MTH310 EXAM 2 REVIEW

SA LI

4.1 Polynomial Arithmetic and the Division Algorithm

A. Polynomial Arithmetic

*Polynomial Rings

If R is a ring, then there exists a ring T containing an element x that is not in R and the set R[x] of all elements of T such that

$a_0 + a_1x + a_2x^2 + ... + a_nx^n$ (where n $\geq$ 0 and a_i $\in$ R) is a subring of T containing R.

*Polynomial addition, multiplication and contribution law.

*Definition: Let f(x) = $a_0 + a_1x + a_2x^2 + ... + a_nx^n$ be a polynomial in R[x] with $a_n \neq 0_R$, Then a_n is called the leading coefficient of f(x). The degree of f(x) is the integer n; it is denoted "deg f(x) ". In other words, deg f(x) is the largest exponent of x that appears with a nonzero coefficient, and this coefficient is the leading coefficient.

Example: f(x) = $3 + 2x + 7x^2 + 8x^3$

deg f(x) = 3

leading coefficient =8

*Thm 4.2 If R is an integral domain and f(x), g(x) are nonzero polynomials in R[x]. Then deg (f(x)*g(x)) = deg f + deg g.

*Cor: If R is an integral domain, then so is R[x].

*Cor 4.4: Let R be a ring. If f(x), g(x), and f(x)g(x) are nonzero in R[x], then
deg (f(x)g(x)) $\leq$deg f(x) + deg g(x)

*Cor 4.5: Let R be an integral domain and $f(x) \in R[x]$. Then f(x) is a unit in R[x] if and only if f(x) is a constant polynomial that is a unit in R.

In particular, if F is a field, the units in F[x] are the nonzero constants in F.

Example 8: 5x+1 is a unit in $\mathbb{Z}_{25}[x]$ that is not a constant.

proof: (5x+1)(20x+1) = $100x^2$ + 20x + 5x +1 = $100x^2$ + 25x + 1 = 1 in $\mathbb{Z}_{25}[x]$

B. The Division Algorithm in F[x]

*Thm 4.6

Let F be a field and f(x), g(x) $\in$ F[x] with g(x) $\neq 0_F$. Then there exist unique polynomials q(x) and r(x) such that
f(x) = g(x) q(x) + r(x) and either r(x) = 0_F or deg r(x)<deg g(x)

Example 9: Divide f(x) = $3x^5$ + $2x^4$ + $2x^3$ + $4x^2$ + x -2 by g(x) = $2x^3$ + 1.

f(x)= g(x) ($\frac{3}{2}x^2$ + x +1) + $\frac{5}{2}x^2$ -3)

4.2 Divisibility in F[x]

*Definition: Let F be a field and a(x), b(x) $\in$ F[x] with b(x) $\neq 0_F$, we say that b(x) divides a(x) [or that b(x) is a factor of a(x)] and write $b(x)|a(x)$ if
a(x) = b(x) h(x) for some h(x) $\in$ F[x].

Ex: $(2x+1)|(6x^2-x-2)$ in $\mathbb{Q}[x]$ because $6x^2$-x -2 = (2x+1)(3x-2).

*Thm 4.7
Let F be a field and a(x), b(x) $\in$ F[x] with b(x) $\neq 0_F$
(1) If b(x) divides a(x), then cb(x) divides a(x) for each nonzero c$\in F$;
(2) Every divisor of a(x) has degree less than or equal to deg a(x).

Proof: see textbook

*Definition: Let F be a field and a(x), b(x) $\in$ F[x], not both zero. The greatest common divisor (gcd) of a(x) and b(x) is the monic polynomial of highest degree that divides both a(x) and b(x). In other words, d(x) is the gcd of a(x) and b(x) provided that d(x) is monic and
(1) $d(x)|a(x)$ and $d(x)|b(x)$
(2) if $c(x)|a(x)$ and $c(x)|b(x)$, then deg c(x) < deg d(x)

Example 2, 3 in 4.2

*Thm 4.8:

Let F be a field, f(x), g(x) $\in F[x]$, not both zero. Then there is a unique gcd d(x) of f(x) and g(x). Furthermore, there exist (not necessarily unique) polynomials u(x) and v(x) such that
d(x) = f(x)u(x) + g(x) v(x).

*Cor 4.9
Let F be a field and a(x), b(x) $\in F[x]$, not both zero. A monic polynomial d(x) $\in F[x]$ is greatest common divisor of a(x) and b(x) if and only if d(x) satisfies these conditions:
(1) $d(x)|a(x)$ and $d(x)|b(x)$
(2)If $c(x)|a(x)$ and $c(x)|b(x)$, then $c(x)|d(x)$

*Thm 4.10
Let F be a field and a(x), b(x), c(x) $\in F[x]$. If $a(x)|b(x)c(x)$ and a(x) and b(x) are relatively prime, then $a(x)|c(x)$.

4.3 Irreducible and Unique Factorization

*f(x) is an associate of g(x) in F[x] if and only if f(x) = cg(x) for some nonzero c $\in$ F.

Ex: x^2 + 1 is an associate of $2x^2$ + 2 in $\mathbb{R}[x]$

* Definition:
Let F be a field. A nonconstant polynomial p(x) $\in$ F(x) is said to be irreducible if its only divisors are its associate and the nonzero constant polynomials (units). A nonconstant polynomial that is not irreducible is said to be reducible.

Ex: Every polynomial of degree 1 in F[x] is irreducible in F[x]

*Thm 4.11
Let F be a field. A nonzero polynomial f(x) is reducible in F[x] if and only if f(x) can be written as the product of two polynomials of lower degree.

Ex: x^2 +1 is irreducible in $\mathbb{R}[x]$ but it is reducible in $\mathbb{C}[x]$ since
x^2+1 = (x-i)(x+i)

*Thm 4.12
Let F be a field and p(x) a nonconstant polynomial in F[x]. Then the following conditions are equivalent:
(1) p(x) is irreducible.
(2) If b(x) and c(x) are any polynomials such that $p(x)|b(x)c(x)$, then $p(x)|b(x)$ or $p(x)|c(x)$
(3) If r(x) and s(x) are any polynomials such that p(x) = r(x)s(x), then r(x) or s(x) is a nonzero constant polynomials.

*Cor
Let F be a field and p(x) is an irreducible polynomial in F[x]. If $p(x)|a_1(x)a_2(x)...a_n(x)$, then p(x) divides at least one of the $a_i(x)$ for some i.

* Thm 4.14
Let F be a field. Every nonconstant polynomial f(x) in F[x] is a product of irreducible polynomials in F[x]. This factorization is unique in the following sense: If
f(x) = $p_1(x)p_2(x)...p_r(x)$ and
f(x) = $q_1(x)q_2(x)...q_s(X)$
with each $p_i(x)$ and $q_j(x)$ irreducible, then r=s (that is, the number of irreducible factors is the same). After the $q_j(x)$ are reordered and relabeled, if necessary
$p_i(x)$ is an associate of $q_i(x)$. (i=1, 2, 3, ... , r).

4.4 Polynomial Functions, Roots, and Reducibility

* Roots of Polynomials
Definition:
Let R be a commutative ring and f(x) $\in$ R[x]. An element a of R is said to be a root (or zero) of the polynomial f(x) if f(a)=0_R, that is, if the induced function f: R $\rightarrow$ R maps a to 0_R.

*Example 3, 4.

* Thm 4.15 The Remainder Theorem
Let F be a field, f(X) $\in$ F(x) and a $\in$ F. The remainder when f(x) is divided by the polynomial x-a is f(a).

Proof of Thm 4.15: By the Division Algorithm.

Ex: Find the remainder when f(x) = x^{79} + $3x^{24}$ + 5 is divided by x-1.

f(1) = 1+3+5= 9 is the remainder.

* Thm 4.16 The Factor Theorem
Let F be a field, f(x) $\in$ F[x] and a $\in$ F. Then a is a root of the polynomial f(x) if and only if x-a is a factor of f(x) in F[x].
(Proof see textbook)

Ex: Show f(x) = x^7 - x^5 + $2x^4$ - $3x^2$ -x +2 is reducible in $\mathbb{Q}[x]$
f(1) = 1 - 1 + 2 - 3 -1 + 2 = 0
then x-1 is a factor of f(x).

* Cor 4.17
Let F be a field and f(x) a nonzero polynomial of degree n in F[x]. Then f(x) has at most n roots in F.

* Cor 4.18
Let F be a field and f(x) $\in$ F[x] with degf(x) $\geq$ 2. If f(x) is irreducible in F[x] then f(x) has no roots in F.

The converse of Cor 4.18 is false in general.

* Cor 4.19
Let F be a field and let f(x) $\in$ F[x] be a polynomial of degree 2 or 3. Then f(x) is irreducible in F[x] if and only if f(x) has no roots in F.

* Cor 4.20
Let F be an infinite field and f(x), g(x) $\in$ F[x]. Then f(x) and g(x) induce the same function from F to F if and only if f(x) = g(x) in F[x].

4.4 2-11,15,17,27,29 suggested problems

4.5 Irreducibility in $\mathbb{Q}[x]$

* Thm 4.21 Rational Root Test
Let f(x) = $a_nx^n + a_{n-1}x^{n-1} + ... + a_0$ be a polynomial with integer coefficient. if r $\neq$ 0 and the rational number r/s (in lowest terms) is a root of f(x). then $r|a_0$ and $s|a_n$.

Ex 1 in textbook.

* Lemma 4.22

Let f(x), g(x), h(x) $\in \mathbb{Z}[x]$ with f(x) = g(x) h(x). If p is a prime that divides every coefficient of f(x), then either p divides every coefficient of g(x) or p divides every coefficient of h(x).

Proof: if f(x) is a constant polynomial
if c = ab
$p|c$ implies $p|a$ or $p|b$ (Thm 1.5)
if deg f = 1, f(x) = px+2p = p(x+2) = g(x)h(x)
at least one is a constant

* Thm 4.23

Let f(x) be a polynomial with integer coefficients. Then f(x) factors as a product of polynomials of degree m and n in $\mathbb{Q}[x]$ if and only if f(x) factors as a product of polynomials of degree m and n in $\mathbb{Z}[x]$

Ex: f(x) = $x^4 - 5x^2 + 1$, prove f(x) is irreducible in $\mathbb{Q}[x]$.
x + 1 or x - 1 are only possible rational factors.
f(1) $\neq$ 0, f(-1) $\neq$ 0 $\Rightarrow$ f(x) doesn't have rational factors.

* Only possible way to factor f(x) is two products of degree 2 polynomials.
f(x) = $(x^2 + ax + b)$*$(x^2 + cx + d) = x^4 - 5x^2 + 1$
Then we have:
1. a = -c
2. 5 = $c^2 - b - d$
3. bd =1

Then we have c^2 = 7 or c^2 =3 but c $\notin \mathbb{Q}[x]$
Therefore, we conclude that f is irreducible.

* Thm 4.24 Eisenstein's Criterion

Let f(x) = $a_n x^n + a_{n-1}x^{n-1}$ + ... + a_0 be a nonconstant polynomial with integer coefficients. If there is a prime p such that p divides each a_0, a_1, ..., a_{n-1}, but p does not divide a_n and p^2 does not divide a_0, then f(x) is irreducible in $\mathbb{Q}[x]$.

Ex: f(x) = $x^{17} + 6x^{13} - 15x^4 + 3x^2 - 9x + 12$
prove f(x) is irreducible in $\mathbb{Q}[x]$
p = 3 divides a_{n-1}, a_{n-2}, ... , a_0
but p does not divide 1 and p^2 does not divide 12
Therefore, we say f(x) is irreducible.

Ex: $x^9 + 5$ is irreducible or reducible in $\mathbb{Q}[x]$
p = 5
p^2 does not divide 5
so $x^9 + 5$ is irreducible.