FIELD THEORY HOMEWORK SET II

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) Let F be a field, and let $Aut(F)$ be the set of automorphisms of F.
   (a) Show that $Aut(F)$ forms a group under composition.
   Routine: the main point is that the inverse (as a function) of an AM is an AM.
   (b) Show that if $X \subseteq Aut(F)$ and we define $Fix(X) = \{a \in F : \forall \sigma \in X\ \sigma(a) = a\}$ then $Fix(X)$ is a subfield of F.
   Routine and covered in class.
   (c) Show that $Fix(X) = Fix(\langle X \rangle)$, where as usual $\langle X \rangle$ is the subgroup generated by X.
   Obviously $Fix(X) \supseteq Fix(\langle X \rangle)$. But conversely if $a \in Fix(X)$ then every product of elemnts of X and their inverses fixes a, so that $a \in Fix(\langle X \rangle)$.

(2) Let $E = \mathbb{Z}/2\mathbb{Z}$.
   (a) Find an irreducible element in $E[x]$ of degree 3.
   If a polynomial of degree 3 is not irreducible it has a linear factor. So it's enough to find a polynomial which vanishes nowhere. I'll use $x^3 - x + 1$.
   (b) Construct a finite field with 8 elements.
   Let $m = x^3 - x + 1$ and $F = E[x]/(m)$. As usual if $\alpha = x + (m)$ then $\{1, \alpha, \alpha^2\}$ is a basis.
   (c) Find all the subfields of the field you just constructed, and also find its automorphism group.
   $[F : E] = 3$ which is prime so there are (why?) no intermediate fields, and the subfields are E and F.
   $Aut(F)$ has order 3. A generator is given by the map which takes α to α^2 and fixes E.

(3) What is the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over each of the fields
   (a) $\mathbb{Q}$?
   (b) $\mathbb{Q}(\sqrt{2})$?
   (c) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$?
   Respectively: $x^4 - 10x^2 + 1$, $(x - \sqrt{2})^2 - 3$, $x - (\sqrt{2} + \sqrt{3})$.

(4) Let $\mathbb{Z}$ be a subring of S and let $a \in S$. a is *integral* over $\mathbb{Z}$ iff there is $g \in \mathbb{Z}[x]$ such that g is monic and $g(a) = 0$.

   Show that a is integral over $\mathbb{Z}$ iff $(\mathbb{Z}[a], +)$ is a finitely generated abelian group, where as usual $\mathbb{Z}[a] = \{f(a) : f \in \mathbb{Z}[x]\}$ is the least subring of S containing $\mathbb{Z} \cup \{a\}$.

$\mathbb{Z}$ is all $\mathbb{Z}$-linear combinations of powers of a. If a is integral then for some n we have an expression of a^n in terms of lower powers, and can argue that $\mathbb{Z}$ is all $\mathbb{Z}$-linear combinations of $\{a^j : j < n\}$.

Conversely if we have generators $f_1(a), \dots f_n(a)$ for f_i polynomials then let $N > \max(deg(f_i))$. Then a^N is a $\mathbb{Z}$-linear combination of $f_1(a), \dots f_n(a)$ and so easily a is integral.

(5) Prove that if $f \in \mathbb{R}[x]$ has odd degree then f has at least one root. Hint: use calculus.

WLOg f is monic. The leading term dominates so $f(x)$ is large and positive (resp negative) for x large and positive (resp negative). Now use the intermediate value theorem.

(6) Prove that $\mathbb{Z}[x]$ is not a PID. (Harder) What are the prime ideals?

The ideal $(2, x)$ is not principal.

Other part is hard, here is a sketch. Let P be prime. Argue using primeness that P is generated by irreducibles. $P \cap \mathbb{Z}$ is prime so is (0) or (p) for prime p. If it is (p) then reduce mod p, and argue that $P = (p)$ or $P = (p, g)$ for irreducible g which remains irreducible when we reduce mod p. If it is (0) then argue $P = (g)$ for irreducible g.

(7) Prove that $\mathbb{C}$ is a vector space over $\mathbb{R}$. What is its dimension? Find a basis. For each $z \in \mathbb{C}$ prove that the map which takes a to za is linear; also find its trace and determinant.

Dimension is 2, basis is $\{1, i\}$. Routine to see that map is linear. If $z = c + di$ then express wrt the standard basis to see that the trace is $2c$ and the determinant is $c^2 + d^2$.