Assignment 4 – All 2 parts – Math 612

Due in class: Thursday, Feb. 11, 2016

(1) Let $f(x)$ be an irreducible quartic polynomial over a field F of characteristic $\neq 2$ and let Δ be the discriminant of f. Show that if $\mathrm{Gal}(f) \cong D_4$, then $f(x)$ is irreducible over $F(\sqrt{\Delta})$. (Hint: this is equivalent to showing that $F(\alpha) \not\supseteq F(\sqrt{\Delta})$, where α is a root of f, so you can just show these two extensions correspond to subgroups H and H' of D_4 such that $H \not\subseteq H'$.) (Note that this finishes up the determination of the Galois group of an irreducible quartic; see §14.6 of Dummit–Foote for a more conceptual explanation of the difference between C_4 and D_4.)

(2) Wreath products. We'll use this shortly in class. We've been talking about Galois groups G with come equipped with a fixed embedding into S_n (for some n) from the action on the roots of a polynomial. There's a name for this: by a *permutation group* we mean a group G together with a G-set X, equivalently, a group G together with an embedding into S_X, the permutations of X. So, a permutation group is more than just a group, it's a group thought of in a concrete way as acting on some specified set. Still, one will often refer to the pair (G, X) as simply G.

Given two permutation groups (G, X) and (H, Y), we will define another permutation group called the *wreath product of* G *and* H, and denoted $(G \wr H, X \times Y)$, as follows. Assume that X is a *right* G-set and that Y is a *right* H-set, and so denote the action of $g \in G$ on $x \in X$ by x^g and similarly for H and Y.

(a) Let $\mathrm{Map}(Y, G)$ be the set of functions from Y to G (which you can also think of as $\prod_{y \in Y} G$). Note that this is a group, where $(f_1 f_2)(y) = f_1(y) f_2(y)$. Then, H acts on $\mathrm{Map}(Y, G)$ on the *left* by

$$(h \cdot f)(y) = f(y^h)$$

(from the point of view of the direct product, this is just permuting the indices). Thus, we get a group $G \wr H := \mathrm{Map}(Y, G) \rtimes H$. Show that $G \wr H$ acts on $X \times Y$ on the *right* by

$$(x, y)^{(f,h)} := (x^{f(y)}, y^h),$$

where $f \in \mathrm{Map}(Y, G)$ and $h \in H$.

(b) Consider the case $G = H = X = Y = C_2$ (where C_2 acts on C_2 by left multiplication). Show that $G \wr H \cong D_4$ and that the action of $G \wr H$ on

$X \times Y = C_2 \times C_2$ is faithful and transitive. This gives another way of seeing D_4 as a transitive subgroup of S_4 (it's the same one we've seen already, just a more complicated approach!). (Hint: it's probably easier here to think of $\mathrm{Map}(Y, G)$ as simply $C_2 \times C_2 = V_4$ and the generator of $H = C_2$ acting on $C_2 \times C_2$ by switching the coordinates. Recall that $C_2 \times C_2 = \mathrm{Map}(Y, G)$ will be a normal subgroup of $G \wr H = (C_2 \times C_2) \rtimes C_2$.)

(c) More generally, let p be a prime and let $G = H = X = Y = C_p$ (where C_p acts on itself by left multiplication). Show that the action of $G \wr H$ on $X \times Y$ is again faithful and transitive. Conclude that $C_p \wr C_p$ can be considered as a (transitive) subgroup of S_{p^2}. Show that it is the Sylow p-subgroup of S_{p^2}. (Hint: for the last part, what is the power of p in the factorization of $(p^2)!$? And what is the order of $C_p \wr C_p$?)

(3) Let K/F be a (finite) Galois extension with Galois group G. Let $H \leq Z(G)$ and let $E = K^H$.

(a) Explain why E/F is Galois.

(b) Let $\overline{G} := \mathrm{Gal}(E/F)$. For $\overline{g} \in \overline{G}$ and $h \in H$, let $g \in G$ be any lift of $\overline{g}$ and define $\overline{g} \cdot h := ghg^{-1}$. Show that this gives a well-defined action of $\overline{G}$ on H.

(4) Numbers of the form $\sqrt{a + b\sqrt{d}}$.

(a) First off, let K/F be a degree 4 extension with Galois closure $\widetilde{K}$ and let $G = \mathrm{Gal}(\widetilde{K}/F)$. Show that K/F has a non-trivial intermediate (quadratic) extension if and only if $G = D_4, V_4$, or C_4. (Hint: for A_4, you can simply show if has no index 2 subgroup. For S_4, which has a unique index 2 subgroup, you need to show its fixed field is not in K.)

(b) Now, suppose $K/\mathbf{Q}$ is a quartic extension and $G = D_4, V_4, C_4$. By part (a), there is at least one intermediate quadratic extension, which we will denote $K_2 = \mathbf{Q}(\sqrt{d})$. Then, that means that $K = K_2(\sqrt{a + b\sqrt{d}}) = \mathbf{Q}(\sqrt{a + b\sqrt{d}})$ for some non-square element $a + b\sqrt{d} \in K_2$. Now, suppose you are given three rational numbers $a, b, d \in \mathbf{Q}$ with d not a square and you want to figure out $\mathbf{Q}(\alpha)$ for $\alpha = \sqrt{a + b\sqrt{d}}$. First, you can find a degree four polynomial $f(x) \in \mathbf{Q}[x]$ that has α as a root as in class:

$$\alpha^2 = a + b\sqrt{d}$$
$$(\alpha^2 - a)^2 = b^2 d,$$

so α is a root of $f(x) = x^4 - 2ax^2 + a^2 - b^2 d$. Show that the roots of $f(x)$ are $\pm\alpha$ and $\pm\beta$, where $\beta = \sqrt{a - b\sqrt{d}}$.

(c) But here's the thing, $a + b\sqrt{d}$ may be a square in $\mathbf{Q}(\sqrt{d})$, so $f(x)$ may not be irreducible and $\mathbf{Q}(\alpha)/\mathbf{Q}$ won't be degree 4. In this case, explain why $\mathbf{Q}(\alpha) = \mathbf{Q}(\sqrt{d})$.

(d) Let $\alpha = \sqrt{3 + 2\sqrt{2}}$. Show that its $f(x)$ is reducible and factor it (over $\mathbf{Q}$). Use this to rewrite α in the form $m + n\sqrt{r}$, for $m, n, r \in \mathbf{Q}$.

(e) From now on, suppose $K = \mathbf{Q}(\alpha)/\mathbf{Q}$ is degree 4. Show that the discriminant of f is $2^8 b^4 d^2 (a^2 - b^2 d)$ and conclude that $K/\mathbf{Q}$ has Galois group V_4 if and only if $a^2 - b^2 d$ is a square in $\mathbf{Q}$ if and only if $\alpha\beta \in \mathbf{Q}$. (Hint: you know the four roots of f.)

(f) From now on, let $a' = -2a$ and $b' = a^2 - b^2 d$. Prove that $G = C_4$ if and only if $b'(a'^2 - 4b')$ is a square in $\mathbf{Q}$ if and only if $\mathbf{Q}(\alpha\beta) = \mathbf{Q}(\alpha^2)$.

(g) Prove that $G = D_4$ if and only if neither b' nor $b'(a'^2 - 4b')$ are squares in $\mathbf{Q}$ if and only if $\alpha\beta \notin \mathbf{Q}(\alpha^2)$.