0.1 Algebras

Definition 0.1.1: Algebra

F-algebra A or linear algebra A/F is an F-v.s. with a product structvue $A \times A \to A$ which has ass., dis., comm. where multiplication is not necesserily comm. If A has an element $1_A \in A$ s.t. $\forall \alpha \in A$ $(1_A \cdot \alpha = \alpha \cdot 1_A = \alpha)$ then we say A is an F-algebra with 1.

Example 0.1.1

(i) $F[x]$: finite polynomial with coeff. in F is F-algebra with unity 1.
(ii) $F[[x]]$: formal power series in x with coeff. in F : $\sum_{i=1}^{\infty} a_i x^i$ form is F-algebra with unity 1.
(iii) Suppose $n \geq 1$ with field F. $M_{n\times n}(F)$: F-algebra with unity $1_A = I_n$
(iv) V : F-v.s. $A = L(V, V)$ is F-algebra with unity $1_A = Id_V$ with $+$ and $\circ$.

0.2 The Algebra of Polynomials

Note:-

$f, g \in F[x]$. $f := \sum a_i x_i$, $g := \sum b_j x_j$ We say $f = g \iff \forall i = j$ $(a_i = b_j)$. But this is not equiv. to say that $\forall \alpha \in F$ $(f(\alpha) = g(\alpha))$.

Example 0.2.1

$F = \mathbb{Z}/p$. Then Fermat's Little Theorem says $\forall \alpha \in F$ $(\alpha^p \equiv \alpha)$. Consider $f = 1 + x^p$ and $g = 1 + x$. Then $f \neq g$ but $f(\alpha) = g(\alpha)$.

Definition 0.2.1: Degree of Polynomials

Suppose $f \in F[x] \backslash \{0\}$. Degree of f is defined to be n if $f = a_0 + \cdots + a_n x^n$ with $a_n \in F \backslash \{0\}$. Note that we don't define degree of 0.

Definition 0.2.2: Monic

$f \in F[x] \backslash \{0\}$ is monic if the coeff. of highest deg. is 1.

Exercise 0.2.1

$f, g \in F[x] \backslash \{0\}$. Then $fg \in F[x] \backslash \{0\}$ where $\deg(fg) = \deg(f) + \deg(g)$ and if f, g is monic, fg either.

Definition 0.2.3: Evaluation

A is an F-algebra and $f(x) \in F[x]$ where $f = \sum_{i=0}^{n} a_i x^i$. Let $\alpha \in A$ be a fixed element. Define $f(\alpha) = \sum_{i=0}^{n} a_i \alpha^i$ and we call it the evaluation of α in $f(x)$.
$ev_\alpha : F[x] \to A : f(x) \mapsto f(\alpha)$. $f_1 + f_2$, $f_1 f_2$, cf_1 are all respected.

Definition 0.2.4: Homomorphism

Let A_1 and A_2 be both F-algebras. A function $\varphi : A_1 \to A_2$ is called a homomorphism of F-algebra if:

1. It is an F-lin. trans.
2. $\varphi(\alpha_1\alpha_2) = \varphi(\alpha_1)\varphi(\alpha_2)$

Theorem 0.2.1 Euclidean Algorithm on $F[x]$

$f, g \in F[x]$ for nonzero g with property $\deg(f) \geq \deg(g)$. $\exists q \in F[x]$ $(r = f - qg)$. we have either $r = 0$ or $r \neq 0$ for $\deg(r) < \deg(g)$.

Note:-

In modern algebra, a ring with this property is called an Euclidean domain.

Definition 0.2.5: Divisibility

If $r = 0$, $f = qg$. Then we denote this situation as $g \mid f$.

Lemma 0.2.1

$f(x) \in F[x] \backslash \{0\}$, $(x-c) \in F[x]$ for $c \in F$. Then $(x-c) \mid f(x) \iff f(c) = 0$.

Proof. $f = qg + r = q(x-c) + r$. Then $f(c) = r$, so $(x-c)|f \iff r = 0$. These are called a zero, solution, or root of f. □

Exercise 0.2.2

$f(x) \in F[x]$, $\deg(f) = n \geq 1$. Then f has at most n roots.

0.3 Lagrange Interpolation

This Chapter is Intentionally Skipped at Lectures

0.4 Polynomial Ideals

Definition 0.4.1: Ideals

F : field. $F[x]$: polynomial ring over F. An ideal $M \subset F[x]$ is an F-subspace s.t. if $f \in F[x]$ and $g \in M$, then $fg \in M$.

Example 0.4.1

$M = (x)$: poly. divisible by x.

Definition 0.4.2: Principal Ideal

An ideal of the form $M = (g_0)$: poly. divisible by g_0 is called a principal ideal.

Theorem 0.4.1

F : field. $M \subset F[x]$: a nonzero ideal. Then M is a principal ideal given by a monic.

Proof. Since $M \neq 0$, M does contain nonzero poly. So, the set of deg. of nonzero poly. in $\mathbb{N}_0$ is nonempty. Let $g_0 \in M$ hs the minimal possible deg. If $g_0 = a_d x^d + \cdots a_1 x + a_0$, then $\frac{1}{a_d} g_0 = x^d + \cdots$ with the same deg. So using this instead, call it g_0, the g_0 is monic.

Claim 0.4.1

$M = (g_0)$.

Proof. $g_0 \subset M$ is obvious.

$(M \subset g_0)$: N.T.S. $\forall f \in M \ (f = qg_0)$. By the Euclidean algorithm, $\exists q, r \in F[x] \ (f = g_0 q + r)$. Suppose $r \neq 0$. Then $f = qg_0 + r$ with $\deg(r) < \deg(g_0)$. But $r = f - qg_0$ where $f, g_0 \in M$, $r \in M$. This is contradiction to minimality of g. Thus $r = 0$, which means f is multiple of g_0. □

□

Note:-

By putting g_0 monic, g_0 is also unique.

Corollary 0.4.1

$p_1, p_2, \cdots, p_n \in F[x]$ not all zero. Then $\exists!$ monic $g_0 \in F[x]$ s.t.

i) $p_1 F[x] + \cdots + p_n F[x] = (g_0)$

ii) $\forall i \ (g_0 \mid p_i)$

iii) if $f \mid p_i$ for all i, then $f \mid g_0$. Such g_0 is called G.C.D. of p_i.

Proof. Check $p_1 F[x] + \cdots + p_n F[x]$ is an ideal. By this, $M \neq 0 \Rightarrow \exists! g_0 \ ((g_0) = M)$. Also, $(p_i) \subset M = (g_0) \Rightarrow p_{\in}(g_0) \Rightarrow g_0 \mid p_i$. Also, $f \mid p_i \Rightarrow p_i = f h_i$ thus $g_0 = f h_1 F[x] + \cdots + f h_n F[x] \Rightarrow f \mid g_0$. □

Definition 0.4.3: Coprime (Relatively Prime)

p_i are coprime of relatively prime if $\gcd(p_1, \ldots, p_n) = (1)$.

0.5 The Prime Factorization of a Polynomial

Definition 0.5.1: Reducible

F : field. $f \in F[x] \backslash \{0\}$. We say f is reducible if $f = gh$ for some $g, h \in F[x]$ where $\deg(g), \deg(h) \geq 1$. If we can't, we say it is irreducible.

Definition 0.5.2: Prime Element

We say f is a prime element if it has property that whenever $f \mid gh$, either $f \mid g$ or $f \mid h$.

Example 0.5.1

F : field. f : poly. of deg. 1 in $F[x]$ is irreducible.

Example 0.5.2

$F:\mathbb{R}$. $f(x)=x^2+ax+b$. f is irreducible $\iff$ f has a root in $\mathbb{R}$ $\iff$ $D\geq 0$.

Example 0.5.3

$F:\mathbb{F}_p=\mathbb{Z}/p$. Then there are many irreducible poly. of deg. d.

Theorem 0.5.1

Let $p(x)\in F[x]\backslash\{0\}$. Then it is irreducible $\iff$ it is prime.

Proof. $(\Leftarrow)$: Suppose it is reducible. $p=gh$ for some $g,h\in F[x]$ with $\deg.\geq 1$. Since p is prime, $p\,|\,g$ or $p\,|\,h$. But then, $\deg(p)\leq\deg(g)$ or $\deg(p)\leq\deg(h)$. But this is impossible since $\deg(g),\deg(h)<\deg(p)$.

$(\Rightarrow)$: $\gcd(p,g)=(d)\Rightarrow d\,|\,p\Rightarrow p$ is irreducible, so $d=1$ or $d=p$. If $d=p$, $d\,|\,g$ leads $p\,|\,g$. If $d=1$, $\exists p_0,g_0$ $(pp_0+gg_0=1)$. Thus $php_0+ghg_0=h$ leads $p\,|\,h$. □