Corso:Algebra Anelli (Unimib)/Anelli/Teorema cinese dei resti

1 Definizioni utili

Definizione (313 Ideali coprimi)

In generale, sia R un anello commutativo. Siano I, J ideali di R . I, J si dicono *coprimi* se $I + J = R$.

Definizione (314 Somma e prodotto nel prodotto cartesiano di anelli)

Siano $R_1, R_2, \ldots, R_n$ anelli. Allora si dà al prodotto cartesiano $R_1 \times R_2 \times R_n$ una naturale struttura di anello. Si definiscono per ogni $X = (x_1, x_2, x_n)$ e $Y = (y_1, y_2, y_n)$ la somma $X+Y = (x_1+y_1, x_2+y_2, x_n+y_n)$ (calcolata rispettivamente negli anelli $R_1, R_2 R_n$) e il prodoto $XY = (x_1y_1, x_2y_2, x_ny_n)$.

2 Teorema cinese dei resti

Proviamo la seguente condizione $*$:

Proposizione (315 Condizione $\ast$)

per ogni $i = 1, n$, se considero l'ideale J_i e l'intersezione $\bigcap\{J_k\}$ con $k \neq i$, è anch'esso un ideale di R e la somma tra J_i e $\bigcap\{J_k\}$ è R . In altre parole, se gli ideali sono a due a due coprimi, allora uno è coprimo con l'intersezione degli altri.

Dimostrazione

Per ipotesi, per ogni $k \neq i$, $J_i + J_k = R$. Dunque esistono un elemento $a_i \in J_i$ e $a_k \in J_k$ tali che $a_i + a_k = 1_R$. Questo vale per ogni $k \neq j$. Segue che posso scrivere 1_R come il prodotto per ogni $k \neq i$ $\prod\{a_i + a_k\}$ al variare di i, k (prodotto di unità), dove per ogni ideale J_k con $k \neq i$ si ha che esiste a_k tale che $a_i + a_k = 1_R$.

Usando le proprietà distributive posso esplicitare il prodotto:

$$1_R = \prod(a_i + a_k) = J_i + \prod_{k \neq i} J_k$$

.

Ma siccome il prodotto è contenuto nell'intersezione si ha la seguente catena di inclusioni:

$$1_R = \prod(a_i + a_k) \subset J_i + \prod J_k \subset J_i + \bigcap_{k \neq i} J_k$$

.

Allora l'unità è contenuta nell'ideale intersezione, quindi l'ideale coincide con R . Ho provato che $J_i + \bigcap_{i \neq k} J_k = R$.

Osservazione (316)

Deduco che esistono un elemento $d_i \in J_i$ ed $e_i \in \bigcap_{k \neq i} J_k$ tali che $d_i + e_i = 1_R$.

Se $j \neq i$, applichiamo al primo e al secondo membro dell'uguaglianza la proiezione canonica π_j . Allora

$$1_{R/J_j} = \pi_j(d_i) + \pi_j(e_i) = \pi_j(d_i) + 0_{R/J_i}$$

(questo perché $e_j \in \bigcap I_k$ e quindi anche in e_J con $j \neq i$, la sua imagine è lo zero del quoziente).

In particolare, se $j \neq i$, $\pi_j(e_i) = 0_{R/J_j}$ Se $j = i$, $1_{R/J_i} = \pi_i(d_i) + \pi_i(e_i) = 0 + \pi_i(e_i)$. ($\pi_i(d_i) = 0$ perché $d_i \in J_i$ e la sua immagine mediante π è lo zero del quoziente) Si ha quindi $\pi_j(e_i)$ uguale all'unità $1_{R/J_i}$.

per ogni i e j , $\pi_j(e_i) = \delta_{ij}$ cioè il δ di Kroneker.

Teorema (317 Teorema cinese dei resti)

Sia R un anello commutativo e siano J_1, J_2, J_n n ideali di R a due a due coprimi. Sia per $i = (1, n)$ π_i la proiezione canonica da R all'anello quoziente rispetto all'anello J_i . Allora l'applicazione ϕ: $R \to R/J_1 * \cdots * R/J_n$ (anello prodotto degli anelli quoziente) definita ponendo per ogni $x \in R$, $\phi(x)$ uguale alla n -upla delle immagini di x mediante π_i , cioè $(\pi_1(x), \pi_2(x), \pi_n(x))$ è un epimorfismo di anelli con nucleo $\bigcap\{J_i\}$, in particolare $R/\ker f = \frac{R}{\bigcap\{J_i\}}$ è isomorfo a $R/J_1 \times \cdots \times R/J_n$

Dimostrazione

Si verifica immediatamente che ϕ è un morfismo di anelli e il nucleo è l'intersezione dei J_i , perché un elemento sta nel nucleo se per ogni i , $\pi_i(x) = 0$ nell'anello quoziente R/J_i . Ma lo zero dell'anello quoziente è J_i , quindi se $\pi_i(x)$ è uguale allo zero del quoziente, allora $\pi_i(x) = J_i$. Quindi è ovvio che $\ker \phi = \bigcap\{J_i\}$.

L'ipotesi che i due ideali sono a due a due coprimi serve per dimostrare che ϕ è suriettiva. Proviamo la suriettività di ϕ . Prendiamo una qualsiasi n -upla dell'anello prodotto, che chiamo $Y = (y_1, y_2, y_n)$ nell'anello di arrivo (prodotto dei quozienti) e ne prendo la controimmagine. Per ogni i prendo y_i e ne considero una preimmagine x_i nell'epimorfismo canonico, cioè $x_i = \pi^{-1}(y_i)$. Supponiamo che $x = \sum_{i=1}^{n} e_i x_i$ dove e_i è in $\bigcap_{i \neq k} J_k$.

Alora devo provare che $\phi(x) = y$, cioè che ho effettivamente costruito una preimmagine x di y .

$$\phi(x) = \phi(\sum_{j=1}^{n} e_i * x_i) = \sum_{i=1}^{n} \phi(e_i) * \phi(x_i)$$

$$\phi(e_i) = \pi_1(e_i), \pi_2(e_i), \pi_i(e_i), \pi_n(e_i)$$

$$\phi(x_i) = \pi_1(x_i), \pi_i(x_i), \pi_n(x_i)$$

Ho una sommatoria di prodotti di n -uple

$$\sum_{i=1}^{n}(0, 0, \pi_i(e_i) = 1, 0, 0,) * (\pi_1(x_i), \pi_i(x_i), \pi_n(x_i)) = \sum_{i=1}^{n}(0, 0, \pi_i(x_i), 0, 0)$$

Ma $\pi_i(x_i)$ è y_i . Ho una somma di n -uple che risulta $y_1, y_2, y_n = Y$. Quindi ϕ è suriettiva.

3 Congruenze modulo un ideale

Definizione (318)

Sia R un anello commutativo. Sia J un ideale di R . Due elementi $x, y \in R$ si dicono *congrui modulo* l'ideale J *($x \equiv y \mod J$) se* $j + x = j + y$ *, ovvero se* $x - y \in J$.

Se in particolare $J = (a)$ è principale e generato da un elemento $a \in R$, scriveremo $x \equiv y \mod a$.

Osservazione (319)

Osserviamo che la suriettività di ϕ si può interpretare nel modo seguente: assegnati comunque degli elementi x_1, x_2, x_n nell'anello R , esiste sempre $x \in R$ tale che sia $x \equiv x_i \mod j_i$ per $i = 1, n$. Cioè presi $J_1 + x_1, J_2 + x_2, J_n + x_n$ si ha che x e x_i stanno nello stesso laterale di J_i per ogni i . (il punto y del teorema cinese ha come coordinate gli $a_i = J_i + x_i$, gli x_i sono le controimmagini degli a_i e x è la controimmagine di y di cui il teorema garantisce l'esistenza).

4 Teorema cinese per gli interi

Esiste una versione del teorema cinese per $R = (\mathbb{Z}, +, \cdot)$. Nell'anello degli interi ogni ideale è principale.

Osservazione (320)

Se due interi sono primi, allora i rispettivi ideali principali sono coprimi. Infatti $(a)+(b)$ è un ideale principale e se d è il suo generatore, allora $d = M.C.D.(a, b) =$

1 . Quindi $(a) + (b)$ è un ideale generato dall'unità ed è R , cioè (a) e (b) sono coprimi.

Corollario (321)

Siano a_1, a_2, a_n interi a due a due coprimi (in questo modo i rispettivi ideali sono coprimi). Allora assegnati comunque $x_1, x_2, x_n \in \mathbb{Z}$ il sistema di congruenze lineari

$$\begin{cases} x \equiv x_1 & \mod a_1 \\ x \equiv x_2 & \mod a_2 \\ x \equiv x_n & \mod a_n \end{cases}$$

ammette soluzioni intere. Questo significa che esiste un intero x che è una soluzione simultanea delle congruenze.

Se $\bar{x}$ è una soluzione, ogni altra soluzione è congrua a $\bar{x}$ modulo N , con $N = a_1 a_2 a_n$.

Dimostrazione

Basta osservare che gli ideali generati da a_1, a_2, a_n sono a due a due coprimi. Il nucleo di ϕ è $\bigcap_{i=1}^{n} \{J_i\}$. L'intersezione è l'ideale generato dall' $L.C.M.$ (dominio a ideali principali), ma siccome a_1, a_2, a_n sono a due a due coprimi, si ha $L.C.M. = a_1 * a_2 * a_n$.

Tutte le soluzioni differiscono da questa per un elemento nel nucleo di ϕ .

La dimostrazione del teorema cinese dei resti contiene un algoritmo esplicito per la risoluzione di sistemi di questo tipo.

5 Teorema cinese per i polinomi

Corollario (322)

Su un campo F considero l'anello dei polinomi in una indeterminata x .

Siano $a_1(x), \ldots, a_n(x)$ polinomi appartenenti a $F[x]$. Supponiamo che siano coprimi. Allora assegnati comunque i polinomi $f_1(x), f_2(x), f_n(x)$ a coefficienti in f , il sistema di congruenze lineari polinomiali

$$\begin{cases} f(x) \equiv f_1(x) & \mod a_1(x) \\ f(x) \equiv f_2(x) & \mod a_2(x) \\ f(x) \equiv f_n(x) & \mod a_n(x) \end{cases}$$

ammette soluzioni in $F[x]$. Se $f(x)$ è una soluzione, $f(x) \equiv \bar{f}(x) \mod a_1(x) * a_2(x) * \cdots * a_n(x)$.

In particolare esiste ed è unico un polinomio di grado inferiore a $a_1(x) + a_2(x) + a_n(x)$ soluzione del sistema.

Su $\mathbb{Z}$ e $F[x]$ esiste un algoritmo della divisione.

6 Fonti per testo e immagini; autori; licenze

6.1 Testo

- **Corso:Algebra Anelli (Unimib)/Anelli/Teorema cinese dei resti** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_Anelli_(Unimib)/Anelli/Teorema_cinese_dei_resti?oldid=48157 *Contributori:* Toma.luca95 e Mmontrasio

6.2 Immagini

6.3 Licenza dell'opera

- [Project:Copyright Creative Commons Attribution Share Alike 3.0 & GNU FDL]
- Creative Commons Attribution-Share Alike 3.0