Galois Group Mystery Hunt

Download the program `pari/gp` from the web. (It is open source. Find it, for example, here: `http://pari.math.u-bordeaux.fr/download.html`. One (of the many) things this program does is compute Galois groups of the splitting fields of polynomials over $\mathbf{Q}$. For example:

```
? polgalois(x^3-2)
%2 = [6, -1, 1, "S3"]
? polgalois(x^4 + x + 1)
%1 = [24, -1, 1, "S4"]
```

The first entry gives the order of the group. Hence the Galois group of the splitting field of $x^3 - 2$ has order 6, and goes by the name `S3`, and that the Galois group of the splitting field of $x^4 + x + 1$ has order 24, and goes by the name `S4`. The Galois group of the splitting field of a polynomial of degree d is a transitive subgroup of S_d, so we divine that the Galois groups in these cases are S_3 and S_4 respectively.

```
? polgalois(x^4 + x^3 + x^2 + x + 1)
%3 = [4, -1, 1, "C(4) = 4"]
```

The Galois group has order 4, and the notation `C(4)` suggests that it is the cyclic group of order 4. The polynomial in this case is the cyclotomic polynomial $\Phi_5(x)$, so the Galois group is $\mathrm{Gal}(\mathbf{Q}(\zeta_5)/\mathbf{Q}) = (\mathbf{Z}/5\mathbf{Z})^\times \simeq \mathbf{Z}/4\mathbf{Z}$.

```
? polgalois(x^4 - 10*x^2 + 1)
%4 = [4, 1, 1, "E(4) = 2[x]2"]
```

The Galois group has order 4 in this case also. The second entry 1 indicates that the Galois group is a subgroup of the alternating group A_4. (Correspondingly, the -1 in the enties above indicated that the Galois group was not a subgroup of A_n for the appropriate $n = \deg(f)$.) The only such group is $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$; which we can also guess from the notation. The roots of the polynomial are given explicitly by $\pm\sqrt{2} \pm \sqrt{3}$. The factor $+1$ in the second term means that the subgroup is a subgroup of the alternating group A_4.

```
? polgalois(x^7 - 2)
%5 = [42, -1, 1, "F_42(7) = 7:6"]
```

Here we get the Frobenius group F_7 in S_7 of order 42, which is not a subgroup of A_7. (The final term is suggestive of the structure of F_7, namely, that it has a normal cyclic subgroup of index 7 and a cyclic quotient of order 6.)

Let's see what happens when we take polynomials of the form $h(g(x))$ for certain $h(x)$ and $g(x)$. Let's try $h(x) = x^4 + x + 1$ and $g(x) = x^2 + 1$.

```
? h(x)=x^4+x+1;
? g(x)=x^3-2;
? polgalois(h(g(x)))
%6 = [384, -1, 44, "[2^4]S(4)"]
? polgalois(g(h(x)))
%7 = [1152, -1, 47, "[S(4)^2]2"]
```

Note that the program is not perfect:

```
? polgalois(x^2-1)
  *** polgalois: sorry, galois of reducible polynomial is not yet implemented.
? polgalois(x^12-2)
  *** polgalois: sorry, galois of degree higher than 11 is not yet implemented.
```

Here is another useful trick. Given two polynomials, say $x^3 - 2$ and $x^2 + 1$, the following command produces a new polynomial whose splitting field is the compositum of the splitting fields of the two polynomials.

```
? polcompositum(x^2 + 1,x^3-2)
%8 = [x^6 + 3*x^4 - 4*x^3 + 3*x^2 + 12*x + 5]
? polgalois(%[1])
%9 = [12, -1, 1, "D(6) = S(3)[x]2"]
```

Problem: For each $d = 1, \ldots, 7$, find as many different subgroups of S_d as you can which occur as the Galois group of an irreducible polynomial of degree d. Your grade depends only on the number of different groups you collect!