FIELD THEORY HOMEWORK SET IV SOLUTIONS

JAMES CUMMINGS

You may collaborate on this homework set, but must write up your solutions by yourself. Please contact me by email if you are puzzled by something, would like a hint or believe that you have found a typo.

(1) An *ordered field* is a field F together with a set $P \subseteq F$ of elements such that (defining $-P = \{-a : a \in P\}$)
   (a) P is closed under $+$ and $\times$
   (b) $P \cap -P = \{0\}$.
   (c) $P \cup -P = F$.

   Intuitively, you can think of P as the set of field elements which have been designated as non-negative.

   Prove that
   (a) There is a unique set $P \subseteq \mathbb{R}$ such that $(\mathbb{R}, P)$ is an ordered field.
   The non-negative reals form such a set, so one exists. Suppose that P is such a set. Then for $b \geq 0$, let $a = \sqrt{b}$. Either $a \in P$ or $-a \in P$ and in either case $b = a^2 = (-a)^2 \in P$. So P contains the non-negative reals, so easily it is equal to the non-negative reals.
   (b) There is no set $P \subseteq \mathbb{C}$ such that $(\mathbb{C}, P)$ is an ordered field.
   If P is such a set then either i or $-i$ is in P, so -1 is in P. Similarly 1 or -1 is in P so 1 is in P. Contradiction!
   (c) There are at least two sets $P \subseteq \mathbb{Q}(\sqrt{2})$ such that $(\mathbb{Q}(\sqrt{2}), P)$ is an ordered field.
   There are two embeddings of the field into the real numbers, namely $a + b\sqrt{2} \mapsto a \pm b\sqrt{2}$. Each one induces an ordering and they are different.
   (d) If (F, P) is an ordered field then F has characteristic zero and -1 is not a sum of squares in F.
   As we saw $1 \in P$. If the field has characteristic p then the sum of $p-1$ many 1's is in P, so -1 is in P. This is impossible so the characteristic is zero. Now -1 is not in P but any sum of squares is in P, hence -1 is not a sum of squares.

(2) Let F be a field extending the field E and let $a \in F$ be algebraic over E. Show that the following are equivalent:
   (a) a is separable over E.
   (b) There is a field F' extending E such that there exist $[E(a) : E]$ distinct monomorphisms $\sigma : E(a) \to F'$ with $\sigma \restriction E = id$.

   Suppose that a is separable and let F' be a splitting field for m_a^E over E. Then m_a^E has $deg(m_a^E) = [E(a) : E]$ distinct roots in F', and as usual these are possible values for $\sigma(a)$.

Conversely suppose that F' as above exists. Each value of $\sigma(a)$ is a root of m_a^E, so that polynomial has distinct roots in a field where it splits, hence it is separable.

(3) Let $f = x^4 - 2$.
   (a) Show that f is irreducible in $\mathbb{Q}[x]$.
   Eisenstein.
   (b) Find the complex roots of f, and show that f splits over the complex numbers.
   Let $\alpha = 2^{1/4}$, then the roots are αi^m for $0 \leq m < 4$.
   (c) Let E be the subfield of $\mathbb{C}$ generated by the roots of f (so that E is a splitting field for $\mathbb{Q}$). Find $[E : \mathbb{Q}]$.
   α has degree 4 over $\mathbb{Q}$. $i \notin \mathbb{Q}(\alpha)$ since α is real, so i has degree 2 over $\mathbb{Q}(\alpha)$. Hence $E = \mathbb{Q}(i, \alpha)$ has degree 8.
   (d) Compute the group $Aut(E/\mathbb{Q})$, and describe how each element of this group permutes the roots of f.
   Any member of the group moves i to $\pm i$ and α to $\pm\alpha, \pm i\alpha$. This gives 8 possibilities, all of which can occur.
   Label the roots clockwise in the complex plane so that α gets label 1, $i\alpha$ gets label 2, $-\alpha$ gets label 3, $-i\alpha$ gets label 4.
   Let σ be the AM which fixes α and exchanges $\pm i$. Let τ be the AM which fixes i and maps α to $i\alpha$.
   τ generates a group of order 4 where as permutations

$$\tau^0 = e, \tau = (1234), \tau^2 = (13)(24), \tau^3 = (1432).$$

   $\sigma = (24)$ and $\tau^\sigma = (1432) = \tau^3$, so we readily see that this is the dihedral group of order 8. Of course the other four elements are

$$\sigma = (24), \sigma\tau = (24)(1234) = (14)(23), \sigma\tau^2 = (13), \sigma\tau^3 = (24)(1432) = (12)(34)$$

   (e) Find all the subgroups of $Aut(E/\mathbb{Q})$ and their fixed fields.
   Possible orders are 2, 4 and 8.
   Order one: $H_1 = \{e\}$ with fixed field E.
   Order eight: $H_2 = Aut(E/\mathbb{Q})$ with fixed field $\mathbb{Q}$.
   Order two: each element of order two gives a subgroup of order two, whose fixed field will be an extension of degree four. We cheat a bit and use the easy fact that $Fix(H^\rho) = \rho[Fix(H)]$.
   $H_3 = \{e, \sigma\} = \{e, (24)\}$ has fixed field $\mathbb{Q}(\alpha)$.
   $H_4 = H_3^\tau = \{e, \sigma\tau^2\} = \{e, (13)\}$ has fixed field $\mathbb{Q}(i\alpha)$.
   Note that $\alpha^2 = \sqrt{2}$ and that τ^2 fixes this and i. It follows that:
   $H_5 = \{e, \tau^2\} = \{e, (13)(24)\}$ has fixed field $\mathbb{Q}(i, \sqrt{2})$. We note that H_5 is normal and corresponds to a Galois extension of $\mathbb{Q}$.
   Note that $\sigma\tau = (14)(23)$ moves α to $-i\alpha$ and $i\alpha$ to $-\alpha$, so i moves to $-i$. A little thought (actually I found it by a tedious linear algebra calculation using the obvious basis for E over $\mathbb{Q}$) shows that if $\beta = (1 - i)\alpha$ then β is fixed. More linear algebra (use the obvious basis again) shows that β has degree 4 over $\mathbb{Q}$, so the minimal polynomial is $x^4 + 8$.
   $H_6 = \{e, (14)(23)\}$ has fixed field $\mathbb{Q}(\beta)$.
   Now conjugating by $\tau = (1234)$ takes $(14)(23)$ to $(12)(34)$, and τ maps β to $\gamma = (1 + i)\alpha$.

$H_7 = \{e, (12)(34)\}$ has fixed field $\mathbb{Q}(\gamma)$.
Finally we think about subsgroups of order 4. They must either be cyclic or isomorphic to the Klen four group. Each one has fixed field an extension of degree 2.
It's readily seen that τ generates a cyclic group of order 4. Noting that τ fixes i we have
$H_8 = \{e, (1234), (13)(24), (1432)\}$ has fixed field $\mathbb{Q}(i)$.
Now there is also a subgroup
$H_9 = \{e, (13), (24), (1324)\}$. A little thought shows that the fixed field is $\mathbb{Q}(\sqrt{2})$.
Finally there is a subgroup $H_{10} = \{e, (12)(34), (13)(24), (14)(23)\}$. A little thought shows that the fixed field is $\mathbb{Q}(i\sqrt{2})$.

(4) Let F have characteristic p. Use the binomial theorem to show that the map $a \mapsto a^p$ is a monomorphism from F to F. Show that if F is finite this map is an automorphism of F, and in that case describe its fixed field.