Alma Mater Studiorum · Università di Bologna

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI
Corso di Laurea in Matematica

CONFRNTO TRA ALGEBRE MONOUNARIE E ALGEBRA UNIVERSALE

Tesi di Laurea in Algebra

Relatore:
Chiar.mo Prof.
LIBERO VERARDI

Presentata da:
ELENA GALBUCCI

terza sessione
Anno accademico 2009/2010

Indice

INTRODUZIONE

In una storia di fantascienza noi umani riceviamo un messaggio misterioso da intelligenze aliene. Forse la conversazione fra di loro languisce, ed hanno pensato di inviare i loro discorsi dal loro salotto al primo pianeta sconosciuto con cui ci si intenda. Ma su che base due intelligenze prese a caso nell'universo possono mai sperare di sintonizzarsi? Che cosa c'è nell'intersezione, nel nocciolo di tutte le intelligenze possibili? Che cosa si può prendere come stele di Rosetta cosmica? Finalmente il colpo di genio: il messaggio è una versione extraterrestre degli assiomi di Peano.

Giuseppe Peano nacque in una fattoria fuori Cuneo. Suo padre era un contadino e sua madre era una casalinga. Quando era un bambino, suo zio, che era un sacerdote, riconobbe che Peano era uno studente di talento e lo iscrisse in una scuola superiore che lo preparò per l'università. Dopo la laurea, si iscrisse all'Università di Torino, dove studiò la geometria analitica, algebra, calcolo, geometria descrittiva, l'analisi, la geometria, le altre classi avanzate e, infine, la meccanica. Nel 1880, Peano si laureò come doctor mathematicae. L'Università di Torino prontamente lo assunse. Peano pubblicò quattro articoli di matematica durante i due anni successivi. Nel 1884 conseguì il titolo di professore universitario a Torino e vi insegnò per tutto il resto della sua vita. Insegnò anche presso il vicino Accademico Militaire (Accademia Militare), dal 1895 fino al 1908. Fu eletto all'Accademia delle Scienze di Torino nel 1981 e fu relatore a numerosi Congressi Internazionali di Matematica. Una delle cose più famose per cui è noto sono i cinque assiomi, ora detti, di Peano.

In logica matematica, gli Assiomi di Peano, anche conosciuti come Assiomi di Dedekind-Peano o Postulati di Peano, sono un insieme di assiomi per i numeri naturali, elaborati nel diciannovesimo secolo.

L'esigenza di formalismo nell'aritmetica non era molto sentita fino al lavoro di Hermann Grassmann, che ha indicato nel 1860 che molti fatti nell'aritmetica potrebbero essere derivati dai fatti più fondamentali circa il funzionamento del successore e dell'induzione. Nel 1888, Richard Dedekind propose una collezione di assiomi su i numeri, e nel 1889 Peano ha pubblicato una loro versione, più precisamente formulata, come collezione di assiomi in suo libro.

Un modo informale di definire tali assiomi è:
1. Esiste un numero naturale, 0 .
2. Ogni numero naturale n ha un numero naturale successore, n + 1 .
3. Numeri naturali diversi hanno successori diversi.
4. 0 non è il successore di alcun numero naturale.
5. Ogni insieme di numeri naturali contenente lo zero e il successore di ogni proprio elemento coincide con l'intero insieme dei numeri naturali (Principio di induzione).

In termini più astratti, l'algebra descritta da Peano è del tipo: $(N, 0, \sigma)$ con
$\sigma : N \to N$ iniettiva , $Im(\sigma) = N\backslash\{0\}$, non ci sono sottoalgebre proprie.
(N, σ) è, cioè, un'*algebra monounaria*, con elemento iniziale 0 e priva di sottoalgebre proprie.

Scopo di questa tesi è proprio lo studio delle algebre monounarie poste a confronto con i gruppi e gli anelli.

Capitolo 1

DEFINIZIONI E PROPRIETÀ FONDAMENTALI DELLE ALGEBRE MONOUNARIE

Per prima cosa, definiamo un'algebra monounaria e vediamo come rappresentarle sia algebricamente sia geometricamente, almeno nel caso finito.

Definizione 1.1 :

Siano X un insieme[1] ed $f : X \to X$ un'applicazione. Se interpretiamo f come una operazione unaria su X, possiamo considerare la struttura algebrica (X,f), che chiameremo *algebra monounaria*.

Definizione 1.2:

Si chiama *ordine* dell'algebra (X,f) il numero cardinale $|X|$.
L'algebra si dice finita se $|X|$ è finito.

Osservazione 1.3 :

Se $|X|$=n, finito, ci sono n^n aplicazioni da X a se stesso, quindi n^n algebre monounarie diverse sullo stesso insieme sostegno.

[1] *Non escludiamo il caso dell'insieme vuoto, in esso il prodotto cartesiano $\emptyset \times \emptyset$ è un'applicazione, detta applicazione vuota ed è anche biiettiva. Ossia consiederiamo anche l'algebra monounaria banale $(\emptyset, \emptyset \times \emptyset)$*

RAPPRESENTAZIONI DI f

Sia f un'algebra monounaria. Se l'insieme sostegno X è finito con n elementi, possiamo rappresentare f come di consueto con una tabella che elenchi le coppie (x,f(x)).
Sia n≥1. Identificando X con l'insieme dei primi n numeri naturali non nulli, si può rappresentare f mediante la scrittura a due righe

$$\begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}$$

ridotta eventualmente alla lista

$$\begin{pmatrix} f(1), & \dots, & f(n) \end{pmatrix}$$

Si può anche usare la matrice $M_f = [m_{ij}]$ di ordine n, definita da

$$m_{ij} = \begin{cases} 1 & \text{se } f(i) = j \\ 0 & \text{altrimenti} \end{cases}$$

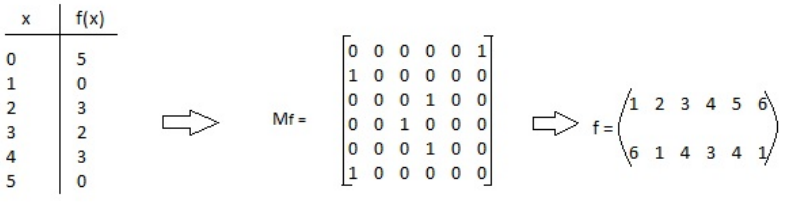
Essa è la *matrice d'incidenza* della relazione f tra X e se stesso.

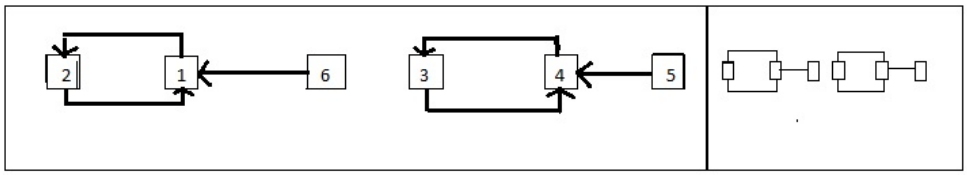
Un'altra rappresentazione assai utile delle algebre monounarie finite è la rappresentazione grafica. Essa consiste nell'associare ad un'algebra monounaria finita (X,f) un *grafo orientato* $\Gamma = \Gamma(X, f)$, i cui vertici sono gli elementi di X ed in cui $x \to y \Leftrightarrow y = f(x)$ e poiché f è una funzione, da ogni vertice esce una ed una sola freccia.
In particolare, partendo da un elemento $x_0 \in X$ ed applicando ripetutamente f, si ottiene una successione finita $x_0 \to x_1 = f(x_0) \to \dots \to x_{i+1} = f(x_i)$ dove l'ultimo termine uguaglia uno dei termini x_j già incontrati. Si genera così un *circuito* comprendente $x_j, x_{j+1}, \dots, x_i$ a cui è attaccato il *co-albero* $x_0, x_1, \dots, x_{j-1}$.
Ogni circuito può avere più accessi, ma non più uscite; più precisamente, ad ogni nodo di un circuito possono essere attaccati dei co-alberi attraverso il loro nodo terminale.

Quindi, più precisamente e riassumendo, il grafo $\Gamma(X, f)$ ha le seguenti caratteristiche:
a) Ogni vertice di Γ ha grado 1 in uscita.
b) I cappi sono i punti uniti di f.
c) I circuiti sono i cicli $C_{0,d}$, descritti più avanti

Inversamente, per ogni grafo Γ con la proprietà a), detto X l'insieme dei vertici e posto $y = f(x)$ se x è adiacente ad y (graficamente: $x \to y$), allora (X,f) è un'algebra monounaria e risulta $\Gamma = \Gamma(X, f)$.

Esempio: Sia data la funzione $f : Z_6 \to Z_6$, $f : x \to x^2 - 1$. L'algebra monounaria si può rappresentare nei vari modi seguenti, algebrici e geometrici. Sono mostrate in particolare due versioni del digrafo, una dettagliata ed una astratta.





Per ottenere la versione astratta si è seguita la seguente convenzione:
• i cicli sono orientati in senso antiorario,
• i co-alberi sono orientati verso il ciclo cui sono attaccati.
Per esigenze tipografiche, i nodi sono rappresentati da quadratini anzichè da cerchietti come più consueto.

Definizione 1.4 :

Due vertici x,y del digrafo sono detti *connessi* se esiste una sequenza finita $x = x_0, x_1, \ldots, x_n = y$ di vertici, ciascuno adiacente al successivo. In tal caso esiste al più un j tale che $x = x_0 \to x_1 \to \ldots \to x_j \leftarrow \ldots \leftarrow x_n = y$ dato che, altrimenti, da almeno un vertice dovrebbero uscire due frecce. Se si ha $x_0 \to x_1 \to \ldots \to x_n$ oppure $x_0 \leftarrow \ldots \leftarrow x_n$ si considera rispettivamente $j = n$ e $j = 0$. Posto ciò, la relazione di connessione C è una relazione d'equivalenza, le cui classi sono dette *componenti connesse*. Il rango r(f) dell'algebra (X,f) è il numero di tali componenti.

Definizione 1.5 :

Due algebre monounarie (X,f) ed (X',f') si dicono *isomorfe* se esiste $\phi : X \to X'$, biiettivo, tale che per ogni $x \in X$ si ha $\phi(f(x)) = f'(\phi(x))$.

Dal punto di vista geometrico, due grafi Γ e Γ' sono detti *isomorfi* se esiste una biezione φ tra i loro nodi, tale che per ogni coppia di nodi x, y di Γ si abbia: $x \to y \Leftrightarrow \varphi(x) \to \varphi(y)$. Ne segue la proposizione seguente.

Proposizione 1.6:

Due algebre monounarie (X, f) ed (X', f') sono isomorfe se e solo se lo sono i loro digrafi $\Gamma(X, f)$ e $\Gamma(X', f')$.

Siano ora m, d tali che $0 \leq m \leq \infty$, $1 \leq d \leq \infty$. Si denotano con $C_{m,d}$ le algebre monounarie isomorfe alle seguenti:
- Tipo $C_{\infty,\infty}$: (Z, σ), dove $\sigma(x) = x + 1$. La σ è biiettiva.
- Tipo $C_{0,\infty}$: (N, σ), dove N è l'insieme dei numeri naturali e $\sigma(x) = x + 1$. In questo caso σ è iniettiva, $Im(\sigma) = N \backslash 0$.
-Tipo $C_{m,d}$, $0 \leq m \leq \infty$, $1 \leq d < \infty$: $(x \in Z | -m \leq x \leq d-1, \psi)$ dove:

$$\psi(x) = \begin{cases} x+1 & \text{se } x < d-1 \\ 0 & \text{se } x = d-1 \end{cases}$$

Circa queste ultime, se $m = 0$, le algebre di tipo $C_{0,d}$ saranno dette cicli e in tal caso ψ è una permutazione ciclica di lunghezza d.
Se $m > 0$, allora 0 è l'unico elemento con due preimmagini. Sul sottoinsieme $0, \ldots, d-1$ l'applicazione ψ agisce come un ciclo di lunghezza d. In particolare, se $d = 1$ allora 0 è un *punto unito* per ψ. Si osservi che se $0 < m < \infty$ allora $Im(\psi) =$\{-m+1, ..., d-1\}, mentre se $m = \infty, \psi$ è suriettiva.

Le algebre $C_{m,\infty}$ del tipo $(\{x \in Z | -m \leq x\}, \sigma)$, dove $\sigma(x) = x + 1$, sono tutte isomorfe a $C_{0,\infty}$.

Dato n$\in$ N, n$\geq$2, il numero delle algebre monounarie di ordine n, a meno di isomorfismi, coincide col numero di digrafi d'ordine n, tali che ogni nodo ha grado 1 in uscita. in appendice sarà esaminato il caso di n=2,3,4.

Capitolo 2

CONFRONTO

La parte dell'algebra che studia le proprietà generali delle strutture algebriche si chiama Algebra Universale; è un settore della matematica come la Geometria Algebrica o l'Algebra Commutativa, ma ha lo scopo di delineare ciò che hanno in comune (definizioni, teoremi, costruzioni) i vari tipi di strutture algebriche.
In questo capitolo si presenteranno le proprietà generali delle strutture algebriche e si vedrà come diventeranno in particolare nel caso delle algebre monounarie.

2.1 RICHIAMI DI ALGEBRA

Definizione 2.1.1:

Siano A, B due insiemi; una *relazione* da A a B è un sottoinsieme R del prodotto cartesiano AxB.
Tra le relazioni, le più importanti sono le funzioni $f : A \to B$.

Definizione 2.1.2:

Un'operazione su un insieme X si chiama *binaria interna* se agisce su due fattori (binaria), è a valori in X (interna) ed è una funzione $f : X \times X \to X$, ossia ad ogni coppia ordinata di fattori associa uno ed un solo risultato.

Più in generale, un'*operazione n-aria*, n≥1, è una funzione $f : X^n \to X$ (dove $X^1 = X$ e se $n \geq 1, X^n = \underbrace{X \times X \times \cdots \times X}_{n \text{ volte}}$).

Per ragioni che si vedranno in seguito, è conveniente definire infine *operazione zero-aria* (o 0-aria) un elemento $x_0 \in X$.

Definizione 2.1.3:

Si chiama *operazione finitaria* su un insieme X un'operazione n-aria, con $n \geq 0$.
Le operazioni unarie sono dunque le funzioni $f : X \to X$.

2.2 STRUTTURA

Una struttura algebrica è una sequenza formata da un insieme e da una o più operazioni finitarie: (X,$f_1, f_2, \ldots, f_r$).

Definizione 2.2.1:

Siano M un insieme non vuoto ed e un suo elemento, sia poi $\cdot$ un'operazione di M binaria ed interna. La terna (M, $\cdot$, e) viene chiamata *monoide* se valgono le seguenti proprietà:

proprietà associativa: $a \cdot (b \cdot c) = (a \cdot b) \cdot c \ \forall \ a, b, c \in G$
elemento neutro e di $\cdot$: $\forall$a$\in$ M, $a \cdot e = e \cdot a = a$.

Esempi:

• L'insieme moltiplicativo dei numeri naturali (N, $\cdot$, 1), con 1 elemento neutro, è un monoide. Poichè l'operazione è commutativa, è detto commutativo.

• Sia X un insieme non vuoto; si consideri l'insieme di applicazioni X^X=$\{f, f : X \to X\}$.
Sia $\circ$ l'operazione composizione in X^X definita, $\forall$ f,g$\in$M(X), nel modo seguente:

$$f\circ g: X \to X \ , \ x \to (f\circ g)(x) = f(g(x))$$

Sia poi $id_x : X \to X$ la funzione identità. Allora (X^X, $\circ$, id_x) è un monoide. In generale, ossia per $|x| \geq 2$, non è commutativo.

Definizione 2.2.2:

Sia G un insieme non vuoto e sia $\cdot$ un'operazione di G binaria ed interna. (G,$\cdot$,1_G,σ) è un *gruppo* se l'operazione binaria $\cdot$ è associativa, 1_G ne è l'elemento neutro e ogni elemento x ha il simmetrico $x^{-1} = \sigma(x)$, dove con il simbolo σ si indica la funzione, cioè l'operazione unaria che ad ogni x associa il suo simmetrico x^{-1}. Tale funzione è biiettiva e coincide con la sua inversa. Se l'operazione $\cdot$ è commutativa il gruppo si dice *abeliano*. Solitamente un gruppo è indicato soltanto con (G, $\cdot$).

Esempi:

• L'insieme additivo dei numeri interi (Z,+) è un gruppo, di cui 0 è l'elemento neutro ed in cui ogni elemento x ha l'opposto -x.

• Si considerino l'insieme delle applicazioni biiettive di insiemi,
S(X)=$\{f, f : X \to X$ applicazione biiettiva$\}$, e l'operazione di composizione $\circ$ su S(X). Sappaiamo infatti che la composta di funzioni biiettive è biiettiva
(S(X), $\circ$) è un gruppo, detto *gruppo simmetrico* su X, in cui l'elemento neutro è l'identità id_x ed in cui l'inverso di f$\in S_X$ è la funzione inversa f^{-1}, anch'essa biiettiva.

Definizione 2.2.3:

Sia (G, $\cdot$) un gruppo. Si chiama *ordine* del gruppo la cardinalità dell'insieme G, che si denota con $|G|$.

Definizione 2.2.4:

Si chiama *anello* (associativo) una terna ordinata (A, +, $\cdot$) dove A è un insieme non vuoto, + e $\cdot$ sono operazioni binarie interne, (A, +) è un gruppo abeliano il cui elemento neutro è denotato con 0_A. Inoltre valgono:
proprietà associativa del prodotto: $x \cdot (y \cdot z) = (x \cdot y) \cdot z \ \forall x, y, z \in A$
proprietà distributiva del $\cdot$ *rispetto al* +: $x \cdot (y + z) = x \cdot y + x \cdot z \ \forall x, y, z \in A$

Inoltre, se esiste l'elemento neutro 1_A per il prodotto, si dice che A è un *anello unitario*, se il prodotto gode della proprietà commutativa A si dice *anello commutativo*.
Nel caso della struttura di anello unitario, la notazione generale è (A,+,$\cdot$, 0_A, 1_A, $-$) (dove - indica l'operazione unaria di opposto).
Di solito si usa la notazione abbreviata (A,+,$\cdot$, 1_A) che mette in luce sia la struttura (A,+) di gruppo, sia quella (A,$\cdot$, 1_A) di monoide.
Nel seguito, la parola anello designerà sempre un anello con unità.

Esempi:

• (Q,+,·,1), dove Q è l'insieme dei razionali, è un anello.

• Sia m∈ N, m>0 e sia $Z_m = \{0, 1, \ldots, m-1\}$.
In questo insieme si definiscano le seguenti operazioni:

· $x +_m y$= *resto della divisione di x+y per m*
· $x \mathsf{x}_m y$= *resto della divizione di xy per m.*

L'elemento neutro di $+_m$ è 0, quello per x_m è 1; l'opposto di x è m-x.

$(Z_m, +_m, \mathsf{x}_m, 1)$ è un anello, ed è commutativo.

Definizione 2.2.5:

Un anello (A,+,·, 1_A) è un *dominio d'integrità* se è commutativo e vale la legge di annullamento del prodotto: $\forall a, b \in A, a \cdot b = 0_A \Rightarrow a = 0_A$ oppure $b = 0_A$.

Esempio:

(Z, +, ·,1) con Z insieme dei numeri interi è un dominio d'integrità.

Definizione 2.2.6:

Un *campo* è un anello commutativo in cui tutti gli elementi diversi da 0 sono invertibili. Un campo di sostegno K si denota usualmente con (K,+,·).
Esempio:

(R, +, ·), con R insieme dei numeri reali, è un campo.

Definizione 2.2.7:

Sia L un insieme non vuoto, la terna (L, ∨, ∧) è un *reticolo* se ∨ e ∧ sono operazioni binarie associative, commutative e tali che per ogni a, b ∈ L si ha:

$$\begin{aligned} a \vee a = a \wedge a \quad & \text{(idempotenza delle due operazioni)} \\ a \vee (a \wedge b) = a = a \wedge (a \vee b) \quad & \text{(legge di assorbimento)} \end{aligned} .$$

Gli eventuali elementi neutri di ∨ ed ∧ si indicano rispettivamente con 0_L ed 1_L.

Un reticolo si dice *complementato* se ha gli elementi neutri e per ogni elemento x esiste un elemento x' tale che $x \vee x' = 1_L, x \wedge x' = 0_L$.

Un reticolo si dice *distributivo* se le due operazioni sono distributive l'una rispetto rispetto all'altra. Se è anche complementato, ogni suo elemento ha un solo complemento.

Un reticolo si dice, infine, *algebra di Boole* se è distributivo e complementato, e si indica in tal caso con $(A, \vee, \wedge, 0_A, 1_A, ')$.

Esempi di algebra di Boole sono:

• Siano X un insieme e $\wp$(X) l'insieme dei suoi sottoinsiemi, $(\wp(X), \cup, \cap, \emptyset, X, ')$ è un'algebra di Boole (indicando con Y' il complementare di un sottoinsieme Y di X).

• Sia D=$\{1, 2, 3, 5, 6, 10, 15, 30\}$ l'insieme dei divisori di 30; indicando con x' il quoziente 30/x, si ha che (D, MCD, mcm, 30, 1, ') è un'algebra di Boole.

2.3 SOTTOALGEBRE E SOTTOSTRUTTURE

SOTTOSTRUTTURA

Sia (X, ·) una struttura algebrica. Un sottinsieme Y di X si dice *chiuso* rispetto all'operazione se, ogni volta che si esegue l'operazione su elementi appartenenti ad Y, anche il risultato appartiene ad Y. In tal caso si può considerare l'operazione · ristretta a Y ed ottenere una nuova struttura algebrica (Y, ·).
Più in generale, data una struttura (X, f_1, f_2, …, f_r), una sua *sottostruttura* è costituita da un sottoinsieme Y di X, chiuso rispetto a tutte le operazioni di X, e dalle restrizioni ad Y delle operazioni di X. In tal caso, (Y,f_1,f_2,…,f_r) risulta una struttura dello stesso tipo di (X, f_1, f_2, …, f_r).

Definizione 2.3.1:

Siano (M, ·, e) un monoide e $T \subset M$, T è *sottomonoide* se vale:
e∈T;
∀a, b ∈T risulta $a \cdot b \subset T$.

Esempio:

(Q,$\cdot$, 1) è sottomonoide di (R,$\cdot$, 1).

Definizione 2.3.2:

Sia (G, $\cdot$, 1_G,σ) un gruppo, un *sottogruppo* è una struttura (H,$\cdot$, 1_G,σ), dove H è un sottoinsieme di G chiuso rispetto alle tre operazioni finitarie di G; in particolare H contiene 1_G e contiene il simmetrico di ogni suo elemento. Risulta quindi che (H,$\cdot$ 1_G,σ) è un gruppo e $1_H = 1_G$.

Esempio:

(Z,+) è sottogruppo di (Q, +).

Osservazione:

I sottogruppi *banali* di un gruppo (G, $\cdot$) sono $\{1_G\}$ e G.

Definizione 2.3.3:

Siano (A, +, $\cdot$) un anello unitario e S un sottoinsieme non vuoto di A; allora (S,+,$\cdot$) è un *sottoanello* dell'anello (A, +, $\cdot$) se valgono:
(S, +) sottogruppo di (A, +);
(S, $\cdot$,1_A) sottomonoide di (A, $\cdot$,1_A)

Esempio:

(Q,+,$\cdot$,1) è un sottoanello di (R,+,$\cdot$,1).

Definizione 2.3.4:

Un *sottoreticolo* di un reticolo (L, $\vee$, $\wedge$) è costituito da un sottoinsieme chiuso rispetto alle due operazioni $\vee$, $\wedge$.

Esempio:

L'insieme dei divisori di n è un sottoreticolo del reticolo (N, MCD, mcm).

SOTTOALGEBRE :

Nel caso delle algebre monounarie, una *sottoalgebra* di (X,f) è costituita da un sottoinsieme Y⊆X, *chiuso* rispetto ad f, ossia tale che per ogni $y \in Y$ si ha $f(y) \in Y$, ovvero f(Y)⊆Y ed è la coppia $(Y, f|_Y)$.

Esempi:

• Ogni componente connessa del grafo Γ(X) di un'algebra (X, f) è una sottoalgebra.

• Per ogni algebra (X,f), ∅ , X e Im(X) sono sottoalgebre; come di consueto, le prime due sono dette rispettivamente sottoalgebra *banale* e *impropria*.

NOTA:

Nel caso dei gruppi finiti, vale il seguente teorema:

Teorema di Lagrange:

L'ordine di ogni sottogruppo divide l'ordine del gruppo.

Questa proprietà vale anche per i sottoanelli, ma non è una proprietà universale, infatti, nelle algebre monounarie non vale in quanto: ∅ è una sottoalgebra, ma 0 non divide $|X|$.

Osservazioni:

a) Le algebre di tipo $C_{0,d}$ non hanno sottoalgebre proprie, e sono dette algebre *minimali*.

b) Ogni sottoalgebra dell'algebra $C_{0,\infty}$ che contenga lo zero è impropria; questo è quanto affermato dal principio d'induzione di Peano.

Reticolo delle sottostrutture

Lemma 2.3.5:

L'intersezione di una famiglia di sottoalgebre è una sottoalgebra.

Dimostrazione:

Siano $(X, f_1, f_2, \ldots, f_r)$ una struttura algebrica e Ω un insieme di sottostrutture. Per ogni i$\in \{1, 2, \ldots, r\}$ sia f_i operazione k-aria. Se k>0, siano $x_1, \ldots, x_k \in Y$ con Y= $\cap_{H\in\Omega} H$, e proviamo che f($x_1, \ldots, x_k$) $\in$Y; allora essi appartengono ad ogni H$\in \Omega$ e quindi, essendo H una sottostruttura di X, si ha f($x_1, \ldots, x_k$) $\in$H.
Ma allora f($x_1, \ldots, x_k$) $\in \cap_{H\in\Omega} H$.

Se k=0, f_i è un elemento u di X: poichè ogni H è una sottostruttura, si ha u$\in$H, quindi u$\in$Y. Pertanto, Y è chiuso rispetto a tutte le operazioni $f_1, \ldots, f_r$ ed è una sottostruttura.

Nell'algebra universale non è vero in generale per l'unione, infatti, prendendo il monoide (N, +, 0) si considerino i due sottomonoidi 2N e 3N costituiti dai numeri pari e dai multipli di 3; l'intersezione è l'insieme 6N, insieme dei multipli di 6 ed è un sottomonoide di (N, +, 0), mentre l'unione è l'insieme: $\{0, 2, 3, 4, 6, 8, 9, 10, 12, 14, \ldots\}$ e questo insieme non è chiuso rispetto all'addizione, quindi non è un sottomonoide.
Nelle algebre monounarie, invece, l'unione di una famiglia di sottoalgebre è una sottoalgebra.

Definizione 2.3.6:

Siano (X,$f_1, \ldots, f_n$) ed S$\subseteq$X. La sottoalgebra generata da S è l'intersezione delle sottoalgebre che contengono S e si denota con $\langle S \rangle$.

Date ora due sottostrutture H e K di X, si definisca la *sottostruttura somma* di H e K la sottostruttura $\langle H \cup K \rangle$ generata dall'unione insiemistica di H e K; ne segue che $\mathcal{L}$(X), insieme delle sottostrutture della struttura X, è un reticolo ed è *completo*, nel senso che ogni ogni sottoinsieme non vuoto possiede estremi superiore ed inferiore.
Quindi, a partire da ogni struttura algebrica è possibile costruire un reticolo, il *reticolo delle sottostrutture*. Esso, nell'algebra universale, non è in generale un sottoreticolo di $(\wp(X), \cup, \cap)$, poichè $\mathcal{L}$(X) non è chiuso rispetto all'unione, ma solo rispetto all'intersezione, come dice il lemma precedente.

Nell'algebra monounaria, invece, dato che sia l'unione, sia l'intersezione di una famiglia qualunque di sottoalgebre è sottoalgebra, risulta che il reticolo delle sottoalgebre $\mathcal{L}(X, f)$ è un sottoreticolo completo del reticolo $(\mathcal{P}(X), \cap, \cup)$ dei sottoinsieme di X.

Nel caso dei gruppi, l'intersezione di tutti i sottogruppi è il sottogruppo banale $\{1_G\}$ costituito dal solo elemento neutro.
Nel caso degli anelli è il *sottoanello fondamentale*, costituito dai multipli interi di 1_A.
Nel caso delle algebre monounarie, l'intersezione di tutte le sottoalgebre è l'algebra vuota.

Vediamo ora per quali f può accadere che $\mathcal{L}$(X,f) sia un'algebra di Boole; si ha:

Teorema 2.3.7:

a) Se $\mathcal{L}$(X,f) è un'algebra di Boole allora f è biiettiva.
b) Se f è biiettiva di periodo finito nel gruppo simmetrico su X, allora $\mathcal{L}$(X,f) è un'algebra di Boole.

Corollario 2.3.8:

Sia X un insieme finito e sia f: X→X. Allora f è una permutazione di X se e solo se $\mathcal{L}$(X,f) è un'algebra di Boole.

Osservazione:

Nell'algebra (Z, σ) in cui si ha $\sigma : Z \to Z$, σ(x)=x+1, σ ha periodo infinito e le sottoalgebre di (Z,σ) sono solo quelle cicliche. Pertanto, pur essendo σ biiettiva, $\mathcal{L}(Z, \sigma)$ non è un'algebra di Boole.

Definizione 2.3.9:

Si dice *catena* un insieme totalmente ordinato.

È noto che il reticolo dei sottogruppi di un gruppo finito G è una catena se e solo se G è un p-gruppo ciclico, ossia $|G| = p^n$, p primo e G ciclico.

Nell'algebra monounaria si ha:

Teorema 2.3.10:

Se $\mathcal{L}(X, f)$ è totalmente ordinato, allora (X,f) è uno dei tipi seguenti:

1) Se f non è suriettiva, (X,f) è ciclica, ossia di tipo $C_{0,\infty}$ o $C_{m,d}$, m>0.

2) Se f è suriettiva, allora (X,f) è di tipo $C_{0,d}$, $C_{\infty,\infty}$ oppure $C_{\infty,n}$.

2.4 SOTTOALGEBRE GENERATE DA UN ELEMENTO

Nelle sottoalgebre generate, considerato come in precedenza S⊆X, importante è il caso in cui S=$\{x\}$, formato da un solo elemento; in tal caso la sottoalgebra generata da S si dice *1-generata*.

Nel caso dei gruppi, il sottogruppo $< a >$ è detto *sottogruppo ciclico* e si ha
$< a >= \{a^k | k \in Z\}$.
G si dice ciclico se è generato da un suo elemento, ossia se esiste b ∈ G, tale che G=$< b >$.

Esempio:

Il gruppo additivo (Z,+) è generato da 1

Nota:

In notazione additiva, il sottogruppo ciclico generato da un elemento diventa:
$< a >= \{a \cdot k | k \in Z\}$.

Si può aggiungere che, richiamando il teoreme di Lagrange, una sua conseguenza immediata risulta essere:

Se G ha ordine primo, G è necessariamente ciclico.

Nel caso degli anelli, Sia (A,+,·, 1_A) un anello, $< 1_A >$ è il *sottoanello fondamentale*, isomorfo a Z o a qualche Z_n; mentre per ogni x∈ A non multiplo di 1_A risulta:

$$< x >= \{\sum_{k=0}^{m} a_k x^k, a_k \in Z, m \in N\}$$

.

Nell'algebra monounaria, per ogni $x \in X$, la minima sottoalgebra che contiene x viene denotata con $\langle x \rangle$, ed è detta sottoalgebra 1-generata.
Ora, posto $x_0 = x$ e, per induzione, $x_{x+1} = f(x_n)$ per ogni $n \geq 0$, si ha subito: $\langle x \rangle = \{x_n | n \in N\}$. In particolare, ogni sottoalgebra Y è unione di sottoalgebre 1-generate, in quanto se Y è sottoalgebra ed $x \in Y$ allora per ogni $n \in N$ si ha $x_n = f^n(x) \in Y$.
Inoltre, per ogni x, si ha $|\langle x \rangle \setminus Im(f)| \leq 1$. Vediamo ora la loro struttura.

Proposizione 2.4.1:

Siano dati l'algebra monounaria (X,f) ed $x \in X$. Allora sono possibili per $\langle x \rangle$ i due casi seguenti:
a) Se $\langle x \rangle$ è infinito, è di tipo $C_{0,\infty}$.
b) Se $\langle x \rangle$ è finito, è di tipo $C_{m,d}$, con m,d finiti.

Fra le sottoalgebre 1-generate ci sono quelle di tipo $C_{0,1}$, ossia i singoletti $\{x\}$ in cui x è un elemento *unito* per f.

2.5 CONGRUENZE

Sia nelle algebre monounarie, sia in algebra universale si definisce *congruenza* una particolare *relazione d'equivalenza* compatibile con le operazioni, dove una relazione d'equivalenza è una relazione R su un insieme X che gode delle proprietà *riflessiva*, *simmetrica* e *transitiva*.

Nell'algebra universale, data una struttura con un'operazione binaria (X, $\cdot$), una relazione d'equivalenza $\sim$ in X si dice congruenza rispetto a $\cdot$ se dati a, b, a', b' $\in$ X, dall'essere $a \sim a'$, $b \sim b'$ segue $a \cdot b \sim a' \cdot b'$. Si indichi con [x] la classe di equivalenza di x, ossia $[x] = \{y \in X | y \sim x\}$ e si consideri l'insieme quoziente $X/\sim$ costituito dalle classi di equivalenza. Definita tra le classi l'operazione seguente: per ogni a,b $\in$ X, $[a] \cdot [b] = [a \cdot b]$, si ottiene una nuova struttura $(X/\sim, \cdot)$, detta *struttura quoziente* di X rispetto alla congruenza $\sim$.
Più in generale, data una struttura algebrica (X,$f_1, \ldots, f_n$), una relazione $\sim$ d'equivalenza è una congruenza se è compatibile con tutte le operazioni $f_1, \ldots, f_n$ (per le operazioni 0-arie è sempre vero).
Si ottiene così la struttura quoziente di X rispetto a $\sim$.

Definizione 2.5.1:

Una partizione di X è una congruenza se è tale la relazione d'equivalenza ad essa associata.
Vediamo ora alcuni esempi nelle algebre monounarie.

Esempi:

• Esempi ovvi di congruenze sono l'identità (o *congruenza discreta*) e il prodotto cartesiano XxX (o *congruenza banale*).
Ciò è vero in ogni struttura algebrica.

• Si ponga $x \sim_f x'$ se f(x)=f(x'). Questa relazione, detta *nucleo* di f, è una congruenza per f.

• La partizione $\{Im(f), X \backslash Im(f)\}$ è una congruenza. Più in generale, per ogni partizione $\mathcal{B}$ di $X \backslash Im(f)$, la partizione $\mathcal{B} \cup \{Im(f)\}$ è una congruenza. Infatti, se x e x' stanno nello stesso blocco, anche f(x) ed f(x') stanno nello stesso blocco Im(f).
• La partizione in componenti connesse del digrafo Γ(X) è una congruenza.

Importante è il caso dei gruppi; sia G un gruppo e sia $\mathcal{R}$ una relazione di equivalenza su G, compatibile con il prodotto di G, cioè tale che, se $a\mathcal{R}a'$ e $b\mathcal{R}b'$, allora $aa'\mathcal{R}bb'$.
L'insieme delle classi di equivalenza di $\mathcal{R}$, con il prodotto definito da $[a] \cdot [b] = [ab]$, è il *gruppo quoziente*, ed è denotato con $G/\mathcal{R}$. L'elemento neutro di $G/\mathcal{R}$ è $[1_G]$, e per ogni $[a] \in G/\mathcal{R}$ l'inverso di $[a]$ è $[a^{-1}]$.

Esempi:

• Data una congruenza $\sim$ in un gruppo G, la classe K contenente l'elemento neutro 1_G è un sottogruppo di G ed è *normale* in G, ossia tale che $\forall$ x $\in$ G, posto xK=$\{xk|k \in K\}$ e Kx=$\{kx|k \in K\}$, si ha che xK=Kx. Non solo, ma la classe di equivalenza [x] di x coincide con Kx e la congruenza data coincide con la relazione $x\mathcal{R}y \Leftrightarrow x \cdot y^{-1} \in K$.
Inversamente, per ogni sottogruppo K normale in G la relazione $x\mathcal{R}y \Leftrightarrow x \cdot y^{-1} \in K$ è una congruenza, di cui K è la classe contenente l'elemento neutro e per ogni x si ha che [x]=Kx.
Pertanto, le congruenze nei gruppi sono completamente descritte dai sottogruppi normali e ciascuno di essi individua una ed una sola congruenza, le cui classi sono i suoi laterali.

Il *gruppo quoziente* di G rispetto alla congruenza associata al sottogruppo normale K si denota con G/K.
Nel caso di gruppi abeliani, tutti i sottogruppi sono normali, perciò si può determinare il gruppo quoziente rispetto ad ogni sottogruppo.

• Nel gruppo (Z, +) si considerino il numero m$\geq$1 ed il sottogruppo ciclico $< m >$ generato da m ed indicato con mZ.
La relazione d'equivalenza associata è la *congruenza modulo m*: si ha x$\equiv$y (mod m) se e solo se x-y $\in$ mZ, ovvero se e solo se x-y è multiplo di m.
Le classi di equivalenza sono le *classi di resti modulo m*. L'insieme quoziente Z/mZ ha come elementi le classi [0], [1], ..., [m-1].
Si può verificare che la congruenza modulo m in Z è una congruenza anche rispetto alla moltiplicazione; essa dunque consente di ottenere l'anello quoziente z/mz, che risulta isomorfo all'anello Z_m.

• Sia (A, +, ·, 1_A) un anello e I un suo *ideale*, dove I si dice ideale se è sottogruppo di (A,+) e se per ogni i∈I e se per ogni x∈A si ha $x \cdot i \in I$ e $i \cdot x \in I$.
La relazione $x \sim_I y \Leftrightarrow x - y \in I$ è una congruenza nell'anello, nella quale la classe di 0_A è I e la classe di un elemento a è a+I=$\{a + i | i \in I\}$. Inversamente, data una congruenza $\sim$ in A, posto I=$[0_A]_\sim$, I è un ideale e si ha $\sim=\sim_I$. Pertanto, le congruenze negli anelli sono completamente descritte dagli ideali.

Definizione 3.5.2:

Una struttura algebrica si dice *semplice* se le sole congruenze sono quelle ovvie.

Nel caso dei gruppi, come detto in precedenza, le congruenze sono determinate dai sottogruppi normali; in particolare l'identità è associata al sottogruppo $\{1_G\}$, mentre il prodotto cartesiano è associato a G. Pertanto, il gruppo G è semplice se e solo se i soli suoi sottogruppi normali sono 1_G e G.

Esempi:

• I gruppi di ordine primo sono gruppi semplici e sono gli unici gruppi semplici abeliani.

• Altro importante esempio di gruppi semplici sono i gruppi alterni A_n con n>4, dove il gruppo alterno è l'insieme delle permutazioni di α con segno 1, cioè l'insieme delle permutazioni pari.
(Le permutazioni sono gli elementi del gruppo simmetrico S_n.)

Nel caso di un anello A, l'essere semplice equivale a non possedere altri ideali all'infuori di $\{0_A\}$ e A stesso.

Esempi:

• I campi sono anelli semplici e sono gli unici anelli semplici commutativi.

• Altri importanti anelli semplici sono gli anelli di matrici quadrate ad elementi in un campo.

Nell'algebra monounaria (X,f) una *congruenza* $\sim$ è una relazione d'equivalenza tale che, per ogni x, $x' \in X$, se $x \sim x'$ allora $f(x) \sim f(x')$.
Nell'insieme quoziente $X/\sim$ è possibile definire l'operazione monounaria quoziente $f_\sim$ definita da $f_\sim([x]) = [f(x)]$.

Teorema 2.5.3:

Un'algebra monounaria (X,f) è semplice se e solo se è di tipo $C_{0,p}$, con p primo.

Negli anelli e nei monoidi si dà la nozione di ideale, che in generale non è una sottostruttura.
Nei gruppi questa nozione non c'è, ma c'è quella di sottogruppo normale, definita in precedenza, e che si può tradurre nel modo seguente: in una congruenza, è la classe dell'elemento neutro, ed è l'unica classe, che sia una sottogruppo.

In analogia, si potrebbe definire ideale di una congruenza $\sim$ di (X,f) una classe che sia una sottoalgebra.

Tuttavia, nelle algebre monounarie si ha:

Teorema 2.5.4:

Per ogni sottoalgebra Y di X esiste una congruenza $\sim$ rispetto alla quale Y è un ideale.

dimostrazione:

Sia $x_1 \sim x_2$ se:

a) $x_1, x_2 \in Y$
b) $x_1, x_2 \notin Y$ e $x_1 = x_2$

Allora $\forall x_1, x_2 \in X$, $x_1 \sim x_2$: nel caso a) si ha $f(x_1)$ ed $f_{x_2} \in Y$, quindi $f(x_1) \sim f(x_2)$
nel caso b) ovviamente $f(x_1) = f(x_2)$, quindi $f(x_1) \sim f(x_2)$.
Dunque $\sim$ è una congruenza e Y è una sua classe, quindi è un ideale di $\sim$.

Altra stranezza: la partizione in componenti connesse è una congruenza, ed ogni componente connessa è sottoalgebra.
Ecco che abbiamo un esempio di congruenza in cui ogni classe è un ideale.

2.6 OMOMORFISMI

Riprendiamo la definizione di *omomorfismo* nell'algebra monounaria e nell'algebra universale.

Definizione 2.6.1:

Un *omomorfismo* fra due algebre monounarie (X,f) ed (X',f') è un'applicazione $\psi : X \to X'$, tale che per ogni $x \in X$ si ha $\psi(f(x)) = f(\psi(x))$.

Definizione 2.6.2:

Date due strutture (X, *) e (Y, $\cdot$), si chiama *omomorfismo* una funzione $\Phi : X \to Y$ tale che per ogni coppia a, b di elementi di X risulti $\Phi(a * b) = \Phi(a) \cdot \Phi(b)$.
Un omomorfismo biiettivo si chiama *isomorfismo* e, in tal caso, anche l'inversa f^{-1} di f è un isomorfismo.
Un omorfismo suriettivo si chiama *epimorfismo* e in tal caso si dice che Y è *immagine omomorfa* di X. Un omorfismo iniettivo si chiama *monomorfismo* (o *immersione*) di X in Y e Y si chiama *estensione* di X.
Più in generale si definisce omomorfismo tra due strutture algebriche (X, f_1, f_2, ..., f_r) e (Y, g_1, g_2, ..., g_r) dello stesso tipo, una funzione $\Phi : X \to Y$ tale che sia omomorfismo tra (X, f_i) e (Y, g_i) per ogni $i = 1, 2, \ldots, r$. In tal caso, l'immagine Φ(X) è una sottostruttura di Y.

Esempio:

Tra (X,$\cdot$) e $(X/\sim, \cdot)$ vi è un epimorfismo, che si chiama *proiezione canonica*, $\pi : X \to X/\sim$, tale che $\pi(x) = [x]$ per ogni x$\in$X.

OMOMORFISMO DI GRUPPI

Siano (G$*$) e (G',$\cdot$) due gruppi.
Si dice che un'applicazione di insiemi f:$G \to G'$ è un omomorfismo di gruppi se vale f(a$*$b)=f(a)$\cdot$f(b).

Questo perchè automaticamente si ha $f(1_G) = 1_{G'}$ e $f(x^{-1}) = f(x)^{-1}$.

OMOMORFISMO DI ANELLI

Siano A, A' due anelli.
Si dice che f:A$\to$A' è un omomorfismo di anelli se vale, $\forall a, b \in A$:

$\cdot$ f:(A,+)$\to$(A',+) è un omomorfismo di gruppi, ossia $f(a + b) = f(a) + f(b)$
$\cdot$ f(ab)=f(a)f(b)
$\cdot$ f(1_A)=$1_{A'}$

C'è una connessione tra omomorfismi e congruenze, come prova il noto teorema fondamentale d'omomorfismo.

Teorema 2.6.3:

Siano X ed Y due strutture dello stesso tipo ed f un omomorfismo tra di esse; risulta:
a) L'immagine Im f è una sottostruttura di Y.
b) La relazione $\sim_f$ così definita, per ogni a, b $\in$ X: $a \sim_f b$ se $f(a) = f(b)$, è una congruenza.
c) Detta [x] la classe di equivalenza di x, la funzione $\pi : X \to X/\sim_f$ tale che $\pi(x) = [x]$, è un epimorfismo.
d) Ponendo: $F([x]) = f(x)$, è ben definita la funzione F da $X/\sim_f$ ad Y, la cui immagine coincide con quella di f e che risulta un monomofismo.
e) Risulta: $f = F \circ \pi$, ed F è la sola funzione da $X/\sim_f$ ad Y che ha questa proprietà.
f) Se f è un epimorfismo, F è un isomorfismo tra $X/\sim_f$ ed Y.

Nel caso particolare di un omomorfismo $f : G \to H$ fra due gruppi G ed H, la congruenza $\sim_f$ dà luogo in G ad un sottogruppo normale K = ker f, detto *nucleo* di f (mentre nell'algebra monounaria il concetto di nucleo non è presente in questa forma).

Il nucleo costituisce la classe dell'elemento neutro; più esplicitamente, si ha ker f = $\{x \in G | f(x) = 1_H\}$. Le altre classi sono i suoi laterali, così che il teorema precedente si riformula nel modo seguente :

Teorema 2.6.4:

Dati due gruppi G ed H ed un omomorfismo $f : G \to H$ tra di essi:
a) l'immagine Im f è un sottogruppo di H;
b) Il nucleo Ker f è un sottogruppo normale di G;
c) G/Ker f è isomorfo ad Im f;
d) f è un monomorfismo se e solo se ker f = $\{1_G\}$.

Nota:

Nel caso degli anelli, la formulazione del teorema fondamentale di omomorfismo è sostanzialmente simile a quella dei gruppi, solo che Ker f è ora un ideale; risulta quindi:

Dati due anelli A ed B ed un omomorfismo $f : A \to B$ tra di essi:
a) l'immagine Im f è un sottoanello di H;
b) Il nucleo Ker f = $\{x \in A | f(x) = 0_B\}$ è un ideale di A;
c) A/Ker f è isomorfo ad Im f;

d) f è un monomorfismo se e solo se ker f = $\{0_A\}$.

2.7 GRUPPO DEGLI AUTOMORFISMI

Nell'algebra universale, gli omorfismi tra una struttura algebrica e se stessa si chiamano *endomorfismi*, e formano il sottomonoide End(X) del monoide $(X^X, \circ, id_X)$ delle funzioni da X ad X. Gli isomorfismi tra la struttura X e se stessa si chiamano *automorfismi*, e formano il gruppo delle unità di End(X). Tale gruppo si denota di solito con Aut(X), è un sottogruppo del gruppo simmetrico S_X (gli elementi di S_X sono le biezioni da X in sé) e viene detto *automorfo* di X.
Dunque, a partire da ogni struttura algebrica è possibile costruire il gruppo degli automorfismi della struttura.

Esempi:

• Aut(Z, +) possiede due soli elementi: l'identità e la funzione σ che ad ogni x associa l'opposto -x. Invece. Aut(Z, +, ·, 1) è costituito solo dall'identità.

• Più in generale, se G è un gruppo ciclico, si prova facilmente che, posto D=$\{y \in G | \langle y \rangle = G\}$, allora $|Aut(G)| = |D|$. Infatti, sia g un fissato generatore di G. $\forall y \in D, \forall k \in Z$, poniamo $f_y : G \to G, f_y(g^k) = y^k$. Si prova subito che f_y è una funzione e che appartiene ad Aut(G). Inversamente, se f è automorfismo, posto y=f(g) si ha f=f_y. Pertanto, $|Aut(G)| = |D|$. In particolare, come detto, se G $\cong$ Z allora $|Aut(G)| = 2$; se $G \cong Z_n$ allora D=$(Z)^* = \{x \in Z_n | \exists x^{-1}\} = \{x \in Z_n | (x, n) = 1\}$ e quindi $Aut(G) \cong (Z_n)^*$ ha $\varphi(n)$ elementi, dove φ è la funzione di Eulero.

• Il campo reale ha solo l'automorfo banale. Infatti, per cominciare, se f è un automorfismo del campo R, allora f(1)=1, quindi per ogni $m \in N$ si ha f(m) = f($\sum_{i=0}^{m} 1$)=$\sum_{i=0}^{m} f(1) = m \cdot 1 = m$. Ma allora si ha anche f(-m) = -m e, in definitiva, per ogni numero razionale $\frac{m}{n}$ si ha $f(\frac{m}{n}) = \frac{f(m)}{f(n)} = \frac{m}{n}$ e quindi f induce l'identità sui razionali. Inoltre, $\forall x > 0 \Rightarrow \exists y \in R$ tale che $x = y^2$, quindi $f(x) = f(y^2) = (f(y))^2 \Rightarrow f(x) > 0$. Pertanto. f conserva l'ordinamento di R. Ne viene che, essendo Q denso in R, allora f è l'identità anche su R.

Analogamente, nell'algebra monounaria, l'insieme degli automorfismi di (X,f) è un sottogruppo del gruppo simmetrico di X e si denota con Aut(X,f) e si chiama *automorfo* di (X, f).

Sia ora G = Aut(X, f); ogni $g \in G$ conserva $Im(f^m)$ per ogni m≥0, ossia, $Im(f^m)$ è G-invariante. Inoltre, ogni $g \in G$ permuta le sottoalgebre minimali e quelle massimali (sottoalgebre incluse propriamente solo in X). Similmente, anche l'insieme dei punti fissi Fix(X, f) è G-invariante. Infine, per ogni $g \in G$, le orbite di g, definite subito in seguito, danno luogo ad una congruenza, ossia se y = $g^k(x)$ allora f(y) = $f(g^k(x)) = g^k(f(x))$.
Ma G coincide con l'automorfo del grafo $\Gamma(X, f)$; pertanto ogni $g \in G$ conserva le adiacenze e le distanze e permuta le componenti connesse.

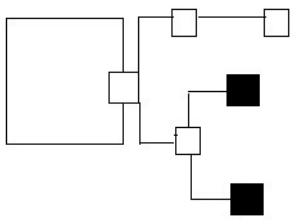
Se G è un gruppo finito, in generale non esiste un'algebra monounaria di cui G sia l'automorfo, perchè G ha una struttura di tipo particolare.
Tuttavia, se G è abeliano, la questione cambia, infatti:

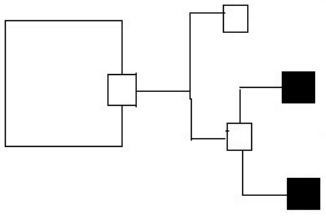
Lemma 2.7.1:

Sia G un gruppo finito e sia (X,f) un'algebra monounaria connessa di cui G è l'automorfo. Allora esistono infinite algebre a due a due non isomorfe di cui G è l'automorfo.

Esempio:

Grafo di due algebre con lo stesso automorfo.





In entrambi i casi, l'unico automorfismo diverso dall'identità scambia i due nodi colorati. I due grafi non sono però isomorfi perchè hanno un numero diverso di nodi.

Lemma 2.7.2:

Siano G ed H due gruppi che sono automorfi di algebre monounarie, allora lo è anche il loro *prodotto diretto*; dove il prodotto diretto è definito nel modo seguente:

siano (G,·) e (G',∗) due gruppi con 1 e 1' elementi neutri corrispondenti.
Il prodotto diretto di G e G' è :

(GxG)x(GxG')→(GxG')
((a,b)x(c,d))→(a·c,b∗d)

Lemma 2.7.3

Ogni gruppo ciclico finito G è l'automorfo di un'algebra $C_{n,0}$, $n = |G|$.

Lemma 2.7.4

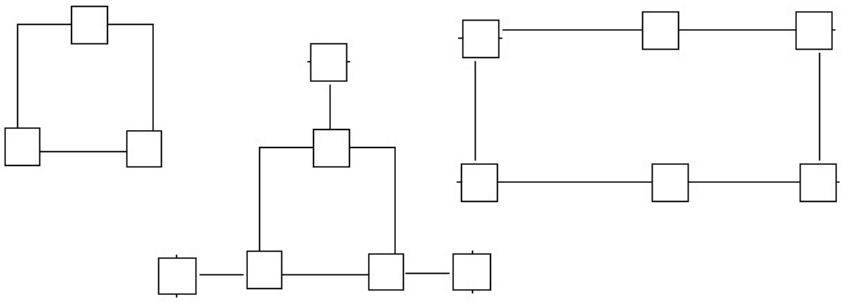
Ogni gruppo abeliano finito è prodotto diretto di gruppi ciclici (cfr. [3], p93).

Teorema 2.7.5:

Sia G abeliano, allora esiste un'algebra monounaria (X,f) di cui G è l'automorfo.

Esempio:

Grafo di algebra con automorfo $\cong Z_6 \mathrm{x} (Z_3)^2$.



2.8 PRODOTTO DIRETTO

Come per i gruppi, date due strutture algebriche dello stesso tipo (X,$f_1 \ldots, f_n$) e (Y,$g_1, \ldots, g_n$) si può definire una nuova struttura dello stesso tipo avente come sostegno X×Y e tale che, se f_i e g_i sono operazioni k-arie, k≥1, $f_i \times g_i : ((x_1), \ldots, (x_k, y_k)) = ((f_i(x_1, \ldots, x_k), g_i(y_1, \ldots, y_k)) \in X \times Y$.
Se sono elementi di X e Y (0-arie) allora $f_i \times g_i = (f_i, g_i) \in X \times Y$.

Il prodotto diretto conserva le proprietà universali, ossia quelle che valgono per ogni elemento di X e di Y, pertanto il prodotto diretto di gruppi è un gruppo, e se sono abeliani è abeliano; il prodotto diretto di anelli è un anello, e se sono commutativi è commutativo.

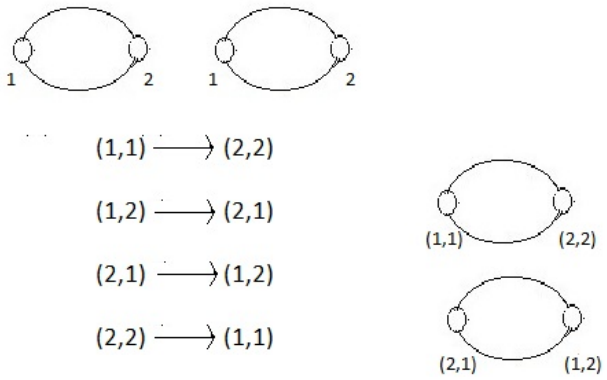
Invece, le proprietà in cui è posta qualche condizione o eccezione non valgono.
Per esempio, se G ed H sono ciclici, non è detto che G×H lo sia; se A e B sono domini d'integrità, A×B non è mai un dominio d'integrità; perchè non vale la legge d'annullamento del prodotto: $(0_A, 1_B)\cdot(1_A, 0_B) = (0_A, 0_B)$, dove $(0_A, 1_B), (1_A, 0_B), (0_A, 0_B) \neq 0_{A\times B}$

Il prodotto diretto di algebre monounarie è un'algebra monounaria.
Una proprietà importante è la seguente:

Teorema 2.8.1:

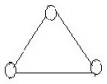
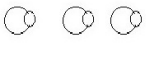
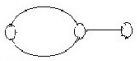
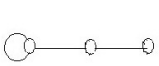
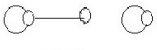
Se le funzioni sono entrambe biiettive, anche il prodotto diretto lo è.
Invece, la connessione non si conserva per prodotti diretti.

Esempio:



In questo esempio si mostra un prodotto diretto di due connessi che è sconnesso.

Appendice A

ORDINE	GRUPPI	ANELLI	ALGEBRE MONO-UNARIE
1	Gruppo banale	Anello banale (0=1)	({1},id) 
2	$Z_2 \simeq S_2$ aut = 1l	Z_2 (campo) aut = 1l	 ({1,2},(1 2))  ({1,2},id)  ({1,2},f) $f = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} \simeq \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}$
3	Z_3 aut $\simeq Z_2$	Z_3 (campo) aut = 1l	 aut $\simeq Z_3$  aut $\simeq Z_2$  aut $\simeq S_3$  aut = 1l  aut = 1l  aut $\simeq S_2$  aut = 1l

È noto che ci sono due gruppi di ordine 4 (Z_4 e $Z_2 \times Z_2$), tre anelli (Z_4, $Z_2 \times Z_2$ e GF(4)

campo di ordine 4), mentre ci sono diciannove algebre monounarie delle quali nove sono connesse.

CONCLUSIONE

In questa tesi ho rivisto le strutture, enunciati e proprietà generali dell'algebra universale, richiamando concetti incontrati nel corso della laurea triennale e adattati al caso delle algebre monounarie.
Si è partiti dalla definizione di queste ultime, presentandone anche rappresentazioni algebriche, grafiche, ed il concetto d'isomorfismo.
Si considerano poi la la definizione generale di struttura algebrica, con un breve richiamo ai gruppi, agli anelli ed ai reticoli.
Si passa poi ad esaminare e ad adattare ai vari tipi di strutture, comprese le algebre monounarie, le principali nozioni universali: sottostruttura, reticolo delle sottostrutture, congruenze e strutture quoziente, omomorfismi e teorema fondamentale, gruppo degli automorfismi e prodotti diretti. In particolare, si specificano le varie nozioni nei gruppi, negli anelli e nelle algebre unarie, mostrando somiglianze e differenze. Per esempio, mentre l'intersezione di sottostrutture è sempre una sottostruttura, per l'unione in generale non è vero, mentre lo è sempre nelle algebre monounarie; invece, il teorema di Lagrange vale per gruppi e anelli, ma non per le nostre algebre.
Si definiscono e si caratterizzano poi le sottoalgebre 1-generate, nei vari casi, e si caratterizzano le algebre monounarie biiettive mediante il reticolo delle sottoalgebre.
Approfondendo la nozione di congruenza, si analizza la nozione di ideale, che nelle algebre monounarie è definita come una classe che sia anche sottoalgebra; si mostra così che ogni sottoalgebra è ideale di qualche congruenza.
L'argomento successivo è la nozione di omomorfismo; vengono messi in evidenza l'omomorfismo di gruppi e di anelli; in particolare negli omomorfismi di gruppi è presente la nozione di nucleo, nozione non presente nell'algebra monounaria. Per quanto riguarda il teorema fondamentale di omomorfismo, questa formulazione è universale in quanto vale per tutti i tipi di algebre.
In relazione agli omomorfismi, si può parlare di gruppo degli automorfismi, definito in ugual modo nell'algebra universale e nelle algebre monounarie e di queste ultime si danno alcuni esempi.
Infine, si parla del prodotto diretto, costruzione che mantiene invariato il tipo di struttura sia nell'algebra universale sia nell'algebra monounaria, ossia il prodotto diretto di gruppi è un gruppo, di anelli è anello e di algebre unarie è algebra unaria. Si osserva poi che se i fattori sono algebre biiettive, anche il prodotto diretto lo è.

In appendice, una pagina di confronto mostra, a meno d'isomorfismi, quanti gruppi, anelli e algebre monounarie esistono di ordini 1, 2, 3, 4.

Bibliografia

[1] Bela Bollobas, Graph Theory, Springer (1979)

[2] M. Bianchi, A Cillio, L. Verardi, Finite simple monounary algebras, Contemporary Mathematics Vol 42 (2006) pagine 119-132

[3] L. Verardi, Appunti di Algebra Superiore (2004)

[4] A. Vistoli, Note di Algebra, Bologna (1993/94)

[5] www.worldlingo.com

Ringraziamenti

Nel momento in cui si raggiungono determinate tappe della vita, viene naturale pensare a quelle persone che, in un modo o nell'altro, ci hanno accompagnato fino a quel punto.
Quelle persone che ci hanno spronato, che hanno riso e pianto insieme a noi, che hanno avuto pazienza, che ci hanno fatto crscere.
Io, per mia fortuna, sono circondata da tantissime persone che mi vogliono bene, che mi sostengono, che mi correggono, e voglio cogliere questa occasione per dir loro ancora una volta grazie.
Ovviamente i primi a cui penso sono i miei genitori, mia mamma e mio babbo mi hanno sempre sostenuta, anche quando le mie decisioni si discostavano dalle loro, anche quando non siamo d'accordo, ma da sempre mi sono vicini, nel bene e nel male. Se sono cresciuta così è grazie al loro amore e alla loro pazienza e di questo grazie.
Grazie ad Alessio, che nell'ultimo anno e mezzo ha sopportato quotidianamente i miei sbalzi d'umore, e senza il quale non so se sarei riuscita a raggiungere questa tappa così presto. Grazie a lui sono cresciuta, maturata, ho scoperto quelle cose che auguro a tutti di poter trovare. Non aggiungo altro se non: grazie.
Un pensiero particolare va alla mia migliore amica e confidente Valentina, che mi sostiene, mi ascolta, mi sgrida, ma è sempre dalla mia parte.
Come lei, anche Giulia M. è una parte fondamentale per me, amica storica, compagna di studi dalle elementari alle superiori, amica e confidente fidata, si può dire che lei è stata testimone di tutti i miei cambiamenti, da quando ero bambina ad ora.
Altro amico stupendo, nonostante le molteplici diversità di opinione, è Fabio, sempre pronto ad ascoltarmi e ad aiutarmi.
Insieme a loro non si possono dimenticare tutte quelle persone meravigliose che posso fieramente chiamare amici, ciascuno dei quali ha innumerevoli pregi, e senza di loro non avrei una vita così piena e allegra: Sara M., Jenny, Elisa, Francesca P., Lucia, Silvia, Mattia(Fido), Lorenzo, Francesca M.
Grazie alle mie compagne di corso, grazie alle quali lo studio è risultato più facile e divertente: Cami, Dani, Ari, Sara Z., Sara B., Francesco.
Un ringraziamento particolare va alla mia meravigliosa squadra con la quale passo sempre giornate esilaranti: Ilaria, Beatrice, Giulia N., Linda, Stefania, Elisa, Laura, Alessan-

dro(Casty).
Una ragazza stupenda a cui dico un grazie speciale è la mia olp di case finali Lisa, la quale mi accoglie sempre con un meraviglioso sorriso ed è sempre pronta ad ascoltare.
Ovviamente ringrazio il mio relatore Libero Verardi che ha avuto una straordinaria cortesia e disponibilità durante la realizzazione di questa tesi.
Ci sarebbero tantissime altre persone a cui dire grazie, a cui sono riconoscente per tantissime cose e senza le quali non sarei quello che sono; per cui Grazie.
E soprattutto grazie a Dio, tutto quello per cui gioisco e per cui posso essere riconoscente, riempie la mia vita grazie a Lui.