Appunti del corso

Elementi di Algebra da un Punto di Vista Superiore

tenuto dal Prof. Libero Verardi

Università di Bologna - Anno Accademico 2013/2014

Michele Santa Maria

Indice

Introduzione

Questo testo è ricavato dagli appunti da me presi durante il corso *Elementi di Algebra da un Punto di Vista Superiore*, tenuto dal professor Libero Verardi nell'anno accademico 2013/14 all'Università di Bologna.

Nel corso degli appunti ho lasciato come esercizi quelle verifiche che in classe sono state lasciate da fare autonomamente a casa e che risultano prove non troppo complesse o comunque di tipo meccanico. Quegli esercizi che sono stati lasciati e che hanno invece richiesto uno sforzo maggiore li ho riportati come osservazioni dimostrate o esempi.

Prego chiunque legga questo testo di contattarmi nel caso trovasse alcuni errori nel testo (o anche solo per osservazioni/domande/chiarimenti) all'indirizzo email: msm139@gmail.com

Capitolo 1

24/02/2014

1.1 Introduzione al Linguaggio Algebrico

Per iniziare vediamo alcuni elementi che si usano molto in Algebra e che dobbiamo saper manipolare e discutere.

- Cos'è (a, b): potremmo definirlo usando la relazione

$$(a, b) = (a', b') \iff \begin{cases} a = a' \\ b = b' \end{cases}$$

  A partire da questo possiamo poi definire il *prodotto cartesiano* di due insiemi A e B come

$$A \times B := \{(a, b) \mid a \in A, b \in B\}$$

- Cos'è una *relazione* tra insiemi: possiamo pensare una relazione $\mathcal{R}$ come un sottoinsieme di $A \times B$.

- Cos'è una *funzione* da A a B: possiamo definire $f : A \longrightarrow B$ funzione se è una relazione che verifichi la seguente proprietà

$$\forall a \in A \quad \exists! b \in B \text{ tale che } (a, b) \in f \quad (\text{oppure } f(a) = b)$$

  chiamiamo in questo caso A "dominio", B "codominio" e $f(A)$ "immagine" (indicata con $Im(f)$).

- Cos'è una funzione *iniettiva* (o anche *suriettiva*, *bigettiva*) da A a B: ci sono diverse possibili definizioni, vediamone alcune.

  - $\forall b \in B$ esiste al più un $a \in A$ tale che $f(a) = b$
  - $\forall a, a' \in A$ vale $f(a) = f(a') \implies a = a'$

  - $\forall a, a' \in A$ vale $a \neq a' \Longrightarrow f(a) \neq f(a')$
  - $\forall b \in B$ l'equazione $f(x) = b$ ha al più una soluzione
  - Spieghiando con i diagrammi di Venn e le frecce

- Cos'è la funzione *inversa* di una funzione bigettiva: è una funzione $f^{-1} : B \longrightarrow A$ definita come $f^{-1}(y) = x$ se $f(x) = y$.

  A partire dalla nozione di bigettività si sono sviluppati molteplici concetti: le cardinalità, i gruppi di permutazione,...

- Cos'è una funzione *costante*: è una funzione per cui $\forall a, a' \in A$ vale $f(a) = f(a')$.

1.2 Calcolo Combinatorio

Vediamo alcuni punti chiave del Calcolo Combinatorio che devono essere ben chiari nella mente di tutti noi:

- **Principio di Addizione**: data una partizione di una insieme X, il numero di elementi di X è uguale alla somma degli elementi dei "pezzi" della partizione.
- **Principio di Moltiplicazione**: il numero di parole di k lettere composte in un alfabeto di N lettere sono al massimo N^k.
- In una gara di n partecipanti, i podi possibili sono $n(n-1)(n-2)$.
- $\left|B^A\right| = |\{\text{funzioni da } A \text{ a } B\}| = |B|^{|A|}$
- Se $|A| = |B| = n$, allora $|\{\text{funzioni bigettive da } A \text{ a } B\}| = n!$
- La parola "matrice" ha 7! anagrammi, tanti quanti le sue lettere.

  La parola "cavallo" ha lo stesso numero di lettere, ma contiene delle doppie, ovvero due "a" e due "l", che anche se scambiate non modificano la parola, quindi gli anagrammi possibili sono $\frac{7!}{2! \cdot 2!}$.

  La parola "mamma" ha cinque lettere, ma in realtà sono solo due lettere ripetute, quindi anche stavolta non avremo 5! possibili anagrammi bensì $\frac{5!}{3!2!}$.
- Se $|X| = n$, allora $|\{\text{sottoinsiemi di } X\}| = 2^n$.
- Se $|X| = n$, allora $|\{\text{sottoinsiemi di } X \text{ di } k \text{ elementi}\}| = \binom{n}{k}$.

Capitolo 2

03/03/2014

2.1 Monoidi di parole

In questa lezione vediamo un esempio di struttura algebrica che si collega con moltissime altre.

Prendiamo l'insieme *alfabeto* A, i cui elementi sono le *lettere*. Chiamiamo *parole* le successioni finite di lettere, e *lunghezza* di una parola il numero delle lettere che la compongono. Esiste la parola vuota che indichiamo con "$\emptyset$" a cui associamo la lunghezza 0.

Introduciamo a questo punto un'operazione in questa struttura: la *concatenazione* tra parole, indicata con "&", che associa ad una coppia di parole la parola ottenuta attaccando la seconda dopo la prima. Quest'operazione tra parole risulta essere associativa e con elemento neutro $\emptyset$.

Se indichiamo con $\mathcal{F}_A$ l'insieme delle parole nell'alfabeto A, la struttura $(\mathcal{F}_A, \&, \emptyset)$ è un monoide chiamato *monoide delle parole* (libere da regole).

Questa struttura ha delle proprietà: l'operazione & è associativa e vale la *legge di cancellazione*, ovvero $\forall w_1, w_2, w_3 \in \mathcal{F}_A$ valgono le seguenti uguaglianze:

$$w_1 \,\&\, w_2 \equiv w_1 \,\&\, w_3 \implies w_2 \equiv w_3$$

$$w_2 \,\&\, w_1 \equiv w_3 \,\&\, w_1 \implies w_3 \equiv w_2$$

Inoltre se indichiamo con $l(\cdot)$ la funzione che associa ad ogni parola la sua lunghezza, sono verificate le seguenti uguaglianze:

$$l(w_1 \,\&\, w_2) = l(w_1) + l(w_2) \qquad\qquad l(\emptyset) = 0$$

Vediamo dei casi particolari di questo monoide:

Esempio 2.1 (Alfabeto unitario) Se l'insieme A è formato solo da una lettera, ovvero $A = \{a\}$, le parole possibili sono stringhe del tipo

parola	$\emptyset$	a	aa	aaa	$aaaa$	$aaaaa$	$\dots$
lunghezza	0	1	2	3	4	5	$\dots$

Possiamo quindi trovare una corrispondenza biunivoca con l'insieme $\mathbb{N}$ e costruire addirittura un isomorfismo tra le strutture $(\mathcal{F}_{\{a\}}, \&, \emptyset) \longleftrightarrow (\mathbb{N}, +, 0)$.

A questo punto sorge una domanda: è vero che ogni monoide di parole con alfabeto $\{a\}$ è isomorfo a $(\mathbb{N}, +, 0)$? In realtà no, infatti possiamo aggiungere delle "regole" per far cambiare drasticamente struttura algebrica al nostro monoide di partenza.

Se introduciamo la regola del "mangiare", ovvero poniamo che la parola "$aaaaa$" sia equivalente a "$\emptyset$". Cosa succede?

Se introduciamo la notazione esponenziale $a^n = \overbrace{aa\cdots a}^{n \text{ volte}}$ e indichiamo la parola vuota con il simbolo "1", possiamo studiare le concatenazioni tra le possibili parole nel nostro alfabeto tramite una tabella:

$\&$	1	a	a^2	a^3	a^4
1	1	a	a^2	a^3	a^4
a	a	a^2	a^3	a^4	1
a^2	a^2	a^3	a^4	1	a
a^3	a^3	a^4	1	a	a^2
a^4	a^4	1	a	a^2	a^3

Come possiamo vedere dalla tabella, in questo caso ogni elemento ha inverso! Quindi il nostro monoide diventa un *gruppo*, isomorfo a C_5 (o $\mathbb{Z}_5$), il *gruppo ciclico di ordine 5.*

In generale, se nel monoide $(\mathcal{F}_{\{a\}}, \&, \emptyset)$ poniamo la regola "$a^n \equiv \emptyset$", otteniamo un gruppo ciclico di ordine n, quindi isomorfo a C_n (o $\mathbb{Z}_n$), che possiamo proprio rappresentare come $C_n =< a \mid a^n \equiv \emptyset >$.

Esercizio 2.1 Se introduciamo nel monoide $(\mathcal{F}_{\{a\}}, \&, \emptyset)$ la regola "$aaaa \equiv aaaaa$", che struttura algebrica otteniamo?

Esempio 2.2 (Alfabeto binario) Consideriamo ora il caso in cui il nostro alfabeto è formato da due lettere: $A = \{a, b\}$.

In questo caso le parole possibili sono molto diverse:

parola	$\emptyset$	a	b	a^2	ab	ba	b^2	a^3	a^2b	aba	ab^2	ba^2	bab	$\dots$
lunghezza	0	1	1	2	2	2	2	3	3	3	3	3	3	$\dots$

e la struttura così definita risulta non commutativa.

E se la rendessimo commutativa? L'insieme di parole a questo punto cambia molto (in particolare si restringe):

parola	$\emptyset$	a	b	a^2	$ab \equiv ba$	b^2	a^3	a^2b	ab^2	b^3	a^4	a^3b	$\dots$
lunghezza	0	1	1	2	2	2	3	3	3	3	4	4	$\dots$

proviamo anche ad usare diverse regole di equivalenza per vedere cosa otteniamo:

- $ab \equiv ba$ e $ab \equiv 1$

  Se $ab = 1$, visto che partiamo da una struttura commutativa, ogni volta che una parola contiene una lettera a e una lettera b esse si "annullano", quindi le parole possibili in questo caso contengono solo la lettera a o solo la lettera b, quindi l'insieme $\mathcal{F}_A$ è di questo tipo:

parola	$\dots$	b^3	b^2	b	1	a	a^2	a^3	$\dots$
lunghezza	$\dots$	3	2	1	0	1	2	3	$\dots$

  Inoltre ogni parola ha inverso poiché $a^n \,\&\, b^n = 1$, quindi abbiamo ottenuto un gruppo isomorfo a $(\mathbb{Z}, +, 0)$, che ha due generatori a e b invece che $+1$ e -1.

- $ab \equiv ba$ e $a^3 \equiv 1 \equiv b^2$

  In questo caso le parole possibili sono solo sei, visto che la struttura è commutativa: $1, a, a^2, b, ab, a^2b$. Analizziamo i loro prodotti (o concatenazioni).

$\cdot$	1	a	a^2	b	ab	a^2b
1	1	a	a^2	b	ab	a^2b
a	a	a^2	1	ab	a^2b	b
a^2	a^2	1	a	a^2b	b	ab
b	b	ab	a^2b	1	a	a^2
ab	ab	a^2b	b	a	a^2	1
a^2b	a^2b	b	ab	a^2	1	a

  Sebbene i prodotti possano sembrare piuttosto strani, possiamo ragionare in maniera algebrica per capire cosa abbiamo ottenuto: ogni elemento ha un inverso, quindi è un gruppo. Inoltre questo gruppo (commutativo) ha solo 6 elementi, quindi è necessariamente isomorfo a C_6 (o $\mathbb{Z}_6$).

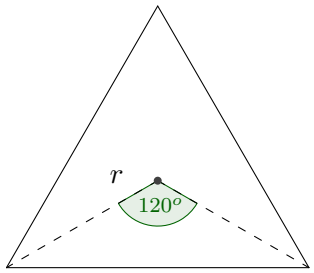
- $a^3 \equiv 1 \equiv b^2$ e $ba = a^2b$

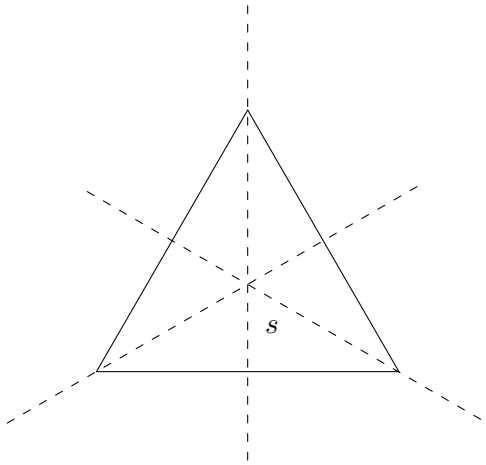
  In questo caso l'insieme delle parole è lo stesso di prima: $1, a, a^2, b, ab, a^2b$; ma la struttura non è più commutativa. La "tavola degli elementi" in questo caso risulta essere

$\cdot$	1	a	a^2	b	ab	a^2b
1	1	a	a^2	b	ab	a^2b
a	a	a^2	1	ab	a^2b	b
a^2	a^2	1	a	a^2b	b	ab
b	b	a^2b	ab	1	a^2	a
ab	ab	b	a^2b	a	1	a^2
a^2b	a^2b	ab	b	a^2	a	1

  Questa struttura, la cui tabella è più complessa di quelle viste in precedenza, è isomorfa a D_3, il gruppo *diedrale* di tre elementi, ovvero il gruppo delle isometrie del piano che mantengono fisso un triangolo equilatero.

  Preso un triangolo equilatero sul piano euclideo, le isometrie del piano che mandano il triangolo in sé sono generate da due elementi: la rotazione r di 120^o attorno al centro[1] del triangolo, e la simmetria s rispetto ad un asse del triangolo.





  Per queste isometrie valgono infatti le stesse "regole" che abbiamo introdotto: $r^3 = id$, $s^2 = id$, $s \circ r = r^2 \circ s$. Quindi abbiamo ottenuto un gruppo non commutativo isomorfo a D_3.

[1] Come "centro" del triangolo intendiamo il punto di incontro degli assi, o delle altezze, visto che il triangolo è equilatero.

Capitolo 3

05/03/2014

3.1 Gruppo Diedrale e prodotto diretto

Nella scorsa lezione abbiamo parlato dei gruppi *Diedrali*, adesso cerchiamo di analizzarli meglio.

In generale, il *gruppo diedrale n-esimo* D_n è un gruppo generato da due elementi r, s in cui r ha ordine n e s ha ordine 2, e vale la relazione $sr = r^{n-1}s$. In linguaggio algebrico scriveremo

$$D_n := < r, s \mid r^n = 1,\ s^2 = 1,\ sr = r^{n-1}s >$$

Il gruppo diedrale D_n così definito ha ordine $2n$ e non è commutativo.

Definizione 3.1 Dati due gruppi $(H, \cdot)$ e $(G, *)$, chiamiamo *prodotto diretto* di H e G il gruppo definito come

$$K := H \times G := \{(h, g) \mid h \in H,\ g \in G\}$$

con l'operazione di gruppo così definita:

$$(h_1, k_1) \star (h_2, k_2) = (h_1 \cdot h_2, k_1 * k_2)$$

ed elemento neutro e inverso di questa forma:

$$1_K = (1_H, 1_G) \qquad\qquad (h, g)^{-1} = (h^{-1}, g^{-1})$$

Vale la pena osservare che il gruppo $G \times H$ risulta isomorfo ad $H \times G$, tramite l'isomorfismo $\varphi(h, g) := (g, h)$.

3.2 Esempi di monoidi

Continuiamo a parlare dei *monoidi di parole* descritti nella scorsa lezione.

Esempio 3.1 Prendiamo un alfabeto numerabile $A = \{p_1, p_2, \ldots\}$ con la proprietà commutativa.

Visto che l'alfabeto è commutativo, le parole scrivibili (oltre la parola vuota che indichiamo con "1") sono del tipo $p_1^{k_1}\, p_2^{k_2}\, \ldots\, p_r^{k_r}$, in cui abbiamo usato la notazione esponenziale per descrivere la concatenazione ripetuta di una stessa lettera p_i.

Questo altro non è che il monoide dei numeri naturali positivi $(\mathbb{N}^+, \cdot, 1)$ in cui le "lettere" rappresentano i numeri *primi*! Quello che abbiamo costruito poco fa è solo un modello astratto del monoide concreto.

Vediamo altri esempi di monoidi:

- $(\mathbb{N}, MCD, 0)$: è commutativo, ha elemento *assorbente* 1, difatti $MCD(n, 1) = 1$.
- $(\mathbb{N}, mcm, 1)$: è commutativo, ha elemento *assorbente* 0, difatti $mcm(n, 0) = 0$.
- $(\mathcal{P}(X), \cup, \emptyset)$ (in cui X è un insieme): è commutativo, ha elemento *assorbente* X, difatti $A \cup X = X$.

3.3 Potenze nei monoidi e nei gruppi

Nei monoidi è possibile definire l'operazione di *potenza* nel seguente modo: sia $(M, \cdot, 1_M)$ monoide, e $a \in M$; poniamo:

$$\begin{cases} a^0 = 1 \\ a^{n+1} = a^n \cdot a \end{cases}$$

Proprietà:

1. $a^m \cdot a^n = a^{m+n}$;
2. $(a^m)^n = a^{m \cdot n}$;
3. Se il monoide M è commutativo, vale $(a \cdot b)^n = a^n \cdot b^n$.

Nei gruppi si fa la stessa cosa, per cui si definisce a^n come sopra, ma c'è di più: nei gruppi ogni elemento a ha un inverso a^{-1}, per cui si definisce

$$a^{-n} := \left(a^{-1}\right)^n$$

e si dimostra che $(a^n)^{-1} = \left(a^{-1}\right)^n$.

Definizione 3.2 Dato il gruppo $(G, \cdot)$ e un elemento $g \in G$, denotiamo con $< g >:= \{g^n \mid n \in \mathbb{Z}\} \subseteq G$ il *sottogruppo generato da g*. Chiamiamo *ordine* (o *periodo*) di g il numero di elementi del sottogruppo $< g >$, che indichiamo con $o(g) = |g| := | < g > |$.

Esempio 3.2 In ogni gruppo G l'elemento neutro 1_G ha ordine 1, visto che vale sempre $< 1_G >= \{1_G\}$.

In $(\mathbb{Z}, +)$ ogni elemento non nullo n ha ordine infinito: $|n| = \infty$.

Osservazione

- Gli elementi di un gruppo finito hanno sempre ordine finito[1].
- Un gruppo infinito può avere elementi di ordine infinito (l'abbiamo appena mostrato con l'esempio di $(\mathbb{Z}, +)$.
- Un gruppo infinito può avere anche elementi di ordine finito, vediamo un esempio:

  Prendiamo un insieme X e definiamo sull'insieme delle sue parti $\mathcal{P}(X)$ l'operazione $A \triangle B := (A \setminus B) \cup (B \setminus A)$.

  Questa operazione è commutativa e associativa, con elemento neutro $\emptyset$. L'opposto di un elemento $A \in \mathcal{P}(X)$ secondo l'operazione $\triangle$ è l'elemento A stesso, visto che $A \triangle A = (A \setminus A) \cup (B \setminus A) = \emptyset$.

  Dunque ogni elemento diverso dal vuoto ha ordine 2, come volevamo.

Contare gli elementi del sottogruppo $< g >$ non è però l'unico modo (né il più veloce) di sapere l'ordine dell'elemento g. Vale infatti la seguenti proprietà:

Se $\exists\, n \in \mathbb{N}$ tale che $g^n = 1_G$, allora se chiamiamo $k := \min\{n \in \mathbb{N} \mid g^n = 1_G\}$ vale $|g| = k$.

Definizione 3.3 Un gruppo G si dice *ciclico* se $\exists\, g \in G$ tale che $G =< g >$.

Esempio 3.3 L'esempio più semplice di gruppo ciclico (infinito) è il gruppo $\mathbb{Z} =< 1 >=< -1 >$.

Nella scorsa lezione abbiamo anche visto $C_n =< a \mid a^n = 1 >$, che è invece un gruppo ciclico finito (di ordine n).

3.4 Anelli

Si chiamano *anelli* le strutture algebriche del tipo $(A, +, \cdot, 0_A, 1_A, (-))$ (in cui '$(-)$' indica l'operazione di "cambiamento di segno"), che gode delle seguenti **proprietà**:

[1] Si sa di più: il teorema di Lagrange dimostra che l'ordine di un elemento divide sempre l'ordine del gruppo a cui appartiene.

- $(A, +, 0_A)$ è un gruppo abeliano
- $(A, \cdot, 1_A)$ è un monoide
- vale la distributività della somma rispetto al prodotto in entrambi i lati, ovvero $\forall a, b, c \in A$

$$(a+b)\cdot c = a\cdot c + b\cdot c \qquad\qquad c(a+b) = c\cdot a + c\cdot b$$

All'interno di un anello A è molto importante la struttura $A^* := \{a \in A \mid \exists a^{-1}\}$, chiamata *gruppo delle unità* (o *degli invertibili*) *di* A, ovvero il gruppo formato da quegli elementi di A che possiedono inverso moltiplicativo (indicato con a^{-1}).

Altra sottostruttura molto importante è rappresentata da $< 1_A >= \{n1_A \mid n \in \mathbb{Z}\}$, che risulta chiuso per le operazioni di A:

$$(m1_A)\cdot(n1_A) = (mn)1_A \qquad\qquad (m1_A) + (n1_A) = (m+n)1_A$$

$$01_A = 0_A \qquad\qquad 11_A = 1_A \qquad\qquad -(n1_A) = (-n)1_A$$

ed è quindi un vero e proprio sottoanello chiamato *sottoanello fondamentale di* A.

Si chiama *caratteristica* dell'anello A (indicata con $char(A)$) la quantità così definita:

$$char(A) = \begin{cases} 0 & \text{se } |1_A| = \infty \\ n & \text{se } |1_A| = n \end{cases}$$

Sicuramente $0_A \notin A^*$, visto che l'inverso di 0_A non esiste mai, dunque al più si può avere $A^* = A \setminus \{0_A\}$; gli anelli per cui vale questa proprietà sono detti *corpi*, e se sono anche commutativi allora sono detti *campi*.

Infine, un anello che non contiene elementi invertibili (ovvero in cui $A^* = \emptyset$) è detto *dominio di integrità* o semplicemente anello *integro*.

Capitolo 4

06/03/2014

4.1 Anello delle Funzioni

Nota: si considerano già acquisite le nozioni base e le proprietà degli **anelli**, che non verranno qui ripetute.

Sia A un anello commutativo, che supponiamo sempre con identità, con la seguente struttura: $(A, +, \cdot, 1_A)$; e sia X un insieme non vuoto.

Introduciamo il seguente simbolo

$$A^X := \{f \mid f : X \longrightarrow A\}$$

che rappresenta l'insieme delle funzioni da X ad A, definite punto per punto:

- $(f + g)(x) = f(x) + g(x)$
- $(f \cdot g)(x) = f(x) \cdot g(x)$
- $0(x) = 0_A$
- $1(x) = 1_A$
- $(-f)(x) = -\big(f(x)\big)$

Grazie a questa definizione sulle funzioni, la struttura $(A^X, +, \cdot, 1)$ è un anello commutativo.

Osservazione A^X <u>non</u> è un dominio di integrità se $|X| > 1$.

Dimostrazione. Se $|X| > 1$ possiamo prendere $x_1 \neq x_2$ e costruire due funzioni

$$f_1(x) = \begin{cases} 1_A & \text{se } x = x_1 \\ 0_A & \text{altrimenti} \end{cases} \qquad f_2(x) = \begin{cases} 1_A & \text{se } x = x_2 \\ 0_A & \text{altrimenti} \end{cases}$$

A questo punto il prodotto $f_1 \cdot f_2$ risulta nullo, anche se le due funzioni sono non nulle

$$(f_1 \cdot f_2)(x) = 0 \quad \forall x$$

che dimostra che A^X non è un dominio.

□

Chi sono gli invertibili di A^X?
Sono le funzioni che hanno immagine tutta contenuta negli invertibili di A.

Se consideriamo $A = \mathbb{R}$ e $X \subseteq \mathbb{R}$, abbiamo appena costruito le classiche *funzioni reali*, invece se consideriamo $A = \mathbb{R}$ e $X \subseteq \mathbb{N}$ si formano le *successioni*.

4.2 Anello delle Successioni

L'anello delle successioni, che abbiamo visto come costruire, ha alcune proprietà particolari. Riscriviamo le proprietà scritte sopra per gli elementi di $A^{\mathbb{N}}$ (ovvero le successioni):

- $(f + g)(n) = f(n) = a_n$
- $(-f)(n) = -f(n) = -a_n$
- $0(n) = 0_A$
- Moltiplicazione per *convoluzione*:

$$(f \cdot g)(n) = \sum_{i=0}^{n} f(i) \cdot g(n - i)$$

- Identità moltiplicativa:

$$1(n) = \begin{cases} 1_A & \text{se } n = 0 \\ 0_A & \text{se } n > 0 \end{cases}$$

Con le operazioni così definite, l'anello $A^{\mathbb{N}}$ risulta essere un anello commutativo diverso dalle funzioni da $\mathbb{N}$ ad A definite punto per punto.

Infatti $A^{\mathbb{N}}$ risulta essere un dominio di integrità se e solo se A è un dominio di integrità, dimostriamolo.

Dimostrazione. $\boxed{\Rightarrow}$ Per assurdo: supponiamo che A non sia un dominio, ovvero che $\exists\, a, b \in A \backslash \{0\}$ tali che $a \cdot b = 0$.
Definiamo allora le due funzioni

$$f(n) = \begin{cases} a & \text{se } n = 0 \\ 0_A & \text{se } n > 0 \end{cases} \qquad g(n) = \begin{cases} b & \text{se } n = 0 \\ 0_A & \text{se } n > 0 \end{cases}$$

che portano al nostro assurdo perché risulta

$$(f \cdot g)(n) = \sum_{i=0}^{n} f(i)g(n-i) = 0_A + 0_A + \ldots + 0_A = 0_A$$

$$\implies \qquad f \cdot g = 0 \quad \wedge \quad f, g \neq 0$$

che è assurdo perché siamo partiti dall'ipotesi che A^X fosse un dominio di integrità.

$\boxed{\Leftarrow}$ Se A è un dominio, prendiamo $f, g \in A^{\mathbb{N}} \setminus \{0\}$.
Allora esistono due indici minimi $m, n \in \mathbb{N}$ per cui vale $f(m) \neq 0_A$ e $g(n) \neq 0_A$.
Senza perdita di generalità supponiamo $m \leq n$ ed otteniamo:

$$f \cdot g(m+n) = \sum_{i=0}^{m+n} f(i)g(m+n-i)$$

Suddividiamo la sommatoria in tre parti:

- $i < m \implies f(i) = 0_A \implies f(i)g(m+n-i) = 0_A$
- $i = m \implies f(m)g(n) \neq 0_A$
- $i > m \implies m+n-i < n \implies f(i)g(m+n-i) = 0_A$

$$f \cdot g(m+n) = \sum_{i=0}^{m+n} f(i)g(m+n-i) = f(m)g(n) \neq 0_A$$

il che dimostra che $A^{\mathbb{N}}$ è un dominio.

□

Esercizio 4.1 Individuare gli elementi invertibili di $A^{\mathbb{N}}$.

Osservazione Se A è un dominio deve avere caratteristica 0 o un primo p. In particolare, se la caratteristica è un primo p, ogni elemento non nullo ha ordine p nel gruppo $(A, +)$.
Un tale gruppo è detto *p-gruppo abeliano elementare*.

Osservazione Ogni dominio finito è un campo.

Dimostrazione. Sia D un dominio finito.
Se prendiamo un suo elemento $a \neq 0_D$, possiamo definire la funzione $f_a(x) := a \cdot x$, che risulta iniettiva:

$$f_a(x) = f_a(y) \quad \iff \quad ax = ay \quad \iff \quad x = y$$

Se D è finito, $f_a : D \longrightarrow D$ risulta necessariamente bigettiva, quindi $1_D \in Img(f_a)$. Questo vuol dire che $\exists\, x_0 \in D$ tale che $f_a(x_0) = ax_0 = 1_D$, il che significa che a è invertibile.

Abbiamo appena dimostrato che un elemento qualsiasi non nullo di D è invertibile, quindi D è un campo.

□

Esercizio 4.2 Dimostrare che se A è un anello con unità allora l'operazione $+$ di gruppo deve essere commutativa.

Capitolo 5

10/03/2014

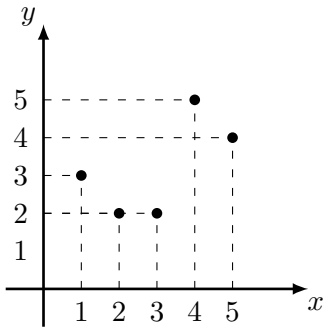
5.1 Seminario sulle Funzioni

Dopo la presentazione di due studentesse (Anna ed Elisa) del seminario sulle funzioni nelle scuole abbiamo continuato a parlare un po' di questo argomento, concentrandoci principalmente sul fatto che ci sono molti modi di rappresentare una stessa funzione:

1. La tabella

x	1	2	3	4	5
$f(x)$	3	2	2	5	4

2. Il grafico cartesiano



3. Rappresentazione mediante una matrice "booleana": 1=vero, 0=falso

$$M_f = \begin{array}{c|ccccc} & 1 & 2 & 3 & 4 & 5 \\ \hline 1 & 0 & 0 & 1 & 0 & 0 \\ 2 & 0 & 1 & 0 & 0 & 0 \\ 3 & 0 & 1 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & 0 & 1 \\ 5 & 0 & 0 & 0 & 1 & 0 \end{array}$$

in cui in ogni riga c'è uno ed un solo 1. L'immagine in questo caso è costituita dai numeri delle colonne non nulle. In particolare, se la funzione è bigettiva in ogni riga e colonna c'è uno ed un solo 1 e la matrice è quadrata.

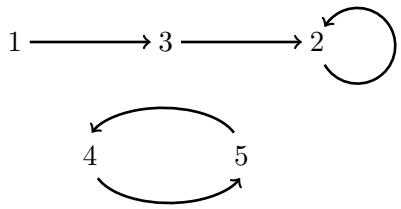
Nel caso di una matrice quadrata la matrice presentata ci dà molte altre informazioni: si può calcolarne il rango $r(M_f)$ per trovare il numero di elementi dell'immagine; oppure il determinante, che risulta essere

$$det(M_f) = \begin{cases} 0 & \text{se } f \text{ non è iniettiva} \\ 1 & \text{se } f \text{ è pari} \\ -1 & \text{se } f \text{ è dispari} \end{cases}$$

Inoltre la traccia $tr(M_f)$ ci dice quanti sono gli elementi "fissi", cioè tali che $f(x) = x$.

Nell'esempio: $r(M_f) = 4$, $det(M_f) = 0$, $tr(M_f) = 1$.

4. Rappresentiamo $f : X \longrightarrow X$ con un grafo orientato:



I punti x_i disegnati sono detti "vertici" e le frecce che li uniscono sono detti "archi". Se è possibile disegnare il grafo in modo che gli archi non si intersechino mai, il grafo si dice "planare".

Capitolo 6

14/03/2014

6.1 Reticoli

Oggi vorremmo arrivare a dare la nozione di *reticolo* algebrico, ma per farlo dovremo prima lavorare su relazioni già probabilmente conosciute.

Definizione 6.1 Sia $(L, \leq)$ un insieme ordinato e siano $x, y \in L$, con $x < y$. Diciamo che x è *coperto* da y se $\forall z \in L$, $x \leq z \leq y \implies z = x$ oppure $z = y$.

Si scrive $x \prec y$.

Definizione 6.2 Se L ha minimo, che indichiamo con "0_L", gli eventuali elementi che lo coprono sono detti *atomi* o *minimali*.

Dualmente, se L ha massimo, che indichiamo con "1_L", gli elementi coperti da 1_L sono detti *co-atomi* o *massimali*.

Osservazione Se l'ordine è denso la relazione appena descritta è vuota.

Esempio 6.1 In $(\mathbb{N}, \leq)$ ogni $n \in \mathbb{N}$ è coperto da $n + 1$. L'unico atomo è quindi 1.

Esempio 6.2 Sia X un insieme. L'insieme $(\mathcal{P}(X), \subseteq)$ ha minimo, $\emptyset$, e massimo, X.

Gli atomi sono i "singoletti" $\{x\} \in \mathcal{P}(X)$, in cui $x \in X$.

I co-atomi sono i sottoinsiemi del tipo $X \setminus \{x\} \in \mathcal{P}(X)$, con $x \in X$.

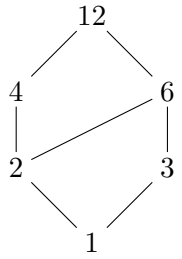
Per un insieme L finito si può usare un particolare di grafo per rappresentare la relazione di copertura, che descrive poi tutta la relazione $\leq$ nel seguente modo:

- Gli elementi più grandi sono "più in alto" rispetto ai più piccoli.
- Un arco collega x con y se x è coperto da y.

Grafi di questo tipo si chiamano **Diagrammi di Hasse**.

Esempio 6.3 L'insieme $X = \{1, 2, 3, 4, 5, 6, 12\}$, con l'ordinamento $\leq$ classicamente definito in $\mathbb{N}$.

Possiamo definire un'altra relazione di ordine su X attraverso un diagramma dello stesso tipo:



Dunque se è vero che un ordinamento definisce un diagramma di Hasse è vero anche il viceversa: da un diagramma di Hasse si può risalire ad un ordinamento.

Definizione 6.3 Preso $(L, \leq)$, siano $a, b \in L$.

L'*estremo superiore* S di $\{a, b\}$, indicato con $\sup\{a, b\}$ è un elemento di L tale che

1. $a \leq S$, $b \leq S$
2. $\forall x \in L$ vale la seguente proprietà: $a \leq x$ e $b \leq x \Longrightarrow S \leq x$

In maniera analoga si definisce l'*estremo inferiore* di $\{a, b\}$, che viene indicato con $\inf\{a, b\}$.

Definizione 6.4 L'insieme $(L, \leq)$ si dice *reticolo* se per ogni coppia $(a, b) \in L^2$ esistono l'estremo superiore e inferiore di $\{a, b\}$.

In tal caso si pone $a \vee b := \sup\{a, b\}$ e $a \wedge b := \inf\{a, b\}$.

Se il reticolo ammette minimo 0_L e massimo 1_L indicheremo con $(L, \vee, \wedge, 0_L, 1_L)$ il *reticolo con minimo e massimo.*

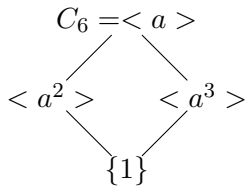
Nelle definizioni precedenti i simboli "$\vee$" e "$\wedge$" possono essere visti come due operazioni binarie in L con le seguenti proprietà:

- **Commutativa:** $a \vee b = b \vee a$ $\qquad$ $a \wedge b = b \wedge a$
- **Idempotenza:** $a \vee a = a$ $\qquad$ $a \wedge a = a$
- **Associativa:** $(a \vee b) \vee c = a \vee (b \vee c)$ $\qquad$ $(a \wedge b) \wedge c = a \wedge (b \wedge c)$
- **Legge di Assorbimento:** $a \vee (b \wedge a) = a$ $\qquad$ $a \vee (b \wedge a) = a$

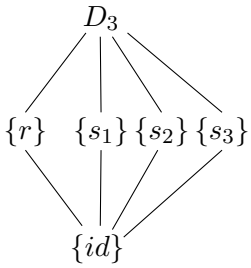
Esempio 6.4 Ci sono molti esempi di insiemi che danno luogo a reticoli:

1. $(\mathcal{P}(X), \subseteq) \longrightarrow (\mathcal{P}(X), \cup, \cap)$
2. $(\mathbb{N}, \leq) \longrightarrow (\mathbb{N}, \max, \min)$
3. $(\mathbb{N}, |) \longleftarrow (\mathbb{N}, mcm, MCD)$[1]

Esempio 6.5 $C_6 =< a \mid a^6 = 1 >$ ha la struttura di reticolo definita dal seguente diagramma:



Esempio 6.6 D_3[2] è generato dalla rotazione r di 120^o, e dai tre ribaltamenti possibili s_1, s_2, s_3 lungo gli assi del triangolo. Anche questo possiede la struttura di reticolo definita da un diagramma di Hasse:



[1] In questo esempio usiamo i simboli standard dell'aritmetica per indicare con "|" la relazione "divisore", con "mcm" il "minimo comune multiplo" tra due numeri, e con "MCD" il "massimo comun divisore".

[2] Ricordiamo che con D_3 indichiamo il gruppo delle trasformazioni del piano che lasciano immutato un triangolo equilatero.

Quindi a partire da un insieme ordinato abbiamo visto che si possono generare dei reticoli con due operazioni che hanno le quattro proprietà di prima. Il procedimento però si può anche invertire:

Presa $(L, \vee, \wedge)$ una struttura algebrica con due operazioni binarie che hanno le quattro proprietà elencate sopra possiamo definire in L una relazione d'ordine

$$a \leq b \iff a \wedge b = a$$

Esercizio 6.1 Dimostrare che è un ordinamento ben definito.

Inoltre $\forall a, b \in L$ risulta $\sup\{a, b\} = a \vee b$ e $\inf\{a, b\} = a \wedge b$, quindi $(L, \leq)$ è un reticolo!

Pensando meglio a ciò che abbiamo scritto, a volte $(L, \leq)$ ha minimo 0_L e massimo 1_L. Ma questi che ruolo hanno?

Poiché $0_L \leq a \ \forall a$ si ha $0_L \wedge a = 0_L$, $0_L \vee a = a$, dunque 0_L è elemento neutro per $\vee$ e elemento assorbente per $\wedge$.

Allo stesso modo 1_L risulta essere elemento neutro per $\wedge$ e elemento assorbente per $\vee$.

Definizione 6.5 I reticoli in cui le due operazioni sono distributive l'una rispetto all'altra si dicono *reticoli distributivi.*

Osservazione Tutti gli insiemi totalmente ordinati danno luogo a reticoli distributivi, ma non sono gli unici possibili (anche gli esempi fatti sopra lo sono).

6.2 Reticoli e Sottostrutture

Un esempio di reticolo molto interessante è presentato dalle sottostrutture di una struttura algebrica:

Presa $(X, f_1, f_2, \ldots, f_r)$ una struttura algebrica, un sottoinsieme Y di X si dice *chiuso* rispetto all'operazione n-aria f_i se $\forall y_1, \ldots, y_n \in Y \, f_i(y_1, \ldots, y_n) \in Y$.

Una *sottostruttura* è costituita da un sottoinsieme chiuso rispetto a tutte le operazioni della struttura.

Lemma *L'intersezione di un insieme di sottostrutture è ancora una sottostruttura.*

Osservazione Per l'unione questo non è affatto vero: preso $(\mathbb{Z}, +)$ come gruppo possiamo considerare i sottogruppi $2\mathbb{Z}$ e $3\mathbb{Z}$, ma la loro unione non è un sottogruppo poiché $2 + 3 = 5 \notin (2\mathbb{Z} \cup 3\mathbb{Z})$.

Definizione 6.6 Dato un sottoinsieme $S \subseteq X$ possiamo considerare

$$< S >:= \bigcap \{Y \mid Y \text{ sottostruttura di } X, \ S \subseteq Y\}$$

che chiamiamo *sottostruttura generata da* S.

Se ora consideriamo $\mathcal{L}(X)$ l'insieme delle sottostrutture di X e per ogni $H, K \in \mathcal{L}(X)$ definiamo

$$H \wedge K := H \cap K \qquad H \vee K :=< H \cup K >$$

allora $(\mathcal{L}(X), \vee, \wedge)$ è un reticolo per cui risulta

$$\max(\mathcal{L}(X)) = X \qquad \min(\mathcal{L}(X)) =< \emptyset >= \bigcap\{H \in \mathcal{L}(X)\}$$

Esempio 6.7 Per un gruppo G, vale $< \emptyset >= \{1_G\}$.

Per un anello A, risulta $< \emptyset >=< \{0_A, 1_A\} >=< \{1_A\} >$.

Esempio 6.8 L'unica sottostruttura dell'anello $(\mathbb{Z}, +, \cdot, 0, 1)$ è sé stesso, poiché $< \emptyset >=< \{1\} >= \mathbb{Z}$.

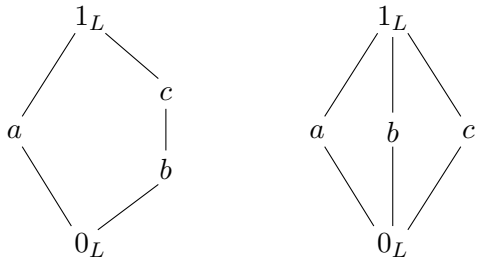
6.3 Algebre di Boole

Definizione 6.7 Preso $x \in L$ chiamiamo *complementare* di x, indicato con x', un elemento di L tale per cui

$$\begin{cases} x \vee x' = 1_L \\ x \wedge x' = 0_L \end{cases}$$

Attenzione: tale elemento potrebbe non essere unico.

Esempio 6.9 Facciamo un esempio di complementare usando i diagrammi di Hasse:



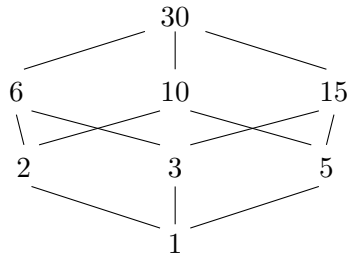
In entrambi questi diagrammi b e c sono complementari di a.

Teorema 6.1 *In un reticolo distributivo il complementare, se esiste, è unico.*

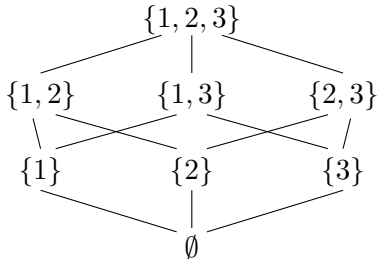
Definizione 6.8 Se in un reticolo distributivo ogni elemento ha complementare, la struttura algebrica $(L, \vee, \wedge, 0_L, 1_L, ')$, in cui la funzione bigettiva " $'$ " associa ad ogni $x \in L$ il suo complementare, viene detta *Algebra di Boole*.

Esempio 6.10 L'esempio più generale di Algebra di Boole $(\mathcal{P}(X), \bigcup, \bigcap, \emptyset, X, ')$, dove $'$ indica il complementare dell'insieme dato.

Esempio 6.11 I divisori di 30 formano un'algebra di Boole, in cui il complementare di x è quel numero x' tale che $x \cdot x' = 30$. Possiamo anche disegnare il diagramma di Hasse di questa struttura:



Esempio 6.12 Preso $X = \{1, 2, 3\}$ con l'ordinamento $\subseteq$ di inclusione possiamo definire il seguente diagramma



e ottenere un'algebra di Boole identica a quella dell'esempio precedente.

A ben vedere tutti gli esempi precedenti sembravano abbastanza simili tra di loro, e questo in effetti non è un caso. Si è infatti dimostrato il seguente teorema:

Teorema 6.2 *Tutte le algebre di Boole sono isomorfe a* $(\mathcal{P}(X), \cup, \cap, \emptyset, X, ')$.

Capitolo 7

17/03/2014

7.1 Omomorfismi e Isomorfismi

Definizione 7.1 Siano $(X, f_1, f_2, \ldots, f_r)$, $(Y, g_1, g_2, \ldots, g_r)$ due strutture algebriche dello stesso tipo[1].

Un *omomorfismo* è una funzione $\varphi : X \longrightarrow Y$ tale che $\forall i, 1 \leq i \leq r$ valgono le seguenti proprietà:

1. Se f_i e g_i sono operazioni n-arie, $n \geq 1$

$$\forall x_1, \ldots, x_n \in X \qquad \varphi\big(f_i(x_1, \ldots, x_n)\big) = g_i\big(\varphi(x_1, \ldots, x_n)\big)$$

2. Se $f_i = x_0 \in X$, $g_i = y_0 \in Y$ vale $\varphi(x_0) = y_o$

Esempio 7.1 Se $(M, \cdot, 1_M)$, $(N, *, 1_N)$ sono due monoidi, un omomorfismo tra essi è una funzione $\varphi : M \longrightarrow N$ tale che $\forall x, y \in M$ vale $\varphi(x \cdot y) = \varphi(x) * \varphi(y)$, e $\varphi(1_M) = 1_N$.

Esempio 7.2 Se $(G, \cdot, 1_G)$, $(H, *, 1_H)$ sono due gruppi, un omomorfismo tra essi è una funzione $\varphi : M \longrightarrow N$ tale che $\forall x, y \in M$ vale $\varphi(x \cdot y) = \varphi(x) * \varphi(y)$.

Le condizioni $\varphi(1_G) = 1_H$ e $\varphi(x^{-1}) = \varphi(x)^{-1}$ sono infatti verificate direttamente in conseguenza della proprietà di sopra.

Esempio 7.3 Se $(A, +, \cdot, 1_A)$, $(B, +, \cdot, 1_B)$ sono due anelli, un omomorfismo tra essi è una funzione $\varphi : M \longrightarrow N$ tale che

1. $\forall x, y \in A$ vale $\varphi(x + y) = \varphi(x) + \varphi(y)$
2. $\forall x, y \in A$ vale $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$
3. $\varphi(1_A) = 1_B$

[1] Due monoidi, due gruppi, due anelli, due reticoli, o altri esempi del genere. Ovvero in cui $\forall i$ le operazioni f_i e g_i devono avere le stesse proprietà.

Definizione 7.2 Un omomorfismo φ bigettivo si dice *isomorfismo*.

Esempio 7.4 Presi i due gruppi $(\mathbb{R}^+, \cdot)$, $(\mathbb{R}, +)$, la funzione di logaritmo naturale $\ln : \mathbb{R}^+ \longrightarrow \mathbb{R}$ definito come

$$\ln(x) := \int_1^x \frac{1}{t} dt$$

è un isomorfismo:

1. La funzione $\ln(x)$ è surgettiva perché valgono i seguenti limiti

$$\lim_{x \longrightarrow +\infty} \ln(x) = +\infty \qquad \lim_{x \longrightarrow 0^+} \ln(x) = -\infty$$

2. La funzione è iniettiva perché la sua derivata risulta

$$\big(\ln(x)\big)' = \frac{1}{x} > 0 \quad x \in \mathbb{R}^+$$

3. Per ogni $x_1, x_2 \in \mathbb{R}^+$ vale

$$\ln(x_1 \cdot x_2) = \ln(x_1) + \ln(x_2)$$

Esempio 7.5 La funzione inversa di $\ln(x)$, che indichiamo con $f(x) = e^x$ è un isomorfismo tra $(\mathbb{R}, +)$ e $(\mathbb{R}^+, \cdot)$. Non abbiamo niente da dimostrare, è causa diretta dell'esempio precedente.

Esempio 7.6 $(\mathbb{Z}, +)$ e $(\mathbb{R}, +)$ non sono isomorfi perché $\mathbb{Z}$ è numerabile ma $\mathbb{R}$ no.
$(\mathbb{Z}, +)$ e $(\mathbb{Q}, +)$ non sono isomorfi perché $\mathbb{Z}$ è ciclico ma $\mathbb{Q}$ no.

Esercizio 7.1 $(\mathbb{Q}, +)$ e $(\mathbb{Q}^+, \cdot)$ sono isomorfi?

Capitolo 8

19/03/2014

In questa sezione vorremmo parlare del concetto di **congruenze**, ma prima di definire e studiare questo concetto facciamo alcuni discorsi sulle strutture algebriche in generale.

8.1 Sottogruppi Normali

Teorema 8.1 (di Lagrange) *Siano G un gruppo finito e H un suo sottogruppo. Allora l'ordine di H divide l'ordine di G.*

Dimostrazione. Poniamo in G la relazione di equivalenza

$$x \sim y \quad \iff \quad \exists\, h \in H \text{ tale che } y = hx$$

Per ogni $x \in G$ abbiamo che la sua classe di equivalenza è data da $[x]_\sim = Hx = \{hx \mid h \in H\}$, che chiamiamo *laterale destro di H in G*.

Ogni laterale Hx è equipotente ad H, e $\{Hx \mid x \in G\}$ è una partizione di G in blocchi tutti equipotenti.

Il principio di addizione implica, nel caso finito, che

$$|G| = |H| \cdot [G : H]$$

in cui il simbolo $[G : H]$ indica il numero di laterali distinti di H in G.

□

Definizione 8.1 Dato un gruppo G e un suo sottogruppo H, il numero dei laterali (sinistri o destri) di H in G, indicato con $[G : H]$ è detto *indice di H in G*.

Osservazione Nella dimostrazione avremmo potuto usare allo stesso modo i *laterali sinistri*, definiti dalla relazione

$$x \sim y \quad \iff \quad \exists\, h \in H \text{ tale che } y = xh$$

Ma le due classi laterali Hx e xH sono in generale diverse, visto che il gruppo G potrebbe non essere commutativo.

Definizione 8.2 Se per ogni $x \in G$ si ha $xH = Hx$, H si dice sottogruppo *normale* in G, e si indica con $H \lhd G$.

Esempio 8.1 Il sottogruppo $\{1_G\}$ di un gruppo G è sempre normale in G.

Esempio 8.2 Se per il sottogruppo H di G vale $|H| = \frac{|G|}{2}$ allora $H \lhd G$.
Questo perché preso un $x_0 \notin H$ allora i laterali destri sono H e $Hx_0 \Longrightarrow H_x 0 = G \setminus H$.
I sinistri sono H e $x_0 H \Longrightarrow x_0 H = G \setminus H$.
Quindi $x_0 H = H x_0 = G \setminus H$.

Esempio 8.3 Preso $X = \{1, 2, \ldots, n\}$, $n \geq 2$, e preso $S_n = S_X$ il gruppo simmetrico di X, ogni $\alpha \in S_n$ si può rappresentare con una matrice $M_\alpha = m_{ij}$ dove $m_{ij} = 1$ se $\alpha(i) = j$ e 0 altrimenti.

Dal fatto che α è bigettiva sicuramente in ogni riga e colonna di M_α c'è uno ed un solo 1. Quindi M_α è ortogonale: $M_\alpha^{-1} = M_\alpha^t$, il che implica che il determinante $det(M_\alpha) = \pm 1$.

Le permutazioni α tali che $det(M_\alpha) = 1$ sono dette *pari* e costituiscono il *sottogruppo alterno* A_n di S_n, che ha $\frac{n!}{2} = \frac{|S_n|}{2}$ elementi, quindi è normale: $A_n \lhd S_n$.

Definizione 8.3 Dato un gruppo G, definiamo *centro* di G, indicato $Z(G)$ il sottogruppo

$$Z(G) := \{g \in G \mid gx = xg \ \ \forall x \in G\}$$

Osservazione $Z(G) \lhd G$, $\forall G$.

Osservazione G è abeliano $\Longleftrightarrow Z(G) = G$.

Esempio 8.4 $Z(S_n) = \{id\}$.

Esempio 8.5 $Z(GL_n(\mathbb{K})) = \{kI_n \mid k \in \mathbb{K}^*\}$.

8.2 Congruenze

Siamo ora pronti a dare la definizione principale di questa sezione.

Definizione 8.4 Prendiamo la struttura algebrica $(X, f_1, f_2, \ldots, f_r)$, e una relazione di equivalenza $\sim$ definita su di essa.

Diciamo che $\sim$ è *compatibile* con f_i se vale una delle seguenti proprietà

- $f_i = x_0 \in X$
- f_i è operazione n-aria e verifica

$$\forall x_1, \ldots, x_n, x'_1, \ldots, x'_n \in X,\ x_i \sim x'_i \quad \Longrightarrow \quad f_i(x_1, \ldots, x_n) \sim f_i(x'_1, \ldots, x'_n)$$

La relazione $\sim$ è detta *congruenza* della struttura se è compatibile con ognuna delle operazioni f_i.

Se abbiamo una congruenza $\sim$ definita su $(X, f_1, f_2, \ldots, f_r)$, allora le operazioni f_i si possono trasferire al quoziente $X/_\sim$ ponendo

$$f_i([x_1]_\sim, \ldots, [x_n]_\sim) = [f_i(x_1, \ldots, x_n)]_\sim$$

Allora $X/_\sim$ diventa una struttura dello stesso tipo.

Esempio 8.6 Scriviamo gli elementi di $\mathbb{N} \times \mathbb{N}^+$ non come $(a, b),\ b \neq 0$, ma come $\frac{a}{b}$.

In questo insieme definiamo la relazione

$$\frac{a}{b} \sim \frac{a'}{b'} \Longleftrightarrow ab' = a'b$$

e chiamiamo le classi "razionali assoluti".

A questo punto definiamo le operazioni

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \qquad\qquad \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

che risultano compatibili con $\sim$.

Se avessimo definito

$$\frac{a}{b} + \frac{c}{d} = \frac{a + c}{b + d}$$

questa funzione non sarebbe risultata compatibile con la relazione $\sim$.

In ogni struttura algebrica ci sono sempre due congruenze banali:

- L'identità, in cui ogni elemento è in relazione a sé stesso: $[x]_{id} = \{x\}$.

- Il prodotto cartesiano, in ogni elemento è in relazione con ogni altro elemento dell'insieme: $[x]_{X\times X} = X$.

Può anche accadere che queste siano le sole congruenze possibili. In tal caso la struttura si dice *semplice*.

In un gruppo $(G, \cdot)$ una relazione d'equivalenza $\sim$ è una congruenza se e solo se è compatibile con l'operazione binaria del gruppo, ovvero

$$x \sim x',\ y \sim y' \Longrightarrow x \cdot y \sim x' \cdot y'$$

questo basta perché da questa proprietà si dimostra che $x \sim x' \Longrightarrow x^{-1} \sim x'^{-1}$.

Di più: preso $K = [1_G]_\sim$ è un sottogruppo normale in G e $\forall x \in G$ vale

$$[x]_\sim = Kx (= xK)$$

Non solo, vale anche il viceversa: se $K \lhd G$, allora la relazione

$$x \sim_K y \text{ se } \exists\, k \in K \text{ tale che } y = k \cdot x$$

è una congruenza, di cui K è la classe $[1_G]$ e le altre classi sono i suoi laterali Kx.

Dunque nei gruppi le congruenze sono descritte completamente dai sottogruppi normali.

All'identità è associato il sottogruppo $\{1_G\} \lhd G$ e al prodotto cartesiano è associato il sottogruppo $G \lhd G$.

Corollario *Un gruppo G è semplice se e solo se i suoi sottogruppi normali sono solo $\{1_G\}$ e G.*

Esempio 8.7 In un gruppo abeliano tutti i sottogruppi sono normali. Quindi può essere semplice se e solo se è ciclico di ordine primo, ovvero $G \cong C_p \cong \mathbb{Z}_p$.

Un altro esempio è fornito dal seguente teorema.

Teorema 8.2 (di Galois) *A_n è semplice per ogni $n \geq 5$.*

Passiamo a vedere cosa accade nel caso degli anelli:

Dato l'anello $(A, +, \cdot, 1_A)$, la relazione d'equivalenza $\sim$ è una congruenza se è compatibile con $+$ e $\cdot$:

$$a \sim a',\ b \sim b' \Longrightarrow a + b \sim a' + b' \qquad a \cdot b \sim a' \cdot b'$$

La compatibilità con $+$ ci dice che $\sim$ è una congruenza nel gruppo $(A, +)$, quindi la classe $I = [0_A]$ è un sottogruppo normale e $\forall a \in A\ [a]_\sim = I + a$.

La compatibilità con $\cdot$ ci dice qualcos'altro sul sottogruppo I:

$\forall a \in A, i \in I$ vale $a \sim a$, $i \sim 0_A$ e quindi $a \cdot i \sim a \cdot 0_A = 0_A$, ovvero $a \cdot i \in I$. E lo stesso $i \cdot a \in I$.

Quindi I è un *ideale* (bilatero) di A.

Definizione 8.5 Dato l'anello A, un suo sottoinsieme I si dice *ideale sinistro* se $\forall a \in A$, $\forall i \in I$ vale $a \cdot i \in I$, ovvero $a \cdot I = I \ \forall a \in A$.

Allo stesso modo si definiscono gli *ideali destri* o *bilateri* (se sono sia destri che sinistri).

Viceversa, se I è un ideale di A, la relazione

$$a \sim_I b \text{ se } \exists\, i \in I \text{ tale che } b = i + a$$

è una congruenza dell'anello, nella quale $I = [0_A]$ e le altre classi sono i suoi laterali $I + a$.

Dunque negli anelli le congruenze sono descritte completamente dagli ideali.

Definizione 8.6 Dato un anello commutativo A, l'ideale I è detto *ideale principale* (*generato da* $a \in A$) se è della forma

$$I = (a) := \{ax \mid x \in A\}$$

Proposizione 8.1 *Sia A^* il gruppo degli invertibili dell'anello A, e sia I un ideale di A. Vale la seguente proprietà*

$$I \cap A^* \neq \emptyset \quad \Longrightarrow \quad I = A$$

Dimostrazione. Sia $a \in I \cap A^*$, allora esiste a^{-1} e $1_G = a^{-1} \cdot a \in I$.

Ma allora $\forall x \in A$ abbiamo che $x = x \cdot 1_G \in I$, quindi $I = A$.

□

Esempio 8.8 Sia A un anello commutativo. A è semplice se e solo se A è un campo.

Esempio 8.9 $M_n(\mathbb{K})$, ovvero l'anello delle matrici quadrate di ordine n nel campo $\mathbb{K}$, è un anello semplice.

Teorema 8.3 (Teorema Fondamentale di Omomorfismo) *Siano* $(X, f_1, \ldots, f_r)$ *e* $(Y, g_1, \ldots, g_r)$ *due strutture dello stesso tipo. Preso* $\phi : X \longrightarrow Y$ *un omomorfismo, valgono le seguenti proprietà:*

1. $Im(\phi)$ *è una sottostruttura di* Y*.*
2. *La relazione di equivalenza definita come*

$$x_1 \sim_\phi x_2 \text{ se } \phi(x_1) = \phi(x_2)$$

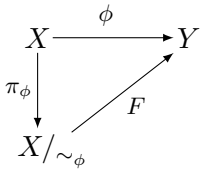
   è una congruenza in X*.*

3. *La proiezione canonica*

$$\begin{array}{rcl} \pi_\phi : X & \longrightarrow & X/_{\sim_\phi} \\ x & \longmapsto & [x]_{\sim_\phi} \end{array}$$

   è un omomorfismo suriettivo.

4. $\exists!\ F : X/_{\sim_\phi} \longrightarrow Y$ *omomorfismo iniettivo tale che* $\phi = F \circ \pi_\phi$*, ovvero il seguente diagramma risulta commutativo:*



Capitolo 9

20/03/2014

9.1 Polinomi, Parte 1

Nel capitolo precedente abbiamo parlato di omomorfismi. Proviamo a pensare ad un caso ben specifico: un morfismo da un insieme X all'anello delle funzioni con dominio e codominio l'insieme stesso, X^X.

L'esempio a cui stiamo pensando in particolare è il seguente

$$\begin{array}{rcl} \phi : \mathbb{R} & \longrightarrow & (\mathbb{R}^{\mathbb{R}}, +, \cdot, id) \end{array}$$

$$\begin{array}{rcl} r & \longmapsto & f = r : \mathbb{R} \longrightarrow \mathbb{R} \\ & & x \longmapsto r \end{array}$$

La funzione ϕ appena definita associa quindi ad ogni reale r la funzione costante $f(x) = r \ \forall x$. Visto che nell'anello $\mathbb{R}^{\mathbb{R}}$ le operazioni tra funzioni le abbiamo definite punto per punto, la funzione ϕ risulta automaticamente un omomorfismo iniettivo.

L'immagine di questo omomorfismo sono tutte le funzioni costanti da $\mathbb{R}$ in $\mathbb{R}$, quindi da ora in poi diremo che un numero reale r può essere interpretato $r \in \mathbb{R}^{\mathbb{R}}$ come la funzione costante $f(x) = r$.

Nell'anello $(\mathbb{R}^{\mathbb{R}}, +, \cdot, id)$ la funzione identità è definita come $id(x) = x \ \forall x$, quindi possiamo indicarla semplicemente con il simbolo "x".

Poniamoci dunque questa domanda: chi è il sottoanello di $\mathbb{R}^{\mathbb{R}}$ generato dalla funzione identità e dalle funzioni costanti? In altre parole, chi è $< \mathbb{R} \cup \{x\} >$?

Questo anello deve contenere

- le costanti;
- le potenze x^n, $\forall n \geq 1$;

- i loro prodotti: ax^n, $\forall n \geq 0$ ($x^0 := 1$);
- le somme finite di questi prodotti:

$$f(x) = \sum_{i=0}^{n} a_i x^i$$

Arrivando quindi alla definizione che ci interessa:

Definizione 9.1 Sono chiamati *polinomi* o *funzioni polinomiali* gli oggetti del tipo

$$f(x) = \sum_{i=0}^{n} a_i x^i$$

L'anello dei polinomi è indicato con il simbolo $\mathbb{R}[x]$.

Infatti si verifica facilmente che i polinomi formano a loro volta un sottoanello di $\mathbb{R}^{\mathbb{R}}$, perché presi due polinomi f e g, anche $f + g$ e $f \cdot g$ sono anch'essi polinomi.

Inoltre dato un polinomio f esiste il suo inverso $-f$ definito come

$$-f(x) = \sum_{i=0}^{n} (-a_i) x^i$$

e l'anello dei polinomi contiene gli elementi neutri di entrambe le operazioni definire nell'anello $\mathbb{R}^{\mathbb{R}}$:

$$0 = 0 + 0 \cdot x + 0 \cdot x^2 + 0 \cdot x^3 + \ldots = \sum_{i=0}^{n} 0 \cdot x^i$$

$$1 = 1 + 0 \cdot x + 0 \cdot x^2 + 0 \cdot x^3 + \ldots = 1 + \sum_{i=1}^{n} 0 \cdot x^i$$

Teorema 9.1 $< \mathbb{R} \cup \{x\} >= \mathbb{R}[x]$.

Dimostrazione. $\boxed{\subseteq}$ Per definizione $< \mathbb{R} \cup \{x\} >$ è il più piccolo sottoanello di $\mathbb{R}^{\mathbb{R}}$ contenente le costanti e la funzione identità x.

Ma esse sono contenute anche in $\mathbb{R}[x]$:

$$r = r + 0 \cdot x + 0 \cdot x^2 + 0 \cdot x^3 + \ldots = r + \sum_{i=1}^{n} 0 \cdot x^i$$

$$x = 0 + 1 \cdot x + 0 \cdot x^2 + 0 \cdot x^3 + \ldots = x + \sum_{i=2}^{n} 0 \cdot x^i$$

quindi quest'inclusione è dimostrata.

$\boxed{\supseteq}$ Abbiamo visto poco fa che $\mathbb{R}[x]$ contiene le costanti reali e l'identità x. Essendo un anello deve contenere anche i loro prodotti e le loro somme finite, che sono contenute anche in $< \mathbb{R} \cup \{x\} >$, quindi anche quest'inclusione è dimostrata.

□

Avendo dimostrato l'uguaglianza di questi due anelli da adesso in poi useremo il simbolo $\mathbb{R}[x]$ per indicare entrambi, senza incorrere in incomprensioni.

Lemma *Sia* $f = \sum_{i=0}^{n} a_i \cdot x^i \in \mathbb{R}[x]$*, allora* $f = 0 \iff a_i = 0 \; \forall i$*.*

Dimostrazione. $\boxed{\Leftarrow}$ Ovviamente se $a_i = 0 \; \forall i$, il polinomio f non può che essere la funzione nulla 0.

$\boxed{\Rightarrow}$ Supponiamo per assurdo che $\exists \, n$ tale che $a_n \neq 0$.
Sappiamo che $f = 0$ per ipotesi, quindi da un lato vale

$$\lim_{x \longrightarrow +\infty} f = \lim_{x \longrightarrow +\infty} 0 = 0$$

D'altra parte se $a_n \neq 0$ abbiamo

$$\lim_{x \longrightarrow +\infty} f = \lim_{x \longrightarrow +\infty} \sum_{i=0}^{n} a_i \cdot x^i =$$

$$= \lim \begin{array}{ccccccccccc} x^n & \Big(& \frac{a_0}{x^n} & + & \frac{a_1}{x^{n-1}} & + & \dots & + & \frac{a_{n-1}}{x} & + & a_n \Big) = \pm\infty \\ \downarrow & & \downarrow & & \downarrow & & & & \downarrow & & \downarrow \\ +\infty & & 0 & & 0 & & & & 0 & & a_n \end{array}$$

in cui il segno $\pm\infty$ dipende dal segno di a_n.

Qualunque sia il segno questi calcoli portano comunque ad un assurdo, che conclude la nostra dimostrazione.

□

Teorema 9.2 (Principio di Identità dei Polinomi) *Presi due polinomi* $f(x) = \sum_{i=0}^{m} a_i \cdot x^i$*,* $g(x) = \sum_{i=0}^{n} b_i \cdot x^i$*, vale* $f =^1 g$ *se e solo se* $a_i = b_i \; \forall i$*.*

Dimostrazione. Essere l'insieme dei polinomi un anello, è definita su di esso l'operazione di sottrazione, vista come somma dell'opposto di uno dei due, quindi esiste il polinomio $f - g$, che è necessariamente definito come

$$\sum_{i=0}^{n} (a_i - b_i) \cdot x^i$$

[1] Questa è un'uguaglianza tra polinomi, che sono in fin dei conti funzioni, quindi $f = g$ vuol dire che $f(x) = g(x) \; \forall x \in \mathbb{R}$.

Dunque abbiamo che $f = g \iff f - g = 0$, e per il lemma dimostrato sopra questo accade se e solo se $(a_i - b_i) = 0 \; \forall i$, ovvero $a_i = b_i \; \forall i$.

□

Come conseguenza di questo importante teorema è possibile definire nell'anello dei polinomi la funzione *grado*, indicata con $deg(\cdot)$, che ad ogni polinomio associa il massimo indice n tale che $a_n \neq 0$:

$$deg(f(x)) = deg\left(\sum_{i=0}^{n} a_i \cdot x^i\right) = n \quad \iff \quad n = \max\{k \in \mathbb{N} \mid a_k \neq 0\}$$

Teorema 9.3 (dei Gradi) *Dati due polinomi f e g, di gradi rispettivamente m ed n, il polinomio $f \cdot g$ ha grado $m \cdot n$.*

Dimostrazione. Se scriviamo i due polinomi nella forma

$$f(x) = \sum_{i=0}^{m} a_i \cdot x^i \qquad\qquad g(x) = \sum_{i=0}^{n} b_i \cdot x^i$$

il polinomio prodotto risulta

$$(f \cdot g)(x) = a_0 b_0 + (a_1 b_0 + a_0 b_1)x + \ldots + a_m b_n x^{m+n}$$

Dunque se $a_m, b_n \neq 0$ necessariamente $a_m b_n \neq 0$, il che implica che il grado di $f \cdot g$ sia proprio $m \cdot n$.

□

Corollario *$\mathbb{R}[x]$ è un dominio di integrità.*

Dimostrazione. Presi due polinomi non nulli f e g, essi avranno gradi m ed n.

Il teorema precedente ci dice che $f \cdot g$ ha grado $m \cdot n$, quindi in particolare non è nullo.

□

Non solo è un dominio, ma sull'anello dei polinomi è anche possibile definire una **divisione euclidea**, ovvero una divisione con resto, proprio come negli insiemi numerici:

Teorema 9.4 *Per ogni $f, g \in \mathbb{R}[x]$, $g \neq 0$, $\quad \exists!\, q, r \in \mathbb{R}[x]$ tali che*

$$f = q \cdot g + r$$

e che valga $r = 0$ oppure $deg(r) < deg(g)$.

Corollario *$\mathbb{R}[x]$ è un* dominio euclideo*, ovvero un dominio di integrità in cui è definita una divisione euclidea.*

Capitolo 10

24/03/2014

10.1 Polinomi, Parte 2

Osservazione I polinomi li abbiamo scritti come

$$f(x) = \sum_{i=0}^{n} a_i x^i$$

Questa scrittura ha due interpretazioni possibili:

1. $a_i \in \mathbb{R}$ fissati, $x \in \mathbb{R}$ variabile
2. a_i funzioni costanti, x funzione identità, quindi

$$f \in < \mathbb{R} \cup \{id_{\mathbb{R}}\} > \subseteq \mathcal{C}^{\infty}_{\mathbb{R}}$$

Una conseguenza diretta del teorema dei gradi è la semplice classificazione degli elementi invertibili dell'anello dei polinomi $\mathbb{R}[x]$:

Proposizione 10.1 $(\mathbb{R}[x])^* = \mathbb{R}^*$

Dimostrazione. Se $f \cdot g = 1$ allora abbiamo che $deg(fg) = deg(1) = 0$, ma $deg(fg) = deg(f) + deg(g)$, quindi l'unica possibilità è che si abbia $deg(f) = deg(g) = 0$.

□

Definizione 10.1 L'anello A si dice *Dominio a Ideali Principali* (abbreviato in *PID*) se ogni ideale è generato da un solo elemento: $I = (a)$, con $I \subseteq A$ ideale e $a \in A$.

Proposizione 10.2 $\mathbb{R}[x]$ *è un PID.*

Dimostrazione. L'ideale nullo è generato da 0, quindi è principale.

Se I è un ideale non nullo esso contiene polinomi non nulli, quindi con grado ≥ 1. Allora l'insieme H dei gradi dei polinomi in I non è vuoto ed è incluso in $\mathbb{N}$.

Per il principio del minimo H ammette minimo m. Sia dunque $g \in I$ un polinomio di grado m.

Allora abbiamo che

$$(g) = \{g \cdot q \mid q \in \mathbb{R}[x]\} \subseteq I$$

Vale però anche l'altra inclusione, infatti $\forall f \in I$, $\exists\, q, r \in \mathbb{R}[x]$ tali che $f = g \cdot q + r$, con $r = 0$ oppure $deg(r) < deg(g) = m$.

Ma $r = f - g \cdot q \in I \implies r = 0$ perché m era il grado minimo dei polinomi in I, e $f = g \cdot q$, il che implica $I \subseteq (g)$.

□

Definizione 10.2 Si dice che $x_0 \in \mathbb{R}$ è *radice* (o *zero*) di $f \in \mathbb{R}[x]$ se $f(x_0) = 0$.

Teorema 10.1 (del Resto) *Presi $x_0 \in \mathbb{R}$ e $f \in \mathbb{R}[x]$, è possibile scrivere*

$$f(x) = (x - x_0)q(x) + f(x_0)$$

Dimostrazione. Sappiamo di poter fare la divisione euclidea e scrivere

$$f(x) = (x - x_0)q(x) + r$$

Dunque posto $x = x_0$ si ha $f(x_0) = r$.

□

Corollario *x_0 è radice di $f \iff f(x) = (x - x_0)q(x)$.*

Definizione 10.3 Preso x_0 radice di f sappiamo di poter scrivere

$$f(x) = (x - x_0)q(x)$$

x_0 si dice radice *semplice* di f se $q(x_0) \neq 0$. Altrimenti, se $q(x_0) = 0$, x_0 si dice radice *multipla* di f.

Se la radice è multipla possiamo scrivere $f(x) = (x - x_0)^m \overline{q}(x)$, con $\overline{q}(x_0) \neq 0$, e chiamiamo m la *molteplicità* della radice x_0.

Teorema 10.2 *Sia $f \in \mathbb{R}[x]$ di grado $n \geq 1$ e siano $x_1, \ldots, x_r$ le radici distinte con molteplicità $k_1, \ldots, k_r$ rispettivamente. Possiamo quindi scrivere*

$$f(x) = (x - x_1)^{k_1}(x - x_2)^{k_2} \cdots (x - x_r)^{k_r} \cdot \overline{q}(x)$$

con $\overline{q}(x_i) \neq 0 \ \forall i$, e vale

$$\sum_{i=1}^{r} k_i \leq n$$

Teorema 10.3 *Sia f un polinomio di grado dispari. Allora f ha almeno una radice.*

Dimostrazione. Visto che il grado è dispari valgono i seguenti limiti

$$\lim_{x \longrightarrow -\infty} f(x) = (-\infty) \cdot sgn(a_n) \qquad \lim_{x \longrightarrow +\infty} f(x) = (+\infty) \cdot sgn(a_n)$$

Quindi $Im(f) =]-\infty, +\infty[= \mathbb{R}$, ed essendo f una funzione continua $\exists\, x_0 \in \mathbb{R}$ tale che $f(x_0) = 0$.

□

Esercizio 10.1 In quali casi un polinomio $f : \mathbb{R} \longrightarrow \mathbb{R}$ è

1. una funzione suriettiva
2. una funzione iniettiva
3. una funzione bigettiva

Svolgimento:

1. Abbiamo dimostrato poco fa che un polinomio di grado dispari è una funzione suriettiva.

   D'altra parte se il polinomio f è di grado pari non può essere una funzione suriettiva, perché:

   (supponiamo che $a_n > 0$)

   - Se f non ha radici allora $f(x) > 0 \ \forall x$
   - Se f ha delle radici $x_1 < x_2 < \ldots < x_r$ allora restringendo f all'intervallo $[x_1, x_r]$ per il teorema di Weierstrass f ha minimo m, da cui

     $$Im(f) \subseteq [m, +\infty[\neq \mathbb{R}$$

2. Escludiamo innanzitutto le funzioni con più di una radice.

   Inoltre con un ragionamento simile a quanto fatto nel caso precedente, che quindi non ripetiamo, possiamo escludere tutti i polinomi f con grado pari.

   Per escludere gli altri casi problematici usiamo il seguente risultato:

Lemma *$f \in \mathbb{R}[x]$ ha una radice x_0 di molteplicità $k > 1 \iff x_0$ è radice di f'.*
Se $k > 2$, x_0 è radice anche di $f'', \ldots, f^{(k)}$.

Inoltre, dal teorema del valor medio, sappiamo che se su un intervallo si ha $f'(x) > 0 \; \forall x$ allora f è crescente, mentre se $f'(x) < 0 \; \forall x$ allora f è decrescente.

Da questo fatto possiamo dire che se f ha un punto di massimo o minimo relativo allora la funzione f non è iniettiva.

Allora se x_0 è radice di f', può essere solo un punto di flesso, quindi di molteplicità pari per f'.

$$f'(x) = (x - x_1)^{2k_1}(x - x_2)^{2k_2} \cdots (x - x_r)^{2k_r} \cdot q(x)$$

con $q(x)$ privo di zeri.

Allora, dato che f ha grado dispari, f' ha grado pari, dunque q ha grado pari, il che implica che q ha segno costante.

Quindi i polinomi iniettivi sono le possibili primitive della funzione f' scritta sopra.

3. L'intersezione dell'insieme dei polinomi iniettivi con quello dei polinomi suriettivi ci fornisce la risposta, quindi l'abbiamo già trovata con i punti precedenti.

□

Capitolo 11

26/03/2014

11.1 Divisibilità

Prima di definire i due concetti base di questo capitolo introduciamo una relazione tra gli elementi di un anello commutativo qualsiasi.

Definizione 11.1 Sia A un anello commutativo. Siano $a, b \in A$. Diciamo che a *divide* b, indicato con $a|b$, se $\exists\, q \in A$ tale che $b = a \cdot q$.

Enunciamo le proprietà di questa relazione omettendo le dimostrazioni piuttosto semplici:

- $a|a$ (Proprietà *Riflessiva*)
- $a|b$, $b|c \implies a|c$ (Proprietà *Transitiva*)
- $a|b$, $a|c \implies a|(b + c)$
- $a|b \implies a|(b \cdot c) \quad \forall c$
- $a|0_A \quad \forall a$
- $0_A|b \iff b = 0_A$
- $1_A|a \quad \forall a$
- $u|1_A \quad \forall u \in A^*$
- $u \in A^* \implies u|a \quad \forall a$
- $\forall a, b \quad a|b \iff b \in (a) \iff (b) \subseteq (a)$

Definizione 11.2 Chiamiamo *associati* due elementi $a, a' \in A$ tali che $a|a'$ e $a'|a$, e li indichiamo con $a \sim a'$.

Questa è una relazione di equivalenza in A (quindi rispetta le proprietà riflessiva, transitiva e antisimmetrica). Studiamo anche le proprietà di quest'altra relazione:

- $[0_A]_\sim = \{0_A\}$
- $[1_A]_\sim = A*$
- è compatibile con l'operazione "$\cdot$": $a \sim a'$, $b \sim b' \Longrightarrow a \cdot b \sim a' \cdot b'$
- non è compatibile con l'operazione "+" (possiamo trovare molti controesempi)
- è compatibile con "$|$"

  Possiamo quindi definire nell'anello quoziente $A/_\sim$ la relazione "$[a]_\sim \Big| [b]_\sim$ se $a|b$", che risulta ben posta.

  Non solo, ma risulta essere anche una relazione d'ordine, con i seguenti estremi: $\min(A/_\sim) = [1_A]_\sim$ e $\max(A/_\sim) = [0_A]_\sim$.
- Se A è un dominio vale $a \sim a' \Longleftrightarrow \exists\, u \in A^*$ tale che $a' = a \cdot u$
- $a \sim a' \Longleftrightarrow (a) = (a')$

11.2 MCD e mcm

Adesso che abbiamo definito la relazione di divisore nell'anello A siamo pronti per ciò che volevamo enunciare.

Definizione 11.3 Sia A un anello commutativo e siano $a, b \in A$. Un elemento $c \in A$ si dice *divisore comune* di a e b se $c|a$ e $c|b$.

c si dice inoltre *massimo comun divisore* (o *MCD*) se c divide ogni altro divisore comune di a e b.

Osservazione Se c è un MCD per a e b e $c' \sim c$ (associato), allora anche c' è un MCD per a e b.

Dunque in particolare in un anello con elementi invertibili l'MCD non è unico!

Definizione 11.4 Sia A un anello commutativo e siano $a, b \in A$. Un elemento $d \in A$ si dice *multiplo comune* di a e b se $a|d$ e $b|d$.

d si dice inoltre *minimo comune multiplo* (o *mcm*) se d divide ogni altro multiplo comune di a e b.

Teorema 11.1 *Se A è un PID, ogni coppia di elementi in A ammette MCD e mcm.*

Dimostrazione. Presi $a, b \in A$, ricordando che A è un PID, quindi ogni ideale di A deve ammettere un generatore, otteniamo che:

- $MCD(a, b)$ è il generatore dell'ideale $(a) + (b) = \{ax + by \mid x, y \in A\}$.
- $mcm(a, b)$ è il generatore dell'ideale $(a) \cap (b)$.

□

Corollario (Identità di Bezout) *Se A è un PID, allora $\forall a, b \in A \; \exists\, u, v \in A$ tali che*

$$au + bv = MCD(a, b)$$

Osservazione Preso $d = MCD(a, b)$, se scriviamo i due elementi come $a = da', b = db'$ risulterà necessariamente $MCD(a', b') = 1$.

Proposizione 11.1 *$\forall a, b \in A$ vale*

$$mcm(a, b) \cdot MCD(a, b) = a \cdot b$$

Osservazione Se A è un PID, $(A/_\sim, |)$ è un reticolo, in cui $\sup(a, b) = mcm$, $\inf(a, b) = MCD(a, b)$.

Teorema 11.2 (Lemma di Euclide) *Preso A PID, $\forall a, b, c \in A$ vale*

$$\left.\begin{array}{c} a|bc \\ MCD(a, b) = 1_A \end{array}\right\} \Longrightarrow a|c$$

Dimostrazione. Diciamo che $bc = aq$.
$MCD(a, b) = 1_A \Longrightarrow \exists\, u, v \in A$ tali che $au + bv = 1_A$.
Allora $a(cu) + bcv = c \Longrightarrow a(cu) + aqv = c \Longrightarrow a(cu + qv) = c$

□

$\mathbb{R}[x]$ è un dominio euclideo, quindi per trovare il MCD di due polinomi a e b si può usare il procedimento euclideo delle divisioni successive, basato sulla divisione euclidea definita nel capitolo precedente:

- $a = bq_0 + r_0$, con $r = 0$ oppure $deg(r) < deg(b)$.

  Se $r_0 = 0 \Longrightarrow b = MCD(a, b)$.

  Se $r_0 \neq 0 \Longrightarrow MCD(a, b) = MCD(b, r_0)$ e il procedimento continua.

- $b = r_0 q_1 + r_1$

  Se $r_1 = 0 \Longrightarrow r_0 = MCD(b, r_0) = MCD(a, b)$.

  Se $r_0 \neq 0 \Longrightarrow MCD(r_0, r_1) = MCD(b, r_0) = MCD(a, b)$ e il procedimento continua.

- $r_0 = r_1 q_2 + r_2$

  Se $r_2 = 0 \Longrightarrow r_1 = MCD(r_0, r_1) = MCD(b, r_0) = MCD(a, b)$.

  Se $r_0 \neq 0 \Longrightarrow MCD(r_1, r_2) = MCD(r_0, r_1) = MCD(b, r_0) = MCD(a, b)$ e il procedimento continua.

  $\vdots$

Ad un certo punto si avrà un resto $r_{n+1} = 0$ perché i gradi ad ogni passo calano.

Allora abbiamo $r_n \neq 0$, che implica $r_n = MCD(r_{n-1}, r_n) = MCD(r_{n-2}, r_{n-1}) = \ldots = MCD(a, b)$.

Capitolo 12

31/03/2014

12.1 Elementi Primi e/o Irriducibili

Nell'insieme dei numeri interi un numero si dice *primo* se è divisibile solo per 1 e per sé stesso. Quello che faremo in questo paragrafo è estendere questa semplice definizione intuitiva ad un anello qualsiasi, ma dobbiamo prima fare una distinzione che tra i numeri non si riesce a cogliere.

Definizione 12.1 Sia A un anello commutativo. Un elemento $a \in A$, $a \neq 0_A$, $a \notin A^*$ è detto *irriducibile* (o *indecomponibile*) se $\forall b, c \in A$ vale

$$a = b \cdot c \quad \Longrightarrow \quad b \in A^* \text{ oppure } c \in A^*$$

Definizione 12.2 Sia A un anello commutativo. Un elemento $p \in A$, $p \neq 0_A$, $p \notin A^*$ si dice *primo* se $\forall b, c \in A$ vale

$$p|bc \quad \Longrightarrow \quad p|b \text{ oppure } p|c$$

Queste due definizioni combaciano in $\mathbb{Z}$, ma in un anello qualsiasi sono ben distinte, seppur sempre strettamente collegate.

Proposizione 12.1 *p primo $\Longrightarrow$ p irriducibile.*

Dimostrazione. Se $p = a \cdot b$ abbiamo che $p|ab$. Ma p è primo per ipotesi, quindi $p|a$ oppure $p|b$.

Allo stesso tempo, dalla relazione $p = ab$ ricaviamo che $a|p$ e $b|p$, quindi

- se $p|a$ allora $p \sim a$ e $b \sim 1_A$
- se $p|b$ allora $p \sim b$ e $a \sim 1_A$

quindi p è irriducibile.

□

Osservazione p irriducibile $\not\Rightarrow$ p primo.

Controesempio: nell'anello $\mathbb{Z}[i\sqrt{5}]$ gli elementi $\{2, 3, 1+i\sqrt{5}, 1-i\sqrt{5}\}$ risultano irriducibili, ma $2 \cdot 3 = 6 = (1+i\sqrt{5}) \cdot (1-i\sqrt{5})$, quindi nessuno di questi numeri è primo.

Proposizione 12.2 *Se A è un PID, allora p irriducibile $\Longrightarrow$ p primo.*

Dimostrazione. Supponiamo che si abbia $p|ab$ e $p \not| a$.

Visto che p divide il prodotto ab sappiamo che $\exists\, q$ tale che $pq = ab$.

Inoltre, se p non divide a allora $MCD(a, p) = 1_A$, quindi possiamo applicare l'identità di Bezout ed ottenere che $\exists\, u, v \in A$ tali che $1 = pu + av$, che possiamo riscrivere come

$$b = pbu + abv = pbu + pqv = p(bu + qv)$$

$$\Longrightarrow \quad p|b$$

dimostrando così che p è primo.

□

Corollario *In un PID p indecomponibile $\Longleftrightarrow$ p primo.*

Ma allora se le due nozioni di elemento primo e irriducibile sono equivalenti, in un PID avremo una fattorizzazione unica proprio come accadeva in $\mathbb{Z}$!

Teorema 12.1 (Fattorizzazione Unica) *Preso A PID, $\forall a \in A$, $a \notin A^*$, vale una delle seguenti proprietà:*

1. *a è irriducibile*
2. *a è scrivibile come prodotto di un numero finito di fattori irriducibili in maniera unica a meno di elementi invertibili.*

Osservazione Visto che anche $\mathbb{R}[x]$ è un PID, il teorema di fattorizzazione vale anche al suo interno. Questo ci dice che ogni polinomio può essere scritto come prodotto di polinomi irriducibili in maniera unica, a meno di costanti moltiplicative.

Esercizio 12.1 Chi sono gli elementi irriducibili di $\mathbb{R}[x]$?

Per poter rispondere a questa domanda, dovremo definire una nuova struttura algebrica.

12.2 Numeri Complessi

Definizione 12.3 Preso un anello A, un suo ideale I è detto *massimale* se $I \neq A$ e $\forall J$ ideale di A tale che $I \subseteq J \subseteq A$ vale $I = J$ oppure $J = A$.

Se prendiamo un ideale massimale I dell'anello A, l'anello quoziente $A/_I$ non ha ideali propri, quindi è un campo i cui elementi sono i laterali del tipo $a + I$.

Se l'anello di partenza A è un PID, l'ideale I si deve poter scrivere come $I = (p)$. In questo caso si ha che I è massimale $\iff p$ è primo $\iff p$ è irriducibile.

D'altra parte p primo $\implies A/_{(p)}$ è un campo.

Allora se prendiamo $A = \mathbb{R}[x]$, $p = x^2 + 1$, il quoziente $\mathbb{R}[x]/_{(x^2+i)} := \mathbb{C}$ risulta un campo che chiamiamo **Campo Complesso**, o **Campo dei Numeri Complessi**.

Capitolo 13

02/04/2014

13.1 Funzioni di $\mathbb{C}$.

Dato $\mathbb{C}$ il campo complesso, possiamo definire l'anello $(\mathbb{C}^{\mathbb{C}}, +, \cdot, 1)$ delle funzioni con operazioni definite punto per punto.

Questo anello ha molti sottoanelli di notevole importanza. Uno dei più importanti, dopo quello delle *funzioni olomorfe*, è sicuramente l'anello delle *funzioni polinomiali*, ovvero funzioni del tipo

$$f(z) = \sum_{k=0}^{n} \alpha_k z^k$$

in cui $\alpha_k \in \mathbb{C}$ e $z = x + iy$ è una variabile complessa, formano il sottoanello $\mathbb{C}[z]$, che è un sottoanello dell'anello delle funzioni olomorfe.

Per queste funzioni vale il **Principio di identità**: se $\alpha_k = a_k + ib_k$ vale

$$f(z) = \sum_{k=0}^{n} \alpha_k z^k = \sum_{k=0}^{n} a_k z^k + i \sum_{k=0}^{n} b_k z^k$$

Osservazione $f(z) \equiv 0 \iff \alpha_k = 0 \; \forall k$

Inoltre vale anche il teorema dei gradi esattamente come enunciato su $\mathbb{R}[x]$, quindi $\mathbb{C}[z]$ è un dominio euclideo, e di conseguenza anche un PID.

Questo anello di funzioni è molto interessante perché riporta con sé notevoli risultati.

Teorema 13.1 (Teorema Fondamentale dell'Algebra) *Ogni polinomio $f \in \mathbb{C}[x]$ di grado ≥ 1, ha in $\mathbb{C}$ almeno una radice*[1]*.*

Teorema 13.2 (di Liouville) *Se f è olomorfa su $\mathbb{C}$ ed è limitata, allora è costante.*

[1] Il Teorema Fondamentale dell'Algebra si può enunciare più concisamente dicendo che "$\mathbb{C}$ è algebricamente chiuso".

Corollario *Se f è un polinomio di grado ≥ 1 privo di radici, anche $\frac{1}{f}$ è una funzione olomorfa.*

Corollario *Ogni polinomio in $\mathbb{C}[z]$ di grado > 1 è fattorizzabile.*
Ovvero i soli polinomi irriducibili sono quelli di primo grado.

13.2 Endomorfismi ed automorfismi di una struttura algebrica.

Definizione 13.1 Gli omomorfismo da una struttura $(X, f_1, \ldots, f_r)$ in sé stessa sono detti *endomorfismi.*

Osservazione Poiché la composizione di endomorfismi dà endomorfismi, allora l'insieme $End(X)$ degli endomorfismi costituisce un sottomonoide del monoide $(X^X, \circ, id_X)$.

Definizione 13.2 Gli elementi invertibili di $End(X)$ sono detti *automorfismi*, e formano un gruppo, denotato con $Aut(X)$.

Osservazione $Aut(X) = End(X) \cap S_X$.

Facciamo alcuni esempi di gruppi di automorfismi:

- $Aut(\mathbb{Z}, +)$: contiene soltanto l'identità e la funzione degli opposti.

  Infatti, posto $m = f(1)$, con $f \in Aut(\mathbb{Z}, +)$, allora $f(\mathbb{Z}) = m\mathbb{Z}$. Poiché f è suriettiva si deve avere $m\mathbb{Z} = \mathbb{Z}$, e ciò si verifica se e solo se $m = \pm 1$.

  Allora se $m = 1 \Longrightarrow f = id_{\mathbb{Z}}$, mentre se $m = -1 \Longrightarrow f = -id_{\mathbb{Z}}$.

- $Aut(\mathbb{Z}, +, \cdot, 1)$: se $f \in Aut(\mathbb{Z}, +, \cdot, 1) \Longrightarrow f \in Aut(\mathbb{Z}, +) \Longrightarrow f(x) = \pm x$.

  Ma se f è un automorfismo di anelli deve valere $f(1) = 1$, quindi l'unica possibilità è che $f = id_{\mathbb{Z}}$.

- $Aut(\mathbb{Q}, +, \cdot)$: preso $f \in Aut(\mathbb{Q}, +, \cdot)$ vediamo dove manda i razionali

$$f\left(\frac{m}{n}\right) = \frac{f(m)}{f(n)} = \frac{m}{n} \Longrightarrow f = id_{\mathbb{Q}}$$

- $Aut(\mathbb{R}, +, \cdot)$: preso f automorfismo, sappiamo già che $f\big|_{\mathbb{Q}} = id$.

  $\forall y > 0$ sappiamo che $\exists\, x \in \mathbb{R}$ tale che $y = x^2$, dunque $f(y) = f(x^2) = f(x)^2 > 0$. Ma allora f è crescente, perché presi $x_1 < x_2 \in \mathbb{R}$ vale

$$x_2 - x_1 > 0 \Longrightarrow 0 < f(x_2 - x_1) = f(x_2) - f(x_1) \Longrightarrow f(x_1) < f(x_2)$$

Se prendiamo $x_0 \in \mathbb{R} \setminus \mathbb{Q}$ abbiamo $\forall r, s \in \mathbb{Q}$ tali che $r < x_0 < s$ vale

$$r = f(r) < f(x_0) < f(s) = s$$

quindi x_0 e $f(x_0)$ separano gli stessi due insiemi contigui $\{r \in \mathbb{Q} \mid r < x_0\}$, $\{s \in \mathbb{Q} \mid x_0 < s\}$, quindi $f(x_0) = x_0$, ovvero $f = id_{\mathbb{R}}$.

- $Aut(\mathbb{C})$: se $Aut(\mathbb{Z}) = Aut(\mathbb{Q}) = Aut(\mathbb{R}) = \{id\}$, sarà anche $Aut(\mathbb{C}) = \{id\}$?

  In realtà no, poiché il *coniugio*, ovvero la funzione che a $z = x + iy$ associa $\overline{z} = x - iy$, è un automorfismo.

  Infatti $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$, $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$, quindi esso mantiene le operazioni, e inoltre $\overline{\overline{z}} = z$, quindi è bigettivo.

  C'è anche una interessante curiosità: il coniugio è l'<u>unico</u> automorfismo che lascia invariato il sottoinsieme $\mathbb{R}$.

Capitolo 14

03/04/2014

14.1 Polinomi Irriducibili di $\mathbb{R}[x]$

Qualche lezione fa ci eravamo posti la domanda di quali fossero i polinomi irriducibili di $\mathbb{R}[x]$, senza poi arrivare alla risposta. Adesso enunciamola e dimostriamola:

Teorema 14.1 *I soli polinomi irriducibili in* $\mathbb{R}[x]$ *sono quelli di* $1°$ *grado e quelli di* $2°$ *grado con discriminante* $\Delta < 0$.

Dimostrazione. Ogni polinomio reale $f \in \mathbb{R}[x]$ può chiaramente essere visto come polinomio complesso $f \in \mathbb{C}[z]$, ma con coefficienti reali:

$$f(z) = \sum_{k=0}^{n} a_k z^k, \qquad a_k \in \mathbb{R}$$

Se prendiamo una sua radice $\alpha = a + ib$, con $b \neq 0$, vale che

$$0 = f(\alpha) = \sum_{k=0}^{n} a_k \alpha^k$$

Sapendo che $0 = \overline{0}$, possiamo ricavare

$$0 = \overline{0} = \overline{f(\alpha)} = \overline{\sum_{k=0}^{n} a_k \alpha^k} = \sum_{k=0}^{n} a_k \overline{\alpha}^k = f(\overline{\alpha})$$

perciò anche $\overline{\alpha}$ è una radice di f.

Allora f si può scrivere come prodotto di

$$f(z) = (z - \alpha)(z - \overline{\alpha})q(z) \qquad \text{con } deg(q) = deg(f) - 2$$

Dalle proprietà del coniugato scopriamo che

$$\left.\begin{array}{l}\alpha = a + ib \\ \overline{\alpha} = a - ib\end{array}\right\} \Longrightarrow \alpha\overline{\alpha} = a^2 + b^2 \qquad \alpha + \overline{\alpha} = 2a$$

quindi possiamo calcolare

$$(z - \alpha)(z - \overline{\alpha}) = z^2 - 2az + (a^2 + b^2)$$

che deve quindi essere un polinomio di secondo grado a coefficienti reali con discriminante $\Delta < 0$.

Restringendo f ad $\mathbb{R}$, avremo allora

$$f(x) = (x^2 - 2ax + (a^2 + b^2))q(x)$$

La conclusione di questo ragionamento è che ogni polinomio a coefficienti reali, di grado ≥ 1, di scompone nel prodotto di fattori di I grado (corrispondenti alle radici reali) e di fattori di II grado con $\Delta < 0$ (corrispondenti alle radici complesse), che equivale alla tesi da dimostrare.

□

14.2 Polinomi Irriducibili di $\mathbb{Q}[x]$

Prendiamo ora $f \in \mathbb{Q}[x]$, ovvero

$$f(x) = \sum_{k=0}^{n} \frac{a_k}{b_k} x^k \qquad \text{con } MCD(a_k, b_k) = 1$$

se chiamiamo $m = mcm(b_1, b_2, \ldots, b_n)$ possiamo riscrivere

$$f(x) = \sum_{k=0}^{n} \frac{a_k}{b_k} x^k = \frac{1}{m} \cdot \sum_{k=0}^{n} c_k x^k \in \mathbb{Z}[x]$$

Detto ora $d = MCD(c_1, c_2, \ldots, c_n)$, possiamo scomporre nuovamente

$$f(x) = \frac{1}{m} \cdot \sum_{k=0}^{n} c_k x^k = \frac{d}{m} \cdot \sum_{k=0}^{n} q_k x^k = g(x)$$

ottenendo un polinomio $g(x) \in \mathbb{Z}[x]$ con coefficienti coprimi tra loro.

Definizione 14.1 Il polinomio $g(x) = \frac{m}{d} f(x)$ costruito come sopra è detto "polinomio *primitivo* associato ad f".

Se supponiamo positivo il coefficiente di testa di g[1], allora il polinomio primitivo associato ad f è unico.

$$g(x) = \sum_{k=0}^{n} a_k x^k, \qquad a_k \in \mathbb{Z},\ a_n > 0$$

Proposizione 14.1 *f e g hanno le stesse radici e gli stessi divisori.*

Questa proposizione ci assicura che è sufficiente studiare i polinomi primitivi, ovvero quelli con coefficienti tutti coprimi, per aver studiato tutti i polinomi razionali.

Proposizione 14.2 *Le radici razionali di g sono tutte della forma $\frac{p}{q}$, dove $p|a_0$ e $q|a_n$, $q > 0$.*

Proposizione 14.3 (Criterio di Irriducibilità di Eisenstein) *Dato il polinomio primitivo $g(x) = a_n x^n + \ldots + a_1 x + a_0$, se $\exists p$ primo tale che $p|a_i$ $\forall 0 \leq i \leq n-1$, ma $p^2 \nmid a_0$, allora il polinomio è irriducibile.*

Esempio 14.1 $\forall n \geq 1$ il polinomio $x^n - 2$ è irriducibile poiché 2 divide tutti i polinomi, ma $2^2 = 4$ non divide il termine noto $a_0 = 2$.

Osservazione Il criterio di Eisenstein non è prescrittivo, infatti esistono polinomio che non lo soddisfano ma che sono comunque irriducibili in $\mathbb{Q}[x]$, ad esempio x^2+1 o x^2-2x+4.

14.3 Polinomi Irriducibili di $\mathbb{C}[z]$

Teorema 14.2 *In $\mathbb{C}[z]$ ogni polinomio di grado > 1 è riducibile.*

Dimostrazione. Sia $f \in \mathbb{C}[z]$. Sappiamo che f ha una radice multipla α se e solo se α è radice anche della derivata $f'(z)$. Dunque $z - \alpha$ divide sia f sia f', quindi divide $MCD(f, f')$.

Se α ha molteplicità $m > 1$ come radice di f, allora ha molteplicità $m - 1$ come radice di f', e quindi di $d = MCD(f, f')$.

Pertanto $g = \frac{f}{d}$ ha α come radice semplice. Ciò vale per ogni radice di f.

Dunque, g ha le stesse radici di f, ma tutte semplici.

In particolare, $f = d \cdot g$, quindi f è riducibile.

□

[1]Questo si può sempre fare, basta che in uno dei passaggi in cui si raccogli un MCD o un mcm lo si raccolga col segno che ci serve.

Capitolo 15

07/04/2014

15.1 Polinomi in n Variabili

I *polinomi in n variabili* sono particolari elementi dell'anello commutativo delle funzioni $f : \mathbb{R}^n \longrightarrow \mathbb{R}$.

Tra queste funzioni da $\mathbb{R}^n$ ad $\mathbb{R}$, chiamiamo *i-esima proiezione* la funzione definita come $x_i(r_1, \ldots, r_n) := r_i$.

Ci sono anche le funzioni costanti, che possiamo identificare con gli elementi di $\mathbb{R}$.

Proviamo ad analizzare quindi il sottoanello generato dalle funzioni costanti e le n proiezioni, indicato con $< \mathbb{R}, x_1, \ldots, x_n >$: esso contiene le costanti, le proiezioni, i loro prodotto e le loro potenze. Quindi contiene elementi del tipo $r \cdot x_1^{k_1} \cdots x_n^{k_n}$, con $r \in \mathbb{R}$ e $k_i \geq 0$, ovvero contiene i *monomi*.

Inoltre contiene anche tutte le possibili somme di questi ultimi, quindi contiene tutte le funzioni che diremo "*polinomiali*", o *polinomi*.

Se identifichiamo l'insieme dei polinomi con $\mathbb{R}[x_1, \ldots, x_n]$, abbiamo appena dimostrato che $\mathbb{R}[x_1, \ldots, x_n] \subseteq < \mathbb{R} \cup \{x_1, \ldots, x_n\} >$.

D'altra parte lo stesso $\mathbb{R}[x_1, \ldots, x_n]$ è un sottoanello delle funzioni da $\mathbb{R}^n$ ad $\mathbb{R}$ contenente le costanti e le proiezioni, quindi

$$\Longrightarrow \qquad \mathbb{R}[x_1, \ldots, x_n] = < \mathbb{R} \cup \{x_1, \ldots, x_n\} >$$

Ora che abbiamo identificato l'anello dei polinomi, vediamone alcune caratteristiche.

Definizione 15.1 Due monomi $ax_1^{k_1} \cdots x_n^{k_n}$, $bx_1^{h_1} \cdots x_n^{h_n}$ si dicono *simili* se $k_i = h_i \; \forall i$.

Due monomi simili all'interno di uno stesso polinomio si possono "ridurre", ovvero scrivere nella forma

$$a\,x_1^{l_1}\cdots x_n^{l_n} + b\,x_1^{l_1}\cdots x_n^{l_n} = (a+b)x_1^{l_1}\cdots x_n^{l_n}$$

Definizione 15.2 Un polinomio privo di monomi simili si dice *ridotto*.

Grazie a questa piccola precisazione possiamo dimostrare un importantissimo risultato sui polinomi:

Teorema 15.1 (Principio di Identità) *Due polinomi ridotti sono uguali come funzioni se e solo se sono somma degli stessi monomi.*

Dimostrazione. Dimostriamolo per induzione su n:

$\boxed{n=1}$ Siamo nel caso dei polinomi in una variabile, $\mathbb{R}[x]$, in cui abbiamo già dimostrato questo teorema nei capitoli precedenti.

$\boxed{n \Rightarrow n+1}$ Poniamo $y := (x_1, \ldots, x_n)$, $x := x_{n+1}$.

Con questa notazione un polinomio $f \in \mathbb{R}[x_1, \ldots, x_{n+1}] = \mathbb{R}[y, x]$ può essere visto nella forma

$$f = f_0(y) + f_1(y)x + \ldots + f_r(y)x^r \in (\mathbb{R}[y])\,[x]$$

per cui f è nullo se e solo se $f_i(y) = 0\ \forall i,\ \forall y \in \mathbb{R}^n$.

Ma i polinomi f_i sono polinomi in $\mathbb{R}[y] \simeq \mathbb{R}[x_1, \ldots, x_n]$, per cui vale l'ipotesi induttiva, ovvero che f_i è nullo se e solo se sono nulli tutti i suoi coefficienti.

Perciò anche f è nullo se e solo se tutti i suoi coefficienti (che sono le componenti dei singoli f_i) sono nulli, il che completa la dimostrazione.

□

Definizione 15.3 Chiamiamo *grado* di un monomio, indicato con $deg(\cdot)$, la somma degli esponenti delle x_i:

$$deg\left(a\,x_1^{k_1}\cdots x_n^{k_n}\right) = \sum_{i=1}^{n} k_i$$

Teorema 15.2 (dei Gradi) *Il grado del prodotto di due monomi non nulli è uguale alla somma dei loro gradi*

$$deg\left(\left(a\,x_1^{k_1}\cdots x_n^{k_n}\right)\cdot\left(b\,x_1^{h_1}\cdots x_n^{h_n}\right)\right) = deg\left(a\,x_1^{k_1}\cdots x_n^{k_n}\right) + deg\left(b\,x_1^{h_1}\cdots x_n^{h_n}\right)$$

Definizione 15.4 Il *grado* di un polinomio è uguale al massimo dei gradi dei suoi monomi.

Proposizione 15.1 *$\mathbb{R}[x_1, \ldots, x_n]$ è un dominio di integrità per ogni n.*

Osservazione Per $n \geq 2$ l'anello $\mathbb{R}[x_1, \ldots, x_n]$ non è un PID (quindi nemmeno un dominio euclideo).

Proposizione 15.2 $\mathbb{R}[x, y]$ *è un* dominio a fattorizzazione unica *(UFD).*

Definizione 15.5 Un polinomio si dice *omogeneo* se tutti i suoi monomi hanno lo stesso grado.

15.2 Polinomi Simmetrici

Preso un polinomio $f \in \mathbb{R}[x_1, \ldots, x_n]$, possiamo considerare l'azione su di esso di un elemento α del gruppo delle permutazioni di n elementi, S_n, definita come

$$\alpha\left(f(x_1, \ldots, x_n)\right) := f\left(x_{\alpha(1)}, \ldots, x_{\alpha(n)}\right)$$

Se $\alpha(f) = f$ allora il polinomio si dice *stabilizzato da* α, mentre α si dice che *stabilizza* f.

Non finisce qui: l'insieme degli α che stabilizzano un polinomio f forma un sottogruppo di S_n chiamato *sottogruppo degli stabilizzatori di* f. Se per un determinato polinomio f questo sottogruppo risulta essere tutto S_n, il polinomio si dice allora *simmetrico.*

Esempio 15.1 Nel caso $n = 2$ alcuni dei polinomi simmetrici sono

$$x_1 + x_2 \qquad x_1 x_2 \qquad x_1^2 + x_2^2 \qquad \left(x_1^2 + x_2^2\right)^2 \qquad \ldots$$

mentre per $n = 3$ possiamo avere

$$x_1 + x_2 + x_3 \qquad x_1 x_2 + x_1 x_3 + x_2 x_3 \qquad x_1 x_2 x_3 \qquad \ldots$$

questi ultimi esempi presi per il caso $n = 3$ sono detti polinomi *elementari in 3 variabili.*

Osservazione Sia $f \in \mathbb{C}[z]$ con $deg(f) = n \geq 2$, e siano $\alpha_1, \ldots, \alpha_n$ le sue radici.

Sappiamo già di poter scrivere $f(z) = (z - \alpha_1) \cdots (z - \alpha_n)$, ma possiamo fare di più: si dimostra che è possibile scrivere f nella forma

$$f(x) = z^n + (\alpha_1 + \ldots + \alpha_n) z^{n-1} + (\alpha_1 \alpha_2 + \alpha_1 \alpha_3 \ldots + \alpha_1 \alpha_n) z^{n-2} + \ldots + (-1)^n \alpha_1 \cdots \alpha_n$$

ovvero in cui i coefficienti del polinomio monico f sono funzioni elementari delle radici.

Osservazione Se consideriamo polinomi a coefficienti in un campo finito $\mathbb{Z}_p$ possiamo riscontrare comportamenti insoliti.

Consideriamo ad esempio in $\mathbb{Z}_3$ il polinomio $f = [1]_3 x^3 + [2]_3 x$. Questo polinomio ha coefficienti non nulli, ma qualsiasi valore della x rende nullo il polinomio:

$x = 0 \implies f(0) = 0$

$x = 1 \implies f(1) = [1]_3 + [2]_3 = 0$

$x = 2 \implies f(2) = [2]_3 + [1]_3 = 0$

Quindi abbiamo dimostrato che f è un polinomio nullo pur avendo coefficienti non nulli.

15.3 Elementi Trascendenti

Consideriamo adesso una costruzione astratta dell'anello dei polinomi a coefficienti in un anello commutativo qualsiasi.

Sia B un anello commutativo, di cui A è un sottoanello proprio, e prendiamo $x \in B \setminus A$. Consideriamo poi l'anello generato da A e da x, ovvero

$$< A \cup \{x\} >= \left\{ \sum_{k=0}^{n} a_k x^k \;\middle|\; a_k \in A \subseteq B \right\}$$

Esempio 15.2 1. Possiamo considerare $A = \mathbb{Q}$ e $x = \sqrt{2} \notin \mathbb{Q}$, per cui in $A \cup \{x\}$ lo zero si può scrivere come "0" oppure come "$2 - x^2$".

2. Se prendiamo $A = \mathbb{Q}$, $B = \mathbb{R}$, $x = \pi \notin \mathbb{Q}$, un elemento del tipo $a_0 + a_1\pi + \ldots + a_n\pi^n$ è nullo se e solo se gli a_i sono tutti nulli, quindi ogni elemento di $< \mathbb{Q} \cup \{\pi\} >$ si scrive in un solo modo.

   Si usa dire che π è *trascendente* rispetto a $\mathbb{Q}$.

Seguendo l'idea dell'esempio precedente diamo una definizione:

Definizione 15.6 Se ogni elemento dell'anello $< A \cup \{x\} >$ si scrive in un solo modo nella forma $\sum_{k=0}^{n} a_k x^k$, diremo che x è *trascendente* rispetto ad A.

Teorema 15.3 *Siano A, A', B, B' anelli commutativi con $A \subseteq B$, $A' \subseteq B'$. Siano poi $x \in B \setminus A$ trascendente rispetto ad A, e $x' \in B' \setminus A'$ trascendente rispetto ad A'. Infine sia $\varphi : A \xrightarrow[su]{1-1} A'$ un isomorfismo.*

Allora anche $< A \cup \{x\} >$ e $< A' \cup \{x'\} >$ sono isomorfi.

Dimostrazione. Basta definire la seguente funzione

$$\begin{array}{ccc} \phi : < A \cup \{x\} > & \longrightarrow & < A' \cup \{x'\} > \\ \sum a_k x^k & \longmapsto & \sum a'_k x^k \end{array}$$

e dimostrare i seguenti punti:

1. ϕ è ben definita: si ha per l'unicità delle scritture sugli elementi del dominio.
2. ϕ è bigettiva: si ha per unicità delle scritture del codominio.
3. ϕ è un omomorfismo di anelli tale che $\phi|_A = \varphi$.

□

La conseguenza di questo teorema è che ogni anello commutativo ha, a meno di isomorfismi, una sola estensione trascendente. Chiameremo *anello dei polinomi* $A[x]$ questa estensione $< A \cup \{x\} >$, con x trascendente (per cui vale il principio di identità).

Ma questo x trascendente esiste sempre? Si!

Esempio 15.3 Sia $B = A^{\mathbb{N}}$ l'anello delle successioni, con le operazioni definite come nella lezione del 6/03/2014. In B c'è un elemento trascendente rispetto ad A?

L'elemento $X \in B$ definito come

$$X(n) = \begin{cases} 1_A & \text{se } n = 1 \\ 0_A & \text{se } n \neq 1 \end{cases}$$

è una "successione" di questo tipo: $X = \{0, 1, 0, 0, 0, \ldots\}$.

Le sue potenze risultano:
$X^2 = \{0, 0, 1, 0, 0, \ldots\}$
$X^3 = \{0, 0, 0, 1, 0, 0, \ldots\}$
$\vdots$

In generale

$$X^k(n) = \begin{cases} 1_A & \text{se } n = k \\ 0_A & \text{se } n \neq k \end{cases}$$

A questo punto possiamo definire $\forall a_k \in A$ l'elemento

$$a_k X^k = \begin{cases} a_k & \text{se } n = k \\ 0_A & \text{se } n \neq k \end{cases}$$

da cui la successione

$$\sum_{k=0}^{n} a_k X^k = \{a_0, a_1, \ldots, a_n, 0, 0, \ldots\}$$

Questa successione risulta nulla se e solo se $a_k = 0 \; \forall k$, quindi X è trascendente rispetto ad A.

Capitolo 16

10/04/2014

A partire da una struttura algebrica abbiamo visto come costruirne altre dello stesso tipo: sottostrutture, quozienti rispetto a congruenze, e così via.

Inoltre ad ogni struttura algebrica ne sono associate altre: il reticolo (con minimo e massimo) delle sottostrutture, il monoide degli endomorfismi $(End(X), \cdot, id_X)$, il gruppo degli automorfismi $(Aut(X), \cdot)$.

In questo capitolo vedremo come creare un'altra struttura a partire da due strutture di partenza usando il *Prodotto Diretto*.

16.1 Prodotti Diretti

Iniziamo col considerare strutture semplici: i gruppi.

Dati due gruppi $(H, \cdot)$, $(K, *)$, definiamo sul prodotto cartesiano $G = H \times K$ un'operazione binaria a partire da quelle definite sui due gruppi:

$$(h_1, k_1) \star (h_2, k_2) := (h_1 \cdot h_2, k_1 * k_2)$$

Poniamo poi $1_G := (1_H, 1_K)$ e $(h, k)^{-1} := (h^{-1}, k^{-1})$.

In questo modo abbiamo definito la nuova struttura G chiamata *prodotto diretto di H e K*.

Se invece di considerare inizialmente due gruppi avessimo preso in considerazione due strutture qualsiasi il procedimento sarebbe stato lo stesso, solamente un po' più lungo a causa della necessità di definire ogni operazione singolarmente.

Le proprietà universali[1] delle operazioni passano automaticamente al prodotto diretto, proprio perché si definiscono le nuove operazioni a partire da quelle di base.

Ne segue che se H e K sono gruppi abeliani, lo stesso varrà per G.

Inoltre le proprietà che sono conseguenza diretta degli assiomi passano al prodotto diretto (ad esempio la legge di cancellazione dei gruppi).

Mentre non passano le proprietà che fanno uso di "$\exists$", che potremmo chiamare "non universali", e quelle che non dipendono dagli assiomi.

Facciamo un esempio per chiarire.

Esempio 16.1 Prendiamo H e K due gruppi ciclici: $H = (\mathbb{Z}_2, +)$, $K = (Z_4, +)$.

Il concetto di ciclicità (o la proprietà di essere ciclico) si esprime in termini logici come "$\exists x \in H$ per cui $\forall h \in H$ $h = x + x + \ldots + x$".

Quindi la ciclicità parte dall'assunzione dell'esistenza (quindi usiamo "$\exists$") di un elemento che genera tutti gli altri.

Il gruppo $G = H \times K = \mathbb{Z}_2 \times \mathbb{Z}_4$ non risulta ciclico, poiché tutti i suoi elementi hanno ordine 2 o 4, e nessuno ha ordine 8 (che è l'ordine del gruppo).

Questo si può vedere in diversi modi. Essendo un gruppo di ordine molto basso si possono calcolare facilmente gli ordini di tutti i suoi elementi uno ad uno. Oppure possiamo dimostrare che in generale nel gruppo $G = H \times K$, qualunque siano H e K, se $h \in H$ ha ordine n e $k \in K$ ha ordine m, l'elemento $(h, k) \in G$ avrà ordine $mcm(n, m)$.

Ci sono dunque diverse proprietà che passano al prodotto diretto e tante altre che non passano, facciamone un paio di esempi:

Se A e B sono gruppi commutativi allora $A \times B$ risulta essere commutativo, difatti la definizione di gruppo commutativo è data come "$\forall h, k \in (G, +)$ vale $h + k = k + h$", quindi nella commutatività non si fa uso di quantificatori "$\exists$".

Se A e B sono domini di integrità $A \times B$ non risulta invece un dominio di integrità (a meno che uno dei due sia banale), poiché potremmo sempre fare $(1_A, 0_B) \cdot (0_A, 1_B) = (0_A, 0_B)$ trovando così due elementi non nulli il cui prodotto risulta nullo.

16.2 Proprietà Comuni ai Prodotti Diretti

Ci sono alcune proprietà che si mantengono in ogni prodotto diretto di $m \geq 2$ strutture algebriche.

[1] Con proprietà "universali" si intende quelle che hanno davanti un "$\forall$", ad esempio se nei due gruppi H e K di partenza le operazioni binarie sono associative, o commutative, lo stesso varrà per l'operazione definita su G.

La **Proiezione**: prese le strutture $X_1, \ldots, X_n$ risultano definite gli n epimorfismi di proiezione

$$\begin{array}{rcl} p_i : X_1 \times \ldots \times X_n & \longrightarrow & X_i \\ (x_1, \ldots, x_n) & \longmapsto & x_i \end{array}$$

Solo per i gruppi vi sono poi le **immersioni**: presi $H_1, \ldots, H_n$ gruppi, si definiscono n omomorfismi di immersione

$$\begin{array}{rcl} i_k : H_k & \longrightarrow & H_1 \times \ldots \times H_n \\ h & \longmapsto & \left(1_{H_1}, \ldots, 1_{H_{k-1}}, h, 1_{H_{k+1}}, \ldots, 1_{H_n}\right) \end{array}$$

C'è anche una relazione tra questi due tipi di funzioni: se analizziamo il caso più semplice di 2 fattori, ovvero in cui $G = H \times K$, abbiamo che la proiezione $p_1(h,k) = h$ e l'immersione $i_2(k) = (1_H, k)$ sono legate poiché

$$\{(1_H, k) \mid k \in K\} = Im(i_2) = Ker(p_1) \triangleleft G$$

$$\{(h, 1_K) \mid h \in H\} = Im(i_1) = Ker(p_2) \triangleleft G$$

Lo stesso vale anche con più fattori, risulta solo leggermente più lungo da scrivere.

Capitolo 17

14/04/2014

Abbiamo parlato del prodotto diretto, che ci permette di definire nuove strutture algebriche, di cui conosciamo già alcuni esempi:

$$(\mathbb{R}^2, +) \cong (\mathbb{R}, +) \times (\mathbb{R}, +) \cong (\mathbb{C}, +)$$

$$< a, b \mid ab = ba, a^2 = 1 = b^2 > \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

17.1 Modulo e Argomento in $\mathbb{R}$ e in $\mathbb{C}$

Nel gruppo $(\mathbb{R}^*, \cdot)$, la funzione *valore assoluto*, definita come

$$|x| = \begin{cases} x & \text{se } x > 0 \\ -x & \text{se } x < 0 \end{cases}$$

ha la proprietà che $|xy| = |x| \cdot |y|$, e quindi è un endomorfismo di $\mathbb{R}^*$.

L'immagine è il sottogruppo $\mathbb{R}^+$, mentre il nucleo è $\{x \in \mathbb{R}^* \mid |x| = 1\} = \{\pm 1\} = \mathbb{Z}^*$.

Ogni $x \in \mathbb{R}^*$ è prodotto di un *segno* (± 1) e di un *modulo* (dato da $|x|$).

La funzione *segno*, definita come

$$sign(x) = \begin{cases} 1 & \text{se } x > 0 \\ -1 & \text{se } x < 0 \end{cases}$$

ha immagine $\mathbb{Z}^*$, e nucleo $\mathbb{R}^+$.

Inoltre vale $sign(xy) = sign(x) \cdot sign(y)$.

$\forall x \in \mathbb{R}^*$ possiamo scrivere $x = sign(x) \cdot |x| \in \mathbb{Z}^* \cdot \mathbb{R}^+$, quindi evidentemente $\mathbb{R}^* = \mathbb{Z}^* \cdot \mathbb{R}^+$.

Non solo, abbiamo anche che $\mathbb{Z}^* \cap \mathbb{R}^+ = \{1\}$, quindi $\mathbb{R}^*$ è isomorfo a $\mathbb{Z}^* \times \mathbb{R}^+$.

Ora vediamo $\mathbb{C}^*$:

Preso un elemento $z = x + iy$ diciamo che il suo modulo è $|z| = \sqrt{x^2 + y^2}$, e si ha $|z_1 z_2| = |z_1| \cdot |z_2|$, quindi il modulo è un endomorfismo di $\mathbb{C}^*$.

L'immagine è $\mathbb{R}^+$, il nucleo è $\{z \in \mathbb{C}^* \mid |z| = 1\} = \{z \in \mathbb{C}^* \mid x^2 + y^2 = 1\}$, che è un sottogruppo di $\mathbb{C}^*$ descritto dalla circonferenza trigonometrica (o unitaria).

Ad ogni $z \in \mathbb{C}^*$ possiamo inoltre associare un angolo φ (detto *argomento di* z) tale che se z si scrive come $x + iy$ risulta

$$\begin{cases} x = |z| \cdot \cos\varphi \\ y = |z| \cdot \sin\varphi \end{cases}$$

Attenzione: l'argomento non è unico, infatti ogni numero complesso ha infiniti argomenti della forma $\varphi + 2k\pi$, con $k \in \mathbb{Z}$, a causa della periodicità delle funzioni seno e coseno.

Vale però la seguente relazione: se $arg(z_1) = \varphi_1$ e $arg(z_2) = \varphi_2$, allora $arg(z_1 z_2) = \varphi_1 + \varphi_2$.

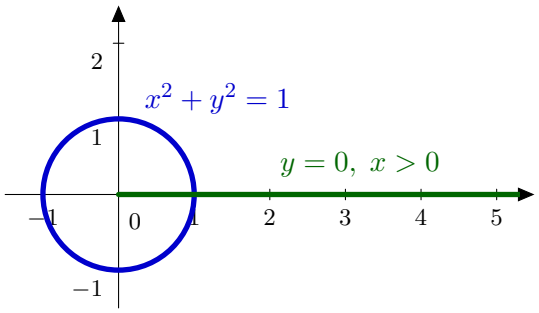
Inoltre i numeri $2k\pi$ sono elementi del gruppo ciclico generato da 2π (denotato con $< 2\pi > \subseteq (\mathbb{R}, +)$), quindi $\varphi + 2k\pi \in \varphi + < 2\pi >$ che è un suo laterale.

Quindi $\varphi + 2k\pi \in \mathbb{R}/_{<2\pi>}$, e possiamo convenire di scegliere $\varphi \in [0, 2\pi[$, così da rendere unico anche l'argomento.

Con questi accorgimenti ad ogni argomento φ corrisponde un unico punto $(\cos\varphi, \sin\varphi)$ della circonferenza unitaria. In tal modo la funzione $arg(z) = \varphi$ risulta essere un epimorfismo da $\mathbb{C}^*$ al quoziente $\mathbb{R}/_{<2\pi>}$, ovvero al sottogruppo $\{|z| = 1\}$ di $\mathbb{C}^*$, con nucleo $\{z \in \mathbb{C}^* \mid arg(z) = 0\} = \mathbb{R}^+$.

Possiamo quindi definire un isomorfismo che associa ad ogni $z \in \mathbb{C}^*$ l'elemento $(|z|, arg(z)) \in \mathbb{R}^+ \times \mathbb{R}/_{<2\pi>}$, dimostrando così che

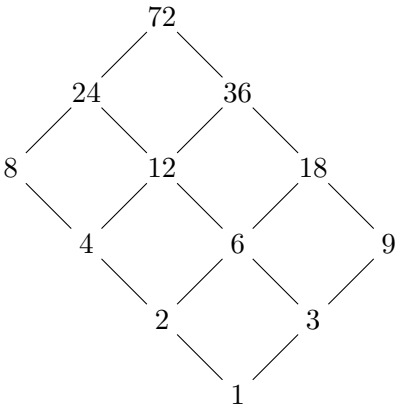
$$(\mathbb{C}^*, \cdot) \cong (\mathbb{R}^+, \cdot) \times (\mathbb{R}/_{<2\pi>}, +)$$



Osservazione Se nei gruppi A, B vale la distributività, allora lo stesso varrà in $A \times B$.

Inoltre gli insiemi totalmente ordinati possono essere visti come reticoli distributivi, quindi il prodotto di due insiemi totalmente ordinati risulta ancora un reticolo distributivo.

Esempio 17.1 $72 = 2^3 \cdot 3^2$. Ogni divisore di 72 è del tipo $2^h \cdot 3^k$, quindi il reticolo dei divisori di 72 è il prodotto diretto dei reticoli dei divisori di 8 e 9, che risultano distributivi, il che dimostra che esso stesso è distributivo.



17.2 Regole del Calcolo Letterale

Alfabeto $\longrightarrow$ parole

Linguaggio = insieme di parole con regole di formazione che ci dicono se una parola può o no essere ammessa nel nostro linguaggio (ortografia).

Assiomi o Regole Grammaticali, che ci dicono quali manipolazioni possiamo eseguire sulle parole del linguaggio.

Sintassi: regole per formare sequenza corrette di parole (periodi).

Allo stesso modo possiamo analizzare il caso del calcolo letterale, in cui l'alfabeto è costituito da:

- elementi di un anello commutativo, ad esempio $\mathbb{R}$

- alcune "indeterminate", ossia oggetti $\notin \mathbb{R}$

- i segni $+$ e $-$

- le parentesi (,)

Occorrono però delle regole di formazione:

- mai due segni consecutivi
- due numeri consecutivi sono da sostituire col loro prodotto
- ogni parentesi (deve essere seguita prima o poi da) e) non può precedere (
- le indeterminate commutano fra loro e con i numeri, ma non con i segni o con le parentesi
- due o più indeterminate uguali possono essere accorpate con le potenze

le parole così formate le chiamiamo *polinomi*.

Poi si definiscono le operazioni fra polinomi con gli assiomi necessari ad ottenere l'anello dei polinomi che conosciamo.

Ci sono un sacco di altre regole che non abbiamo scritto, quindi come vediamo non è per nulla semplice capire tutto quello che c'è dietro al calcolo letterale.

Vi sono inoltre molti significati per il simbolo "+":

- ogni numero reale ha un segno
- è un carattere del nostro alfabeto
- è il simbolo dell'addizione

e lo stesso per il simbolo "−":

- ogni numero reale ha un segno
- è un carattere del nostro alfabeto
- è il simbolo della sottrazione
- è l'operazione unaria "opposto"

Capitolo 18

16/04/2014

18.1 Azione di un Insieme su un Altro

Definizione 18.1 Dati due insiemi Ω, X, una *azione di* Ω *su* X è una funzione $\mu : \Omega \times X \longrightarrow X$ (così descritta viene detta a volte azione *sinistra*).

L'immagine di un punto (ω, x) si denota con ωx (perciò l'azione si chiama spesso *moltiplicazione esterna* di Ω per X).

La terna (X, Ω, μ) è detta Ω-*insieme*. Per abbreviare spesso si dice che X è un Ω-*insieme*.

Tutto ciò però si può dire anche diversamente:
Per ogni $\omega \in \Omega$ definiamo la funzione

$$\begin{array}{rcl} \tau_\omega : X & \longrightarrow & X \\ x & \longmapsto & \omega x \end{array}$$

In questo caso $\tau_\omega \in X^X$, quindi a partire dalle τ_ω possiamo considerare la funzione

$$\begin{array}{rcl} \rho : \Omega & \longrightarrow & X^X \\ \omega & \longmapsto & \tau_\omega \end{array}$$

che viene chiamata *rappresentazione* di Ω su X.

Viceversa, data una funzione $\rho : \Omega \longrightarrow X^X$, posto $\tau_\omega = \rho(\omega)$ e $\mu(\omega, x) = \tau_\omega(x)$, possiamo definire $\mu : \Omega \times X \longrightarrow X$ trovando così una *azione di* Ω *su* X.

Esempio 18.1 Per fare un esempio di azione possiamo pensare ad un campo vettoriale: in questo caso Ω è l'insieme degli scalari e X è l'insieme dei vettori. L'azione è rappresentata dalla "moltiplicazione" scalare-vettore che conosciamo tutti.

Le proprietà degli Ω-insiemi sono simili a quelle delle strutture algebriche:
Sia X un Ω-insieme.

- $Y \subseteq X$ si dice Ω-*sottoinsieme* di X se $\forall \omega \in \Omega$, $\forall y \in Y$ vale $\omega y \in Y$.

  Si può dimostrare che l'intersezione di Ω-sottoinsiemi è un Ω-sottoinsieme, poi definire l'Ω-sottoinsieme generato da un sottoinsieme $S \subseteq X$ o anche ottenere il reticolo degli Ω-sottoinsiemi.

- Una Ω-*congruenza* in X è una relazione d'equivalenza $\sim$ di X tale che $\forall \omega \in \Omega$, $\forall x, x' \in X$, $x \sim x' \iff \omega x \sim \omega x'$.

  A partire da una relazione d'equivalenza su X con questa proprietà si può porre $\omega[x]_\sim = [\omega x]_\sim$ e trasformare $X/_\sim$ in un Ω-insieme.

- Un Ω-*omomorfismo* tra due Ω-insiemi X e Y è una funzione $f : X \longrightarrow Y$ tale che $\forall \omega \in \Omega$, $\forall x \in X$ vale $f(\omega x) = \omega f(x)$.

  Vale anche il **Teorema Fondamentale di Omomorfismo**, enunciato e dimostrato allo stesso modo.

- Si può considerare il monoide degli Ω-*endomorfismi* ed il gruppo degli Ω-*automorfismi* di X, allo stesso modo di come abbiamo fatto per le strutture algebriche nei capitoli precedenti.

- Nel prodotto cartesiano $X \times Y$ di due Ω-insiemi X e Y basta porre $\omega(x, y) = (\omega x, \omega y)$ per far sì che anche $X \times Y$ sia un Ω-insieme.

18.2 Azione Insieme-Struttura e Viceversa

Se almeno uno dei due insiemi Ω e X è già fornito di una struttura algebrica dovremmo fare in modo che l'azione rispetti le sue proprietà. Ci servono quindi delle *condizioni di compatibilità*. Vediamo i vari casi:

1. Ω insieme, X struttura algebrica.

   Si postula che $\forall \omega \in \Omega$ deve valere $\tau_\omega \in End(X)$, ovvero $Im(\rho) \subseteq End(X)$.

2. Ω struttura algebrica, X insieme.

   Dobbiamo postulare che in X^X ci sia una struttura algebrica dello stesso tipo di Ω e che ρ sia un omomorfismo tra le due strutture.

3. Ω e X entrambe strutture algebriche.

   Devono valere entrambe le condizioni scritte sopra.

Esempio 18.2 Come Ω prendiamo un anello A, mentre come X prendiamo un gruppo abeliano $(V, +)$.

Dire che $\tau_a \in End(V)$ significa che $\forall a \in A$, $\forall u, v \in V$ vale

$$\tau_a(v + w) = a(v + w) = av + aw = \tau_a(v) + \tau_a(w)$$

Lemma *Sia $(V, +)$ un gruppo abeliano. Nel monoide $(End(V), \circ, id_V) \subseteq V^V$ si può definire l'addizione punto per punto come $(\alpha + \beta)(v) = \alpha(v) + \beta(v)$, con $0(v) = 0_V$ e $(-\alpha)(v) = -(\alpha(v))$, ottenendo un gruppo abeliano.*

La composizione è distributiva rispetto a $+$, ovvero $\forall \alpha, \beta, \gamma \in End(V)$ vale

$$(\alpha + \beta) \circ \gamma = \alpha \circ \gamma + \beta \circ \gamma$$

$$\gamma \circ (\alpha + \beta) = \gamma \circ \alpha + \gamma \circ \beta$$

Dunque $(End(V), +, \circ, id_V)$ risulta un anello.

Grazie al lemma possiamo ragionare sul significato del fatto che $\rho : A \longrightarrow End(V)$ è un omomorfismo di anelli. Significa che valgono delle condizioni:

- $\forall a, b \in A$ vale $\rho(a + b) = \rho(a) + \rho(b)$, ovvero $\tau_{a+b} = \tau_a + \tau_b$, che significa $\forall v \in V$ vale $(a + b)v = av + bv$.
- $\forall a, b \in A$ vale $\rho(ab) = \rho(a) \circ \rho(b)$, che significa $\forall v \in V$ vale $(ab)v = a(bv)$.
- $\rho(1_A) = id_V$, ovvero $\forall v \in V$ vale $1_A(v) = v$.

Allora, se vale questa compatibilità, V diventa un *A-modulo.*

Se poi come anello prendiamo un campo K, V diventa un *K-spazio vettoriale.*

Capitolo 19

28/04/2014

19.1 A-moduli

Riguardo le azioni di insiemi ce ne sono alcune particolari.

Consideriamo l'azione di un anello A su un gruppo abeliano $(V, +)$.

Se $A = K$ è un campo otteniamo uno *spazio vettoriale*.

Proprietà particolari:

- $\forall k \in K,\ v \in V \qquad kv = 0_V \iff k = 0_K$ oppure $v = 0_V$.
- Tutte le basi sono equipotenti[1].
- Le sottostrutture sono chiamate *sottospazi*.
- I morfismi sono le *applicazioni lineari*.

Esempio 19.1 Facciamo un esempio di A-modulo un po' strano:

Preso A anello commutativo e $(A, +)$ gruppo, definiamo un'operazione a partire dalla moltiplicazione definita sull'anello:

$$\begin{array}{rcl} \mu : A \times A & \longrightarrow & A \\ (a, x) & \longmapsto & a \cdot x \end{array}$$

Dalla proprietà distributiva e dall'associatività della moltiplicazione segue che $(A, +)$ è un A-modulo.

Le sue **sottostrutture** sono sottogruppi I di $(A, +)$ tali che sono anche A-sottoinsiemi, ovvero $\forall a \in A$ e $\forall i \in I$ vale $a \cdot i \in I$; quindi sono gli ideali di A.

[1] Da questo concetto possiamo iniziare per definire una *dimensione* dello spazio vettoriale.

19.2 Azione di un gruppo su un insieme

Prendiamo un gruppo G e un insieme $X \neq \emptyset$.

Su di essi vogliamo definire un'azione $\mu : G \times X \longrightarrow X$. Perché μ sia un'azione del gruppo G su X, la rappresentazione $f : G \longrightarrow X^X$ deve essere un omomorfismo, ossia

$$\begin{cases} f(g_1 g_2) = f(g_1) \circ f(g_2) & \forall g_1, g_2 \in G \\ f(1_G) = id_X \end{cases}$$

Ora, da queste proprietà possiamo ricavare alcune cose utili:

$$\left.\begin{array}{l} id_X = f(1_G) = f(g \cdot g^{-1}) = f(g) \circ f(g^{-1}) \\ id_X = f(1_G) = f(g^{-1} \cdot g) = f(g^{-1}) \circ f(g) \end{array}\right\} \Longrightarrow f(g^{-1}) = f(g)^{-1} \Longrightarrow f \text{ bigettiva}$$

Da cui sappiamo che $Im(f) \subseteq S_X$, per cui $f(g)$ è una permutazione, che indichiamo con $f(g) := \tau_g$.

Analizziamo meglio l'effetto dell'azione del gruppo G sull'insieme X:

Definizione 19.1 Sia $x \in X$, definiamo lo *stabilizzatore di x in G* come l'insieme

$$St_G(x) = G_x = \{g \in G \mid \tau_g(x) = x\}$$

Osservazione $St_G(x)$ è un sottogruppo di G, qualunque sia x.

Definizione 19.2 Definita l'applicazione $\rho(g) := \tau_g \in X^X$, diciamo che l'azione di G su X è *fedele* se ρ è bigettiva (ovvero $Ker\,\rho = \{id_X\}$).

Osservazione $Ker\,\rho = \bigcap_{x \in X} G_x$

A partire dalla nozione di stabilizzatore possiamo definire una relazione di equivalenza sull'insieme X del tipo

$$x \sim_G y \quad \Longleftrightarrow \quad \exists\, g \in G \text{ tale che } y = \tau_g(x)$$

Questa è una vera e propria relazione di equivalenza:

- $\forall x \in X$, $x = \tau_{1_G}(x) \Longrightarrow x \sim_G x$
- $\forall x, y \in X$, se $y = \tau_g(x)$ allora $x = \tau_{g^{-1}}(y) \Longrightarrow y \sim_G x$
- $\forall x, y \in X$, se $x \sim_G y$ e $y \sim_G z$, abbiamo

  $$\exists\, g_1 \quad y = \tau_{g_1}(x) \qquad\qquad \exists\, g_2 \quad z = \tau_{g_2}(y)$$

  da cui ricaviamo

  $$z = \tau_{g_2}\big(\tau_{g_1}(x)\big) = \tau_{g_2} \circ \tau_{g_1}(x) = \tau_{g_2 g_1}(x) \Longrightarrow \quad z \sim_G x$$

Definizione 19.3 Le classi di equivalenza di $[x]_G$ secondo la relazione appena descritta si dicono *orbite* (o *G-ordbite*).

Può accadere che l'orbita di un elemento x coincida con tutto l'insieme X. In tal caso l'azione di G su X si dice *transitiva*.

Teorema 19.1 *Data l'azione del gruppo G sull'insieme X, per ogni $x \in X$ sia $[x]_G$ la sua orbita, G_x il suo stabilizzatore ed $S := \{g \cdot G_x \mid g \in G\}$ l'insieme dei laterali sinistri di G_x in G.*

Allora $[x]_G$ e S sono equipotenti.

In particolare, se G è un gruppo finito, $|[x]_G|$ divide $|G|$.

Dimostrazione. $\forall y \in [x]_G$ sappiamo per definizione che $\exists\, g \in G$ tale che $y = \tau_g(x)$.

L'associazione $y \longrightarrow gG_x$ è una funzione?

Se esiste un altro $g' \in G_x$ tale che $y = \tau_{g'}(x)$ allora avremo

$$\tau_g(x) = \tau_{g'}(x) \iff x = \tau_g^{-1} \circ \tau_{g'}(x) \iff \tau_{g^{-1}g'}(x) = x \iff$$

$$\iff g^{-1}g' \in G_x \iff gG_x = g'G_x$$

Quindi si, questa è una funzione:

$$\begin{array}{rcl} \Phi : [x]_G & \longrightarrow & S \\ y & \longmapsto & gG_x \end{array}$$

e con i ragionamenti di prima abbiamo dimostrato anche che Φ è iniettiva.

D'altra parte la suriettività di Φ è quasi ovvia: a gG_x facciamo corrispondere $y = \tau_g(x)$, cosicché $\Phi(y) = gG_x$.

Nel caso finito abbiamo che $|S| = [G : G_x]$; ma sappiamo che l'indice di G_x in G è un divisore di $|G|$, per cui $|[x]_G| = |S|$ divide $|G|$.

□

Esempio 19.2 (Coniugio) Come gruppo prendiamo $(G, \cdot)$ qualsiasi, e come X prendiamo G stesso.

Come azione prendiamo il *coniugio*: $\mu(g, x) = gxg^{-1}$.

Le funzioni associate ai $g \in G$ si indicano con γ_g (anziché τ_g), poiché questa è un'azione di gruppo molto particolare. Dunque abbiamo $\gamma_g(x) = gxg^{-1}$.

Le proprietà si mantengono:

$$\gamma_{g_1g_2}(x) = g_1g_2x(g_1g_2)^{-1} = g_1g_2xg_2^{-1}g_1^{-1} =$$

$$= g_1\gamma_{g_2}(x)g_1^{-1} = \gamma_{g_1}\big(\gamma_{g_2}(x)\big) = \gamma_{g_1} \circ \gamma_{g_2}(x)$$

e anche $\gamma_{1_G}(x) = x = id_G(x)$.

Allora $\rho : G \longrightarrow G^G$ è un omomorfismo di gruppi e μ un'azione.

Le orbite degli elementi si chiamano *classi di coniugio.*

Lo stabilizzatore di un elemento x si chiama *centralizzante di* x, e si indica con $\mathcal{C}_G(x)$.

Il teorema di poco fa ci dice che $|G| = |\mathcal{C}_G(x)| \cdot |[x]_G|$.

Nota: in realtà è un'azione di G su se stesso, visto che ogni γ_g è un endomorfismo, anzi essendo bigettiva è addirittura un automorfismo di G, detto automorfismo *interno.*

$\gamma_g(x_1x_2) = gx_1x_2g^{-1} = gx_1g^{-1}gx_2g^{-1} = \gamma_g(x_1)\gamma_g(x_2)$

Vediamo chi è il nucleo di ρ: $Ker\ \rho = \{\gamma_g = id_G,\ g \in G\}$, ma possiamo spacificarli meglio:

$$\gamma_g(x) = x \iff gxg^{-1} = x \iff gx = xg \quad \forall x \in G$$

$$\implies \quad Ker\,\rho = Z(G)$$

Posto $In(G) = Imm(\rho) = \{$ automorfismi interni $\}$, allora vale

$$G\Big/_{Z(G)} \simeq In(G)$$

Esempio 19.3 Sia G il gruppo delle isometrie del piano euclideo (insieme X), ovvero le funzioni $f : X \longrightarrow X$ che mantengono le *distanze* tra i punti del piano.

Preso un punto P del piano, chi è la sua orbita?

Se consideriamo un punto qualsiasi Q del piano, esiste sempre l'asse di PQ, per cui esiste sempre una simmetria assiale che manda P in Q. Dunque l'orbita è tutto il piano, ovvero l'azione è transitiva sui punti.

Chi è lo stabilizzatore di P?

L'identità fa parte degli stabilizzatori, ma non è l'unico elemento. Abbiamo anche le simmetrie passanti per P e le rotazioni di centro P.

L'azione di G sul piano si trasferisce alle figure, quindi potremmo pensare a qual'è l'orbita di una retta o di un poligono dato; lasciamo questi approfondimenti per esercizio.

Capitolo 20

30/04/2014

20.1 Estensione di Campi

Sia K un sottocampo di $\mathbb{C}$, e sia $u \in \mathbb{C} \setminus K$.

Gli elementi dell'anello $< K \cup \{u\} > \subseteq \mathbb{C}$ sono del tipo $a_0 + a_1 u + \ldots + a_n u^n$, con gli $a_i \in K$.

Prendiamo quindi il polinomio $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in K[x]$. Quell'elemento di $< K \cup \{u\} >$ lo possiamo indicare con "$f(u)$".

Nasce così una funzione $\mu_u : K[x] \longrightarrow \mathbb{C}$ che associa ad $f(x)$ l'elemento $f(u)$, con le seguenti proprietà:

- μ_u è un omomorfismo;
- $\mu_u(a) = a \quad \forall a \in K$;
- $\mu_u(x) = u$;
- $Imm(\mu_u) =< K \cup \{u\} >= K[u]$.

Sappiamo che il nucleo di un omomorfismo è un ideale dell'anello di partenza:

$$I = Ker\, \mu_u = \{f \in K[x] \mid \mu_u = f(u) = 0\}$$

ed esso è costituito dai polinomi che hanno u come radice.

Se $Ker\, \mu_u = \{0\}$, allora u è trascendente rispetto a K, e $K[u] \simeq K[x]$.

Se invece $Ker\, \mu_u \neq \{0\}$, poiché $K[x]$ è un PID (perché euclideo), allora esiste un polinomio p che lo genera: $Ker\, \mu_u = (p)$.

Possiamo supporre che p sia monico di grado $n \geq 2$, e deve essere necessariamente irriducibile[1]. Chiamiamo questo polinomio p il *polinomio minimo di u*.

[1] Perché genera l'ideale, quindi non può avere divisori altrimenti anch'essi sarebbero generatori dell'ideale (p).

Poiché p è irriducibile, (p) è massimale in $K[x]$, quindi il quoziente $K[x]/_{(p)}$ è un campo!

I suoi laterali sono i laterali del tipo $f + (p)$, quindi possiamo scrivere

$$f = pq + r \qquad r = 0 \ \vee \ deg(r) < n$$

da cui $f + (p) = r + (p)$.

Dal Teorema Fondamentale di Omomorfismo segue che

$$< K \cup \{u\} >= Im(\mu_u) \simeq K[x]/_{Ker\,\mu_u} = K[x]/_{(p)}$$

dunque $K(u) =< K \cup \{u\} >$ è un campo, i cui elementi sono del tipo

$$\Phi(r + (p)) = \mu_u(r) = a_0 + a_1 u + \ldots + a_{n-1} u^{n-1}$$

Esempio 20.1 Prendiamo $K = \mathbb{Q}$ e $u = \sqrt[3]{2}$.

Ricaviamo il polinomio minimo:

$$x = \sqrt[3]{2} \qquad x^3 = 2 \qquad \Longrightarrow \quad p(x) = x^3 - 2$$

Da cui otteniamo l'indicazione degli elementi dell'estensione:

$$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$$

Essendo un campo ogni elemento non nullo ha un inverso $(a + b\sqrt[3]{2} + c\sqrt[3]{4})^{-1}$, che appartiene al campo quindi si deve poter scrivere nella forma $x + y\sqrt[3]{2} + z\sqrt[3]{4}$, anche se trovare x, y, z a volte potrebbe non essere semplice.

Posto $H = K(u)$, possiamo prendere $v \in \mathbb{C} \setminus H$, e procedere allo stesso modo per estendere ancora H al campo $H(v)$ tramite il polinomio minimo q di v di grado m.

Ogni elemento di $H(v)$ si scrive nella forma $h_0 + h_1 v + \ldots + h_{m-1} v^{m-1}$, ma visto che $H = K(u)$ vale

$$h_i \in H = K(u) \Longrightarrow h_i = \sum_{k=0}^{n-1} a_i k u^k$$

da cui troviamo che gli elementi di $H(v)$ hanno una scrittura della forma

$$\sum_{i=0}^{m-1} \sum_{k=0}^{n-1} a_{ik}\, u^k v^i$$

Esempio 20.2 Riprendendo l'esempio di prima, prendiamo $H = \mathbb{Q}(\sqrt[3]{2})$ e $v = \sqrt{-3}$.

Il polinomio minimo di v in H è $q(x) = x^2 + 3$, quindi una base dell'estensione $H(v)$ su H è data da $\{1, i\sqrt{3}\}$.

Da questo ricaviamo una base dello spazio vettoriale $H(v)$ su $\mathbb{Q}$ come

$$\{1, \sqrt[3]{2}, \sqrt[3]{4}, i\sqrt{3}, i\sqrt{3}\sqrt[3]{2}, i\sqrt{3}\sqrt[3]{4}\}$$

Capitolo 21

05/05/2014

21.1 Equazioni di Grado ≥ 4

Le equazioni di grado alto sappiamo che non si risolvono generalmente per radicali, ma ci sono dei casi particolari (anche se pochi):

Equazione Trinomia $ax^4 + bx^2 + c = 0$ si risolve come sappiamo:
Poniamo $y = x^2$ ed otteniamo

$$ay^2 + by + c = 0$$

da cui possiamo calcolare i valori della y tramite la formula risolutiva solita di secondo grado

$$y = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

da questi valori possiamo trovare le soluzioni dell'equazione di partenza considerando le soluzioni positive per la y e calcolando $x = \sqrt{y}$.

Equazione Simmetrica $ax^4 + bx^3 + cx^2 + bx + a = 0$ si risolve nel seguente modo:
Per $x \neq 0$ poniamo $y = x + \frac{1}{x}$ ed otteniamo

$$ax^2 + bx + c + \frac{b}{x} + \frac{a}{x^2} = 0$$

$$a\underbrace{\left(x^2 + \frac{1}{x^2}\right)}_{y^2-2} + b\underbrace{\left(x + \frac{1}{x}\right)}_{y} + c = 0$$

$$ay^2 + by + (c - 2a) = 0$$

e risolviamo l'equazione di secondo grado come al solito.

21.2 Ampliamenti Normali

Preso un polinomio $f \in \mathbb{C}[x]$, sappiamo di poterlo scrivere nella forma

$$f(x) = \sum_{k=0}^{n} a_k x^k \qquad \text{con } a_n = 1$$

liberandolo dalle sue radici multiple, se le ha, e dividendolo per il coefficiente di testa, se non è monico.

Se chiamiamo K il sottocampo di $\mathbb{C}$ generato dai coefficienti $a_0, a_1, \ldots, a_{n-1}$, possiamo considerare $f \in K[x]$.

Indichiamo con $\alpha_1, \ldots, \alpha_n$ le sue radici complesse e con F il sottocampo di $\mathbb{C}$ da esse generato.

Poiché i coefficienti sono funzioni polinomiali simmetriche delle radici, risulta $K \subseteq F$, in cui l'uguaglianza è verificata solo se le radici stanno tutte in K.

Se $K \neq F$, prendiamo[1] $\alpha_1 \in F \setminus K$ e consideriamo il polinomio minimo p_1 di α_1 in $K[x]$. Allora $K(\alpha_1) \subseteq F$ ha dimensione $deg(p_1)$ rispetto a K.

Inoltre sia p_1 che f sono divisibili per $x - \alpha_1$ in $F[x]$, quindi $d = MCD(p_1, f) \neq 1$. Ma p_1 è irriducibile, quindi $d \simeq p_1 \Longrightarrow p_1 | f$.

Definizione 21.1 Un ampliamento H di K si dice *normale* se vale la seguente proprietà: se H contiene una radice di un polinomio irriducibile in K, allora le contiene tutte, ovvero H è il suo campo di spezzamento[2].

Secondo questa definizione, può darsi che $K(\alpha_1)$ sia ampliamento normale di K.

In $K(\alpha_1)$, infatti, f ha sicuramente alcune radici; Se le ha tutte, allora $F = K(\alpha_1)$, altrimenti possiamo prendere $\alpha_2 \in F \setminus K(\alpha_1)$ e costruire $K(\alpha_1)(\alpha_2)$ allo stesso modo.

Questo procedimento può essere ripetuto per tutte le radici fino a raggiungere tutto F. Ogni volta l'ampliamento ha dimensione finita sul campo di partenza, quindi anche F ha dimensione finita su K.

Esempio 21.1 Prendiamo $K = \mathbb{Q}$ e $f(x) = x^3 - 2 \in \mathbb{Q}[x]$.

Se chiamiamo $u = \sqrt[3]{2} \notin \mathbb{Q}$, l'ampliamento $\mathbb{Q}(u) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$ non è normale perché le altre due radici di $x^3 - 2$ (che è irriducibile) non sono reali, quindi non appartengono a $\mathbb{Q}(u) \subseteq \mathbb{R}$.

Possiamo però procedere: il polinomio $x^3 - 2 = (x - u)(x^2 + ux + u^2) \in \mathbb{Q}(u)[x]$ contiene tutte le radici di f (visto che è lo stesso polinomio scritto in forma diversa), ma stavolta le

[1] Stiamo prendendo α_1 per semplicità, visto che non abbiamo fissato un ordinamento sulle radici.

[2] Ricordiamo che il *campo di spezzamento* di un polinomio p è definito come il minimo sottocampo di $\mathbb{C}$ che contiene tutte le sue radici.

sappiamo trovare tramite la formula delle equazioni di secondo grado:

$$x = \frac{-u \pm \sqrt{u^2 - 4u^2}}{2} = u\left(\frac{-1 \pm \sqrt{-3}}{2}\right)$$

se chiamiamo $v = i\sqrt{3}$ le radici risultano essere

$$x = u\left(\frac{-1 \pm v}{2}\right) \in \mathbb{Q}(u)(v) = F$$

e la dimensione può essere calcolata facilmente:

$$\left.\begin{array}{l} dim_{\mathbb{Q}}\ \mathbb{Q}(u) = 3 \\ dim_{\mathbb{Q}(u)}\ F = 2 \end{array}\right\} \Longrightarrow dim_{\mathbb{Q}}\ F = 6$$

una base per F su $\mathbb{Q}$ è $\{1, u, u^2, v, uv, u^2v\}$. I passaggi che abbiamo eseguito hanno portato ad ampliamenti normali e non normali:

$$\mathbb{Q} \xrightarrow{\text{non normale}} \mathbb{Q}(u) \xrightarrow{\text{normale}} \mathbb{Q}(u)(v) = F$$

ma questa non era la sola strada possibile! Il polinomio minimo di v su $\mathbb{Q}$ è x^2+3. In $\mathbb{Q}(v)$ il polinomio $f(x) = x^3 - 2$ è tuttora irriducibile, quindi possiamo considerare $\mathbb{Q}(v)(u)$. In questo ampliamento il polinomio f ha tutte le radici, quindi siamo arrivati ad F seguendo il cammino:

$$\mathbb{Q} \xrightarrow[dim=2]{\text{normale}} \mathbb{Q}(v) \xrightarrow[dim=3]{\text{normale}} F = \mathbb{Q}(v)(u)$$

21.3 Gruppo di Galois

Se prendiamo $f \in K[x]$, F= campo di spezzamento di f, allora $Aut(F)$ è un gruppo.

Se selezioniamo gli automorfismi φ di F tali che $\varphi_{|_K} = id_K$, questi costituiscono a loro volta un gruppo $G = G_f$ detto *Gruppo di Galois* di f.

Presi $\varphi \in G$ e α radice di f, risulta $f(\alpha) = 0$, quindi

$$0 = \varphi(0) = \varphi(f(\alpha)) = \varphi\left(\sum_{k=0}^{n} a_k\alpha^k\right) = \sum_{k=0}^{n} \varphi(a_k)\varphi(\alpha^k) = \sum_{k=0}^{n} a_k\varphi(\alpha)^k = f(\varphi(\alpha))$$

$$\Longrightarrow \quad \varphi(\alpha) \text{ è una radice di } f$$

Se chiamiamo $X = \{\alpha_1, \ldots, \alpha_n\}$ l'insieme delle radici di f, abbiamo appena mostrato che $\forall \varphi \in G$, φ trasforma X in se stesso, quindi induce in X una permutazione.

Allora la funzione $\rho : G \longrightarrow S_X$, $\rho(\varphi) = \varphi_{|_X}$ risulta essere un omomorfismo di gruppi.

Abbiamo dunque un'azione di G su X. Chi è $Ker(\rho)$?

$$\varphi \in Ker\rho \iff \varphi_{|X} = \rho(\varphi) = id_X$$

ma F è generato dalle radici, ovvero dagli elementi di X, quindi φ è identità in tutto F, ovvero $\varphi = id_F = 1_G$ e ρ è iniettiva.

Ciò significa che G è isomorfo a $Im(\rho)$, che è un sottogruppo di $S_X \simeq S_n$, dunque G divide $n!$.

Si può anche dimostrare che $|G| = dim_K\ F$.

21.4 Gruppi Risolubili e Teorema di Galois

Definizione 21.2 Sia G un gruppo. Una successione finita

$$1 = G_0 \triangleleft G_1 \triangleleft \ldots \triangleleft G_n = G$$

di sottogruppi normali è detta *serie subnormale di G*.

I quozienti $\frac{G_{i+1}}{G_i}$ sono detti *fattori* della serie.

Definizione 21.3 *Raffinare* una serie subnormale significa inserire tra due termini G_i e G_{i+1} un sottogruppo H di G tale che $G_i \triangleleft H \triangleleft G_{i+1}$.

Una serie non raffinabile si dice *serie di composizione*.

Attenzione: la normalità non è transitiva! Ovvero, se abbiamo una situazione del tipo $H \triangleleft K \triangleleft G$ non è detto che si abbia $H \triangleleft G$.

Definizione 21.4 Una serie subnormale si dice *abeliana* se tutti i fattori sono abeliani.

Definizione 21.5 Un gruppo che ammette una serie subnormale abeliana si dice *risolubile*.

Osservazione Ogni gruppo ha almeno una serie subnormale ($1 \triangleleft G$ funziona sempre), ma se è infinito non è detto che abbia una serie di composizione (ad esempio $(\mathbb{Z}, +)$ non ce l'ha).

Osservazione Una serie subnormale è di composizione $\iff$ i fattori sono tutti gruppi semplici.

Osservazione Nel caso di un gruppo finito risolubile, in ogni serie di composizione i fattori sono ciclici di ordine primo.

Osservazione G abeliano $\implies$ G risolubile, visto che $1 \triangleleft G$ è una serie abeliana.

Esempio 21.2 $G = S_3$, $1 \triangleleft S_3$ non è abeliana, ma possiamo raffinarla inserendo $1 \triangleleft A_3 \triangleleft S_3$.

I quozienti $\frac{A_3}{1}$ e $\frac{S_3}{A_3}$ ha ordini primi (3 e 2), quindi sono ciclici, quindi abeliani $\implies$ S_3 è risolubile.

Esempio 21.3 $G = S_4$, il ragionamento di prima non funziona: $1 \triangleleft S_4$ non è abeliana, $1 \triangleleft A_4 \triangleleft S_4$ non è abeliana.

Però A_4 contiene il **sottogruppo di Klein** $K = \{id, (12)(34), (13)(24) \triangleleft, (14)(23)\} \triangleleft A_4$, e raffinando la serie con K abbiamo $1 \triangleleft K \triangleleft A_4 \triangleleft S_4$ una serie abeliana $\implies S_4$ è risolubile.

Non solo, la serie si può raffinare ancora ottenendo $1 \triangleleft \{id, (12)(34)\} \triangleleft K \triangleleft A_4 \triangleleft S_4$, in cui i fattori hanno ordini 2,2,3,2.

Esempio 21.4 $G = S_n$, con $n \geq 5$. La serie $1 \triangleleft A_n \triangleleft S_n$ non si può raffinare, quindi è una serie di composizione (in realtà l'unica), e non è abeliana.

Questo deriva direttamente dal teorema di Galois: A_n è semplice $\forall n \geq 5$.

Quindi S_n, per $n \geq 5$, non è risolubile.

I gruppi risolubili, ideati da Galois poco prima della sua morte prematura, sono stati fondamentali per l'algebra a causa di un teorema rivoluzionario:

Teorema 21.1 (di Galois) *Una equazione $f(x) = 0$ è risolubile per radicali $\iff$ il suo gruppo di Galois G è risolubile.*

Il gruppo di Galois del generico polinomio di grado n è S_n. Dunque per $n \geq 5$ non è risolubile per radicali, ovvero non esiste una formula generale. Invece per $n \leq 4$ c'è e la conosciamo.

Capitolo 22

08/05/2014

22.1 Maggiori dettagli sulla teoria di Galois in $\mathbb{C}$

Oggi vedremo altri contenuti ritenuti rivoluzionari per tutta l'algebra che sono stati trovati negli appunti di Galois dopo la sua morte.

Prendiamo $f \in K[x]$ polinomio monico a radici distinte di grado $n \geq 2$, su K campo. Sia F il suo campo di spezzamento.

Tra K ed F ci sono sottocampi intermedi, cioè dei sottocampi H di F tali che $K \subseteq H \subseteq F$. Denotiamo con $[K, F]$ l'insieme di questi sottocampi, chiamato *intervallo* tra K ed F, che ordinato per inclusione è un reticolo con minimo K e massimo F.

Chiamiamo G il gruppo di Galois di f, ovvero $G = \{g \in Aut(F) \mid \forall x \in K \ g(x) = x\}$, e $l(G)$ il reticolo dei sottogruppi di G.

Si può dimostrare che $|G| = dim_K F$ è un divisore di $n!$.

Galois stabilì due funzioni tra i reticoli $l(G)$ e $[K, F]$:

$\forall H \in [K, F]$ sia $G_H = \{g \in G \mid \forall x \in H, \ g(x) = x\}$, allora G_H è un sottogruppo di G. Quindi possiamo definire la funzione

$$\begin{array}{rcl} [K, F] & \longrightarrow & l(G) \\ H & \longmapsto & G_H \end{array}$$

Inversamente, $\forall L \in l(G)$, ovvero L sottogruppo di G, sia $K_L = \{x \in F \mid \forall g \in L, \ g(x) = x\}$, allora K_L è un sottocampo di F. Quindi possiamo definire la funzione

$$\begin{array}{rcl} l(G) & \longrightarrow & [K, F] \\ L & \longmapsto & K_L \end{array}$$

Galois dimostra anche che le due funzioni sono una l'inversa dell'altra. Questo implica in particolare che esse sono bigezioni tra i due reticoli, da cui ricaviamo che $|l(G)| = |[K, F]|$.

Non solo, Galois dimostra anche che sono funzioni "decrescenti", ovvero $L_1 \subseteq L_2 \iff K_{L_2} \subseteq K_{L_1}$, ovvero sono isomorfismi tra i due reticoli.

C'è un'altra relazione più sottile trovata da Galois:

L_1 è sottogruppo normale di $L_2 \iff K_{L_1}$ è un ampliamento normale di K_{L_2}

Allora ad una serie subnormale $1 = G_0 \triangleleft G_1 \triangleleft \ldots \triangleleft G_m = G$ corrisponde una successione $K_m = K, K_{m-1}, \ldots, K_0 = F$ di sottocampi, ciascuno ampliamento normale del precedente.

Inoltre, se G è risolubile, ha una serie di composizione a fattori ciclici di ordine primo, la successione di sottocampi corrispondenti è fatta da ampliamenti di dimensione un numero primo.

Ossia, un polinomio irriducivile d'ordine primo il cui gruppo di Galois sia ciclico d'ordine primo è risolubile per radicali aventi per indice quel primo.

Pertanto, estraendo radici di ordine primo, a partire dai coefficienti si arriva ad una formula finale per radicali.

22.2 Regola di Cartesio per il trinomio

Prendiamo $ax^2 + bx + c = 0$, con $a \neq 0$ (supponiamo $a > 0$).

a	b	c
$+$	$+$	$+$
$+$	$-$	$+$
$+$	$+$	$-$
$+$	$-$	$-$

ogni sequenza $++$ o $--$ si dice *permanenza* e ogni sequenza $+-$ o $-+$ si dice *variazione*.

Se le radici sono reali, ad ogni variazione corrisponde una radice positiva, e ad ogni permanenza una negativa.

In più, solo nel primo e nel quarto caso è necessaria la realtà delle radici, dato che negli altri due si ha $\Delta > 0$.

Capitolo 23

15/05/2014

23.1 Riga e Compasso

Cosa vuol dire *costruire con riga e compasso*?

Cosa possiamo fare con gli strumenti *riga* e *compasso*?

Dati due punti A e B, possiamo fare due cose:

- Costruire la retta AB, o il segmento AB (riga).
- Costruire la circonferenza di centro A e passante per B (compasso)

Se ci mettiamo nel piano cartesiano, e denotiamo con K il minimo sottocampo di $\mathbb{R}$ che contiene le coordinate dei punti iniziali (in numero finito), possiamo considerare $A = (x_1, y_1)$, $B = (x_2, y_2) \in K^2$, e costruire

- Retta AB, che ha tre equazioni possibili:

$$x = x_1 \qquad y = y_1 \qquad \frac{y - y_1}{y_2 - y_1} = \frac{x - x_1}{x_2 - x_1}$$

  quindi con coefficienti tutti contenuti in K.

- Circonferenza di centro A e raggio AB, che ha equazione:

$$(x - x_1)^2 + (y - y_1)^2 = (x - x_2)^2 + (y - y_2)^2$$

  quindi di nuovo con coefficienti $\in K$.

- Intersezione di due rette a coefficienti in K.

  Facendo questo si risolve il sistema lineare delle loro equazioni, quindi la soluzione appartiene ancora a K^2.

- Intersezione di una retta e una circonferenza:
$$\begin{cases} x^2 + y^2 + \alpha x + \beta y + \gamma = 0 \\ ax + by + c = 0 \end{cases}$$
che si riconduce ad una equazione di secondo grado.
Le radici di questa equazione possono contenere (se Δ non è un quadrato in K) delle radici, per cui da K si va nel campo $K(\sqrt{\Delta})$.
$\sqrt{\Delta}$ ha come polinomio minimo (irriducibile) $x^2 - \Delta \in K[x]$, dunque l'ampliamento ha dimensione 2 su K ed è normale, perché contiene entrambi le radici $\pm\sqrt{\Delta}$.

- Intersezione di due circonferenze:
$$\begin{cases} x^2 + y^2 + \alpha x + \beta y + \gamma = 0 \\ x^2 + y^2 + \alpha' x + \beta' y + \gamma' = 0 \end{cases}$$
che ci riconduce di nuovo ad un ampliamento di grado 2, in modo analogo al caso precedente (visto che stiamo ancora lavorando su equazioni di secondo grado).

- Scelta di un punto su una retta: si può scegliere l'ascissa in K.

- Scelta di un punto su una circonferenza: si può scegliere un'ascissa in K, e la sua ordinata con eventuale radice quadrata.

Quindi, una costruzione con riga e compasso a partire da un numero finito di punti dati, a coordinate in un sottocampo K di $\mathbb{R}$, prevede una successione finita dei passaggi appena elencati.

Ciò comporta l'ampliamento successivo di K

$$K = K_0 < K_1 < \ldots < K_n = F$$

in cui $dim_{K_i} K_{i+1} = 2$, $K_{i+1} = K_i(\sqrt{\Delta_i})$, e sono tutti ampliamenti normali.

Conclusione: $dim_K F = 2^n$; il gruppo di Galois G di F rispetto a K ha ordine 2^n e ha una serie di composizione a fattori di ordine 2, quindi è risolubile.

Si dimostra che questa condizione è anche sufficiente.

Esempio 23.1 (Duplicazione del cubo) Un cubo di lato l ha volume l^3. Dato un cubo di lato $l = 1$, si può costruire con riga e compasso un cubo di lato x, in modo che il volume sia 2?

Per farlo dobbiamo costruire il numero x, che deve verificare $x^3 = 2$. Quindi per costruire x si deve estrarre $\sqrt[3]{2}$, che non è una radice quadrata.

Il campo di spezzamento di $x^3 - 2$ (polinomio minimo di $\sqrt[3]{2}$) ha dimensione 6 su $\mathbb{Q}$, quindi non si può fare con riga e compasso, poiché 6 non è una potenza di 2.

Seguendo la logica dell'esempio presentato, facciamo una lista di cose che si possono fare, o non fare, con riga e compasso:

1. Non si può costruire un segmento lungo come una circonferenza di diametro 1, poiché π è trascendente su $\mathbb{Q}$.

2. Non si può trisecare un angolo qualsiasi, con alcune eccezioni (angoli retti o piatti).

3. Si può costruire un poligono regolare con n lati inscritto in una circonferenza di raggio $1 \iff n = 2^k p$, con p primo del tipo $p = 2^{2^n} + 1$:[1]

n	0	1	2	3	4	???
p	3	5	17	257	65537	???

   Nota: i punti interrogativi sono lì perché ad oggi non si conoscono altri primi di quella forma, e per ora non si conoscono costruzioni esplicite del poligono regolare di 65537 lati.

[1] Un primo $p = 2^{2^n} + 1$ è detto *primo di Gauss*