9));
PolynomialRing(..., [ x ])
gap> factors:= Factors(polyring, x^9-x);
[ x, Z(3)^0+x, -Z(3)^0+x, Z(3^2)+x, Z(3^2)^2+x, Z(3^2)^3+x,
  Z(3^2)^5+x, Z(3^2)^6+x, Z(3^2)^7+x ]
gap> List(factors, DegreeOfLaurentPolynomial);
[ 1, 1, 1, 1, 1, 1, 1, 1, 1 ]
```

The above output shows that $x(x^{3^2-1} - 1) = x(x+1)(x+2)(x+b)(x+b^2)(x+b^3)(x+b^5)(x+b^6)(x+b^7)$ where b is a generator of the cyclic group

of nonzero elements in $GF(9)$.

Section 13, Project

13.1 Factor the polynomial $f(x) = x^{p^n} - x \in \mathbf{Z}_p[x]$ for $p = 5$ and $n = 3$.

13.2 If you adjoin a zero of a nonlinear irreducible factor of the polynomial in Exercise 13.1 to \mathbf{Z}_p , what field do you get? Does $f(x)$ split in this extension field? If it does not split continue adjoining zeros until you get the splitting field.

13.3 Repeat Exercises 13.1 and 13.2 for $p = 7$ and $n = 2$.

13.4 Repeat Exercises 13.1 and 13.2 for $p = 7$ and $n = 4$.