(23)

EXAMPLES :-

If F is a field and d is a poly... F, the set $M = dF[x]$, of all multip... of d by arbitrary f in $F[x]$, is an ... For M is non-empty, M in fact contain... If $f, g \in F[x]$ and c is a scalar, the... $c(df) - dg = d(cf - g) \in M$, so that M is ... subspace. Finally M contains $(df)g = d(fg)$ as well. The ideal M is called the principal ideal generated by d. $M = (d)$

2. Let $d_1, \dots, d_n$ be a finite number of polynomials over F. Then the sum M of the subspaces $d_i F[x]$ is a subspace and is also an ideal. For suppose $p \in M$. Then $\exists$ polynomials $f_1, \dots, f_n$ in $F[x]$ such that $p = d_1 f_1 + \dots + d_n f_n$. If g is an arbitrary polynomial over F, then $pg = d_1(f_1 g) + \dots + d_n(f_n g)$ so that pg also belongs to M. Thus M is an ideal, and we say that M is the ideal generated by the polynomials $d_1, \dots, d_n$.

Theorem :- 7

If F is a field, and M is any non-zero ideal in $F[x]$, there is a unique monic polynomial d in $F[x]$ such that M is the principal ideal generated by d.

Proof :-

By assumption, M contains a non-zero polynomial, among all non-zero polynomials in M there is a polynomial d of minimal degree.

We may assume d is monic.

Now if $f \in M$, by known theorem shows that $f = dq + r$ where $r = 0$ (or) $\deg r < \deg d$.

since d is in M, dq and $f - dq = r$ also belong to M.

Because d is an element of M of minimal degree we cannot have $\deg r < \deg d$, so $r = 0$.

Thus $M = dF[x]$.

If g is another monic polynomial such that $M = gF[x]$, then $\exists$ non-zero polynomials p, q such that $d = gp$ and $g = dq$.

Thus $d = dpq$ and $\deg d = \deg d + \deg p + \deg q$.

Hence $\deg p = \deg q = 0$, and as d, g are ~~monic~~ monic, $p = q = 1$.

Thus $d = g$.

This completes the proof of the theorem.

Corollary :-

If $p_1, \dots, p_n$ are polynomials over a field F, not all of which are zero, there is a unique monic polynomial d in $F[x]$ such that (a) d is in the ideal generated by $p_1, \dots, p_n$.

(b) d divides each of the polynomials p_i.

Any polynomial satisfying (a) and (b) necessarily satisfies

(c) d is divisible by every polynomial which divides each of the polynomials $p_1, \dots, p_n$.

Proof :-

Let d be the monic generator of the ideal $p_1 F[x] + \dots + p_n F[x]$.

Every member of this ideal is divisible by d.

Thus each of the polynomials p_i is divisible by d.

Now suppose f is a polynomial which divides each of the polynomials $p_1, \dots, p_n$.

Then $\exists$ polynomials $g_1, \dots, g_n$ such that $p_i = f g_i$, $1 \le i \le n$.

Also since d is the ideal:

$$p_1 F[x] + \dots + p_n F[x]$$

$\exists$ polynomials $q_1, \dots, q_n$ in $F[x]$ such that $d = p_1 q_1 + \dots + p_n q_n$.

$$\text{Thus } d = f\left[g_1 q_1 + \dots + g_n q_n\right].$$

We have shown that d is a monic polynomial satisfying (a), (b) and (c).

If d' is any polynomial satisfying (a) and (b) it follows, from (a) and the defn of d that d' is a scalar multiple of d and satisfies (c) as well.

Finally, d' is a monic polynomial, we have $d' = d$.

This completes the proof of the corollary.

DEFINITION :-

If $p_1, \ldots, p_n$ are polynom... are ... field F, not all of which ... ideal $p_1 F[x$ ... monic generator d of the ... is called the greatest common divisor ... $p_1, \ldots, p_n$.

DEFINITION :-

The polynomials $p_1, \ldots, p_n$ are relatively prime if their greatest common divisor is one (or) equivalently if the ideal they generate is all of $F[x]$.

THE PRIME FACTORIZATION OF A POLYNOMIAL

DEFINITION :-

Let F be a field. A polynomial f in $F[x]$ is said to be reducible over F $\exists$ polynomials g, h in $F[x]$ of degree ≥ 1 such that $f = gh$, and if not, f is said to be irreducible over F.

DEFINITION :-

A non-scalar irreducible polynomial over F is called a prime polynomial over F, and we sometimes say it is a prime in $F[x]$.

the ... polynomial ... then either ... Proof :-

Theorem :- 8

Let p, f and g be polynomials over the field F. Suppose that p is a prime polynomial and that p divides the product fg. Then either p divides f (or) p divides g.

Proof :-

Without loss of generality to assume that p is a monic prime polynomial.

The fact that p is prime then only monic divisors of p are 1 and p.

Let d be the g.c.d of f and p.

$d = (f, g) = 1$ $d = 1$

Then either $d = 1$ (or) $d = p$, since d is a monic polynomial which divides p.

If $d = p$, then p divides f.

Suppose $d = 1$. ie suppose f and p are relatively prime.

We shall P.T p divides g.

Since $(f, p) = 1$, there are polynomials f_0 and p_0 such that $1 = f_0 f + p_0 p$.

Multiplying by g, we obtain

$$g = f_0 f g + p_0 p g$$

$J = (fg)f_0 + p(P_0 g)$.

Since p divides fg it divides $(fg)f_0$,

and certainly p divides $p(P_0 g)$.

Thus p divides g.

This completes the proof of the theorem.

Corollary :-

If p is a prime and divides a product $f_1 \cdots f_n$ then p divides one of the polynomials $f_1, \ldots, f_n$.

Proof :-

The proof is by induction.

When $n = 2$, the result is the statement of known theorem.

Suppose we have proved the corollary for $n = k$, and that p divides the product $f_1 \cdots f_{k+1}$ of some $(k+1)$ polynomials.

Since p divides $(f_1 \cdots f_k) f_{k+1}$, either p divides f_{k+1} (or) p divides $f_1 \cdots f_k$.

By the induction hypothesis, if p divides $f_1 \cdots f_k$, then p divides f_i for some i, $1 \le i \le k$.