H + K, Chap 4, Pol's.

Algebra A over a field F:

A v.s. over F
$(+,$ sc. mult)

together with mult. law on A
— compatible: assoc.
distrib. over +

$c(\alpha\beta) = (c\alpha)\beta = \alpha(c\beta)$
$c \in F \quad \alpha, \beta \in A$

If we have a mult id in A:
"alg. with identity"

If mult. is commutative:
"Commutative alg"

Ex. $M_n(F)$, +, sc. mult, mx mult
dim n^2 mult id: id. mx $I = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$
Not comm unless $n=1$

Ex. $L(V) = End(V)$
$V \to V$ lin. ops. on V
dim $= n^2$ if $\dim V = n$
non-comm unless $\dim V = 1$.

E.g. $V = F^n$:

$L(V) \xrightarrow{\sim} M_n(F)$ iso of algs

+, sc. mult, comp $\circ$ | +, sc. mult, mx mult.

Ex $F[x] = \{$polys $f(x)$ with coeffs in $F\}$

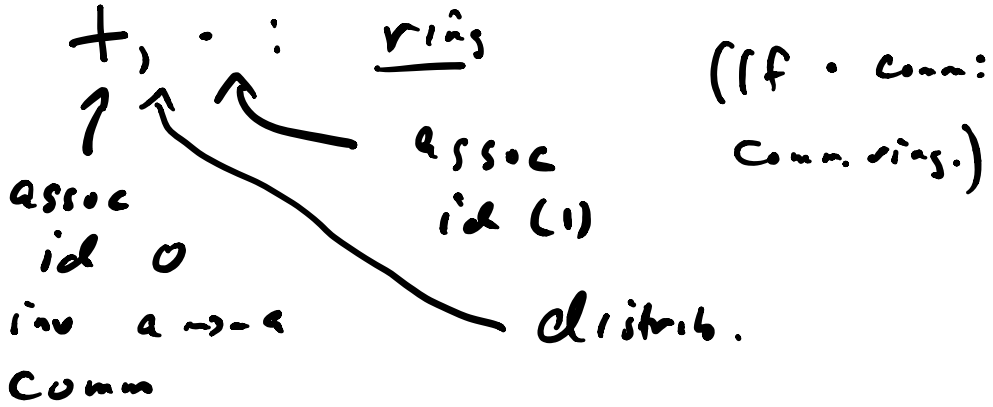
alg +, sc. mult, poly mult

alg. w id (1)

Comm. dim $F[x]$: inf.

Basis: $1, x, x^2, \ldots$

Another description of alg.^{A} w id over F



Ex. $\mathbb{Z}$ = {integers}, comm ring.

alg $\rightarrow$ $F[x]$: comm ring

(over F) $\mathbb{Z}[x]$: " "

a/s → $F[x,y]$: " "

→ $M_n(F)$: ring not comm unless $n=1$.

A v.s. A is an algebra over F (w. id)

if: also have sc. mult

that makes A into a v.s. over F

+ st $c(\alpha\beta) = (c\alpha)\beta = \alpha(c\beta)$

$1\alpha = \alpha$ $\quad (c_1 c_2)\alpha = c_1(c_2\alpha)$

$c(\alpha+\beta) = c\alpha + c\beta$ $\quad (c_1+c_2)\alpha = c_1\alpha + c_2\alpha$

Homomorphism of a/s's?

" " rings?

$T: A \to B$ hom:

rings $T(a_1+a_2) = T(a_1) + T(a_2)$

$T(a_1 a_2) = T(a_1)T(a_2)$

$T(0) = 0$ [automatic]

$T(1) = 1$

$T: A \to B$ hom:
a/s's over F

• hom of v.s.'s, ↓
• " " rings.

v.s.: $T: V \to W$ lin. tr.
is injective $\iff \ker T = 0$.

rings: $T: A \to B$ hom of rings
is inj $\iff \ker T = 0$.

algs: $T: A \to B$ hom of algs
is inj $\iff \ker T = 0$.

As f.d. v.s.'s: A hom is
invertible (iso) $\iff$ bijective.

Ex. $M_n(F) \xrightarrow[T]{\sim} End(F^n)$

$A \longmapsto T_A$ $\quad T_{A+B} = T_A + T_B$

$[T_A(v)] = A[v]$ $\quad T_{cA} = cT_A$

iso of algs.

$T_{AB} = T_A \circ T_B$

Alg. of poly $F[x]$

Division algorithm:

If $f(x), g(x) \in F[x]$,
$+ g(x) \neq 0$

Then $\exists\ q(x), r(x)$ s.t.

$$f(x) = g(x)q(x) + r(x)$$

where <u>either</u> $r(x), f(x) = g(x)q(x)$

<u>or</u> $\deg r(x) < \deg g(x)$

Ex. $f(x) = x^2$, $g(x) = x-1$, $\deg = 1$

$$f(x) = x^2 = (x-1)(x+1) + 1$$

$q(x)$ $r(x)$, $\deg = 0 < 1$

<u>Poly. division</u>

Analogous to div. algorithm for integers

Ex. $a = 13$, $b = 5$ s.t. $b \neq 0$

$\exists\ q, r$ $a = bq + r$ $13 = 5 \cdot 2 + 3$

$0 \leq r < |b|$ q r

Poly div — div. alg. for $F[x]$.

→ Now F is a field.

Ex. Fails for $\mathbb{Z}[x]$.

Can't divide x^2 by $2x$ + get a remainder

→ need one variable.

Ex $\mathbb{R}[x,y]$

Can't divide x by y + get remainder

Applic's + lin. alg.

A $n \times n$ matrix over F

$f(x) \in F[x]$

Can evaluate $f(x)$ on A.

Ex. $f(x) = x^2 - 2x + 1$.

$$f(A) = A^2 - 2A + I$$

Given A

$I = \{f(x) \in F[x] \mid f(A) = 0\}$

$\neq 0$

poly

We will show:

$\exists$ poly $P_A(x)$ of deg $= n$

(the characteristic poly of A)

s.t. $P_A(A) = 0$

So $P_A(x) \in I$

Consider all the degrees of non-0 polys in I. ↑ one of them is n.

Let d be the smallest of these.

$0 \le d \le n$

Let $p(x) \in I$, of degree d

↑ This exists

$p(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0$

Mult by $1/a_d$ $\quad a_d \neq 0$

WMA $p(x)$ is monic

↑ top coeff $= 1$.

Thm For every poly $f(x) \in I$

$p(x)$ divides $f(x)$.

(& vice versa $\quad (f(x) = p(x) g(x).)$ $\quad p(x) \mid f(x)$

Pf: by div. alg. for polys.

$p(x) \neq 0$ $\quad$ $\deg p(x) = d$

Div. alg. applies.

$$f(x) = p(x)\,q(x) + r(x)$$

r: 0 or lower deg (deg $r <$ deg $p(x)$)

$$r(x) = f(x) - p(x)\,q(x)$$

$$r(A) = f(A) - p(A)\,q(A) = 0$$

$f(A) = 0$, $p(A) = 0$

$r(x) \in I$

$p(x)$ has smallest degree among all non-0 polys in I.

But r has smaller degree.

$\therefore r(x) = 0$. $\quad f(x) = p(x)\,q(x)$

A, I, $p(x) \in I$ (monic) minimal degree

Every poly in I is div by $p(x)$.

In particular, $p_A(x)$ (char poly, deg n) $\cdots\cdots\cdots p(x)$.

Write $p(x) = p_A(x)$

minl poly of A.

Note: $p_A(x)$ is unique.

Recall: Say $p(x), s(x) \in I$ of deg d, monic.

p_{minl}

$p(x) \mid s(x)$ $\quad$ $s(x) \mid p(x)$

(interchanging role of p, s)

So: $p(x) = s(x)$

Some general comments; $F[x]$

Above we needed 2 facts about I:

i) If $f(x), g(x) \in I$ then $f(x)+g(x) \in I$.

ii) If $f(x) \in I$ & $g(x) \in F[x]$ then $f(x)g(x) \in I$.

More generally: $\not\in \phi$

For any subset $I \subset F[x]$ (or in any comm. ring)

if I satisfies (i), (ii),

we call I an **ideal** of F.

Same argument generalizes

If $I \subset F[x]$ is an ideal,
then $\exists\, p(x) \in I$ st <u>every</u>
element of I is a poly. multiple of $p(x)$:

$$I = \{ p(x) g(x) \mid g(x) \in F[x] \} \quad (*)$$

If I contains any non-0 p.ly's,
then we can take $p(x)$ to be monic.
Otherwise, $I = \{0\}$, $p(x) = 0$.

Conversely, if $p(x) \in F[x]$,
then $\{ p(x) g(x) \mid g(x) \in F[x] \}$
is an ideal. ← "<u>principal ideal</u>"

So: In $F[x]$, every ideal is principal.

Key: div. alg.

$\mathbb{Z}$ also has a div. alg.
$\therefore$ In $\mathbb{Z}$, every ideal is principal.
⟹ Unique factorization!

In $F[x]$: every non-0 poly is a product of irreducible p.b's unique up to order & up to mult by const.

$$x^2 - 1 = (x+1)(x-1)$$

In $\mathbb{Z}$ every non-0 integer is a product of primes, unique up to order & up to mult by ± 1:

$$6 = 2 \cdot 3$$

$\mathbb{Z}[x]$, $F[x,y]$; n.c. div alg.

$\exists$ non-principal ideals.

Nevertheless, these two rings do have unique fact'n (different proof)

Some rings don't have unique fact'n.

$$\mathbb{Z}[\sqrt{-5}] = \{ a + b\sqrt{-5} \mid a, b \in \mathbb{Z} \}$$

Non-unique factorization

$$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$$

More: H+K, Chap 4 (370/502)