KMB, November 29, 2013

M3P11 Galois Theory, Solutions to Problem Sheet 5

1. $(x-\alpha)^n = \sum_i \binom{n}{i}\alpha^{n-i}x^i$ so $D((x-\alpha)^n) = \sum_i \binom{n}{i} i\alpha^{n-i}x^{i-1}$; now $\binom{n}{i}i = \binom{n-1}{i-1}n$ and the result follows easily.

2. We need to check that K is algebraically closed (which is given) and that it's algebraic over E, which is true because algebraic over algebraic is algebraic.

3. By 6.7, we only need to check $[K:E] = [K:E]_s$. But $[K:E] = [K:F][F:E] = [K:F]_s[F:E]_s = [K:E]_s$ (by the tower law, 6.7 and 6.6 respectively) so we're home.

4.

(i) $k(s,t)$ is a field; the addition of two ratios-of-polynomials can be done by putting them over a common denominator (e.g. the product) and multiplication is even easier. All the axioms of a ring follow (by clearing denominators) from the fact that they are true for the two-variable polynomial ring $k[s,t]$, and it's clear that anything non-zero has an inverse – the inverse of f/g is g/f.

Any subfield of $k(s,t)$ containing k, s and t must contain any polynomial $f(s,t) \in k[s,t]$; because it's a field it also contains $1/g(s,t)$ if $g \neq 0$, and so must be $k(s,t)$.

(ii) Set $K = E(s) = k(s,t^p)$. Then $F = K(t)$ and I claim $[F:K] = [K:E] = p$, which suffices (by the tower law). We have $[F:K] = [K(t):K]$ which will be the degree of the minimum polynomial of t over K. I claim that this min poly is $x^p - t^p$; indeed clearly t is a root of this, and over F this poly factors as $(x-t)^p$, so any monic irreducible factor of it over K must be $(x-t)^i$ for some i; but this polynomial has constant term t^i which is not in K unless $i = 0$ or $i = p$; hence $x^p - t^p$ is irreducible over K. Similarly $x^p - s^p$ is irreducible over E and $[K:E] = p$.

(iii) If $\lambda = f(s,t)/g(s,t) \in F$ then $\lambda^p = f(s^p,t^p)/g(s^p,t^p) \in E$. In particular the degree of the min poly of λ over E must be at most p, so $[E(\lambda):E] \leq p < p^2$ and hence $E(\lambda) \neq F$.

(iv) Say $E_\gamma = E_\delta$. Then $s + \delta t \in E_\gamma$, and hence E_γ is a field containing k, $s + \gamma t$ and $s + \delta t$; if $\gamma \neq \delta$ then looking at linear combinations we see that E_γ contains s and t too, so $E_\gamma = F$. However this is impossible as $[F:E] = p^2$ from (ii) and $[E_\gamma : E] \leq p$ from (iii). So if $\delta \neq \gamma$ then $E_\delta \neq E_\gamma$ and we're done.

5. The polynomial $x^2 - e$ must be irreducible over E, as if it factored the factors would be linear and of the form $x - d$ with $d^2 = e$; however no such λ exists in E, by assumption. Let's adjoin one root of this polynomial to E and get $E(\sqrt{e}) = E[x]/(x^2 - e)$. This bigger field now contains one and hence both roots of $x^2 - e$, so it's the splitting field F of E, hence $[F:E] = 2$ (the degree of $x^2 - e$). In particular F/E is finite. It's a splitting field, so it's normal. The map $\tau : F \to F$ sending $a + b\sqrt{e}$ to $a - b\sqrt{e}$ is easily checked to be a field isomorphism, so $[F:E]_s \geq 2 = [F:E]$ and hence F/E is separable. Hence the extension is Galois; thus the Galois group must have size 2, and we can see two elements, namely the identity and τ, and $\mathrm{Gal}(F/E) = \{1, \tau\}$ is isomorphic to the cyclic group of order 2.

6. Let's start by adjoining one root of $x^4 - p$, say, α, the positive real 4th root of p. We get a field $K = \mathbb{Q}(\alpha)$. By Eisenstein, $x^4 - p$ is irreducible over $\mathbb{Q}$, so $[K:\mathbb{Q}] = 4$. Is K a splitting field though? No, because it's a subfield of the reals, and $x^4 - p$ has some non-real roots (namely $\pm i\alpha$). However K does contain two roots of $x^4 - p$, namely $\pm\alpha$, so $x^4 - p$ must factor as $(x+\alpha)(x-\alpha)q(x)$, with $q(x) \in K[x]$ of degree 2 and irreducible (as no roots in K). If $\beta = i\alpha$ is a root of $q(x)$ and $F = K(\beta)$ then $[F:K] = 2$ so $[F:\mathbb{Q}] = 8$ by the tower law. We can alternatively write $F = K(i)$ as $\beta = i\alpha$, so $F = \mathbb{Q}(i,\alpha)$.

F is a splitting field over $\mathbb{Q}$ so it's finite and Galois (separability isn't an issue as we're in characteristic 0). So we know $\mathrm{Gal}(F/\mathbb{Q})$ has size 8. We also know that if $\tau : F \to F$ is an isomorphism then $\tau(\alpha)$ had better be a 4th root of $\tau(p) = p$, so it's $\pm\alpha$ or $\pm i\alpha$; there are at most 4 choices for $\tau(\alpha)$. Similarly $\tau(i) = \pm i$ so there are at most 2 choices for $\tau(i)$. This gives at most 8 choices for τ; however we know that $\mathrm{Gal}(F/\mathbb{Q})$ has size 8, so all eight choices must work. It is not hard now to convince yourself that $\mathrm{Gal}(F/\mathbb{Q})$ is isomorphic to D_8 (think of a square with corners labelled $\alpha, i\alpha, -\alpha, -i\alpha$).

7. We know $x^p - 1 = (x-1)(1 + x + x^2 + \cdots + x^{p-1})$, and $f(x) := 1 + x + x^2 + \cdots + x^{p-1}$ is irreducible over $\mathbb{Q}$ (by the trick just after Eisenstein in lectures). Hence if $\zeta = e^{2\pi i/p}$ then $f(x)$

must be the min poly of ζ. Note that the roots of $p(x)$ are just the roots of $x^p - 1$ other than $x = 1$, so they're ζ^j for $1 \leq j \leq p-1$. Moreover if $F = \mathbb{Q}(\zeta)$ then $[F : \mathbb{Q}] = \deg(f) = p - 1$, and K contains ζ^j for all j, so $x^p - 1$ splits completely in K. Hence K is the splitting field of $x^p - 1$ and it has degree $p - 1$.

Now $F/\mathbb{Q}$ is finite, normal and separable, so it's Galois, so by 6.3 we know $\mathrm{Gal}(F/\mathbb{Q})$ will have size $p - 1$. If $\tau \in \mathrm{Gal}(F/\mathbb{Q})$ then, because $F = \mathbb{Q}(\zeta)$, τ is determined by $\tau(\zeta)$, which is a root of $\tau(f) = f$, so is ζ^j for some $1 \leq j \leq p - 1$. It's not immediately clear that, given j, some field automorphism τ of F sending ζ to ζ^j will exist – but it has to exist because we know there are $p - 1$ field automorphisms by 6.3. So the elements of the Galois group can be called τ_j for $1 \leq j \leq p - 1$. The remaining question is what this group is. We can figure out the group law thus: $\tau_i \circ \tau_j$ – where does this send ζ? Well $\tau_j(\zeta) = \zeta^j$, and $\tau_i(\zeta) = \zeta^i$ so $\tau_i(\zeta^j) = \zeta^{ij}$ as τ_i is a field homomorphism. Note finally that ζ^{ij} only depends on ij mod p, as $\zeta^p = 1$. So if we identify $\mathrm{Gal}(F/\mathbb{Q})$ with $\{1, 2, \ldots, p-1\}$ then the group law is just "multiplication mod p" , and we see $\mathrm{Gal}(F/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$.