LAIS, Lecture #10

Dfn 1 An ideal of $K[x]$ is a subset I, closed under subtraction and closed under multiplication by elements of $K[x]$. ☺

Dfn 2 $p_1, \dots, p_s \in K[x]$, the ideal generated by p_i's

$$(p_1, \dots, p_s) = \left\{ \sum_{i \in [s]} r_i p_i,\ r_i \in K[x] \right\}$$

☺

Ex 3 $x^2-1,\ x^3+1 \in K[x]$

$$(x^2-1, x^3+1) = \left\{ r_1(x^2-1) + r_2(x^3+1) \right\} \quad \forall r_1, r_2 \in K[x]$$

☺

Prp 4 $K[x]$ is a "Euclidean Division Domain." In particular, $\forall f(x), g(x) \in K[x]$ there exist unique $q(x), r(x) \in K[x]$, with $\deg r(x) < \deg g(x)$ s.t.

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

☺

Prp 5 $k[x]$ is a "Principal Ideal Domain". In particular, for every ideal I of $k[x]$ $I = (p(x))$, where $p(x)$ is the unique monic polynomial of smallest degree in I.

Prf $f(x) \in I$

Divide $f(x)$ with $p(x)$

$$\underbrace{f(x)}_{\in I} = \underbrace{q(x)p(x)}_{\in I} + r(x)$$

$\deg r(x) < \deg p(x)$

$r(x) \in I \Rightarrow r(x) = 0$

$\Rightarrow f(x) = q(x)p(x)$ $\square$

Prp 6 $(p_1(x), \dots, p_s(x)) = (p(x))$

$p(x) = \gcd(p_1(x), \dots, p_s(x))$

Prf By Prp 5 $(p_1, \dots, p_s) = (p)$ for some p. So $p_i \in (p)$

$\Rightarrow p_i = q_i p$ for some q_i

$\Rightarrow p \mid p_i \ \forall i \Rightarrow p \mid \gcd(p_1, \dots, p_s)$

$p(x) = r_1(x)p_1(x) + \dots + r_s(x)p_s(x)$

$\Rightarrow \gcd(p_1, \dots, p_s) \mid p.$ $\square$

Cor 7 If $p(x), q(x)$ are coprime then $\exists\ \alpha(x), \beta(x)$ s.t.
$$\alpha(x)p(x)+\beta(x)q(x)=1$$
\beta

Prf By Prp 6
$$(p(x),q(x)) = (\gcd(p(x),q(x))) = \underbrace{(1)}_{k[x]}$$
∎

Dfn 8 $p(x)$ is called irreducible if whenever $p(x)=\alpha(x)\beta(x)$ then either $\alpha(x)\in k$ or $\beta(x)\in k$ ∎

Prp 9 $k[x]$ is a "Unique Factorization Domain". In particular, for every $p(x)\in k[x]$ $\exists$ unique monic, distinct, irreducible polynomials $p_1(x),\dots,p_s(x)$ and $c\in k$ s.t.
$$p(x)=c\,p_1^{l_1}(x)\cdots p_s^{l_s}(x)$$
∎

$A\in k^{n\times n}$

$$\varphi_A : k[x] \longrightarrow \mathrm{End}(k^n)$$
$$1, x, x^2, \dots, x^{n^2} \longmapsto I, A, A^2, \dots, A^{n^2} \in k^{n\times n}$$

φ:

Rem 10 I, are $\Rightarrow$ ...

-zation Domain".

-ticular, for

$p(x) \in k[x]$ $\exists$

monic, distinct, irreducible

-mials $p_1(x), \dots, p_s(x)$

$\in k$ s.t.

$c\, p_1(x)^{l_1} \cdots p_s(x)^{l_s}$ ☺

$k^{n\times n}$

$k[x] \longrightarrow End(k^n)$

$x^2, \dots, x^{n^2} \mapsto I, A, A^2, \dots, A^{n^2} \in k^{n\times n}$

$\varphi: R \longrightarrow S$ ring homomorphism

$Ker\varphi$: ideal

Rem 10 $I, A, A^2, \dots, A^{n^2}$ are l.d. in $k^{n\times n}$

$\Rightarrow \exists\, c_0, \dots, c_{n^2} \in k$ s.t.

$c_{n^2} I + c_{n^2-1} A + c_{n^2-2} A^2 + \cdots + c_0 A^{n^2} = 0$

$p(x) = c_0 x^{n^2} + c_1 x^{n^2-1} + \cdots + c_{n^2-1} x + c_{n^2}$

$p(x) \in Ker\varphi_A$

Prp 11 $R \xrightarrow{\varphi} S$ ring homomorphism

$Ker\varphi$: ideal of R ☺

LAIS, Lecture #10

Dfn 12. The minimal polynomial $m_A(x)$ of A is the unique monic generator of $\mathrm{Ker}\,\varphi_A$.

Dfn 13 S : subset of K^n

$$\underbrace{\mathrm{ann}(S)}_{\text{ideal}} = \{ f(x)\in K[x] : f(x)v = 0 \ \forall v\in S \}$$

$\varphi_A(f(x))v$

Prp 14 $\mathrm{ann}(K^n) = \{ f(x)\in K[x] : f(x)v=0 \ \forall v\in K^n \} = \mathrm{Ker}\,\varphi_A$
$= (m_A(x))$.

$A^d v\in V$

Dfn 15 A subspace $V\subset K^n$ is called A-invariant if $Av\in V$ $\forall v\in V$.

Prp 16 V: A-invariant

$\tau_A|_V : V \longrightarrow V$

$\mathrm{ann}(V) = (m_{\tau_A|_V}(x))$

Dfn 17 An A-invariant subspace V is called cyclic, if $\exists\, v\in V$ s.t. $v, Av, A^2v, \dots, A^{d-1}v$ is a basis for V.

Dfn 18 $v \in k^n$

the cyclic subspace generated by v

$\mathrm{Span}(v, Av, A^2v, \dots)$ $\ominus$

Prp 20 $k[x]v$ is an A-cyclic subspace of dimension $\deg(p(x))$ where $(p(x)) = \mathrm{ann}(v)$.

Prf check $k[x]v$ is A-invariant: $\xi \in k[x]v$

$\xi = f(x)v \Rightarrow A\xi = A(f(x)v)$

$A\xi = x\xi = \underbrace{xf(x)}_{g(x)}v = g(x)v \in k[x]v$...

Lem 19

Let d be maximal s.t. $v, Av, \dots, A^{d-1}v$ are l.i.

So $A^dv = c_{d-1}v + c_{d-2}Av + \dots + c_0A^{d-1}v$ for some c_i's. $\Rightarrow$

$A^dv - c_0A^{d-1}v - \dots - c_{d-2}Av - c_{d-1}v = 0$

$p(x) = x^d - c_0x^{d-1} - \dots - c_{d-2}x - c_{d-1}$

Claim: $(p(x)) = \mathrm{ann}(v)$

Prf $p(x) \in \mathrm{ann}(v)$

$f(x) \in \mathrm{ann}(v)$

divide $f(x)$ with $p(x)$:

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

$\deg r(x) < \deg p(x)$

...imal

$\ldots^{d-1} v$ are l.i.

$\ldots c_{d-2} A v + \ldots + c_0 A^{d-1} v$

$\ldots \Rightarrow$

$\ldots - c_{d-2} A v - c_{d-1} v = 0$

$\ldots^{d-1} - \ldots - c_{d-2} x - c_{d-1}$

$\ldots = \operatorname{ann}(v)$

$\ldots v)$

$p(x)$:

$r(x)$

$r(x) \in \operatorname{ann}(v)$

$\Rightarrow r(x) = 0$ ☺

... Let $p(x)$ be as in Lem 19.

Then $x^i v \in k[x] v$ $\forall i$ and $\{x^i v\}_{i=0}^{d-1}$ are l.i.

$\Rightarrow \dim k[x] v \geq d$.

$\xi \in k[x] v \Rightarrow$

$\xi = f(x) v =$

$= [q(x) p(x) + r(x)] v$

$= r(x) v =$ l.c. of $\{x^i v\}_{i=0}^{d-1}$ ☺

Prp 9 $k[x]$ is a "Uni... Factorization Doma... In particular, for every $p(x) \in k[x]$ ... unique monic, distinct, irre... polynomials $p_1(x), \ldots$ and $c \in k$ s.t.

$p(x) = c\, p_1^{l_1}(x) \cdots p_s^{l_s}(x)$

$A \in k^{n \times n}$

$\varphi_A : k[x] \longrightarrow E\ldots$

$1, x, x^2, \ldots, x^{n^2} \mapsto I, \ldots$