Math 603 Assignment 12, 2020-21

Part I. From Gallier–Shatz:

- problem 127 (This problem is related to the two problems in part III.)
- problem 126
- problem 129
- problem 131, part 4
- (extra credit) problem 132

Part II. The questions in this part belong to the old "theory of equations" for cubic and quartic polynomials. The groups involved are subgroups of S_3 and S_4, hence solvable.

1. Let k be a field such that $2 \in k^\times$. Let

$$f(T) = T^3 + a_1T^2 + a_2T + a_3$$

be a cubic polynomial in $k[T]$. Fix an algebraic closure k^{a} of k. Let

$$f(T) = (T-\alpha_1)(T-\alpha_2)(T-\alpha_3), \quad \alpha_1, \alpha_2, \alpha_3 \in k^{\mathrm{a}},$$

and let $E_{f(T)} := k(\alpha_1, \alpha_2, \alpha_3)$ be the splitting field of $f(T)$ in k^{a}. Let

$$D_{f(T)} = (\alpha_1-\alpha_2)^2(\alpha_2-\alpha_3)^2(\alpha_1-\alpha_3)^2$$

be the discriminant of $f(T)$. Similarly, for a quartic polynomial

$$g(T) = T^4 + b_1T^3 + b_2T^2 + b_3T + b_4 \in k[T],$$

factor $g(T)$ as

$$g(T) = \prod_{i=1}^{4}(T-\beta_i), \quad \beta_1, \beta_2, \beta_3, \beta_4 \in k^{\mathrm{a}},$$

and let

$$D_{g(T)} := \prod_{1\le i<j\le 4} (\beta_i - \beta_j)^2 \in k^\times.$$

Note that the Galois group of the splitting field of $f(T)$ is contained in the alternation group $A_3 \subseteq S_3$ if and only $D_{f(T)} \in (k^\times)^2$; and the Galois group of the splitting field of $g(T)$ is contained in the alternation group $A_4 \subseteq S_4$ if and only $D_{f(T)} \in (k^\times)^2$. The assumption that the characteristic of the field k is different from 2 is used in this statement.

(a) Find an explicit expression of $D_{f(T)}$ in terms of the coefficients $a_1, \ldots, a_3$ of $f(T)$, and an explicit expression of $D_{g(T)}$ in terms of the coefficients $b_1, \ldots, b_4$ of $g(T)$.

Note: The computations are a bit tedious. The formulas are classical, which you can easily find, at least when $a_1 = 0$ and $b_1 = 0$. The polynomial $D_{f(T)}$ in the a_j's is homogeneous of degree 6, while $D_{g(T)}$ is homogeneous of degree 12, if a_j and b_j are given weight j for each j.

(b) Suppose that $f(T)$ is separable and irreducible in $k[T]$. Let $E_{f(T)} := k(\alpha_1, \alpha_2, \alpha_3)$ be the splitting field of $f(T)$.

(b1) Let $\delta_{f(T)} := (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_1 - \alpha_3)$. Show that $f(T)$ is irreducible in $k(\delta)[T]$ and $[E_{f(T)} : k(\delta)] = 3$.

(b2) Show that $\mathrm{Gal}(E_{f(T)})/k$ is isomorphic to S_3 if $D_{f(T)} \notin (k^\times)^2$.

(b3) Show that $\mathrm{Gal}(E_{f(T)})/k$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}$ if $D_{f(T)} \in (k^\times)^2$.

2. We recall the discussion on Friday March 5th about the Galois group of the splitting field E/k of a separable irreducible quartic polynomial

$$g(T) = T^4 + b_1T^3 + b_2T^2 + b_3T + b_4 \in k[T].$$

- Write $g(T) = \prod_{i=1}^4 (T - \beta_i)$, where $\beta_1, \beta_2, \beta_3, \beta_4$ are four distinct elements of an algebraic closure k^{a} of k.
- Let $E = k(\beta_1, \beta_2, \beta_3, \beta_4)$ be the splitting field of $g(T)$, and let $G = \mathrm{Gal}(E/k)$.
- The solvable group $S_4 = \mathrm{Perm}(\{\beta_1, \beta_2, \beta_3, \beta_4\})$ has a composition series

$$S_4 \rhd A_4 \rhd V_4 \rhd C \rhd \{1\},$$

where $V_4 = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$ is the normal subgroup of S_4 isomorphic to $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, and C is one of the three cyclic subgroups of V_4 of order 2. This gives rize to a composition series

$$G \rhd (G \cap A_4) \rhd (G \cap V_4) \rhd (G \cap C) \rhd \{1\}$$

of G.

- Let $\delta := \prod_{1 \le i < j \le 4} (\beta_i - \beta_j)$, and let $D = D_{g(T)} := \delta^2 \in k$ be the discriminant of $g(T)$. We explained that the subfield $E^{(G \cap A_4)}$ corresponding to $G \cap A_4$ is equal to $k(D)$. In particular $G \subseteq A_4$ if and only if $D \in (k^\times)^2$.
- Let $\gamma_1 := \beta_1\beta_2 + \beta_3\beta_4$, $\gamma_2 := \beta_1\beta_3 + \beta_2\beta_4$, $\gamma_3 := \beta_1\beta_4 + \beta_2\beta_3$. Let $\theta_1 := (\beta_1 + \beta_2)(\beta_3 + \beta_4)$, $\theta_2 := (\beta_1 + \beta_3)(\beta_2 + \beta_4)$, $\theta_3 := (\beta_1 + \beta_4)(\beta_2 + \beta_3)$.

(a) Show that the subfield $E^{(G \cap V_4)} =: L$ of E corresponding to $G \cap V_4$ is equal to $k(\gamma_1, \gamma_2, \gamma_3)$.

(It may help to verify first that $\gamma_1, \gamma_2, \gamma_3$ are mutually distinct.)

(b) Show that $k(\gamma_1, \gamma_2, \gamma_3) = k(\theta_1, \theta_2, \theta_3)$.

(c) Show that the subfield $E^{(G \cap \{\mathrm{id}, (12)(34)\})}$ of E corresponding to the subgroup $G \cap \{\mathrm{id}, (12)(34)\}$ of G is equal to $L(\beta_1 + \beta_2, \beta_1\beta_2)$.

(d) We did in class a complete classification of subgroups of S_4 acting transitively on $\{1, 2, 3, 4\}$; such a subgroup is one of: S_4, A_4, V_4, a Sylow 2-subgroup, or a cyclic group of order 4 generated by a 4-cycle. Prove the following.

  - If $[L : k] = 6$, then $G = S_4$.
  - If $[L : k] = 3$, then $G = A_4$.

– If $[L:k]=1$, then $G=V_4$.
– If $[L:k]=2$, then G is either a Sylow 2-subgroup of S_4 or cyclic of order 4.

(This is an easy consequence of the classification of transitive subgroups $H \subseteq S_4$, by examining the image of H in S_4/V_4, as explained in class. The next question looks at $H \cap V_4$.)

(e) Suppose that $[L:k]=2$. Show that G is a Sylow 2-subgroup of S_4 if and only if $g(T)$ is irreducible in $L[T]$.

3. We further explore the question of "solving a irreducible quartic polynomial equation by radicals", in the setting of problem 2.

(a) Show that $(T-(\beta_1+\beta_2))\cdot(T-(\beta_3+\beta_4)) \in k(\theta_1)[T]$ and find this quadratic polynomial explicitly. (Your answer will involve some coefficients of $g(T)$.)

(b) Show that both cubic polynomials $R_1(T) := \prod_{j=1}^3 (T-\gamma_j)$ and $R_2(T) := \prod_{j=1}^3 (T-\theta_j)$ are elements of $k[T]$. Compute them explicitly in terms of the coefficients of $g(T)$.

(Often one assumes that the characteristic of the field k is not 2, therefor after changing T to $T-\frac{1}{4}b_1$ one may assume that $b_1=0$. Both $R_1(T)$ and $R_2(T)$ are called *cubic resolvent polynomials* of $g(T)$; their coefficients are given by homogeneous polynomials in b_1, b_2, b_3, b_4 if b_j is given weight j for $j=1,\dots,4$.)

(c) The composition series for G gives rise to three towers of sub-extension fields

$$k = E^G \subseteq E^{G\cap A_4} \subseteq L = E^{G\cap V_4} \subseteq E^{G\cap C} \subseteq E,$$

one for each of the three nontrivial subgroup C of V_4. In each tower, every immediate field extension is Galois with Galois group a subgroup of $\mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/3\mathbb{Z}$.

Assume that $6 \in k^\times$ and T^3-1 splits in $k[T]$. Explain how the above considerations produce "explicit formulas" for the roots of a quartic polynomial,.

(Hint: The assumption that $6 \in k^\times$ and T^3-1 splits in $k[T]$ implies that every such immediate field extension can be obtained by adjoining either a square root or a cubit root. The resulting formulas are quite clean if $b_1=0$; old books on the "theory of equations" devote a whole chapter with such forumlas. Note that this assumption is not "absolutely necessary": you just say "adjoin a root of this quadratic/cubic polynomial" instead of "adjoin a square/cubic root of this element".)

4. Let K be a field of characteristic 2, and let $h(T)=x^3+ax+b \in K[T]$ be an irreducible element of $K[T]$. Prove that the Galois group of the splitting field of $h(T)$ is A_3 or S_3 according to whether the quadratic polynomial $Y^2+bY+a^3+b^2 \in K[T]$ has a root in K or not.

(Hint: The two roots η_1, η_2 of $Y^2+bY+a^3+b^2$ are polynomials in the three roots of $h(T)$ which are fixed by every element of A_3 but not by S_3.)