GALOIS COHOMOLOGY
EXERCISES 6 (SEPARABLE SPLITTING FIELDS)

The letter k denotes a field. The purpose of this exercise sheet it to describe another proof of the fact that every finite-dimensional central division k-algebra contains a maximal subfield which is separable over k. This alternative approach is longer (and for this reason was not included in the notes), but is in a sense much more natural if one is familiar with algebraic geometry. It can also more easily be adapted to prove other statements in the same vein.

The first exercise contains a construction of the discriminant of a polynomial. If you already know about this (or are not interested), you can skip to Exercise 2, which use only the fact stated in (iii) of Exercise 1.

Exercise 1. (i) Let $P = p_n X^n + \cdots + p_0$ and $Q = q_m X^m + \cdots + q_0$ be polynomials in $k[X]$. Construct a matrix $S \in M_{m+n}(k)$ having the following property. If $A = a_{m-1}X^{m-1} + \cdots + a_0$ and $B = b_{n-1}X^{n-1} + \cdots + b_0$ are polynomials in $k[X]$, writing

$$S \begin{pmatrix} a_{m-1} \\ \vdots \\ a_0 \\ b_{n-1} \\ \vdots \\ b_0 \end{pmatrix} = \begin{pmatrix} u_{m+n-1} \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ u_0 \end{pmatrix}$$

we have

$$PA + QB = u_{m+n-1}X^{m+n-1} + \cdots + u_0 \in k[X].$$

(ii) Assume that $p_n \neq 0$ and $q_m \neq 0$. Show that P and Q admit a nontrivial common factor if and only if $\det S = 0$. (The value $\det S$ is called the *resultant* of P and Q.)

(iii) Fix an integer d. Show that there exists a polynomial $\delta \in k[X_0, \dots, X_d]$ such that $\delta(a_0, \dots, a_d) \neq 0$ if and only if the polynomial $a_d X^d + \cdots + a_0$ is separable. (Hint: a polynomial is separable if and only if it is prime to its derivative.)

Exercise 2. Let A be a finite-dimensional k-algebra and $a \in A$. The kernel of the k-algebra morphism $k[X] \to A$ is a principal ideal. Recall that the *minimal polynomial* of a is the unique generator of that ideal having leading coefficient 1.

(i) Let L/k be a field extension. If $P \in k[X]$ is the minimal polynomial of a in the k-algebra A, show that its image $P \in L[X]$ is the minimal polynomial of $a \otimes 1$ in the L-algebra $A \otimes_k L$.

(ii) Let $M \in M_n(k)$ and $\chi \in k[X]$ its characteristic polynomial. Show that if χ is separable, then χ is the minimal polynomial of M.

(iii) Fix an integer n. Show that there exists a polynomial $\pi \in k[X_{i,j}, 1 \leq i, j \leq n]$ having the following property: if M is a matrix in $M_n(k)$ having coefficients $m_{i,j} \in k$ for $1 \leq i, j \leq n$, then $\pi(m_{1,1}, \dots, m_{n,n}) \neq 0$ if and only if the minimal polynomial of $M \in M_n(k)$ is separable of degree n. (Hint : use (iii) of the previous exercise.)

Let now D be a central division k-algebra of degree n, and F an algebraic closure of k.

(iv) Let $e_1, \dots, e_{n^2}$ be a k-basis of D. Show that there exists a polynomial $\rho \in F[X_1, \dots, X_{n^2}]$ having the following property: if $x \in D$ has coefficients $x_1, \dots, x_{n^2}$ in the basis $e_1, \dots, e_{n^2}$, then $\rho(x_1, \dots, x_{n^2}) \neq 0$ if and only if the minimal polynomial of x in the k-algebra D is separable of degree n.

(v) Assume that k is infinite. Let L/k be a field extension and d an integer. Let $P \in L[X_1, \dots, X_d]$ be a polynomial. Assume that there exist $y_1, \dots, y_d \in L$ such that $P(y_1, \dots, y_d) \neq 0$. Show that there exist $x_1, \dots, x_d \in k$ such that $P(x_1, \dots, x_d) \neq 0$. (Hint: find $x_1, \dots, x_m \in k$ by induction on m so that $P(x_1, \dots, x_m, y_{m+1}, \dots, y_d) \neq 0$.)

(vi) Conclude that D contains a separable extension of k of degree n. (Hint: observe that the case when k is finite is easy.)