

**52) (4 points)** Let  $p = x^4 - 2$  and  $E$  be the splitting field of  $p$  over  $\mathbb{Q}$ .

a) Show that  $E = \mathbb{Q}(\sqrt[4]{2}, i)$  and express  $p$  as a product of linear factors over  $E$ .

b) Determine  $[E : \mathbb{Q}]$ .

c) Determine all field automorphisms of  $E$  over  $\mathbb{Q}$ .

d) For each automorphism determined in c), write the corresponding permutation of the roots of  $p$  (cf. problem 50).

e) Let  $G$  be the group generated by the permutations in d). (By the argument in problem 50, it is isomorphic to  $\text{Aut}(E/\mathbb{Q})$ .) Determine all subgroups of  $G$ , for example in GAP, you may use the command:

```
sub:=Union(List(ConjugacyClassesSubgroups(G),Elements));
```

f) Draw the lattice (i.e. inclusion relation) amongst the subgroups. (You can use for example the GAP commands `IsSubset(sub[5],sub[4])`; to test inclusion)

g) For each subgroup  $S \leq G$ , determine the corresponding subgroup  $T \leq \text{Aut}(E/\mathbb{Q})$  (use the translation from d)!) and  $\mathbb{Q} \leq (\text{Fix})(T) \leq E$ .

h) Sketch the inclusion relation amongst these subfields. Compare with f).

**53)** Determine the irreducible polynomials of degree dividing 4 over  $\mathbb{F}_2$  and show that their product is  $x^{16} - x$ .

(Hint: You can verify the result in GAP:

```
x:=X(GF(2),"x");
```

```
Factors(x^16-x);
```

**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  $x^{p^d} - x$  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  $x^{p^n} - x$  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  $\mathbb{F}_4 \not\leq \mathbb{F}_8 \not\leq \mathbb{F}_{16}$ .)

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