Solution for homework 6

by 9622534

1.

Since F is a field, F[x]is an UFD. Let $F = \sum_{i=0}^{n} a_i x^i$, $g = \sum_{i=0}^{m} b_i x^i$ with $n > m$. Then $F = Q_1 g + f_0$ for some Q_1 with degree $n - m$. Let $r = \lfloor \frac{deg(f)}{deg(g)} \rfloor$, then $f = f_r g^r + e_{r-1}$, $e_i = f_i g^i + e_{i-1}$, where $deg(f_i) < deg(g)$ for $deg(e_i) < deg(g^{i+1})$. For uniqueness, suppose
$f = f_0 + f_1 g + ... + f_r g^r = h_0 + h_1 g + ... + h_r g^r$, then we have
$0 = (f_0 - h_0) + (f_1 - h_1)g + ... + (f_r - h_r)g^r$
$-(f_0 - h_0) = (f_1 - h_1)g + ... + (f_r - h_r)g^r \Rightarrow f_0 = h_0$
W.L.O.G. Let i be the smallest index such that $h_i \neq f_i$, then
$-(f_i - h_i) = (f_{i+1} - h_{i+1})g^{i+1} + ... + (f_r - h_r)g^r$
$\Rightarrow \frac{-(f_i - h_i)}{g^i} = (f_{i+1} - h_{i+1})g + ... + (f_r - h_r)g^{r-i} \Rightarrow f_i = h_i$
Thus we are done.

2.(a)

Since $f(x)$ has positive degree, $\exists i \geq 1$, $a_i > 0$. Since char R = 0, then $ia_i \neq 0 \Rightarrow f'(x_i) \neq 0$.

2.(b)

($\Rightarrow$)Let $f(x) = \sum_{i=0}^{n} a_i x^i$, then $f'(x) = \sum_{i=1}^{n} a_i x^{i-1}$. Since $f'(x) = 0$, $ia_i = 0$ $\forall 1 \leq i \leq n$. If $a_i \neq 0 \Rightarrow p|i$, thus $i = pj$ and we have $f(x) = \sum_{j=0}^{n} a_{pj} x^{pj}$.

($\Leftarrow$)Since $f'(x) = b_1 p x^{p-1} + ... + b_n p x^{p-1}$ and char $R = 0$, we have $f'(x) = 0$.

3.(a)

($\Rightarrow$)Suppose not. Then $f(x) = x^p - x - c$ has a root r in F, i.e. $f(r) = 0$. By Corollary 6.3, there exists a unique $q(x) \in F$ such that $f(x) = q(x)(x - r) + f(r) = q(x)(x - r)$. Since $q(x)$ and $(x - r)$ are not unit in F, $f(x)$ is irreducible in $F[x]$, a contradiction.

($\Leftarrow$)By theorem V 1.10, there exists an extention field $F' \supseteq F$ and $a \in F' \backslash F$ such that $a^p - p - c = 0$. Note char(F)=char(F')=p.
Claim: $\forall i \in F$, $a + i$ is a root of $x^p - x - c$.
proof of the claim : $(a + i)^p - (a + i) - c = (a^p + i^p - (a + i) - c) = (a^p - a - c) + (i^p - i) = 0 + (i - i) = 0$
Since $0, 1, 2, ..., p - 1 \in F$, $a, a + 1, a + 2, ..., a + (p - 1)$ are p distinct roots of $x^p - x - c$.
Hence $f(x) = \prod(x - (a + i))$ over F' where $i \in \{0, ..., p - 1\}$.

Now suppose not, i.e. $f(x)$ is reducible in $F[x]$. Then $f(x) = q(x)g(x)$ over F, $q(x) = \prod_{i \in I \subset \{0,...,p-1\}, |I|=s} (x - (a + i))$ with $deg(q(x)) = s < p$.
Consider the coefficient of x^{s-1} which is $-sa + k \in F$. Since $k \in F$ we have $-sa \in F \Rightarrow -a \in F$, a contradiction.

3.(b)

Since the only integers that divide -1 are 1 and -1, and $f(-1) = -1$, $f(1) = 1$, we have that f(x) has no root in $\mathcal{Q}$.

3.(c)

Use same argument we know f(x) has no divisor of degree 1. Thus if f(x) is reducible, it must have form

$f(x) = (x^3 + ax^2 + bx + c)(x^2 + dx + e)$. Since it contains 1 as a coefficient, f(x) is primitive, thus it is reducible over $\mathcal{Q}$ if and only if it is reducible over $\mathcal{N}$. Thus we only need to solve a, b, c, d, e in $\mathcal{N}$. It's trivial to get that there is no solution, thus f(x) is irreducible.

3.(d)
$x^5 - x + 15 = (x^3 + x^2 - 2x - 5)(x^2 - x + 3)$. And it's easy to find out that it has no root in $\mathcal{Q}$.

4.(a) ($\Rightarrow$) Suppose $f(x - c)$ is not irreducible in $D[x]$, $c \in D$
$\Rightarrow f(x-c) = (\sum_{i=0}^{m} a_i x^i)(\sum_{i=0}^{k} b_i x^i)$ where $a_i, b_i \in D$ and $(\sum_{i=0}^{m} a_i x^i), (\sum_{i=0}^{k} b_i x^i)$ are not unit in $D[x]$.
Thus $f(x) = f((x + c) - c) = (\sum_{i=0}^{m} a_i (x + c)^i)(\sum_{i=0}^{k} b_i (x + c)^i)$
$= (a_m x^m + ...)(b_k x^k + ...) \Rightarrow a_m b_k \neq 0$
Thus $(a_m x^m + ...), (b_k x^k + ...)$ are not unit in $D[x]$.

($\Leftarrow$)Since $f(x) = f(x + c) - c$, it's clear to see.

4.(b) $f(x) = \frac{(x-1)^{p-1}}{x-1} = x^p + \binom{p}{p-1} x^{p-1} + ... + \binom{p}{1}$,
Thus $p | \binom{p}{r}$ $\forall 1 \leq r \leq p-1$ and $p \not| 1$, $p^2 \not| p$, by Eisenstein's criterion we are done.

5.(a) Suppose there are more than one polynomial $f(x)$, $g(x)$ of degree at most n in $D[x]$ such that $f(a_i) = d_i$, $g(a_i) = d_i$, for $0 \leq i \leq n$.
Then $(f - g)(a_i) = 0$ $\forall$ i and $deg((f - g)(x)) \leq n$.
Let F be the quotient field of D, then $(f - g)(x) \in F[x]$,
Since $x - a_0$ is irreducible in $F[x]$,
Then $(f - g)(a_0) = 0 \Leftrightarrow (x - a_0) \mid (f - g)(x)$, similarly for $x - a_1$,... ,$x - a_n$,
Since $F[x]$ is an UFD, we have
$(f - g)(x) = c(x - a_0) \cdots (x - a_n)$ has degree $> n$, a contradiction.
Thus $f = g$.
5(b) Suppose $\exists h$ such that $h(a_i) = c_i \forall i$, with $deg(h) < n$. The rest is clear to see.