Example Sheet 4. **Lectures 19–23, Galois Theory Michaelmas 2010**

Cubics, quartics and discriminants

4.1. Let P be an irreducible cubic polynomial over K with $\operatorname{char} K \neq 2$, and let δ be a square root of the discriminant of P. Show that P remains irreducible over $K(\delta)$.

4.2. (i) Show that the discriminant of X^4+pX+q is $-27p^4+256q^3$. [Hint: It is a symmetric polynomial of degree 12, hence a linear combination of p^4 and q^3. By making good choices for p, q, determine the coefficients.]

(ii) Show that the discriminant of $X^5 + pX + q$ is $4^4p^5 + 5^5q^4$. (The discriminant of a general quintic will have 59 terms...)

4.3. Let P be an irreducible quartic polynomial over K with $\operatorname{char} K \neq 2$, whose Galois group is A_4. Show that its splitting field can be written in the form $L(\sqrt{a}, \sqrt{b})$ where L/K is a Galois cubic extension and $a, b \in L$.

4.4. Let P be an irreducible separable quartic, and Q its resolvent cubic. Show that the discriminants of P and Q are equal.

4.5. Show that $\mathbb{Q}(\boldsymbol{\mu}_{21})$ has exactly three subfields of degree 6 over $\mathbb{Q}$. Show that one of them is $\mathbb{Q}(\boldsymbol{\mu}_7)$, one is real, and the other is a cyclic extension $K/\mathbb{Q}(\boldsymbol{\mu}_3)$. Use a suitable Lagrange resolvent to find $a \in \mathbb{Q}(\boldsymbol{\mu}_3)$ such that $K = \mathbb{Q}(\zeta_3, \sqrt[3]{a})$.

4.6.* Let $P(X) = X^4 + 8X + 12 \in \mathbb{Q}[X]$. Compute the discriminant and resolvent cubic Q of P. Show P and Q are both irreducible, and that the Galois group of P is A_4.

4.7.* (i) **(Vandermonde determinant)** Show that if $X_1, \dots, X_n$ are indeterminates, then

$$\begin{vmatrix} X_1^{n-1} & X_2^{n-1} & \cdots & X_n^{n-1} \\ X_1^{n-2} & X_2^{n-2} & \cdots & X_n^{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ X_1 & X_2 & \cdots & X_n \\ 1 & 1 & \cdots & 1 \end{vmatrix} = \prod_{1 \le i < j \le n} (X_i - X_j).$$

(First show that each $(X_i - X_j)$ is a factor of the determinant.)

(ii) For $P(X) = \prod_{i=1}^n (X - x_i)$, show that $P'(x_i) = \prod_{j \neq i}(x_i - x_j)$, and deduce that its discriminant is given by $\Delta_P = (-1)^{n(n-1)/2} \prod_{i=1}^n P'(x_i)$.

(iii) Now suppose $P(X) = X^n + pX + q = \prod_{i=1}^n (X - x_i)$, with $n \geq 2$. Show that

$$x_i P'(x_i) = (n-1)p\Big(\frac{-nq}{(n-1)p} - x_i\Big)$$

and deduce that

$$\Delta_P = (-1)^{n(n-1)/2}\left((1-n)^{n-1}p^n + n^n q^{n-1}\right).$$

4.8.* Compute the discriminant of $X^{p^n} - 1$ for a prime p and $n \geq 1$.

Galois groups over $\mathbb{Q}$

4.9. (i) Determine the Galois groups of the following cubics in $\mathbb{Q}[X]$:

$$X^3 + 3X,\ X^3 + 27X - 4,\ X^3 - 21X + 7,\ X^3 + X^2 - 2X - 1,\ X^3 + X^2 - 2X + 1.$$

(ii) Determine the Galois groups of the following quartics in $\mathbb{Q}[X]$:

$$X^4 + 4X^2 + 2,\ X^4 + 2X^2 + 4,\ X^4 + 4X^2 - 5,\ X^4 - 2,\ X^4 + 2,$$
$$X^4 + X + 1,\ X^4 + X^3 + X^2 + X + 1.$$

4.10. (i) What are the transitive subgroups of S_4? Find a monic polynomial over $\mathbb{Z}$ of degree 4 whose Galois group is $V_4 = \{e, (12)(34), (13)(24), (14)(23)\}$.

(ii) Let $P \in \mathbb{Z}[X]$ be monic and separable of degree n. Suppose that the Galois group of P over $\mathbb{Q}$ doesn't contain an n-cycle. Prove that the reduction of P modulo p is reducible for every prime p (see Problem 2.13).

4.11. Compute the Galois group of $X^5 - 2$ over $\mathbb{Q}$.

4.12. (i) Let p be prime. Show that any transitive subgroup G of S_p contains a p-cycle. Show that if G also contains a transposition then $G = S_p$.

(ii) Prove that the Galois group of $X^5 + 2X + 6$ is S_5.

(iii) Show that if $P \in \mathbb{Q}[X]$ is an irreducible polynomial of degree p which has exactly two non-real roots, then its Galois group is S_p. Deduce that for an odd prime p and a sufficiently large $m \in \mathbb{Z}$,

$$P(X) = X^p + mp^2(X-1)(X-2)\cdots(X-p+2) - p$$

has Galois group S_p.

4.13.* (i) Show that the Galois group of $X^5 - 4X + 2$ over $\mathbb{Q}$ is S_5, and determine its Galois group over $\mathbb{Q}(i)$.

(ii) Find the Galois group of $X^4 - 4X + 2$ over $\mathbb{Q}$ and over $\mathbb{Q}(i)$.

4.14.* Let $\alpha = \sqrt[3]{a + b\sqrt{2}}$ for $a, b \in \mathbb{Q}$, and let F be the splitting field for the minimal polynomial of α over $\mathbb{Q}(\boldsymbol{\mu}_3)$. Determine the possible groups for $\mathrm{Gal}(F/\mathbb{Q}(\boldsymbol{\mu}_3))$.

Linear algebraic approach

4.15. We saw that we can prove the fundamental theorem of Galois theory without using the primitive element theorem. Now deduce the primitive element theorem from the fundamental theorem. (Use Problem 1.17.)

4.16. Let F/K be a cyclic extension of prime degree p, and σ a generator of $\mathrm{Gal}(F/K)$. Denote the trace of F/K by $T_{F/K} : F \to K$.

(i) Show that $T_{F/K}(\sigma(x) - x) = 0$ for all $x \in F$. Deduce that if $y \in F$ then $T_{F/K}(y) = 0$ if and only if $y = \sigma(x) - x$ for some $x \in F$.

(ii) **(Artin-Schreier theory)** Suppose that K has characteristic p. Use (i) to show that every element of K can be written in the form $\sigma(x) - x$ for some $x \in F$. Show also that if $\sigma(x) - x \in \mathbb{F}_p$ then $x^p - x \in K$. Deduce that F/K is an Artin-Schreier extension (described in Problem 2.5).

[This is the analogue of Kummer theory in characteristic $p > 0$. The natural analogue of radical extensions in characteristic p is to consider the tower of abelian extensions which involve Kummer and Artin-Schreier extensions.]

4.17.* (**Normal Basis Theorem**) In this example we show that if F/K if a finite Galois extension of infinite fields, then there exists $y \in F$ such that $\{\sigma(y) \mid \sigma \in \mathrm{Gal}(F/K)\}$ is a basis for F/K. (Such a basis $\{\sigma(y)\}$ is said to be a **normal basis** for F/K.)

(i) Let $P \in K[X]$ be a monic separable polynomial of degree n, with roots x_i in a splitting field F. Let

$$Q_i(X) = \frac{P(X)}{P'(x_i)(X - x_i)} \in F[X] \qquad (1 \le i \le n).$$

Show that, in $F[X]$:

$$(1) \qquad Q_1 + \cdots + Q_n = 1$$

$$(2) \qquad Q_i Q_j \equiv \begin{cases} 0 & (\mathrm{mod}(P)) \quad \text{if } j \neq i \\ Q_i & (\mathrm{mod}(P)) \quad \text{if } j = i \end{cases}$$

(Equation (1) is the "partial fractions" decomposition of $1/P(X)$.)

(ii) Let F/K be a finite Galois extension and $\mathrm{Gal}(F/K) = \{\sigma_1, \ldots, \sigma_n\}$ with $\sigma_1 = \mathrm{id}$. Let $x \in F$ be such that $F = K(x)$ and its minimal polynomial over K is $P \in K[X]$, and $x_i = \sigma_i(x)$. Let $A = (a_{ij})$ be the matrix with entries $a_{ij} := \sigma_i \sigma_j Q_1 \in F[X]$. Use (1),(2) of (i) to show that $A^t A \equiv I_n \ (\mathrm{mod}(P))$.

(iii) Assume that K is infinite. Use (ii) to show that there exists $b \in K$ such that $\det(\sigma_i \sigma_j Q_1(b)) \neq 0$. Deduce that $\{\sigma_1(y), \ldots, \sigma_n(y)\}$ for $y = Q_1(b)$ is a K-basis of F.

---

t.yoshida@dpmms.cam.ac.uk