Example Sheet 4. **Galois Theory Michaelmas 2011**

SEPARABILITY

4.1. Show that every irreducible polynomial over a finite field is separable. More generally, show that if K is a field of characteristic $p > 0$ such that every element of K is a p-th power, then any irreducible polynomial over K is separable. [This shows that, a field of characteristic $p > 0$ is **perfect** (i.e., its every algebraic extension is separable) if and only if every element is a p-th power in that field.]

4.2. Let F/K be a finite extension. Show that there is a unique intermediate field $K \subset L \subset F$ such that L/K is separable and F/L is **purely inseparable**, i.e. $|\mathrm{Hom}_L(F, E)| \leq 1$ for every extension E/L. (This L is called the **separable closure** of K in F.)

4.3. Let $F = \mathbb{F}_p(X, Y)$ be the field of rational functions in two variables (i.e. the field of fractions of $\mathbb{F}_p[X, Y]$) and K the subfield $\mathbb{F}_p(X^p, Y^p)$. Show that for any $f \in F$ one has $f^p \in K$, and deduce that F/K is not a simple extension.

DISCRIMINANTS

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

4.5. (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 $\mathbb{Z}$-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...)

4.6. Let P be an irreducible separable quartic, and Q its resolvent cubic. Show that the discriminants of P and Q are equal. [Recall: if $\alpha + \beta + \gamma + \delta = a$ and $\alpha' = \alpha - \frac{a}{4}$ etc, then the roots of Q are $(\alpha' + \beta')^2$, $(\alpha' + \gamma')^2$ and $(\alpha' + \delta')^2$.]

GALOIS GROUPS OVER $\mathbb{Q}$

4.7. (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 $\mathbb{Q}[X]$:

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

4.8. (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 strictly separable (i.e. no multiple root in its splitting field) 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 3.13).

4.9. (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.

Linear algebraic approach

4.10. 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 1.10.)

4.11. 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 3.10).

[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.]

Optional (not necessarily harder)

4.12.* Let K be a field of characteristic $p > 0$, and let x be algebraic over K. Show that x is separable over K if and only if and only if $K(x) = K(x^p)$.

4.13.* (i) Let K be a field of characteristic $p > 0$ and c an element of K which is not a p-th power. Let $n > 0$ and $q = p^n$. Show that $P(X) = X^q - c$ is irreducible in $K[X]$ and is inseparable, and that its splitting field is of the form $F = K(x)$ with $x^q = c$.

(ii) Let F/K be a finite, purely inseparable extension (see Problem 4.2) of characteristic p. Show that if $x \in F$ then $x^{p^n} \in K$ for some $n \in \mathbb{N}$. Deduce that there is a chain of subfields $K = K_0 \subset K_1 \subset \cdots \subset K_r = F$ where each extension K_i/K_{i-1} is of the type described in (i).

4.14.* 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.

4.15.* (i) (**Vandermonde determinant**) Show that if $X_1, \ldots, X_n$ 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 $P'(x_i) = \prod_{j \ne i}(x_i - x_j)$, 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 $n \ge 2$. Show that

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

and deduce that

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

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

4.17.* (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 $\mathbb{Q}(i)$.

4.18.* 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 $\mathrm{Gal}(F/\mathbb{Q}(\boldsymbol{\mu}_3))$.

4.19.* (**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 strictly separable (i.e. no multiple root in its splitting field) 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) $$Q_1 + \cdots + Q_n = 1$$

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

(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 $A^t A \equiv I_n \pmod{P}$.

(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.

November 24, 2011

t.yoshida@dpmms.cam.ac.uk