Lezione del 23 marzo; Registro dettagliato

In questa lezione si e' tracciata a grandi linee la teoria degli anelli di polinomi con coefficienti in un anello commutativo in una indeterminata. Argomenti trattati:

(1) $A[x]$, con A anello commutativo; e' una $A-$algebra; proprieta' universale.

(2) $A[x]$, con A dominio d'integrita'; grado di un polinomio, proprieta'; $A[x]$ e' un dominio d'integrita'; relazione di divisibilita', polinomi associati; elementi invertibili; elementi irriducibili.

(3) $K[x]$, con K campo; e' una $K-$algebra; elementi invertibili; elementi irriducibili; divisione con resto; irriducibile equivale a primo; fattorizzazione unica.

(4) $\mathbb{Z}[x], \mathbb{Q}[x]$, e gli $\mathbb{Z}_p[x]$, irriducibilta'; lemma di Gauss; criterio di Eisenstein.

(5) $K[x]$, struttura; e' un dominio ad ideali principali; quozienti; quozienti campi e polinomi irriducibili.

(1) $A[x]$, con A anello commutativo.

$A[x]$ ha una struttura di $A-$modulo ed una struttura di anello commutativo fra loro compatibili, e' una $A-$algebra commutativa. Possiede una proprieta' universale un po' piu' forte di quella data in prima battuta.

Proposizione 1. *$A[x]$ e' un anello commutativo, si ha una immersione $i : A \to A[x]$, ed un elemento speciale $x \in A[x]$; per ogni anello commutativo B, ogni omomorfismo $j : A \to B$, ed ogni elemento $c \in B$, esiste uno ed un solo omomorfismo $\hat{j} : A[x] \to B$ tale che $j(a) = \hat{j}(i(a))$ per ogni $a \in A$, e $\hat{j}(x) = c$.*

In particolare, si ha

Proposizione 2. *Dati due anelli commutativi A e A', identificati tramite i monomorfismi canonici i, i' con sottoanelli di $A[x]$ e $A'[x]$, per ogni omomorfismo $f : A \to A'$, esiste uno ed un solo omomorfismo $\hat{f} : A[x] \to A'[x]$ tale che $i'(f(a)) = \hat{f}(i(a))$ per ogni $a \in A$, e $\hat{f}(x) = x$.*

(2) $A[x]$, con A dominio d'integrita'.

$A[x]$ e' un dominio d'integrita'.

Per ciascun polinomio non nullo $f = f(x) = a_0 + a_1 x + a_2 x^2 + \cdots$ in $A[x]$ si definisce il grado $\deg(f)$ come il massimo indice i tale che il coefficiente a_i sia diverso da zero; si definisce il grado del polinomio nullo ponendo $\deg(0) = -\infty$. Le operazioni e l'ordine su $\mathbb{N}$ si estendono nel modo solito a $\mathbb{N} \cup \{-\infty\}$; in particolare si ha $\deg(f) \geq 0$ se e solo se $f \neq 0$. La funzione grado $\deg : A[x] \to \mathbb{N} \cup \{-\infty\}$ possiede le proprieta'

$$\deg(f+g) \leq \mathrm{Max}(\deg(f), \deg(g)); \qquad \deg(fg) = \deg(f) + \deg(g).$$

La seconda proprieta' implica in particolare che un polinomio f in $A[x]$ e' invertibile in $A[x]$ se e solo se $f = a$ con $a \in A$ invertibile in A.

Per ogni f, g in $A[x]$ si dice che f divide g, e si scrive $f|g$ se e solo se esiste $h \in A[x]$ tale che $fh = g$ (cosi' ogni polinomio divide il polinomio nullo, ed il polinomio nullo divide solo se' stesso). La relazione "divide" su $A[x]$ e' riflessiva e transitiva, cioe' e' un preordine su $A[x]$; in generale non e' antisimmetrica e quindi in generale non e' un ordine parziale. Un polinomio f si dice associato a un polinomiio g se e solo se $f|g$ e $g|f$; la relazione "... e' associato a ..." e' una relazione d'equivalenza, e la relazione "... divide ..." induce una relazione d'ordine parziale sull'insieme delle classi d'equivalenza. Si ha che due polinomi f e g sono associati se e solo se $f = hg$ e $g = kf$, con h, k costanti in A invertibili (una inversa dell'altra).

Un polinomio f si dice irriducibile se e solo se f non e' nullo ne' invertibile e per ogni fattorizzazione $f = gh$ si ha che uno fra g ed h e' invertibile, e l'altro e' associato ad f.

(3) $K[x]$, con K campo.

$K[x]$ ha una struttura di $K-$spazio vettoriale ed una struttura di anello commutativo fra loro compatibili, e' una $K-$algebra commutativa; ha dimensione infinita, e base canonica $1, x, x^2, \ldots$

Gli elementi invertibili sono tutti e soli i polinomi costanti $\neq 0$, cioe' i polinomi di grado uguale a 0.

Un polinomio f risulta essere irriducibile se e solo se f non e' costante e per ogni fattorizzazione $f = gh$ si ha che almeno uno fra g ed h e' costante; in altri termini: f ha grado strettamente positivo e non si puo' scrivere come $f = gh$ con f, g polinomi di grado strettamente positivo.

Si ha l'operazione di divisione con resto:

Teorema 1. *Per ogni $f, g \in K[x]$ con $g \neq 0$ esistono e sono unici q ed r in $K[x]$ tali che*

$$f = qg + r, \quad \deg(r) < \deg(g).$$

Un polinomio f si dice primo se e solo se f non e' costante e ogni volta che f divide un prodotto gh si ha che f divide almeno uno fra i due fattori g, h. Si ha l'analogo del Lemma di Euclide:

Lemma 1. *In $K[x]$ ciascun polinomio irriducibile e' primo.*

Vale l'analogo del Teorema Fondamentale dell'aritmetica:

Teorema 2. *Ciascun polinomio non costante si puo' scrivere come prodotto di (un numero finito di) polinomi irriducibili; ogni due scritture di uno stesso polinomio hanno lo stesso numero di fattori e si possono riordinare in modo che fattori corrispondenti siano associati.*

Ce ne sono altre forme ...

(4) $\mathbb{Z}[x], \mathbb{Q}[x]$, e gli $\mathbb{Z}_p[x]$; irriducibilta'

Ogni polinomio in $\mathbb{Q}[x]$ e' associato ad un polinomio in $\mathbb{Z}[x]$ (associato in senso stretto, cioe' uguale a meno di una costante in $\mathbb{Q}$ non nulla), dunque lo studio dei polinomi in $\mathbb{Q}[x]$ irriducibili in $\mathbb{Q}[x]$ si riconduce allo studio dei polinomi in $\mathbb{Z}[x]$ irriducibili in $\mathbb{Q}[x]$. Il Lemma di Gauss afferma che se un polinomio non costante in $\mathbb{Z}[x]$ e' irriducibile in $\mathbb{Z}[x]$ allora esso e' anche irriducibile in $\mathbb{Q}[x]$. Il criterio di Eisenstein permette di costruire polinomi irriducibili in $\mathbb{Z}[x]$ e dunque anche in $\mathbb{Q}[x]$.

L'idea chiave e' quella di polinomio primitivo. Si dice che un polinomio $p(x) = a_n x^n + \cdots + a_1 x + a_0$ non costante in $\mathbb{Z}[x]$ e' primitivo se e solo se il massimo comun divisore dei suoi coefficienti e' 1. Si ha che ogni polinomio non costante in $\mathbb{Q}[x]$ e' associato (in senso stretto) ad un polinomio primitivo in $\mathbb{Z}[x]$.

Lemma 2. *(di Gauss, I) Il prodotto di due polinomi primitivi in $\mathbb{Z}[x]$ e' un polinomio primitivo.*

Lemma 3. *(di Gauss, II) Un polinomio non costante in $\mathbb{Z}[x]$ irriducibile in $\mathbb{Z}[x]$ e' irriducibile anche in $\mathbb{Q}[x]$.*

Dimostrazione della II parte. Sia $p(x)$ un polinomio non costante di $\mathbb{Z}[x]$ irriducibile in $\mathbb{Z}[x]$; supponiamo per assurdo che $p(x)$ sia riducibile in $\mathbb{Q}[x]$. Si ha una fattorizzazione $p(x) = g(x)h(x)$ con $g(x)$ e $h(x)$ polinomi di grado positivo in $\mathbb{Q}[x]$, e dunque anche una fattorizzazione $p(x) = \frac{d}{e}\, g_1(x)h_1(x)$ con $g_1(x)$ e $h_1(x)$ polinomi primitivi di grado positivo in $\mathbb{Z}[x]$ e d, e coprimi in $\mathbb{Z}$; da questa fattorizzazione si ha $e\, p(x) = d\, g_1(x)h_1(x)$; da cio' segue che e divide il polinomio $g_1(x)h_1(x)$, che e' primitivo per la I parte del Lemma di Gauss, e dunque $e = \pm 1$; si ha cosi' una fattorizzazione $p(x) = \pm d g_1(x)h_1(x)$ con $g_1(x)$ e $h_1(x)$ polinomi di grado positivo in $\mathbb{Z}[x]$, assurdo.

Proposizione 3. *(Criterio di Eisenstein). Sia $f(x) = a_n x^n + \cdots + a_1 x + a_0$ un polinomio primitivo in $\mathbb{Z}[x]$; se esiste un primo p tale che $p \not| a_n$, $p | a_i$ per ogni $n > i \geq 0$, e $p^2 \not| a_0$, allora $f(x)$ e' irriducibile in $\mathbb{Z}[x]$ e dunque, per il lemma di Gauss, anche in $\mathbb{Q}[x]$.*

Dimostrazione. Per assurdo $f(x)$ possieda una fattorizzazione propria $f(x) = g(x)h(x)$ con $g(x), h(x)$ polinomi di grado $i, j > 0$ in $\mathbb{Z}(x)$. L'omomorfismo canonico $\mathbb{Z}[x] \to \mathbb{Z}_p[x]$ fornisce una fattorizzazione $\bar{f}(x) = \bar{g}(x)\bar{h}(x)$ con $\bar{g}(x), \bar{h}(x)$ polinomi in $\mathbb{Z}_p[x]$. Per le ipotesi $p \not| a_n$ e $p | a_i$ per ogni $n > i \geq 0$, si ha $\bar{f}(x) = [a_n]x^n$ con $[a_n] \neq [0]$. Dunque $\bar{g}(x) = [b]x^i$ e $\bar{h}(x) = [c]x^j$ con $i, j > 0$. Allora p divide il termine costante di $g(x)$ ed il termine costante di $h(x)$, e dunque p^2 divide il termine costante di $g(x)h(x) = f(x)$, contro l'ipotesi $p^2 \not| a_0$.

(5) $K[x]$, con K campo, struttura

Se A e' un anello commutativo e $a \in A$, l'ideale (a) di A generato da a e' l'insieme dei prodotti ax ottenuti al variare di x in A; un ideale generato da un elemento si dice ideale principale.

Teorema 3. *Ogni ideale di $K[x]$ e' principale; ciascun ideale non nullo possiede uno ed un solo polinomio monico generatore.*

La dimostrazione segue dal teorema che fornisce la divisione con resto.

Teorema 4. *Sia $f(x)$ un polinomio monico di grado $n > 0$ in $K[x]$. Nell'anello quoziente $K[x]/(f(x))$, l'insieme dei polinomi di grado minore di n costituisce un sistema di rappresentanti per le classi di equivalenza; per ogni polinomio $p(x)$, il rappresentante canonico della classe di $p(x)$ e' dato dal resto della divisione di $p(x)$ su $f(x)$. In particolare $K[x]/(f(x))$ ha la base $[1], [x], \dots [x^{n-1}]$ ed ha dunque dimensione n.*

Una parte delle proprieta' dei quozienti propri di $K[x]$ deriva da fatti generali sulle $K-$algebre di dimensione finita.

Proposizione 4. *Una $K-$algebra di dimensione finita e' un dominio di integrita' se e solo se e' un corpo.*

Dimostrazione (parte non banale) Sia A una $K-$algebra di dimensione finita. Ciascun elemento $a \in A$ si puo' rappresentare come un endomorfismo di spazi vettoriali $t_a : A \to A$, $x \mapsto ax$; se $a \neq 0$, per l'ipotesi A dominio di integrita', questo endomorfismo e' iniettivo e dunque, per l'ipotesi A $K-$spazio vettoriale di dimensione finita, e' anche suriettivo; esiste allora un $a' \in A$ tale che $t_a(a') = 1$, cioe' $aa' = a$. Abbiamo cosi' provato che ciascun elemento non nullo di A posside un inverso destro; in modo analogo si prova che ciascun elemento non nullo di A possiede un inverso sinistro; cio' basta per affermare che ciascun elemento di A possiede un inverso bilatero.

Teorema 5. *Sia $f(x)$ un polinomio monico di grado $n > 0$ in $K[x]$. Le seguenti condizioni sono equivalenti: (1) $K[x]/(f(x))$ e' un domnio di integrita'; (2) $K[x]/(f(x))$ e' un campo; (3) $f(x)$ e' irriducibile.*