

33 Chapter: Cyclotomic Extensions

Let n be an integer greater than 1 and let $\phi(n)$ denote the number of positive integers less than n and relatively prime to n . For any positive integer n there are $\phi(n)$ primitive n th roots of unity. Denote these primitive n th roots of unity by $\omega_i, i = 1, \dots, \phi(n)$. The n th cyclotomic polynomial over \mathbf{Q} is the polynomial $\Phi_n(x) = (x - \omega_1)(x - \omega_2) \cdots (x - \omega_{\phi(n)})$. The command in GAP for the n th cyclotomic polynomial is `CyclotomicPolynomial(Rationals,n)`. For example the following commands output $\Phi_{15}(x)$:

```
gap> x:= X(Rationals, "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 the smallest extension field of \mathbf{Q} that contains a primitive n th root of unity. The n th cyclotomic extension of \mathbf{Q} is denoted in GAP by `CF(n)`. 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.

Exercises

33.1 a) Factor $x^{12} - 1$ as a product of irreducibles over \mathbf{Z} .

b) Factor $x^8 - 1$ as a product of irreducibles over \mathbf{Z}_2 , \mathbf{Z}_3 and \mathbf{Z}_5 . [Gallian, Chapter 33, Exercises 2 and 3]

33.2 Use GAP to show the Galois groups of $x^9 - 1$ and $x^7 - 1$ over \mathbf{Q} are isomorphic. [Gallian, Chapter 33, Exercise 16]

33.3 Use GAP to show the Galois groups of $x^{10} - 1$ and $x^8 - 1$ over \mathbf{Q} are not isomorphic. [Gallian, Chapter 33, Exercise 18]

33.4 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 .

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

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

33.7 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 33.6.