Identification of a Galois group

We create a polynomial and find that it is squarefree modulo all primes \( > 7 \). There are 164 such primes \( < 1000 \).

\[
gap> x:=X(Rationals,"x");;f:=x^8-16*x^4-98;;
gap> Set(Factors(Discriminant(f)));
\[
\begin{bmatrix}
-2, 2, 3, 7
\end{bmatrix}
\]
\[
gap> 1:=Filtered([8..1000],IsPrimeInt);;Length(1);
164
\]

Let's consider the first such prime, 11. We reduce \( f \) modulo 11 and find that it is the product of two factors of degree 4.

\[
gap> p:=l[1];
11
\]
\[
gap> UnivariatePolynomial(GF(p),CoefficientsOfUnivariatePolynomial(f) *
One(GF(p)),1);
\]
\[
x_1^8+Z(11)^9*x_1^4+Z(11)^0
\]
\[
gap> fmod:=UnivariatePolynomial(GF(p),CoefficientsOfUnivariatePolynomial(f) *
One(GF(p)),1);
\]
\[
x_1^8+Z(11)^9*x_1^4+Z(11)^0
\]
\[
gap> List(Factors(fmod),Degree);
\[
[ 4, 4 ]
\]

The 'Collected' command transforms such a list into a nicer form: 2 factors of degree 4. We start a list in which we collect this information and do the same calculation in a loop over all other primes.

\[
gap> shape:=Collected(List(Factors(fmod),Degree));
[ [ 4, 2 ] ]
\]
\[
gap> a:=[];
\]
\[
gap> Add(a,shape);
\]
\[
gap> for i in [2..Length(1)] do
> p:=l[i];
> fmod:=UnivariatePolynomial(GF(p),CoefficientsOfUnivariatePolynomial(f) *
One(GF(p)),1);
> shape:=Collected(List(Factors(fmod),Degree)); Add(a,shape);
> od;
\]

We now collect the information over all primes, considering (inverse) frequencies out of 164. For example 1/3 of all primes gave a factorization into 2 linear factors and 3 quadratic, 1/54 of all primes into a product of 8 linear factors.

\[
gap> Collected(a);
[ [[[1,2],[2,3]],42], [[[1,4],[2,2]],9], [[[1,8]],3],
\]
We now want to compare this information to the cycle shape distribution in a permutation group. Consider for example the 10-th group in the list of transitive groups of degree 8. We collect the cycle structures of all elements and again count frequency information: $1/16$ of all elements have only 1-cycles, $1/2$ have two 4-cycles, $1/8$ has two 2-cycles, $1/3$ four 2-cycles.

```
gap> g:=TransitiveGroup(8,10);;
gap> Collected(List(Elements(g),CycleStructurePerm));
[ [ [ ], 1 ], [ [ , , 2 ], 8 ], [ [ 2 ], 2 ], [ [ 4 ], 5 ] ]
gap> List(Collected(List(Elements(g),CycleStructurePerm)),
> i->[i[1],Int(Size(g)/i[2])]);
[ [ [ ], 16 ], [ [ , , 2 ], 2 ], [ [ 2 ], 8 ], [ [ 4 ], 3 ] ]
```

This apparently does not agree with the frequencies we got. Thus do this calculation for all (50) transitive groups of degree 8:

```
gap> NrTransitiveGroups(8);
50
gap> e:=[];;
gap> for i in [1..50] do
    > g:=TransitiveGroup(8,i);
    > freq:=List(Collected(List(Elements(g),CycleStructurePerm)),
    > i->[i[1],Int(Size(g)/i[2])]);
    > Add(e,freq);
    > od;
```

We certainly are only interested in groups which contain cycle shapes as we observed. We thus check, which groups (given by indices) contain elements that are: three 2-cycles, two 2-cycles, four 2-cycles, two 4-cycles, and one 8-cycle.

```
gap> sel:=[1..50];;
gap> sel:=Filtered(sel,i->ForAny(e[i],j->j[1]=[3]));
[ 6, 8, 15, 23, 26, 27, 30, 31, 35, 38, 40, 43, 44, 47, 50 ]
gap> sel:=Filtered(sel,i->ForAny(e[i],j->j[1]=[2]));
[ 15, 26, 27, 30, 31, 35, 38, 40, 44, 47, 50 ]
gap> sel:=Filtered(sel,i->ForAny(e[i],j->[1]=[4]));
[ 15, 26, 27, 30, 31, 35, 38, 40, 44, 47, 50 ]
gap> sel:=Filtered(sel,i->ForAny(e[i],j->[1]=[,2]));
[ 15, 26, 27, 30, 31, 35, 38, 40, 44, 47, 50 ]
gap> sel:=Filtered(sel,i->ForAny(e[i],j->[1]=[,.,,1]));
[ 15, 26, 27, 35, 40, 44, 47, 50 ]
```

8 Groups remain. All but the first contain elements of shapes we did not observe, but we can also consider frequencies:
Comparing with the frequencies in the group again, we find that the first group (index 15) gives the best correspondence overall.

```plaintext
gap> List(Collected(a), i->[i[1],Int(164/i[2])]);
[[[1,2],[2,3]],3],[[[1,4],[2,2]],18],[[[1,8]],54],[[[2,4]],7],
[[4,2]],3], [[[8,1]],3]
```