

## Abstract Algebra with GAP Solution to 14.11

The following produces all the subgroups of the Galois group of  $x^{60} - 1$  over  $\mathbb{Q}$ .

```
gap> g:= GaloisGroup(AsField(Rationals, CF(60)));
<group with 3 generators>
gap> classes:= ConjugacyClassesSubgroups(g);
gap> Size(classes);
27
gap> subs:=List( classes , x->Representative(x) );
gap> subs_as_elts:=List( subs , x->Elements(x) );
[ [ IdentityMapping( CF(60) ) ],
  [ IdentityMapping( CF(60) ), ANFAutomorphism( CF(60), 11 ) ],
  [ IdentityMapping( CF(60) ), ANFAutomorphism( CF(60), 19 ) ],
  [ IdentityMapping( CF(60) ), ANFAutomorphism( CF(60), 29 ) ],
  [ IdentityMapping( CF(60) ), ANFAutomorphism( CF(60), 31 ) ],
  [ IdentityMapping( CF(60) ), ANFAutomorphism( CF(60), 41 ) ],
  [ IdentityMapping( CF(60) ), ANFAutomorphism( CF(60), 49 ) ],
  [ IdentityMapping( CF(60) ), ANFAutomorphism( CF(60), 59 ) ],
  [ IdentityMapping( CF(60) ), ANFAutomorphism( CF(60), 11 ),
    ANFAutomorphism( CF(60), 19 ), ANFAutomorphism( CF(60), 29 ) ],
  [ IdentityMapping( CF(60) ), ANFAutomorphism( CF(60), 11 ),
    ANFAutomorphism( CF(60), 31 ), ANFAutomorphism( CF(60), 41 ) ],
  [ IdentityMapping( CF(60) ), ANFAutomorphism( CF(60), 11 ),
    ANFAutomorphism( CF(60), 49 ), ANFAutomorphism( CF(60), 59 ) ],
  [ IdentityMapping( CF(60) ), ANFAutomorphism( CF(60), 19 ),
    ANFAutomorphism( CF(60), 31 ), ANFAutomorphism( CF(60), 49 ) ],
  [ IdentityMapping( CF(60) ), ANFAutomorphism( CF(60), 19 ),
    ANFAutomorphism( CF(60), 41 ), ANFAutomorphism( CF(60), 59 ) ],
  [ IdentityMapping( CF(60) ), ANFAutomorphism( CF(60), 29 ),
    ANFAutomorphism( CF(60), 31 ), ANFAutomorphism( CF(60), 59 ) ],
  [ IdentityMapping( CF(60) ), ANFAutomorphism( CF(60), 29 ),
    ANFAutomorphism( CF(60), 41 ), ANFAutomorphism( CF(60), 49 ) ],
  [ IdentityMapping( CF(60) ), ANFAutomorphism( CF(60), 7 ),
    ANFAutomorphism( CF(60), 43 ), ANFAutomorphism( CF(60), 49 ) ],
  [ IdentityMapping( CF(60) ), ANFAutomorphism( CF(60), 13 ),
```

ANFAutomorphism( CF(60), 37 ), ANFAutomorphism( CF(60), 49 ) ],  
 [ IdentityMapping( CF(60) ), ANFAutomorphism( CF(60), 17 ),  
 ANFAutomorphism( CF(60), 49 ), ANFAutomorphism( CF(60), 53 ) ],  
 [ IdentityMapping( CF(60) ), ANFAutomorphism( CF(60), 23 ),  
 ANFAutomorphism( CF(60), 47 ), ANFAutomorphism( CF(60), 49 ) ],  
 [ IdentityMapping( CF(60) ), ANFAutomorphism( CF(60), 11 ),  
 ANFAutomorphism( CF(60), 19 ), ANFAutomorphism( CF(60), 29 ),  
 ANFAutomorphism( CF(60), 31 ), ANFAutomorphism( CF(60), 41 ),  
 ANFAutomorphism( CF(60), 49 ), ANFAutomorphism( CF(60), 59 ) ],  
 [ IdentityMapping( CF(60) ), ANFAutomorphism( CF(60), 7 ),  
 ANFAutomorphism( CF(60), 11 ), ANFAutomorphism( CF(60), 17 ),  
 ANFAutomorphism( CF(60), 43 ), ANFAutomorphism( CF(60), 49 ),  
 ANFAutomorphism( CF(60), 53 ), ANFAutomorphism( CF(60), 59 ) ],  
 [ IdentityMapping( CF(60) ), ANFAutomorphism( CF(60), 11 ),  
 ANFAutomorphism( CF(60), 13 ), ANFAutomorphism( CF(60), 23 ),  
 ANFAutomorphism( CF(60), 37 ), ANFAutomorphism( CF(60), 47 ),  
 ANFAutomorphism( CF(60), 49 ), ANFAutomorphism( CF(60), 59 ) ],  
 [ IdentityMapping( CF(60) ), ANFAutomorphism( CF(60), 7 ),  
 ANFAutomorphism( CF(60), 13 ), ANFAutomorphism( CF(60), 19 ),  
 ANFAutomorphism( CF(60), 31 ), ANFAutomorphism( CF(60), 37 ),  
 ANFAutomorphism( CF(60), 43 ), ANFAutomorphism( CF(60), 49 ) ],  
 [ IdentityMapping( CF(60) ), ANFAutomorphism( CF(60), 17 ),  
 ANFAutomorphism( CF(60), 19 ), ANFAutomorphism( CF(60), 23 ),  
 ANFAutomorphism( CF(60), 31 ), ANFAutomorphism( CF(60), 47 ),  
 ANFAutomorphism( CF(60), 49 ), ANFAutomorphism( CF(60), 53 ) ],  
 [ IdentityMapping( CF(60) ), ANFAutomorphism( CF(60), 7 ),  
 ANFAutomorphism( CF(60), 23 ), ANFAutomorphism( CF(60), 29 ),  
 ANFAutomorphism( CF(60), 41 ), ANFAutomorphism( CF(60), 43 ),  
 ANFAutomorphism( CF(60), 47 ), ANFAutomorphism( CF(60), 49 ) ],  
 [ IdentityMapping( CF(60) ), ANFAutomorphism( CF(60), 13 ),  
 ANFAutomorphism( CF(60), 17 ), ANFAutomorphism( CF(60), 29 ),  
 ANFAutomorphism( CF(60), 37 ), ANFAutomorphism( CF(60), 41 ),  
 ANFAutomorphism( CF(60), 49 ), ANFAutomorphism( CF(60), 53 ) ],  
 [ IdentityMapping( CF(60) ), ANFAutomorphism( CF(60), 7 ),  
 ANFAutomorphism( CF(60), 11 ), ANFAutomorphism( CF(60), 13 ),  
 ANFAutomorphism( CF(60), 17 ), ANFAutomorphism( CF(60), 19 ),  
 ANFAutomorphism( CF(60), 23 ), ANFAutomorphism( CF(60), 29 ),  
 ANFAutomorphism( CF(60), 31 ), ANFAutomorphism( CF(60), 37 ),

```

ANFAutomorphism( CF(60), 41 ), ANFAutomorphism( CF(60), 43 ),
ANFAutomorphism( CF(60), 47 ), ANFAutomorphism( CF(60), 49 ),
ANFAutomorphism( CF(60), 53 ), ANFAutomorphism( CF(60), 59 ) ] ]

```

The above lists the all the subgroups of the Galois group of  $x^{60} - 1$  over the rationals. Let  $\omega$  denote a primitive 60th root of unity. The notation `ANFAutomorphism( CF(60), 13 )`, for example, denotes the automorphism that maps  $\omega$  to  $\omega^{13}$ . The following produces the subfields of the 60th cyclotomic extension of the rationals.

```

gap> f:= Subfields(CF(60));
[ Rationals, CF(3), GaussianRationals, CF(5), NF(5,[ 1, 4 ]), CF(12),
  NF(12,[ 1, 11 ]), CF(15), NF(15,[ 1, 2, 4, 8 ]), NF(15,[ 1, 4 ]),
  NF(15,[ 1, 14 ]), CF(20), NF(20,[ 1, 3, 7, 9 ]), NF(20,[ 1, 9 ]),
  NF(20,[ 1, 19 ]), CF(60), NF(60,[ 1, 7, 11, 17, 43, 49, 53, 59 ]),
  NF(60,[ 1, 7, 43, 49 ]), NF(60,[ 1, 11 ]), NF(60,[ 1, 11, 19, 29 ]),
  NF(60,[ 1, 11, 49, 59 ]), NF(60,[ 1, 17, 49, 53 ]), NF(60,[ 1, 19 ]),
  NF(60,[ 1, 23, 47, 49 ]), NF(60,[ 1, 29 ]), NF(60,[ 1, 49 ]),
  NF(60,[ 1, 59 ]) ]

```

The notation `NF(60,[ 1, 11, 19, 29 ])`, for example, denotes the subfield  $\mathbf{Q}(\omega + \omega^{11} + \omega^{19} + \omega^{29})$ . So the corresponding subgroup (in the Galois Group) is the subgroup of automorphisms that fix this field.

Denote the subgroups in the order listed above as  $g_1, g_2, \dots, g_{27}$  and the subfields in the order listed above as  $f_1, f_2, \dots, f_{27}$ . The fields corresponding to  $g_1, g_2, \dots, g_{27}$  are respectively:  $f_{16}, f_{19}, f_{23}, f_{25}, f_8, f_{12}, f_{26}, f_{27}, f_{20}, f_4, f_{21}, f_{10}, f_{15}, f_{11}, f_{14}, f_{18}, f_6, f_{22}, f_{24}, f_5, f_{17}, f_7, f_2, f_9, f_{13}, f_3, f_1$ .