Homework

Frederick Robinson

14 April 2010

Contents

1 Chapter 13 Section 4

1.1 Problem 1

1.1.1 Question

Determine the splitting field and its degree over $\mathbb{Q}$ for $x^4 - 2$.

1.1.2 Answer

Note that

$$f(x) = x^4 - 2 = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x + i\sqrt[4]{2})(x - i\sqrt[4]{2})$$

So, the splitting field is just $\mathbb{Q}(\sqrt[4]{2}, i)$. This is a field extension of degree 8 over $\mathbb{Q}$ since the degree of $\mathbb{Q}(\sqrt[4]{2})$ is 4 (minimal polynomial f), the degree of $\mathbb{Q}(i)$ is 2 and these extensions have nothing in common (in particular $\mathbb{Q}(\sqrt[4]{2}) - \mathbb{Q} \subset \mathbb{R}$ and $\mathbb{R} \cap (\mathbb{Q}(i) - \mathbb{Q}) = \emptyset$).

1.2 Problem 2

1.2.1 Question

Determine the splitting field and its degree over $\mathbb{Q}$ for $x^4 + 2$.

1.2.2 Answer

Again we note that

$$f(x) = x^4 + 2 = (x + \sqrt[4]{-2})(x + i\sqrt[4]{-2})(x - i\sqrt[4]{-2})(x - \sqrt[4]{-2})$$

The splitting field is then $\mathbb{Q}(\sqrt[4]{-2}, i)$. The degree of this extension is 8 since $\mathbb{Q}(\sqrt[4]{-2})$ is a degree 4 extension (minimal polynomial f) and $\mathbb{Q}(i)$ is a degree 2 extension over $\mathbb{Q}(\sqrt[4]{2})$.

1.3 Problem 3

1.3.1 Question

Determine the splitting field and its degree over $\mathbb{Q}$ for $x^4 + x^2 + 1$.

1.3.2 Answer

Again we note that

$$f(x) = x^4 + x^2 + 1 = (x + (-1)^{1/3})(x - (-1)^{1/3})(x + (-1)^{2/3})(x - (-1)^{2/3})$$

The splitting field is then $\mathbb{Q}((-1)^{1/3})$ which has degree 3 over $\mathbb{Q}$ (minimal polynomial $g(x) = x^3 + 1$).

1.4 Problem 5

1.4.1 Question

Let K be a finite extension of F. Prove that K is a splitting field over F if and only if every irreducible polynomial in $F[x]$ that has a root in K splits completely in $K[x]$. [Use Theorems 8 and 27.]

1.4.2 Answer

Proof. Say K is a splitting field for some polynomial $f \in F[x]$ over f and $p(x) \in F[x]$ is an irreducible polynomial with roots in K say α. Let D be the splitting field of $p(x)$ over K and β be any root. $F(\alpha) \cong F[x]/(p(x)) \cong F(\beta)$ so by Theorem 27 this extends to an isomorphism of splitting fields σ. Since K is the splitting field of f we have $\sigma(K) = K$. In particular $\sigma(\alpha) = \beta = K$, and $p(x)$ splits over K.

Conversely if every irreducible polynomial in $F[x]$ with a root in K splits over F there exist a set of $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$ which generate K over F. If we denote the minimal polynomial for each α_i by p_i then K is the splitting field of $p_1 p_2 \ldots p_n$ over F.

$\square$

2 Chapter 13 Section 5

2.1 Problem 2

2.1.1 Question

Find all irreducible polynomials of degrees $1, 2$ and 4 over $\mathbb{F}_2$ and prove that their product is $x^{16} - x$

2.1.2 Answer

An exhaustive search reveals that the following are all irreducible polynomials of degree $1, 2, 4$ over $\mathbb{F}_2$

$$x,\ x+1,\ x^2+x+1,\ x^4+x+1,\ x^4+x^3+1,\ x^4+x^3+x^2+x+1$$

Moreover we compute the product of all the above to yield

$$\begin{aligned} x + 4x^2 + 8x^3 + 12x^4 \quad &+ \quad 18x^5 + 26x^6 + 32x^7 + 34x^8 + 34x^9 \\ &+ \quad 32x^{10} + 26x^{11} + 18x^{12} + 12x^{13} + 8x^{14} + 4x^{15} + x^{16} \end{aligned}$$

which, reducing coefficients mod 2 is just

$$x + x^{16}$$

as desired.

2.2 Problem 3

2.2.1 Question

Prove that d divides n if and only if $x^d - 1$ divides $x^n - 1$. [Note that if $n = qd + r$ then $x^n - 1 = (x^{qd+r} - x^r) + (x^r - 1)$.]

2.2.2 Answer

Proof. $x^d - 1$ divides $x^n - 1$ if and only if every root of $x^d - 1$ is also a root of $x^n - 1$. In particular then $x^d - 1$ divides $x^n - 1$ if and only if $x^n = 1$ for every x such that $x^d = 1$. Writing $n = qd + r$ we see that $x^n = x^{qd+r} = \left(x^d\right)^q x^r$, so $x^d - 1$ divides $x^n - 1$ if and only if $r = 0$: that is, if and only if d divides n. $\square$

2.3 Problem 4

2.3.1 Question

Let $a > 1$ be an integer. Prove for any positive integers n, d that d divides n if and only if $a^d - 1$ divides $a^n - 1$ (cf. previous exercise). Conclude in particular that $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$ if and only if d divides n.

2.3.2 Answer

Proof. By the previous if d divides n if and only if $a^d - 1$ divides $a^n - 1$. .

So, since $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$ if and only if $a^d - 1$ divides $a^n - 1$, $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$ if and only if d divides n. $\square$