M345P11 Galois Theory, Progress Test 1, 4/11/2013, solutions.

Q1.

(a) This is standard bookwork. Say $f = gh$ with $g, h \in \mathbf{Q}[x]$. Clear denominators and get $Df = g_0h_0$ with $g_0, h_0 \in \mathbf{Z}[x]$ and $D \in \mathbf{Z}_{>0}$. If we can prove that for any prime $p|D$ we have that either all the coefficients of g_0 are multiples of p, or all the coefficients of h_0 are, then we're home (by induction on D). So say $p|D$. Reducing modulo p (and putting a bar on top of things to denote the reduction) we have $\overline{g_0}\,\overline{h_0} = 0 \in (\mathbf{Z}/p\mathbf{Z})[x]$. Those that know $(\mathbf{Z}/p\mathbf{Z})[x]$ is an integral domain can now just say "…and hence $\overline{g_0} = 0$ or $\overline{h_0} = 0$ and now we're done"; those of you who know less ring theory can argue more prosaically (as I did in lectures) thus: if it's not true that p divides all the coefficients of $g_0 = \sum a_i x^i$ then choose i as small as possible such that $p \nmid a_i$. Similarly if p doesn't divide all the b_j in $h_0 = \sum_j b_j x^j$ then choose j as small as possible such that $p \nmid b_j$; now an explicit calculation shows that p doesn't divide the coefficient of x^{i+j} in g_0h_0 either – a contradiction. Four marks for this piece of standard algebra.

(b) Eisenstein's criterion says that if q is a prime and if $p(x) = \sum_{i=0}^{n} a_i x^i \in \mathbf{Z}[x]$ is a polynomial, such that $q \nmid a_n$, $q|a_i$ for $i < n$ and $q^2 \nmid a_0$, then $p(x)$ is irreducible. One mark.

(c) One mark each.

(i) Irreducible by Eisenstein ($q = 17$).

(ii) Reducible: $(x - \sqrt[8]{17})$ is a factor.

(iii) Reducible: $p(1) = 0$ so $(x - 1)$ is a factor of p.

(iv) This is irreducible, because it's cubic so if it were reducible then one factor will have to be linear – however neither $x = 0$ nor $x = 1$ are roots and those are the only possibilities in such a small field.

(v) This is reducible and indeed a cube – it's $(x^2 + x + 2)^3$.

Q2.

(a) The degree $[F : E]$ is the dimension of F considered as a vector space over E. One mark. The extension $\mathbf{C}/\mathbf{Q}$ has infinite degree, because if it were finite then $\mathbf{C}$ would be isomorphic to $\mathbf{Q}^n$ as a vector space and hence countable, which it isn't. One mark.

(b) If $E \subseteq F \subseteq K$ are fields, then $[K : E] = [K : F][F : E]$. I stated and proved this in lectures only for the case $[K : E]$ finite, and it's fine if you stick to this case. One mark.

(c) For a to be algebraic over E we need a non-zero polynomial $p(x) \in E[x]$ such that $p(a) = 0$. But $[F : E] = n$ is finite, so there's an E-linear relation between the $n + 1$ numbers $1, a, a^2, \ldots, a^n$, and this gives the polynomial we seek. One mark.

If the min poly of a over E has degree d, and if $L = E(a) \subseteq F$, then a result from lectures says that $[L : E] = d$, so $[F : E] = [F : L][L : E]$ has degree a multiple of d. One mark.

(d) Let's use the tower law. Set $F = \mathbf{Q}(\sqrt{5}, \sqrt{11})$, set $K = \mathbf{Q}(\sqrt{5})$ and set $E = \mathbf{Q}$. Then $[K : E]$ must be 2, because $x^2 - 5$ is irreducible (as $\sqrt{5} \notin \mathbf{Q}$). And similarly $[F : K] = 2$ as $F = K(\sqrt{11})$ and the min poly of $\sqrt{11}$ over K must be $x^2 - 11$, as $\sqrt{11} \notin K$. So by the tower law $[F : E] = 4$. Two marks.

(e) We have $[F : E] = 2$ and $1 \in E \subseteq F$; extend to a basis $\{1, b\}$ of F as an E-vector space. Then $b^2 \in F$ so $b^2 = \lambda b + \mu$ with $\lambda, \mu \in E$. Completing the square we see that if $a = b - \lambda/2$ then $a^2 \in E$, but $a \notin E$ as $b \notin E$, so $F = E(a)$ as $E(a)$ is strictly bigger than E so has E-dimension at least 2, but it is contained in a space of dimension 2 and is hence equal to it. Two marks.

(f) If $F = E(a)$ then certainly $a \notin E$ (as $[F : E] = 2$ so F is strictly bigger than E). But if $a^2 \in E$ then a is either a root of $x^2 = 0$ or $x^2 - 1 = 0$ and both of these polynomial factor into linear factors over E, so all their roots are in E, and hence $a \in E$, a contradiction! One mark.