

## 32 Chapter: An Introduction to Galois Theory

Recall the GAP commands, discussed in Chapter 21 of this manual, for creating algebraic extensions of fields. For example, 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 below commands create the field  $F = \mathbf{Q}(\sqrt{2} + \sqrt{3})$ .

```
gap> x:= X(Rationals,"x");
x
gap> F:= AlgebraicExtension(Rationals, x^4-10*x^2+1);
<algebraic extension over the Rationals of degree 4>
```

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 (see Chapter 20 of this manual) the splitting field of  $x^{p^n} - x$  over  $\text{GF}(p)$  is  $\text{GF}(p^n)$ .

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

Let  $E$  be an extension field of the field  $F$ . The *Galois group* of  $E$  over  $F$ ,  $\text{GAL}(E/F)$ , is the set of all automorphisms of  $E$  that map every element of  $F$  to themselves. GAP 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> Elements(g);
[ IdentityMapping( GF(3^4) ), FrobeniusAutomorphism( GF(3^4) )^2,
  FrobeniusAutomorphism( GF(3^4) ), FrobeniusAutomorphism( GF(3^4) )^3 ]
```

Notice the GAP command `GaloisGroup` requires that the subfield of the extension field be listed first.

From the above output we see that the Galois group  $\text{Gal}(\text{GF}(81)/\text{GF}(3))$  is a cyclic group of order 4.

The commands for listing the subfields of a field is `Subfields`. 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  $\text{Gal}(GF(p^n)/GF(p^m))$ .

### Exercises

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

32.3 Repeat Exercise 32.1 for  $p = 3$ ,  $m = 1$  and  $n = 2, 6$ .

32.3 Repeat Exercise 32.1 for  $p = 3$ ,  $m = 2$  and  $n = 4, 8$  and  $10$  and for  $p = 5$ ,  $m = 2$  and  $n = 4$  and  $6$ .

32.4 Repeat Exercise 32.1 for  $p = 3$ ,  $m = 3$  and  $n = 6, 9$ .

32.5 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  $m \leq n$ ?

GAP has commands for determining when a group  $G$  is solvable and, in the case when  $G$  is solvable, for producing a series

$$\{e\} = H_0 \subset H_1 \subset \cdots \subset H_k = G$$

such that  $H_i$  is normal in  $H_{i+1}$  and  $H_{i+1}/H_i$  is Abelian for  $0 \leq i < k$ .

```
gap> S:=SymmetricGroup(3);
Sym( [ 1 .. 3 ] )
gap> DerivedSeries(S);
[ Sym( [ 1 .. 3 ] ), Group([ (1,3,2) ]), Group(()) ]
```

The above output is a series of subgroups  $H_0 = \{e\}$ ,  $H_1 = \langle (1, 3, 2) \rangle = \{e, (1, 3, 2), (1, 2, 3)\}$  and  $S_3 = H_k = \langle (2, 3), (1, 3, 2) \rangle$ . This series shows  $S_3$  is solvable. For another example, the following finds a series for  $D_4$  which shows it is solvable:

```
gap> d4:=Group((1,2,3,4),(1,4)(2,3));
Group([ (1,2,3,4), (1,4)(2,3) ])
gap> DerivedSeries(d4);
[ Group([ (1,2,3,4), (1,4)(2,3) ]), Group([ (1,3)(2,4) ]), Group(()) ]
```

If the command `DerivedSeries(G)` is used on a group that is not solvable the last element in the series will not be the identity subgroup.

```

gap> S5:=SymmetricGroup(5);
Sym( [ 1 .. 5 ] )
gap> DerivedSeries(S5);
[ Sym( [ 1 .. 5 ] ), Group([ (1,3,2), (1,4,3), (3,5,4) ]) ]
gap> IsSolvable(S5);
false

```

### *Exercises*

32.6 By hand find a series of subgroups of  $D_n$  that shows  $D_n$  is solvable for  $n = 5, 10, 30$ .

32.7 Rework Exercise 32.6 using GAP. Is there only one possible such series for a given dihedral group?

32.8 Determine if  $A_n$  is solvable for  $n = 4, 5$  and  $8$ .

32.9 Determine if  $D_4 \oplus D_8$  is solvable.

32.10 Determine if  $S_3 \oplus S_3$  is solvable.

32.11 Prove or disprove: The direct product of solvable groups is solvable.