Algebra Anelli (Unimib)

21 ottobre 2021

wikitolearn
collaborative textbooks

This book is the result of a collaborative effort of a community of people like you, who believe that knowledge only grows if shared.
We are waiting for you!

Get in touch with the rest of the team by visiting http://join.wikitolearn.org

Capitolo 1

Anelli

1.1 Generalità sugli anelli

1.1.1 Definizione

Definizione (239 Anello)

Una terna costituita da un insieme non vuoto A su cui si definiscono due operazioni binarie $+, \cdot$ si dice *anello* se sono soddisfatti i seguenti assiomi:

1. $(A, +)$ è un gruppo abeliano;
2. $(A, \cdot)$ è un monoide, cioè un semigruppo con unità;
3. Valgono le proprietà distributive, cioè per ogni $a, b, c \in A$, $a*(b+c) = ab+ac$ e anche $(a + b) * c = ac + bc$.

Se inoltre il prodotto è commutativo, si dice che A è un *anello commutativo*.

Nota: Non è necessario che il prodotto sia commutativo, per questo si definiscono le proprietà distributive a sinistra e a destra.

L'elemento neutro rispetto alla somma si indica con 0_A e si chiama *zero dell'anello*.

L'unità rispetto al prodotto, 1_A , cioè l'unità del monoide $(A, \cdot)$ si dice *unità dell'anello*.

1.1.2 Esempi

Esempio (240)

$(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ $(\mathbb{R}, +, \cdot)$ e $(\mathbb{C}, +, \cdot)$ rispetto alla somma e al prodotto sono anelli infiniti commutativi.

Esempio (241)

Nell'insieme delle classi di resti modulo n $\mathbb{Z}/n\mathbb{Z}$ con $n > 1$ fissato, si possono definire la somma e il prodotto di classi. Quindi la terna $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ è un anello finito commutativo.

Esempio (242)

Ci sono anche anelli non commutativi, ad esempio $M = Mat(n, A)$, cioè l'insieme di tutte le matrici $n \times n$, a coefficienti nell'anello A , con le operazioni di somma e di prodotto righe per colonne. Questo anello è non commutativo se $n > 1$, se $n = 1$ l'anello si identifica con A . Se A è finito, $mat(n, A)$ è finito.

1.1.3 Proprietà elementari

Proposizione (243)

Sia A un anello. $\forall a, b \in A$, $\forall n \in \mathbb{Z}$ valgono le seguenti proprietà:

1. Proprietà dello zero: $\forall a \in A$, $0 * a = a * 0 = 0$.
2. Regola dei segni: Presi due elementi a, b , allora $(-a) * b = a * (-b) = -(ab)$.
3. Multipli: $(na)b = a(nb) = nab$ $na =$ multiplo di a secondo n .

Dimostrazione (Proprietà dello zero)

Prendo il quadrato di A , cioè $a^2 = a \cdot a = (a+0) * a = a * a + a * 0$ per la proprietà distributiva. Quindi $a^2 = a^2 + a * 0$. Nel gruppo additivo valgono le proprietà di cancellazione, cioè posso togliere a^2 da entrambi i membri. Quindi $a * 0 = 0$.

Dimostrazione (Regola dei segni)

E' una conseguenza della proprietà dello zero. Possiamo scrivere:

$$0 = a * 0 = a * (b + (-b)) = a * b + a * (-b)$$

cioè

$$0 = ab + a(-b)$$

cioè $a * (-b)$ è l'opposto di ab e quindi è uguale a $-ab$. Similmente si prova che $(-a) * b$ è l'opposto di ab .

Dimostrazione (Multipli)

Si dimostra per induzione su n se $n \geq 0$. L'asserto è vero per $n = 0$ e quindi il multiplo na è 0 . Per $n = 1$ si ottiene

$$(a)b = a(b) = ab$$

quindi l'asserto è vero. Supponiamo vero l'asserto per $n = k - 1 > 0$ e lo dimostriamo per $n = k$.

$$[((n-1)+1)a]b = (na)b$$

Applicando la proprietà distributiva:

$$[(n-1)a + a]b = ((n-1)a)b + (a)b$$

Per l'ipotesi induttiva posso scrivere:

$$a * ((n-1)b) + a(1b)$$
$$a * [(n-1)b + 1b] = a * [(n-1+1)b] = a * (nb)$$

Se $n < 0$ si passa a considerare $-n$ che è positivo. Per $-n$ questo è vero per la dimostrazione per induzione.

Definizione (244 Anello banale)

Un anello con il solo zero si chiama anello banale. Siccome l'anello dev'essere anche un monoide, l'unità coincide con lo zero.

Osservazione (245)

Conseguenza della proprietà dello zero: Supponiamo $a \in A, a \neq 0$, cioè l'anello A è diverso dall'anello banale. L'unità e lo zero non coincidono, infatti $a * 1_A = a$ ma per la proprietà dello zero $a * 0 = 0$, quindi $1_A \neq 0$ perché ho scelto $a \neq 0$.

1.2 Classi di elementi

In un anello ci sono due classi di elementi che svolgono una funzione importante:

1. i divisori dello zero;
2. gli elementi unitari.

1.2.1 Divisore dello zero

Ci sono anelli in cui è possibile che il prodotto di due elementi diversi dallo zero sia uguale a 0.

In altri anelli invece il prodotto di due elementi diversi da 0 è sempre diverso da 0 (vale la proprietà di annullamento del prodotto).

Definizione (246)

Un elemento $a \in A$, $a \neq 0$ si dice *divisore dello zero* se esiste almeno un altro elemento anch'esso diverso dallo zero dell'anello tale che sia $a * b = 0$ o $b * a = 0$ (l'anello non è necessariamente commutativo).

In altre parole, un anello A diverso da $\{0\}$ è privo di divisori dello zero se e solo se, il prodotto tra due elementi qualsiasi diversi da zero, il prodotto è sempre diverso da zero.

Se chiamo $A^* = A \setminus 0$ un anello è privo di divisori dello zero se A^* è chiuso rispetto al prodotto.

Esempio (247)

L'anello $(\mathbb{Z}, +, \cdot)$ è un anello privo di divisori dello zero. Questa è una conseguenza degli assiomi dell'aritmetica degli interi. Anche gli anelli $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sono privi di divisori dello zero.

Esempio (248)

L'anello delle classi di resti modulo n è privo di divisori dello zero se e solo se n è primo.

Dimostrazione

Sia n non primo, allora si può fattorizzare come prodotto di due primi $r * s$, dove $1 < r < n$ e $1 < s < n$. Allora considerando il prodotto $[r] * [s]$ le due classi sono diverse dalla classe $[0]$ ma il loro prodotto $[r] * [s] = [n] = [0]$. Viceversa, sia p primo e si supponga che ci siano divisori dello zero. Allora se ab sta nella classe zero, è divisibile per p . Se $p \mid ab$, allora o $p \mid a$ o $p \mid b$, cioè $[a] = [p] = [0]$ oppure $[b] = [p] = [0]$. Quindi se $n = p$ non ci sono divisori dello zero.

Definizione (249 Numero primo)

Un intero relativo $n \in \mathbb{Z}$, $n \neq 0, n \neq \pm 1$ si dice *primo* se ogni volta che $p \mid ab$, o $p \mid a$ o $p \mid b$.

Definizione (250 Numero irriducibile)

Un numero p è *irriducibile* se è divisibile solo per se stesso e per ± 1 .

Queste due definizioni definiscono la stessa classe di interi, cioè, un intero è primo se e solo se è irriducibile.

Esempio (251)

Consideriamo l'anello non commutativo delle matrici quadrate $mat(n, A)$. Per ogni $n > 1$ questo anello cotiene i divisori dello zero. Se chiamiamo E_{ij} la matrice elementare che ha 1_A nel posto ij e 0 altrove, e facciamo il prodotto righe per colonne con e_{kl} , il prodotto è

$$\delta_{ij} * \delta_{kl}$$

per $j = k$.

Per ogni $j \neq k$ si ottiene la matrice nulla.

1.2.2 Condizione necessaria e sufficiente

Lemma (252)

Un anello A è privo di divisori dello zero se e solo se valgono le leggi di cancellazione rispetto al prodotto, ovvero se per ogni $a \neq 0$, e per ogni $x, y \in A$ si ha che se $ax = ay$, allora $x = y$ e analogamente se $xa = ya$ allora $x = y$.

Nota: Nell'anello delle matrici $Mat(n, A)$ non valgono le leggi di cancellazione.

Dimostrazione

Supponiamo che A sia privo di divisori dello zero. Sia $a \neq 0$ e $ax = ay$. Segue che

$$ax - ay = ax + (-ay) = 0$$

Per le proprietà distributive:

$$a * (x - y) = 0$$

Si conclude che siccome $a \neq 0$ e siccome a è privo di divisori dello zero, $x - y = 0$ e quindi $x = y$. Similmente a destra.

Viceversa, supponiamo che valgano le leggi di cancellazione e sia $a * b = 0$, con $a \neq 0$. Allora usando la proprietà dello zero, si può scrivere

$$ab = a * 0 = 0$$

Siccome valgono le leggi di cancellazione si può semplificare per a e quindi si ottiene $b = 0$. Similmente se $b = 0$.

Definizione (253 Dominio di integrità)

Un anello commutativo e privo di divisori dello zero si dice *dominio (di integrità)*.

1.2.3 Elementi invertibili rispetto al prodotto

In un anello, preso un elemento $x \in A$, non necessariamente esiste l'inverso di x rispetto al prodotto (infatti negli assiomi di anello, $(A, \cdot)$ è un monoide). Inoltre in ogni anello diverso da quello banale, lo zero non è mai invertibile.

Definizione (254 Elemento unitario)

Un elemento $a \in A$ si dice *unitario* (unit) se ammette inverso in A rispetto al prodotto, cioè se esiste un elemento $\bar{a} = a^{-1}$ tale che $a^{-1} * a = a * a^{-1} = 1_A$.

L'unità dell'anello coincide con il suo inverso, quindi è unitario (in un anello banale lo zero è unitario). Quindi l'insieme degli elementi unitari non è mai vuoto.

1.2.4 Relazione tra unitari e divisori dello zero

Lemma (255)

Un elemento unitario in A non può mai essere un divisore dello zero.

Dimostrazione

Sia a un elemento unitario, e supponiamo che $a * b = 0$. Allora moltiplicando per l'inverso di a si ottiene $a^{-1} * (ab) = a^{-1} * 0$, quindi $1_A * b = a^{-1} * 0 = 0$. Similmente se $ba = 0$.

Esempio (256)

Nell'anello degli interi gli unici elementi invertibili sono ± 1 . Anche se un elemento non è un divisore dello zero, non è necessariamente un unitario.

Alcuni anelli sono unione disgiunta di 0 , di divisori dello zero e di elementi unitari.

1.2.5 gruppo degli elementi unitari

Lemma (257)

Sia U l'insieme degli elementi unitari di un anello $(A, +, \cdot)$. Allora se considero la restrizione del prodotto agli elementi unitari, essi formano un gruppo.

Dimostrazione

1. $U \neq \emptyset$ poiché $1_A \in U$.
2. Se $a, b \in U$, anche $ab \in U$, infatti $(ab) * b^{-1}a^{-1} = a * 1_A * a^{-1} = 1_A$, cioè ab ammette inverso e $(ab)^{-1} = b^{-1} * a^{-1}$. (siccome $a, b \in U$, sappiamo che $\exists a^{-1} \in A, \exists b^{-1} \in b$)

$$(b^{-1} * a^{-1}) * (ba) = 1_A$$

1. Infine, se $a \in U$, anche $a^{-1} \in U$ e quindi U è chiuso rispetto agli inversi ed è un gruppo.

1.2.6 Particolari tipi di anelli

Definizione (258 Corpo)

Un anello $(A, +, \cdot)$ con $|A| > 1$ si dice *corpo* se ogni elemento diverso dallo zero è invertibile rispetto al prodotto, cioè è unitario. In altre parole, A^* è chiuso rispetto al prodotto ed è un gruppo rispetto al prodotto.

Definizione (259 Campo)

Un *campo* è un corpo commutativo.

Osservazione (260)

Un corpo K non ha divisori dello zero, infatti ogni elemento di un corpo è unitario. Un anello (anche commutativo) privo di divisori dello zero non è però necessariamente un corpo.

Un anello commutativo privo di divisori dello zero non è necessariamente un campo.

Esempio (261)

$\mathbb{Z}$ è un anello commutativo privo di divisori dello zero, ma non un corpo perché nessun elemento ha un inverso oltre a ± 1 .

Osservazione (262)

Ogni corpo finito è un campo.

L'anello delle classi di resti modulo n è un campo finito se e solo se è privo di divisori dello zero, e quindi se n è un primo. In questo anello si ha una partizione tra divisori dello zero e elementi unitari.

Anticipazione: Ogni campo finito ha come potenza un numero primo e si costruisce estendendo un campo delle classi di resto modulo n .

1.2.7 Relazione tra anelli finiti e corpi

Teorema (263)

Un anello finito non ridotto al solo zero e privo di divisori dello zero è un corpo.

Dimostrazione

Bisogna dimostrare che ogni elemento diverso dallo zero è invertibile rispetto al prodotto. Sia $a \neq 0$, $a \in A$ e consideriamo tutti gli elementi che si possono scrivere come potenze di a . Se l'anello è finito, esistono degli interi r, s con $r > s$ tali che $a^r = a^s$.

Poniamo $h = r - s$. Allora $a^r = a^{h+s} = a^h * a^s = a^s$. Siccome per ipotesi a è privo di divisori dello zero, valgono le leggi di cancellazione e $a^s \neq 0$, e quindi si ottiene $a^h = 1_A$.

Se $h = 1$, $a = 1_A$ ed è unitario. Se $h > 1$, posso scrivere $a^h = a * a^{h-1}$ e quindi a^{h-1} è l'inverso di a . Quindi in ogni caso $a \neq 0$ ammette un inverso.

Corollario (264)

L'anello delle classi di resto modulo n , cioè $(\frac{\mathbb{Z}}{n\mathbb{Z}}, +, \cdot)$ è un corpo e quindi un campo se e solo se il modulo n è un numero primo.

Dimostrazione

Questo anello è privo di divisori dello zero se e solo se n è primo. Nel caso del "se", se questo anello è privo di divisori dello zero, dal teorema precedente segue che è un corpo, siccome il prodotto delle classi di resto è commutativo è anche un campo.

1.3 Sottoanello

1.3.1 Definizione generale

Definizione (265)

Sia $(A, +, \cdot)$ un anello. Un sottoinsieme $B \subset A$ si dice *sottoanello* di A se valgono le seguenti proprietà:

1. $(B, +)$ è un sottogruppo del gruppo additivo $(A, +)$ (cioè, per il criterio $ab^{-1} \in A$ questo equivale a dire che B è chiuso

rispetto alla differenza);

1. $(B, \cdot)$ è un sottomonoide del monoide $(A, \dot{})$, cioè $1_A \in B$ e B è chiuso rispetto al prodotto.

Esempio (266)

L'insieme degli interi pari non è un sottoanello, perché 1_A non è contenuta nel sottoanello. Ciononostante, è vero che questo è un sottogruppo dell'anello.

Osservazione (267)

Per provare che un sottoinsieme B è un sottoanello dell'anello A basta provare che 1_A sta in B e che B è chiuso rispetto alla differenza e al prodotto.

1.3.2 Sottocorpi e sottocampi

Se ci si restringe alla classe dei campi, le sottostrutture sono i sottocorpi e i sottocampi.

Definizione (268)

Sia K un corpo (campo). Un sottoinsieme K_0 di K con $|K_0| > 1$ si dice *sottocorpo* (*sottocampo*) di K se K_0 è un sottoanello di K e $K_0^* = K_0 \setminus 0$ è un sottogruppo di K^* rispetto al prodotto.

Osservazione (269)

Preso un elemento in K_0 diverso da 0 , il suo inverso k_0^{-1} che esiste in K deve esistere in $(K_0)^*$.

Criterio: Un sottoinsieme di cardinalità maggiore di 1 di un corpo o un campo è un sottocorpo (sottocampo) se e solo se $\forall a, b, \in K_0$, allora $a-b \in K_0$ e $\forall a, b \in (K_0)^*$ allora $ab^{-1} \in (K_0)^*$.

1.4 Polinomi

1.4.1 Polinomi come successioni

Sia $(A, +, \cdot)$ un anello commutativo.

Definizione (270 Polinomio)

Si dice *polinomio sull'anello* A una successione $(a_0, a_1, \dots, a_i, \dots,)$ di elementi di A che sia definitivamente nulla, cioè tale che a partire da un certo posto in poi, $a_i = 0_A$.

Gli elementi a_0, a_1, a_i sono i *coefficienti* del polinomio.

Definizione (271 Somma e prodotto di polinomi)

Data la successione $(a_0, a_1, a_i, \dots)$ e $(b_0, b_1, b_i, \dots)$ definiamo la *somma* di polinomi come la successione $(a_0 + b_0, a_1 + b_1, \dots, a_i + b_i, \dots)$.

Prese due successioni definitivamente nulle come sopra, si definisce *prodotto* di polinomi la successione

$$(a_0, a_1, a_i) \cdot (b_0, b_1, b_i) = (a_0 * b_0, a_0 * b_1 + a_1 * b_0, \sum_{h=0}^{i} a_h * b_{i-h}, \dots$$

Senza imporre che la successione sia definitivamente nulla si ha una serie formale su A .

1.4.2 Anello dei polinomi

Proposizione (272)

L'insieme di tutti i polinomi su A con le operazioni di somma e prodotto sopra definite è un anello commutativo.

Dimostrazione

Basta verificare che si ha un gruppo abeliano rispetto alla somma, che il prodotto è commutativo e che il prodotto è associativo, che valgono le proprietà distributive e che lo zero e l'unità sono presenti. Lo zero è la successione identicamente nulla, cioè $0_A, 0_A, \dots, 0_A, \dots$; l'unità è la successione $(1_A, 0_A, \dots, 0_A)$.

1.4.3 Polinomi come espressioni formali

Due polinomi coincidono quando sono uguali termine a termine.

Per ottenere la rappresentazione usuale dei polinomi scegliamo un simbolo x (indeterminata). Se $A_i = 0_A \forall i > m$ e $a_m \neq 0$. La successione $(a_0, a_1, a_m, 0, 0, 0, \dots)$ viene scritta come

$$a_m * x^m + a_{m-1} * x^{m-1} + a_1 * x^1 + a_0 * x^0 = A(x)$$

Questa è una scrittura puramente formale.

Se qualche coefficiente a_j per $0 < j < n - 1$ è nullo, allora si omette il termine $a_j * x^j$.

Le operazioni di somma e prodotto di polinomi coincidono con quelle usuali nella usuale rappresentazione.

1.4.4 Interpretazione della scrittura formale

Considerando la scrittura:

$$A(x) = a_m * x^m + \cdots + a_1 * x + a_0$$

il polinomio $A(x)$ si può vedere come somma di particolari polinomi che chiamiamo *monomi* $a_i * x^i$, dove il simbolo $a_i * x^i$ è la successione $(0, 0, 0, a_i, 0, 0, \dots)$ con $0 \leq i \leq m$. La somma di queste successioni secondo la regola definita prima si ottiene proprio $A(x) = (a_0, a_1, \dots, a_i, \dots, a_m)$.

Il monomio $a_i * x^i$ è a sua volta prodotto del monomio $a_i = a_i * x^0 = (a_i, 0, 0, \dots)$ e il monomio $x_i = 1_A * x^i = (0, 0, 1_A, 0, 0, \dots)$.

x^i è sua volta si può intrerpretare come la potenza i -esima del polinomio $1_A * x$.

A questa scrittura formale si possono applicare le regole usate per i polinomi a coefficienti numerici.

L'anello dei polinomi su A nell'indeterminata x si denota con il simbolo $A[x]$.

1.4.5 Anticipazione: morfismi tra anelli

Definizione (273 Morfismo di anelli)

Siano A e B due anelli. Un'applicazione $f\colon A \to B$ si dice *morfismo di anelli* se

1. $\forall x, y \in A$, $f(x + y) = f(x) + f(y)$
2. $\forall x, y$, $f(xy) = f(x) * f(y)$
3. $f(1_A) = 1_B$

Un morfismo di anelli è un morfismo di gruppi abeliani e un morfismo di monoidi moltiplicativi.

Come nel caso dei gruppi, un morfismo può essere iniettivo (monomorfismo), suriettivo (epimorfismo) e biettivo (isomorfismo).

1.4.6 Sottoanello delle costanti

Osservazione (274)

I monomi di tipo $a*x^0 = a$ con $a \in A$, cioè le successioni $(a, 0, 0, \dots)$ formano un sottoanello di $A[x]$. Infatti l'unità, le differenze e i prodotti appartengono ancora al sottoanello. Questo sottoanello è isomorfo all'anello A (infatti se al monomio $a * x^0$ si associa a , si verifica subito che c'è un omomorfismo di anelli).

In questo senso, si può identificare A come un sottoanello di $A[x]$ chiamato *anello delle costanti*. In particolare, lo zero e l'unità di A sono identificati con lo zero e l'unità di $A[x]$.

1.4.7 Grado

Definizione (275 Grado di un polinomio e coefficiente direttivo)

Sia $A[x] = a_n*x^n+a_{n-1}*x^{n-1}+\cdots+a_1*x+a_0$ con $a_n \neq 0$ un qualsiasi polinomio non nullo ($\neq 0_{A[x]}$) in $A[x]$. Allora per ogni $m > n$, $A_m = 0$. Diremo che n è il *grado di* $A[x]$ e si scrive $n = gr(A[x])$. a_n si dice *coefficiente direttivo* di $A[x]$ e se $a_n = 1_A$, $A(x)$ si dice *monico*. Al polinomio nullo si attribuisce convenzionalmente grado -1 .

NB: i polinomi di grado zero sono le costanti con $a \neq 0$.

Proposizione (276)

Siano $A(x), B(x) \in A[x]$. Allora

1. il grado della somma $A(x) + B(x) \leq \max\{gr(A(x)), gr(B(x))\}$.

(non vale sempre l'uguale, infatti, se ad esempio i due polinomi hanno lo stesso grado e i due termini di grado massimo sono opposti, il grado della somma è $n-1$)

1. Il grado del prodotto $gr(A(x) * B(x)) \leq gr(A(x)) + gr(B(x))$

Dimostrazione

2. Se $A(x) = a_n * x^n + a_1 * x + a_0$ e $B_x = b_m * x^m + \cdots + b_1 * x + b_0$, allora $A(x) * B(x) = (a_n * b_m) * x^{m+n} + (a_n * b_{n-1}) * x^{n-1} + \cdots + a_0 * b_0$ e quindi il grado del prodotto non può superare la somma dei gradi. Non è necessariamente uguale, perché se A ha divisori dello zero, allora può avvenire che $a_n * b_n = 0$ anche se $a_n \neq 0, b_n \neq 0$.

Se A è un dominio, il grado del prodotto è esattamente uguale a $m + n$.

Ad esempio, se A è l'anello delle classi di resto modulo 6 , allora $A(x) = [2]x^3 + [1]$ e $B(x) = [3]x^2 + [2]$ allora la somma dei gradi è 5 ma il prodotto è $[4]x^3 + [3]x^2 + [2]$ (grado 3).

Proposizione (277 Proprietà di trasposto)

Se A è un dominio, anche il corrispondente anello $A[x]$ è un dominio, cioè è privo di divisori dello zero.

Dimostrazione

Dalla formula del prodotto: se prendo due polinomi non nulli con grado m e n , che sono diversi da zero, dalla formula si ha che il prodotto ha grado $n + m$ (il coefficiente di grado $n + m$ non può essere uguale a zero) e quindi il prodotto di due polinomi non nulli è sempre un polinomio non nullo se l'anello delle costanti è un dominio.

Sia A un dominio. Se il grado del prodotto di due polinomi non nulli è 0 , anche il grado dei fattori dev'essere 0 .

Se A è un dominio, un polinomio è invertibile se e solo se ha grado 0 . (se ha grado maggiore di 0 , anche il grado del prodotto dev'essere maggiore di 0 e quindi non esiste nessun polinomio che moltiplicato con quello di partenza è uguale all'unità). Gli elementi unitari sono tutte e sole le costanti invertibili nel dominio A . Ad esempio, se $A = \mathbb{Z}$, tutti gli elementi unitari di $A[x]$ sono ± 1 .

Preso l'anello dei polinomi delle classi di resto modulo 4 , ad esempio il polinomio $(2x + 1)^2 = [4]x^2 + [4]x + 1 = 1$. In questo anello $2x + 1$ è un polinomio di grado 1 che ha come inverso se stesso.

1.5 Corpo dei quaternioni

1.5.1 Corpo finito non commutativo

Teorema (278 di Weidtreurn)

Ogni corpo finito è un campo, cioè in ogni corpo finito il prodotto è necessariamente commutativo.

Un esempio di corpo infinito e con prodotto non commutativo fu dato da Hamilton ed è costituito dal *corpo dei quaternioni reali*.

Considero l'inzieme H :

$$H = \{\alpha_0 + \alpha_1 * i + \alpha_2 * j + \alpha_3 * k \, \alpha_i \in \mathbb{R} \, i = 1, 2, 3\}$$

i, j, k sono simboli. Due espressioni di H si ritengono coincidenti se e solo se hanno i coefficienti uguali nello stesso ordine.

1.5.2 Somma e prodotto

Siano

$$\bar{\alpha} = \alpha_0 + \alpha_1 * i + \alpha_2 * j + \alpha_3 * k$$
$$\bar{\beta} = \beta_0 + \beta_1 * i + \beta_2 * j + \beta_3 * k$$

Definizione (279 Somma di quaternioni reali)

Definiamo la *somma* in H nel modo seguente:

$$\bar{\alpha} + \bar{\beta} = (\alpha_0 + \beta_0) * 1 + (\alpha_1 + \beta_1) * i + (\alpha_2 + \beta_2) * j + (\alpha_3 + \beta_3) * k$$

Il primo coefficiente $\alpha_0 + \beta_0$ è un reale.

$1, i, k, j$ sono le unità dei quaternioni.

Definizione (280 Prodotto di quaternioni reali)

Si definisce il *prodotto* in H nel modo seguente:

$$\bar{\alpha}*\bar{\beta} = \alpha_0*\beta_0+\alpha_0*(\beta_1*i+\beta_2*j+\beta_3*k)+\alpha_1*i*(\beta_0+i*\beta_1+j*\beta_2+k*\beta_3)+k*\alpha_3*(\beta_0+i*\beta_1+j*\beta_2+k*\beta_3)$$

Tale prodotto è determinato da somma e prodotto dell'insieme dei numeri reali $\mathbb{R}$, dall'uso delle proprietà distributive e dalle "tavole di moltiplicazione" delle unità:

$$i^2 = j^2 = k^2 = -1$$
$$i * j = k = -j * i \text{ il prodotto non è commutativo}$$
$$j * k = i = -k * j$$
$$k * i = j = -ik$$

Con queste operazioni si può verificare che H è un anello non commutativo, infinito, in cui ogni espressione formale tranne quella identicamente nulla ha un'inversa in H . E' un corpo ma non un campo.

1.5.3 Isomorfismo tra H e Mat(2, C)

Sia $\bar{H}$ il sottoinsieme dell'anello $Mat(2, \mathbb{C})$. Consideriamo il sottoinsieme costituito da tutte e sole le matrici della forma:

$$\begin{matrix} a & b \\ -\bar{b} & \bar{a} \end{matrix},$$

dove a, b variano in tutto il campo complesso.

Si verifica facilmente che questo è un sottoanello di $Mat(2, \mathbb{C})$.

La matrice identica è di questo tipo e anche il prodotto e l'inverso appartengono ancora al gruppo.

a, b sono numeri complessi. Poniamo $a = \alpha_0 + \alpha_1 * i$ e $b = \alpha_2 + \alpha_3 * i$. Consideriamo le matrici di $\bar{H}$:

$$\bar{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\bar{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

$$\bar{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

$$\bar{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

Facendo i conti si ha che la matrice

$$\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$$

è uguale a $\alpha_0 * \bar{1} + \alpha_1 * \bar{i} + \alpha_2 * \bar{j} + \alpha_3 * \bar{k}$. Possiamo quindi identificare questa matrice con l'espressione formale $\bar{\alpha} = \alpha_0 + \alpha_1 * i + \alpha_2 * j + \alpha_3 * k$ e riconoscere che previa tale identificazione il prodotto e la somma definiti nell'insieme delle espressioni formali H coincidono con la somma e il prodotto righe per colonne nell'anello $\bar{H}$. In altre parole, H è isomorfo come anello a $\bar{H}$, quindi l'anello non commutativo può essere rappresentato con l'anello delle matrici a elementi complessi.

1.5.4 Inversi

Sia ora

$$X = \begin{matrix} a & b \\ -\bar{b} & \bar{a} \end{matrix}$$

un elemento di $\bar{H}$ e calcoliamo il determinante di X .

$$\det X = a * \bar{a} - (-b * \bar{b}) = \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2$$

(infatti moltiplicando un numero complesso per il suo coniugato si ottiene il modulo al quadrato) Il determinante è una somma di quadrati di numeri reali che è strettamente positiva tranne nel caso in cui tutti i coefficienti sono uguali a 0 , quindi se X non è la matrice nulla.

L'inversa esiste perché $\det > 0$ per ogni matrice in $Mat(2, \mathbb{C})$ della forma considerata, diversa dalla matrice nulla.

Calcolando l'inversa si ottiene ancora una matrice di questo tipo di $\bar{H}$.

Si conclude che $\bar{H}$ e quindi anche H è un corpo (perché ogni elemento è unitario) non commutativo (il prodotto in H definito come sopra non è commutativo) e quindi non è un campo.

1.5.5 Osservazioni

Si può anche definite il prodotto di uno scalare per $\bar{\alpha}$, cioè $r * \bar{\alpha} = r * \alpha_0 + r * \alpha_1 * i + r * \alpha_2 * j + r * \alpha_3 * k$. Unendo la somma e il prodotto esterno si ottiene uno spazio vettoriale di dimensione 4 sui reali. Se $r * \bar{\alpha}$ è definito per ogni reale, esso è legato al prodotto, perché $(r\bar{\alpha}) * \bar{\beta} = r * (\bar{\alpha} * \bar{\beta}) = (r * \bar{\beta}) * \bar{\alpha}$.

Si definisce *algebra* una struttura con tre operazioni (somma, prodotto, prodotto esterno) che è uno spazio vettoriale rispetto a somma e prodotto esterno e un anello rispetto a somma e prodotto e con le proprietà formali definite sopra.

Quella dei quaternioni è un'algebra quattrodimensionale associativa sui reali. I reali considerati come sottoinsieme di quest'algebra commutano con tutte le espressioni formali, cioè stanno nel centro dell'algebra.

In questa rappresentazione $\bar{H}$ si può anche vedere come uno spazio vettoriale 2-dimensionale sui complessi

1.6 Congruenze in un anello

1.6.1 Definizione

Definizione (281 Congruenza in un anello)

Una relazione di equivalenza r definita sugli elementi di un anello $(A, +, \cdot)$ si dice *congruenza sull'anello* A se è compatibile sia con la somma che con il prodotto.

In altre parole, una congruenza su un anello ha le seguenti proprietà:

1. r è una congruenza sul gruppo additivo (abeliano) $(A, +)$ e ha come nucleo la classe contenente 0 , cioè $[0]_r$.
2. r è una congruenza sul monoide $(A, \cdot)$.

Poiché per ogni $x \in [0]_r$ $xR0$ e poiché ogni elemento è associato a se stesso, cioè aRa , segue che $axRa * 0$ e $xaR0 * a$, perché r è compatibile rispetto al prodotto. Ma siccome $0 * a = 0$, allora $axR0$ e $xaR0$. Cioè, preso un qualsiasi elemento x associato a zero, allora il prodotto di x con un qualsiasi elemento dell'anello è associato allo zero. In altre parole, la classe $[0]_R$ è "chiusa" rispetto al prodotto sia a sinistra che a destra per un qualsiasi elemento di A .

Osservazione (282)

r è completamente determinata dalla classe $[0]_r$ che si dice *nucleo di* r .

NB: Se considero la classe $[a]_r$ che contiene un generico elemento di A , essa è il laterale del nucleo che contiene questo elemento (rispetto alla somma), cioè $\{i + a : i \in [0]_r\}$.

1.6.2 Ideale

L'analisi delle congruenze in un anello conduce alla definizione di ideale.

Definizione (283 Ideale)

Un sottogruppo I del gruppo additivo $(A, +)$ si dice rispettivamente

1. *ideale sinistro*, se $\forall a \in A, \forall i \in I$, $a * i \in I$;
2. *ideale destro*, se $\forall a \in A, \forall i \in I$, $i * a \in I$;
3. *ideale (bilatero)*, dell'anello A se per ogni $i \in I$ e per ogni $a \in A$, $a * i \in I$ e $i * a \in I$.

In un anello commutativo un ideale sinistro è anche destro e quindi bilatero.

Esempio (284)

Considerando $Mat(n, A)$ anello delle matrici quadrate con $n > 1$ e considero l'insieme di tutte le matrici che hanno tutte le colonne nulle tranne una colonna fissata che ha elementi arbitrari: questo soottoinsieme è un sottogruppo del gruppo additivo di $Mat(n, A)$ ed è un ideale sinistro.

Se si prende invece l'insieme che ha tutte le righe nulle tranne una riga arbitraria, si ottiene un ideale destro.

1.6.3 Relazione tra nucleo e ideale

Il nucleo di una congruenza di A è un ideale, perché è un sottogruppo del gruppo additivo dell'anello, inoltre per ogni $x \in I$ e per ogni $a \in A$, ax e xa stanno entrambi nel nucleo per l'osservazione precedente.

Inversamente, vale la seguente proposizione:

Proposizione (285)

Sia I un ideale dell'anello A , allora se considero la relazione di equivalenza D_i definita ponendo: $aD_ib \iff \exists i \in I t.c. b = i + a$, essa è una congruenza in A avente come nucleo l'ideale I .

(Gli ideali sono tutti e soli i nuclei delle congruenze)

Dimostrazione

Sappiamo che rispetto alla somma $(I, +)$ è un sottogruppo normale del gruppo abeliano $(A, +)$. Dunque D_i è una congruenza di gruppi abeliani e ha come nucleo il sottogruppo I . Resta solo da provare che D_i è compatibile con il prodotto e quindi che è una congruenza sull'anello.

Siano aD_ia' e bD_ib' allora per come D_i è definita esistono elementi $i_1, i_2 \in I$ tali che $a' = i_1 + a$ e $b' = i_2 + b$. Segue che $a'b' = (i_1 + a)(i_2 + b) = i_1 * b + i_2 * a + i_1 * i_2 + ab$. I primi tre elementi sono tutti elementi di I per le proprietà dell'ideale, quindi $abD_ha'b'$.

La S_i coincide con la D_i perché I è normale.

1.6.4 Costruzione di ideali

Sia A un anello, $a \in A$, e prendiamo i seguenti sottoinsiemi di A :

1. $$(a)_s = \{y \in At.c.xa = y,\ x \in A\}$$
2. $$(a)_d = \{y \in At.c.ax = y, x \in A\}$$

.

Entrambi gli insiemi contengono lo zero se pongo $x = 0$.

Nota: non è richiesto che un ideale contenga l'unità. Infatti, se un ideale contiene l'unità, allora contiene il prodotto dell'unità per gli altri elementi dell'anello, quindi coinciderebbe con l'intero anello.

Esempio (286)

Nell'insieme $\mathbb{Z}$ l'insieme dei numeri pari è un ideale ma non un sottoanello.

Proposizione (287)

1. $(a)_s$ è un ideale sinistro di A e $(a)_d$ è un ideale destro.
2. Se I_s e I_d sono ideali sinistri o destri dell'anello A contenente a , allora l'ideale $(a)_s \subset I_s$ e $(a)_d \subset I_d$.
3. Sia A un anello commutativo, allora $(a)_s$ coincide con $(a)_d$ e lo indico con (a) (gli ideali sono bilateri).

(a) coincide con l'intero anello se e solo se a è un elemento unitario.

Dimostrazione

1. Consideriamo $x_1 * a, x_2 * a \in (a)_s$. Mostriamo che la loro differenza $x_1 * a - x_2 * a$ sta ancora in $(a)_s$, cioè mostriamo che $(a)_s$ è

un sottogruppo additivo di $(A, +)$.

$$x_1 * a - x_2 * a = (x_1 - x_2) * a \in (a)_s,$$

quindi è un sottogruppo del gruppo abeliano. Prendiamo un qualsiasi elemento di $(a)_s$ della forma $x * a$, allora devo provare che $y(xa)$ sta ancora nell'insieme. Per l'associatività posso scrivere $y(xa) = yxa = (yx)a$ similmente per $(a)_d$. Ho così dimostrato la chiusura rispetto al prodotto con elementi dell'anello.

1. Se $a \in I_s$, siccome I_s è un ideale sinistro, per ogni $x \in A$ anche $xa \in I_s$. Quindi $(a)_s$ è contenuto nell'ideale I_s .

Similmente per I_d .

1. Se $(a)_s = (a)_d = (a)$ è uguale all'intero anello A , allora l'unità 1_A appartiene a (a) , quindi esiste

$\bar{x} \in A$ tale che $1_a = \bar{x} * a = a * \bar{x}$, ovvero a è invertibile rispetto al prodotto. Inversamente supponiamo che a sia unitario. Allora $\forall y \in A$ posso scrivere $y = y * 1_A = y * a^{-1} * a = (ya^{-1}) * a$, cioè y sta nell'ideale generato da a .

In particolare se ho un ideale di un anello ed esso contiene l'unità, allora è l'intero anello.

1.6.5 Ideale principale

Definizione (288 Ideale principale)

Si definisce *ideale principale* generato dall'elemento a l'insieme ottenuto moltiplicando a per ogni elemento dell'anello: l'ideale principale è il più piccolo ideale che contiene a .

Se l'anello è commutativo, l'ideale principale generato da a coincide con tutto A se e solo se a è unitario.

Corollario (289)

Se A è un anello commutativo con $|A| > 1$, allora A è un campo se e solo se non ha ideali non banali, cioè diversi dall'ideale nullo (solo zero) e l'intero.

In altre parole, i campi sono anelli che hanno solo ideali banali.

Dimostrazione

Questo deriva dal fatto che siccome ogni elemento $a \in A$ è unitario, allora l'ideale (a) coincide con l'intero anello e non esistono ideali più piccoli che contengono a .

1.6.6 Ideali in un dominio

Proposizione (290)

Sia A un dominio (un anello commutativo privo di divisori dello zero). Se considero due elementi $a, b \in A$, allora l'ideale principale generato da a e quello generato da b coincidono se e solo se a differisce da b per un elemento unitario, cioè se $a = ub$.

Dimostrazione

Supponiamo che i due ideali principali coincidano. Allora l'elemento a sta nell'ideale generato da b , quindi $a = x_1 b$, ma anche b appartiene all'ideale generato da a , quindi si può scrivere $b = x_2 * a$. Segue $a = x_1 b = x_1 x_2 * a$. Se $a = 0$ anche $b = 0$ e in questo caso gli elementi differiscono per qualsiasi elemento unitario.

Altrimenti, se $a \neq 0$ valgono le leggi di cancellazione, quindi cancellando a si ottiene $1 = x_1 * x_2$, cioè x_1 e x_2 sono entrambi elementi unitari. In particolare $x_1 \in U$ e $a = ub$.

Inversamente, supponiamo che $a = ub$ con u unitario. Allora a (e quindi (a)) è contenuto in (b) . D'altra parte, u è unitario e ha inverso quindi posso scrivere $b = u^{-1} * a$ e quindi $(a) \supset (b)$. Vale la doppia inclusione e i due ideali coincidono.

Definizione (291 Domini a ideali principali)

Un dominio è detto a ideali principali se ogni ideale è principale.

Esempio (292)

Tra questi domini ci sono il dominio degli interi relativi e il dominio dei polinomi in un'indeterminata x a coefficienti in un campo. C'è un parallelismo tra questi due domini (esistenza di un algoritmo per la divisione).

1.7 Fattorizzazione

1.7.1 Divisibilità e fattori

Nei domini si ha una nozione di divisibilità.

Definizione (293)

Sia D un dominio e siano $a, b \in D$. Diciamo che *a divide b* e scriviamo $a \mid b$ se esiste $c \in D$ tale che $b = a * c$ (ovvero, b appartiene all'ideale principale generato da a).

Osservazione (294)

$a \mid b$ e $b \mid a$ se e solo se (a) e (b) coincidono, ovvero a e b differiscono per un elemento unitario.

Definizione (295 Fattore)

Se $a \mid b$, diremo che a è un *fattore* di b nel dominio D e diremo che a è un fattore banale se a è unitario o differisce da b per un elemento unitario, cioè $a = ub$ con $u \in U$. Gli altri si chiamano fattori propri.

1.7.2 Elementi primi e irriducibili

Definizione (296 Elemento primo)

Sia D un dominio. Un elemento $p \in D$ diverso dallo zero e non unitario si dice *primo* se ogni qualvolta $p \mid xy$, allora $p \mid x$ o $p \mid y$.

Definizione (297 Elemento irriducibile)

Se $p \in D$ non nullo e non unitario, si dice *irriducibile* in D se non ammette fattorizzazioni non banali, cioè se $p = xy$ implica $x \in U$ o $y \in U$.

In $\mathbb{Z}$ un numero primo è diverso da zero e da ± 1 con la proprietà che se divide il prodotto di due interi, divide almeno uno dei due elementi.

Ad esempio, 4 non è primo perché $4 \mid 12 = 4 * 3 = 2 * 6$ e $4 \not| 2$ e $4 \not| 6$. Gli irriducibili sono quelli che si scrivono come $z = z * 1$ o $z = -1 * z$, perché gli unici unitari sono ± 1 .

In $\mathbb{Z}$ le nozioni di numeri primi e irriducibili coincidono, ma in un dominio generico le due nozioni possono indicare classi distinte.

1.7.3 Relazione tra primi e irriducibili

Proposizione (298)

In ogni dominio D ogni elemento primo è anche irriducibile, ma in generale non vale viceversa.

Dimostrazione

Sia $p \in D$ primo. Proviamo che è irriducibile.

Supponiamo che $p = b * c$ con $b, c \in D$. Allora p è un fattore del prodotto bc , se scrivo $1 * p = bc$. Siccome p è primo, allora divide uno dei due fattori. Allora se divide b esiste d tale che $b = p * d$. Segue che $p = bc = pdc$ e semplificando ottengo $dc = 1$. Questo significa che d, c sono unitari.

Se $p \nmid b$, allora $p \mid c$ ed esiste $e \in D$ tale che $c = e * p$. Cioè $p = bc = bpe$, allora semplificando per p ottengo $be = 1$ e quindi $b \in U$. Anche in questo caso la fattorizzazione $d = b * c$ è banale.

1.8 Morfismi

1.8.1 Anello quoziente

Se ho due anelli arbitrari A, B un'applicazione lineare tra i due anelli è un morfismo se conserva la somma, il prodotto e l'unità.

Il nucleo di un morfismo è l'insieme di tutti gli elementi di A che hanno come immagine lo zero di B (è il nucleo del morfismo che si avrebbe se si considerano i due anelli come gruppi additivi).

$$\ker f = \{a \in A t.c. f(a) = 0_B\}$$

Come nel caso dei gruppi, ad ogni congruenza e quindi ad ogni ideale e ad ogni nucleo è associato un anello quoziente.

Sia A un anello e I un ideale (bilatero). Allora l'insieme quoziente di A rispetto alla congruenza di nucleo I si denota con A/I .

Gli elementi di A/I sono i laterali additivi di $I \in A$, cioè un generico elemento $I + a$ consiste di tutti gli elementi che differiscono da a per un elemento di I .

Siccome I è il nucleo di una congruenza, le operazioni di somma e prodotto definite su A inducono operazioni di somma e prodotto di laterali nell'insieme quoziente A/I . La somma è tale che $(I + A) + (I + B) = I + (a + b)$ Analogamente il prodotto $(I + a)(I + b) = I + ab$.

Con queste operazioni l'insieme quoziente è un anello chiamato *anello quoziente* di A rispetto all'ideale I .

Lo zero dell'anello quoziente è la classe che contiene lo zero di A , cioè il laterale $I + 0_A$ che coincide con I . L'unità è $I + 1_A$.

Se A è un anello commutativo, anche il quoziente lo è.

Se A è privo di divisori dello zero, il quoziente potrebbe non esserlo.

1.8.2 Epimorfismo canonico

Possiamo considerare l'applicazione $\pi\colon A \to A/I$ tale che preso un elemento a la sua immagine è il laterale che contiene a . Quest'applicazione è un epimorfismo e ha come nucleo I .

Pensando ai gruppi additivi π può essere considerato come epimorfismo canonico.

Anche in questo caso π si definisce *epimorfismo canonico* di A sul quoziente.

Quindi il quoziente A/I per qualsiasi ideale I di A è epimorfo a A .

1.8.3 Teorema fondamentale di epimorfismo per gli anelli

Dati due anelli A, B e un morfismo $f\colon A \to B$, se consideriamo il nucleo del morfismo esso è un ideale. Infatti, $\ker f$ è l'ìinsieme degli elementi che hanno come immagine 0_B . Rispetto alla relazione r_f che è la relazione di equivalenza associata a f come applicazione, il ker è un ideale: infatti, mediante la r_f , gli elementi con la stessa immagine sono associati tra loro, siccome l'immagine di 0_A è uguale a 0_B , allora il ker è l'insieme degli elementi associati a zero mediante r_f , ed è il nucleo della congruenza r_f , che è un ideale.

Possiamo dire che r_f è una congruenza perché se $aRf(a)$ e $bRf(b)$ allora $abRf(a) * f(b) = f(ab)$.

Teorema (299)

Sia $f\colon A \to B$ un morfismo. Allora

1. Se r_f è la relazione di equivalenza associata a f , questa relazione è una congruenza sull'anello A (compatibile

con somma e prodotto); $\ker f$ è la classe dello zero ed è un ideale di A .

1. Se considero l'anello quoziente $\frac{A}{\ker f}$ e considero l'epimorfismo canonico:

$$\pi \colon A \to \frac{A}{\ker f}$$

allora esiste ed è unica un'applicazione $\bar{f}$ da $\frac{A}{\ker f}$ a B tale che si possa fattorizzare f come $\bar{f} \circ \pi$. $\bar{f}$ è l'applicazione che porta un laterale $\ker f + a$ in $f(a)$.

1. $\bar{f}$ è un monomorfismo (per la parte di questo teorema riguardante i gruppi), è un isomorfismo se e solo se f è suriettivo.

Il teorema fondamentale sui morfismi dice che se B è immagine epimorfa di A , allora è isomorfa all'anello quoziente $\frac{A}{\ker f}$.

1.8.4 Il caso degli interi

Se consideriamo l'anello degli interi $(\mathbb{Z}, +, \cdot)$, osserviamo che ogni sottogruppo di $(\mathbb{Z}, +)$ è ciclico cioè ha la forma: $n\mathbb{Z} = nh$, $h \in \mathbb{Z}$.

Se $n = 0$ ho il sottogruppo del solo zero, se $n = \pm 1$ ho tutto $\mathbb{Z}$. Negli altri casi il sottogruppo è un ideale dell'anello $(\mathbb{Z}, +, \cdot)$. Infatti, preso un qualsiasi elemento nh multiplo di n , se lo moltiplico per un qualsiasi intero z , esso è ancora un multiplo di n . Quindi ogni sottogruppo ciclico di quella forma è ancora un ideale.

Gli ideali sono tutti e soli i sottogruppi ciclici di $\mathbb{Z}$.

Poniamo $I = nz$. Allora se $n \neq 0$ o $n \neq \pm 1$, l'anello quoziente $\frac{\mathbb{Z}}{n\mathbb{Z}}$ con $i = n\mathbb{Z}$ è l'anello delle classi di resto modulo n .

I laterali sono della forma $n\mathbb{Z} + a$ che è l'insieme di tutti gli elementi che differiscono da a per un multiplo di n .

Se $n = 0$ il quoziente è isomorfo all'anello $\mathbb{Z}$.

Se consideriamo il teorema fondamentale sui morfismi, siccome tutte e sole le immagini epimorfe sono a meno di isomorfismo i gruppi quoziente, allora tutte le immagini epimorfe di $\mathbb{Z}$ sono 0 , $\mathbb{Z}$ e l'anello delle classi di resto modulo n .

1.8.5 Caratteristica di un anello

Sia A un anello non banale, generico e definiamo l'applicazione

$$C \colon \mathbb{Z} \to A$$

definita ponendo $f(z) = z * 1_A$, cioè per ogni intero z si associa il multiplo secondo z dell'unità di A . Questo è un morfismo di anelli.

Siano z_1, z_2 due interi. C è un morfismo, infatti:

1. conserva la somma;

$$C(z_1 + z_2) = (z_1 + z_2) * 1_A = z_1 * 1_A + z_2 * 1_A$$

(l'immagine della somma è la somma delle immagini. Si dimostra applicando la proprietà delle potenze in versione additiva)

1. Conserva il prodotto:

$$C(z_1 z_2) = z_1 z_2 * 1_A = z_1 * (z_2 * 1_A) = z_1 * (1_A * z_2 * 1_A) = z_1 * 1_A * z_2 * 1_A$$

Dipende dalla proprietà $n * (ab) = nab$ e dalle proprietà delle potenze.

1. conserva l'unità: $g(1) = 1_A$

Quindi C è un morfismo. La sua immagine è un sottonaello di A . In questo caso il sottoanello che si ottiene è l'insieme dei multipli dell'unità.

Il nucleo di C è l'insieme $\{z \in \mathbb{Z} t.c. z * 1_A = 0_A\}$ (in notazione additiva). Nel gruppo additivo dell'anello A l'insieme dei multipli di a equivale all'insieme delle potenze additive di a .

Se $o(1_A) = n$ in $(A, +)$ è finito, allora $\ker C = \{n * \mathbb{Z}\}$, cioè è l'ideale costituito dai multipli di n .

Se invece $o(1_A) = \infty$ (nel gruppo additivo) allora non esiste $z \neq 0$ per cui $z * 1_A = 0$ e quindi $\ker C = 0$.

Nel primo caso per il teorema fondamentale sui morfismi, se $o(1_A) \in (A, +)$ è uguale a n finito, allora $\frac{\mathbb{Z}}{n\mathbb{Z}} = \frac{\mathbb{Z}}{\ker C}$ (classi di resto modulo n) è isomorfo all'immagine del morfismo C , cioè ai multipli dell'unità.

Se invece $o(1_A)$ in $(A, +)$ è infinito, si ha che l'immagine $C(\mathbb{Z})$ è isomorfo a $\frac{\mathbb{Z}}{\ker C} = \frac{\mathbb{Z}}{0} = \mathbb{Z}$.

Definizione (300 Caratteristica)

Se $o(1_A)$ in $(A, +)$ è $n < \infty$, diremo che A è un anello di *caratteristica* n . Altrimenti se $o(1_A) = \infty$, allora A ha caratteristica zero.

Se l'anello A è un dominio, allora ci sono due possibilità:

1. se $o(1_A) = \infty$ si ha un dominio di caratteristica 0 , come $\mathbb{Z}$
2. se A ha caratteristica finita, è isomorfo alle classi di resto modulo n , ma l'insieme delle classi modulo n

è privo di divisori dello zero se e solo se n è primo. Quindi in un dominio di caratteristica n il periodo dell'unità è necessariamente primo. $pa = p * 1_A * a = 0$ perché $p * 1_A = 0$. Quindi in un campo di caratteristica p , non solo l'unità ma anche ogni elemento diverso da 0 ha periodo p .

Osservazione (301)

L'identità di Bézout vale in ogni dominio in cui ogni coppia di elementi ha un $M.C.D$ ..

1.9 Ideali primi e massimali

1.9.1 Somma, prodotto e intersezione

Supponiamo di avere un anello A commutativo. Supponiamo che I, J siano ideali di A , allora possiamo considerare

1. la *somma*, cioè

$$I + J = \{i + j,\, i \in I,\, j \in J\}$$

questo è un ideale (è chiuso rispetto alla differenza e rispetto al prodotto per elementi dell'anello). Esso è il più piccolo ideale che contiene I, J .

1. l'*intersezione* insiemistica $I \cap J$, che è un ideale di A .
2. il *prodotto* di due ideali IJ è l'insieme

$$\left\{ \sum_{i=1}^{n} a_i b_i \right\}$$

. (infatti non è detto che l'insieme di tutti i possibili prodotti sia chiuso rispetto alla somma).

Nota: Il prodotto così definito è contenuto nell'intersezione.

1.9.2 Ideale generato da un insieme

In generale, presa una qualsiasi famiglia di ideali, si può definire l'ideale generato dalla famiglia.

Definizione (302 Ideale generato da un insieme)

Sia $X = \{a_1, a_2, a_n\}$ un insieme finito di elementi di A . Allora si dice *ideale generato dall'insieme* X l'ideale $(a_1) + (a_2) + (a_n)$.

Proposizione (303)

Sia A un anello, non necessariamente commutativo e I un ideale. Allora possiamo considerare l'anello quoziente A/I . Il morfismo canonico $\pi\colon A \to A/I$ che ad ogni elemento associa il laterale $I + a$ induce una biezione fra l'insieme degli ideali di A contenenti I e l'insieme degli ideali dell'anello quoziente A/I .

Dimostrazione

Consideriamo per ogni ideale J contenente I l'immagine $\pi(J)$. Allora verifichiamo che $\pi(J)$ è un ideale di A/I contenente I . Verifichiamo che $\pi(J)$ è chiusa rispetto alla differenza, cioè che

$$\forall j_1, j_2 \in J,\ \pi(j_1) - \pi(j_2) \in \pi(J)$$
$$\pi(j_1) - \pi(j_2) = \pi(j_1 - j_2)$$

perché π è un morfismo.

Siccome un ideale è chiuso rispetto alla differenza, $j_1 - j_2 \in J$, cioè $\pi(j_1 - j_2) \in \pi(J)$.

Inoltre devo verificare che per ogni $j \in J, a \in A$, se moltiplico $(I + a) * \pi(j)$ ottengo ancora un elemento di $\pi(J)$ (chiusura rispetto al prodotto: gli $I + a$ sono gli elementi dell'anello quoziente). Questo è vero perché per definizione di epimorfismo canonico

$i + a = \pi(a)$ e quindi

$$(i + a) * \pi(j) = \pi(a) * \pi(j) = \pi(aj)$$

e ottengo $\pi(aj) \in \pi(J)$, perché siccome J è un ideale, $aj \in J$.

La biezione richiesta dall'enunciato è l'applicazione $\bar{\pi}$ che a ogni J associa la sua immagine $\pi(J)$ nell'epimorfismo canonico.

1. $\bar{\pi}$ è iniettiva. Supponiamo che J_1, J_2 siano due ideali contenenti I e supponiamo $\bar{\pi}(J_1) = \bar{\pi}(J_2)$. Questo significa che per ogni $j_1 \in J_1$ esiste $j_2 \in J_2$ tale che $i + j_1 = i + j_2$. Segue che se i due laterali coincidono, allora i due rappresentanti differiscono per un elemento di I , quindi esiste $i \in I$ tale che $j_1 = i + j_2$.

J_2 contiene I , quindi $i \in J_2$. Ho la somma di due elementi di J_2 che appartiene a J_2 . Quindi $J_1 \subset J_2$. Per simmetria, è vero che $J_2 \subset J_1$. Quindi $J_1 = J_2$. Se due ideali hanno la stessa immagine, allora coincidono.

1. $\bar{\pi}$ è suriettiva. Sia $\bar{J}$ un qualsiasi ideale di A/I , allora devo mostrare che ha una preimmagine. Sia G l'insieme di

tutte le preimmagini $\pi^{-1}(\bar{J})$ mediante l'epimorfismo canonico π . Si verifica facilmente che J è un ideale di A (contenente I). L'insieme di tutte le preimmagini dello zero dell'anello quoziente è I . $\bar{\pi}(J) = \bar{J}$. (la preimmagine di un ideale in un morfismo è un ideale)

Quindi $\bar{\pi}$ è una biezione.

Notazione: Per comodità si scrive spesso $\bar{\pi}(J) = J/I$ (J è un ideale che contiene I).

1.9.3 Teoremi di isomorfismo per gli anelli

Teorema (304)

Sia A un anello. Se I è un ideale di A e J un sottoanello di A , allora la somma $I + J$ è un sottoanello di A . Siccome $0_A \in J$, l'intersezione $I \cap J$ è un ideale di J e c'è un isomorfismo tra l'anello quoziente $(I + J)/I$ e il quoziente $J/(I \cap J)$.

Dimostrazione

Si consideri il morfismo dall'anello J all'anello quoziente $(I + J)/I$ che ad ogni elemento $j \in J$ associa il laterale $I + j$. Questa mappa è un epimorfismo, è suriettiva perché ogni elemento del quoziente $I + j$ ha come preimmagine $j \in J$.

Il nucleo è

$$\ker f = \{j \in J \, t.c. \, f(j) = [0]\} = \{j \in J \, t.c. I + j = I\}$$

ed è fatto da tutti e soli gli elementi di J che stanno anche in I , quindi se quoziento J rispetto al nucleo che è $I \cap J$, ottengo un anello isomorfo a quello di arrivo, cioè $(I + J)/I$.

Teorema (305)

Sia $I \subset J$ e siano I, J ideali di A . Allora $\bar{\pi}(J) = J/I$ è un ideale dell'anello quoziente A/I e il quoziente $(A/I)/(J/I)$ è isomorfo all'anello quoziente A/J (posso semplificare per I).

Dimostrazione

Considero la mappa che a ogni elemento di A/I associa l'elemento $J+a$. Il nucleo è

$$\ker f = \{(I + a) \in A/I t.c. f(I + a) = J\} = \{(I + a) t.c. a + J = J\}$$

e questo avviene quando $a \in J$.

Quindi il nucleo è J/I e l'anello di arrivo è isomorfo all'anello di partenza quozientato per il nucleo.

1.9.4 Ideali primi e massimali

Definizione (306 Ideali primi e massimali)

Considero un anello commutativo A non banale. Sia $I \neq A$ un ideale nell'anello A .

1. I si dice *primo* se per $a, b \in A$, se il prodotto $a * b \in I$, allora $a \in I$ o $b \in I$.
2. I si dice *massimale* se la catena di inclusioni $I \subset J \subset A$ con J ideale di A implica $J = I$ o $J = A$.

(in altre parole, non esiste nessun altro ideale dell'anello che contenga I e che sia diverso da I o da A)

L'ideale nullo dell'anello (0_A) è primo se e solo se A è un dominio.

Proposizione (307)

Sia A un anello commutativo e $I \neq A$ un ideale di A . Allora

1. l'ideale I è primo se e solo se l'anello quoziente A/I è un dominio
2. I è massimale se e solo se A/I è un campo.

Dimostrazione

Siano $a, b \in A$.

L'asserzione $ab \in I$ implica $a \in I \vee b \in I$ è equivalente all'asserzione $(I + ab) = (I + a)(I + b) = I$ implica $I + a = I$ o $I + b = I$. Siccome $0 \in I$, la seconda asserzione dice che A/I è un dominio, cioè è privo di divisori dello zero.

Dire che I è massimale di A equivale a dire che non c'è nessun ideale J compreso tra I e A nella catena di inclusioni. Questo avviene se e solo se A/I è privo di ideali non banali (questo perché preso un ideale J che contiene I , la sua immagine mediante π è un ideale di A/I . Se A/I ha solo ideali banali, si ha che $J = A$ o $J = I$). Se A è un anello commutativo, allora è privo di ideali non banali se e solo se è un campo (per un corollario), cioè se è generato da un elemento unitario, quindi se e solo se A/I è un campo.

1.9.5 osservazioni sui fattori

In un dominio, $b \mid a$ se e solo se esiste c tale che $a = bc$. b è un fattore banale se differisce da a per un elemento unitario c , oppure se è lui stesso unitario.

Due fattori si dividono a vicenda se i due ideali principali coincidono.

Sia D un dominio. Dire che b è un fattore proprio non banale di un elemento a nel dominio equivale a dire che l'ideale principale (a) è contenuto propriamente nell'ideale principale generato da (b) .

1.9.6 Domini a ideali principali

Definizione (308 Dominio a ideali principali)

Un dominio D si dice a *ideali principali* (PID) se e solo se ogni suo ideale è principale.

Proposizione (309)

Sia D un dominio a ideali principali.

1. Sia $a \in D, a \neq 0$, a non unitario. L'ideale principale generato da un elemento a è primo se e solo se a è primo.
2. L'ideale (a) è massimale se e solo se a è irriducibile.

Dimostrazione

1. Basta applicare la definizione, infatti se a è un elemento non unitario, $(a) = a * x$, con $x \in A$.

Se a è primo, si ha che ogni volta che $a \mid bc$, o $a \mid b$ o $a \mid c$. Segue immediatamente che se $bc \in (a)$, allora $bc = ax$ e $a \mid bc$. Allora $a \mid b$ o $a \mid c$ e quindi o $c \in (a)$ o $b \in (a)$, cioè (a) è primo. Viceversa, se (a) è primo, si ha che se $bc \in (a)$, o $b \in (a)$ o $c \in A$, quindi $a \mid b \vee a \mid c$, cioè a è primo.

1. Se l'elemento a è irriducibile, non ammette fattori non banali, e quindi non si può trovare un

fattore b tale che $b \mid a$ e $(a) \subset (b)$ diverso da a .

1.9.7 m.c.m. e M.C.D.

Definizione (310 Massimo comun divisore)

Sia D un dominio e siano $a, b \in D$. Un elemento $d \in D$ si dice *massimo comun divisore* tra a, b se $c \mid a\, c \mid b$ e per ogni elemento c tale che $c \mid a$ e $c \mid b$, allora $c \mid d$.

Non è detto che due elementi in un dominio abbiano sempre un $M.C.D.$.

Osservazione (311)

Se ho due massimi comun divisori, allora $d_1 \mid d_2$ e $d_2 \mid d_1$ quindi i due ideali coincidono, e questo implica che d_1 e d_2 differiscono per un elemento unitario.

Un $M.C.D.$ è unico a meno di un elemento unitario. Ad esempio, negli anelli dei polinomi gli elementi unitari sono le costanti, quindi due massimi comun divisori differiscono al più+ per una costante.

Un elemento $t \in D$ si dice *minimo comune multiplo* ($l.c.m.$) di a, b se $a \mid d$ e $b \mid d$ e per ogni $s \in D$ tale che $a \mid s$ e $b \mid s$, allora $d \mid s$.

Condizione necessaria e sufficiente affinché $A[x]$ sia a ideali principali è che A sia un campo. $\mathbb{Z}$ è un dominio a ideali principali.

Proposizione (312)

Sia D un dominio a ideali principali. Siano $a, b \in D$. Allora valgono le seguenti proprietà:

1. $(a) + (b)$ (ideale generato da a e b) è a sua volta principale,

cioè contiene un elemento d che genera l'intero ideale. $d = M.C.D(a, b)$. Quindi $d = xa + yb$ e in ogni dominio a ideali principali vale l'identità di Bézout.

1. $(a) \cap (b)$ è un ideale principale. Se t è un suo generatore, $t = l.c.m.(a, b)$

Dimostrazione

Per il punto 1, esiste $d \in D$ tale che $(d) = (a) + (b)$. Allora a, b appartengono a (d) , ovvero $d \mid a$ e $d \mid b$. Inoltre, siccome $d \in (a) + (b)$, esistono $y, x \in D$ tali che $d = xa + yb$. Se $c \mid a$ e $c \mid b$, allora $d = xec + yfc = (xe + yf)c$, cioè $c \mid d$. In particolare, vale la cosiddetta identità di Bézout.

Per il punto 2, esiste $t \in D$ tale che $(a) \cap (b) = (t)$. Allora t dev'essere un multiplo sia di a che di b , cioè $a \mid t$, $b \mid t$. Se s è tale che $a \mid s$ e $b \mid s$, allora $s \in (a)$ e $s \in (b)$ quindi $s \in (a) \cap (b)$. Siccome $(t) = (a) \cap (b)$ allora $s \in (t)$ cioè $t \mid s$. Quindi t è un $l.c.m.$.

Dato un anello commutativo A e presi due ideali I e J , essi sono coprimi se la somma $I+J$ è l'intero dominio. La somma è l'intero dominio quando $M.C.D.(a, b)$ è unitario.

1.9.8 M.C.D. di una lista

Presi due elementi $a, b \in D$ si possono definire $M.C.D.$ e $l.c.m.$. Se considero l'ideale generato da a e b , cioè $(a) + (b)$ anch'esso è principale e se d è un suo generatore, $d = M.C.D.(a, b)$. Per quanto riguarda $(a) \cap (b)$, se t è un suo generatore, allora $t = l.c.m.(a, b)$

Se considero $a_1, a_2, a_s \in D$ posso definire induttivamente $M.C.D.(a_1, \ldots, a_s)$. Similmente si definisce l' $l'c.m.$ di una lista $a_1, \ldots a_s$ di elementi.

Se considero $(a_1, a_2, a_s) = (a_1) + (a_2) + (a_s)$ esso è principale quindi è generato da d con $d = M.C.D.(a_1, \ldots, a_s)$. Analogamente, l'ideale $(a_1) \cap (a_2) \cap (a_s)$ è un ideale principale generato da $t = l.c.m.(a_1, \ldots, a_s)$.

1.10 Teorema cinese dei resti

1.10.1 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_2R_n) e il prodoto $XY = (x_1y_1, x_2y_2, x_ny_n)$.

1.10.2 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: $R \to R/J_1 \ast \cdots \ast R/J_n$ (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.

1.10.3 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).

1.10.4 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.

1.10.5 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.

Capitolo 2

Fonti per testo e immagini; autori; licenze

2.1 Testo

- **Corso:Algebra Anelli (Unimib)/Anelli/Generalità sugli anelli** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_Anelli_(Unimib)/Anelli/Generalit%C3%A0_sugli_anelli?oldid=48448 *Contributori:* Toma.luca95 e Mmontrasio
- **Corso:Algebra Anelli (Unimib)/Anelli/Classi di elementi** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_Anelli_(Unimib)/Anelli/Classi_di_elementi?oldid=48414 *Contributori:* Toma.luca95 e Mmontrasio
- **Corso:Algebra Anelli (Unimib)/Anelli/Sottoanello** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_Anelli_(Unimib)/Anelli/Sottoanello?oldid=48138 *Contributori:* Toma.luca95 e Mmontrasio
- **Corso:Algebra Anelli (Unimib)/Anelli/Polinomi** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_Anelli_(Unimib)/Anelli/Polinomi?oldid=48111 *Contributori:* Toma.luca95 e Mmontrasio
- **Corso:Algebra Anelli (Unimib)/Anelli/Corpo dei quaternioni** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_Anelli_(Unimib)/Anelli/Corpo_dei_quaternioni?oldid=48013 *Contributori:* Toma.luca95 e Mmontrasio
- **Corso:Algebra Anelli (Unimib)/Anelli/Congruenze in un anello** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_Anelli_(Unimib)/Anelli/Congruenze_in_un_anello?oldid=48164 *Contributori:* Toma.luca95 e Mmontrasio
- **Corso:Algebra Anelli (Unimib)/Anelli/Fattorizzazione** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_Anelli_(Unimib)/Anelli/Fattorizzazione?oldid=48242 *Contributori:* Toma.luca95 e Mmontrasio
- **Corso:Algebra Anelli (Unimib)/Anelli/Morfismi** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_Anelli_(Unimib)/Anelli/Morfismi?oldid=48218 *Contributori:* Toma.luca95 e Mmontrasio
- **Corso:Algebra Anelli (Unimib)/Anelli/Ideali primi e massimali** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_Anelli_(Unimib)/Anelli/Ideali_primi_e_massimali?oldid=48303 *Contributori:* Toma.luca95 e Mmontrasio
- **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

2.2 Immagini

2.3 Licenza dell'opera

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