54) a) For positive integers $d, n$ prove that $d$ divides $n$ if and only if $x^d - 1$ divides $x^n - 1$ (use $n = qd + r$).

b) Setting $x = p$ for a prime $p$, show that $d$ divides $n$ if and only if $p^d - 1$ divides $p^n - 1$.

c) Show (this is using parts a) and b)), that $x^d - x$ divides $x^{p^n} - x$ if and only if $d$ divides $n$.

We have seen in Problem 48, that for every prime power $p^n$ there is a field with $p^n$ elements, namely the splitting field of $x^p - x$ over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. We call this field $\mathbb{F}_{p^n}$.

d) Show that $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^n}$ if and only if $d$ divides $n$.

(Thus, for example, $\mathbb{F}_2 \leq \mathbb{F}_4 \leq \mathbb{F}_{16}$, but $\mathbb{F}_4 \not\subset \mathbb{F}_8 \not\subset \mathbb{F}_{16}$.)

55) Let $\alpha$ be algebraic over $F$ with minimal polynomial $m(x) \in F[x]$ and $F(\alpha) \cong F[x]/(m(x))$ the corresponding algebraic extension. Suppose that $g(x) \in F(\alpha)[x]$ and that $\beta$ is a root of $g(x)$. Consider $h(x,y) \in F[x,y]$ such that $g(x) = h(x,\alpha)$ (i.e. we replace occurrences of $\alpha$ in the coefficients of $g$ by a new variable $y$). Then the resultant $r(x) = \text{Res}_y(h(x,y), m(y))$ is a polynomial that has $\beta$ as root, i.e. $r(\beta) = 0$.

(Note: $r(x)$ is not necessarily irreducible, the minimal polynomial of $\beta$ is an irreducible factor of $r$.)

For example, suppose we want to construct a rational polynomial that has a root of $x^4 + 5x + \sqrt{2}$ as a root. Set $p(x) = x^3 - 2$ (minimal polynomial of $\sqrt{2}$) and $h(x,y) = x^4 + 5x + y$.

```
gap> x:=X(Rationals,"x");;y:=X(Rationals,"y");;
gap> p:=x^3-2;;
gap> h:=x^4+5*x+y;;
gap> r:=Resultant(h,Value(p,y),y); # The Value command takes p in y
-x^12-15*x^9-75*x^6-125*x^3-2
gap> Factors(r);
[ -x^12-15*x^9-75*x^6-125*x^3-2 ]
```

We can use this method to construct iterative extensions, in particular splitting fields. We take an irreducible polynomial $p$ and construct the field $F(\alpha)$, adjoining one root of $\alpha$ of $p$. Then we factor $p$ over $F(\alpha)$ and take an irreducible factor $q(x)$. We replace $x$ by $x + k \cdot \alpha$ for some integer $k$ (this is needed to avoid just getting a power of $p$ again, as all roots of $q$ are also roots of $p$ and thus have the same minimal polynomial. Typically $k = 1$ works. Proof for this later.) The resultant then defines the field with two roots adjoined and so on.

For example, we can construct the splitting field of $x^3 - 2$ over $\mathbb{Q}$:

```
gap> p:=x^3-2;;
gap> e:=AlgebraicExtension(Rationals,p);
<algebraic extension over the Rationals of degree 3>
gap> a:=PrimitiveElement(e); # a is alpha
```
gap> pe:=Value(p,X(e)); # make it a polynomial over e.
> x_1^3+(-2)

gap> qs:=Factors(pe);q:=qs[2];;
> [ x_1+(-a), x_1^2+a*x_1+a^2 ]

gap> Value(q,X(e)+a); $ Note X(e) is the proper ‘x’
> x_1^2+3*a*x_1+3*a^2

gap> h:=x^2+3*y*x+3*y^2;
> x^2+3*x*y+3*y^2

gap> r:=Resultant(h,Value(p,y),y);
> x^6+108

gap> Factors(r); # As r is irreducible it now defines the double extension
> [ x^6+108 ]

gap> e:=AlgebraicExtension(Rationals,r); # now verify that p splits
> <algebraic extension over the Rationals of degree 6>

gap> Factors(Value(p,X(e)));
> [ x_1+(1/36*a^4-1/2*a), x_1+(1/36*a^4+1/2*a), x_1+(-1/18*a^4) ]

(If p would not split here we would take again one of the factors and repeat the process.) Note that the printed a now is a root of r, which is (from the way we modified q, replacing x by x + √2) the difference of two roots of p, e.g. we can assume it it be γ := √2(1 - e^iπ/3). Indeed, we can calculate γ^6 = -108, thus it is a root of our r. Considering the irreducible factors of r calculated above, we can also check (by tedious complex arithmetic) that \( \frac{γ^4}{36} - \frac{γ}{2} = -\sqrt{2}, \frac{γ^4}{36} + \frac{γ}{2} = -\sqrt{2}e^{iπ/3}, \) and \( -\frac{1}{18}γ^4 = -\sqrt{2}e^{4iπ/3}, \) so these are indeed the factors.

56) Use this method to determine the splitting field of \( x^4 + x + 1 \) over \( \mathbb{Q} \).

If r defines the splitting field of p and we factor r over this field \( \mathbb{Q}[x]/ (r) = \mathbb{Q}(γ) \), we get roots (we'll see later why r must split as well over this field). In the above example:

gap> s:=RootsOfUPol(Value(r,X(e)));
> [ -1/12*a^4-1/2*a, -a, 1/12*a^4-1/2*a, 1/12*a^4+1/2*a, a, -1/12*a^4+1/2*a ]

We thus know the possible automorphisms of \( \mathbb{Q}(γ) \), for example \( γ \mapsto -γ \), or \( γ \mapsto -\frac{γ^4}{12} - \frac{γ}{2} \).

57) We know (in this example) that \( \mathbb{Q}(γ) = \mathbb{Q}(\sqrt{2}, ζ = e^{iπ/3}) \) and have seen already that \( \sqrt{2} = -\frac{γ^4}{36} + \frac{γ}{2} \). By factorizing \( x^2 + x + 1 \) over \( \mathbb{Q}(γ) \), express ζ in terms of γ. Using this, describe the images of \( \sqrt{2} \) and of ζ under the automorphism \( γ \mapsto -γ \).

Problems marked with a * are bonus problems for extra credit.