

**MAT 535: HOMEWORK 8**

DUE WED, APRIL 9

1. (a) Prove that any extension  $K \subset L$  of degree 2 is of the form  $L = K(\sqrt{d})$  for some  $d \in K$  which is not a square in  $K$ .  
 (b) Prove that any extension of degree two is normal.
2. Determine the splitting field and degree for the following polynomials (over  $\mathbb{Q}$ ):  
 (a)  $x^4 + 2$   
 (b)  $x^3 - 3x + 1$   
 (c)  $x^3 + 3x + 1$
3. Let  $f = f_0 + f_1x + \cdots + f_nx^n$ ,  $g = g_0 + g_1x + \cdots + g_mx^m$  be polynomials of degrees  $n, m$  respectively with coefficients in a field  $K$ . Prove that the following are equivalent  
 (a)  $f, g$  are relatively prime  
 (b) Least common multiple of  $f, g$  has degree  $n + m$   
 (c) Every polynomial  $p$  of degree  $d < m + n$  can be uniquely written in the form  $p(x) = a(x)f(x) + b(x)g(x)$ ,  $\deg a < m$ ,  $\deg b < n$ .  
 (d)  $R(f, g) \neq 0$ , where

$$R(f, g) = \det \begin{bmatrix} f_0 & f_1 & f_2 & \cdots & & f_n & 0 & 0 & \cdots & 0 \\ 0 & f_0 & f_1 & f_2 & \cdots & & f_n & 0 & \cdots & 0 \\ 0 & 0 & f_0 & f_1 & f_2 & \cdots & & f_n & \cdots & 0 \\ & & & & \cdots & & & & & \\ \cdots & \cdots & & & f_0 & f_1 & f_2 & \cdots & & f_n \\ g_0 & g_1 & g_2 & \cdots & & g_m & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & g_2 & \cdots & & g_m & 0 & \cdots & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & \cdots & & g_m & \cdots & 0 \\ & & & & \cdots & & & & & \\ \cdots & \cdots & & & g_0 & g_1 & g_2 & \cdots & & g_m \end{bmatrix}$$

$(n + m) \times (n + m)$  matrix;  $m$  rows containing coefficients of  $f$ ,  $n$  rows containing coefficients of  $g$ . (The polynomial  $R(f, g)$  is called the resultant.)

4. Prove that the polynomial  $f$  is separable iff the resultant  $R(f, f') \neq 0$  (see the previous problem). Verify that for  $f(x) = x^2 + px + q$  it gives the familiar condition you learned in school:  $p^2 - 4q \neq 0$ .
5. Let  $K(\alpha)$  be a simple extension of  $K$  such that  $[K(\alpha) : K]$  is odd. Prove that then  $K(\alpha) = K(\alpha^2)$ .
6. Let  $n$  be a positive integer. As in class, define polynomial  $\Phi_n(x) \in \mathbb{C}[x]$  by

$$\Phi_n(x) = \prod (x - \zeta)$$

where the product is taken over all primitive roots of order  $n$  of 1, i.e. over  $\zeta = e^{k \cdot 2\pi i/n}$ ,  $1 \leq k \leq n$ ,  $(k, n) = 1$ .

- (a) Prove that

$$(1) \quad x^n - 1 = \prod_{d|n} \Phi_d(x),$$

where the product is taken over all divisors  $d$  of  $n$  (including 1 and  $n$ ).

- (b) Use induction and previous part to prove that  $\Phi_n$  has integer coefficients. Deduce from this that formula (1) is valid in any field.
- (c) Prove that if  $K$  is a field of characteristic which does not divide  $n$ , then  $x^n - 1$  is separable.
- (d) Let  $K$  be a field of characteristic which does not divide  $n$ , and  $L$  — the splitting field of  $x^n - 1$  over  $K$ . Prove that then  $L$  contains a primitive root of unity  $\zeta$ , i.e. an element  $\zeta$  such that  $\zeta^n = 1$ , but  $\zeta^k \neq 1$  for all  $1 \leq k < n$ .