**47)** Let $F$ be a field of characteristic $p$. (I.e. $\underbrace{1+\cdots+1}_{p \text{ times}} = 0$ in $F$.) Show that $(a+b)^p = a^p + b^p$. Conclude that the map $x \to x^p$ is a field automorphism of $F$.

**48)** Let $p$ be a prime, $n$ a natural number and $q = p^n$. Let $f(x) = x^{p^n} - x = x^q - x \in \mathbb{F}_p[x]$.
a) Suppose $E$ is a field with $q$ elements. Show that $f(\alpha) = 0$ for every element $\alpha \in E$.
b) Vice versa, suppose that $E$ is the splitting field of $f$ in a suitable algebraic closure of $\mathbb{F}_p$. Let $S = \{\alpha_0 = 0, \alpha_1 = 1, \alpha_2, \ldots, \alpha_{q-1}\}$ be the set of roots of $f$ in $E$. Show that $S$ itself is a field (and thus $E = S$). (You just need to show that sum/difference,product, quotient of two roots is again a root. Use problem 47!)
**Note:** This shows, that for every prime power $q$, there is — up to isomorphism — exactly one field with $q$ elements, namely the splitting field of $x^q - x$ over $\mathbb{F}_p$.

**49)** Let $E$ be the splitting field of $x^3-5$ over $\mathbb{Q}$ (cf. problem 44). Determine the field automorphisms of $E$. Which one is complex conjugation? Can you identify the group formed by them?

**50)** Let $E$ be the splitting field over $F$ of the polyonomial $f(x) \in F[x]$. Suppose that $f$ has degree $n$ and $f(x) = \prod_{i=1}^{n}(x - \alpha_i)$ over $E$.
a) Let $\varphi: E \to E$ be a field automorphism, fixing $F$. Show that $\varphi$ permutes the roots of $f$, i.e. that $\alpha_i^\varphi = \alpha_j$ for some $j$.
b) Show that this defies for each $\varphi \in \mathrm{Aut}(E/F)$ a permutation $\pi_\varphi \in S_n$. (It is sufficient to show that the map $\alpha_i^\varphi = \alpha_j$ is one-to-one.)
c) Show that the map $\gamma: \mathrm{Aut}(E/F) \to S_n$, $\varphi \mapsto \pi_\varphi$ is a homomorphism.
d) Show that $\ker \gamma$ is trivial. We can thus consider $\mathrm{Aut}(E/F)$ as a subgroup of $S_n$.
**Note:** One can show further that if $f$ is irreducible, the image of $\gamma$ must be *transitive*, i.e. it for any pair $i, j$ there exists an element $g$ such that $i^g = j$. GAP contains an algorithm for computing this image (up to labelling of the roots). For an irreducible rational polynomial `f`, the commands

```
t:=GaloisType(f);
g:=TransitiveGroup(Degree(f),t);
```

return the image group $g$. This can be used to determine abstract properties of the group (e.g. its cardinality), though it does not give actual field automorphisms.
For example

```
gap> f:=x^6+x^3+1;Factors(f); # check that the polynomial is irreducible
[ x^6+x^3+1 ]
gap> t:=GaloisType(f);
1
gap> g:=TransitiveGroup(Degree(f),t);
```

```
C(6) = 6 = 3[x]2
gap> Size(g); # test for some properties of the group
6
gap> IsAbelian(g);
true
gap> IsCyclic(g);
true
gap> f:=x^6+x^3-x+1;Factors(f);
x^6+x^3-x+1
[ x^6+x^3-x+1 ]
gap> t:=GaloisType(f);
16
gap> g:=TransitiveGroup(Degree(f),t);
S6
gap> Size(g);
720
```

**51*)** There are 5 classes of transitive groups of degree 4: $1 : \langle (1,2,3,4) \rangle \cong C_4$, $2 : \langle (1,2)(3,4), (1,3)(2,4) \rangle \cong V_4$, $3 : \langle (1,2,3,4), (1,3) \rangle \cong D_8$, $4 : \langle (1,2,3), (2,3,4) \rangle \cong A_4$, and $5 : \langle (1,2,3,4), (1,2) \rangle \cong S_4$. Using GAP, find polynomials of degree 4 that have each of these groups as `GaloisType`.

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