

Exploring Abstract Algebra with Computer Software

PREP Workshop 2004

Section 14: Galois Theory

In this section we will investigate algebraic extensions of fields. If we want to construct the field $\mathbf{Q}(\sqrt{2}, \sqrt{3}) = \mathbf{Q}(\sqrt{2} + \sqrt{3})$, we adjoin a root of the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over \mathbf{Q} to \mathbf{Q} . The polynomial $x^4 - 10x^2 + 1$ is the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over \mathbf{Q} . The commands below create the field $F = \mathbf{Q}(\sqrt{2} + \sqrt{3})$.

```
gap> x:=Indeterminate(Rationals, "x");
x
gap> F:=AlgebraicExtension(Rationals, x^4-10*x^2+1);
<field in characteristic 0>
```

We can now give this adjoined root, $\sqrt{2} + \sqrt{3}$, a name:

```
gap> a:=RootOfDefiningPolynomial(F);
(a)
gap> a^4;
(-1+10*a^2)
```

A similar construction can be done over finite fields. Recall the finite field of order p^n is denoted in GAP by $\text{GF}(p^n)$. Also recall the splitting field of $x^{p^n} - x$ over $\text{GF}(p)$ is $\text{GF}(p^n)$.

```
gap> x:=Indeterminate(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 ]
gap> F:=AlgebraicExtension(GF(3),Z(3)^0+x^2);
<field of size 9>
```

The field F was constructed by adjoining a root of an irreducible factor of $x^9 - x$ of degree two. Since $|F| = 9$, F must be $\text{GF}(9)$.

GAP also has a command for setting up Galois groups. For example the following creates the Galois group $\text{Gal}(\text{GF}(81), \text{GF}(3))$:

```

gap> g:=GaloisGroup(AsField(GF(3),GF(81)));
<group with 1 generators>
gap> Size(g);
4
gap> Elements(g);
[ IdentityMapping( GF(3^4) ), FrobeniusAutomorphism( GF(3^4) )^2,
  FrobeniusAutomorphism( GF(3^4) ), FrobeniusAutomorphism( GF(3^4) )^3 ]

```

Thus the Galois group $\text{Gal}(GF(81), GF(3))$ is a cyclic group of order 4. The commands for listing the subfields of a field is `Subfield`. For example, the below output shows $GF(81)$ contains three subfields:

```

gap> Subfields(GF(81));
[ GF(3), GF(3^2), GF(3^4) ]

```

Let E be the splitting field of $x^{p^n} - x$ over $GF(p^m)$ for some positive integer m that divides n . That is, $E = GF(p^n)$. By the Fundamental Theorem of Galois Theory, there is a correspondence between the set of subfields of $GF(p^n)$ containing $GF(p^m)$ and the subgroups of $\text{Gal}(GF(p^n), GF(p^m))$.

Section 14, Project 1

14.1 Determine the isomorphism class of $\text{Gal}(GF(p^n), GF(p^m))$ for $p = 2$, $m = 1$ and $n = 3, 5, 9$.

14.2 Repeat Exercise 14.1 for $p = 3$, $m = 1$ and $n = 2, 6$.

14.3 Repeat Exercise 14.1 for $p = 3$, $m = 2$ and $n = 4, 8$ and 10 and for $p = 5$, $m = 2$ and $n = 4$ and 6.

14.4 Repeat Exercise 14.1 for $p = 3$, $m = 3$ and $n = 6, 9$.

14.5 Make a conjecture about the isomorphism class of $\text{Gal}(GF(p^n), GF(p^m))$. *Careful:* Is it always the case that $GF(p^m)$ is a subfield of $GF(p^n)$ for $m \leq n$?

The command in GAP for the n th cyclotomic polynomial, $\Phi_n(x)$, is `CyclotomicPolynomial(Rationals,n)`. For example the following commands output $\Phi_{15}(x)$:

```

gap> x:= Indeterminate(Rationals, "x");
x
gap> CyclotomicPolynomial(Rationals,15);
1-x+x^3-x^4+x^5-x^7+x^8

```

The n th cyclotomic extension of \mathbf{Q} is denoted in GAP by `CyclotomicField(n)`. (Some versions of GAP allow this field to be denoted by `CF(n)` for short.) The element $\cos(2\pi/n) + i \sin(2\pi/n)$ in `CF(n)` is denoted by `E(n)`.

```

gap> f:= CF(8);
CF(8)
gap> E(8)^8;
1
gap> E(8)^2;
E(4)
gap> E(8)^4;
-1

```

Unfortunately polynomials can only be factored in GAP over finite fields or over the rationals. So we will not be able to factor polynomials over `CF(n)`. We can list the subfields of `CF(n)`:

```

gap> Subfields(f);
[ Rationals, GaussianRationals, CF(8), NF(8,[ 1, 3 ]), NF(8,[ 1, 7 ]) ]

```

The first three subfields listed are \mathbf{Q} , $\mathbf{Q}(i)$, and $\mathbf{Q}(\omega)$ where ω is a primitive 8th root of unity. The notation `NF(8,[1, 3])` means the subfield $\mathbf{Q}(\omega + \omega^3)$. Similarly `NF(8,[1, 7])` means the subfield $\mathbf{Q}(\omega + \omega^7)$.

GAP will also find the Galois groups of cyclotomic fields:

```

gap> g:=GaloisGroup(AsField(Rationals,CF(8)));
<group of size 4 with 2 generators>
gap> Elements(g);
[ IdentityMapping( CF(8) ), ANFAutomorphism( CF(8), 3 ),
  ANFAutomorphism( CF(8), 5 ), ANFAutomorphism( CF(8), 7 ) ]

```

The above output tells us that $\text{Gal}(\mathbf{Q}(\omega)/\mathbf{Q})$ has the four elements: the identity map, the automorphism of $\mathbf{Q}(\omega)$ that maps $E(8)$ to $E(8)^3$, the automorphism that maps $E(8)$ to $E(8)^5$ and the automorphism that maps $E(8)$

to $E(8)^7$.

Since $\mathbf{Q}(\omega)$ has five subfields, the Fundamental Theorem of Galois Theory says that $\text{Gal}(\mathbf{Q}(\omega), \mathbf{Q})$ must have five subgroups. Notice each nonidentity element of $\text{Gal}(\mathbf{Q}(\omega), \mathbf{Q})$ has order 2:

```
gap> e:=Elements(g);
gap> Order(e[1]);
1
gap> Order(e[2]);
2
gap> Order(e[3]);
2
gap> Order(e[4]);
2
```

Thus the five subgroups of $\text{Gal}(\mathbf{Q}(\omega), \mathbf{Q})$ are the identity subgroup, the whole group, and three subgroups of order 2.

Section 14, Project 2

14.6 Use GAP to show the Galois groups of $x^9 - 1$ and $x^7 - 1$ over \mathbf{Q} are isomorphic.

14.7 Use GAP to show the Galois groups of $x^{10} - 1$ and $x^8 - 1$ over \mathbf{Q} are not isomorphic.

14.8 Let G be the group $\text{Gal}(\mathbf{Q}(\omega), \mathbf{Q})$, where ω is a primitive 15th root of unity. Find the orders of all the elements in G .

14.9 Use GAP to determine whether or not the Galois groups of $x^{64} - 1$ and $x^{80} - 1$ over \mathbf{Q} are isomorphic.

14.10 Find all the subfields of the 60th cyclotomic extension of \mathbf{Q} .

14.11 Find all the subgroups of the Galois group of $x^{60} - 1$ over \mathbf{Q} . List the correspondence (from the Fundamental Theorem of Galois Theory) with the fields obtained in Exercise 14.10.