Math 241

Problem Set 12 solution manual

Exercise. A12.1

- a- Notice that using Fermat's theorem we can see that for any $x \in \mathbb{Z}_p$ we have that $x^p - x = 0$, and hence we can write $x^p - x = x(x-1)(x-2)...(x-(p-1))$.
- b- The roots of $x^3 - x$ in $\mathbb{Z}_6$ are 0,1,2,3,4,5.

  It is not surprising to have 6 roots for an equation of degree 3 since our ring is not integral domain.

Section. 22

Exercise. 3
$f(x) + g(x) = (2x^3 + 3x + 4) + (3x^2 + 2x + 3) = 5x^2 + 5x + 7 = 5x^2 + 5x + 1$. $f(x).g(x) = (2x^3 + 3x + 4).(3x^2 + 2x + 3) = 6x^4 + 13x^3 + 24x^2 + 17x + 12 = x^3 + 5x$.

Exercise. 4
$f(x) + g(x) = 3x^4 + 2x^3 + 4x^2 + 1$. $f(x).g(x) = x^7 + 2x^6 + 4x^5 + x^3 + 2x^2 + x + 3$

Exercise. 5
A polynomial of degree three is of the form $a_0 + a_1x + a_2x^2 + a_3x^3$, where a_0, a_1, a_2, and a_3 are in $\mathbb{Z}_2$, hence we have 16 such polynomials.

Exercise. 9
$\Phi_3[f(x)] = f(3) = (3^4 + 6)(3^3 + 3.3^2 + 3) = (81 + 6)(27 - 27 + 3) = (87)(3) = (3)(3) = 9 = 2$.

Exercise. 11

Using Fermat's theorem and since 4 is not equal to 0 $mod 7$, $\implies (4^6) \equiv 1 \; mod 7$.

$(4^{106}) = (4^{102}).4^4 = (4^6)^{17}.4^4 = 256 = 4 \; mod 7$, also similarly you can find out that $4^{99} = 1$, and $4^5 3 = 2$. Hence $\Phi_4(3x^{99} + 5x^{11} + 2x^{53}) = 3.4 + 5.1 + 2.2 = 0$.

Exercise. 12
$f(1) = 1^2 + 1 = 0$, hence 1 is a root.

$f(0) = 1$, hence 0 is not a root.

So the only root is 1.

Exercise. 14

$f(0) = 0$
$f(1) = 2$
$f(2) = 4$
$f(3) = 4$
$f(4) = 0$
Hence the roots of f are 0, and 4.

Exercise. 15

By simple calculation you can see that 0 and 2 are the roots of f, and that 0 and 4 are the roots of g. Hence $0, 2, 4$ are the roots of $f.g$.

Exercise. 27

a- Let $f(x) = a_0 + a_1x + ... + a_nx^n$, and $g(x) = b_0 + b_1x + ... + b_mx^m$, without loss of generality we can assume that $m \geq n$. Hence $f + g = (a_0 + b_0) + (a_1 + b_1)x + ... + (a_n + b_n)x^n + b_{n+1}x^{n+1} + ... + b_mx^m$.

$D(f + g) = a_1 + b_1 + 2(a_2 + b_2)x + ... + n(a_n + b_n)x^{n-1} + (n + 1)b_n + 1x^n + ... + mb_mx^{m-1} = (a_1 + 2a_2x + ... + na_nx^{n-1}) + (b_1 + 2b_2x + ... + mb_mx^{m-1}) = D(f) + D(g)$. So D is a well defined map satisfying $D(f + g) = D(f) + D(g)$, hence D is a group homomorphism of the group $< F[x], + >$.

This map can't be a ring homomorphism since it doesn't satisfy $D(fg) = D(f) + D(g)$, in fact we are going to prove that $D(fg) = fD(g) + gD(f)$ for all $f, g \in F[x]$.

So let $f, g \in F[x]$ (f, g as defined above). Then $f.g = c_0 + c_1x + ... + c_{n+m}x^{n+m}$ where $c_i = \sum_{j=0...i} a_jb_{i-j}$.

$D(f.g) = c_1 + 2c_2x + ... + (n+m)c_{n+m}x^{n+m-1}$, and on the other hand $fD(g) + gD(f) = (a_0 + a_1x + ... + a_nx^n)(b_1 + 2b_2x + ... + mb_mx^{m-1}) + (b_0 + b_1x + ... + b_mx^m)((a_1 + 2a_2x + ... + na_nx^{n-1}) = (a_0b_1 + b_0a_1) + (2a_0b_2 + 2a_2b_0 + a_1b_1 + a_1b_1)x + ... + ((n + m)a_nb_m)x^{n+m-1} = D(f.g)$.

b- $Ker(f) = \{f = a_0 + a_1 + ... + a_nx^n \mid D(f) = 0\} = \{f = a_0 + a_1 + ... + a_nx^n \mid a_1 + 2a_2x + ... + na_nx^{n-1} = 0\} = \{f = a_0 \mid a_0 \in F\}$, and this is because our field F is of characteristic 0 hence the polynomial $a_1 + 2a_2x + ... + na_nx^{n-1}$ is only a 0 polynomial if all its coefficients are zero.

c- The image of our map is $F[x]$, since given $g = b_0 + b_1x + ... + b_mx^m$, we let $f = c + b_0x + \frac{1}{2}b_1x^2 + ... + \frac{1}{m+1}b_mx^{m+1}$, and hence it is easy to see that $D(f) = g$, so f is surjective.

Section. 23

Exercise. 2

	$5x^4 + 5x^2 + 6x$
$x^6 + 3x^5 + 4x^2 - 3x + 2$	$3x^2 + 2x - 3$
$x^6 + 3x^5 + 6x^4$	
$x^4 + 4x^2 - 3x + 2$	
$x^4 + 3x^3 + 6x^2$	
$4x^3 + 5x^2 + 4x + 2$	
$4x^3 + 5x^2 + 3x$	
$x + 2$	

Exercise. 4

We do the same as above to get $q(x) = 9x^2 + 5x + 10$, and $r(x) = 2$.

Exercise. 7
Check Solution manual for problem set 5, ex 3 section 20.

Exercise. 10
$f(x) = x^3 + 2x^2 + 2x + 1$, notice that $f(2) = 0$, and hence $x - 2$ is a factor of f, so using the division algorithm as in ex 3 above, we get that $f = (x - 2)(x^2 + 4x + 3)$. Now let $g(x) = x^2 + 4x + 3$, and we can see now that $g(-1) = g(6) = 0$, and hence again $x - 6$ is factor of g, so dividing again we get that $f(x) = (x - 2)(x - 6)(x + 3)$.

Exercise. 12

Following the same technique as in ex 10 , we can factorize $f(x)$ into $(x - 2)(x - 4)(x + 1) = (x - 2)(x + 1)^2$.

Exercise. 13

f is a polynomial of degree 3, which has no roots in the field $\mathbb{Z}_5$, hence by theorem 23.10 we deduce that f is irreducible.