Brevissima introduzione all'algebra universale (teoria generale dei sistemi algebrici)

Paolo Lipparini

(3 dicembre 2016)

> *And then, you see, I'm a don. And a don in the middle of long vacation is almost a non-existent creature, as you ought to remember. College neither knows nor cares where he is, and certainly no one else does.*
>
> (E poi di mestiere faccio il professore universitario. E durante le vacanze un professore praticamente non esiste, come tu certo ricorderai. L'università non sa e non si preoccupa di sapere dove sia, e nel mio caso non c'è proprio nessun altro che se ne interessi.)
>
> — C. S. Lewis, *Out of the Silent Planet* (Lontano dal pianeta silenzioso), 1938

Questa è una versione preliminare, potrebbe contenere (mooolti) orrori. Anche le versioni successive, naturalmente, potranno contenere errori, ma si spera sia più difficile. Sarò naturalmente grato a chi mi farà notare errori di qualunque natura (anche tipografici, la mia tastiera ha una certa età).

L'interdipendenza delle varie sezioni verrà indicata in seguito. I commenti indicati come "osservazioni" possono essere saltati ad una prima lettura, o da chi intendesse leggere queste note nella maniera più veloce possibile, o comunque da chi non trovasse difficoltà durante la lettura. Lo stesso vale per gli esempi. Potrebbe forse essere utile a volte in caso di difficoltà tornare indietro e leggere qualche osservazione precedente.

NB: le osservazioni fanno però parte del programma del corso!!!

Queste note sono state scritte in occasione di un corso tenuto nell'anno accademico 2016-2017 presso l'Università di Tor Vergata. (Una volta completate e rifinite) possono essere usate per un corso molto breve di introduzione all'algebra universale. Ringrazio gli studenti che hanno seguito il corso non solo per la pazienza, ma anche per avermi chiesto di tenere il corso.

Indice

Breve introduzione all'algebra universale

Premessa. La *teoria generale dei sistemi algebrici*, o delle *strutture algebriche*, frequentemente ma forse meno precisamente chiamata *algebra universale*, studia le strutture algebriche (frequentemente ma meno precisamente chiamate algebre), cioè insiemi dotati di un certo numero di operazioni, senza nessuna restrizione sul numero di queste operazioni, né sul numero di argomenti di ciascuna di queste operazioni.

Lo scopo di queste brevi note è quello di presentare alcuni teoremi significativi sui sistemi algebrici generali utilizzando solo un minimo indispensabile di nozioni tecniche. Questo va naturalmente a discapito della completezza e della generalità; la nostra intenzione è quella di presentare alcuni risultati interessanti (almeno ritenuti tali da alcuni studiosi di algebra generale) nella maniera più breve e semplice possibile. Esistono eccellenti testi per chi, incuriosito dall'argomento, desiderasse poi approfondirlo in maniera più completa

Prerequisiti. Non ci sono particolari prerequisiti per leggere queste note, se non una minima familiarità coi metodi di base della matematica moderna, ad esempio, aver seguito alcune ore dei corsi del primo anno di un corso di laurea in matematica. Può essere utile una conoscenza degli argomenti di base di algebra (non generale), ma ripeteremo comunque la maggior parte delle definizioni necessarie. Assumiamo inoltre una certa dimestichezza con la nozione intuitiva di insieme, e con le notazioni comunemente usate.

Per ora supponiamo che chi legge conosca la definizione di reticolo (*lattice* in inglese), e le principali nozioni riguardanti i reticoli. Esiste materiale in italiano liberamente consultabile sui reticoli, fra le tante possibilità, ad esempio, [**Pa**] (per ora è sufficiente arrivare fino alla Proposizione 2.2 + la def 3.11 + la Sezione 5 sui sottoreticoli + Teorema 1); può essere utile anche la sezione matematica della voce sulla Treccani [**Trec**]. Oppure si può consultare il capitolo XIV di [**MB**]. La definizione di reticolo modulare e la caratterizzazione mediante l'omissione del "pentagono" $\mathbf{N}_5$ si possono trovare in [**MB**] oppure in [**Be**, def. 2.5(b) e Teorema 2.8].

1. Nozioni di base

1.1. Operazioni. Ricordiamo che, dati n insiemi $a_1, a_2, \ldots, a_n$ (alcuni di questi insiemi potrebbero essere uguali fra loro), è possibile costruire la *n-upla ordinata* $(a_1, a_2, \ldots, a_n)$. La costruzione può essere effettuata in molti modi equivalenti; la sua proprietà fondamentale è che due n-uple $(a_1, a_2, \ldots, a_n)$ e $(b_1, b_2, \ldots, b_n)$ sono uguali se e solo se $a_1 = b_1$, $a_2 = b_2$, $\ldots$, e $a_n = b_n$.

DEFINIZIONE 1.1. Ricordiamo che, se $n \in \mathbb{N}$, un'*operazione n-aria*, od *operazione ad n argomenti* su un insieme A è una funzione $f : A^n \to A$. Questo significa che ad ogni n-upla ordinata $(a_1, a_2, \ldots, a_n)$ di elementi di A, f associa uno ed un solo elemento di A, indicato con $f(a_1, a_2, \ldots, a_n)$. Il numero n si dice la *arietà* dell'operazione f, e si dirà che f è n-aria.

Nel caso di operazioni binarie (cioè nel caso $n = 2$), solitamente si scriverà $a\, f\, b$ al posto di $f(a, b)$, e, magari, invece che con f, l'operazione verrà indicata con altri simboli, quali $+$, $\cdot$, $\times$, $\vee$, $\wedge$, $\perp$, o addirittura verrà omessa (cioè $f(a, b)$ verrà indicata mediante la giustapposizione ab di a e b). Altre notazioni di questo genere che potrebbero essere utilizzate dovrebbero essere familiari a chi legge, oppure risultare intuitivamente chiare.

Ricordiamo che chi trovasse le seguenti osservazioni troppo discorsive può saltarle in prima lettura.

OSSERVAZIONE 1.2. Il termine "operazione" viene talvolta utilizzato con significati più generali di quello indicato nella Definizione 1.1.

Operazioni "esterne". Per esempio, talvolta si indica come operazione il prodotto di un vettore per uno scalare nell'ambito degli spazi vettoriali. Questa *non* è un'operazione nel senso indicato in 1.1: noi considereremo sempre operazioni *interne*, non *esterne*, cioè le operazioni che consideriamo dipendono solo da elementi in A e non da elementi esterni ad A, come sarebbe nel caso del prodotto per uno scalare. Comunque, anche gli spazi vettoriali o, più in generale, i moduli, si possono considerare come algebre, nel senso delle definizioni che daremo. Vedi 1.5 nella prossima sottosezione e l'Osservazione 11.6. Vedi l'esempio 1.13.

Operazioni parziali e infinitarie. Inoltre, è spesso interessante considerare operazioni cosiddette *parziali*, cioè funzioni da un sottoinsieme *proprio* di A^n ad A. Noi considereremo sempre solo operazioni *totali*, cioè sempre definite, per ogni n-upla di A^n. È anche possibile considerare operazioni *infinitarie*, cioè dipendenti da un numero infinito di argomenti, ed entrambe le cose contemporaneamente, cioè operazioni infinitarie parziali. Nonostante queste possibilità abbiano un interesse notevole, le relative teorie risultano decisamente più complesse, e non le prenderemo in considerazione in questa sede.

Osservazione 1.3. (esclusivamente per i più pedanti) Una n-upla viene indicata con $(a_1, \ldots, a_n)$. Se $f : A \to B$ è una funzione, indicheremo con $f(a)$ l'immagine di $a \in A$ tramite f. Quindi, se f è un'operazione n-aria, l'immagine della n-upla $(a_1, \ldots, a_n)$ dovrebbe essere indicata con $f((a_1, \ldots, a_n))$. Abbiamo omesso (e continueremo ad omettere) le doppie parentesi, perché questo piccolo abuso di notazione non creerà mai problemi all'interno di queste note.

Naturalmente, dando per nota l'arietà di f, si sarebbe potuto scrivere $fa_1a_2 \ldots a_n$ senza rischio di ambiguità. Abbiamo mantenuto la notazione che, a nostro parere, appare più leggibile.

Anche la seguente osservazione potrebbe sembrare dovuta ad eccessiva pignoleria. Vedremo in seguito che non è esattamente così.

Osservazione 1.4. Spesso in algebra classica si usa lo stesso simbolo per indicare operazioni formalmente diverse. Per esempio, se si considerano i due gruppi abeliani $(\mathbb{Z}_p, +)$ e $(\mathbb{R}, +)$ il significato dei due $+$ è diverso: il primo $+$ indica una funzione da $\mathbb{Z}_p \times \mathbb{Z}_p$ in $\mathbb{Z}_p$, mentre il secondo indica una funzione da $\mathbb{R} \times \mathbb{R}$ in $\mathbb{R}$, dunque oggetti relativamente diversi.

Naturalmente, all'atto pratico, questa ambiguità di notazione non causa quasi mai inconvenienti e non è necessario scrivere, ad esempio, $(\mathbb{Z}_p, +^{\mathbb{Z}_p})$ e $(\mathbb{R}, +^{\mathbb{R}})$ per sottolineare la differenza. Però in alcuni casi questa notazione estesa può essere utile, o addirittura necessaria, e noi utilizzeremo convenzioni di questo tipo quando ci sarà bisogno di completa chiarezza. Torneremo comunque sull'argomento.

1.2. Strutture algebriche (algebre). Una *struttura algebrica* o *sistema algebrico* o, per brevità e per adattarci alla consuetudine, un'*algebra* è un insieme *non vuoto* A su cui sono definite alcune operazioni.

Per semplcità, considereremo soprattutto il caso in cui il numero di operazioni su A è finito. In realtà questa ipotesi di finitezza non verrà mai utilizzata; ma il caso di un numero infinito di operazioni comporta notazioni e terminologia relativamente più complesse, che possono essere risparmiate al lettore che si sta avvicinando all'argomento. Mostreremo comunque in un'osservazione a parte (vedi 11.6) come trattare il caso più generale di un insieme infinito (di qualunque cardinalità) di operazioni.

Definizione 1.5. Un'*algebra (con un numero finito di operazioni)* $\mathbf{A}$ è una $m+1$-pla ordinata $(A, f_1, f_2, \ldots, f_m)$, tale che A è un insieme non vuoto e, per ogni $j = 1, \ldots, m$, esiste $n_j \in \mathbb{N}$ tale che f_j è un'operazione n_j-aria su A.

A si dice *sostegno* o *insieme di base* o *universo* di $\mathbf{A}$ ed $f_1, f_2, \ldots, f_m$ si dicono le operazioni di $\mathbf{A}$. A volte diremo semplicemente che $\mathbf{A}$ è *su* A, o è *basata* su A, anzichè dire che A è il sostegno di $\mathbf{A}$. Naturalmente,

adotteremo la convenzione che se $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$, $\mathbf{A}'$ etc. sono algebre, i rispettivi sostegni verranno indicati con A, B, C, A' etc.[1]

È da notare che nella precedente definizione ammettiamo il caso $m = 0$, cioè ammettiamo la possibilità che $\mathbf{A}$ non abbia operazioni. In altre parole, un insieme senza operazioni è da considerarsi un'algebra a tutti gli effetti.

Osservazione 1.6. A prima vista, verrebbe spontaneo definire un'algebra come una coppia (A, F), dove F è un *insieme* di operazioni su A, cioè, metti, nel caso finito, l'ordine in cui compaiono gli elementi di F non è rilevante.

Questa definizione apparentemente più semplice potrebbe andar bene per alcuni dei prossimi argomenti, ma vedremo presto quali difficoltà comporterebbe.

Osservazione 1.7. Il termine *algebra* viene usato con diverso significato in altri campi della matematica. Alcune di queste "algebre" sono casi (molto) speciali delle algebre considerate nella Definizione 1.5. In altri casi si tratta di strutture algebriche a cui viene aggiunta ulteriore struttura di tipo "non algebrico" (ad esempio, una topologia).

Precisato che lo scopo di questa osservazione è semplicemente quello di evitare possibili ambiguità, va detto che anche in algebra universale a volte vengono studiate algebre dotate di ulteriore struttura. Di nuovo, si tratta di argomenti di notevole interesse, che esulano però dallo scopo di questa breve nota.

Esempio 1.8. (a) Un gruppo può essere considerato un'algebra $(G, \cdot)$, dove, naturalmente, $\cdot$ è un'operazione binaria (se ciò non causerà confusione, ometteremo di indicare $\cdot$ nelle formule).

Naturalmente, non tutte le algebre con una sola operazione binaria sono gruppi. Si richiede che un gruppo soddisfi a:

(a1) (proprietà associativa) per ogni $g, h, j \in G$, si ha $g(hj) = (gh)j$;

(a2) (esistenza dell'elemento neutro) esiste $e \in G$ tale che, per ogni $g \in G$, si ha $eg = ge = g$;

(a3) per ogni $g \in G$, esiste $h \in G$ (detto *inverso* di g) tale che $gh = hg = e$ (dove e è l'elemento dato da (a2), e il nostro enunciato è non ambiguo, poiché segue immediatamente da (a2) che l'elemento e è unico).

(b) Siccome a partire da (a1)-(a3) si dimostra che, per ogni $g \in G$, l'elemento h dato da (a3) sopra è unico, un gruppo si può anche considerare come un'algebra $(G, \cdot, ^{-1})$, dove $^{-1}$ indica l'operazione unaria che associa ad ogni $g \in G$ quell'h dato da (a3), cioè $g^{-1} = h$.

[1]Per essere precisi, sullo stesso insieme non vuoto A possono essere considerate molte algebre diverse. In alcune situazioni questa considerazione può essere molto interessante e fruttuosa; ma in queste note la situazione non si presenterà mai, quindi la nostra notazione non causerà ambiguità.

In questo senso, le condizioni (a2)-(a3) sono sostanzialmente equivalenti a

(b2) Per ogni $g, h \in G$, si ha $gg^{-1}h = g^{-1}gh = hgg^{-1} = hg^{-1}g = h$ (alcune condizioni sono ridondanti; nello scrivere l'ultima catena di uguaglianze abbiamo fatto uso della proprietà associativa, altrimenti la scrittura sarebbe stata ambigua.)

Dal punto di vista di uno studioso di teoria dei gruppi, e nella stragrande maggioranza dei casi, le due definizioni (a) e (b) date sopra sono completamente equivalenti. Vedremo presto che così non è per il nostro studio delle algebre.

Per ora osserviamo che nelle condizioni (a) e (b2) si richiede che certe identità valgano per elementi arbitrari di G, mentre in (a2) ed (a3) si richiede l'*esistenza* di elementi soddisfacenti a certe proprietà. Questa differenza fra *per ogni* ed *esiste* si rivelerà in seguito un vero e proprio spartiacque.

Esempio 1.9. Un campo $\mathbf{K}$ può essere considerato un'algebra $(K, +, \cdot)$, o $(K, +, -, \cdot)$, ma *non* un'algebra $(K, +, \cdot, ^{-1})$. Questo perché l'inverso (moltiplicativo) in un campo non è sempre definito (è definito per tutti i $k \in K$ tranne che per $k = 0$).

Quindi $(K, +, \cdot, ^{-1})$ potrebbe essere considerata come un'algebra solo ammettendo anche operazioni parziali (v. Osservazione 1.2), ma, come precisato, noi non tratteremo questa situazione. Oppure potremmo definire in maniera arbitraria 0^{-1}, ad esempio, $0^{-1} = 0$; questo renderebbe $(K, +, \cdot, ^{-1})$ un'algebra secondo la nostra definizione, ma va tenuto presente che, con questa definizione, l'identità $kk^{-1} = 1$ non vale più per *tutti* gli elementi di K.

Esempio 1.10. Altri esempi (per ora) si possono trovare in [**Be**, Sezione 1.2, pagine 4–6]. (NB: fa parte del programma!) In particolare: anelli, reticoli, semireticoli, semigruppi, quasigruppi.

N.B.: nella definizione di *anello* non includeremo la richiesta dell'esistenza di 1 (elemento neutro rispetto alla moltiplicazione). Tutte le volte che avremo la necessità di 1 specificheremo esplicitamente *anello con unità*.

Nella maggior parte dei casi non ci sarà una differenza sostanziale se considereremo la classe degli anelli commutativi o la classe degli anelli in cui non si richiede la commutatività. Nel secondo caso, comunque, tutte le volte che parleremo di ideale, sottintenderemo che si tratta di "ideale bilatero". In tutti i casi in cui sarà necessario, preciseremo comunque esplicitamente se stiamo considerando anelli commutativi o non commutativi.

Osservazione 1.11. Nelle Definizioni 1.1 e 1.5 non abbiamo posto alcuna limitazione ai possibili valori di n e degli n_j. È una questione di convenzione se supporre o meno che 0 appartenga ad $\mathbb{N}$; noi supporremo sempre $0 \in \mathbb{N}$. Viene allora spontaneo chiedersi come debba essere interpretata una "operazione 0-aria".

Intuitivamente, un'operazione 0-aria su un insieme A dovrebbe essere un'operazione che non dipende da nessun argomento, cioè che sceglie un

elemento fissato di A. In altre parole, interpreteremo una operazione 0-aria come una *costante* scelta fra gli elementi di A. Precisiamo che si tratta comunque di una convenzione; nell'Osservazione 11.1 in appendice renderemo ancora più espliciti i motivi che fanno pensare ad un'operazione 0-aria come ad una costante.

Indipendentemente dal modo in cui viene introdotta, è comunque a volte conveniente avere a disposizione la nozione di costante. Se il lettore trovasse difficoltà nel considerare le costanti come operazioni zero-arie o se, semplicemente, così preferisse, può modificare la Definizione 1.5 nel seguente modo: un'algebra è una $m+\ell+1$-pla ordinata $(A, f_1, f_2, \dots f_m, c_1, \dots, c_\ell)$, dove A e le f_j sono come in 1.5 (ma con $n_j > 0$ per ogni j), e $c_1, \dots, c_\ell$ sono elementi di A. È ammessa la possibilità che m, oppure ℓ, oppure entrambi siano 0.

Volendo, tutto quello che diremo può essere modificato senza nessun problema in modo da concordare con questa definizione.

Esempio 1.12. Avendo a disposizioni le costanti, si possono considerare i gruppi come algebre ancora in un altro modo, oltre a quelli presentati in 1.8.

(c) Un gruppo si può anche considerare come un'algebra $(G, \cdot, ^{-1}, e)$, dove $^{-1}$ è un'operazione unaria come in 1.8(b), ed e è una costante che indica l'elemento neutro del gruppo. Le condizioni (a2), (a3) e (b2) in 1.8 si possono semplificare adesso al seguente modo:
   (c2) per ogni $g \in G$, si ha $eg = ge = g$;
   (c3) per ogni $g \in G$, si ha che $gg^{-1} = g^{-1}g = e$.
   Quindi un gruppo è un algebra $(G, \cdot, ^{-1}, e)$ che soddisfa ad (a1), (c2) e (c3).

C'è una sottile differenza fra le proprietà di questa definizione di gruppo e quella data mediante 1.8(b), a parte l'innegabile maggiore semplicità di (c) rispetto a (b). Notiamo, comunque che, sia nella definizione data in 1.8(b) che in questa definizione (c), le condizioni che definiscono un gruppo non usano il termine "esiste", che, come abbiamo fatto notare, è necessario invece per esprimere (a2) ed (a3).

Esempio 1.13. Uno spazio vettoriale $\mathbf{V}$ su un campo $\mathbf{K}$ si può considerare un'algebra $(V, +, -, 0, \dots)$, dove $+$ è binaria, $-$ è unaria (e indica l'opposto), 0 è una costante e, per ogni $k \in K$, si aggiunge un'operazione unaria λ_k, che manda un vettore $v \in V$ nel suo "prodotto" $\lambda_k(v) = kv$ per lo scalare k.

Naturalmente, la definizione appena data rientra nel caso considerato nella Definizione 1.5 solo se K è finito. In questo caso, se $K = \{k_1, k_2, \dots, k_\ell\}$, allora $\mathbf{V}$ si può considerare come l'algebra $(V, +, -, 0, \lambda_1, \lambda_2, \dots, \lambda_\ell)$.

Se invece K è infinito, bisogna considerare la definizione più generale di algebra (cui accenneremo nell'Osservazione 11.6) in cui è ammessa la possibilità di avere un numero infinito di operazioni.

Lasciamo al lettore il compito di tradurre gli assiomi che definiscono gli spazi vettoriali nel contesto dato nella presente definizione. Per esempio,

cosa significa la condizione $k(v+w) = kv + kw$? E la condizione $(k+h)v = kv + hv$? (per $k, h \in K$ e $v, w \in V$)

Il simbolo + usato nelle formule precedenti ha sempre lo stesso significato?

1.3. Sottoalgebre.

Osservazione 1.14. Come nell'algebra classica, ci occuperemo adesso di costruire nuove algebre a partire da algebre date. La prima costruzione che considereremo è quella di sottoalgebra di un'algebra. Sviluppare questa idea non comporta particolari difficoltà in confronto, per esempio, con la nozione di sottogruppo di un gruppo o sottoanello di un anello. L'unico dettaglio di cui bisogna tenere conto è che, in certi casi, e a differenza che nel caso dei gruppi e degli anelli, a volte un'intersezione di sottoalgebre può essere il vuoto.

Siccome la definizione viene data in un ambito piuttosto generale, presteremo però particolare attenzione ai dettagli della definizione e alle notazioni. In questo caso avremmo potuto essere decisamente meno formali, ma l'attenzione a questo tipo di dettagli si rivelerà comunque necessaria in seguito.

Definizione 1.15. Se f è un'operazione n-aria su A, un sottoinsieme B di A si dice *chiuso per* f, o *chiuso rispetto a* f se, per ogni n-upla $(b_1, \dots, b_n)$ di elementi in B, si ha che $f(b_1, \dots, b_n) \in B$. Se f è 0-aria, corrispondente alla costante $c \in A$, la definizione precedente va intesa nel senso che c deve appartenere a B.

Se B è chiuso per f, allora f può essere considerata un'operazione su B, più precisamente, possiamo definire la *restrizione* $f_{\restriction B}$ di f a B mediante la regola banale $f_{\restriction B}(b_1, \dots, b_n) = f(b_1, \dots, b_n)$, per ogni n-upla $(b_1, \dots, b_n)$ di elementi di B (l'ipotesi che B sia chiuso per f è necessaria affinché il codominio di $f_{\restriction B}$ sia proprio B. Se la presenza di indici può causare confusione, scriveremo $f \restriction B$ invece di $f_{\restriction B}$).

Definizione 1.16. Se $\mathbf{A} = (A, f_1, f_2, \dots, f_m)$ è un'algebra, un sottoinsieme non vuoto B di A si dice *(sostegno per) una sottoalgebra di* $\mathbf{A}$ se B è chiuso per tutte le operazioni di $\mathbf{A}$. In tal caso, la *sottoalgebra* di $\mathbf{A}$ determinata da B è l'algebra $\mathbf{B} = (B, g_1, g_2, \dots, g_m)$, dove $g_1 = f_1 \restriction B$, $g_2 = f_2 \restriction B$, etc.

Siccome $\mathbf{B}$ è determinata univocamente da B, e viceversa, chiameremo indifferentemente B o $\mathbf{B}$ una *sottoalgebra*. Dal contesto risulterà sempre chiaro se si tratta di un insieme B o di un'algebra $\mathbf{B}$, quindi ci permetteremo anche questo abuso di terminologia.

Definizione 1.17. Una notazione che può essere comoda in questa e altre situazioni è quella di indicare le operazioni di $\mathbf{A}$ con $f_1^{\mathbf{A}}$, $f_2^{\mathbf{A}}$ etc., e le operazioni di $\mathbf{B}$ con $f_1^{\mathbf{B}}$, $f_2^{\mathbf{B}}$ etc. Cf. l'osservazione 1.4. Vedremo

più avanti che a questa notazione può essere attribuita una valenza più significativa.

Così, la definizione precedente può essere scritta $f_1^{\mathbf{B}} = f_1^{\mathbf{A}} \restriction B$, $f_2^{\mathbf{B}} = f_2^{\mathbf{A}} \restriction B$, etc.

Ancor più brevemente, potremo dire che le operazioni di $\mathbf{B}$ sono definite da $f^{\mathbf{B}} = f^{\mathbf{A}} \restriction B$, con $f^{\mathbf{A}}$ che varia fra le operazioni di $\mathbf{A}$. È intuitivo che questa convenzione può essere applicata anche nel caso di algebre con un numero infinito di operazioni.

Esempio 1.18. Se si considera la definizione di gruppo data in 1.8(a), allora le nozioni di sottogruppo e quella di sottoalgebra non coincidono. Secondo la Definizione 1.8(a), ad esempio, $(\mathbb{N}, +)$ è una sottoalgebra di $(\mathbb{Z}, +)$, ma $(\mathbb{N}, +)$ evidentemente non è un sottogruppo di $(\mathbb{Z}, +)$. Notiamo che anche, ad esempio, $(A, +)$, dove $A = \{n \in \mathbb{N} \mid n > 10\}$ è una sottoalgebra di $(\mathbb{Z}, +)$ in questo senso. Cosa succederebbe invece se considerassimo $A = \{n \in \mathbb{N} \mid n > -10\}$? Oppure $A = \{n \in \mathbb{N} \mid n < -10\}$? Oppure $A = \{n \in \mathbb{N} \mid |n| > 10\}$?

Usando invece la definizione data in 1.8(b), si ha che una sottoalgebra di un gruppo è sempre essa stessa un gruppo. Lo stesso vale anche usando la definizione 1.12(c).

Comunque, con ciascuna delle precedenti definizioni di gruppo come algebra, un sottogruppo in senso classico è sempre una sottoalgebra nel senso di 1.16.

Esempio 1.19. (a) Se $\mathbf{A}$ è un'algebra senza operazioni, tutti i sottoinsiemi non vuoti sono sottoalgebre.

(b) Il caso precedente non si presenta esclusivamente quando $\mathbf{A}$ è senza operazioni.

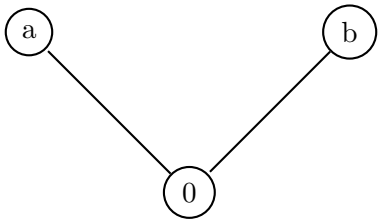
Sia $(A, \leq)$ un insieme totalmente ordinato, e sia $\mathbf{A} = (A, \max)$, dove qui max si considera come un'operazione binaria.

Anche in questo caso, tutti i sottoinsiemi non vuoti sono sottoalgebre di $\mathbf{A}$.

Lo stesso vale anche se si considera $\mathbf{A} = (A, \max, \min)$. Notiamo che quest'ultima algebra è un reticolo.

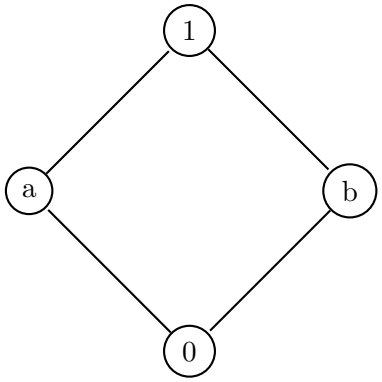
Cosa succederebbe se si considerasse max come un'operazione n-aria, con n fissato > 2?

(c) Si consideri il semireticolo $\mathbf{S} = (S, \cdot)$ con 3 elementi che non è una *catena* (cioè non è totalmente ordinato). S ha tre elementi $\{0, a, b\}$ tali che $0a = 0b = ab = 0$, oltre alle identità che devono essere soddisfatte in ogni semireticolo.



Tutti i sottoinsiemi di S sono sottoalgebre, tranne l'insieme vuoto e $\{a, b\}$.

(d) Si consideri il seguente reticolo, chiamato $\mathbf{D}_2$.



$\mathbf{D}_2$

Ad esempio, $\{0, a, 1\}$ è una sottoalgebra, ma $\{a, b\}$ non lo è. Ci sono altri sottoinsiemi che non sono sottoalgebre?

(e) Se $\mathbf{L} = (L, \wedge, \vee)$ è un reticolo, allora, per ogni $\ell \in L$, $\{\ell\}$ è una sottoalgebra di $\mathbf{L}$.

Più in generale, se $C \subseteq L$ è una *catena*, cioè un insieme totalmente ordinato, allora C è una sottoalgebra.

In particolare, se $|L| > 1$, allora l'intersezione di tutte le sottoalgebre di $\mathbf{L}$ è il vuoto.

PROPOSIZIONE 1.20. *Se $\mathbf{A}$ è un'algebra, $(\mathbf{B}_i)_{i\in I}$ è una famiglia qualunque di sottoalgebre di $\mathbf{A}$, e $\bigcap_{i\in I} B_i \neq \emptyset$, allora $\bigcap_{i\in I} B_i$ è (il sostegno per) una sottoalgebra di $\mathbf{A}$.*

DIMOSTRAZIONE. Sia $B = \bigcap_{i\in I} B_i$. B è diverso dal vuoto per ipotesi. Bisogna quindi dimostrare che B è chiuso per tutte le operazioni di $\mathbf{A}$. Sia f un'operazione n-aria di $\mathbf{A}$ e sia $(b_1, \ldots, b_n)$ una n-upla di elementi di B. Per la definizione di B, $b_1, \ldots, b_n \in B_i$, per ogni $i \in I$. Siccome ciascuna $\mathbf{B}_i$ è una sottoalgebra di $\mathbf{A}$, $f(b_1, \ldots, b_n) \in B_i$, per ogni $i \in I$. Ma allora $f(b_1, \ldots, b_n) \in \bigcap_{i\in I} B_i$, quello che dovevamo dimostrare. □

NB: se $\mathbf{A}$ ha almeno una costante (cioè un'operazione 0-aria), allora l'eventualità che l'intersezione sia vuota non si può verificare. Infatti, se c è una costante, allora c deve appartenere anche a ciascuno dei B_i,

La proposizione precedente implica che l'insieme delle sottoalgebre di un'algebra è un reticolo, salvo il fatto che in alcuni casi l'insieme vuoto deve essere considerato membro di questo reticolo. Per rendere esplicita questa osservazione, se $\mathbf{A}$ è un'algebra con almeno una costante, definiamo[2] $\mathrm{Sub}(\mathbf{A})$ come l'insieme di tutte le sottoalgebre di $\mathbf{A}$. Se invece $\mathbf{A}$ non ha costanti, richiediamo anche che $\emptyset \in \mathrm{Sub}(\mathbf{A})$. In altre parole, gli elementi di $\mathrm{Sub}(\mathbf{A})$ sono tutti i sottoinsiemi di A che sono chiusi rispetto a tutte le operazioni di $\mathbf{A}$ (NB: dalla definizione di "chiuso" segue che l'insieme vuoto è chiuso rispetto a tutte le operazioni di arietà > 0).

Per semplicità, consideriamo dapprima il caso in cui l'algebra $\mathbf{A}$ ha una costante.

Corollario 1.21. *Sia $\mathbf{A}$ un'algebra con almeno una costante e sia $C \subseteq A$.*

(1) Esiste il più piccolo elemento $\langle C\rangle$ di $\mathrm{Sub}(\mathbf{A})$ *che contiene C e $\langle C\rangle$ è una sottoalgebra di $\mathbf{A}$, detta* sottoalgebra di $\mathbf{A}$ generata da C.

(2) L'insieme $\mathrm{Sub}(\mathbf{A})$*, ordinato per inclusione, è un reticolo, detto* reticolo delle sottoalgebre di $\mathbf{A}$.

Dimostrazione. (1) Dimostriamo che $\langle C\rangle = \bigcap\{B \subseteq A \mid C \subseteq B$ e $\mathbf{B}$ è una sottoalgebra di $\mathbf{A}\}$ soddisfa alla proprietà desiderata. Innanzitutto, osserviamo che esiste almeno un elemento nella famiglia di cui stiamo prendendo l'intersezione, poichè A vi appartiene.

Per la definizione di $\langle C\rangle$, abbiamo ovviamente $C \subseteq \langle C\rangle$. Per quanto abbiamo osservato sopra, siccome $\mathbf{A}$ ha una costante, $\langle C\rangle$ è diverso dal vuoto, quindi è una sottoalgebra di $\mathbf{A}$, per la Proposizione 1.20. Resta da dimostrare che $\langle C\rangle$ è il più piccolo elemento di $\mathrm{Sub}(\mathbf{A})$ che contiene C. Ma ogni elemento di $\mathrm{Sub}(\mathbf{A})$ che contiene C fa parte dell'insieme dei B di cui $\langle C\rangle$ è l'intersezione, quindi $\langle C\rangle$ è contenuto in ciascuno di tali B.

(2) Se $B, D \in \mathrm{Sub}(\mathbf{A})$, allora $B \cap D \in \mathrm{Sub}(\mathbf{A})$, per 1.20. Quindi ovviamente $B \cap D$ è il più grande elemento di $\mathrm{Sub}(\mathbf{A})$ contenuto sia in B che in D, cioè $B \wedge D = B \cap D$.

Inoltre, per (1), esiste il più piccolo elemento E di $\mathrm{Sub}(\mathbf{A})$ che contiene $C = B \cup D$. Ma ogni elemento di $\mathrm{Sub}(\mathbf{A})$ che contenga sia B

[2]A grande richiesta popolare, ci vediamo costretti ad usare $\mathrm{Sub}(\mathbf{A})$ anziché $\mathrm{Sot}(\mathbf{A})$.

che D deve contenere $B \cup D$, quindi, per sopra, deve contenere E. Del resto E contiene sia B che D, per costruzione, quindi $E = B \vee D$. □

Osservazione 1.22. Osserviamo che, dalla dimostrazione di (4), si ricava la semplice descrizione di $B \wedge D$ come $B \cap D$, e quindi, in questo caso, $\wedge$ è anche indipendente dalla struttura su $\mathbf{A}$ (ma ovviamente la proprietà di essere o meno una sottoalgebra *dipende* dalla struttura di $\mathbf{A}$).

D'altro canto, la dimostrazione di (4) non fornisce una descrizione di $B \vee D$ utilizzabile in pratica. Una tale descrizione verrà fornita nella Proposizione 1.60. Anche in questo caso, si verificherà che $\vee$ risulta indipendente dalla struttura su $\mathbf{A}$.

Esempio 1.23. Come abbiamo visto nell'esempio 1.19(a), se $\mathbf{A}$ è un'algebra senza operazioni, tutti i sottoinsiemi non vuoti sono sottoalgebre; quindi il reticolo delle sottoalgebre di $\mathbf{A}$ è $(\mathcal{P}(A), \cap, \cup)$, dove $\mathcal{P}(A)$ indica l'*insieme delle parti*, o *insieme potenza* di A, cioè l'insieme di tutti i sottoinsiemi di A.

La stessa situazione si presenta nel caso di un insieme totalmente ordinato, dove come operazioni si prendono min e max, o anche una sola delle due.

Passando ad un altro esempio, sareste in grado di disegnare il reticolo delle sottoalgebre di $\mathbf{D}_2$? ($\mathbf{D}_2$ è stato introdotto in 1.19(d))

Esempio 1.24. Torniamo un'ultima volta sulle possibili definizioni di gruppo. Vedi 1.8(a)(b) e 1.12(c).

Abbiamo visto in 1.18 che, usando la definizione 1.8(a), le nozioni di sottogruppo e quella di sottoalgebra non coincidono. Usando invece la definizione 1.8(b) oppure la definizione 1.12(c) si ha che una sottoalgebra di un gruppo è sempre essa stessa un gruppo.

C'è quindi una qualche differenza sostanziale fra le definizioni (b) e (c)? Abbiamo notato che la nozione di sottoalgebra non cambia, sia che si consideri (b), sia che si consideri (c). Si può dire lo stesso del "reticolo delle sottoalgebre"?

Per completezza, diamo ora la versione generale del Corollario 1.21. Il lettore non interessato può saltare la dimostrazione.

Corollario 1.25. *Sia* $\mathbf{A}$ *un'algebra e* $C \subseteq A$.

(1) Esiste il più piccolo elemento $\langle C \rangle$ *di* $\mathrm{Sub}(\mathbf{A})$ *che contiene* C.
(2) $\langle C \rangle \neq \emptyset$ *se e solo se* $C \neq \emptyset$ *oppure*[3] $\mathbf{A}$ *ha almeno una costante.*
(3) Se $\langle C \rangle \neq \emptyset$, $\langle C \rangle$ *è una sottoalgebra di* $\mathbf{A}$, *detta* sottoalgebra di $\mathbf{A}$ generata da C.

[3]A scanso di equivoci, "o" ed "oppure" verranno sempre intesi in senso non esclusivo, cioè, date due condizioni X e Y, le espressioni "X o Y" e "X oppure Y" significheranno sempre che vale almeno una delle due fra X e Y (cioè, potrebbero valere entrambe.) Per farla breve, "X oppure Y" significa "X, oppure Y, oppure sia X che Y".

(4) *L'insieme* $\mathrm{Sub}(\mathbf{A})$*, ordinato per inclusione, è un reticolo, detto* reticolo delle sottoalgebre di $\mathbf{A}$.

OSSERVAZIONE 1.26. Ovviamente, l'espressione "reticolo delle sottoalgebre" usata in (4) è leggermente impropria, perché può succedere che $\emptyset \in \mathrm{Sub}(\mathbf{A})$, mentre noi non considereremo mai il vuoto come un'algebra. Resta comunque comodo usare "reticolo delle sottoalgebre".

DIMOSTRAZIONE. (1) Se $\langle C\rangle$ è non vuoto, allora è una sottoalgebra di $\mathbf{A}$, per la Proposizione 1.20. Se $\langle C\rangle = \emptyset$, allora $\mathbf{A}$ non ha costanti (perché, come già precisato, se c fosse una costante di $\mathbf{A}$, allora c apparterrebbe a tutte le sottoalgebre di $\mathbf{A}$, quindi, per la definizione di $\langle C\rangle$, avremmo $c \in \langle C\rangle$). Ma, allora, per la definizione di $\mathrm{Sub}(\mathbf{A})$, abbiamo $\langle C\rangle = \emptyset \in \mathrm{Sub}(\mathbf{A})$. In ogni caso, abbiamo dunque $\langle C\rangle \in \mathrm{Sub}(\mathbf{A})$. Il resto è come in 1.21.

(2) Abbiamo dimostrato sopra che se $\mathbf{A}$ ha almeno una costante, allora $\langle C\rangle \neq \emptyset$. Ovviamente, $\langle C\rangle \neq \emptyset$ anche quando $C \neq \emptyset$, poiché $\langle C\rangle \supseteq C$. Viceversa, se $\mathbf{A}$ non ha costanti, allora $\emptyset \in \mathrm{Sub}(\mathbf{A})$, per definizione, e se $C = \emptyset$, allora la definizione di $\langle C\rangle$ fornisce $\langle C\rangle = \emptyset$.

(3) è immediato da (1).

(4) L'unica differenza con 1.21(2) è che l'intersezione di elementi di $\mathrm{Sub}(\mathbf{A})$ potrebbe essere l'insieme vuoto, ma questo può avvenire solo se $\mathbf{A}$ non ha costanti, e in questo caso $\emptyset \in \mathrm{Sub}(\mathbf{A})$, per definizione. □

1.4. Morfismi.

DEFINIZIONE 1.27. Se $\mathbf{A} = (A, f_1, f_2, \dots, f_m)$ è un'algebra, il *tipo di similarità di* $\mathbf{A}$ o, per brevità, semplicemente il *tipo di* $\mathbf{A}$ è la m-upla $(n_1, n_2, \dots, n_m)$, dove, per $j = 1, \dots, m$, indichiamo con n_j l'arietà di f_j.

Osserviamo che se $\mathbf{B}$ è una sottoalgebra di un'algebra $\mathbf{A}$ secondo la Definizione 1.16, allora $\mathbf{B}$ ha lo stesso tipo di $\mathbf{A}$.

ESEMPIO 1.28. I gruppi considerati come nell'Esempio 1.8(a) sono algebre di tipo (2), mentre il tipo dei gruppi considerati come in 1.8(a) è $(2, 1)$. Un gruppo dato come in 1.12(c) ha invece tipo $(2, 1, 0)$.

Un reticolo ha tipo $(2, 2)$. A volte nella definizione di reticolo si aggiunge l'esistenza di un elemento massimo 1 e di un elemento minimo 0 (tali elementi esistono sempre nel caso di reticoli finiti; ma, ad esempio, $\mathbb{Z}$ è un reticolo senza elemento massimo e senza elemento minimo). In tal caso, un reticolo può essere considerato un'algebra di tipo $(2, 2, 0, 0)$, dove 0 e 1 sono interpretate come costanti. Noi considereremo sempre i reticoli come algebre di tipo $(2, 2)$.

Uno spazio vettoriale (su un campo finito) considerato come un'algebra nel senso dell'esempio 1.13 ha tipo $(2, 1, 0, 1, 1, 1, \dots)$.

DEFINIZIONE 1.29. Se $\mathbf{A}$ e $\mathbf{B}$ sono due algebre dello stesso tipo, una funzione $\varphi : A \to B$ si dice *morfismo* da $\mathbf{A}$ a $\mathbf{B}$ se

$$\varphi(f^{\mathbf{A}}(a_1, a_2, \ldots, a_n)) = f^{\mathbf{B}}(\varphi(a_1), \varphi(a_2), \ldots, \varphi(a_n)), \tag{1}$$

per ogni operazione $f^{\mathbf{A}}$ di $\mathbf{A}$, per l'operazione corrispondente $f^{\mathbf{B}}$ di $\mathbf{B}$ (stiamo usando la convenzione introdotta in 1.17) e per ogni n-upla di elementi di A, dove n è l'arietà di $f^{\mathbf{A}}$ ed $f^{\mathbf{B}}$. Notiamo che, affinché l'equazione (1) abbia senso, è effettivamente necessario che $f^{\mathbf{A}}$ ed $f^{\mathbf{B}}$ abbiano la stessa arietà. Per questo, la definizione di morfismo si può dare solo fra algebre dello stesso tipo.

Se φ è un morfismo da $\mathbf{A}$ a $\mathbf{B}$, scriveremo $\varphi : \mathbf{A} \to \mathbf{B}$, e, viceversa, ogni volta che useremo la formula precedente, intenderemo che φ è un morfismo da $\mathbf{A}$ a $\mathbf{B}$ (e quindi, anche se non specificato espressamente, che $\mathbf{A}$ e $\mathbf{B}$ sono algebre dello stesso tipo.)

PROPOSIZIONE 1.30. *Se* $\mathbf{A}$*,* $\mathbf{B}$ *e* $\mathbf{C}$ *sono algebre dello stesso tipo e* $\varphi : \mathbf{A} \to \mathbf{B}$*,* $\psi : \mathbf{B} \to \mathbf{C}$ *sono morfismi, allora* $\varphi \circ \psi : \mathbf{A} \to \mathbf{C}$ *è un morfismo.*

PROPOSIZIONE 1.31. *Se* $\mathbf{B}$ *è una sottoalgebra di* $\mathbf{A}$*, allora l'inclusione* $\iota : B \to A$ *è un morfismo.*

Le dimostrazioni sono lasciate per esercizio.

Un'*isomorfismo* è un morfismo biiettivo; e due algebre $\mathbf{A}$ e $\mathbf{B}$ dello stesso tipo si dicono *isomorfe* se esiste un isomorfismo $\varphi : \mathbf{A} \to \mathbf{B}$. In questo caso scriveremo $\mathbf{A} \cong \mathbf{B}$. È facile verificare che l'inverso di un isomorfismo è ancora un isomorfismo e che la relazione di essere isomorfe, in un insieme di algebre dello stesso tipo, è una relazione di equivalenza, quindi si può parlare di *classe di isomorfismo*.

PROPOSIZIONE 1.32. *Se* $\varphi : \mathbf{A} \to \mathbf{B}$*, allora* $Im\varphi = \{b \in B \mid$ *esiste* $a \in A$ *tale che* $\varphi(a) = b\}$ *è una sottoalgebra di* $\mathbf{B}$*.*

La dimostrazione è lasciata per esercizio.

1.5. Quozienti (congruenze). Se $\varphi : A \to B$ è una funzione, φ induce una relazione di equivalenza su A, se si considerano "identificati" due elementi di A se e solo se hanno la stessa immagine secondo φ. Sarebbe naturale chiamare questa relazione di equivalenza "nucleo" di φ, ma, per evitare conflitti di terminologia, per esempio, col nucleo di un morfismo di gruppi, modificheremo leggermente la terminologia.

DEFINIZIONE 1.33. Se $\varphi : A \to B$ è una funzione, il *nucleo di* φ *nel senso di relazione di equivalenza* di φ è la seguente relazione su A: $KerEq(\varphi) = \{(a, b) \in A^2 \mid \varphi(a) = \varphi(b)\}$.

DEFINIZIONE 1.34. Una *relazione (binaria)* su un insieme A è un sottoinsieme di $A \times A$. Se α è una relazione binaria e $a, b \in A$, spesso si scriverà $a\ \alpha\ b$ al posto di $(a, b) \in \alpha$.

DEFINIZIONE 1.35. Se $\mathbf{A}$ è un'algebra e α è una relazione binaria su A, si dice che α è *compatibile (rispetto ad $\mathbf{A}$)*, o *ammissibile*, o che ha la *proprietà di sostituzione* se, per ogni $n \in \mathbb{N}$ e per ogni operazione n-aria f di $\mathbf{A}$, abbiamo che

$$a_1\ \alpha\ b_1,\ a_2\ \alpha\ b_2,\ \ldots,\ \text{e}\ a_n\ \alpha\ b_n \ \text{ implicano } f(a_1, a_2, \ldots, a_n)\ \alpha\ f(b_1, b_2, \ldots, b_n),$$

per tutte le n-uple $(a_1, a_2, \ldots, a_n)$ e $(b_1, b_2, \ldots, b_n)$ di elementi di A.

Se α è una relazione di equivalenza su un insieme A e $a \in A$, indicheremo con a/α la classe di equivalenza di a rispetto a α; cioè, $a/\alpha = \{b \in A \mid a\ \alpha\ b\}$. L'insieme delle classi di equivalenza di α è $A/\alpha = \{a/\alpha \mid a \in A\}$. La funzione $\pi_\alpha : A \to A/\alpha$ definita da $\pi_\alpha(a) = a/\alpha$ si dice *proiezione (canonica)*. Se non c'è rischio di confusione, scriveremo semplicemente π al posto di π_α.

PROPOSIZIONE 1.36. *Se $\varphi : \mathbf{A} \to \mathbf{B}$ è un morfismo, allora $KerEq(\varphi)$ è una relazione di equivalenza compatibile rispetto ad $\mathbf{A}$.*

Viceversa, se $\mathbf{A}$ è un'algebra e α è una relazione di equivalenza compatibile, allora all'insieme quoziente A/α può essere data la struttura di un algebra $\mathbf{A}/\alpha$ dello stesso tipo di $\mathbf{A}$, mediante le condizioni:

$$f^{\mathbf{A}/\alpha}(a_1/\alpha, \ldots, a_n/\alpha) = (f^{\mathbf{A}}(a_1, \ldots, a_n))/\alpha \tag{2}$$

dove, al solito, $f^{\mathbf{A}}$ varia fra le operazioni di $\mathbf{A}$.

Con la definizione precedente, si ha che π_α è un morfismo da $\mathbf{A}$ ad $\mathbf{A}/\alpha$, e $KerEq(\pi_\alpha) = \alpha$.

Inoltre, se $\varphi : \mathbf{A} \to \mathbf{B}$ è un morfismo, allora $\mathbf{A}/KerEq(\varphi)$ è isomorfa ad $Im(\mathbf{B})$.

Naturalmente, si deve verificare che la condizione (2) sia ben posta. Cioè, se $a_1/\alpha = b_1/\alpha, \ldots,$ cioè $a_1\ \alpha\ b_1, \ldots,$ allora $(f^{\mathbf{A}}(a_1, \ldots, a_n))/\alpha = (f^{\mathbf{A}}(b_1, \ldots, b_n))/\alpha$, cioè $f^{\mathbf{A}}(a_1, \ldots, a_n)\ \alpha\ f^{\mathbf{A}}(b_1, \ldots, b_n)$, ma questa implicazione segue dall'assunto che α sia compatibile (anzi, la compatibilità di α si usa esclusivamente per questa verifica).

Lasciamo le altre verifiche al lettore; osserviamo solo che, per dimostrare l'ultimo enunciato, basta considerare l'isomorfismo $\psi : \mathbf{A}/KerEq(\varphi) \to Im(\mathbf{B})$ che manda a/α in $\varphi(a)$ (c' è da controllare che ψ è effettivamente una biiezione, e che è un morfismo. Ci sarebbe altro da controllare?)

Osservazione 1.37. Ad alcuni lettori probabilmente farà piacere sapere che, se $\varphi : \mathbf{A} \to \mathbf{B}$ e $\alpha = KerEq(\varphi)$ allora φ si può scomporre come

$$\mathbf{A} \xrightarrow{\pi_\alpha} \mathbf{A}/\alpha \xrightarrow{\psi} Im(\varphi) \xrightarrow{\iota} \mathbf{B}$$

dove ψ è l'isomorfismo or ora introdotto, e ι è dato da 1.32 e 1.31.

La Proposizione 1.36 giustifica l'introduzione del seguente concetto che verrà ampiamente usato in seguito.

Definizione 1.38. Una *congruenza* di (o su) un'algebra $\mathbf{A}$ è una relazione di equivalenza compatibile su A. L'insieme delle congruenze su $\mathbf{A}$ si indicherà con $Con(\mathbf{A})$. Se α è una congruenza, a volte diremo che due elementi a, b sono *congruenti* modulo α se $a\ \alpha\ b$.

Esempio 1.39. In ogni algebra $\mathbf{A}$ esistono sempre la congruenza massima $1_\mathbf{A} = A \times A$ e la congruenza minima $0_\mathbf{A} = \{(a, a) \mid a \in A\}$.

$1_\mathbf{A}$ e $0_\mathbf{A}$ sono ovviamente di equivalenza e compatibili.

Altrettanto ovviamente, $\mathbf{A}/1_\mathbf{A}$ è un'algebra con un solo elemento, e $\mathbf{A}/0_\mathbf{A}$ è isomorfa ad $\mathbf{A}$ (infatti la proiezione canonica in questo caso è iniettiva, quindi è un isomorfismo).

Esempio 1.40. Se $\mathbf{G}$ è un gruppo ed $\mathbf{N}$ è un suo sottogruppo normale, la (relazione di equivalenza associata alla) partizione costituita dai laterali di $\mathbf{N}$ è una congruenza di $\mathbf{G}$. Viceversa, se α è una congruenza di $\mathbf{G}$, allora la classe e/α è un sottogruppo normale. Queste due corrispondenze sono una l'inversa dell'altra, quindi sono biunivoche fra l'insieme dei sottogruppi normali di $\mathbf{G}$ e l'insieme delle congruenze di $\mathbf{G}$ (in questo caso non ci sono differenze se si usano le definizioni 1.8(a), (b) o 1.12(c). È in grado di verificarlo il lettore?).

Un discorso completamente analogo vale per gli anelli: per ogni ideale I di un anello $\mathbf{A}$, l'insieme dei laterali di I induce una relazione di equivalenza che è una congruenza in $\mathbf{A}$. Se α è una congruenza in $\mathbf{A}$, allora $0/\alpha$ è un ideale di $\mathbf{A}$. Nel caso si considerassero anelli non commutativi, per "ideale" bisogna intendere "ideale bilatero".

Esempio 1.41. In questi esempi indicheremo una congruenza tramite la partizione associata.

(a) Le congruenze del semireticolo $\mathbf{S}$ descritto in 1.19(c) sono $0_\mathbf{S}$, $1_\mathbf{S}$, e le congruenze associate alle partizioni $\{\{a\}\{0, b\}\}$ e $\{\{b\}\{0, a\}\}$.

Invece la partizione $\{\{0\}\{a, b\}\}$ non determina una congruenza perché, se α è la relazione di equivalenza associata, allora, ad esempio, $a\ \alpha\ a$, $a\ \alpha\ b$, ma non vale $aa = a\ \alpha\ 0 = ab$.

Quindi $Con(\mathbf{S})$ ha 4 elementi.

(b) Verificare che $\mathbf{D}_2$ ha 4 congruenze.

Esempio: $\{\{0, a\}\{b, 1\}\}$ determina una congruenza.

Esiste una congruenza α non banale tale che $a\ \alpha\ b$?

PROPOSIZIONE 1.42. *Se* $\mathbf{A}$ *è un'algebra e* $(\alpha_i)_{i\in I}$ *è una famiglia qualunque di congruenze di* $\mathbf{A}$ *allora* $\bigcap_{i\in I}\alpha_i$ *è ancora una congruenza di* $\mathbf{A}$.

La definizione di $\bigcap_{i\in I}\alpha_i$, per una famiglia $(\alpha_i)_{i\in I}$ di relazioni binarie non dovrebbe creare problemi al lettore, ma per scrupolo esplicitiamo che $\bigcap_{i\in I}\alpha_i = \{(a,b)\in A\times A \mid a\ \alpha_i\ b,\ \text{per ogni } i\in I\}$. In altri termini, $\bigcap_{i\in I}\alpha_i$ è quella relazione binaria α tale che $a\ \alpha\ b$ se e solo se $a\ \alpha_i\ b$, per ogni $i\in I$.

DIMOSTRAZIONE. Una congruenza è una relazione binaria simmetrica, riflessiva, transitiva e compatibile. È facile verificare che l'intersezione di una famiglia di relazioni simmetriche è ancora simmetrica. Infatti, se poniamo $\alpha = \bigcap_{i\in I}\alpha_i$, e $a\ \alpha\ b$, allora $a\ \alpha_i\ b$, per ogni $i\in I$. quindi, siccome per ipotesi tutte le α_i sono simmetriche, si ha che $b\ \alpha_i\ a$, per ogni $i\in I$. Ma questo significa che $b\ \alpha\ a$, cioè, α è simmetrica.

Un ragionamento simile si applica a tutte le altre proprietà menzionate all'inizio. Quindi l'intersezione di una famiglia di relazioni che soddisfano a tutte le proprietà menzionate continua a soddisfarle tutte. □

NB: a differenza che nel caso delle sottostrutture di un'algebra (vedi Proposizione 1.20) qui non dobbiamo preoccuparci della possibilità che $\bigcap_{i\in I}\alpha_i$ sia vuota, perché ogni congruenza contiene $0_{\mathbf{A}}$, che è non vuota.

Come nel caso delle sottoalgebre, la Proposizione 1.42 implica che l'insieme delle congruenze di un'algebra è un reticolo, indicato con $\mathbf{Con}(\mathbf{A})$.

COROLLARIO 1.43. *Sia* $\mathbf{A}$ *un'algebra. Se* $\theta\subseteq A\times A$ *è una relazione binaria, allora esiste la più piccola congruenza* $\langle\theta\rangle_c$ *di* $Con(\mathbf{A})$ *che contiene* θ*, detta* congruenza di $\mathbf{A}$ generata da θ*. Inoltre, l'insieme* $Con(\mathbf{A})$*, ordinato per inclusione, è un reticolo, detto* reticolo delle congruenze di $\mathbf{A}$.

DIMOSTRAZIONE. Per la Proposizione 1.42, la relazione $\langle\theta\rangle_c = \bigcap\{\alpha\in Con(\mathbf{A}) \mid \theta\subseteq\alpha\}$ è una congruenza di $\mathbf{A}$, e quindi è la più piccola congruenza che contiene θ. Il resto è simile alla (e più semplice della) dimostrazione di 1.25. □

OSSERVAZIONE 1.44. NB: casi particolari del reticolo delle congruenze di un'algebra sono sostanzialmente noti dai corsi di algebra classica.

Per esempio, il reticolo dei sottogruppi normali di un gruppo $\mathbf{G}$ è isomorfo al reticolo $\mathbf{Con}(\mathbf{G})$ (vedi 1.40). Le operazioni (di reticolo[4]) nel caso

[4]Il lettore non deve fare confusione fra le operazioni di $\mathbf{G}$ (o, in generale, di un'algebra $\mathbf{A}$) e le operazioni nei reticoli $\mathbf{Con}(\mathbf{G})$ o $\mathbf{Con}(\mathbf{A})$. Ad ogni algebra

dei sottogruppi normali di $\mathbf{G}$ sono però solitamente indicate con $\cap$ e con la giustapposizione MN.

Analogamente, le operazioni nel reticolo degli ideali di un anello commutativo si indicano con $\cap$ e $+$.

Esempio 1.45. Se $\mathbf{S}$ è il semireticolo descritto in 1.19(c), allora $\mathbf{Con}(\mathbf{S})$ è isomorfo al reticolo $\mathbf{D}_2$ di 1.19(d) (vedi l'esempio 1.41(a)).

Osservazione 1.46. (non fa parte del programma) Il lettore potrebbe osservare una notevole somiglianza fra le proposizioni 1.20 e 1.42, e fra le loro conseguenze.

In effetti, tutti questi risultati seguono dal fatto che sia l'insieme delle sottoalgebre (con l'eventuale aggiunta del vuoto) di un'algebra, che l'insieme delle congruenze di un'algebra formano un *sistema di chiusura*. Per questioni di spazio non approfondiremo l'argomento in questa sede; il lettore interessato è invitato a consultare, ad esempio, la sezione 2.4 di [**Be**].

Inoltre, sia il reticolo delle sottoalgebre che il reticolo delle congruenze di un'algebra sono reticoli *completi*, nel senso che esistono minimi e massimi per ogni sottoinsieme del reticolo (non solo per sottoinsiemi di due elementi o, equivalentemente, per sottoinsiemi finiti). Di nuovo, invitiamo il lettore interessato a consultare [**Be**], o altri libri di teoria dei reticoli, ad esempio, [**Gr2, Gr3, GHKLMS**].

Un'altra proprietà importante di questi reticoli è che sono *algebrici*. In termini di reticoli (o, più precisamente, di sistemi di chiusura), questo traduce il fatto che, ad esempio, la sottostruttura generata da C è l'unione delle sottostrutture generate dai sottoinsiemi finiti di C (vedi l'Osservazione 1.66; vedi anche 3.17). Facciamo di nuovo riferimento ai lavori citati per maggiori dettagli.

Osservazione 1.47. Esiste una descrizione *esplicita* della congruenza $\langle\theta\rangle_c$ la cui *esistenza* è data da 1.43. Cf. la Proposizione 1.64. Non avremo bisogno in seguito di questa caratterizzazione, un po' più complicata della caratterizzazione parallela data in 1.64.

1.6. Prodotti. Per semplificare le notazioni, d'ora in poi adotteremo frequentemente la seguente convenzione.

$\mathbf{A}$ vengono associati naturalmente i reticoli $\mathbf{Sub}(\mathbf{A})$ e $\mathbf{Con}(\mathbf{A})$. Questi reticoli sono essi stessi algebre (solitamente di natura completamente diversa da $\mathbf{A}$). Le operazioni di, metti, $\mathbf{Con}(\mathbf{A})$ sono le operazioni di reticolo $\wedge$ e $\vee$; dal punto di vista di $\mathbf{A}$ queste operazioni si applicano alle congruenze di $\mathbf{A}$, non agli elementi di $\mathbf{A}$, quindi non sono affatto operazioni dell'algebra $\mathbf{A}$. È ovvio che, all'inizio, queste considerazioni potrebbero creare una certa confusione nel lettore. Del resto, le operazioni di reticolo di $\mathbf{Con}(\mathbf{A})$ sono esse stesse operazioni a tutti gli effetti, e indicarle con un altro termine creerebbe alla fine una confusione ancora maggiore.

A volte, data un'operazione f, non menzioneremo esplicitamente l'arietà di f e scriveremo semplicemente $f(a, b, \dots)$ per indicare il risultato di f applicata alla n-upla $(a, b, \dots)$. In tutti questi casi sottintendiamo che l'arietà di f e la lunghezza dell'n-upla argomento di f coincidono.

DEFINIZIONE 1.48. Se $\mathbf{A}_1$ e $\mathbf{A}_2$ sono due algebre dello stesso tipo, il loro prodotto $\mathbf{A}_1 \times \mathbf{A}_2$ è l'algebra dello stesso tipo che ha per sostegno il prodotto cartesiano $A_1 \times A_2$ e le cui operazioni sono definite da

$$f^{\mathbf{A}_1 \times \mathbf{A}_2}((a_1, a_2), (b_1, b_2), \dots) = (f^{\mathbf{A}_1}(a_1, b_1, \dots), f^{\mathbf{A}_2}(a_2, b_2, \dots))$$

dove, al solito, abbiamo usato la convenzione introdotta in 1.17, cioè $f^{\mathbf{A}_1}$ varia fra le operazioni di $\mathbf{A}_1$, $f^{\mathbf{A}_2}$ varia fra le corrispondenti operazioni di $\mathbf{A}_2$ (notiamo che abbiamo supposto che $\mathbf{A}_1$ e $\mathbf{A}_2$ hanno lo stesso tipo), ed abbiamo inoltre usato la convenzione appena introdotta sopra sull'arietà delle operazioni.

LEMMA 1.49. *Se $\mathbf{A}_1$ e $\mathbf{A}_2$ sono due algebre dello stesso tipo, si definisca $\pi_1 : A_1 \times A_2 \to A_1$ con $\pi_1(a_1, a_2) = a_1$. Allora π_1 è un morfismo suriettivo*[5] *da $\mathbf{A}_1 \times \mathbf{A}_2$ ad $\mathbf{A}_1$.*

Se π_2 è definito in maniera simmetrica, allora $\pi_2 : \mathbf{A}_1 \times \mathbf{A}_2 \to \mathbf{A}_2$ è un morfismo.

Prodotti infiniti. La definizione 1.48 può essere estesa senza difficoltà al caso del prodotto di un numero finito di algebre dello stesso tipo. Oppure si può iterare il prodotto definito in 1.48, ad esempio, costruendo $(\mathbf{A}_1 \times \mathbf{A}_2) \times \mathbf{A}_3$. Ma, nota bene: $(\mathbf{A}_1 \times \mathbf{A}_2) \times \mathbf{A}_3$ e $\mathbf{A}_1 \times (\mathbf{A}_2 \times \mathbf{A}_3)$ sono algebre *isomorfe* (esercizio!) ma *non* identiche.

In seguito sarà necessario considerare anche prodotti di un numero infinito di algebre (per esempio, durante la dimostrazione del Teorema 2.7, teorema che poi verrà utilizzato quasi ovunque nel seguito). Come afferma C. Bergman, nel caso infinito *è abbastanza difficile capire bene i prodotti ed esercitarsi su di essi (ma è tuttavia necessario).* Il lettore non si deve spaventare per le notazioni, perché nascondono comunque un'idea relativamente semplice. Per abituarsi a trattare coi prodotti infiniti, può essere utile dapprima considerare il caso di un prodotto numerabile, e pensarlo come un prodotto $A_0 \times A_1 \times A_2 \times \dots$.

La definizione di un prodotto infinito di algebre dello stesso tipo infatti non si discosta di molto dalla Definizione 1.48, ma è opportuno

[5]Qui si usa l'assunzione che ogni algebra abbia come sostegno un insieme *non vuoto*. Se si ammettesse la possibilità $A_1 = \emptyset$, allora π_1 non sarebbe suriettivo, se $A_2 \neq \emptyset$.

chiarire, ad ogni evenienza, cosa si intenda per prodotto di una famiglia (eventualmente infinita) di insiemi, e fissare le opportune notazioni.

Il caso numerabile. Presentiamo comunque per primo, a mo' di introduzione per il caso generale, l'esempio del caso numerabile. Il lettore che pensi di non incontrare difficoltà può saltare questo paragrafo e passare direttamente al caso generale. Se $(A_i)_{i\in\mathbb{N}}$ è una successione di insiemi, il prodotto $\prod_{i\in\mathbb{N}} A_i$ è l'insieme delle successioni $(a_i)_{i\in\mathbb{N}}$ tali che $a_i \in A_i$, per ogni $i \in \mathbb{N}$.

Si può pensare a $\prod_{i\in\mathbb{N}} A_i$ come ad $A_0 \times A_1 \times A_2 \times \dots$, e ai suoi elementi come alle successioni $(a_0, a_1, a_2, \dots)$ tali che $a_0 \in A_0$, $a_1 \in A_1$, etc.

Se adesso ciascuna $\mathbf{A}_i$ è un'algebra (tutte dello stesso tipo), definiamo il prodotto $\mathbf{A} = \prod_{i\in\mathbb{N}} \mathbf{A}_i = \mathbf{A}_0 \times \mathbf{A}_1 \times \mathbf{A}_2 \times \dots$ Vogliamo che questo prodotto sia un'algebra con sostegno $\prod_{i\in\mathbb{N}} A_i = A_0 \times A_1 \times A_2 \times \dots$ Consideriamo per semplicità il caso in cui ciascuna $\mathbf{A}_i$ ha un'operazione binaria $\odot^{\mathbf{A}_i}$. In questo caso, la corrispondente operazione di $\mathbf{A} = \prod_{i\in\mathbb{N}} \mathbf{A}_i$ è definita da

$$(a_0, a_1, a_2, \dots) \odot^{\mathbf{A}} (b_0, b_1, b_2, \dots) = \\ (a_0 \odot^{\mathbf{A}_0} b_0,\ a_1 \odot^{\mathbf{A}_1} b_1,\ a_2 \odot^{\mathbf{A}_2} b_2,\ \dots)$$

Se adesso chiamiamo $a = (a_0, a_1, a_2, \dots)$ e $b = (b_0, b_1, b_2, \dots)$, possiamo scrivere la formula precedente in maniera più compatta come

$$a \odot^{\mathbf{A}} b = (a_i \odot^{\mathbf{A}_i} b_i)_{i\in\mathbb{N}}$$

Se abbandoniamo la convenzione di scrivere il risultato dell'operazione come $a \odot^{\mathbf{A}} b$, ma lo scriviamo $\odot^{\mathbf{A}}(a, b)$ (come saremmo "costretti" a fare se $\odot$ avesse arietà > 2), allora le definizioni precedenti vengono scritte, rispettivamente, come

$$\odot^{\mathbf{A}}((a_0, a_1, \dots), (b_0, b_1, \dots)) = \big(\odot^{\mathbf{A}_0}(a_0 b_0), \odot^{\mathbf{A}_1}(a_1, b_1), \dots\big) \tag{3}$$

$$\odot^{\mathbf{A}}(a, b) = \big(\odot^{\mathbf{A}_i}(a_i, b_i)\big)_{i\in\mathbb{N}} \tag{4}$$

Il lettore che trovasse difficoltà nel seguire le argomentazioni successive può rifarsi agli esempi precedenti per chiarire le proprie idee sulla situazione. In prima lettura, probabilmente, potrebbe anche limitarsi a considerare il caso di prodotti di un'infinità numerabile di algebre, cioè il caso già trattato. Purtroppo, dovremo fare comunque uso di prodotti di un insieme più che numerabile di algebre.

Prodotti nel caso generale.

DEFINIZIONE 1.50. Una *successione generalizzata (ad indici su un insieme I) e (ad elementi in un insieme A)*, per brevità, una *sequenza* è una funzione $a : I \to A$.

Spesso si scriverà a_i al posto di $a(i)$, e la stessa funzione a verrà indicata come $(a_i)_{i\in I}$. Osserviamo che questa notazione combacia con quella usuale per indicare le successioni (ad indici in $\mathbb{N}$). Formalmente,

una successione è una funzione s da $\mathbb{N}$ verso un certo insieme; ma solitamente le successioni vengono indicate con $(s_n)_{n\in\mathbb{N}}$ ed s_n indica l'elemento $s(n)$ della successione.

Così come una successione $(s_n)_{n\in\mathbb{N}}$ si può indicare come $(s_0, s_1, \dots, s_n, \dots)$, o semplicemente $(\dots, s_n, \dots)$, o ancora $(\dots, s_n, \dots, s_m, \dots)$, per aiutare l'intuizione si può indicare una sequenza ad indici in I come $(\dots, a_i, \dots)$, o $(\dots, a_i, \dots, a_j, \dots)$. Questa notazione può essere a volte utile, ma va ricordato che la definizione precisa di sequenza è quella data sopra e che, a differenza di $\mathbb{N}$, non si suppone affatto che sull'insieme I sia definita una relazione di ordine.

DEFINIZIONE 1.51. Se $(A_i)_{i\in I}$ è una sequenza di insiemi, il *prodotto (cartesiano* o *diretto*) $\prod_{i\in I} A_i$ della sequenza $(A_i)_{i\in I}$ è definito da

$$\prod_{i\in I} A_i =$$

$$\{a \mid a \text{ è una funzione da } I \text{ a } \bigcup_{i\in I} A_i \text{ tale che } a(i) \in A_i, \text{ per ogni } i \in I\}$$

In parole, $\prod_{i\in I} A_i$ è l'insieme delle sequenze $(a_i)_{i\in I}$ tali che $a_i \in A_i$, per ogni $i \in I$ (come precisato sopra, $a(i)$ ed a_i sono due modi per indicare lo stesso elemento della sequenza).

Se tutti gli A_i sono uguali ad A, si scriverà A^I al posto di $\prod_{i\in I} A_i$, e si parlerà di *potenza* di A. In questo caso A^I è l'insieme di tutte le funzioni da I ad A.

OSSERVAZIONE 1.52. Può sembrare intuitivamente ovvio che, se tutti gli A_i sono diversi dall'insieme vuoto, allora anche $\prod_{i\in I} A_i$ è non vuoto. Questa asserzione è invece equivalente ad un discusso principio di teoria degli insiemi, detto Assioma di Scelta.

Noi assumeremo sempre in queste note la validità dell'Assioma di Scelta. L'uso di questo assioma non sarà comunque mai necessario nel caso in cui I sia finito, cioè, se I è finito ed ogni A_i è non vuoto, allora $\prod_{i\in I} A_i$ è non vuoto.

Alcuni altri brevi commenti su questo assioma sono presentati nell'Osservazione 11.3 in appendice.

DEFINIZIONE 1.53. Se $(\mathbf{A}_i)_{i\in I}$ è una sequenza di algebre dello stesso tipo, il *prodotto* $\prod_{i\in I} \mathbf{A}_i$ di $(\mathbf{A}_i)_{i\in I}$ è l'algebra che ha per sostegno il prodotto cartesiano $\prod_{i\in I} A_i$ e le cui operazioni sono definite come segue. Se $a = (a_i)_{i\in I}$, $b = (b_i)_{i\in I}$ etc. sono elementi di $\prod_{i\in I} A_i$, si definisce

$$f^{\prod_{i\in I} \mathbf{A}_i}(a, b, \dots) = \left(f^{\mathbf{A}_i}(a_i, b_i, \dots)\right)_{i\in I} \tag{5}$$

per ogni operazione $f^{\mathbf{A}_i}$ delle algebre $\mathbf{A}_i$ e per tutte n-uple $(a, b, \dots)$ di elementi di $\prod_{i\in I} A_i$. In altri termini, $f^{\prod_{i\in I}\mathbf{A}_i}(a, b, \dots)$ è quell'elemento $z = (z_i)_{i\in I}$ di $\prod_{i\in I} A_i$ tale che, per ogni $i \in I$, $z_i = f^{\mathbf{A}_i}(a_i, b_i, \dots)$.

Il lettore può confrontare l'equazione (5) con l'equazione (4) introdotta prima della Definizione 1.50.

Se il lettore preferisce la notazione introdotta alla fine di 1.50, le operazioni di $\prod_{i\in I}\mathbf{A}_i$ si possono definire con

(6)
$$f^{\prod_{i\in I}\mathbf{A}_i}((\dots, a_i, \dots), (\dots, b_i, \dots), \dots) = (\dots, f^{\mathbf{A}_i}(a_i, b_i, \dots), \dots)$$

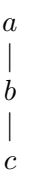
In questo caso può essere utile confrontare (6) con (3).

Il Lemma 1.49 si estende anche al caso infinito.

LEMMA 1.54. *Sotto le ipotesi di 1.53, se $\bar\imath \in I$, allora $\pi_{\bar\imath} : \prod_{i\in I}\mathbf{A}_i \to \mathbf{A}_{\bar\imath}$ è un morfismo, dove $\pi_{\bar\imath}$ è definito da $\pi_{\bar\imath}((a_i)_{i\in I}) = a_{\bar\imath}$.*

1.7. Altri esempi. In questa sezione si presentano alcuni esempi. Questi esempi verranno utilizzati solo sporadicamente nelle sezioni successive, ma possono essere comunque d'aiuto per comprendere le motivazioni di certi risultati.

OSSERVAZIONE 1.55. Si consideri la catena $\mathbf{C}$ con tre elementi



considerata come un reticolo (ma tutto quello che diremo in questo esempio vale anche considerando la sola operazione binaria max o la sola operazione binaria min).

Tutte le relazioni di equivalenza su C sono congruenze di $\mathbf{C}$, ad eccezione della relazione d'equivalenza α associata alla partizione $\{\{a, c\}\{b\}\}$. Infatti $a\ \alpha\ c$ e $b\ \alpha\ b$, ma $\min\{a, b\} = b \not\alpha\ c = \min\{c, b\}$, dunque α non è compatibile.

Il reticolo delle congruenze di $\mathbf{C}$ è isomorfo a $\mathbf{D}_2$ (vedi l'Esempio 1.19(d)).

Il presente esempio mostra che alcune delle proprietà che valgono per le congruenze in certe classi familiari di algebre, come i gruppi e gli anelli, non valgono in generale.

Per esempio, se β è la congruenza associata alla partizione $\{\{b, c\}\{a\}\}$, allora le classi di equivalenza di β non hanno tutte la stessa cardinalità.

Inoltre β e $0_{\mathbf{C}}$ hanno una classe di equivalenza in comune $\{a\}$, ma sono congruenze diverse. Quindi conoscere una classe di equivalenza di una congruenza non determina univocamente la congruenza stessa.

Vedi anche l'Osservazione 1.62.

DEFINIZIONE 1.56. Se $\alpha, \beta \subseteq A \times A$, la *composizione* di α e β è la relazione $\alpha \circ \beta = \{(a, c) \in A \times A \mid \text{esiste } b \in A \text{ tale che } a\ \alpha\ b \text{ e } b\ \beta\ c\}$.

In altre parole, ed estendendo la notazione usata nella Definizione 1.34, abbiamo che $a\ (\alpha \circ \beta)\ c$ se e solo se esiste $b \in A$ tale che $a\ \alpha\ b\ \beta\ c$.

Si noti che l'operazione di composizione è associativa, quindi non c'è necessità di parentesi in scritture del tipo $\alpha \circ \beta \circ \gamma$.

Se α è una relazione binaria su A, la *relazione inversa* di α è la relazione $\alpha^\smile = \{(b, a) \in A \times A \mid a\ \alpha\ b\}$.

LEMMA 1.57. *Se* $\mathbf{A}$ *è un'algebra,* $\alpha, \beta \subseteq A \times A$ *e* α *e* β *sono compatibili, allora anche* $\alpha \circ \beta$ *e* $\alpha^\smile$ *sono compatibili.*

DIMOSTRAZIONE. Se, diciamo, f è n-aria e $a_1\ \alpha \circ \beta\ c_1$, e $a_2\ \alpha \circ \beta\ c_2$, etc., allora esistono $b_1, b_2, \dots \in A$ tali che $a_1\ \alpha\ b_1\ \beta\ c_1$, e $a_2\ \alpha\ b_2\ \beta\ c_2$, etc., quindi, siccome α e β sono compatibili, $f(a_1, a_2, \dots, a_n)\ \alpha\ f(b_1, b_2, \dots, b_n)\ \beta\ f(c_1, c_2, \dots, c_n)$, quindi $f(a_1, a_2, \dots, a_n)\ \alpha \circ \beta\ f(c_1, c_2, \dots, c_n)$. Quindi $\alpha \circ \beta$ è compatibile.

La dimostrazione che $\alpha^\smile$ è compatibile è molto più semplice. □

PROPOSIZIONE 1.58. *Una relazione binaria* α *è transitiva se e solo se* $\alpha \circ \alpha \subseteq \alpha$*; è simmetrica se e solo se* $\alpha^\smile \subseteq \alpha$*. In particolare,* α *è una relazione di equivalenza se e solo se è riflessiva e valgono le inclusioni precedenti.*

LEMMA 1.59. *Se* $\mathbf{A}$ *è un'algebra e* α *è una relazione binaria* riflessiva e transitiva *su* A*, allora* α *è compatibile se e solo se, per ogni* $n \in \mathbb{N}$*, per ogni operazione* n*-aria* f *di* $\mathbf{A}$ *e per ogni* $i = 1, \dots, n$ *si ha che*

(7) $a_i\ \alpha\ b$ *implica*

$$f(a_1, \dots, a_{i-1}, a_i, a_{i+1}, \dots, a_n)\ \alpha\ f(a_1, \dots a_{i-1}, b, a_{i+1}, \dots, a_n)$$

(tutti gli argomenti di f *restano invariati tranne* a_i*, che diventa* b*), per tutti i* $b \in A$ *e tutte le* n*-uple* $(a_1, a_2, \dots, a_n)$ *di elementi di* A*.*

DIMOSTRAZIONE. Se α è compatibile e riflessiva, necessariamente (7) deve essere soddisfatta.

Nell'altra direzione dobbiamo dimostrare che se $a_1\ \alpha\ b_1$, $a_2\ \alpha\ b_2$, etc., allora $f(a_1, a_2, \dots, a_n)\ \alpha\ f(b_1, b_2, \dots, b_n)$. Applicando ripetutamente (7), prima con $i = 1$ e $b = b_1$, poi con $i = 2$ e $b = b_2$, etc., otteniamo

$$\begin{aligned} f(a_1, a_2, a_3, a_4, \dots, a_n)\ \alpha\ f(b_1, a_2, a_3, a_4, \dots, a_n)\ \alpha \\ f(b_1, b_2, a_3, a_4, \dots, a_n)\ \alpha\ f(b_1, b_2, b_3, a_4, \dots, a_n)\ \alpha\ \dots \\ \dots\ \alpha\ f(b_1, \dots, b_{n-3}, a_{n-2}, a_{n-1}, a_n)\ \alpha\ f(b_1, \dots, b_{n-3}, b_{n-2}, a_{n-1}, a_n)\ \alpha \\ f(b_1, \dots, b_{n-3}, b_{n-2}, b_{n-1}, a_n)\ \alpha\ f(b_1, \dots, b_{n-3}, b_{n-2}, b_{n-1}, b_n) \end{aligned}$$

Ma siccome α è transitiva per ipotesi, allora $f(a_1, \ldots, a_n)\ \alpha\ f(b_1, \ldots, b_n)$. □

PROPOSIZIONE 1.60. *[... descrizione di $\alpha \vee \beta$ per relazioni di equivalenza, congruenze per ora vedi* [**Be**, Prop 2.16 e Cor 2.19]*; uno è un sottoreticolo dell'altro (fa parte del programma)]*

PROPOSIZIONE 1.61. *Se $\mathbf{A}$ e $\mathbf{B}$ sono algebre dello stesso tipo e nel prodotto $\mathbf{C} = \mathbf{A} \times \mathbf{B}$ si considerano le congruenze $\alpha_1 = KerEq(\pi_1)$ e $\alpha_2 = KerEq(\pi_2)$ (dove π_1 e π_2 sono definiti nel Lemma 1.49), allora*

$$\alpha_1 \cap \alpha_2 = 0_{\mathbf{C}} \tag{8}$$

$$\alpha_1 \vee \alpha_2 = 1_{\mathbf{C}} \tag{9}$$

$$\alpha_1 \circ \alpha_2 = 1_{\mathbf{C}}. \tag{10}$$

Viceversa, se $\mathbf{C}$ è un'algebra e $\alpha_1, \alpha_2 \in \mathbf{Con}(\mathbf{A})$ soddisfano a (8)-(10)*, allora $\mathbf{C} \cong C/\alpha_1 \times C/\alpha_2$.*

Vedremo in 5.2 che (10) implica (9).

DIMOSTRAZIONE. (fa parte del programma) Per ora, vedi [**Be**, esercizio 1.26.7 e Teorema 3.11] □

OSSERVAZIONE 1.62. Le condizioni (8) e (9) da sole non bastano perché la conclusione di 1.61 sia vera.

Nella catena $\mathbf{C}$ con tre elementi (vedi l'osservazione 1.55) si considerino le congruenze α_1 associata alla partizione $\{\{b, c\}\{a\}\}$, e α_2 associata alla partizione $\{\{c\}\{a, b\}\}$.

Ovviamente, le condizioni (8) e (9) sono soddisfatte, ma $\mathbf{C}$ non è isomorfa a $C/\alpha_1 \times C/\alpha_2$, perchè $|C| = 3$ ma C/α_1 e C/α_2 hanno due elementi ciascuna, quindi il loro prodotto ha 4 elementi.

Del resto $\mathbf{C}$, avendo tre elementi, non può essere il prodotto di due algebre, salvo il caso banale in cui uno dei due fattori è l'algebra banale con un solo elemento.

Una congruenza α su un'algebra $\mathbf{A}$ si dice *finitamente generata* se esistono un numero finito di coppie $(a_1, b_1), \ldots, (a_k, b_k)$ di elementi di A tali che α è la più piccola congruenza di $\mathbf{A}$ che contiene quelle coppie. In altre parole, α è la congruenza generata da $\theta = \{(a_1, b_1), \ldots, (a_k, b_k)\}$. Vedi la Proposizione 1.43.

PROPOSIZIONE 1.63. *Se $(\alpha_i)_{i\in\mathbb{N}}$ è una successione crescente di congruenze di un'algebra $\mathbf{A}$ (cioè $\alpha_i \subseteq \alpha_j$, per $i \leq j \in \mathbb{N}$), allora $\alpha = \bigcup_{i\in\mathbb{N}} \alpha_i$ è una congruenza di $\mathbf{A}$.*

Se inoltre $(\alpha_i)_{i\in\mathbb{N}}$ è strettamente crescente, allora α non è finitamente generata.

DIMOSTRAZIONE. Abbiamo che α è ovviamente riflessiva, poiché tutte le α_i lo sono.

Dimostriamo ora che α è compatibile. Sia quindi f un'operazione n-aria di $\mathbf{A}$ e siano $(a_1, a_2, \ldots, a_n)$ e $(b_1, b_2, \ldots, b_n)$ due n-uple di elementi di A tali che $a_1 \ \alpha \ b_1$, $a_2 \ \alpha \ b_2$, $\ldots$, e $a_n \ \alpha \ b_n$. Vogliamo dimostrare che $f(a_1, a_2, \ldots, a_n) \ \alpha \ f(b_1, b_2, \ldots, b_n)$.

Siccome $\alpha = \bigcup_{i\in\mathbb{N}} \alpha_i$, allora esiste un $i_1 \in \mathbb{N}$ tale che $a_1 \ \alpha_{i_1} \ b_1$; allo stesso modo, $a_2 \ \alpha_{i_2} \ b_2$; per qualche $i_2 \in \mathbb{N}$, etc. Se $i = \sup\{i_1, i_2, \ldots, i_n\}$, allora, poiché la successione è crescente, $a_1 \ \alpha_i \ b_1$, $a_2 \ \alpha_i \ b_2$, $\ldots$, $a_n \ \alpha_i \ b_n$. Siccome α_i è compatibile, $f(a_1, a_2, \ldots, a_n) \ \alpha_i \ f(b_1, b_2, \ldots, b_n)$, ma α_i è contenuta in α, quindi $f(a_1, a_2, \ldots, a_n) \ \alpha \ f(b_1, b_2, \ldots, b_n)$. Abbiamo dimostrato che α è compatibile.

La transitività si dimostra allo stesso modo, e la simmetria è più semplice.

Per dimostrare l'ultima affermazione, supponiamo per assurdo che α sia finitamente generata, diciamo, α è generata da (a_1, b_1), $\ldots$, (a_k, b_k). Come sopra, esistono $i_1, \ldots, i_k \in \mathbb{N}$ tale che $a_1 \ \alpha_{i_1} \ b_1$, $\ldots$, $a_k \ \alpha_{i_k} \ b_k$. Se $i = \sup\{i_1, i_2, \ldots, i_k\}$, allora $a_1 \ \alpha_i \ b_1$, $\ldots$, $a_k \ \alpha_i \ b_k$, quindi $\alpha_i \supseteq \alpha$, perché α è la più piccola congruenza tale che $a_1 \ \alpha \ b_1$, $\ldots$, $a_k \ \alpha \ b_k$. Ma questo contraddice l'ipotesi che $(\alpha_i)_{i\in\mathbb{N}}$ sia strettamente crescente. □

La seguente proposizione fornisce una descrizione più "concreta" della sottoalgebra generata da un sottoinsieme di un'algebra. La proposizione verrà utilizzata esclusivamente nella dimostrazione del Teorema 2.7. Una descrizione più utile (ma che necessita dell'introduzione di nuovi concetti abbastanza astratti anche solo per essere enunciata) verrà presentata nella Proposizione 3.16.

PROPOSIZIONE 1.64. *Sia $\mathbf{A}$ un'algebra e C un sottoinsieme di A tale che $\langle C\rangle \neq \emptyset$. Si definisca per induzione su $i \in \mathbb{N}$:*

$$C_0 = C, \qquad e$$

$$C_{i+1} = C_i \cup \{f(a_1, a_2, \ldots, a_n) \mid f \text{ è un'operazione } n\text{-aria di } \mathbf{A}, \text{ per qualche } n \in \mathbb{N}, \text{ e } a_1, a_2, \ldots, a_n \in C_i\}$$

Allora la sottoalgebra $\langle C\rangle$ di $\mathbf{A}$ generata da C è $\bigcup_{i\in\mathbb{N}} C_i$.

DIMOSTRAZIONE. Per 1.25(1),(3), $\langle C\rangle$ è la più piccola sottoalgebra di $\mathbf{A}$ che contiene C. Siccome $\langle C\rangle \supseteq C$, allora $\langle C\rangle \supseteq C_0$. Siccome $\langle C\rangle$ è una sottoalgebra di $\mathbf{A}$, abbiamo che, per ogni i, se $\langle C\rangle$ contiene C_i allora $\langle C\rangle$ contiene C_{i+1}. Quindi, per induzione, $\langle C\rangle$ contiene tutti i C_i, cioè $\langle C\rangle \supseteq \bigcup_{i\in\mathbb{N}} C_i$.

Resta da dimostrare che $\bigcup_{i\in\mathbb{N}} C_i$ è effettivamente una sottoalgebra di $\mathbf{A}$.

Per ipotesi, $\langle C\rangle \neq \emptyset$, quindi per 1.25(2), $C \neq \emptyset$ oppure $\mathbf{A}$ ha almeno una costante. Nel primo caso $C_0 \neq \emptyset$, nel secondo caso $C_1 \neq \emptyset$, a maggior ragione $\bigcup_{i\in\mathbb{N}} C_i \neq \emptyset$.

Rimane quindi da dimostrare che $\bigcup_{i\in\mathbb{N}} C_i$ è chiuso per le operazioni d $\mathbf{A}$. Se f è un'operazione n-aria e $(a_1, a_2, \dots, a_n)$ è una n-upla di elementi di $\bigcup_{i\in\mathbb{N}} C_i$, allora esisteranno $j_1 \in \mathbb{N}$ tale che $a_1 \in C_{j_1}$, $j_2 \in \mathbb{N}$ tale che $a_2 \in C_{j_2}$, etc. Se $j = \max\{j_1, j_2, \dots\}$, allora $a_1, a_2, \dots \in C_j$. Ma, per definizione di C_{j+1}, abbiamo che $f(a_1, a_2, \dots, a_n) \in C_{j+1} \subseteq \bigcup_{i\in\mathbb{N}} C_i$.

Quindi $\bigcup_{i\in\mathbb{N}} C_i$ è chiuso. □

Esempio 1.65. Sia $\mathbf{G} = (G, \cdot, ^{-1}, e)$ un gruppo, e $C \subseteq G$.

Con le notazioni di 1.64, abbiamo

$$C_0 = C$$

$$C_1 = C \cup \{e\} \cup \{cd | c, d \in C\} \cup \{c^{-1} | c \in C\}$$

Poi C_2 è l'insieme degli elementi di G che (a) sono l'elemento neutro e, oppure si possono scrivere come (b) il prodotto di al massimo 4 elementi di C, oppure (c) come il prodotto dell'inverso di un elemento di C per al massimo 2 elementi di C (d) viceversa, oppure (e) il prodotto di due inversi di elementi di C.

Continuando, si ha che $\langle C\rangle = \bigcup_{i\in\mathbb{N}} C_i = \{e\} \cup \{c_1 c_2 \dots c_\ell \mid c_1, c_2, \dots, c_\ell$ sono tali che $c_k \in C$ oppure $c_k^{-1} \in C$, per $k = 1, \dots \ell\}$.

Quindi $\langle C\rangle$ è effettivamente il sottogruppo generato da C nel senso classico.

Osservazione 1.66. Usando la Proposizione 1.64 si può dimostrare che

$$\langle C\rangle = \bigcup_{F\subseteq C,\ F \text{ finito}} \langle F\rangle \tag{11}$$

Infatti, si dimostra per induzione su i che se $c \in C_i$, allora esiste $F \subseteq C$, F finito tale che $c \in \langle F\rangle$. Un'altra dimostrazione di (11) verrà data nell'Osservazione 3.17.

2. Algebre libere

Osservazione 2.1. Anche se il Teorema di Birkhoff è probabilmente il risultato più eclatante dell'algebra universale di base, molti altri risultati interessanti si possono dimostrare senza farne uso. In effetti, noi non lo utilizzeremo mai. Invece la nozione di algebra libera si rivelerà fondamentale e il teorema di esistenza di algebre libere (Teorema 2.7 in questa sezione) verrà usato parecchie volte in seguito. Naturalmente, il lettore potrà apprezzare le applicazioni del Teorema 2.7 anche qualora non ne volesse leggere la dimostrazione, ovvero la trovasse ostica ad una prima lettura.

Nel seguito parleremo di *classi* di algebre, anziché di *insiemi*. Spiegare il motivo di questa distinzione richiederebbe la trattazione di argomenti che esulano dallo scopo di queste note, anche se vi accenneremo nell'Osservazione 11.4 in appendice. Il lettore può sempre considerare "classe" e "insieme" come sinonimi, o pensare ad una classe come ad un insieme che può essere "tremendamente grande", tanto grande da meritare di essere chiamato in un altro modo. Tanto per fare un esempio, leggermente grossolano ma collegato ad alcuni degli argomenti che seguiranno, non si può considerare il "prodotto di tutti i gruppi" come un gruppo, perché avrebbe cardinalità strettamente maggiore di qualsiasi gruppo, quindi anche di se stesso. Quindi, ad esempio, dobbiamo parlare di *classe* di tutti i gruppi, perché si tratta di un oggetto troppo grande per poter essere considerato come un insieme.

Una classe $\mathcal{K}$ di algebre dello stesso tipo si dice *banale* se contiene solo algebre con un elemento (per *numero di elementi* di un'algebra intenderemo sempre il numero di elementi del suo sostegno). Notiamo che tutte le algebre dello stesso tipo con un solo elemento sono isomorfe. Alcuni dei prossimi teoremi diventerebbero falsi nel caso di classi banali di algebre, pertanto d'ora in poi supporremo sempre che una classe di algebre contenga almeno un'algebra con più di un elemento. Del resto, la teoria delle classi banali di algebre è, appunto, banale.

Definizione 2.2. Se $\mathcal{K}$ è una classe di algebre dello stesso tipo, un'algebra $\mathbf{A}$ si dice *libera in* $\mathcal{K}$ *su* X, o si dice che $\mathbf{A}$ *è un'algebra libera in* $\mathcal{K}$ *generata da* X, se

(1) $X \subseteq A$ e $\mathbf{A}$ è generata da X;
(2) $\mathbf{A} \in \mathcal{K}$;
(3) per ogni algebra $\mathbf{B} \in \mathcal{K}$ e per ogni funzione $\chi : X \to B$, si ha che χ può essere estesa ad un morfismo $\varphi : \mathbf{A} \to \mathbf{B}$ (cioè $\chi(x) = \varphi(x)$, per ogni $x \in X$).

Se esiste un X come sopra, si dirà che $\mathbf{A}$ è un'algebra *libera in* $\mathcal{K}$ *su (un insieme di)* $|X|$ *generatori*.

Se la classe $\mathcal{K}$ è chiara dal contesto, non la menzioneremo.

Osservazione 2.3. Non è difficile verificare che (fissata $\mathcal{K}$) se $\mathbf{A}$ è libera su X, $\mathbf{A}'$ è libera su X' e $|X| = |X'|$, allora $\mathbf{A}$ ed $\mathbf{A}'$ sono isomorfe (e, data una biiezione fra X ed X', c'è un isomorfismo che estende questa biiezione).

Questa osservazione non ci servirà nel seguito, ma ci autorizza a parlare del*la* algebra libera in $\mathcal{K}$ su $|X|$ generatori.

NB: in molti testi si fa la distinzione fra algebra libera *in* $\mathcal{K}$ e algebra libera *per* $\mathcal{K}$. Nel secondo caso *non* si richiede che un'algebra libera stia in $\mathcal{K}$. Ovviamente, un'algebra libera *per* $\mathcal{K}$ non è necessariamente unica. Noi intenderemo sempre algebra libera nel senso di algebra libera *in* $\mathcal{K}$.

Esempio 2.4. (a) Ad esempio, $\mathbb{Z}[x]$ è l'anello libero su 1 generatore (qui $\mathcal{K}$ è la classe degli anelli commutativi con 1).

(b) Allo stesso modo, $\mathbb{Z}[x_1, \ldots, x_n]$ è l'anello commutativo libero (con unità) su n generatori (cosa bisognerebbe modificare se si considerassero anelli non commutativi?)

(c) Se considerato come gruppo additivo, $\mathbb{Z}$ è il gruppo libero generato da un elemento. Il prodotto $\mathbb{Z}^n$ è il gruppo *abeliano* libero generato da n elementi.

(d) [... gruppo libero;]

Per ora si può guardare la sezione "Construction" su wikipedia:

`https://en.wikipedia.org/w/index.php?title=Free_group&oldid=728805336`

(fa parte del programma)

(e) Come esempio meno convenzionale, se $\mathcal{K}$ è la classe delle algebre senza operazioni, ogni algebra è libera su se stessa— più esattamente, sul suo sostegno (in questo caso, morfismo è sinonimo di funzione).

(f) Il reticolo libero su 1 elemento ha cardinalità 1.

(non fa parte del programma) Il reticolo libero su 2 elementi ha cardinalità 4, mentre non è immediato verificare che il reticolo libero su un insieme di 3 elementi è infinito.

Il reticolo *distributivo* libero su 3 elementi ha cardinalità 18 (vedi diagramma a p. 102 di [**Be**]).

Il reticolo *modulare* libero su 3 elementi ha cardinalità 28. Questo risultato è dovuto a Dedekind, che si era posto il problema di quanti sottogruppi di un gruppo abeliano si potessero costruire a partire da tre sottogruppi dati, e usando solo intersezione e somma (i problemi sono collegati per il Teorema 5.5 e la Proposizione 5.7 che vedremo in seguito). Invece il reticolo modulare su 4 o più elementi è infinito.

(g) Descriveremo nella sezione 10 le algebre libere nella classe di *tutte* le algebre di uno stesso tipo.

Osservazione 2.5. Gli esempi precedenti mostrano che la nozione di algebra libera dipende fortemente dalla classe $\mathcal{K}$ presa in considerazione. L'apparente eterogeneità degli esempi precedenti potrebbe far pensare che sia particolarmente difficoltoso costruire, in generale, algebre libere. In realtà esse possono venire costruite in una maniera relativamente uniforme, sotto certe ipotesi su $\mathcal{K}$ (ma questo non significa che se ne possa dare una semplice descrizione concreta, nel senso, diciamo, utile per sviluppare calcoli su di esse).

Per semplicità, nei ragionamenti e nelle dimostrazioni che seguono, ci limiteremo a considerare algebre libere su n generatori, con n finito. Il caso finito, insieme al caso numerabile, sono i casi più significativi per l'utilizzo delle algebre libere (anche se, per dimostrare il Teorema di Birkhoff nella sezione 4, utilizzeremo algebre libere su insiemi di cardinalità arbitraria). Comunque, tutte le argomentazioni seguenti si estendono al caso generale

di cardinalità arbitraria; l'unica difficoltà potrebbe essere quella di scegliere una notazione opportuna.

Osservando che, dato un prodotto $\mathbf{C} = \prod_{i \in I} \mathbf{C}_i$ di algebre, abbiamo che, per ogni $\bar{\imath} \in I$, esiste un morfismo $\pi_{\bar{\imath}} : \mathbf{C} \to \mathbf{C}_{\bar{\imath}}$ (Lemma 1.54), un'idea per fare in modo che la condizione 2.2(3) sia verificata (mettiamo, nel caso in cui $|X| = n$) è quella di considerare il prodotto di tutte le algebre generate da n elementi. Non c'è nessuna ragione per supporre che questo prodotto sia generato da n elementi (vorremmo che anche 2.2(1) fosse verificata!), ma si può provare a considerare un'opportuna sottoalgebra del prodotto. Per finire, se vogliamo che questa algebra che costruiamo appartenga a $\mathcal{K}$ (cioè che valga 2.2(2)), è sufficiente supporre che $\mathcal{K}$ sia chiusa per prodotti e per sottostrutture.

Sostanzialmente, la dimostrazione di esistenza di algebre libere utilizzerà gli argomenti precedenti, ma c'è una difficoltà tecnica: il prodotto di *tutte* le algebre generate da n elementi non esiste! Nel senso che la collezione di tutte le algebre generate da n elementi è una classe propria, cioè una "collezione troppo grande" per essere trattata come un insieme senza correre il rischio di incorrere in paradossi. Come abbiamo notato, il "prodotto di tutti i gruppi" è (cioè, sarebbe...) troppo grande per essere considerato esso stesso un gruppo.

In effetti, non è necessario prendere in considerazione *tutte* le algebre generate da n elementi, ma basta considerare un'algebra per ogni "classe di isomorfismo", nel senso che specificheremo durante la dimostrazione.

Osservazione 2.6. Ci teniamo a precisare che la dimostrazione che presenteremo è ben lontana dall'essere la più elegante possibile. Però, nello spirito dell'introduzione, questa dimostrazione non necessita di molti prerequisiti e non contiene argomenti eccessivamente astratti. Chi proseguirà nello studio dell'algebra universale apprezzerà sicuramente le informazioni aggiuntive che sono fornite da altre dimostrazioni. Cf., in particolare, la Sezione 10.

Teorema 2.7. *Sia $\mathcal{K}$ una classe di algebre dello stesso tipo, chiusa per prodotti e per sottostrutture. Allora, per ogni insieme $Y \neq \emptyset$, esiste un'algebra libera in $\mathcal{K}$ su $|Y|$ generatori.*

Dimostrazione. Per semplicità, dimostreremo il teorema nel caso finito, cioè dimostreremo che, per ogni $n \in \mathbb{N}$, $n > 0$, esiste un'algebra libera in $\mathcal{K}$ su n generatori. Il caso infinito si dimostra esattamente allo stesso modo, semplicemente avendo cura di introdurre una notazione opportuna.

Consideriamo $n+1$-uple della forma $(\mathbf{C}, c_1, \ldots, c_n)$, dove $\mathbf{C} \in \mathcal{K}$ e $\{c_1, \ldots, c_n\}$ è un insieme di generatori per $\mathbf{C}$. Fissiamo un insieme di $n+1$-uple della forma sopra indicata, diciamo, $\{(\mathbf{C}_i, c_{1,i} \ldots, c_{n,i}) \mid i \in I\}$ tale che, per ogni $(\mathbf{C}, c_1, \ldots, c_n)$ di quella forma esistono un $i \in I$ ed un isomorfismo $\psi : \mathbf{C}_i \to \mathbf{C}$ tale che $\psi(c_{1,i}) = c_1$, $\ldots$, $\psi(c_{n,i}) = c_n$.

Consideriamo il prodotto $\prod_{i\in I}\mathbf{C}_i$, e sia $\mathbf{A}$ la sottostruttura di $\prod_{i\in I}\mathbf{C}_i$ generata dagli elementi $\{a_1,\dots,a_n\}$, dove $a_1=(c_{1,i})_{i\in I}$, $a_2=(c_{2,i})_{i\in I}$, etc.

Siccome $\mathcal{K}$ è chiusa per prodotti e sottostrutture, e siccome tutte le $\mathbf{C}_i$ sono in $\mathcal{K}$, abbiamo $\mathbf{A}\in\mathcal{K}$. Per costruzione, $\mathbf{A}$ è generata da $X=\{a_1,\dots,a_n\}$. Resta quindi solo da verificare la proprietà (3) della Definizione 2.2.[6]

Sia dunque $\mathbf{B}$ un'algebra in $\mathcal{K}$, sia $\chi: X\to B$, e sia $\mathbf{B}'$ la sottoalgebra di $\mathbf{B}$ generata da $\{\chi(a_1),\dots,\chi(a_n)\}$. La n+1-pla $(\mathbf{B}',\chi(a_1),\dots,\chi(a_n))$ è della forma considerata all'inizio, quindi esistono un $\bar\imath\in I$ ed un isomorfismo $\psi:\mathbf{C}_{\bar\imath}\to\mathbf{B}'$ tale che $\psi(c_{1,\bar\imath})=\chi(a_1)$, …, $\psi(c_{n,\bar\imath})=\chi(a_n)$.

Se adesso componiamo l'inclusione $\iota:\mathbf{A}\to\prod_{i\in I}\mathbf{C}_i$ (che è un morfismo per la Proposizione 1.31), la proiezione $\pi_{\bar\imath}:\prod_{i\in I}\mathbf{C}_i\to\mathbf{C}_{\bar\imath}$ (che è un morfismo per il Lemma 1.54), l'isomorfismo $\psi:\mathbf{C}_{\bar\imath}\to\mathbf{B}'$ e l'inclusione $\iota':\mathbf{B}'\to\mathbf{B}$ come nel seguente diagramma

$$\mathbf{A}\xrightarrow{\iota}\prod_{i\in I}\mathbf{C}_i\xrightarrow{\pi_{\bar\imath}}\mathbf{C}_{\bar\imath}\xrightarrow{\psi}\mathbf{B}'\xrightarrow{\iota'}\mathbf{B}$$

otteniamo il morfismo cercato, cioè $\varphi=\iota\circ\pi_{\bar\imath}\circ\psi\circ\iota'$ (ricordiamo che la composizione di morfismi è ancora un morfismo, vedi la Proposizione 1.30). □

Osservazione 2.8. Forse alcuni lettori troveranno non del tutto scontata l'esistenza di un insieme come quello fissato all'inizio della dimostrazione di 2.7. Nel caso particolare che abbiamo preso in considerazione (cioè dell'algebra libera su un numero finito di generatori in un tipo con un numero finito di operazioni) si può notare che un'algebra finitamente generata è finita o al massimo numerabile (questo segue immediatamente dalla Proposizione 1.64). Quindi un'algebra di questo tipo è isomorfa ad un'algebra su $\mathbb{N}$ o su un suo sottoinsieme finito, e le ipotesi standard usate in teoria degli insiemi garantiscono che esiste l'insieme di tutte le algebre di un certo tipo su $\mathbb{N}$ o su un suo sottoinsieme[7].

[6] Che gli $a_1,\dots,a_n$ siano tutti diversi, cioè che X abbia effettivamente cardinalità n, segue dall'ipotesi che $\mathcal{K}$ sia non banale. A parte questo, tutto il ragionamento nella dimostrazione sarebbe valido anche nel caso di una classe banale.

[7] Ad essere pignoli, stiamo implicitamente supponendo che $\mathcal{K}$ sia chiusa anche per isomorfismi. Altrimenti sarebbe necessario usare una forma forte dell'assioma di scelta. Oppure, si può prima dimostrare il Teorema 2.7 per la classe $\mathcal{K}'$ di tutte le algebre isomorfe a qualche algebra di $\mathcal{K}$. Siccome $\mathcal{K}'$ è chiusa per isomorfismo, si può applicare il ragionamento precedente a $\mathcal{K}'$; quindi la dimostrazione del teorema ci fornisce un'algebra $\mathbf{A}'$ libera in $\mathcal{K}'$. Ma, per definizione di $\mathcal{K}'$, $\mathbf{A}'$ è isomorfa a qualche algebra $\mathbf{A}\in\mathcal{K}$, e segue subito che $\mathbf{A}$ è libera in $\mathcal{K}$.

Una costruzione esplicita - decisamente più elegante e che vale nel caso più generale - di un insieme $\{(\mathbf{C}_i, c_{1,i} \ldots, c_{n,i}) \mid i \in I\}$ che soddisfa alla proprietà voluta verrà fornita nella Sezione 10.

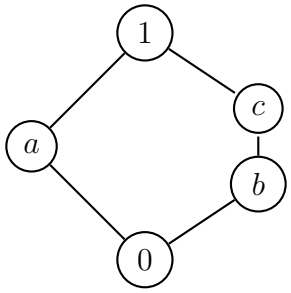
OSSERVAZIONE 2.9. È possibile parlare di "algebra libera su $\emptyset$", cioè di "algebra libera su 0 elementi" solo se consideriamo un tipo con almeno una costante. Infatti, solo in questo caso si può parlare di algebra generata da $\emptyset$. La dimostrazione precedente vale in questo caso.

3. Termini

Il succo di questa sezione. Un *termine* è, grossomodo, un'espressione che si può costruire usando operazioni e variabili. Ad esempio, nel caso dei gruppi, si può pensare ad un termine come ad un'espressione del tipo xyx^{-1}, oppure $xyxy$, oppure x^2yzx^{-1}. Nel caso degli anelli, un termine corrisponde grossomodo ad un polinomio, ad esempio, $p(x)$ dato da $x^3 + 2x^2 - x + 3$ oppure $q(x, y, z)$ dato da $x^2y + y^5z + 2$.

Se assegnamo dei valori alle variabili, possiamo calcolare il valore che assume il termine, proprio come quando calcoliamo il valore di un polinomio. Ad esempio, $p(1) = 5$ e $q(1, -1, 3) = -2$ nel caso dei polinomi che abbiamo indicato.

Naturalmente, possiamo fare tutto questo anche nel caso dei reticoli; ad esempio, il termine $t(x, y, z)$ dato da $(x \vee y) \wedge (x \vee z) \wedge (y \vee z)$ si può pensare come un termine per i reticoli. Il valore di questo termine si può calcolare ogni volta che si assegnano ad x, y, z dei valori in un reticolo. Ad esempio, se calcoliamo $t(a, b, b)$ nel reticolo $\mathbf{D}_2$ presentato nell'esempio 1.19(d) otteniamo $(a \vee b) \wedge (a \vee b) \wedge (b \vee b) = 1 \wedge 1 \wedge b = b$. In realtà $t(a, b, b) = b$ vale in qualunque reticolo. Come altro esempio, calcoliamo $t(a, b, c)$ nel seguente reticolo $\mathbf{N}_5$.



Otteniamo $t(a, b, c) = 1 \wedge 1 \wedge c = c$.

Se poniamo due termini uguali otteniamo una *identità*. Per esempio, un gruppo è abeliano se soddisfa all'identità $xy = yx$, equivalentemente, all'identità $xyx^{-1}y^{-1} = e$. Un anello è commutativo se soddisfa all'identità $xy = yx$. Un reticolo è *distributivo* se soddisfa all'identità

$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ ed è *modulare* se soddisfa all'identità $x \wedge (y \vee (x \wedge z)) = (x \wedge y) \vee (x \wedge z)$.

Naturalmente, nel caso generale, tutte queste espressioni potrebbero essere molto più complicate. Ad esempio, se c è una costante, f è quaternaria e g è binaria, uno fra i tanti possibili termini è

$$g(f(c, x, y, g(z, g(c, g(c, x)))), g(f(z, z, z, z), c))$$

È abbastanza naturale supporre che, se $\mathbf{A}$ è un'algebra e $C \subseteq A$, allora la sottoalgebra generata da C è l'insieme di tutti gli elementi della forma $t(a_1, a_2, \ldots, a_n)$, dove t varia fra tutti i termini e $a_1, a_2, \ldots, a_n \in C$. In effetti, questo è vero, e sarà dimostrato in 3.16. Cf. l'Esempio 1.65.

Inoltre, se $\varphi : \mathbf{A} \to \mathbf{B}$ è un morfismo e $a_1, a_2, \ldots, a_n \in A$, allora $\varphi(t(a_1, a_2, \ldots, a_n)) = t(\varphi(a_1), \varphi(a_2), \ldots, \varphi(a_n))$, per ogni termine t. Anche questo è abbastanza ovvio, e sarà comunque dimostrato in 3.10.

Per finire, se un'identità ε che coinvolge al massimo n variabili vale nell'algebra libera $\mathbf{F}$ in $\mathcal{K}$ su n elementi, allora ε vale in tutte le algebre di $\mathcal{K}$. Questo risultato a prima vista può apparire stupefacente, ma è un'immediata conseguenza della definizione di algebra libera e della relazione appena menzionata fra termini e morfismi. Supponiamo infatti che ε sia della forma $t(x_1, \ldots, x_n) = s(x_1, \ldots, x_n)$. Se $a_1, \ldots, a_n$ sono elementi di un'algebra $\mathbf{A}$ in $\mathcal{K}$, allora, siccome $\mathbf{F}$ è libera, esiste un morfismo $\varphi : \mathbf{F} \to \mathbf{A}$ tale che $\varphi(y_1) = a_1$, $\ldots$, $\varphi(y_n) = a_n$, dove $y_1, \ldots, y_n$ sono i generatori di $\mathbf{F}$. Quindi, $t(a_1, \ldots, a_n) = t(\varphi(y_1), \ldots, \varphi(y_n)) = \varphi(t(y_1, \ldots, y_n)) = \varphi(s(y_1, \ldots, y_n)) = s(\varphi(y_1), \ldots, \varphi(y_n)) = s(a_1, \ldots, a_n)$, dove abbiamo usato due volte la proprietà menzionata nel paragrafo precedente e l'uguaglianza centrale segue dall'ipotesi che ε sia valida in $\mathbf{F}$. Quindi ε vale anche in $\mathbf{A}$. I dettagli completi sono nel Teorema 3.13.

Il lettore che si senta soddisfatto da questa breve introduzione può passare direttamente alle prossime sezioni.

Osservazione 3.1. Osserviamo però che, nell'introduzione precedente, abbiamo usato a ragion veduta l'avverbio *grossomodo*, e ci siamo premurati di precisare spesso *si può pensare come...* etc. Innanzitutto, quando si tratta di anelli, di gruppi, o anche di reticoli, ci si pone in una situazione, sotto un certo punto di vista, relativamente semplice. Le operazioni binarie sono associative, quindi la maggior parte delle espressioni che si scrivono non hanno bisogno di parentesi; inoltre non esistono operazioni che dipendono da più di due argomenti, e si può quindi inserire il simbolo di operazione in mezzo agli operandi. Tutto questo nel caso generale solitamente non è vero,

Quindi, ad esempio, $x(yz)$ e $(xy)z$ *devono essere considerati termini distinti.* Anche solo questo piccolo esempio suggerisce che (purtroppo?) per

estendere in maniera precisa le "definizioni" precedenti è necessario introdurre dettagli tecnici che a prima vista sembrerebbero eccessivamente astratti. Il lettore dovrebbe cercare di tenere sempre a mente come modello gli esempi appena menzionati.

Ci spiace inoltre deludere il lettore che si fosse dichiarato soddisfatto delle considerazioni precedenti, ma abbiamo omesso un punto decisamente importante, cioè la distinzione fra operazioni vere e proprie, da un lato, e simboli algebrici che le rappresentano, dall'altro. Come spieghiamo più sotto, questa distinzione è già implicita nell'uso comune in algebra "classica" (anzi, in un certo senso, è proprio quella che caratterizza la natura "algebrica" dell'algebra), ma, nel nostro ambito generale, non precisare la differenza genererebbe una notevole confusione[8]. Del resto, molte strutture algebriche fondamentali vengono costruite proprio facendo uso di queste nozioni formali e simboliche (abbiamo già visto l'esempio del gruppo libero; in realtà anche la costruzione dell'anello dei polinomi su un anello $\mathbf{A}$ è, all'atto pratico, un esempio di costruzione formale di questo tipo; vedremo nella Sezione 10 che anche le algebre libere in una varietà possono essere viste utilmente come quozienti di un'algebra costruita coi termini di un dato tipo).

Osservazione 3.2. Se $\mathbf{A}$ è un anello, $a \in A$ e $p(x)$ è un polinomio a coefficienti in A, è intuitivamente chiaro cosa significa calcolare $p(a)$. È anche molto chiaro cosa significhi dire che $\mathbf{A}$ soddisfa ad una certa identità, per esempio, che $\mathbf{A}$ soddisfa ad $ab = ba$ (cioè $\mathbf{A}$ è commutativo), oppure ad $a^2 = a$.

In algebra universale è necessario dare le definizioni di concetti analoghi a quelli descritti sopra (valutazione di un "polinomio" e soddisfacimento di un'identità).

Dato un tipo di similarità (per noi ora è una m-upla $(n_1, \dots n_m)$, vedi la Definizione 1.27) è necessario innanzitutto introdurre un simbolo che rappresenta ogni operazione collegata al tipo. Ad esempio, al tipo $(n_1, \dots n_m)$ associamo simboli f_1, ..., f_m che intendono rappresentare operazioni, rispettivamente, n_1-arie, ..., n_m-arie.

Questo corrisponde comunque a ciò che si fa implicitamente in algebra classica per le strutture usuali, come i gruppi. Come abbiamo notato in 1.4, l'operazione $+$ in un gruppo $\mathbf{G}$ andrebbe più precisamente indicata con $+^{\mathbf{G}}$. Ma quando diciamo, ad esempio, che un gruppo abeliano è un gruppo che soddisfa a $g + h = h + g$, non abbiamo in mente nessun gruppo particolare; in questo caso, $+$ non è essa stessa un'operazione, ma un simbolo che rappresenta una possibile operazione. Naturalmente, nel caso dei gruppi e degli anelli, rendere esplicita questa distinzione usando simboli appropriati è solitamente considerata una pedanteria inutile, perché è sempre chiaro

[8]Come afferma argutamente G. Lolli, confondere un simbolo di relazione con una relazione *è come mettere nella stessa pentola la carne e un sacchetto del supermercato.*

(almeno, dovrebbe essere chiaro) di cosa si sta parlando. Nel nostro caso, però, confondere operazioni coi simboli che le rappresentano potrebbe generare parecchia confusione. Introdurremo esplicitamente l'uso di questi simboli nella prossima convenzione. Facciamo comunque notare che l'introduzione di nuovi simboli è anche un possibile modo per estendere le nostre nozioni di tipo e di algebra al caso di un numero infinito di operazioni. Alcuni dettagli sono presentati nelle Osservazioni 11.5 e 11.6 in appendice.

CONVENZIONE 3.3. *D'ora in poi, considereremo un tipo* $\tau = (n_1, \ldots, n_m)$ *arbitrario ma fissato una volta per tutte. Supporremo che tutte le algebre* $\mathbf{A}$ *prese in considerazione siano di questo tipo* τ*, e le operazioni di ogni* $\mathbf{A}$ *verranno sempre indicate con* $f_1^{\mathbf{A}}, \ldots, f_m^{\mathbf{A}}$*, o, semplicemente, con* $f^{\mathbf{A}}$*, facendo variare* $f^{\mathbf{A}}$ *in* $F^{\mathbf{A}} = \{f_1^{\mathbf{A}}, \ldots, f_m^{\mathbf{A}}\}$*, come del resto stiamo facendo a partire dalla Definizione 1.17.*

Ogni volta che parleremo di una classe $\mathcal{K}$ *di algebre sottintenderemo che tutte le algebre di* $\mathcal{K}$ *sono di questo tipo* τ *fissato, anche quando non menzioneremo esplicitamente questa ipotesi.*

Considereremo anche un insieme $F = \{f_1, \ldots, f_m\}$ *detto di* simboli di operazione*, dove gli* $f_1, \ldots, f_m$ *sono distinti e, per* $j = 1, \ldots, m$*, si dirà che* f_j *è un simbolo* n_j*-ario.*

La gran parte delle nozioni che definiremo saranno dipendenti dal tipo τ*, e spesso sottintenderemo questa dipendenza anche quando non menzioneremo esplicitamente* τ*.*

DEFINIZIONE 3.4. Se $X = \{x_1, \ldots, x_n\}$ è un insieme (i cui elementi verranno chiamati *variabili*[9]), l'insieme dei *termini (di tipo* τ *in* $\{x_1, \ldots, x_n\}$, o semplicemente *in* n *variabili*) è definito per induzione come segue.

(1) Ogni simbolo di costante (cioè di operazione 0-aria) è un termine.
(2) Ogni variabile $x_1, \ldots, x_n$ è un termine.
(3) Se f è un simbolo di operazione k-ario e $t_1, \ldots, t_k$ sono termini, allora $f(t_1, \ldots, t_k)$ è un termine.
(4) Nient'altro è un termine. Cioè una sequenza finita di simboli è un termine se e solo se può essere ottenuta mediante l'applicazione di un numero finito dei passi (1), (2) e (3) precedenti.

La natura induttiva della definizione precedente potrebbe sfuggire al lettore, e forse la definizione stessa potrebbe non apparire troppo chiara. La seguente riformulazione sarà comunque utile.

[9]Per evitare sovrapposizioni, si suppone che $X \cap F = \emptyset$.

DEFINIZIONE 3.5. I termini (in $X = \{x_1, \ldots, x_n\}$) di *livello* (o *grado, altezza, complessità*) 0 sono le costanti di F e le variabili di X.

Se $i \in \mathbb{N}$ e abbiamo definito i termini di livello j per ogni $j \leq i$, allora i *termini di livello* $i+1$ sono tutti i termini del tipo $f(t_1, \ldots, t_k)$, dove f è un simbolo di operazione k-ario, $t_1, \ldots, t_k$ sono termini di livello $\leq i$ e almeno uno fra i $t_1, \ldots, t_k$ è di livello i.

Così, una sequenza finita di simboli t è un termine (secondo la Definizione 3.4) se e solo se esiste un $i \in \mathbb{N}$ tale che t è un termine di livello i (secondo la Definizione 3.5).

ESEMPIO 3.6. Ad esempio, se f è quaternaria, g è binaria, c è una costante ed x, y, z, w sono variabili, allora il seguente termine t

$$f(g(x,y), c, g(x, g(z,w)), f(y,y,y, f(c, x, f(x,y,z,w), z)))$$

è un termine di livello 4.

Osserviamo che t è $f(t_1, t_2, t_3, t_4)$, dove t_1 è $g(x,y)$, di livello 1, t_2 è c, di livello 0, t_3 è $g(x, g(z,w))$, di livello 2 e t_4 è $f(y,y,y, f(c, x, f(x,y,z,w), z))$, di livello 3.

ESEMPIO 3.7. Qual è la relazione fra le definizioni appena date e i polinomi a coefficienti in un anello a cui abbiamo accennato all'inizio della sezione?

Come già fatto notare, nel caso degli anelli le operazioni dipendono al massimo da due argomenti, e in quel caso vale la proprietà associativa. Tutto questo nel caso generale solitamente non è vero, quindi la definizione analoga a quella di polinomio diventa estremamente più complicata.

Facciamo adesso vedere che un polinomio, ad esempio, $x^2 - 1$, si può interpretare come un termine, nel senso appena definito. Questo non getta alcuna nuova luce sui polinomi, sia chiaro. Cos'è un polinomio lo si spiega già alle superiori, magari non presentando la definizione più formalmente rigorosa, ma certo non c'è bisogno di definizioni quali 3.4 e 3.5 per introdurre la nozione di polinomio. L'esempio seguente suggerisce però che la nostra definizione di termine potrà svolgere un ruolo analogo a quello svolto dai polinomi per gli anelli.

Se pensiamo ad un anello commutativo con unità come ad un algebra $(A, +, \cdot, -, 0, 1)$, cioè ad un'algebra di tipo $\tau = (2, 2, 1, 0, 0)$ (qui $-$ indica l'opposto, non la sottrazione!), allora il polinomio $x^2 - 1$ si può costruire come un termine $t(x)$ di livello 2 al seguente modo.

Abbiamo che 1 è una costante, quindi un termine di livello 0. Applicando l'operazione unaria $-$ otteniamo il termine $t'(x) = -1$ di livello 1. Inoltre, x è una variabile, quindi un termine di livello 0. Siccome x^2 è un'abbreviazione di $x \cdot x$, o di $\cdot(x, x)$, allora $t''(x) = x^2$ è anch'esso un termine di livello 1. Quindi $x^2 - 1$, abbreviazione di $x^2 + (-1)$ è $t''(x) + t'(x)$, o anche $+(t''(x), t'(x))$, in conclusione, un termine di livello 2.

Generalizzando, abbiamo che ogni polinomio a coefficienti in $\mathbb{Z}$ è (piuttosto, si può esprimere come) un termine di tipo τ, e ad ogni termine corrisponde un polinomio a coefficienti in $\mathbb{Z}$. (Questa corrispondenza non è biunivoca, perché, ad esempio, $(x^2 + x) + 1$ e $x^2 + (x + 1)$ sono due termini diversi, anche se corrispondono allo stesso polinomio, ma questa osservazione non è particolarmente rilevante per il discorso che stiamo facendo ora).

Per ottenere polinomi a coefficienti in un anello $\mathbf{A}$ dovremmo aggiungere al nostro tipo nuove costanti, una per ogni elemento di A, ma gli argomenti non sono significativamente diversi.

Introduciamo adesso una serie di convenzioni sulle notazioni. Queste convenzioni risulteranno molto comode.

Per indicare che t è un termine in $\{x_1, \dots, x_n\}$, scriveremo frequentemente $t(x_1, \dots, x_n)$. È da notare che se consideriamo ulteriori variabili $x_{n+1}, x_{n+2}, \dots$ un termine in $\{x_1, \dots, x_n\}$ si può considerare anche come un termine in $\{x_1, \dots, x_n, x_{n+1}, x_{n+2}, \dots\}$. Questa osservazione non ci creerà nessun problema, ma dobbiamo precisare che, quando scriveremo $t(x_1, \dots, x_n)$, intenderemo che *alcune* fra le variabili $x_1, \dots, x_n$ compaiono in t, ma *non necessariamente tutte* le variabili $x_1, \dots, x_n$ compaiono in t. Infatti, è addirittura possibile che nessuna variabile compaia in t, ad esempio, se t è una costante, oppure se t è costruito solo a partire da costanti senza fare uso di variabili, come ad esempio $f(c_1, c_3, g(c_1, c_2), c_4)$.

Comunque, quando scriveremo $t(x_1, \dots, x_n)$ assumeremo che *tutte* le variabili che compaiono in t (cioè che sono state usate durante la costruzione induttiva di t) siano comprese nell'insieme $\{x_1, \dots, x_n\}$. Assumeremo anche che gli $x_1, \dots, x_n$ siano a due a due distinti.

Introduciamo adesso l'analogo del calcolare il valore $p(a)$ di un polinomio $p(x)$ per un qualche $a \in A$.

DEFINIZIONE 3.8. Se $\mathbf{A}$ è un'algebra e $(a_1, \dots, a_n)$ è una n-upla di elementi di A, definiamo ora la *valutazione* o l'*interpretazione* $t^{\mathbf{A}}(a_1, \dots, a_n)$ di un termine $t(x_1, \dots, x_n)$ (in $\{x_1, \dots, x_n\}$, secondo l'*assegnazione* $x_1 \mapsto a_1, \dots, x_n \mapsto a_n$).

Intuitivamente, $t^{\mathbf{A}}(a_1, \dots, a_n)$ si ottiene sostituendo a_1 ad x_1 etc, nell'espressione di t, ma per dare una definizione precisa la valutazione va definita per induzione sul livello di t.

Se t ha livello 0 ed è il simbolo di costante c, allora poniamo $t^{\mathbf{A}}(a_1, \dots, a_n) = c^{\mathbf{A}}$.

Se t ha livello 0 ed è la variabile x_ℓ, allora poniamo $t^{\mathbf{A}}(a_1, \dots, a_n) = a_\ell$.

Supponiamo adesso di aver definito $s^{\mathbf{A}}(a_1, \dots, a_n)$ per tutti i termini s in $\{x_1, \dots, x_n\}$ e di livello $\leq j$. Se t ha livello $j + 1$, allora t è

della forma $f(s_1, \dots, s_k)$, dove f è un simbolo di operazione k-ario e $s_1, \dots, s_k$ sono termini di livello $\leq j$. Quindi $s_1^{\mathbf{A}}(a_1, \dots, a_n)$, $\dots$, $s_k^{\mathbf{A}}(a_1, \dots, a_n)$ sono definiti (e sono elementi di A). In questo caso poniamo $t^{\mathbf{A}}(a_1, \dots, a_n) = f^{\mathbf{A}}(s_1^{\mathbf{A}}(a_1, \dots, a_n), \dots, s_k^{\mathbf{A}}(a_1, \dots, a_n))$.

Osserviamo che $t^{\mathbf{A}}(a_1, \dots, a_n)$ è sempre un elemento di A perché per ipotesi in t non compaiono altre variabili oltre ad $x_1, \dots, x_n$

Osservazione 3.9. Una notazione più precisa per indicare la valutazione di un termine sarebbe $t^{\mathbf{A}}(x_1|a_1, \dots, x_n|a_n)$, anche se noi non avremo mai bisogno di utilizzare questa notazione.

Più importante, sarebbe necessario verificare che ogni termine t di grado > 0 si scrive in maniera *unica* come $f(s_1, \dots, s_k)$, altrimenti la nostra definizione non sarebbe univoca. Inoltre, ci sarebbe anche da verificare che se t non dipende dalla variabile x_ℓ, allora $t^{\mathbf{A}}(a_1, \dots, a_n)$ non dipende dall'assegnazione di x_ℓ.

Tutte queste affermazioni risultano intuitivamente ovvie, quindi lasciamo al lettore volenteroso il compito di darne una dimostrazione, se ne sente l'esigenza. La nostra personale opinione (ad onor del vero, non universalmente condivisa) è che non ci sono particolari motivi di preoccupazione per il lettore che non senta questa esigenza.

Lemma 3.10. *Se $\varphi : \mathbf{A} \to \mathbf{B}$ è un morfismo, allora*

$$\varphi(t^{\mathbf{A}}(a_1, \dots, a_n)) = (t^{\mathbf{B}}(\varphi(a_1), \dots, \varphi(a_n)),$$

per ogni termine $t(x_1, \dots, x_n)$ e per ogni n-upla di elementi di A.

Dimostrazione. Per induzione sul livello di t.

Questo è ovvio se t ha livello 0. Ad esempio, se t è la variabile x_ℓ, allora $t^{\mathbf{A}}(a_1, \dots, a_n) = a_\ell$ e $t^{\mathbf{B}}(b_1, \dots, b_n) = b_\ell$, quindi $\varphi(t^{\mathbf{A}}(a_1, \dots, a_n)) = \varphi(a_\ell) = t^{\mathbf{B}}(\varphi(a_1), \dots, \varphi(a_n))$.

Supponiamo adesso che la conclusione sia vera per tutti i termini di livello $\leq j$. Se t ha livello $j+1$, allora t è della forma $f(s_1, \dots, s_k)$, dove f è k-ario e $s_1, \dots, s_k$ sono termini di livello $\leq j$. Per l'ipotesi induttiva, $\varphi(s_1^{\mathbf{A}}(a_{1,1}, \dots, a_{1,n_1})) = s_1^{\mathbf{B}}(\varphi(a_{1,1}), \dots, \varphi(a_{1,n_1}))$, e così per s_2, s_3 etc. Quindi

$$\begin{aligned}
&\varphi(t^{\mathbf{A}}(a_{1,1}, \dots, a_{1,n_1}, a_{2,1}, \dots)) = \\
&\qquad \varphi(f^{\mathbf{A}}(s_1^{\mathbf{A}}(a_{1,1}, \dots, a_{1,n_1}), s_2^{\mathbf{A}}(a_{2,1}, \dots, a_{2,n_2}), \dots)) = \\
&\qquad f^{\mathbf{B}}(\varphi(s_1^{\mathbf{A}}(a_{1,1}, \dots, a_{1,n_1})), \varphi(s_2^{\mathbf{A}}(a_{2,1}, \dots a_{2,n_2})), \dots) = \\
&\qquad f^{\mathbf{B}}(s_1^{\mathbf{B}}(\varphi(a_{1,1}), \dots, \varphi(a_{1,n_1})), s_2^{\mathbf{B}}(\varphi(a_{2,1}), \dots \varphi(a_{2,n_2})), \dots) = \\
&\qquad\qquad t^{\mathbf{B}}(\varphi(a_{1,1}), \dots, \varphi(a_{1,n_1}), \varphi(a_{2,1}), \dots)
\end{aligned}$$

dove abbiamo applicato, in ordine, la definizione induttiva 3.8 di valutazione per t, l'ipotesi che φ sia un morfismo, l'ipotesi induttiva applicata ad s_1, s_2 etc., e infine di nuovo la definizione 3.8. □

DEFINIZIONE 3.11. Una *identità* è un'espressione del tipo $t(x_1, \ldots, x_n) = s(x_1, \ldots, x_n)$.

L'identità si dice *valida* o *soddisfatta* in un'algebra $\mathbf{A}$ se $t^{\mathbf{A}}(a_1, \ldots, a_n) = s^{\mathbf{A}}(a_1, \ldots, a_n)$ per ogni assegnazione di elementi di A alle variabili.

L'identità è valida (o soddisfatta) in una classe $\mathcal{K}$ di algebre se è valida in ogni algebra della classe.

OSSERVAZIONE 3.12. Un'identità, così come un termine, va considerata come una sequenza finita di simboli. Quindi il simbolo "=" nell'espressione $t(x_1, \ldots, x_n) = s(x_1, \ldots, x_n)$ *non* è la relazione di uguaglianza che si usa per confrontare due insiemi o due elementi. In effetti, in tutti i casi significativi, t ed s sono termini diversi, quindi la scrittura $t(x_1, \ldots, x_n) = s(x_1, \ldots, x_n)$ sarebbe ambigua. Questa scrittura non denota l'uguaglianza fra due oggetti, ma indica la "richiesta" che due oggetti vengano sempre interpretati nella stessa maniera.

Secondo molti autori, la distinzione è fondamentale (in effetti, lo è!), talmente fondamentale da richiedere una notazione speciale. Pertanto un'identità viene spesso scritta come $t(x_1, \ldots, x_n) \approx s(x_1, \ldots, x_n)$. Sottoponendoci al biasimo di detti autori, continueremo però a scrivere $t(x_1, \ldots, x_n) = s(x_1, \ldots, x_n)$ per comodità tipografica, e perché il lettore accorto saprà sempre riconoscere l'effettivo significato di $=$ in ogni singolo caso.

TEOREMA 3.13. *Se $\mathcal{K}$ è una classe di algebre ed esiste un'algebra libera $\mathbf{F}$ in $\mathcal{K}$ generata da n elementi $\{y_1, \ldots, y_n\}$, allora, per ogni identità ε che coinvolge $\leq n$ variabili, metti, ε è della forma $t(x_1, \ldots, x_n) = s(x_1, \ldots, x_n)$, le seguenti affermazioni sono equivalenti.*

(1) ε vale in tutte la algebre di $\mathcal{K}$.
(2) ε vale in $\mathbf{F}$.
(3) $t^{\mathbf{F}}(y_1, \ldots, y_n) = s^{\mathbf{F}}(y_1, \ldots, y_n)$ in $\mathbf{F}$.

DIMOSTRAZIONE. (1) $\Rightarrow$ (2) è banale, poiché $\mathbf{F} \in \mathcal{K}$, per definizione di algebra libera *in* $\mathcal{K}$.

(2) $\Rightarrow$ (3) è banale.

(3) $\Rightarrow$ (1) Per dimostrare (1), sia $\mathbf{A} \in \mathcal{K}$ e sia $(a_1, \ldots, a_n)$ una n-upla di elementi di A. Dobbiamo dimostrare che $t^{\mathbf{A}}(a_1, \ldots, a_n) = s^{\mathbf{A}}(a_1, \ldots, a_n)$. Siccome $\mathbf{F}$ è libera, esiste un morfismo $\varphi : \mathbf{F} \to \mathbf{A}$ tale che $\varphi(y_1) = a_1$, $\ldots$, $\varphi(y_n) = a_n$. Quindi,

$$t^{\mathbf{A}}(a_1, \ldots, a_n) = t^{\mathbf{A}}(\varphi(y_1), \ldots, \varphi(y_n)) = \varphi(t^{\mathbf{F}}(y_1, \ldots, y_n)) = \\ \varphi(s^{\mathbf{F}}(y_1, \ldots, y_n)) = s^{\mathbf{A}}(\varphi(y_1), \ldots, \varphi(y_n)) = s^{\mathbf{A}}(a_1, \ldots, a_n),$$

dove l'uguaglianza fra le due righe segue da (3), e all'interno di ciascuna riga abbiamo usato il Lemma 3.10. □

La stessa dimostrazione ci fornisce la seguente proposizione.

PROPOSIZIONE 3.14. *Il Teorema 3.13 vale anche sotto l'ipotesi che* $\mathbf{F}$ *sia libera in* $\mathcal{K}$ *generata da* Y*, con* Y *di cardinalità arbitraria e con* $y_1, \dots, y_n \in Y$ *(e gli* y_ℓ *a due a due distinti).*

OSSERVAZIONE 3.15. La prossima proposizione è sostanzialmente una riformulazione della Proposizione 1.64. In effetti, d'ora in poi useremo esclusivamente la seguente Proposizione 3.16. Abbiamo dimostrato la Proposizione 1.64 solo per poter dimostrare il teorema di esistenza delle algebre libere Teorema 2.7 senza dover introdurre la nozione di termine.

Ricordiamo dal Corollario 1.25 che, per ogni algebra $\mathbf{A}$ e ogni sottoinsieme $C \subseteq A$, esiste il più piccolo elemento $\langle C \rangle$ di $\mathrm{Sub}(\mathbf{A})$ che contiene C. Quindi $\langle C \rangle$ è il vuoto, oppure è una sottoalgebra di $\mathbf{A}$, la sottoalgebra generata da C.

PROPOSIZIONE 3.16. *Se* $\mathbf{A}$ *è un'algebra e* C *è un sottoinsieme di* A*, allora*

$$\langle C \rangle = \{t^{\mathbf{A}}(a_1, a_2, \dots, a_n) \mid n \in \mathbb{N},\ t(x_1, \dots, x_n) \text{ è un termine e } a_1, a_2, \dots, a_n \in C\} \tag{12}$$

DIMOSTRAZIONE. Il caso $\langle C \rangle = \emptyset$ è banale (usando il Corollario 1.25(2)). Altrimenti, $\langle C \rangle$ è una sottoalgebra di $\mathbf{A}$, e necessariamente deve contenere tutti i $t^{\mathbf{A}}(a_1, a_2, \dots, a_n)$ dati da (12) (dimostrazione per induzione sul livello di t).

Viceversa, se l'insieme dato da (12) è non vuoto, dobbiamo dimostrare che si tratta di una sottoalgebra di $\mathbf{A}$. Ma dati elementi $t^{\mathbf{A}}(a_1, a_2, \dots, a_n)$, $s^{\mathbf{A}}(b_1, b_2, \dots, b_p) \dots$, e data un'operazione $f^{\mathbf{A}}$ di $\mathbf{A}$, abbiamo che

$$u(x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_p \dots) = f(t(x_1, x_2, \dots, x_n), s(y_1, y_2, \dots, y_p) \dots)$$

è un termine in $x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_p \dots$, quindi

$$f^{\mathbf{A}}(t^{\mathbf{A}}(a_1, a_2, \dots, a_n), s^{\mathbf{A}}(b_1, b_2, \dots, b_p), \dots) = u^{\mathbf{A}}(a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_p, \dots)$$

ha la forma data da (12). Questo dimostra che l'insieme definito in (12) è chiuso, quello che dovevamo dimostrare. □

Osservazione 3.17. Per mostrare la "superiorità" della Proposizione 3.16 rispetto a 1.64, diamo adesso per esempio una dimostrazione più diretta dell'uguaglianza

$$\langle C\rangle = \bigcup_{F\subseteq C,\ F \text{ finito}} \langle F\rangle$$

introdotta nell'Osservazione 1.66. Infatti, per la Proposizione 3.16, se $c \in \langle C\rangle$, allora esistono $a_1, a_2, \ldots, a_n \in C$ ed un termine t tali che $c = t^{\mathbf{A}}(a_1, a_2, \ldots, a_n)$. Ma allora, sempre per la Proposizione 3.16, stavolta applicata all'insieme finito $F = \{a_1, a_2, \ldots, a_n\}$, abbiamo $c \in \langle F\rangle$.

Questo dimostra l'inclusione $\subseteq$; l'altra inclusione è banale.

4. Il Teorema di Birkhoff

Ricordiamo che questa sezione è facoltativa.

Ricordiamo la convenzione 3.3 che abbiamo adottato; in particolare, tutte le algebre che consideriamo saranno di uno stesso tipo fissato, e tutte le nozioni che useremo faranno riferimento a questo stesso tipo, anche quando questo tipo non venga esplicitamente menzionato.

Definizione 4.1. Una classe $\mathcal{K}$ di algebre è *chiusa per sottoalgebre* se, ogni volta che $\mathbf{A} \in \mathcal{K}$ e $\mathbf{B}$ è una sottoalgebra di $\mathbf{A}$, allora $\mathbf{B} \in \mathcal{K}$.

La definizione di classe *chiusa per prodotti* è simile.

Una classe $\mathcal{K}$ di algebre è *chiusa per immagini omomorfe* se, ogni volta che $\mathbf{A} \in \mathcal{K}$ e $\varphi : \mathbf{A} \to \mathbf{B}$ è un morfismo, allora $Im\varphi \in \mathcal{K}$. In base all'Osservazione 1.37, $\mathcal{K}$ è chiusa per immagini omomorfe se e solo se è chiusa per isomorfismi e per "quozienti" $\mathbf{A}/\alpha$.

Ovviamente, si dice che un insieme Σ di identità è valido (o soddisfatto) in un'algebra o in una classe di algebre se ogni $\sigma \in \Sigma$ è valida in quell'algebra o in quella classe. Cf. la Definizione 3.11.

Teorema 4.2. *Se $\mathcal{K}$ è una classe di algebre dello stesso tipo τ, allora le seguenti condizioni sono equivalenti.*

(1) $\mathcal{K}$ è chiusa per sottoalgebre, prodotti e immagini omomorfe.
(2) Esiste un insieme Σ di identità in τ tale che $\mathcal{K}$ è la classe di tutte le algebre di tipo τ in cui tutte le identità di Σ sono valide.

Dimostrazione. (2) $\Rightarrow$ (1) è (quasi) banale. Bisogna verificare che, se σ è un'identità, allora la classe delle algebre che soddisfano a σ è chiusa per sottoalgebre, prodotti e immagini omomorfe. Se questo è vero per una singola identità, allora sarà vero anche per un insieme di identità.

Dimostriamo per esempio che se σ è un'identità, allora la classe delle algebre che soddisfano a σ è chiusa per immagini omomorfe. Sia quindi

$\varphi : \mathbf{A} \to \mathbf{B}$ suriettivo, e sia ε l'identità $t(x_1, \dots, x_n) = s(x_1, \dots, x_n)$. Supponiamo che ε sia valida in $\mathbf{A}$, cioè che $t(a_1, \dots, a_n) = s(a_1, \dots, a_n)$, per ogni n-upla di elementi di A. Se $b_1, \dots, b_n \in B$, allora, siccome φ è suriettivo, esistono $a_1, \dots, a_n \in A$ tali che $\varphi(a_1) = b_1$, $\dots$, $\varphi(a_n) = b_n$. Quindi $t(b_1, \dots, b_n) = t(\varphi(a_1), \dots, \varphi(a_n)) = \varphi(t(a_1, \dots, a_n)) = \varphi(s(a_1, \dots, a_n)) = s(\varphi(a_1), \dots, \varphi(a_n)) = s(b_1, \dots, b_n)$, poiché φ è un morfismo. Quindi ε vale anche in $\mathbf{B}$.

(1) $\Rightarrow$ (2) Sia Σ l'insieme di *tutte* le identità che valgono in *tutte* le algebre di $\mathcal{K}$.

Vogliamo dimostrare che un'algebra soddisfa a Σ se e solo se appartiene a $\mathcal{K}$. Per definizione di Σ, ogni algebra di $\mathcal{K}$ soddisfa a Σ, quindi la parte non banale è dimostrare che se un'algebra $\mathbf{A}$ soddisfa a Σ, allora $\mathbf{A}$ appartiene a $\mathcal{K}$.

Supponiamo dunque che $\mathbf{A}$ soddisfi a Σ. Siccome $\mathcal{K}$ è chiusa, in particolare, per prodotti e sottostrutture, allora, per il Teorema 2.7, esiste un algebra libera $\mathbf{F}$ su $|A|$ generatori, diciamo, $\mathbf{F}$ è libera su Y con $|Y| = |A|$. Quindi esiste una funzione suriettiva $\chi : Y \to A$. Siccome $\mathbf{F}$ è generata da Y, allora, per la Proposizione 3.16, ogni elemento di $\mathbf{F}$ ha la forma $t^{\mathbf{F}}(y_1, \dots, y_n)$, per qualche termine $t(x_1, \dots, x_n)$ e $y_1, \dots, y_n \in Y$. Consideriamo la seguente condizione:

$$\varphi(t^{\mathbf{F}}(y_1, \dots, y_n)) = t^{\mathbf{A}}(\chi(y_1), \dots, \chi(y_n)), \tag{13}$$

dove $y_1, \dots, y_n$ variano in Y e t varia fra tutti i termini.

Affermazione. La condizione (13) *determina un morfismo suriettivo* $\varphi : \mathbf{F} \to \mathbf{A}$.

Dimostriamo questa affermazione. Nel caso φ rappresenti una funzione da F ad A, allora φ estende χ, dunque φ è suriettiva. Sempre se φ rappresenta una funzione, è facile vedere che φ è un morfismo da $\mathbf{F}$ ad $\mathbf{A}$. Dobbiamo dimostrare che

$$\varphi(f^{\mathbf{F}}(t_1^{\mathbf{F}}(y_{1,1}, \dots, y_{1,n_1}), t_2^{\mathbf{F}}(y_{2,1}, \dots, y_{2,n_2}), \dots)) = \\ f^{\mathbf{A}}(\varphi(t_1^{\mathbf{F}}(y_{1,1}, \dots, y_{1,n_1})), \varphi(t_2^{\mathbf{F}}(y_{2,1}, \dots, y_{2,n_2})), \dots),$$

per ogni operazione $f^{\mathbf{F}}$ di $\mathbf{F}$, termini t_1, t_2, $\dots$ ed elementi $y_{1,1}, \dots, y_{1,n_1}$, $y_{2,1}, \dots, y_{2,n_2} \dots$ in Y. Applicando (13) al termine $t(x_{1,1}, \dots, x_{1,n_1}, x_{2,1}, \dots, x_{2,n_2}, \dots)$ definito da $f(t_1(x_{1,1}, \dots, x_{1,n_1}), t_2(x_{2,1}, \dots, x_{2,n_2}), \dots)$ otteniamo

$$\varphi(f^{\mathbf{F}}(t_1^{\mathbf{F}}(y_{1,1}, \dots, y_{1,n_1}), t_2^{\mathbf{F}}(y_{2,1}, \dots, y_{2,n_2}), \dots)) = \\ f^{\mathbf{A}}(t_1^{\mathbf{A}}(\chi(y_{1,1}), \dots, \chi(y_{1,n_1})), t_2^{\mathbf{A}}(\chi(y_{2,1}), \dots, \chi(y_{2,n_2})), \dots)$$

Del resto, applicando (13) a ciascuno dei termini t_1, t_2, ..., otteniamo

$$f^{\mathbf{A}}(\varphi(t_1^{\mathbf{F}}(y_{1,1},\dots,y_{1,n_1})),\varphi(t_2^{\mathbf{F}}(y_{2,1},\dots,y_{2,n_2})),\dots) = \\ f^{\mathbf{A}}(t_1^{\mathbf{A}}(\chi(y_{1,1}),\dots,\chi(y_{1,n_1})),t_2^{\mathbf{A}}(\chi(y_{2,1}),\dots,\chi(y_{2,n_2})),\dots),$$

quello che dovevamo dimostrare.

A priori non è però certo che l'equazione (13) definisca una funzione. Per l'argomento presentato immediatamente prima di (13), la condizione (13) assegna almeno un elemento di A ad ogni elemento di F. Ma non è detto a prima vista che questo elemento di A sia unico, perché può benissimo darsi che $t^{\mathbf{F}}(y_1,\dots,y_n)$ sia uguale a $s^{\mathbf{F}}(y'_1,\dots,y'_p)$, per qualche altro termine $s(x'_1,\dots,x'_p)$ e $y'_1,\dots,y'_p \in Y$. Affinché φ data da (13) sia ben definita, bisogna controllare che, in questo caso, $t^{\mathbf{A}}(\chi(y_1),\dots,\chi(y_n)) = s^{\mathbf{A}}(\chi(z_1),\dots,\chi(z_p))$. Mostriamo adesso che questo è una conseguenza dell'ipotesi che $\mathbf{A}$ soddisfa a tutte le identità valide in $\mathcal{K}$.

In base alle nostre convenzioni sul modo di esprimere i termini, ed eventualmente scambiando qualche variabile, possiamo scrivere t e s come $t(x_1,\dots,x_q)$ e $s(x_1,\dots,x_q)$. Dobbiamo dimostrare che, se $t^{\mathbf{F}}(y_1,\dots,y_p) = s^{\mathbf{F}}(y_1,\dots,y_p)$, allora $t^{\mathbf{A}}(a_1,\dots,a_p) = s^{\mathbf{A}}(a_1,\dots,a_p)$, dove abbiamo scritto a_1 al posto di $\chi(y_1)$ etc. Ma per la Proposizione 3.14, se $t^{\mathbf{F}}(y_1,\dots,y_p) = s^{\mathbf{F}}(y_1,\dots,y_p)$, allora l'identità $t(x_1,\dots,x_q) = s(x_1,\dots,x_q)$ vale in tutte le algebre di $\mathcal{K}$, dunque appartiene a Σ. Ma per ipotesi $\mathbf{A}$ soddisfa a tutte le identità di Σ, quindi anche a questa identità, e questo implica $t^{\mathbf{A}}(a_1,\dots,a_p) = s^{\mathbf{A}}(a_1,\dots,a_p)$.

La dimostrazione dell'affermazione è così completa.

In base all'affermazione, $\mathbf{A}$ è un'immagine omomorfa di $\mathbf{F}$, ma $\mathbf{F} \in \mathcal{K}$ e $\mathcal{K}$ è chiusa per immagini omomorfe, quindi $\mathbf{A} \in \mathcal{K}$, quello che dovevamo dimostrare. □

Definizione 4.3. Una classe $\mathcal{K}$ di algebre dello stesso tipo si dice una *varietà* se $\mathcal{K}$ soddisfa ad una delle condizioni (equivalenti) del Teorema 4.2.

Quello che useremo, comunque, di una varietà, sarà sempre solo la chiusura rispetto a prodotti e sottostrutture (in misura minore, la chiusura per immagini omomorfe). Notiamo che, per il Teorema 2.7, questo ci garantisce l'esistenza di algebre libere.

5. Il Teorema di Mal'cev

Ricordiamo (cf. la Definizione 1.56) che se $\alpha, \beta \subseteq A \times A$, la composizione $\alpha \circ \beta$ di α e β è la relazione γ tale che $a \,\gamma\, c$ se e solo se esiste $b \in A$ tale che $a \;\alpha\; b \;\beta\; c$.

OSSERVAZIONE 5.1. Se $\mathbf{A}$ è un'algebra, $\alpha, \beta \subseteq A \times A$ e α e β sono compatibili, allora anche $\alpha \circ \beta$ è compatibile (v. il Lemma 1.57).

Ma non è sempre vero che se α e β sono congruenze, allora anche $\alpha \circ \beta$ è una congruenza; infatti, non è detto che $\alpha \circ \beta$ sia una relazione d'equivalenza!

Per esempio, nella catena $\mathbf{C}$ con tre elementi (vedi l'osservazione 1.55) si considerino le congruenze α associata alla partizione $\{\{b, c\}\{a\}\}$, e β associata alla partizione $\{\{c\}\{a, b\}\}$. Abbiamo che $c \; \alpha \; b \; \beta \; a$, quindi $c \; \alpha \circ \beta \; a$. Invece, non è vero che $a \; \alpha \circ \beta \; c$; infatti, se così fosse, esisterebbe un x tale che $a \; \alpha \; x \; \beta \; c$, ma a è in relazione solo con se stesso tramite α, quindi per forza $x = a$, ma a non è in relazione con c tramite β, quindi non esiste un x tale che $a \; \alpha \; x \; \beta \; c$, cioè è falso che $a \; \alpha \circ \beta \; c$. In conclusione, $\alpha \circ \beta$ non è simmetrica, quindi non è una relazione d'equivalenza e non è una congruenza.

Tratteremo adesso il caso in cui $\alpha \circ \beta$ è effettivamente una congruenza.

OSSERVAZIONE 5.2. Se α e β sono due congruenze di un'algebra $\mathbf{A}$, allora $\alpha \circ \beta$ è una congruenza se e solo se $\alpha \circ \beta = \alpha \vee \beta$, se e solo se $\alpha \circ \beta = \beta \circ \alpha$, se e solo se $\alpha \circ \beta \subseteq \beta \circ \alpha$.

[...Una dimostrazione si può ottenere come conseguenza della Proposizione 1.60. Una dimostrazione più diretta è la seguente.]

Siccome $\alpha \vee \beta$ è una congruenza che contiene sia α che β, in particolare, $\alpha \vee \beta$ è transitiva, allora necessariamente $\alpha \vee \beta \supseteq \alpha \circ \beta$. Quindi se $\alpha \circ \beta$ è una congruenza, non può che essere $\alpha \vee \beta$ (siccome $\alpha \subseteq \alpha \circ \beta$ e $\beta \subseteq \alpha \circ \beta$, essendo α e β riflessive).

Se $\alpha \circ \beta = \alpha \vee \beta$, allora vale anche $(\alpha \circ \beta)^\smile = (\alpha \vee \beta)^\smile$, ma siccome $\alpha \vee \beta$ è una congruenza, quindi simmetrica, si ha $\alpha \circ \beta = \alpha \vee \beta = (\alpha \vee \beta)^\smile = (\alpha \circ \beta)^\smile = \beta^\smile \circ \alpha^\smile = \beta \circ \alpha$, poiché α e β sono congruenze, quindi simmetriche.

Adesso mostriamo che se $\alpha \circ \beta = \beta \circ \alpha$, allora $\alpha \circ \beta$ è una congruenza. Innanzitutto, $\alpha \circ \beta$ è compatibile, per il Lemma 1.57. Calcoliamo $\alpha \circ \beta \circ \alpha \circ \beta = \alpha \circ (\beta \circ \alpha) \circ \beta = \alpha \circ \alpha \circ \beta \circ \beta = \alpha \circ \beta$. Quindi, ponendo $\gamma = \alpha \circ \beta$, abbiamo $\gamma \circ \gamma = \gamma$, cioè $\gamma = \alpha \circ \beta$ è transitiva. Siccome $\alpha \circ \beta$ è sicuramente riflessiva, resta da dimostrare che $\alpha \circ \beta$ è simmetrica, ma per questo basta calcolare $(\alpha \circ \beta)^\smile = \beta^\smile \circ \alpha^\smile = \beta \circ \alpha = \alpha \circ \beta$.

Per finire, dimostriamo che $\alpha \circ \beta = \beta \circ \alpha$ se e solo se $\alpha \circ \beta \subseteq \beta \circ \alpha$. Un'implicazione è banale. Per dimostrare l'altra implicazione, se $\alpha \circ \beta \subseteq \beta \circ \alpha$, allora $(\alpha \circ \beta)^\smile \subseteq (\beta \circ \alpha)^\smile$, quindi $\beta \circ \alpha = \beta^\smile \circ \alpha^\smile = (\alpha \circ \beta)^\smile \subseteq (\beta \circ \alpha)^\smile = \alpha^\smile \circ \beta^\smile = \alpha \circ \beta$.

DEFINIZIONE 5.3. Se α, β sono due congruenze di un'algebra $\mathbf{A}$, si dice che α e β *permutano* se $\alpha \circ \beta = \beta \circ \alpha$.

L'algebra $\mathbf{A}$ si dice *a congruenze permutabili* se tutte le coppie di congruenze di $\mathbf{A}$ permutano.

Una classe $\mathcal{K}$ di algebre è *a congruenze permutabili* se tutte le algebre in $\mathcal{K}$ lo sono.

Osservazione 5.4. La Proposizione 1.61 (cf. in particolare la condizione (10)) e le Osservazioni 5.1 e 5.2 mostrano l'interesse della nozione di permutabilità. Ad esempio, si confrontino le caratterizzazioni date nella Proposizione 1.60 e nell'Osservazione 5.2.

Il prossimo teorema dimostra che la nozione di permutabilità è in effetti una nozione centrale per la teoria generale dei sistemi algebrici.

Ricordiamo che una *varietà* è una classe di algebre chiusa per prodotti, sottoalgebre e immagini omomorfe.

Teorema 5.5. *[...teorema di Mal'cev* [**Be**, Theorem 4.64] *(fa parte del programma)]*

Dimostrazione. [...] La dimostrazione di un risultato simile è data qui nel Teorema 12.2. Il Teorema di Malc'ev può essere dimostrato allo stesso modo. Altrimenti per ora si può consultare [**Be**]. □

[...esempi: gruppi, quasigruppi [**Be**, p. 123]]

[...NB: In realtà basta che esista l'algebra libera generata da tre elementi, e che, in questa algebra, $\alpha \circ \beta \subseteq \beta \circ \alpha$, per $\alpha = ...$]

Proposizione 5.6. *Se* $\mathbf{A}$ *è un'algebra che appartiene ad una varietà a congruenze permutabili, allora ogni relazione binaria riflessiva e compatibile è una congruenza.*

Dimostrazione. [...] per ora vedi [**Be**, Theorem 4.65(1)] (fa parte del programma) □

Proposizione 5.7. *Se* $\mathbf{A}$ *è un'algebra a congruenze permutabili, allora* $\mathbf{Con}(\mathbf{A})$ *è un reticolo modulare.*

Dimostrazione. Per comodità, d'ora in poi indicheremo spesso $\wedge$ come un prodotto e $\vee$ come una somma.

Siano $\alpha, \beta, \gamma \in \mathbf{Con}(\mathbf{A})$ e siano $a, b \in A$ tali che $(a, c) \in \alpha(\beta + \gamma\alpha)$. In particolare, $a\ \alpha\ c$ e $a\ (\beta + \gamma\alpha)\ c$. Siccome $\mathbf{A}$ è un'algebra a congruenze permutabili, allora $\beta + \gamma\alpha = \beta \circ \gamma\alpha$, quindi esiste $b \in A$ tale che $a\ \beta\ b\ \gamma\alpha\ c$. In particolare, $b\ \alpha\ c$. Siccome α è simmetrica, abbiamo $a\ \alpha\ c\ \alpha\ b$, e siccome α è transitiva, $a\ \alpha\ b$. Quindi $a\ \alpha\beta\ b\ \gamma\alpha\ c$, cioè $(a, c) \in \alpha\beta \circ \gamma\alpha \subseteq \alpha\beta + \gamma\alpha$.

[...disegno]

Abbiamo dimostrato $\alpha(\beta + \gamma\alpha) \leq \alpha\beta + \alpha\gamma$. L'altra inclusione è banale. □

Osservazione 5.8. Notate la differenza fra le proposizioni 5.6 e 5.7. La seconda vale per *ogni* algebra a congruenze permutabili, mentre la prima vale solo si assume che l'algebra appartenga ad una *varietà* a congruenze permutabili.

In altre parole, la Proposizione 5.7 presenta un'implicazione che vale sempre; mentre la Proposizione 5.6 presenta un'implicazione che vale per due proprietà (P_1, l'essere a congruenze permutabili; P_2, essere tale che ogni relazione compatibile e riflessiva sia una congruenza) *solo nel caso* in cui si assuma che queste due proprietà valgano per *tutte* le algebre di una varietà.

Naturalmente, la condizione che, metti, P_1 valga per tutte le algebre di una varietà può essere indebolita (infatti la Proposizione 5.6 è un corollario del teorema di Mal'cev, e abbiamo notato che il teorema vale sotto ipotesi più deboli dell'assunzione che $\mathcal{K}$ sia una varietà). Comunque, $P_1 \Rightarrow P_2$ non vale in generale per singole algebre. L'insieme totalmente ordinato con due elementi $\{a, b\}$ con le operazioni di reticolo è ovviamente a congruenze permutabili (ogni algebra con due elementi è a congruenze permutabili!). Ma $\{(a, a), (b, b), (a, b)\}$ è una relazione compatibile e riflessiva, ma non simmetrica.

Molti dei risultati più significativi dell'algebra universale hanno proprio la forma $P_1 \Rightarrow P_2$, per opportune proprietà, e l'implicazione è non banale, cioè non vale per algebre "singole", ma vale solo assumendo che P_1 valga per *tutte* le algebre di una varietà.

6. Reticoli di relazioni di equivalenza permutabili

Definizione 6.1. Come abbiamo visto in 1.60, l'insieme delle relazioni di equivalenza $\mathbf{Eq}(A)$ su un insieme A ha la struttura di un reticolo. Un sottoreticolo $\mathbf{L}$ di $\mathbf{Eq}(A)$ si dice un *reticolo di relazioni di equivalenza permutabili* se $\alpha \circ \beta = \beta \circ \alpha$, per ogni coppia $\alpha, \beta \in L$.

Osservazione 6.2. Siccome, per ogni algebra $\mathbf{A}$, $\mathbf{Con}(\mathbf{A})$ è un sottoreticolo di $\mathbf{Eq}(\mathbf{A})$ (Proposizione 1.60), allora, se $\mathbf{A}$ è a congruenze permutabili, si ha che $\mathbf{Con}(\mathbf{A})$ è un reticolo di relazioni di equivalenza permutabili. Quindi tutto quello che diremo in questa sezione si applica anche al reticolo delle congruenze di un'algebra a congruenze permutabili.

Osservazione 6.3. Allo stesso modo che in 5.2 si dimostra che se α e β sono due relazioni di equivalenza su un insieme A, allora $\alpha \circ \beta$ è una relazione d'equivalenza se e solo se $\alpha \circ \beta = \alpha \vee \beta$ se e solo se $\alpha \circ \beta = \beta \circ \alpha$.

D'ora in poi, per comodità indicheremo spesso le operazioni di un reticolo con $+$ e $\cdot$ anziché con, rispettivamente, $\vee$ e $\wedge$.

Definizione 6.4. Se α_1, β_1, α_2, β_2, α_3, β_3 sono elementi di un reticolo, utilizzeremo le seguenti abbreviazioni: $\gamma_{12} = (\alpha_1+\alpha_2)(\beta_1+\beta_2)$, $\gamma_{23} = (\alpha_2 + \alpha_3)(\beta_2 + \beta_3)$ e $\gamma_{13} = (\alpha_1 + \alpha_3)(\beta_1 + \beta_3)$.

Un reticolo $\mathbf{L}$ soddisfa all'*identità arguesiana* se

$$(\alpha_1 + \beta_1)(\alpha_2 + \beta_2)(\alpha_3 + \beta_3) \leq \alpha_1(\alpha_2 + \gamma_{12}(\gamma_{23} + \gamma_{13})) + \beta_1$$

per tutti gli elementi α_1, β_1, α_2, β_2, α_3, β_3 di L.

Sia chiaro che l'identità arguesiana coinvolge solo gli elementi α_1, β_1, α_2, β_2, α_3, β_3, e abbiamo usato le espressioni $\gamma_{12}, \gamma_{23}, \gamma_{13}$ per brevità. Senza questa convenzione, l'identità arguesiana va scritta

$$(\alpha_1 + \beta_1)(\alpha_2 + \beta_2)(\alpha_3 + \beta_3) \leq$$
$$\alpha_1(\alpha_2+(\alpha_1+\alpha_2)(\beta_1+\beta_2)((\alpha_2+\alpha_3)(\beta_2+\beta_3)+(\alpha_1+\alpha_3)(\beta_1+\beta_3)))+\beta_1$$

Si può dimostrare (ma noi non lo faremo) che l'identità arguesiana è strettamente più forte della modularità.

Il lettore potrebbe chiedersi perchè chiamiamo *identità* quella che abbiamo scritto come una disuguaglianza. Ma, in un reticolo, la disuguaglianza $A \leq B$ è sempre equivalente all'identità $AB = B$; questo giustifica il nostro uso dell'espressione identità.

Osservazione 6.5. (non fa parte del programma) L'identità arguesiana ha un profondo significato geometrico. Ad ogni spazio proiettivo può essere associato un reticolo (il reticolo dei sottospazi); anzi, in un senso astratto, uno spazio proiettivo potrebbe essere definito come un reticolo soddisfacente a certe proprietà. In questo senso, uno spazio proiettivo soddisfa alla Legge di Desargues, equivalentemente, è coordinatizzabile, se e solo se il suo reticolo dei sottospazi è arguesiano (come reticolo). Maggiori dettagli si possono trovare, ad esempio, in [**JR**, Sezione 3.2].

Osservazione 6.6. (non fa parte del programma) Siccome sia la modularità che la distribuitività di un reticolo sono caratterizzabili mediante l'"omissione" di un numero finito di sottoreticoli (rispettivamente il pentagono $\mathbf{N}_5$, e il pentagono insieme ad $\mathbf{M}_3$), il lettore si potrebbe chiedere se simili caratterizzazioni valgano per qualunque identità di reticoli. D. Pickering [**Pi**] ha invece dimostrato che l'identità arguesiana non si può caratterizzare mediante l'omissione di un numero finito di reticoli.

Teorema 6.7. *In un reticolo di relazioni di equivalenza permutabili vale l'identità arguesiana.*

Dimostrazione. Sia $\mathbf{L}$ un reticolo di relazioni di equivalenza permutabili sull'insieme A e siano α_1, β_1, α_2, β_2, α_3, β_3 elementi di L. Dobbiamo dimostrare che se $(a, c) \in (\alpha_1+\beta_1)(\alpha_2+\beta_2)(\alpha_3+\beta_3)$, allora $(a, c) \in \alpha_1(\alpha_2+\gamma_{12}(\gamma_{23}+\gamma_{13}))+\beta_1$, per ogni coppia di elementi $a, c \in A$. Siccome, per ipotesi, siamo in un reticolo di relazioni di equivalenza permutabili, in particolare, α_1 e β_1 permutano. Siccome, in particolare, $(a, c) \in \alpha_1 + \beta_1 = \alpha_1 \circ \beta_1$, esiste $b_1 \in A$ tale che $a\ \alpha_1\ b_1\ \beta_1\ c$, e così per gli altri indici.

La situazione può essere rappresentata mediante il seguente diagramma.

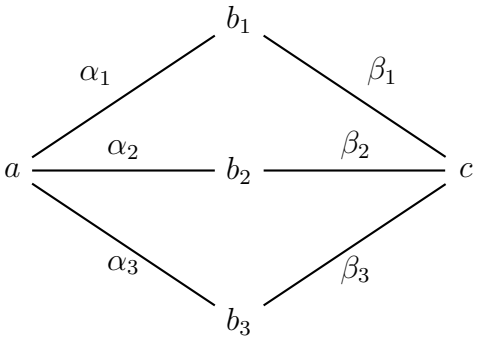


Fig. A

Ora abbiamo che $b_1\ \alpha_1\ a\ \alpha_2\ b_2$ e $b_1\ \beta_1\ c\ \beta_2\ b_2$, quindi $(b_1, b_2) \in (\alpha_1 + \alpha_2)(\beta_1 + \beta_2) = \gamma_{12}$, e lo stesso per gli altri indici. Il diagramma precedente diventa dunque.

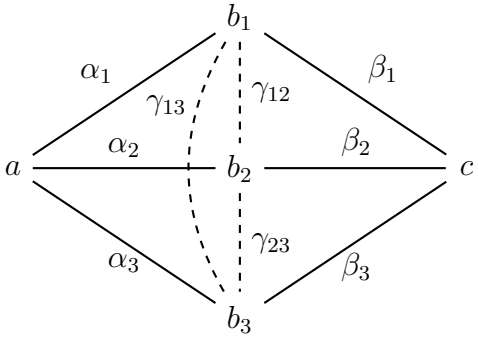


Fig. B

Ora abbiamo $a\ \alpha_1\ b_1$, per costruzione. Inoltre $a\ \alpha_2\ b_2$ e, per quanto appena detto, $b_2\ \gamma_{12}\ b_1$, ma anche $b_2\ \gamma_{23}\ b_3\ \gamma_{13}\ b_1$, per cui $(b_2, b_1) \in \gamma_{12}(\gamma_{23} + \gamma_{13})$. Siccome $a\ \alpha_2\ b_2$, abbiamo $(a, b_1) \in \alpha_2 + \gamma_{12}(\gamma_{23} + \gamma_{13})$, quindi $(a, b_1) \in \alpha_1(\alpha_2 + \gamma_{12}(\gamma_{23} + \gamma_{13}))$.

Siccome $b_1\ \beta_1\ c$, abbiamo finalmente $(a, c) \in \alpha_1(\alpha_2 + \gamma_{12}(\gamma_{23} + \gamma_{13})) + \beta_1$.

Nel seguente diagramma abbiamo lasciato indicate solo le congruenze rilevanti per questa parte conclusiva dell'argomentazione e, per mancanza di spazio, abbiamo indicato $\gamma_{12}(\gamma_{23} + \gamma_{13})$ con γ'.

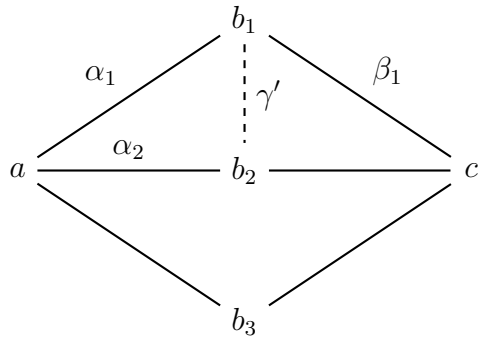


Fig. B'

□

COROLLARIO 6.8. *Un'algebra a congruenze permutabili è a congruenze arguesiane (cioè il suo reticolo delle congruenze soddisfa all'identità arguesiana).*

OSSERVAZIONE 6.9. Gli argomenti precedenti possono essere utilizzati per dimostrare identità apparentemente più forti dell'identità arguesiana, ad esempio,

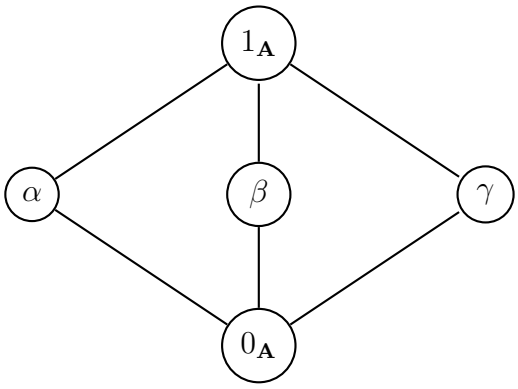
$$(\alpha_1+\beta_1)(\alpha_2+\beta_2)(\alpha_3+\beta_3) \leq \alpha_1(\alpha_2+\gamma_{12}(\gamma_{23}+\gamma_{13}))+\beta_1(\beta_2+\gamma_{12}(\gamma_{23}+\gamma_{13}))$$

In genere, queste identità si rivelano comunque equivalenti all'identità arguesiana.

Sarebbe in grado il lettore di generalizzare la Definizione 6.4 e il Teorema 6.7 al caso di un prodotto con 4 o più fattori? (in questo caso si ottengono identità strettamente più forti, anche se la dimostrazione che si tratta di identità strettamente più forti è tutt'altro che facile.)

7. La *Term Condition*

OSSERVAZIONE 7.1. I risultati a cui accenniamo in questa sezione potrebbero apparire piuttosto tecnici e forse meno attraenti rispetto ai risultati presentati in precedenza. Però mostrano un fatto decisamente sorprendente, e cioè che la "forma" del reticolo delle congruenze di un'algebra ha una profonda influenza sulla struttura (anche sintattica) dell'algebra. Per esempio, se il reticolo delle congruenze di un gruppo è $\mathbf{M}_3$, allora il gruppo è abeliano. È significativo che ci sia una versione dell'enunciato precedente che vale in *qualunque* algebra. In effetti, argomenti collegati alle nozioni introdotte in questa sezione hanno trovato importanti applicazioni in diversi settori dell'algebra universale.



$\mathbf{M}_3$

DEFINIZIONE 7.2. Si dice che un'algebra $\mathbf{A}$ soddisfa alla *term condition (TC)* se $t(a,b) = t(c,b)$ implica $t(a,d) = t(c,d)$, per ogni termine t.

Qui, per semplicità, scriviamo a, b, c, d, ma ammettiamo la possibilità che a e c siano n-uple e b e d siano k-uple di elementi di A, per qualche n e k. Quindi t deve essere un termine $n+k$-ario.

Solitamente, gli elementi coinvolti nella term condition vengono scritti sotto forma di matrice

$$\begin{vmatrix} t(a,b) & t(c,b) \\ t(a,d) & t(c,d) \end{vmatrix} \tag{14}$$

e la term condition richiede che se i due elementi della prima riga sono uguali fra loro, allora anche i due elementi della seconda riga sono uguali fra loro. Per simmetria, la term condition equivale all'assunzione che se due elementi in una riga o in una colonna sono uguali, allora anche gli elementi dell'altra riga o colonna sono uguali.

ESEMPIO 7.3. Un gruppo soddisfa alla term condition se e solo se è abeliano.

Infatti, considerando il termine $t(x,y) = xyx^{-1}y^{-1}$ e ponendo $a = b = e$, elemento neutro, otteniamo

$$\begin{vmatrix} t(a,b) & t(c,b) \\ t(a,d) & t(c,d) \end{vmatrix} = \begin{vmatrix} e & e \\ e & cdc^{-1}d^{-1} \end{vmatrix}$$

Quindi se un gruppo $\mathbf{G}$ soddisfa alla term condition, allora $cdc^{-1}d^{-1} = e$ per tutti gli elementi di G ma questo significa proprio che $\mathbf{G}$ è abeliano.

Viceversa, per ogni termine $t(x_1, \dots, y_1, \dots)$ per il tipo dei gruppi, esiste un termine $s(x_1, \dots, y_1, \dots)$ della forma $x_1^{z_1} x_2^{z_2} \dots y_1^{z_1'} \dots$, con $z_1, \dots z_1', \dots \in \mathbb{Z}$, tale che $t(x_1, \dots, y_1, \dots) = s(x_1, \dots, y_1, \dots)$ vale in ogni gruppo abeliano. Applicando la legge di cancellazione è adesso facile vedere che TC vale in ogni gruppo abeliano.

ESEMPIO 7.4. In un semigruppo che soddisfa a TC vale $abcd = acbd$. [...]

$$\begin{vmatrix} ab \cdot b \cdot d & a \cdot b \cdot bd \\ ab \cdot c \cdot d & a \cdot c \cdot bd \end{vmatrix}$$

Prendendo $a = d = e$ questo fornisce un'altra dimostrazione che un gruppo in cui vale TC è abeliano.

ESEMPIO 7.5. Se c è un elemento di un semigruppo tale che $cc = c$, allora vale $acb = ab$. [...]

$$\begin{vmatrix} c \cdot cb & c \cdot b \\ a \cdot cb & a \cdot b \end{vmatrix}$$

Problema. È vero che un semigruppo con elemento neutro soddisfa a TC se e solo se è commutativo?

ESEMPIO 7.6. Un semireticolo soddisfa a TC se e solo se ha solo un elemento. [...]

$$\begin{vmatrix} aab & bab \\ aaa & baa \end{vmatrix}$$

Come abbiamo detto, scriveremo semplicemente a anche per indicare una n-upla $(a_1, a_2, \ldots, a_n)$. In tal caso, se c è un'altra n-upla $(c_1, c_2, \ldots, c_n)$, la notazione $a\ \alpha\ c$ sarà un'abbreviazione di $a_1\ \alpha\ c_1$, $a_2\ \alpha\ c_2$, ... e $a_n\ \alpha\ c_n$.

Ricordiamo che spesso scriveremo $\alpha\beta$ al posto di $\alpha \wedge \beta$ e $\alpha + \beta$ al posto di $\alpha \vee \beta$.

LEMMA 7.7. *Se $\mathbf{A}$ è un'algebra, $\alpha, \gamma \in Con(\mathbf{A})$ e $\gamma\alpha = 0_{\mathbf{A}}$, allora vale il caso particolare della TC in cui $a\,\gamma\,c$ e $b\,\alpha\,d$.*

DIMOSTRAZIONE. Data una matrice come in (14), se $t(a, b) = t(c, b)$, abbiamo $t(a, d)\ \alpha\ t(a, b) = t(c, b)\ \alpha\ t(c, d)$. Del resto, $t(a, d)\ \gamma\ t(c, d)$, cioè $t(a, d)\ \gamma\alpha\ t(c, d)$. Ma $\gamma\alpha = 0_{\mathbf{A}}$, quindi $t(a, d) = t(c, d)$.

Il tutto può essere illustrato col seguente diagramma.

$$\begin{array}{ccc} & = & \\ \alpha\Big(\begin{vmatrix} t(a,b) & & t(c,b) \\ t(a,d) & & t(c,d) \end{vmatrix}\Big)\alpha & & \\ & \gamma & \end{array}$$

□

TEOREMA 7.8. *(Lemma di Lampe) Se $\mathbf{A}$ è un'algebra, $\alpha, \beta, \gamma \in \mathbf{Con}(\mathbf{A})$ e $\gamma\alpha = \gamma\beta = 0_{\mathbf{A}}$, allora vale il caso particolare della TC in cui $a\,\gamma\,c$ e $b\,\alpha + \beta\,d$.*

DIMOSTRAZIONE. Supponiamo dapprima per semplicità che b e d siano elementi di A, non k-uple (con $k > 1$). Se $b\,\alpha{+}\beta\,d$, allora, per 1.60, $b\ \alpha\ b'_1\ \beta\ b'_2\ \alpha\ b'_3\ \beta\ \ldots d$, per certi $b'_1, b'_2, \ldots$ Se $t(a, b) = t(c, b)$,

otteniamo $t(a,d) = t(c,d)$ applicando ripetutamente il Lemma 7.7 (una volta sì una volta no con β al posto di α. [...]

$$\begin{vmatrix} t(a,b) & t(c,b) \\ t(a,b'_1) & t(c,b'_1) \\ t(a,b'_2) & t(c,b'_2) \\ t(a,b'_3) & t(c,b'_3) \\ \vdots & \vdots \\ t(a,d) & t(c,d) \end{vmatrix}$$

Consideriamo adesso il caso generale. Se $b = (b_1, \ldots, b_k)$ e $d = (d_1, \ldots, d_k)$ sono k-uple (con $k > 1$) e $t(a,b) = t(c,b)$, cioè

$$t(a_1, \ldots, b_1, b_2, b_3, \ldots, b_k) = t(c_1, \ldots, b_1, b_2, b_3, \ldots, b_k),$$

possiamo applicare k volte il ragionamento precedente, ottenendo

$$t(a_1, \ldots, d_1, b_2, b_3, \ldots, b_k) = t(c_1, \ldots, d_1, b_2, b_3, \ldots, b_k),$$

poi

$$t(a_1, \ldots, d_1, d_2, b_3, \ldots, b_k) = t(c_1, \ldots, d_1, d_2, b_3, \ldots, b_k),$$

etc. Alla fine otteniamo

$$t(a_1, \ldots, d_1, d_2, d_3, \ldots, d_k) = t(c_1, \ldots, d_1, d_2, d_3, \ldots, d_k),$$

cioè l'uguaglianza cercata $t(a,d) = t(c,d)$. □

DEFINIZIONE 7.9. Il Lemma 7.7 e il Teorema 7.8 suggeriscono di dare un nome speciale a certi casi particolari della term condition. Così diremo che un'algebra soddisfa alla γ-α-*term condition* se vale il caso particolare della term condition in cui $a \,\gamma\, c$ e $b \,\alpha\, d$.

Secondo questa definizione, la conclusione di 7.7 è che vale la γ-α-term condition, e la conclusione di 7.8 è che vale la γ-$(\alpha + \beta)$-term condition.

OSSERVAZIONE 7.10. (facoltativo) La dimostrazione di 7.8 mostra, più in generale, che se valgono la γ-α-term condition e la γ-β-term condition, allora vale la γ-$(\alpha + \beta)$-term condition. Osserviamo che qui, nonostante le apparenze, non c'è più simmetria. Si possono trovare esempi in cui la γ-α-term condition e la ε-α-term condition *non* implicano la $(\gamma + \varepsilon)$-α-term condition. Si può però ottenere qualche risultato parziale, vedi il Teorema 7.14 più sotto.

TEOREMA 7.11. *Esiste un reticolo* $\mathbf{L}$ *tale che, per ogni algebra* $\mathbf{A}$*, se* $\mathbf{Con}(\mathbf{A}) \cong \mathbf{L}$*, allora* $\mathbf{A}$ *soddisfa a TC.*

DIMOSTRAZIONE. Si consideri il seguente reticolo:

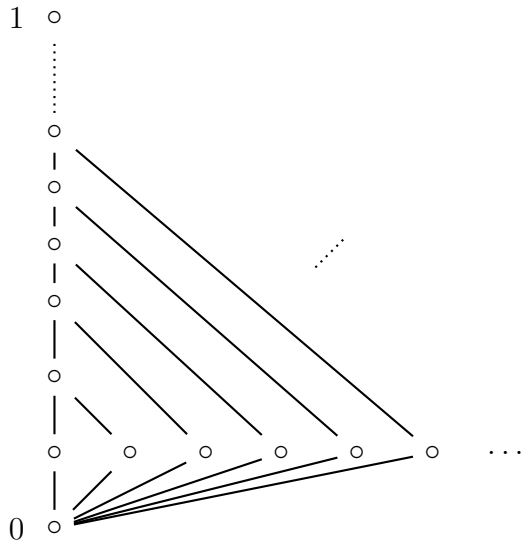


Fig. C

Supponiamo che $\mathbf{Con}(\mathbf{A}) \cong \mathbf{L}$. Per la Proposizione 1.63 abbiamo che $1_{\mathbf{A}}$ non è finitamente generata. Siccome la term condition coinvolge al massimo un numero finito di elementi, basta dimostrare la γ-γ-term condition per ogni $\gamma < 1_{\mathbf{A}}$ (basta prendere come γ la congruenza generata dalle coppie (a_1, c_1), ..., (a_n, c_n), (b_1, d_1), ... (b_k, d_k)). Ma è facile vedere che, per ogni $\gamma < 1$, esistono $\alpha, \beta \in L$ tali che $\gamma\alpha = \gamma\beta = 0$ e $\gamma \leq \alpha + \beta$, quindi è possibile applicare il Teorema 7.8. □

Si può dimostrare (ma noi non lo faremo) che esiste un'algebra $\mathbf{A}$ tale che $\mathbf{Con}(\mathbf{A}) \cong \mathbf{L}$, dove $\mathbf{L}$ è il reticolo usato nella dimostrazione di 7.11. In altre parole, il Teorema 7.11 non è un teorema "vuoto".

Teorema 7.12. *Esiste un reticolo* $\mathbf{L}$ *che è isomorfo a* $\mathbf{Con}(\mathbf{A})$*, per qualche algebra* $\mathbf{A}$*, ma non è isomorfo a* $\mathbf{Con}(\mathbf{S})$*, per nessun semigruppo* $\mathbf{S}$*.*

Facciamo riferimento a [**Ta**] per una dimostrazione completa. Accenniamo solo allo schema della dimostrazione. Dapprima si migliora il Teorema 7.11. Se $\mathbf{L}$ è un reticolo e $\ell \in \mathbf{L}$, sia $\mathbf{L}_\ell$ il sottoreticolo di $\mathbf{L}$ costituito da tutti gli elementi $\geq \ell$. Allora si costruisce un $\mathbf{L}$ tale che, per ogni $\ell \in \mathbf{L}$ con $\ell \neq 1$, esiste $\ell^* \geq \ell$ tale che se $\mathbf{Con}(\mathbf{A}) \cong \mathbf{L}_{\ell^*}$ allora $\mathbf{A}$ soddisfa alla term condition.

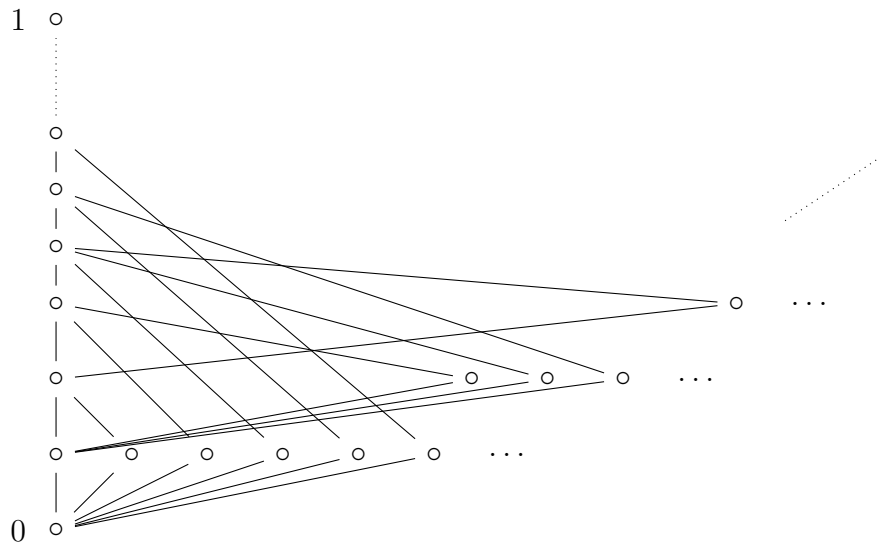


Fig. D

Si suppone adesso che $\mathbf{S}$ sia un semigruppo tale che $\mathbf{Con}(\mathbf{S}) \cong \mathbf{L}_\ell$. Utilizzando gli Esempi 7.4, 7.5 e considerando successivamente vari quozienti si giunge ad un assurdo.

(la parte seguente di questa sezione è opzionale)

Come accennato nell'Osservazione 7.10, non sempre la γ-α-term condition e la ε-α-term condition implicano la $(\gamma+\varepsilon)$-α-term condition. Controesempi possono essere trovati, ad esempio, in [**Wi**]. Esistono però importanti casi particolari in cui questa implicazione vale.

TEOREMA 7.13. *(R. Willard) Se* $\mathbf{A}$ *è un'algebra qualunque,* $\gamma, \varepsilon, \alpha \in \mathbf{Con}(\mathbf{A})$*,* $\gamma + \varepsilon = \gamma \circ \varepsilon \circ \gamma$*,* $\gamma\alpha = \gamma\varepsilon = 0_{\mathbf{A}}$ *e vale la* ε*-*α*-term condition, allora vale la* $(\gamma + \varepsilon)$*-*α*-term condition.*

DIMOSTRAZIONE. Per dimostrare la $(\gamma + \varepsilon)$-α-term condition dobbiamo considerare la situazione data da

$$=$$
$$\begin{vmatrix} t(a,b) & t(c,b) \\ t(a,d) & t(c,d) \end{vmatrix}$$

con $a \ \gamma{+}\varepsilon \ c$ e $b \ \alpha \ d$. Siccome, per ipotesi, $\gamma + \varepsilon = \gamma \circ \varepsilon \circ \gamma$, abbiamo $a \ \gamma \ e \ \varepsilon \ f \ \gamma \ c$, per opportuni $e, f \in A$ (come già osservato, a, c, e, f possono essere n-uple, ma questo non cambia sostanzialmente nulla nel ragionamento successivo). Possiamo quindi scomporre la prima riga della matrice come:

$$=$$
$$t(a\overbrace{,b) \ \gamma \ t(e,b) \ \varepsilon \ t(f,b) \ \gamma \ t(c,}b)$$

Quindi $t(e,b)\ \varepsilon\ t(f,b)$, ma anche $t(e,b)\ \gamma\ t(a,b) = t(c,b)\ \gamma\ t(f,b)$, quindi $t(e,b)\ \gamma\varepsilon\ t(f,b)$, ma siccome $\gamma\varepsilon = 0_{\mathbf{A}}$ per ipotesi, abbiamo $t(e,b) = t(f,b)$.

Possiamo allora applicare la ε-α-term condition alla matrice

$$\begin{array}{c} = \\ \begin{vmatrix} t(e,b) & t(f,b) \\ t(e,d) & t(f,d) \end{vmatrix} \end{array}$$

ottenendo $t(e,d) = t(f,d)$. Abbiamo quindi

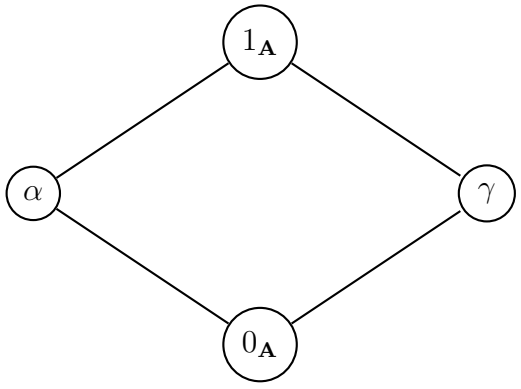
$$\begin{array}{c} = \\ t(a\overbrace{,b)\ \gamma\ t(e,b) = t(f,b)\ \gamma\ t(c,}b) \\ \alpha \qquad\qquad\qquad\qquad\qquad \alpha \\ t(a\underbrace{,d)\ \gamma\ t(e,d) = t(f,d)\ \gamma\ t(c,}_{\gamma}d) \end{array}$$

Dunque $t(a,d)\ \gamma\ t(c,d)$, ma anche, ovviamente, $t(a,d)\ \alpha\ t(a,b) = t(c,b)\ \alpha\ t(c,d)$, quindi $t(a,d)\ \gamma\alpha\ t(c,d)$, ma siccome per ipotesi $\gamma\alpha = 0_{\mathbf{A}}$, abbiamo $t(a,d) = t(c,d)$, quello che dovevamo dimostrare. □

Con una dimostrazione simile ma leggermente più semplice si ottiene il seguente risultato.

PROPOSIZIONE 7.14. *Se* $\mathbf{A}$ *è un'algebra qualunque,* $\gamma, \varepsilon, \alpha \in \mathbf{Con}(\mathbf{A})$*,* $\gamma + \varepsilon = \gamma \circ \varepsilon$*,* $\gamma\varepsilon = 0_{\mathbf{A}}$ *e valgono sia la* ε*-*α*-term condition che la* γ*-*α*-term condition, allora vale la* $(\gamma + \varepsilon)$*-*α*-term condition.*

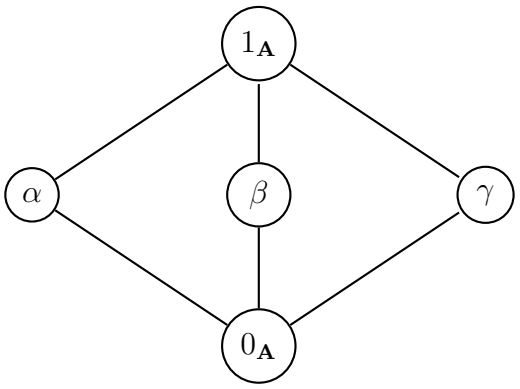
COROLLARIO 7.15. *Se* $\mathbf{A}$ *è un'algebra qualunque,* $\gamma, \alpha \in \mathbf{Con}(\mathbf{A})$*,* $\gamma \circ \alpha \circ \gamma = 1_{\mathbf{A}}$*,* $\gamma\alpha = 0_{\mathbf{A}}$ *e vale la* α*-*α*-term condition, allora* $\mathbf{A}$ *soddisfa alla* $1_{\mathbf{A}}$*-*α*-term condition.*



$\mathbf{D}_2$

DIMOSTRAZIONE. Basta prendere $\varepsilon = \alpha$ nel Teorema 7.13. □

COROLLARIO 7.16. *Se* $\mathbf{A}$ *è un'algebra qualunque,* $\gamma, \alpha, \beta \in \mathbf{Con}(\mathbf{A})$*,* $1_{\mathbf{A}} = \gamma \circ \alpha \circ \gamma = \alpha + \beta = \gamma + \beta$*,* $\gamma\alpha = \alpha\beta = \gamma\beta = 0_{\mathbf{A}}$*, allora* $\mathbf{A}$ *soddisfa alla term condition.*



$\mathbf{M}_3$

(con $1_{\mathbf{A}} = \gamma \circ \alpha \circ \gamma$)

DIMOSTRAZIONE. Per il Lemma di Lampe Teorema 7.8 vale la α-$1_{\mathbf{A}}$-term condition, quindi a maggior ragione la α-α-term condition. Dunque abbiamo la $1_{\mathbf{A}}$-α-term condition per il Corollario 7.15.

Sostituendo nell'enunciato del Teorema 7.13 α al posto di ε e β al posto di α, otteniamo la $1_{\mathbf{A}}$-β-term condition.

Usando la stessa dimostrazione del Lemma di Lampe, abbiamo che la $1_{\mathbf{A}}$-α-term condition insieme alla $1_{\mathbf{A}}$-β-term condition implicano la $1_{\mathbf{A}}$-$(\alpha + \beta)$-term condition (vedi l'Osservazione 7.10).

Ma $\alpha + \beta = 1_{\mathbf{A}}$, quindi abbiamo la $1_{\mathbf{A}}$-$1_{\mathbf{A}}$-term condition, cioè la term condition. □

8. Cenni sulla teoria del commutatore

OSSERVAZIONE 8.1. Come abbiamo osservato in 1.44 (vedi anche 1.40), i reticoli delle congruenze di anelli e gruppi (a meno di isomorfismi di reticoli) sono ben noti a chi ha seguito un corso di algebra. Chi conserva ancora qualche ricordo del corso o dei corsi di algebra, probabilmente noterà che esistono altre utili operazioni sull'insieme degli ideali di un anello e sull'insieme dei sottogruppi (qui consideriamo solo sottogruppi normali) di un gruppo.

Dati due ideali di un anello commutativo, si può costruire un nuovo *ideale prodotto* $IJ = \{i_1 j_1 + i_2 j_2 + \cdots \mid i_1, i_2, \cdots \in I, j_1, j_2, \cdots \in J\}$.

Dati due sottogruppi normali N e M di un gruppo, il loro *commutatore* $[N, M]$ è il sottogruppo generato dagli elementi del tipo $nmn^{-1}m^{-1}$ con $n \in N, m \in M$.

Il prodotto di ideali e il commutatore di sottogruppi normali soddisfano sostanzialmente alle stesse proprietà, anche se indicate con notazioni diverse. Per esempio, la *distributvità*, per gli ideali, è la regola $I(J + K) = IJ +$

IK. La regola corrispondente, nel caso dei sottogruppi normali, si scrive usualmente $[N, MP] = [NM][NP]$.

Abbastanza sorprendentemente, si può definire un commutatore (di due congruenze) anche nel caso più generale del reticolo delle congruenze di una qualunque algebra che appartiene ad una varietà a congruenze modulari. Ancor più sorprendentemente, continuano a valere regole corrispondenti a quelle che valgono nel caso degli ideali e dei sottogruppi normali.

Ricordiamo che indichiamo con la giustapposizione $\alpha\beta$ l'intersezione di due relazioni binarie α e β. Se α e β sono congruenze, scriveremo $\alpha + \beta$ al posto di $\alpha \vee \beta$.

TEOREMA 8.2. *Sia $\mathcal{V}$ una varietà a congruenze modulari. Per ogni algebra $\mathbf{A} \in \mathcal{V}$ è possibile definire un'operazione binaria su $Con(\mathbf{A})$, indicata con $[\alpha, \beta]$ e detta* commutatore (di α e β) *tale che, per tutte le congruenze α, β, γ su $\mathbf{A}$, valgono:*

$$[\alpha, \beta] \leq \alpha\beta \tag{15}$$

$$[\alpha, \beta] = [\beta, \alpha] \tag{16}$$

$$[\gamma, \alpha + \beta] = [\gamma, \alpha] + [\gamma, \beta] \tag{17}$$

$$[\alpha, \beta] \leq [\alpha', \beta'], \text{ se } \alpha \leq \alpha' \text{ e } \beta \leq \beta' \tag{18}$$

Inoltre esiste un termine differenza $d(x, y, z)$ *che soddisfa a*

$$x = d(x, y, y) \text{ e} \tag{19}$$

$$d(x, x, y)[\alpha, \alpha]y, \text{ se } x, y \in A \text{ e } x \,\alpha\, y \tag{20}$$

OSSERVAZIONE 8.3. (non fa parte del programma) Il lettore che desiderasse una dimostrazione del teorema può consultare [**Gu**] o [**FMK**]. Vedi anche [**Ta**].

Nei casi particolari di gruppi e anelli il commutatore di congruenze dato dal Teorema 8.2 coincide con le operazioni menzionate in 8.1 (modulo l'isomorfismo fra i reticoli di congruenze e i reticoli dei sottogruppi normali o degli ideali).

Osserviamo che il commutatore di congruenze non è definito univocamente dalle condizioni (15)-(20). Esiste comunque una condizione relativa ai morfismi che determina univocamente il commutatore di congruenze; facciamo di nuovo riferimento a [**FMK**] per i dettagli.

OSSERVAZIONE 8.4. Per il lettore che desiderasse conoscere la definizione di $[\alpha, \beta]$, precisiamo innanzitutto che esistono parecchie definizioni diverse, che si rivelano tutte equivalenti (limitatamente alle varietà a congruenze modulari). Una fra le tante possibili definizioni di $[\alpha, \beta]$ può essere data tramite una generalizzazione della term condition (vedi la Definizione 7.2). Infatti, $[\gamma, \alpha] = 0$ risulta equivalente a quella che abbiamo chiamato γ-α-term condition nella Definizione 7.9.

La definizione generale di $[\alpha, \beta]$ è leggermente più complessa. Diciamo che una matrice

$$\begin{vmatrix} t(a,b) & t(c,b) \\ t(a,d) & t(c,d) \end{vmatrix}$$

è una γ-α-matrice se $a\ \gamma\ c$ e $b\ \alpha\ d$. Allora $[\gamma, \alpha]$ è la più piccola congruenza δ tale che, per ogni γ-α-matrice, se gli elementi di una riga sono congruenti modulo δ, allora anche gli elementi dell'altra riga sono congruenti modulo δ. (Il lettore saprebbe verificare che esiste effettivamente la più piccola congruenza δ con questa proprietà?)

Il lettore potrebbe aver notato che nella definizione precedente non abbiamo utilizzato affatto l'ipotesi che stiamo considerando un'algebra in una varietà a congruenza modulari, cioè, che la definizione precedente si può dare per *qualunque* algebra. Tale lettore, a nostro parere, avrebbe sicuramente mostrato una notevole vocazione per l'algebra universale. Comunque, così come esistono applicazioni della term condition, esistono applicazioni del commutatore come definito qui per qualunque algebra, anche non appartenente ad una varietà a congruenze modulari.

La proprietà (18) in 8.2 è banale, per il commutatore appena definito; anche la (15) è di facile verifica (e non è necessario usare la modularità: basta verificare che $\alpha\beta$ è una fra le possibili δ fra cui si sceglie la più piccola). La dimostrazione delle altre proprietà è più complessa e necessita comunque di ipotesi addizionali. Vale comunque sempre un caso particolare della proprietà distributiva, detta *proprietà semidistributiva*: se $[\gamma, \alpha] = [\gamma, \beta]$, allora $[\gamma, \alpha + \beta] = [\gamma, \alpha] = [\gamma, \beta]$. Questo si dimostra in maniera simile al Lemma di Lampe 7.8.

Osserviamo inoltre che è facile dimostrare che se $\mathbf{A}$ è un'algebra tale che $\mathbf{Con}(\mathbf{A})$ è modulare (senza bisogno di ipotesi su varietà a cui appartenga $\mathbf{A}$!), allora il commutatore appena introdotto soddisfa a

$$[\gamma, \alpha + \beta] \leq \gamma\alpha + \gamma\beta \tag{21}$$

Anzi, è sufficiente che in $\mathbf{A}$ valga $\gamma(\varepsilon \circ \delta\gamma \circ \varepsilon) \subseteq \gamma\alpha + \gamma\beta$, che è un'ipotesi più debole della modularità (perchè?[10]).

Per dimostrare che se $\mathbf{Con}(\mathbf{A})$ è modulare, allora vale l'equazione (21), basta usare l'inclusione precedente, prendendo alternativamente $\varepsilon = \alpha$ e $\varepsilon = \beta$, e usando $\delta = \gamma\alpha + \gamma\beta$, ragionando come nella dimostrazone di 7.8.

Corollario 8.5. *Sia* $\mathbf{A}$ *un'algebra appartenente ad una varietà a congruenze modulari. Allora, per congruenze* $\alpha, \beta, \gamma \in \mathbf{Con}(\mathbf{A})$*, valgono le seguenti affermazioni.*

(1) $\alpha \circ \beta \subseteq \beta \circ \alpha \circ [\beta, \beta]$
(2) Se $[\beta, \beta] \subseteq \alpha$*, allora* α *e* β *permutano, cioè* $\alpha \circ \beta = \beta \circ \alpha$
(3) $\alpha + \beta = \alpha \circ \beta \circ ([\alpha, \alpha] + [\beta, \beta])$

[10]Qui chiediamo solo perché la modularità implica questa ipotesi, non chiediamo di mostrare che si tratta di un'ipotesi *strettamente* più debole.

(4) $\gamma(\alpha \circ \beta) \subseteq \gamma(\beta \circ \alpha) \circ (\gamma\alpha + \gamma\beta)$
(5) $\gamma(\alpha \circ \beta \circ \alpha) \subseteq \gamma(\beta \circ \alpha) \circ (\gamma\alpha + \gamma\beta)$
(6) Più in generale, $\gamma(\alpha + \beta) \subseteq \gamma(\beta \circ \alpha) \circ (\gamma\alpha + \gamma\beta)$

DIMOSTRAZIONE. (1) Se $a \ \alpha \circ \beta \ c$, allora esiste $b \in A$ tale che $a \ \alpha \ b \ \beta \ c$. Usando il termine differenza d dato dal Teorema 8.2, calcoliamo:

$$a = d(a,b,b) \ \beta \ d(a,b,c) \ \alpha \ d(b,b,c) \ [\beta,\beta] \ c \tag{22}$$

Questo implica che $a \ \beta\circ\alpha\circ[\beta,\beta] \ c$.

(2) Se $[\beta,\beta] \subseteq \alpha$, allora $\alpha \circ [\beta,\beta] = \alpha$, quindi (1) fornisce $\alpha \circ \beta \subseteq \beta \circ \alpha$. Ma questo implica che α e β permutano, per l'Osservazione 5.2.

(3) (è facoltativo) ed è lasciato per esercizio al lettore.

(4) Come in (1), abbiamo $a \ \alpha \ b \ \beta \ c$, per qualche b. Inoltre, da $a \ \alpha\circ\beta \ c$ segue $a \ \alpha+\beta \ c$ e, siccome $a \ \gamma \ c$, abbiamo $a \ \gamma(\alpha+\beta) \ c$. Usando il termine differenza d dato dal Teorema 8.2, calcoliamo:

$$a = d(a,b,b) \ \beta \ d(a,b,c) \ \alpha \ d(a,a,c) \ [\gamma(\alpha+\beta),\gamma(\alpha+\beta)] \ c \tag{23}$$

Questo implica che

$$\gamma(\alpha \circ \beta) \subseteq \beta \circ \alpha \circ [\gamma(\alpha+\beta),\gamma(\alpha+\beta)] \tag{24}$$

Ma per (18), (17) e (15), $[\gamma(\alpha+\beta),\gamma(\alpha+\beta)] \leq [\gamma,\alpha+\beta] = [\gamma,\alpha] + [\gamma,\beta] \leq \gamma\alpha + \gamma\beta$. Sostituendo in (24) otteniamo (4).

Osserviamo una notevole somiglianza fra i calcoli in (22) e (23): l'unica differenza è che, alla fine, abbiamo spostato un b in a, anzichè spostare un a in b. Ma il risultato è di natura completamente diversa, perchè il commutatore non compare nell'inclusione (4)!

Così come (3) può essere pensata come un'iterazione di (1), vediamo adesso che anche (4) si può iterare.

(5) Se $a \ \alpha \circ \beta \circ \alpha \ c$, allora esistono b_1 e b_2 tali che $a \ \alpha \ b_1 \ \beta \ b_2 \ \alpha \ c$. Usando il termine differenza d, calcoliamo: $a = d(a,b_1,b_1) \ \beta \ d(a,b_1,b_2) \ \alpha \ d(a,a,c) \ [\gamma(\alpha+\beta),\gamma(\alpha+\beta)] \ c$. Come nella dimostrazione di (4) sopra, abbiamo $[\gamma(\alpha+\beta),\gamma(\alpha+\beta)] \leq \gamma\alpha+\gamma\beta$, da cui segue (5).

(6) [...] La dimostrazione di (5) si può generalizzare ottenendo, per qualunque $i \in \mathbb{N}$, $\gamma(\underbrace{\alpha \circ \beta \circ \alpha \circ \ldots}_{i+2 \text{ segni di } \circ}) \subseteq \gamma(\underbrace{\beta \circ \alpha \circ \ldots}_{i+1 \text{ segni di } \circ})$. Allora, per induzione (ed eventualmente usando (4) alla fine per scambiare la posizione di α con β) si ottiene $\gamma(\underbrace{\beta \circ \alpha \circ \ldots}_{i+1 \text{ segni di } \circ}) \subseteq \gamma(\beta \circ \alpha) \circ (\gamma\alpha + \gamma\beta)$. Siccome questa inclusione vale per ogni $i \in \mathbb{N}$, si ottiene (6). □

OSSERVAZIONE 8.6. Osserviamo che nella dimostrazione di 8.5 abbiamo usato molto meno dell'ipotesi che $\mathbf{A}$ appartenga ad una varietà a congruenze modulari.

Intanto la modularità di $\mathbf{Con}(\mathbf{A})$ non è mai stata usata direttamente, ma solo per poter applicare il Teorema 8.2.

Per dimostrare (1)-(3) abbiamo usato esclusivamente l'esistenza di un termine differenza. Questa è un'ipotesi molto più debole dell'appartenenza ad una varietà a congruenze modulari.

Per dimostrare (4)-(6) abbiamo usato, oltre al termine differenza, le equazioni (15), (17) e (18). Ma l'unica cosa che serve, è semplicemente la conseguenza che $[\gamma(\alpha+\beta),\gamma(\alpha+\beta)] \leq \gamma\alpha+\gamma\beta$. Come abbiamo visto alla fine dell'Osservazione 8.4, per dimostrare questo basta che $\mathbf{Con}(\mathbf{A})$ sia modulare.

Nonostante le apparenze, queste ipotesi "minime" (cioè l'esistenza di un termine differenza insieme a $[\gamma(\alpha+\beta),\gamma(\alpha+\beta)] \leq \gamma\alpha+\gamma\beta$) sono sufficientemente forti per riottenere la modularità; infatti, per varietà, ciascuna delle inclusioni (4)-(6) è equivalente alla modularità, come dimostrato da S. Tschantz. Lo facciamo vedere nel caso dell'identità (6); nel caso di (4) o (5) le dimostrazioni sarebbero più complesse.

PROPOSIZIONE 8.7. *Se in un algebra* $\mathbf{A}$ *vale 8.5(6), cioè* $\gamma(\alpha+\beta) \subseteq \gamma(\beta\circ\alpha)\circ(\gamma\alpha+\gamma\beta)$*, allora* $\mathbf{Con}(\mathbf{A})$ *è modulare.*

DIMOSTRAZIONE. Considerando $\beta\gamma$ al posto di β, otteniamo $\gamma(\alpha+\beta\gamma) \subseteq \gamma(\beta\gamma\circ\alpha)\circ(\gamma\alpha+\gamma\beta)$. Ma $\gamma(\beta\gamma\circ\alpha) = \gamma\beta\circ\gamma\alpha$ (cf. la dimostrazione della Proposizione 5.7), da cui segue $\gamma(\alpha+\beta\gamma) \leq \gamma\alpha+\gamma\beta$. □

OSSERVAZIONE 8.8. Nel caso si considerasse la classe degli anelli non (necessariamente) commutativi, alle congruenze corrispondono ideali bilateri. Se I e J sono ideali bilateri, allora anche IJ è un ideale bilatero, ma non vale necessariamente $IJ = JI$. In questo caso, l'ideale bilatero che corrisponde al commutatore di congruenze è $IJ + JI$. Con questo ideale, tutte le proprietà menzionate nel Teorema 8.2 valgono.

OSSERVAZIONE 8.9. (non fa parte del programma) Abbiamo detto che il commutatore di congruenze in varietà a congruenze modulari soddisfa sostanzialmente a tutte le proprietà soddisfatte dal prodotto di ideali e dal commutatore di sottogruppi normali. In realtà, esiste una proprietà, il *Lemma dei tre sottogruppi*

$$[[M,N],P] \leq [[N,P],M][[P,M],N]$$

che vale per i sottogruppi normali di un gruppo. Con le nostre notazioni per le congruenze, l'equivalente del Lemma dei tre sottogruppi verrebbe scritto

$$[[\alpha,\beta],\gamma] \leq [[\beta,\gamma],\alpha] + [[\gamma,\alpha],\beta]$$

Questa proprietà vale per gli ideali bilateri di anelli (anche non commutativi; ricordiamo che, in questo caso, dobbiamo prendere $IJ + JI$ come "commutatore"), ma non vale necessariamente per le congruenze in algebre. Per esempio, basta considerare anelli "non associativi" (nel senso che valgono tutti gli assiomi di anello tranne l'associatività del prodotto).

8.1. Il caso di algebre qualunque (senza nessuna ipotesi su varietà). (opzionale)

Osservazione 8.10. Come abbiamo visto in 8.6 e 8.7, l'esistenza di un "commutatore" nel reticolo delle congruenze di un'algebra $\mathbf{A}$ implica che $\mathbf{Con}(\mathbf{A})$ è modulare, purché siano valide (alcune del)le proprietà indicate in 8.2. Quindi il lettore potrà pensare che la teoria del commutatore in algebra universale sia limitata al caso delle algebre in una varietà a congruenze modulari. In realtà, la teoria può essere sviluppata in un ambito molto più generale. Ad alcune delle proprietà elencate in 8.2 sarà necesario rinunciare, per quanto appena detto, ma molte delle conseguenze che avevamo ottenuto si possono ottenere ugualmente anche con ipotesi molto più deboli.

D'ora in poi $\mathbf{A}$ sarà un'algebra qualunque; non si assume che $\mathbf{A}$ appartenga necessariamente ad una varietà a congruenze modulari, anzi, di solito non verrà fatta alcuna ipotesi su varietà. Il commutatore $[\gamma, \alpha]$ di due congruenze in $\mathbf{Con}(\mathbf{A})$ sarà sempre quello definito nell'Osservazione 8.4. Ripetiamo che questa non è l'unica definizione possibile, e che, in alcuni casi, altre definizioni risultano comunque equivalenti. Il lettore interessato ai dettagli può consultare [**KS**] e [**KK**]. Ricordiamo che $[\gamma, \alpha] = 0$ è equivalente a quella che abbiamo chiamato γ-α-term condition (Definizione 7.2); in particolare, $[1_{\mathbf{A}}, 1_{\mathbf{A}}] = 0$ è la term condition.

Definizione 8.11. Un *termine differenza debole* per un'algebra $\mathbf{A}$ è un termine $d(x, y, z)$ (per il tipo di $\mathbf{A}$) che soddisfa a

$$x \; [\alpha, \alpha] \; d(x, y, y) \quad \text{e} \quad d(x, x, y) \; [\alpha, \alpha] \; y, \tag{25}$$

ogni volta che $x, y \in A$ e $x \; \alpha \; y$.

Osservazione 8.12. In altre parole, un termine differenza debole è un termine che soddisfa alle identità di Mal'cev date dal Teorema 5.5 "modulo il commutatore". Un termine differenza (come definito alla fine di 8.2) è una variante intermedia, che soddisfa solo ad una delle due identità.

Dimostriamo adesso alcune conseguenze dell'esistenza di un termine differenza debole; queste conseguenze sono analoghe a quelle trovate nel Corollario 8.5(1)-(3). Per inciso, non sembrano esistere semplici conseguenze dell'esistenza di un termine differenza debole analoghe a 8.5(4)-(6); del resto, come osservato, queste ultime condizioni implicano la modularità, mentre l'esistenza di un termine differenza debole si rivela un'ipotesi soddisfatta in un gran numero di casi (vedi l'esempio 6.4 in [**KK**]).

Corollario 8.13. *Sia* $\mathbf{A}$ *un'algebra con un termine differenza debole. Allora, per congruenze* $\alpha, \beta, \gamma \in \mathbf{Con}(\mathbf{A})$*, valgono le seguenti affermazioni.*

(1) $\alpha \circ \beta \subseteq [\alpha, \alpha] \circ \beta \circ \alpha \circ [\beta, \beta]$

(2) Se $[\beta,\beta] \subseteq \alpha$ *e* $[\alpha,\alpha] \subseteq \beta$*, allora* α *e* β *permutano, cioè* $\alpha \circ \beta = \beta \circ \alpha$
(3) Più in generale, $\alpha+\beta = ([\alpha,\alpha]+[\beta,\beta]) \circ \alpha \circ \beta \circ ([\alpha,\alpha]+[\beta,\beta])$
(4) Se $[\alpha,\alpha] = 0$*, allora* $\alpha \circ \beta \circ \alpha \subseteq \beta \circ \alpha \circ \beta$
(5) Se $[\alpha,\alpha] = 0$*, allora* $\alpha + \beta = \beta \circ \alpha \circ \beta$

DIMOSTRAZIONE. (1) Se $a\ \alpha \circ \beta\ c$, allora esiste $b \in A$ tale che $a\ \alpha\ b\ \beta\ c$. Usando il termine differenza debole d, analogamente a 8.5(1) calcoliamo:

$$a\ [\alpha,\alpha]\ d(a,b,b)\ \beta\ d(a,b,c)\ \alpha\ d(b,b,c)\ [\beta,\beta]\ c \tag{26}$$

Questo implica che $a\ [\alpha,\alpha]\circ\beta\circ\alpha\circ[\beta,\beta]\ c$.

(2) Se $[\beta,\beta] \subseteq \alpha$, allora $\alpha \circ [\beta,\beta] = \alpha$, simmetricamente, da $[\alpha,\alpha] \subseteq \beta$ si ottiene $\beta \circ [\alpha,\alpha] = \beta$, quindi (1) fornisce $\alpha \circ \beta \subseteq \beta \circ \alpha$. Ma questo implica che α e β permutano, per l'Osservazione 5.2.

(3) (è facoltativo) ed è lasciato per esercizio (non immediato) al lettore.

(4) Se $a\ \alpha \circ \beta \circ \alpha\ e$, allora esistono $b, c \in A$ tali che $a\ \alpha\ b\ \beta\ c\ \alpha\ e$. Se d è un termine differenza debole, e siccome $[\alpha,\alpha] = 0$, abbiamo $a = d(a,b,b)$ e $d(c,c,e) = e$. Quindi possiamo calcolare:

$$a = d(a,b,b)\ \beta\ d(a,b,c)\ \alpha\ d(b,b,e)\ \beta\ d(c,c,e) = e \tag{27}$$

Questo implica che $a\ \beta\circ\alpha\circ\beta\ c$. Osserviamo che la dimostrazione è leggermente diversa da quella di (1). Qui nel passo "centrale" $d(a,b,c)\ \alpha\ d(b,b,e)$ abbiamo usato contemporaneamente $a\ \alpha\ b$ e $c\ \alpha\ e$.

(5) segue facilmente da (4). Se $(a,b) \in \alpha + \beta$, allora esiste un $n \in \mathbb{N}$ tale che $(a,b) \in \underbrace{\alpha \circ \beta \circ \alpha \circ \dots}_{n \text{ segni di } \circ}$, per la Proposizione 1.60. Ma, usando $\alpha \circ \beta \circ \alpha \subseteq \beta \circ \alpha \circ \beta$, si vede subito che, per ogni $n \in \mathbb{N}$, si ha $\underbrace{\alpha \circ \beta \circ \alpha \circ \dots}_{n \text{ segni di } \circ} \subseteq \beta \circ \alpha \circ \beta$. Ad esempio, applicando di volta in volta (4) alle congruenze evidenziate in grassetto (e ovviamente utilizzando l'associatività di $\circ$ e la transitività di β), abbiamo $\boldsymbol{\alpha\circ\beta\circ\alpha}\circ\beta\circ\alpha\circ\beta\circ\alpha \subseteq \beta\circ\alpha\circ\beta\circ\beta\circ\alpha\circ\beta\circ\alpha = \beta\circ\boldsymbol{\alpha\circ\beta\circ\alpha}\circ\beta\circ\alpha \subseteq \beta\circ\beta\circ\alpha\circ\beta\circ\beta\circ\alpha = \beta\circ\boldsymbol{\alpha\circ\beta\circ\alpha} \subseteq \beta\circ\beta\circ\alpha\circ\beta = \beta\circ\alpha\circ\beta$.

Il lettore che non fosse convinto che questo esempio si generalizza per n arbitrario può scrivere i dettagli di una dimostrazione per induzione. □

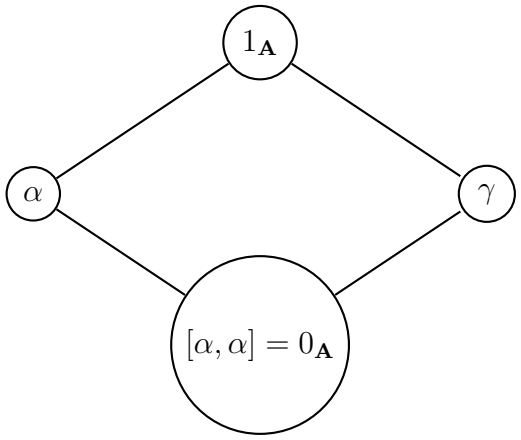
OSSERVAZIONE 8.14. Naturalmente, la dimostrazione di (5) appena presentata ha ben poco a che vedere con la teoria del commutatore. Abbiamo dimostrato che se α e β sono congruenze di un'algebra tali che $\alpha \circ \beta \circ \alpha \subseteq \beta \circ \alpha \circ \beta$, allora $\alpha + \beta = \beta \circ \alpha \circ \beta$.

Si può generalizzare l'enunciato precedente? Per esempio, si può dire qualcosa su $\alpha+\beta$ se $\alpha\circ\beta\circ\alpha\circ\beta \subseteq \beta\circ\alpha\circ\beta\circ\alpha$? È vero che se $\alpha\circ\beta\circ\alpha \subseteq \beta\circ\alpha\circ\beta$ allora $\alpha+\beta = \alpha\circ\beta\circ\alpha$?

Per inciso, osserviamo anche che 8.13(5) non è il miglior risultato possibile. Da 8.13(3), se $[\alpha,\alpha]=0$, segue $\alpha+\beta=[\beta,\beta]\circ\alpha\circ\beta$. Ma la dimostrazione di (3) non è semplice, quindi, per semplificare, abbiamo presentato una dimostrazione diretta di (5). Infatti in queste note utilizzeremo (5) ma non utilizzeremo mai (3).

COROLLARIO 8.15. *Sia* $\mathbf{A}$ *un'algebra con un termine differenza debole e siano* $\gamma,\alpha \in \mathbf{Con}(\mathbf{A})$ *congruenze tali che* $\gamma+\alpha = 1_{\mathbf{A}}$ *e* $\gamma\alpha = 0_{\mathbf{A}}$. *Allora*

(1) $[\alpha,\alpha] = 0_{\mathbf{A}}$ *se e solo se* $[1_{\mathbf{A}},1_{\mathbf{A}}] \leq \gamma$
(2) $[1_{\mathbf{A}},1_{\mathbf{A}}] = 0_{\mathbf{A}}$ *se e solo se* $[\alpha,\alpha] = 0_{\mathbf{A}}$ *e* $[\gamma,\gamma] = 0_{\mathbf{A}}$.



$\mathbf{D}_2$

DIMOSTRAZIONE. (1) Se $[1_{\mathbf{A}},1_{\mathbf{A}}] \leq \gamma$, allora $[\alpha,\alpha] \leq [1_{\mathbf{A}},1_{\mathbf{A}}] \leq \gamma$, siccome il commutatore è monotono. Ma vale anche $[\alpha,\alpha] \leq \alpha$, quindi $[\alpha,\alpha] \leq \alpha\gamma = 0_{\mathbf{A}}$.

Nell'altra direzione, vogliamo dimostrare che se abbiamo

$$\gamma \quad \begin{vmatrix} t(a,b) & t(c,b) \\ t(a,d) & t(c,d) \end{vmatrix}$$

cioè $t(a,b)\ \gamma\ t(c,b)$, allora anche $t(a,d)\ \gamma\ t(c,d)$.

Questo è banale se $b\ \gamma\ d$.

Consideriamo adesso il caso in cui $b\ \alpha\ d$. Se $[\alpha,\alpha] = 0_{\mathbf{A}}$, allora per il Corollario 8.13(5), abbiamo $\alpha+\gamma = \gamma\circ\alpha\circ\gamma$. La dimostrazione adesso segue le linee della dimostrazione del Teorema 7.13. Siccome $\gamma+\alpha = \gamma\circ\alpha\circ\gamma$, abbiamo $a\ \gamma\ e\ \alpha\ f\ \gamma\ c$, per opportuni $e,f \in A$. Come

in 7.13, possiamo scomporre la prima riga della matrice come:

$$t(a, \overbrace{b)\ \gamma\ t(e,b)\ \alpha\ t(f,b)\ \gamma\ t(c,}^{\gamma} b)$$

quindi $t(e,b)\ \alpha\ t(f,b)$, e $t(e,b)\ \gamma\ t(a,b)\ \gamma\ t(c,b)\ \gamma\ t(f,b)$, quindi $t(e,b)\ \gamma\alpha\ t(f,b)$, ma siccome $\gamma\alpha = 0_{\mathbf{A}}$ per ipotesi, abbiamo $t(e,b) = t(f,b)$.

Siccome $[\alpha,\alpha] = 0_{\mathbf{A}}$ è la stessa cosa della α-α-term condition, possiamo applicare quest'ultima alla matrice

$$= \begin{vmatrix} t(e,b) & t(f,b) \\ t(e,d) & t(f,d) \end{vmatrix}$$

ottenendo $t(e,d) = t(f,d)$. Abbiamo quindi $t(a,d)\ \gamma\ t(e,d) = t(f,d)\ \gamma\ t(c,d)$, quindi $t(a,d)\ \gamma\ t(c,d)$, come volevamo dimostrare (vedi diagramma seguente).

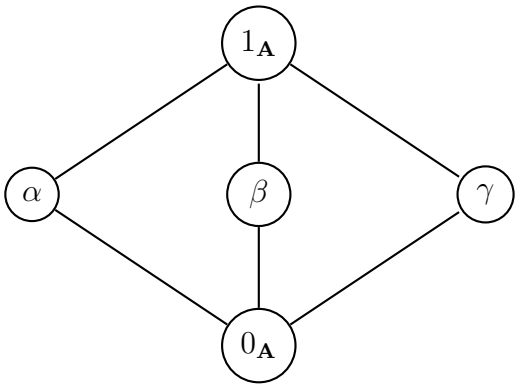
$$\begin{aligned} &t(a,b)\ \gamma\ t(e,b) = t(f,b)\ \gamma\ t(c,b) \\ &t(a, \underbrace{d)\ \gamma\ t(e,d) = t(f,d)\ \gamma\ t(c,}_{\gamma} d) \end{aligned}$$

Dai casi particolari $b\ \gamma\ d$ e $b\ \alpha\ d$ segue il caso in cui b e d sono elementi qualunque di A, ragionando come nella dimostrazione del Teorema 7.8 (anzi, qui la lunghezza della catena è limitata, poichè, per 8.13, abbiamo $b\ \gamma\circ\alpha\circ\gamma\ d$, quindi basta applicare due volte il caso banale $b\ \gamma\ d$ e una volta sola il caso $b\ \alpha\ d$, ovviamente usando nomi diversi per gli elementi che si considerano, diciamo, $b\ \gamma\ b_1$, $b_1\ \alpha\ b_2$ e $b_2\ \gamma\ d$).

(2) La parte necessaria è banale per la monotonia del commutatore.

Per l'altra direzione, se $[\alpha,\alpha] = 0_{\mathbf{A}}$, allora $[1_{\mathbf{A}}, 1_{\mathbf{A}}] \leq \gamma$, per (1). Ma, scambiando α con γ, abbiamo che $[\gamma,\gamma] = 0_{\mathbf{A}}$, implica $[1_{\mathbf{A}}, 1_{\mathbf{A}}] \leq \alpha$. In conclusione, $[1_{\mathbf{A}}, 1_{\mathbf{A}}] \leq \alpha\gamma = 0_{\mathbf{A}}$. □

Corollario 8.16. *Se* $\mathbf{A}$ *è un'algebra con un termine differenza debole,* $\gamma, \alpha, \beta \in \mathbf{Con}(\mathbf{A})$, $1_{\mathbf{A}} = \gamma + \alpha = \alpha + \beta = \gamma + \beta$, $\gamma\alpha = \alpha\beta = \gamma\beta = 0_{\mathbf{A}}$, *allora* $\mathbf{A}$ *soddisfa alla term condition, cioè* $[1_{\mathbf{A}}, 1_{\mathbf{A}}] = 0_{\mathbf{A}}$



$\mathbf{M}_3$

DIMOSTRAZIONE. Per il Lemma di Lampe, $[\alpha, 1_{\mathbf{A}}] = 0_{\mathbf{A}}$, quindi $[\alpha, \alpha] = 0_{\mathbf{A}}$, ma anche $[\gamma, \gamma] = 0_{\mathbf{A}}$. Adesso 8.15(2) implica che $[1_{\mathbf{A}}, 1_{\mathbf{A}}] = 0_{\mathbf{A}}$.

Un'altra dimostrazione (che non fa uso di 8.15): come sopra abbiamo $[\alpha, \alpha] = 0_{\mathbf{A}}$, quindi per 8.13(5) $1_{\mathbf{A}} = \gamma \circ \alpha \circ \gamma$. Adesso basta applicare il Corollario 7.16.

Ancora un'altra dimostrazione. Come all'inizio, abbiamo $[\alpha, \alpha] = 0_{\mathbf{A}}$, e $[\gamma, \gamma] = 0_{\mathbf{A}}$. Per il Corollario 8.13(2), α e γ permutano. Dalla Proposizione 7.14 otteniamo la $1_{\mathbf{A}}$-α-term condition e, per simmetria, la $1_{\mathbf{A}}$-β-term condition e basta applicare il Lemma di Lampe. □

9. Per varietà, la modularità per congruenze implica la legge arguesiana

In questa sezione accenniamo ad una dimostrazione che se un algebra $\mathbf{A}$ appartiene ad una varietà a congruenze modulari, allora $\mathbf{Con}(\mathbf{A})$ è arguesiano. Osserviamo innanzitutto che la dimostrazione del Teorema 6.7 usa solo parzialmente l'ipotesi che siamo in un reticolo di relazioni di equivalenza permutabili. Infatti, nella dimostrazione abbiamo usato solo che α_1 permuta con β_1, α_2 permuta con β_2 e α_3 permuta con β_3. La dimostrazione in realtà ci fornisce il seguente lemma.

LEMMA 9.1. *Se α_1, β_1, α_2, β_2, α_3, β_3 sono relazioni di equivalenza su un insieme A, allora*

$$(\alpha_1 \circ \beta_1)(\alpha_2 \circ \beta_2)(\alpha_3 \circ \beta_3) \leq \alpha_1(\alpha_2 + \gamma_{12}(\gamma_{23} + \gamma_{13})) + \beta_1$$

dove abbiamo usato la convenzione introdotta nella Definizione 6.4, cioè $\gamma_{12} = (\alpha_1 + \alpha_2)(\beta_1 + \beta_2)$, etc.

D'ora in poi supponiamo che $\alpha_1, \beta_1, \alpha_2, \beta_2, \alpha_3, \beta_3$ siano congruenze fissate di un'algebra $\mathbf{A}$, e sia per brevità $\delta = (\alpha_1+\beta_1)(\alpha_2+\beta_2)(\alpha_3+\beta_3)$.

L'idea nella prossima proposizione è che la dimostrazione del Corollario 8.5(5)(6) fornisce un limite superiore a δ. Questo è dovuto al fatto

che l'elemento $d(a, a, c)$ usato nella dimostrazione di 8.5(5) è indipendente dai vari b_1, b_2, etc. Quindi possiamo applicare *simultaneamente* lo stesso ragionamento ad $\alpha_1 + \beta_1$, $\alpha_2 + \beta_2$ e $\alpha_3 + \beta_3$.

Ricordiamo che la definizione di termine-differenza è data nell'enunciato del Teorema 8.2.

PROPOSIZIONE 9.2. *Se* $\mathbf{A}$ *ha un termine-differenza, allora*

$$\delta \subseteq (\alpha_1 \circ \beta_1)(\alpha_2 \circ \beta_2)(\alpha_3 \circ \beta_3) \circ [\delta, \delta] \tag{28}$$

dove $\delta = (\alpha_1 + \beta_1)(\alpha_2 + \beta_2)(\alpha_3 + \beta_3)$.

DIMOSTRAZIONE. Sia $a\ \delta\ c$. Quindi $a\ \alpha_1{+}\beta_1\ c$, quindi esistono $b_{11}, b_{12}, \ldots, b_{1n_1}$ tali che $a\ \alpha_1\ b_{11}\ \beta_1\ b_{12}\ \alpha_1\ \ldots\ b_{1n_1}$. Allo stesso modo, esistono $b_{21}, b_{22}, \ldots, b_{2n_2}$ tali che $a\ \alpha_2\ b_{21}\ \beta_2\ b_{22}\ \alpha_2\ \ldots\ b_{2n_2}$, e lo stesso per il terzo indice.

Possiamo supporre senza perdere in generalità che $n_1 = n_2 = n_3 = n$, e che n sia dispari (perchè?)

Scriviamo $\alpha \circ_m \beta$ per $\underbrace{\alpha \circ \beta \circ \alpha \circ \ldots}_{m \text{ segni di } \circ}$ Quindi, per quanto supposto, abbiamo $(a, c) \in (\alpha_1 \circ_n \beta_1)(\alpha_2 \circ_n \beta_2)(\alpha_3 \circ_n \beta_3)$ (naturalmente, n dipende dalla coppia (a, c), ma per ogni coppia esiste un n tale che la relazione è verificata).

Se $n = 1$, abbiamo $(a, c) \in (\alpha_1 \circ \beta_1)(\alpha_2 \circ \beta_2)(\alpha_3 \circ \beta_3)$ e quindi (28) è verificata.

Supponiamo $n > 1$. Usando il termine-differenza, per ogni $i = 1, 2, 3$, abbiamo

$$a = d(a, b_{i1}, b_{i1})\beta_i d(a, b_{i1}, b_{i2})\alpha_i d(a, a, b_{i3})\beta_i d(a, a, b_{i4}) \ldots d(a, a, c)$$

quindi, ponendo $c_1 = d(a, a, c)$, abbiamo $(a, c_1) \in (\beta_1 \circ_{n-1} \alpha_1)(\beta_2 \circ_{n-1} \alpha_2)(\beta_3 \circ_{n-1} \alpha_3)$. Ripetendo lo stesso ragionamento con c_1 al posto di c, e ponendo $c_2 = d(a, a, c_1)$, abbiamo $(a, c_2) \in (\alpha_1 \circ_{n-2} \beta_1)(\alpha_2 \circ_{n-2} \beta_2)(\alpha_3 \circ_{n-2} \beta_3)$. Ripetendo il ragionamento $n-1$ volte, abbiamo $(a, c_{n-1}) \in (\alpha_1 \circ \beta_1)(\alpha_2 \circ \beta_2)(\alpha_3 \circ \beta_3)$.

Osserviamo che, per definizione di termine differenza, siccome $a\ \delta\ c$, abbiamo $c_1 = d(a, a, c)\ [\delta, \delta]\ c$. Inoltre, siccome $[\delta, \delta] \leq \delta$, vale anche $c_1\ \delta\ c \delta a$, da cui, ancora per le proprietà di un termine differenza, $c_2 = d(a, a, c_1)\ [\delta, \delta]\ c_1$, e così via.

Mettendo tutto insieme, abbaiamo $a\ (\alpha_1 \circ \beta_1)(\alpha_2 \circ \beta_2)(\alpha_3 \circ \beta_3)\ c_{n-1}\ [\delta, \delta]\ c_{n-2}\ [\delta, \delta] \ldots [\delta, \delta]\ c_1\ [\delta, \delta]\ c$, da cui segue (28), poiché $[\delta, \delta]$ è una congruenza, quindi transitiva. □

Sia $\varepsilon = \alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\beta_3 + \alpha_1\beta_2\alpha_3 + \alpha_1\beta_2\beta_3 + \beta_1\alpha_2\alpha_3 + \beta_1\alpha_2\beta_3 + \beta_1\beta_2\alpha_3 + \beta_1\beta_2\beta_3$. In altre parole, ε è "δ calcolata come se fossimo in

un reticolo distributivo". Ricordiamo che, per convenzione, in questa sezione δ è $(\alpha_1 + \beta_1)(\alpha_2 + \beta_2)(\alpha_3 + \beta_3)$.

OSSERVAZIONE 9.3. Usando le proprietà (15) - (18) in 8.2 del commutatore in una varietà a congruenze modulari, si ottiene facilmente $[(\alpha_1 + \beta_1)(\alpha_2 + \beta_2), (\alpha_1 + \beta_1)(\alpha_2 + \beta_2)] \leq \alpha_1\alpha_2 + \alpha_1\beta_2 + \beta_1\alpha_2 + \beta_1\beta_2$.

Infatti, $[(\alpha_1 + \beta_1)(\alpha_2 + \beta_2), (\alpha_1 + \beta_1)(\alpha_2 + \beta_2)] \leq [\alpha_1 + \beta_1, \alpha_2 + \beta_2] = [\alpha_1+\beta_1, \alpha_2]+[\alpha_1+\beta_1, \beta_2] = [\alpha_2, \alpha_1+\beta_1]+[\beta_2, \alpha_1+\beta_1] = [\alpha_2, \alpha_1]+[\alpha_2, \beta_1]+[\beta_2, \alpha_1] + [\beta_2, \beta_1] \leq \alpha_1\alpha_2 + \beta_1\alpha_2 + \alpha_1\beta_2 + \beta_1\beta_2$.

Il lettore potrebbe essere tentato di supporre che valga anche $[\delta, \delta] \leq \varepsilon$, l'analogo "tridimensionale" della precedente uguaglianza. Se così fosse, usando il Lemma 9.1 e la Proposizione 9.2 avremmo una semplice dimostrazione dell'identità arguesiana in varietà a congruenze modulari.

Invece $[\delta, \delta] \leq \varepsilon$ può essere falsa addirittura negli anelli commutativi, come dimostrato da un revisore anonimo. Vedi la Proposizione 5.3 nel lavoro citato in [**An**]. Per inciso, non so se $[\delta, \delta] \leq \varepsilon$ possa essere falsa nel caso dei gruppi (ma la soluzione potrebbe non essere difficile).

L'inconveniente può essere superato abbastanza facilmente. Si verifica come sopra che $[\delta, [\delta, \delta]] \leq \varepsilon$, e H.-P. Gumm (tra le tante altre cose) ha dimostrato che se esiste un termine-differenza, allora esiste anche un termine differenza che "funziona" per $[[\delta, \delta], [\delta, \delta]]$, che è contenuta in $[\delta, [\delta, \delta]]$.

Presentiamo adesso qualche dettaglio.

PROPOSIZIONE 9.4. *Se d è un termine differenza per un'algebra $\mathbf{A}$, allora il termine d^2 definito da*

$$d^2(x, y, z) = d(d(x, y, z), d(y, y, z), z)$$

soddisfa a

$$x = d^2(x, y, y) \text{ e} \tag{29}$$

$$d^2(x, x, y)[[\alpha, \alpha], [\alpha, \alpha]]y, \text{ se } x, y \in A \text{ e } x \,\alpha\, y \tag{30}$$

La dimostrazione è lasciata per esercizio.

OSSERVAZIONE 9.5. La Proposizione 9.4 si può generalizzare al caso di un termine differenza debole. Se d è un termine differenza debole per $\mathbf{A}$, allora il termine d^2 definito da

$$d^2(x, y, z) = d(d(x, y, z), d(y, y, z), z)$$

soddisfa a $x[\alpha, \alpha]d^2(x, y, y)$ e $d^2(x, x, y)[[\alpha, \alpha], [\alpha, \alpha]]y$, se $x, y \in A$ e $x \,\alpha\, y$.

Per induzione, si può ottenere un termine che funziona (da entrambi i lati) relativamente a qualunque iterazione finita del commutatore. Questo fatto non verrà comunque usato qui.

TEOREMA 9.6. *Se un'algebra $\mathbf{A}$ appartiene ad una varietà a congruenze modulari, allora $\mathbf{Con}(\mathbf{A})$ è arguesiano.*

DIMOSTRAZIONE. Ripetendo la dimostrazione della Proposizione 9.2 usando il termine d^2 dato dalla Proposizione 9.4, otteniamo

$$\delta \subseteq (\alpha_1 \circ \beta_1)(\alpha_2 \circ \beta_2)(\alpha_3 \circ \beta_3) \circ [[\delta, \delta], [\delta, \delta]] \tag{31}$$

Per il Lemma 9.1, abbiamo

$$(\alpha_1 \circ \beta_1)(\alpha_2 \circ \beta_2)(\alpha_3 \circ \beta_3) \leq \alpha_1(\alpha_2 + \gamma_{12}(\gamma_{23} + \gamma_{13})) + \beta_1$$

Ragionando come nell'Osservazione 9.3 abbiamo $[[\delta, \delta], [\delta, \delta]] \leq [\delta, [\delta, \delta]] \leq \varepsilon$, dove ε è definito subito prima di 9.3. È facile vedere che $\varepsilon \leq \alpha_1(\alpha_2 + \gamma_{12}(\gamma_{23} + \gamma_{13})) + \beta_1$, quindi l'equazione (31) ci fornisce $\delta \leq \alpha_1(\alpha_2 + \gamma_{12}(\gamma_{23} + \gamma_{13})) + \beta_1$, che è proprio l'identità arguesiana. □

OSSERVAZIONE 9.7. Esiste una versione del Teorema 9.6 per algebre "singole".

Se $\mathbf{Con}(\mathbf{A})$ è modulare e $\mathbf{A}$ ha un termine-differenza, allora $\mathbf{Con}(\mathbf{A})$ è arguesiano. La dimostrazione è simile, ma è laborioso dimostrare $[\delta, [\delta, \delta]] \leq \alpha_1(\alpha_2 + \gamma_{12}(\gamma_{23} + \gamma_{13})) + \beta_1$.

Non si sa se l'ipotesi dell'esistenza di un termine-differenza nell'enunciato precedente può essere indebolita ad un termine differenza debole.

10. Algebre assolutamente libere

NB: questa sezione è facoltativa.

[...]

11. Appendice: altre osservazioni

NB: questa sezione è facoltativa.

OSSERVAZIONE 11.1. Per $n \geq 2$ si può pensare ad una n-upla ordinata come ad una funzione il cui dominio è un insieme $\mathbf{n}$ con n elementi, ad esempio[11] $\mathbf{n} = \{1, 2, \ldots, n\}$. Così, la n-upla ordinata $(a_1, a_2, \ldots, a_n)$ può essere pensata come la funzione $g : \mathbf{n} \to \{a_1, a_2, \ldots, a_n\}$ definita da $g(1) = a_1$, $g(2) = a_2$, $\ldots$, $g(n) = a_n$. Questa possibile definizione di n-upla ordinata soddisfa chiaramente alla proprietà fondamentale enunciata all'inizio della Sezione 1.1.[12]

[11] In alcune situazioni è conveniente utilizzare invece l'insieme $\mathbf{n} = \{0, 1, \ldots, n-1\}$. Nonostante le apparenze, questa *non* è pedanteria, e nemmeno un dettaglio insignificante, ma in questa sede la scelta specifica di un $\mathbf{n}$ con n elementi non avrà assolutamente alcuna rilevanza, e abbiamo effettuato la scelta in base a semplice comodità tipografica.

[12] Purché si identifichi una funzione col suo grafico.

È da notare anche che, usualmente, (il grafico di) una funzione viene considerato come un insieme di coppie ordinate, quindi, per evitare circolarità, la possibile definizione di n-upla ordinata che abbiano dato qui presume che sia già possibile dare una definizione di *coppia ordinata* in qualche altro modo.

Siccome immaginiamo già che c'è chi è curioso, una possibilità per introdurre la coppia ordinata facendo uso solo della nozione di insieme è di definire $(a, b) = \{\{a\}, \{a, b\}\}$. Una volta introdotte le coppie ordinate, le n-uple ordinate possono essere introdotte in vari modi, incluso il modo indicato in questa osservazione, avendo cura di non sovrapporre le due definizioni di coppia ordinata.

Adesso, se $n = 0$, $\mathbf{n}$ deve essere un insieme con zero elementi, cioè $\mathbf{n} = \emptyset$. Una operazione zero-aria su A, quindi, è una funzione da $A^{\mathbf{0}}$ in A, dove $A^{\mathbf{0}}$ è l'insieme di tutte le funzioni da $\emptyset$ ad A. Ma esiste solo una funzione da $\emptyset$ ad A, cioè la funzione "vuota" $g_\emptyset = \emptyset$, la funzione che non associa niente a niente. Quindi $A^{\mathbf{0}}$ è , o comunque può essere pensato, come $\{\emptyset\}$, quindi una 0-upla è una funzione in partenza da un insieme con un elemento, e quindi corrisponde a scegliere esattamente un elemento del codomionio, cioè una costante.

Osservazione 11.2. Per inciso, notiamo che la convenzione di considerare una n-upla ordinata come una funzione in partenza da un insieme con n elementi coincide con la notazione abituale usata per rappresentare le successioni.

Formalmente, una successione ad elementi in un insieme A è una funzione da $\mathbb{N}$ in A.

In questo senso - come del resto è intuitivamente ovvio - una n-upla ordinata può essere pensata come una successione (o sequenza) finita.

Osservazione 11.3. Se alcune formulazioni dell'Assioma di Scelta (vedi 1.52) corrispondono ad affermazioni apparentemente non problematiche, o addirittura che alcuni considererebbero intuitivamente vere, l'assioma di scelta ha anche conseguenze paradossali, come l'esistenza di sottoinsiemi di $\mathbb{R}$ non misurabili, o addirittura il *Paradosso di Banach-Tarski*, che afferma che ogni sfera (piena, cioè una palla) è scomponibile in un numero finito di parti che possono essere utilizzate (mediante movimenti rigidi e, ovviamente, senza usare duplicati) per costruire due sfere con lo stesso raggio della sfera di partenza. Vedi [**Mo**] per ulteriori informazioni sull'Assioma di Scelta e sulla sua storia. Vedi [**RR, HR**] per equivalenze e conseguenze dell'Assioma di Scelta.

Il lettore che desiderasse approfondire questo argomento o, più in generale, conoscere le basi della teoria degli insiemi, può inoltre consultare [**Je**]. Utile materiale in italiano può essere [**Pl**] o [**DN**].

Osservazione 11.4. Verso la fine dell'800 sono stati scoperti alcuni argomenti di natura paradossale che riguardano la teoria degli insiemi.

Il Teorema di Cantor afferma che la cardinalità dell'insieme delle parti $\mathcal{P}(A)$ di un insieme A è strettamente maggiore della cardinalità di A. Se ora A fosse l'insieme di tutti gli insiemi, siccome $\mathcal{P}(A)$ è costituito di insiemi, si ha $\mathcal{P}(A) \subseteq A$, quindi la cardinalità di $\mathcal{P}(A)$ è minore o uguale a quella di A, ma, per il Teorema di Cantor, la cardinalità di $\mathcal{P}(A)$ è strettamente maggiore della cardinalità di A, ottenendo una contraddizione. Questo ragionamento viene chiamato *Paradosso di Cantor* e, oggi (forse rivoltando un po' la frittata), viene interpretato come un teorema che dimostra la non esistenza di un "insieme di tutti gli insiemi".[13]

[13]Anche senza dover introdurre la nozione di cardinalità (sotto certi aspetti, essa stessa è problematica), il Teorema di Cantor dimostra che, per ogni insieme A, non esiste una funzione suriettiva da A verso $\mathcal{P}(A)$. Ma se A fosse l'insieme di tutti gli insiemi, allora $\mathcal{P}(A) \subseteq A$, quindi esisterebbe una funzione suriettiva da A

Un paradosso più noto (e ritenuto di natura più elementare, anche se noi non sottoscriviamo pienamente questa opinione) è quello di Russell. Se X fosse l'insieme di tutti gli insiemi che *non* appartengono a se stessi, allora, per la definizione stessa di X, abbiamo che $X \in X$ se e solo se $X \notin X$, patente contraddizione.

Ovviamente sono stati scritti numerosi libri sull'argomento; molti studiosi hanno proposto possibili soluzioni a questo tipo di paradossi, a volte presentando le loro soluzioni come assolutamente non problematiche ed evidentemente libere da paradossi (anche se, in alcuni casi, questa supposta evidenza si è rivelata fallace, e anche queste teorie si sono rivelate autocontradditorie). Un autorevole testo sull'argomento è [**FBL**], ma va notato che parte del materiale presente nella prima edizione [**FB**] è stato espunto dall'edizione successiva.

[... distinzione fra classi ed insiemi; classi proprie]

Osservazione 11.5. Se, come in 3.2 e 3.3, ad un tipo finito $(n_1, \dots n_m)$ associamo simboli $f_1, \dots, f_m$ che rappresentano corrispondenti operazioni, rispettivamente, n_1-arie, $\dots$, n_m-arie, e poniamo $F = \{f_1, \dots, f_m\}$, possiamo pensare ad un tipo come ad una coppia $\mathcal{F} = (F, \sigma)$, dove $\sigma(f_1) = n_1$, $\dots$, $\sigma(f_m) = n_m$. Cioè, F è un insieme di simboli che contengono i "nomi" delle operazioni delle algebre del tipo, e σ associa ad un simbolo l'arietà delle operazioni che quel simbolo dovrebbe rappresentare[14].

Osservazione 11.6. L'utilizzo di simboli per rappresentare operazioni è un modo conveniente per definire cosa sono i termini e le identità, come

---

a $\mathcal{P}(A)$ (basta definirla come l'identità su $\mathcal{P}(A) \subseteq A$ e definirla arbitrariamente su $A \setminus \mathcal{P}(A)$), ottenendo ancora una contraddizione.

Per inciso, osserviamo che, piuttosto che dimostrare che non esiste l'"insieme di tutti gli insiemi", il paradosso di Cantor dimostra (sotto un altro punto di vista) che non si può costruire l'insieme della parti dell'"insieme di tutti gli insiemi".

Sembra comunque che le argomentazioni originali di Cantor fossero leggermente diverse. Alcuni [**Fe**] indicano come Paradosso di Cantor il "paradosso del massimo cardinale", o "paradosso dell'aleph" riguardante l'(eventuale) insieme di tutte le cardinalità. Per il Teorema di Cantor, per ogni "numero cardinale" $\aleph$, esiste un numero cardinale $\aleph'$ strettamente maggiore di $\aleph$. Cantor allora si chiese: qual è la cardinalità $\aleph$ dell'insieme di tutti i cardinali? Cantor suppose che $\aleph$ sia il cardinale massimo, ma in questo modo si ottiene una contraddizione, poiché gli argomenti precedenti mostrano che esiste un cardinale ancora maggiore (sembrerebbe che in questo argomento sia necessario usare un'assunzione che poi verrà chiamata Assioma di Rimpiazzamento).

Secondo A. Kanamori [**Ka**], però, l'argomento di Cantor utilizzava invece il "massimo ordinale", utilizzava cioè argomenti simili a quello che oggi viene chiamato Paradosso di Burali-Forti. Indirizziamo il lettore che volesse approfondire l'argomento ai testi citati.

[14]Chi conoscesse i rudimenti della teoria dei modelli, riconoscerebbe in questa nuova definizione di tipo quelli che in teoria dei modelli vengono definiti *linguaggi* (ma nel nostro caso non abbiamo simboli di relazione).

abbiamo visto nella Sezione 3. Notiamo comunque che considerare (come sopra) un tipo come una coppia (F, σ) rende immediata una definizione della nozione di algebra con un numero infinito di operazioni. In questo senso, un'algebra di tipo (F, σ) è un'insieme A non vuoto insieme ad una funzione che ad ogni $f \in F$ associa un'operazione $\sigma(f)$-aria $f^{\mathbf{A}}$ su A. In una definizione come questa, la finitezza di F non è affatto richiesta, e non giocherebbe alcun ruolo particolare.

Osserviamo comunque che i metodi indicati non sono gli unici possibili per introdurre le nozioni di tipo infinito e di algebra con un numero infinito di operazioni.

12. Appendice: altre condizioni di Mal'cev

Vi sono molte equivalenze legate alle condizioni di Mal'cev, alcune delle quali a volte non enunciate esplicitamente. Presentiamo un esempio nel caso semplice di un termine italicum.

Un *italicum* (o *termine-maggioranza*, in inglese *majority term*) in un'algebra $\mathbf{A}$ è un termine ternario t tale che $t^{\mathbf{A}}(a, a, b) = t^{\mathbf{A}}(a, b, a) = t^{\mathbf{A}}(b, a, a) = a$, per ogni $a, b \in A$. Una varietà $\mathcal{V}$ ha un italicum se c'è un termine che è un italicum per ogni algebra di $\mathcal{V}$.

Esempio 12.1. Un italicum per la varietà di tutti i reticoli è, ad esempio, $t(x, y, z) = (x \vee y) \wedge (x \vee z) \wedge (y \vee z)$.

Se A è un insieme qualunque, la funzione

$$f(a, b, c) = \begin{cases} a & \text{se } a = b, \\ c & \text{altrimenti} \end{cases}$$

da origine ad un italicum.

In certe formule spesso ometteremo il simbolo di intersezione: se θ e ψ sono due relazioni binarie, $\theta\psi$ starà per $\theta \cap \psi$. Ricordiamo che a volte useremo $+$ al posto di $\vee$.

Teorema 12.2. *Per ogni varietà $\mathcal{V}$, le seguenti condizioni sono equivalenti:*

(1) $\mathcal{V}$ ha un italicum.
(2) Ogni algebra in $\mathcal{V}$ ha un italicum.
(3) L'algebra libera generata da 3 elementi in $\mathcal{V}$ ha un italicum.
(4) Per ogni algebra $\mathbf{A}$ in $\mathcal{V}$, e per ogni α, β, γ congruenze di $\mathbf{A}$, vale

$$\gamma(\alpha \circ \beta) \subseteq \gamma\alpha \circ \gamma\beta \tag{32}$$

(5) L'inclusione (32) precedente vale per tutte le congruenze dell'algebra libera generata da 3 elementi in $\mathcal{V}$.

(6) *Se* $\mathbf{F}$ *è l'algebra libera in* $\mathcal{V}$ *generata da* x, y, z *e* α, β *e* γ *sono, rispettivamente, le congruenze in* $\mathbf{F}$ *generate dalle coppie* (x, y), (y, z) *e* (x, z), *allora* $x\ \gamma\alpha \circ \gamma\beta\ z$.

(7) *Per ogni* $n \in \mathbb{N}$, *per ogni algebra* $\mathbf{A}$ *in* $\mathcal{V}$ *(equivalentemente, per l'algebra libera generata da* 3 *elementi in* $\mathcal{V}$*) e per ogni* α, β, γ *congruenze dell'algebra, vale*

$$\gamma(\alpha \circ \beta \circ \alpha \circ \beta \dots) \subseteq \gamma\alpha \circ \gamma\beta \circ \gamma\alpha \circ \gamma\beta \dots, \tag{33}$$

dove il simbolo $\circ$ *compare* esattamente $n+1$ *volte sia a destra che a sinistra del segno di inclusione.*

Come conseguenza, ogni varietà con un italicum è a congruenze distributive; in particolare, il reticolo delle congruenze di ogni reticolo è distributivo.

Dimostrazione. Le implicazioni (1) $\Rightarrow$ (2) $\Rightarrow$ (3), (4) $\Rightarrow$ (5), (7) $\Rightarrow$ (4) e (7) $\Rightarrow$ (5) sono banali (NB: a priori, (2) e (1) non sono equivalenti, perché (1) richiede un termine che "funzioni" per ogni algebra, mentre i termini forniti da (2), in linea di principio, potrebbero variare da algebra ad algebra).

Dimostriamo adesso che

(*) *in ogni algebra che ha un italicum vale* (32)

Infatti, se $(a, c) \in \gamma(\alpha \circ \beta)$, allora $a\ \gamma\ c$ ed esiste b tale che $a\ \alpha\ b\ \beta\ c$.

Calcoliamo adesso $a = t(a, a, c)\ \alpha\ t(a, b, c)$, $a = t(a, b, a)\ \gamma\ t(a, b, c)$, $t(a, b, c)\beta t(a, c, c) = c$ e $t(a, b, c)\gamma t(c, b, c) = c$.

In conclusione, $a\ \gamma\alpha\ t(a, b, c)\ \gamma\beta\ c$, quindi $(a, c) \in \gamma\alpha \circ \gamma\beta \subseteq \gamma\alpha + \gamma\beta$ e (*) è dimostrato.

Da (*) seguono (2) $\Rightarrow$ (4) e (3) $\Rightarrow$ (5).

(5) $\Rightarrow$ (6) Sotto le ipotesi di (6), abbiamo $x\ \gamma\ z$ e $x\ \alpha\ y\ \beta\ z$, cioè $x\ \alpha \circ \beta\ z$, quindi $(x, z) \in \gamma(\alpha \circ \beta)$, ma allora da (5) segue $(x, z) \in \gamma\alpha \circ \gamma\beta$.

(6) $\Rightarrow$ (1) si dimostra in maniera simile al teorema di Mal'cev. Infatti, se $x\ \gamma\alpha \circ \gamma\beta\ z$, allora esiste $w \in \mathbf{F}$ tale che $x\ \gamma\alpha\ w\ \gamma\beta\ z$. Ma se $w \in \mathbf{F}$, allora, siccome $\mathbf{F}$ è generata da x, y, z, per la Proposizione 3.16 $w = t^{\mathbf{F}}(x, y, z)$, per qualche termine ternario t.

Siccome $x\ \alpha\ y$, allora $x\ \alpha\ t^{\mathbf{F}}(x, y, z)\ \alpha\ t^{\mathbf{F}}(x, x, z)$. Ma questo implica che l'uguaglianza $a = t^{\mathbf{A}}(a, a, c)$ vale in qualunque algebra di $\mathcal{V}$. Infatti, siccome $\mathbf{F}$ è libera in $\mathcal{V}$, esiste un morfismo $\varphi : \mathbf{F} \to \mathbf{A}$ tale che $\varphi(x) = a$, $\varphi(y) = a$ e $\varphi(z) = c$. Quindi $KerEq(\varphi) \supseteq \alpha$, che è la congruenza generata da (x, y). Ma siccome abbiamo visto che $x\ \alpha\ t^{\mathbf{F}}(x, x, z)$, allora $(x, t^{\mathbf{F}}(x, x, z)) \in KerEq(\varphi)$, quindi $\varphi(x) = \varphi(t^{\mathbf{F}}(x, x, z))$, da cui segue $a = \varphi(x) = \varphi(t^{\mathbf{F}}(x, x, z)) = t^{\mathbf{A}}(\varphi(x), \varphi(x), \varphi(z)) = t^{\mathbf{A}}(a, a, c)$,

Che l'uguaglianza $a = t^{\mathbf{A}}(a, a, c)$ vale in qualunque algebra di $\mathcal{V}$ si può dimostrare anche nel seguente modo. Prima si controlla che $\alpha = \{(t^{\mathbf{F}}(x, y, z), s^{\mathbf{F}}(x, y, z)) \mid t^{\mathbf{F}}(x, x, z) = s^{\mathbf{F}}(x, x, z)\}$ (usando 3.13), quindi da $x\ \alpha\ t^{\mathbf{F}}(x, x, z)$ si ottiene $x = t^{\mathbf{F}}(x, x, z)$, e quindi $a = t^{\mathbf{A}}(a, a, c)$ vale in qualunque algebra di $\mathcal{V}$ per il Teorema 3.13.

Le identità $a = t^{\mathbf{A}}(a, b, a)$ e $c = t^{\mathbf{A}}(a, c, c)$ si dimostrano esattamente allo stesso modo.

La dimostrazione che (1) implica (7) è simile alla dimostrazione di (*), ma più lunga. La dimostrazione è sostanzialmente quella del Teorema 2.21 in [**Be**]. Anche se il Teorema 2.21 in [**Be**] parla di reticoli, la dimostrazione usa esclusivamente un italicum.

Per finire, l'ultimo enunciato si dimostra nel seguente modo. Bisogna dimostrare che $\gamma(\alpha+\beta) \leq \gamma\alpha+\gamma\beta$ vale per tutte le congruenze in ogni algebra (l'altra inclusione è banale).

Se $(a, c) \in \gamma(\alpha + \beta)$, allora $(a, c) \in \alpha + \beta = \bigcup_{i\in\mathbb{N}} \underbrace{\alpha \circ \beta \circ \alpha \circ \dots}_{i+1 \text{ segni di } \circ}$, per la Proposizione 1.60, quindi esiste un certo $i \in \mathbb{N}$ tale che $(a, c) \in \alpha \circ \beta \circ \alpha \circ \dots$ con $i + 1$ segni di $\circ$. Ma allora $(a, c) \in \gamma(\alpha \circ \beta \circ \alpha \circ \dots)$ e per (7) abbiamo $(a, c) \in \gamma\alpha \circ \gamma\beta \circ \gamma\alpha \circ \cdots \subseteq \gamma\alpha + \gamma\beta$. □

Osservazione 12.3. NB: La condizione (32) in 12.2 è *molto* diversa dalla condizione apparentemente simile

$$\gamma(\alpha \circ \beta) \subseteq \gamma\beta \circ \gamma\alpha \tag{34}$$

(nel lato sinistro di (34) l'ordine di α e β è scambiato!)

Infatti la condizione (32) implica la distributività (per congruenze), ed è strettamente più forte della distributività, ma non implica la permutabilità. Ad esempio, (32) vale per i reticoli, ma i reticoli non sono a congruenze permutabili, vedi l'Osservazione 5.1.

Invece una varietà soddisfa ad (34) se e solo se è sia distributiva che permutabile. Tali varietà si dicono *aritmetiche*.

Dimostriamo l'equivalenza. Prendendo $\gamma = 1$, otteniamo da (34) la permutabilità. La distributività seque dal Teorema 12.4 sotto. Viceversa, se $\mathcal{V}$ è sia permutabile che distributiva, abbiamo $\gamma(\alpha \circ \beta) = \gamma(\alpha + \beta) = \gamma\alpha + \gamma\beta = \gamma\beta + \gamma\alpha = \gamma\beta \circ \gamma\alpha$, dove abbiamo utilizzato la distributività nell'uguaglianza al centro, e la permutabilità in altre due uguaglianze.

Il lettore interessato a maggiori dettagli sulle varietà aritmetiche può consultare la Sezione 4.7 di [**Be**].

Teorema 12.4. *Caratterizzazione delle varietà a congruenze distributive. Vedi* [**Be**, Theorem 4.66]. *(fa parte del programma con dimostrazione)*

13. Rapida guida alla letteratura

Per chi volesse approfondire lo studio dell'algebra universale, commentiamo brevemente (senza assolutamente alcuna pretesa di completezza!) il contenuto di alcuni manuali. [...]

Per quel che riguarda i reticoli, riferimenti classici sono [**Bi, CD, Gr2**]; volumi più recenti specificatamente dedicati ai reticoli sono [**DP, GHKLMS, Gr3, Na**]. Ai reticoli liberi e alle varietà di reticoli sono dedicati [**FJN, JR**]. Naturalmente, un'introduzione ai reticoli è presente in ciascuno dei libri sull'algebra universale citati. Un libro dedicato anche ai reticoli, ma soprattutto dal punto di vista della teoria dei semireticoli è [....].

Una presentazione - originalissima come sempre, quando si tratta dei lavori di G. C. Rota - di alcuni argomenti di algebra universale, con particolare attenzione ai reticoli, si può trovare in [**Ro**].

Di seguito l'elenco di tutti i lavori citati in queste note (l'elenco deve comunque essere ampliato). Naturalmente spesso sono citati compendi o rassegne al posto dei lavori originali. Facciamo riferimento ai lavori citati per il lettore che volesse conoscere una storia dettagliata degli argomenti e, in particolare, i singoli scopritori di ciascun risultato.

Bibliografia

[An] Revisore anonimo dell'articolo *Congruence modularity implies the Arguesian law for single algebras with a difference term*, J. Algebra **219** (1999), 658–681.

[Be] Clifford Bergman, *Universal Algebra: Fundamentals and Selected Topics*, CRC Press, 2012.

[Bi] G. Birkhoff, *Lattice Theory*, Revised Edition, New York City, 1948.

[BS] S. Burris e H. P. Sankappanavar, *A Course in Universal Algebra*, New York (1981), versione aggiornata scaricabile gratuitamente online https://www.math.uwaterloo.ca/~snburris/htdocs/ualg.html ef

[CD] P. Crawley e R. P. Dilworth, *Algebraic theory of lattices*, Englewood Cliffs, N.J. (1973).

[DP] B. A. Davey e H. A. Priestley, *Introduction to lattices and Order*, Second Edition, Cambridge (2002).

[DN] M. Di Nasso, *Dispense* del corso di *Elementi di teoria degli insiemi 2013-2014*, http://www.dm.unipi.it/cluster-pages/dinasso/eti-2014.html (consultato il 29 ottobre 2016).

[Fe] J. Ferreirós, *The Early Development of Set Theory*, The Stanford Encyclopedia of Philosophy (Fall 2016 Edition), Edward N. Zalta (ed.), URL = http://plato.stanford.edu/archives/fall2016/entries/settheory-early/

[FB] A. A. Fraenkel e Y. Bar-Hillel, *Foundations of set theory*, Amsterdam, 1958.

[FBL] A. A. Fraenkel, Y. Bar-Hillel e A. Levy, *Foundations of set theory. Second revised edition. With the collaboration of Dirk van Dalen* Amsterdam-London, 1973.

[FJN] R. Freese, J. Ježek e J. B. Nation, *Free lattices*, Providence, Rhode Island, 1995.

[FMK] R. Freese e R. McKenzie, *Commutatory Theory for Congruence Modular Varieties*, Cambridge, 1987; seconda edizione in preparazione, versione preliminare disponibile in rete http://math.hawaii.edu/~ralph/Commutator/

[GHKLMS] G. Gierz, K. H. Hofmann, K. Keimel, J. D. Lawson, M. Mislove e D. S. Scott, *Continuous lattices and domains*, Cambridge, 2003.

[Gr1] G Grätzer, *Universal Algebra, Second Expanded Edition*, New York, Berlin, Heidelberg (1979).

[Gr2] G Grätzer, *General lattice theory. Second edition. New appendices by the author with B. A. Davey, R. Freese, B. Ganter, M. Greferath, P. Jipsen, H. A. Priestley, H. Rose, E. T. Schmidt, S. E. Schmidt, F. Wehrung and R. Wille*, Basilea 1998.

[Gr3] G Grätzer, *Lattice theory: foundation*, Basilea 2011.

[Gu] H.-P. Gumm, *Geometrical methods in Congruence Modular Algebras*, Providence, 1983.

[HR] P. Howard e J. E. Rubin, *Consequences of the axiom of choice*, Providence, RI, 1998.

[Je] T. Jech, *Set theory. The third millennium edition, revised and expanded*, Berlin, 2003.

[JR] P. Jipsen e H. Rose, *Varieties of Lattices*, Berlin, 1992.

[Ka] A. Kanamori, *Set theory from Cantor to Cohen*, in *Sets and extensions in the twentieth century* 1–71, Handb. Hist. Log. **6**, Amsterdam, 2012.

[KK] K. A. Kearnes e E. W. Kiss, *The shape of congruence lattices*, Mem. Amer. Math. Soc. **222** (2013).

[KS] K. A. Kearnes e Á. Szendrei, *The relationship between two commutators*, Internat. J. Algebra Comput. **8** (1998), 497–531.

[MB] S. Mac Lane e G. Birkhoff, *Algebra*, prima edizione 1967, terza edizione 1988 [... esiste una traduzione in italiano].

[Mo] G. H. Moore, *Zermelo's axiom of choice. Its origins, development, and influence*, New York, 1982.

[Na] J. B. Nation, *Notes on Lattice theory*, http://www.math.hawaii.edu/~jb/books.html

[Pa] G. Pareschi, *Reticoli*, http://www.mat.uniroma2.it/~gealbis/EALreticoli.pdf (consultato il 10 ottobre 2016).

[Pi] D. Pickering, *On minimal non-Arguesian lattice varieties*, Ph.D. Thesis, U. of Hawaii (1984), citato in [**JR**].

[Pl] P. Plazzi, *Teorie degli insiemi Numeri ordinali e cardinali*, http://campus.unibo.it/74334/1/Insiemi.pdf (consultato il 29 ottobre 2016).

[Ro] G-C. Rota, *The many lives of lattice theory*, Notices Amer. Math. Soc. 44 (1997), 1440–1445.

[RR] H. Rubin e J. E. Rubin, *Equivalents of the axiom of choice*, Amsterdam-Londra, 1963; seconda edizione, 1970.

[Ta] W. Taylor, *Some applications of the term condition*, Algebra Universalis **14** (1982), 11–24.

[Trec] ... http://www.treccani.it/enciclopedia/reticolo (consultato il 10 ottobre 2016).

[Wi] R. Willard, M_n *as a* $0,1$*-sublattice of* $\operatorname{Con} A$ *does not force the term condition*, Proc. Amer. Math. Soc. **104** (1988), 349–356.

Dipartimento di Matematica
Viale della Ricerca Scientifica
II Universalità di Roma (Tor Vergata)
I-00133 ROME ITALY
http://www.mat.uniroma2.it/~lipparin

Indice analitico