Homework set # 8

Due on 3/20

Cubics

1. Verify that the splitting fields of $f = x^3+ax^2+bx+c$ and $g = y^3+py+q$ (where g is obtained using the substitution $x = y-a/3$ where $p = (1/3)(3b-a^2)$ and $q = (1/27)(2a^3-9ab+27c)$) over $\mathbb{Q}$ are the same by showing that their roots differ by $a/3$ which is an element of $\mathbb{Q}$.

2. Let K be a cyclic extension of a field F (i.e. it's Galois group over F is a cyclic group) of degree p where F contains the p-th roots of unity (where p is a prime). Let $\alpha \in K$ and let ω be any p-th root of unity and let σ be the generator of $\mathrm{Gal}(K/F)$. Define the Lagrange Resolvent to be $(\alpha, \omega) = \alpha + \omega\sigma(\alpha) + \omega^2\sigma^2(\alpha) + \cdots + \omega^{p-1}\sigma^{p-1}(\alpha)$ Show that $(\alpha, \omega)^p$ is fixed by $\mathrm{Gal}(K/F)$. Moreover, show that if $\omega \neq 1$ then σ^i does not fix (α, ω) for any $i < p$, so that $F((\alpha, \omega)) = K$ (i.e that $F((\alpha, \omega))$ does not lie in some subfield of K).

3. Let $g = x^3 + px + q$ where $p, q \in \mathbb{Q}$ be an irreducible cubic over $\mathbb{Q}$. Observe that if $\alpha, \beta, \gamma \in \mathbb{C}$ are the roots of g that $Q(\alpha, \beta, \gamma)$ is the splitting field for g (note this field might be able to be generated with fewer elements but this field is at least the splitting field for g).

(a) Let $F = \mathbb{Q}(\omega)$ where ω is a 3-rd root of unity (which is not equal to 1) so that $\omega^2 + \omega + 1 = 0$. Show ω cannot be a root of g and so g is irreducible over F as well. Conclude the splitting field of g over F is $K = F(\alpha, \beta, \gamma)$. In particular this shows that the analysis that we did concerning Galois groups of g over $\mathbb{Q}$ is equivalent to computing Galois groups of g over F.

(b) Show that if α, β, γ are roots of g then $\alpha + \beta + \gamma = 0$.

(c) Let D be the discriminant of g, show that over the field $F(\sqrt{D})$ the Galois group of g is A_3 (hint: you know that the Galois group of g over F is either A_3 or S_3 by part (a)). Conclude that the splitting field K of g over F is a cyclic extension of $F(\sqrt{D})$ of degree 3 and as such is a Kummer extension of $F(\sqrt{D})$.

(d) Consider the elements $\theta_1 = \alpha + \omega\beta + \omega^2\gamma$ and $\theta_2 = \alpha + \omega^2\beta + \omega\gamma$ (note these are Lagrange Resolvents). Show that $\theta_1+\theta_2 = 3\alpha$, $\omega^2\theta_1+\omega\theta_2 = 3\beta$, and that $\omega\theta_1+\omega^2\theta_2 = 3\gamma$.

(e) Show that either θ_1 or θ_2 generates the splitting field K of g over $F(\sqrt{D})$ (hint: look at problem 2).

(f) Show that θ_1^3 and θ_2^3 are elements in $F(\sqrt{D})$ (hint: you should get at the end that $\theta_1^3 = (-27/2)q+(3/2)\sqrt{-3D}$ and that $\theta_2^3 = (-27/2)q-(3/2)\sqrt{-3D}$ note that $\omega-\omega^2 = \sqrt{-3}$). (Hint: You might want to expand everything out in terms of $\omega, \alpha, \beta, \gamma$ and use symmetric polynomials to help you reduce back to having coefficients from g).

(g) Show that $\theta_1\theta_2 = -3p$. (Note you should be able to check this using either the initial definitions of θ_1 and θ_2 or using θ_i equal to the cube root of the expression found in part (d) for θ_i^3 and the formula for the discriminant of the cubic, in particular the cube roots one chooses in order to find θ_1 and θ_2 should satisfy this condition). Conclude that K can be generated by either θ_1 or θ_2.

(h) Part (g) implies that since $\alpha, \beta, \gamma \in K$ they can be expressed in terms of θ_1 and θ_2. Using the results of part (c), solve for α, β, γ in terms of cube roots of the expressions found in part (d). Show that these are in fact roots of g.

(i) Now if g is not irreducible over $\mathbb{Q}$, explain how you would find the roots using the coefficients of g. Check what you get here with what the formulas in part (h) give you.

Congratulations, you have derived Cardano's formula...go challenge people to competitions where you solve cubics!

Quartics

4. Show that the discriminant for the resolvent cubic $h = x^3 - 2px^2 + (p^2 - 4r)x + q^2$ is the same as the discriminant of $g = y^4 + py^2 + qy + r$. Recall h has roots $\theta_1 = (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4), \theta_2 = (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4)$, and $\theta_3 = (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3)$ where $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ are all roots of g.

5. Let f be an irreducible quartic in $\mathbb{Q}[x]$. Prove that if $\mathrm{Gal}(f) = C_4 = \mathbb{Z}/4\mathbb{Z}$ then the discriminant of f is greater than 0. From this deduce that in the cases where $\mathrm{Gal}(f)$ is either C or D_4 that if the discriminant of f is less than 0 that $\mathrm{Gal}(f) = D_4$.