612 Example Sheet 2

Paul Hacking

15 February 2011

(1) For each of the following polynomials, describe the splitting field K over $\mathbb{Q}$ and find the degree $[K : \mathbb{Q}]$.

  (a) $x^4 - 2$.

  (b) $x^6 - 4$.

  (c) $x^4 + 2$. [Hint: cf. HW1 Q9(b)]

  (d) $x^4 + x^2 + 1$.

(2) (a) Let K/F be a splitting field of a polynomial $f(x) \in F[x]$. Let $g(x) \in F[x]$ be an irreducible polynomial such that g has a root in K. Show that g splits completely in K (that is, $g(x)$ is a product of linear factors in $K[x]$). [Hint: Use Thm 8 and Thm 27 from DF Chapter 13.]

  (b) Let $F = \mathbb{F}_q$ be a finite field and $g(x) \in F[x]$ an irreducible polynomial of degree d. Describe the splitting field of g over F. [Hint: Use part (a).]

(3) Let $f(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$. Show that $f(x)$ is irreducible over $\mathbb{F}_2$. Let $K = \mathbb{F}_2(\alpha)$ be the field obtained by adjoining a root α of f to $\mathbb{F}_2$. (So $K \simeq \mathbb{F}_8$.) Find the minimal polynomial over $\mathbb{F}_2$ of each of the elements of K.

(4) The polynomials $f(x) = x^3+x+1$ and $g(x) = x^3+x^2+1$ are irreducible over $\mathbb{F}_2$. Let $K = \mathbb{F}_2(\alpha)$ and $L = \mathbb{F}_2(\beta)$ be the fields obtained by adjoining a root α of f and β of g. Describe explicitly an isomorphism $K \xrightarrow{\sim} L$.

(5) Show from first principles that an algebraically closed field is infinite.

(6) (Frobenius automorphism of finite field.) Let $F = \mathbb{F}_q$ be the finite field with $q = p^r$ elements, where p is a prime and $r \geq 1$. Show that the map

$$\phi\colon F \to F, \quad x \mapsto x^p$$

is an automorphism of F. Show that ϕ has order r, that is, $\phi^r = \mathrm{id}_F$ and $\phi^s \neq 1$ for $1 \leq s < r$.

(7) In class we showed that if K/F is a field extension of degree 2 and $\mathrm{char}(F) \neq 2$ then $K = F(\alpha)$ where $\alpha^2 \in F$. Now suppose that $[K : F] = 2$ and $\mathrm{char}(F) = 2$. Show that $K = F(\alpha)$ where either (i) $\alpha^2 \in F$ or (ii) $\alpha^2 + \alpha \in F$. Show that K/F is inseparable in case (i) and separable in case (ii). Find $\mathrm{Aut}(K/F)$ in each case.

(8) (The theorem of the primitive element is false for inseparable extensions.) Let $F = \mathbb{F}_p(x, y)$, the field of rational functions in two variables x and y with coefficients in $\mathbb{F}_p$. Let K/F be the field extension given by $K = \mathbb{F}_p(u, v)$ where $u^p = x$ and $v^p = y$. Show that $K \neq F(\gamma)$ for any $\gamma \in K$.

(9) (Perfect $\iff$ every algebraic extension is separable.) Let F be a field which is *not* perfect, that is, $\mathrm{char}(F) = p > 0$ and there exist elements of F which are *not* pth powers. Show that there exists an irreducible polynomial $f(x) \in F[x]$ which is *not* separable. [Hint: Show that $f(x) = x^p + a$ is irreducible over F if $a \notin F^p$.]

(10) Let p be a prime. Use the substitution $x = y + 1$ to give another proof that the cyclotomic polynomial

$$\Phi_p(x) = (x^p - 1)/(x - 1) = x^{p-1} + \cdots + x + 1$$

is irreducible.