Homework

Frederick Robinson

3 May 2010

1 Chapter 13 Section 5

1.1 Problem 5

1.1.1 Question

For any prime p and any nonzero $a \in \mathbb{F}_p$ prove that $x^p - x + a$ is irreducible and separable over $\mathbb{F}_p$. [For the irreducibility: One approach — prove first that if α is a root then $\alpha + 1$ is also a root. Another approach — suppose it's reducible and compute derivatives.]

1.1.2 Answer

By Proposition 37 it suffices to show that $x^p - x + a$ is irreducible over $\mathbb{F}_p$

Proof. Let α be a root of $f(x) = x^p - x + a$. Now compute

$$\begin{aligned} f(\alpha+1) &= (\alpha+1)^p - (\alpha+1) + a \\ &= \alpha^p + 1 - \alpha - 1 + a \\ &= \alpha^p - \alpha + a. \end{aligned}$$

So, for any α a root of f, $\alpha + 1$ is also a root and by induction each $\alpha' \in \mathbb{F}_p$ is a root of f. In particular, $f(0) = 0^p - 0 + a = 0 \Rightarrow a = 0$ a contradiction. Therefore f has no roots.

Suppose that f is reducible as

$$f = g_1 \cdot g_2 \cdots g_n$$

There exists some extension of $\mathbb{F}_p$ which contains a root β of f. However, by the previous proof each $\beta + m$ is also a factor for $m \in \mathbb{F}_p$. Hence, our extension field is a splitting field. Since our choice of β was arbitrary we have $deg(g_i) = [\mathbb{F}_p(\beta) : \mathbb{F}_p]$ for any i. Since f has no roots and

$$\prod_{1 \le i \le n} deg(g_i) = p$$

for p prime f must be irreducible as claimed. □

1.2 Problem 7

1.2.1 Question

Suppose K is a field of characteristic p which is not a perfect field: $K \neq K^p$. Prove there exist irreducible inseparable polynomials over K. Conclude that there exists inseparable finite extensions of K.

1.2.2 Answer

Since $K \neq K^p$ there exists some $\beta \in K$ such that $x^p \neq \beta$ for all $x \in K$. The polynomial $f(x) = x^p - \beta$ is irreducible and inseparable.

Proof. Since $D_x(f) = 0$ we have by Proposition 33 that f is inseparable. Moreover, f is irreducible by Eisenstein (Section 9.4 Example 5). □

The finite extension of K obtained by adjoining the roots of f is therefore inseparable.

2 Chapter 13 Section 6

2.1 Problem 1

2.1.1 Question

Suppose m and n a re relatively prime positive integers. Let ζ_m be a primitive m^{th} root of unity and let ζ_{n} be a primitive n^{th} root of unity. Prove that $\zeta_m\zeta_n$ is a primitive mn^{th} root of unity.

2.1.2 Answer

Proof. Since m, n are relatively prime $(\zeta_m\zeta_n)^l = 1 \Rightarrow (\zeta_m)^l = 1$ and $(\zeta_n)^l = 1$ moreover, LCM(m,n)=mn. □

2.2 Problem 2

2.2.1 Question

Let ζ_n be a primitive n^{th} root of unity and let d be a divisor of n. Prove that $\zeta_{\text{n}}^{\text{d}}$ is a primitive $(n/d)^{\text{th}}$ root of unity.

2.2.2 Answer

Proof. Note that $\zeta_{\text{n}}^{\text{d}}$ is a $(n/d)^{\text{th}}$ root of unity since $(\zeta_{\text{n}}^{\text{d}})^{n/d} = 1$. Moreover if there were some $l = m/d < (n/d)$ such that $(\zeta_{\text{n}}^{\text{d}})^l = 1$ we would have $\zeta_n^m = 1$ for $m < n$, a contradiction. Hence $\zeta_{\text{n}}^{\text{d}}$ is primitive as claimed. □

2.3 Problem 3

2.3.1 Question

Prove that if a field contains the n^{th} roots of unity for n odd then it also contains the $2n^{\text{th}}$ roots of unity.

2.3.2 Answer

Proof. By definition of the Euler φ function the cyclotomic polynomials for Φ_n and Φ_{2n} have the same degree. Moreover, since an n^{th} root of unity is also a $2n^{\text{th}}$ root of unity the extension nth cyclotomic extension is a subfield of the $2n$th cyclotomic extension. Thus, both cyclotomic extensions are the same. In particular, we may conclude that any field containing the nth roots of unity, and therefore the nth cyclotomic extension, contains the $2n$th cyclotomic extension, and consequently the $2n$th roots of unity. □

2.4 Problem 9

2.4.1 Question

Suppose A is an $n \times n$ matrix over $\mathbb{C}$ for which $A^k = I$ for some integer $k \geq 1$. Show that A can be diagonalized. Show that the matrix $A = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$ where α is an element of a field of characteristic p satisfies $A^p = I$ and cannot be diagonalized if $\alpha \neq 0$.

2.4.2 Answer

Recall that by Proposition 25 of 12.3 "If A is an $n \times n$ matrix with entries from F and F contains all of the eigenvalues of A, then A is similar to a diagonal matrix over F if and only if the minimal polynomial of A has no repeated roots."

Proof. Since $\mathbb{C}$ is algebraically closed it contains all eigenvalues of A. The minimal polynomial for A is just Φ_k since by construction $A^k = I$. Since Φ_k is separable A is diagonalizable. □

It is easy to check that

$$A^n = \begin{pmatrix} 1 & n\alpha \\ 0 & 1 \end{pmatrix}$$

So, over a field of characteristic p we have $A^p = I$. Moreover, given $\alpha \neq 0$, A cannot be diagonalized since in this field Φ_p is inseparable.

2.5 Problem 10

2.5.1 Question

Let φ denote the Frobenius map $x \mapsto x^p$ on the finite field $\mathbb{F}_{p^n}$. Prove that φ gives an isomorphism of $\mathbb{F}_{p^n}$ to itself (such an isomorphism is called an *automorphism*). Prove that φ^n is the identity map and that no lower power of φ is the identity.

2.5.2 Answer

Proof. By Proposition 35 the Frobenius map is an injective homomorphism of fields. Thus, for a finite field, it is also surjective and an isomorphism, automorphism. We have $\varphi^n(x) = (x^p)^n$ since the multiplicative group is of order $p^n - 1$, $x^{(p^n-1)} = 1$ and $\varphi^n(x)$ is the identity map. However, if φ^l for $l < n$ were the identity then we would have $x^{(l-1)} = 1$ for $l < n$ a contradiction. $\square$

2.6 Problem 11

2.6.1 Question

Let φ denote the Frobenius map $x \mapsto x^p$ on the finite field $\mathbb{F}_{p^n}$ as in the previous exercise. Determine the rational canonical form of $\mathbb{F}_{p^n}$for φ considered as an $\mathbb{F}_{p^n}$-linear transformation of the n-dimensional $\mathbb{F}_p$-vector space $\mathbb{F}_{p^n}$.

2.6.2 Answer

By Artin's Lemma we see that $x^n - 1$ is the minimal polynomial of this transformation. Therefore, it is also the characteristic polynomial. This completely determines the rational canonical form.

2.7 Problem 12

2.7.1 Question

Let φ denote the Frobenius map $x \mapsto x^p$ on the finite field $\mathbb{F}_{p^n}$ as in the previous exercise. Determine the Jordan canonical form (over a field containing all the eigenvalues) for φ considered as an $\mathbb{F}_p$ linear transformation of the n-dimensional $\mathbb{F}_p$-vector space $\mathbb{F}_{p^n}$.

2.7.2 Answer

As in the previous exercise we know that $x^n - 1$ is both the characteristic and minimal polynomial. Since we assume that we are in a field which contains all the eigenvalues the JCF is completely determined by this.