I sedici connettivi binari

		(1) congiunzione AND ($\wedge$)	(2) disgiunzione (inclusiva: vel) OR ($\vee$)	(3) implicazione (condizionale) IF–THEN($\Rightarrow$)	(4) implicazione opposta ($\Leftarrow$)	(5) equivalenza (bicondizionale) ($\Leftrightarrow$)	(6) prima proiezione	(7) seconda proiezione	(8) costante *FALSO*
p	q	$(p \wedge q)$	$(p \vee q)$	$(p \Rightarrow q)$	$(p \Leftarrow q)$	$(p \Leftrightarrow q)$	(p)	(q)	(F)
F	F	F	F	V	V	V	F	F	F
F	V	F	V	V	F	F	F	V	F
V	F	F	V	F	V	F	V	F	F
V	V	V	V	V	V	V	V	V	F

		($1'$) operazione di Sheffer NAND ($\mid$)	($2'$) operazione di Pierce NOR ($\downarrow$)	($3'$) inibizione della seconda	($4'$) inibizione della prima	($5'$) disgiunzione esclusiva AUT ($\dot{\vee}$)	($6'$) negazione della prima	($7'$) negazione della seconda	($8'$) costante *VERO*
p	q	$(p \mid q)$	$(p \downarrow q)$	$(\neg(p \Rightarrow q))$	$(\neg(p \Leftarrow q))$	$(p \dot{\vee} q)$	$(\neg p)$	$(\neg q)$	(V)
F	F	V	V	F	F	F	V	V	V
F	V	V	F	F	V	V	V	F	V
V	F	V	F	V	F	V	F	V	V
V	V	F	F	F	F	F	F	F	V

Si nota che ciascuna coppia di connettivi (i), (i') costruisce due proposizioni ognuna equivalente alla negazione dell'altra.

Interdipendenza dei connettivi binari

Le seguenti tautologie:

$$(p \vee q) \iff \neg(\neg p \wedge \neg q) \qquad (p \Rightarrow q) \iff (\neg p \vee q) \qquad (p \Leftrightarrow q) \iff \big((p \Rightarrow q) \wedge (p \Leftarrow q)\big)$$

mostrano come sia possibile definire ciascuno dei connettivi binari in termini dei soli "$\wedge$" e "$\neg$". Inoltre, dalle tautologie

$$(\neg p) \iff (p \mid p) \qquad \text{e} \qquad (p \wedge q) \iff \neg(p \mid q)$$

segue che è addirittura sufficiente il solo "$\mid$" (lo *stroke* di Sheffer).
In modo analogo, dalla tautologia $(p \wedge q) \iff \neg(\neg p \vee \neg q)$ segue che simile discorso si può fare per "$\vee$" e "$\neg$" (in luogo di"$\wedge$" e "$\neg$") e quindi per il connettivo "$\downarrow$" di Pierce (in luogo di "$\mid$") .

Alcuni esempi di tautologie

1.1 $\neg(\neg p) \iff p$ (legge della doppia negazione)

1.2 $p \vee (\neg p)$ (legge del terzo escluso)

1.3 $\neg\big(p \wedge (\neg p)\big)$ (legge di non contraddizione)

2.1 $\big(p \wedge (p \Rightarrow q)\big) \Longrightarrow q$ (legge dell'inferenza)

2.2 $\big(p \Rightarrow q\big) \iff \big((\neg q) \Rightarrow (\neg p)\big)$ (legge di contrapposizione)

2.3 $(p \Rightarrow q) \Longrightarrow \big((p \Rightarrow \neg q) \Rightarrow \neg p\big)$ (riduzione all'assurdo)

2.4 $(p \Rightarrow \neg p) \Rightarrow \neg p$ (riduzione all'assurdo debole)

2.5 $\big(p \wedge (\neg p)\big) \Rightarrow q$ (legge di Lewis o "*ex falso quodlibet*")

2.6 $\big((p \Rightarrow q) \wedge (q \Rightarrow r)\big) \Longrightarrow (p \Rightarrow r)$ (transitività dell'implicazione o legge del sillogismo)

2.7 $\big(p \Rightarrow (q \Rightarrow r)\big) \iff \big((p \Rightarrow q) \Rightarrow (p \Rightarrow r)\big)$ (distributività dell'implicazione)

2.8 $\big((p \Rightarrow q) \Rightarrow p\big) \Longrightarrow p$ (legge di Peirce)

3.1 $p \Longrightarrow p$ (legge dell'identità)

3.2 $p \Longrightarrow (q \Rightarrow p)$ (legge dell'affermazione del conseguente)

3.3 $(\neg p) \Longrightarrow (p \Rightarrow q)$ (legge della negazione dell'antecedente)

3.4 $\big(p \Rightarrow (q \Rightarrow r)\big) \iff \big((p \wedge q) \Rightarrow r\big)$ (esportazione-importazione degli antecedenti)

3.5 $\big(p \Rightarrow (q \Rightarrow r)\big) \iff \big(q \Rightarrow (p \Rightarrow r)\big)$ (scambio degli antecedenti)

4 $\big(p \Rightarrow q\big) \iff \big((\neg p) \vee q\big)$ (relazione fra implicazione e disgiunzione)

5.1
$$(p \wedge p) \iff p$$
$$(p \vee p) \iff p$$
(leggi di idempotenza)

5.2
$$(p \wedge q) \iff (q \wedge p)$$
$$(p \vee q) \iff (q \vee p)$$
(leggi commutative)

5.3
$$\big((p \wedge q) \wedge r\big) \iff \big(p \wedge (q \wedge r)\big)$$
$$\big((p \vee q) \vee r\big) \iff \big(p \vee (q \vee r)\big)$$
(leggi associative)

5.4
$$\big(p \wedge (q \vee r)\big) \iff \big((p \wedge q) \vee (p \wedge r)\big)$$
$$\big(p \vee (q \wedge r)\big) \iff \big((p \vee q) \wedge (p \vee r)\big)$$
(leggi distributive)

5.5
$$\big(\neg(p \wedge q)\big) \iff \big((\neg p) \vee (\neg q)\big)$$
$$\big(\neg(p \vee q)\big) \iff \big((\neg p) \wedge (\neg q)\big)$$
(leggi di De Morgan)

Tautologie e identità insiemistiche

Le formule nella metà sinistra della pagina sono tautologie (le lettere minuscole a, b, c indicano variabili proposizionali); quelle nella metà destra sono le corrispondenti formule della teoria degli insiemi, che valgono qualsiasi siano le collezioni A, B, C e la collezione S *che le comprenda tutte.*

Proprietà associativa:

$$(a \wedge b) \wedge c \iff a \wedge (b \wedge c) \qquad (A \cap B) \cap C = A \cap (B \cap C)$$
$$(a \vee b) \vee c \iff a \vee (b \vee c) \qquad (A \cup B) \cup C = A \cup (B \cup C)$$

Proprietà commutativa:

$$a \wedge b \iff b \wedge a \qquad A \cap B = B \cap A$$
$$a \vee b \iff b \vee a \qquad A \cup B = B \cup A$$
$$(a \iff b) \iff (b \iff a)$$

Proprietà iterativa:

$$(a \wedge a) \iff a \qquad A \cap A = A$$
$$(a \vee a) \iff a \qquad A \cup A = A$$

Proprietà distributiva:

$$\big(a \wedge (b \vee c)\big) \iff \big((a \wedge b) \vee (a \wedge c)\big) \qquad A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$
$$\big(a \vee (b \wedge c)\big) \iff \big((a \vee b) \wedge (a \vee c)\big) \qquad A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$
$$\big(a \Rightarrow (b \vee c)\big) \iff \big((a \Rightarrow b) \vee (a \Rightarrow c)\big)$$
$$\big(a \Rightarrow (b \wedge c)\big) \iff \big((a \Rightarrow b) \wedge (a \Rightarrow c)\big) \qquad A \subseteq (B \cap C) \iff (A \subseteq B \wedge A \subseteq C)$$

Disgiunzione esclusiva e differenza simmetrica:

$$\big((a \vee b) \wedge \neg(a \wedge b)\big) \iff \big((a \wedge \neg b) \vee (b \wedge \neg a)\big) \qquad (A \cup B) - (A \cap B) = (A - B) \cup (B - A)$$

Doppia negazione:

$$\neg(\neg a) \iff a \qquad S - (S - A) = A$$

Leggi di De Morgan:

$$\neg(a \wedge b) \iff \big((\neg a) \vee (\neg b)\big) \qquad S - (A \cap B) = (S - A) \cup (S - B)$$
$$\neg(a \vee b) \iff \big((\neg a) \wedge (\neg b)\big) \qquad S - (A \cup B) = (S - A) \cap (S - B) \qquad (*)$$

Terzo escluso e non contraddizione:

$$a \vee (\neg a) \qquad S = A \cup (S - A)$$
$$\neg\big(a \wedge (\neg a)\big) \qquad \varnothing = A \cap (S - A)$$

Sull'implicazione:

$$(a \iff b) \iff \big((a \Rightarrow b) \wedge (b \Rightarrow a)\big) \qquad A = B \iff (A \subseteq B \wedge B \subseteq A)$$
$$(a \Rightarrow b) \iff \big((\neg a) \vee b\big) \qquad A \subseteq B \iff S = (S - A) \cup B$$
[contrapposizione] $$(a \Rightarrow b) \iff \big((\neg b) \Rightarrow (\neg a)\big) \qquad A \subseteq B \iff S - B \subseteq S - A$$
[transitività] $$\big((a \Rightarrow b) \wedge (b \Rightarrow c)\big) \Rightarrow (a \Rightarrow c) \qquad (A \subseteq B \wedge B \subseteq C) \Rightarrow A \subseteq C$$
$$\big(a \wedge (a \Rightarrow b)\big) \Rightarrow b$$
$$\neg a \Rightarrow (a \Rightarrow b)$$
$$b \Rightarrow (a \Rightarrow b)$$
$$\neg(a \Rightarrow b) \iff \big(a \wedge (\neg b)\big)$$

(*) le leggi di De Morgan, nella loro versione insiemistica, valgono con identica formulazione anche nel caso in cui A e B non siano parti di S

versione 1.2.4.1 — 5 ottobre 2022.

Logica rudimentale

GIOVANNI CUTOLO

1. Premesse

Lo scopo di queste note è quello di dare alcune indicazioni sull'uso corretto dei simboli logici utili, o piuttosto necessari, nello studio della matematica. Una vera e propria (e più rigorosa) introduzione alla logica va al di là degli obiettivi del corso di Algebra ed è rimandata a corsi degli anni successivi e della laurea magistrale.

Molto informalmente, ci limitiamo qui a dire che ogni teoria matematica è espressa in quello che si chiama un *linguaggio*, che è costituito (1) da un alfabeto di simboli (semplicemente, dei caratteri tipografici), che possono essere messi insieme per costituire parole (stringhe di caratteri) e (2) da regole *sintattiche* che permettano, tra l'altro, di distinguere tra stringhe "correttamente composte", che si chiamano *formule* e stringhe che non sono correttamente composte. L'aggettivo 'sintattiche' indica che le regole riguardano solo le modalità di manipolazione formale dei simboli e non fanno alcun riferimento a ciò che questi simboli intendono rappresentare.

Spero che un esempio possa aiutare a chiarire la nozione di formula. Il linguaggio di una teoria che voglia descrivere l'usuale aritmetica dei numeri interi potrebbe contenere dei simboli per indicare variabili (ad esempio, "x", "y", "z", ...), alcuni simboli che indichino costanti (come "0" e "1"), operazioni (ad esempio, "$+$", "$\cdot$", "$-$"), relazioni (come "$<$", ma anche, su un piano diverso, "$=$"). Le regole sintattiche saranno probabilmente scritte in modo che stringhe come "$x+1=y$" oppure "$x\cdot y<1+z$" siano formule (*ben formate*, come anche si usa dire), mentre "$x<$", "$x==\cdot y$" oppure "$x+y$" non lo siano.[1]

È utile ribadire che la sintassi prescinde completamente dall'interpretazione dei simboli utilizzati nel linguaggio, e va tenuta ben separata da questa interpretazione. Ad esempio, non è affatto detto che i simboli che appaiono nel linguaggio dell'aritmetica appena richiamato debbano davvero essere interpretati come i nostri abituali numeri interi, che "$+$" debba indicare la consueta addizione, che le costanti "0" e "1" rappresentino necessariamente i familiari numeri zero ed uno, e così via. La parte della logica che si occupa di queste "interpretazioni" si chiama semantica e, in una trattazione rigorosa, va tenuta sempre ben distinta dalla sintassi.

[1] Osserviamo di passaggio che le regole sintattiche di un linguaggio hanno anche lo scopo di distinguere, tra le possibili stringhe, i cosiddetti *termini*, che così come i simboli di variabile e di costante intendono rappresentare gli oggetti "di cui parla" la teoria; nel nostro esempio i numeri interi. Delle tre stringhe che non sono formule appena mostrate, le prime due non sono termini, l'ultima ("$x+y$") invece lo è.

Una delle nozioni semantiche fondamentali , che siamo abituati a dare per scontata, è quella di verità o falsità di una affermazione. Ad esempio, facendo ancora riferimento all'aritmetica, con le consuete interpretazioni dei simboli che qui appaiono, siamo abituati a considerare vera la formula "$0 < 1$" e falsa la formula "$0 + 0 = 1$". Abbiamo qualche perplessità, invece, a proposito di "$x > 1 + 1$" (dove x è una variabile); diremmo che il valore di verità (cioè se essa è vera o falsa) di questa formula *dipende* (qualsiasi cosa ciò significhi) da x; quindi questa formula non ha un valore di verità nel senso più intuitivo.

Esiste una classe di formule alle quali, in modo piuttosto ragionevole, è sempre possibile in linea di principio, attribuire un valore di verità. Queste sono le cosiddette *formule chiuse*, che vengono anche chiamate *proposizioni*,[2] o sentenze (con una discutibile traduzione dell'inglese *sentences*).

Daremo solo più avanti una definizione di formula chiusa (e sarà comunque una definizione piuttosto approssimativa; la definizione precisa di formula chiusa richiede tecnicismi di cui in queste note è bene fare a meno). Per ora ci accontentiamo di sapere che sono chiuse tutte le formule ben formate in cui non appaiano variabili (ma, attenzione!, come vedremo esistono formule chiuse contenenti variabili). Delle tre formule esibite poco sopra, sono chiuse le prime due ("$0 < 1$" e "$0+0 = 1$", che non contengono variabili) ma non la terza ("$x > 1 + 1$").

È interessante sapere che la nozione di formula chiusa è sintattica, non semantica; ad essere rigorosi avremmo dovuto introdurre questa nozione prima di quelle semantiche di interpretazione e di verità.

2. Connettivi proposizionali

Ogni linguaggio contiene dei simboli, i cosiddetti simboli logici, che permettono di costruire formule a partire da formule più semplici. Tra i simboli logici appaiono di regola (alcuni dei) *connettivi proposizionali*, che presenteremo in questa sezione. Il nostro punto di vista sarà essenzialmente semantico: descriveremo i connettivi proposizionali guardando a come essi influenzano i valori di verità delle proposizioni in cui appaiono. È appena il caso di ripetere che ci stiamo discostando da quanto sarebbe richiesto da una trattazione rigorosa.

Negazione. Il connettivo più semplice da descrivere è quello di negazione: $\neg$, che si indica anche con NOT o talvolta con $\sim$ e che possiamo semplicemente leggere come "non". Se p è una formula allora $\neg p$ (oppure $\neg(p)$; anche le parentesi, usate come di consueto per suggerire come vadano raggruppati i simboli, sono spesso comprese nell'alfabeto di un linguaggio) è anch'essa una formula. Se p è una proposizione vera, allora $\neg p$ sarà una proposizione falsa; se p è falsa, allora $\neg p$ è vera. Detto in modo più sintetico, il connettivo di negazione ha come argomento una sola formula (questo fatto si esprime dicendo che la negazione è un connettivo *unario*) ed inverte il valore di verità del suo argomento.[3]

Congiunzione. Il connettivo di congiunzione si indica con $\wedge$ (oppure con AND) ed è, come tutti quelli che definiamo di seguito, un connettivo *binario*, vale a dire: richiede due formule come argomenti. Se p e q sono proposizioni, $p \wedge q$ è una proposizione che è vera quando sono vere sia p che q, falsa altrimenti. Dunque, $\wedge$ corrisponde alla congiunzione "e" del linguaggio ordinario, e possiamo leggere $p \wedge q$ come "p e q".

Tavole di verità. La semantica dei connettivi appena introdotti è sintetizzata, in modo molto efficace, da *tavole* (o *tabelle*) *di verità*:

p	$\neg p$
V	F
F	V

negazione

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

congiunzione

Vediamo di cosa si tratta. Ciascuna delle due tavole è divisa in due parti. La parte destra consiste di una colonna, la cui intestazione è una formula ($\neg p$ per la prima tavola, $p \wedge q$ per la seconda); in questa

[2] avvertenza: alcuni autori usano il termine 'proposizione' come sinonimo di 'formula', non necessariamente chiusa.

[3] ad essere più precisi, dovremmo aggiungere la condizione che il valore di verità dell'argomento sia definito.

colonna andrà letto il valore di verità della formula. Nelle formule che stiamo esaminando appaiono delle variabili (p e q), che rappresentano proposizioni. Nella parte sinistra di ciascuna delle tavole abbiamo una colonna per ogni variabile che appare nella formula considerata (quindi solo una colonna, intestata da p, per la prima tavola; due colonne, intestate da p e q, per la seconda). Guardiamo alla prima tavola, quella della negazione. I valori di verità possibili per la variabile p sono ovviamente due: vero (V) e falso (F). In corrispondenza di questi due possibili valori abbiamo due righe: la prima ci dice (guardando la colonna destra) che la formula $\neg p$ è falsa quando p è vera, la seconda che $\neg p$ è vera quando p è falsa, in accordo con quanto avevamo detto definendo il connettivo $\neg$. La seconda tavola ha invece quattro righe, perché la formula $p \wedge q$ ha due variabili e le combinazioni possibili per i valori di verità di due variabili sono quattro. Nell'ordine in cui appaiono nella tavola, le possibilità sono: (1) p e q sono entrambe vere; (2) p è vera e q è falsa; (3) p è falsa e q è vera; (4) p e q sono entrambe false. Anche qui ciascuna riga riporta, nella colonna di destra, il valore di verità della formula (in questo caso $p \wedge q$) in funzione dei valori di verità di p e q che appaiono, nella stessa riga, a sinistra. Come si vede, la tavola fornisce, anche in questo caso, esattamente le stesse informazioni che avevamo dato come definizione (semantica) di $\wedge$.

Completiamo questa introduzione alle tavole di verità con un minimo di terminologia e qualche indicazione ulteriore. Le variabili (come p e q, nei nostri esempi) che rappresentano proposizioni vengono chiamate *variabili proposizionali*; le formule costituite da variabili proposizionali, connettivi proposizionali (i due già definiti e quelli che stiamo per definire) e parentesi si chiamano *forme proposizionali*. Il *calcolo proposizionale* è la parte della logica che studia le forme proposizionali.

Come si può facilmente immaginare, esistono tavole di verità più complesse delle due che abbiamo esibito. Incontreremo tavole di verità che descrivono contemporaneamente più forme proposizionali, e quindi hanno più di una colonna nella parte destra, non solo una come nei nostri esempi. Incontreremo anche tavole che descrivono forme proposizionali con più di due variabili. È utile verificare (esercizio!) e ricordare poi che la tavola di verità di una forma proposizionale con un numero k di variabili richiede 2^k righe, perché 2^k è il numero di possibili combinazioni di valori di verità per k variabili.

Esercizi.
A.1. Scrivere le tavole di verità di ciascuna delle forme proposizionali: "$p \wedge p$", "$(\neg p) \wedge q$" e "$(\neg p) \wedge (\neg q)$".
A.2. Scrivere le tavole di verità delle forme proposizionali "$p \wedge (q \wedge r)$" e "$p \wedge (q \wedge (\neg r))$".

Riprendiamo ora nostra lista di connettivi proposizionali binari. Come nel caso di $\wedge$, anche per i successivi vale questa regola sintattica: se p e q sono formule e $*$ un connettivo binario allora $p * q$ è una formula. Inoltre, se p e q sono proposizioni allora $p * q$ è una proposizione ed il suo valore di verità dipende solo dal connettivo $*$ e dai valori di verità di p e q.

Disgiunzione (inclusiva). Il connettivo di *disgiunzione* si indica con $\vee$ o con OR. Da un punto di vista formale la sua descrizione è altrettanto semplice che quella della congiunzione, ma nell'uso la disgiunzione presenta qualche difficoltà in più. La ragione è che questo connettivo corrisponde ad uno dei significati che la particella[4] "o" ha in italiano (ovvero, che "or" ha in inglese). Il problema è, appunto, che nel linguaggio corrente "o" può assumere più significati, che hanno valore logico molto diverso.[5] Il significato che viene attribuito al connettivo proposizionale $\vee$ in matematica è quello, come si dice, *inclusivo*, per il quale, se p e q sono proposizioni, la forma $p \vee q$ è vera a condizione che *almeno una* tra p e q sia vera, ed è falsa nell'altro caso, cioè quando sia p che q siano false. La tavola di verità che definisce questo connettivo è dunque:

[4]secondo la grammatica della lingua italiana questa 'particella' è una congiunzione, ma evitiamo di chiamarla così per non fare confusione con il connettivo proposizionale $\wedge$, che abbiamo chiamato congiunzione.

[5]la necessità di rimuovere questo genere di ambiguità che sono proprie del linguaggio naturale è uno dei motivi per i quali, nel discorso scientifico, si deve utilizzare un linguaggio almeno parzialmente formalizzato.

disgiunzione (inclusiva)

p	q	$p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

Mettiamo in evidenza che $p \vee q$ risulta vera anche quando p e q sono entrambe vere. Invece, se il menu turistico della trattoria prevede una portata di carne *o* una di pesce, possiamo esser certi che l'oste non intende questo "o" come una disgiunzione inclusiva, ma come quella che si chiama una disgiunzione *esclusiva*: il cliente ha diritto ad avere un piatto di carne oppure uno di pesce, ma non entrambi. Sulla disgiunzione esclusiva (indicata con $\dot{\vee}$, oppure con XOR) torneremo più avanti; per ora diciamo che i valori di verità di $p \vee q$ e $p \dot{\vee} q$ differiscono solo nel caso in cui p e q siano entrambe vere; in questo caso $p \vee q$ è vera, $p \dot{\vee} q$ è falsa. Come detto, in italiano (e in inglese, ed in altre lingue) purtroppo sia la disgiunzione inclusiva che quella esclusiva sono rese dalla stessa particella ("o", "or" etc.), ma qualcuno probabilmente ricorda che in latino questi due connettivi sono ben distinti anche nel linguaggio ordinario: *vel* esprime la disgiunzione inclusiva, *aut* quella esclusiva.[6]

È importante insistere (da parte di chi scrive) e ancora di più ricordare (da parte di chi legge) che in matematica, e generalmente nel linguaggio scientifico, *per disgiunzione si intende* sempre *la disgiunzione inclusiva.* Confusione su questo punto porta invariabilmente a pericolose incomprensioni e macroscopici errori.

Equivalenza, o Doppia implicazione. Questo connettivo, chiamato anche *bicondizionale* e indicato con $\Leftrightarrow$ oppure con $\leftrightarrow$, si potrebbe definire in termini dell'implicazione, che verrà descritta tra poco, ma è molto semplice da descrivere in modo diretto. Se p e q sono proposizioni, "$p \Leftrightarrow q$" (che viene letta come "p se e solo se q", oppure "p equivale a q") è vera se p e q hanno lo stesso valore di verità, falsa altrimenti. La relativa tavola di verità è dunque:

equivalenza

p	q	$p \Leftrightarrow q$
V	V	V
V	F	F
F	V	F
F	F	V

Implicazione. Questo connettivo è chiamato anche *condizionale* e si indica con $\Rightarrow$ o con $\rightarrow$. Ancora più che la disgiunzione, esso presenta delle difficoltà dovute al fatto che l'uso che se fa in logica non combacia con l'uso suggerito dal linguaggio ordinario. Se p e q sono formule, la formula "$p \Rightarrow q$", o meglio la sua espressione verbale: "se p allora q" nel linguaggio quotidiano presuppone che ci sia un qualche nesso tra p e q che faccia apparire q come conseguenza di p. Ad esempio, "se piove allora non esco di casa" appare una frase del tutto naturale: si intende che il fatto che io non esca di casa dipende proprio dalla pioggia. Invece, la frase "se piove allora il Vesuvio è alto più di mille metri sul livello del mare" sembra priva di senso, per chi non ha studiato logica. Chi invece lo ha fatto ed è disposto a trasportare al linguaggio quotidiano i modi di espressione del linguaggio formale potrà convenire che la frase, per quanto di genere poco usuale, presa alla lettera non solo un senso lo ha ma è addirittura vera, come stiamo per vedere.

La tavola di verità che definisce l'implicazione è:

[6] a titolo di (forse comunque istruttiva) curiosità menzionamo il fatto che "o" può assumere in italiano almeno un altro significato. Se le richieste del piccolo Pasqualino superano un certo livello di soglia, la mamma potrà cercare di arginarle dicendogli che può avere "o il gelato o la pizzetta". Probabilmente in questo caso la mamma intende solo dire che non può avere entrambe le cose, ma che è più che soddisfatta se Pasqualino rinuncia ad entrambe. In questo caso, dunque, "o" esprime il connettivo NAND (negazione della congiunzione) a cui faremo cenno in seguito.

implicazione

p	q	$p \Rightarrow q$
V	V	V
V	F	F
F	V	V
F	F	V

Dunque, la formula $p \Rightarrow q$ (dove p e q sono proposizioni) è vera sempre tranne che nel caso in cui p (che si chiama *antecedente* dell'implicazione[7]) è vero e q (che si chiama *conseguente* dell'implicazione) è falso. Mentre più o meno tutti sono subito d'accordo con questa definizione nel caso in cui l'antecedente sia vero, quasi nessuno studente accetta di buon grado la seconda parte della definizione (data dalle ultime due righe della tavola di verità), cioè il fatto che la formula si consideri vera quando l'antecedente è falso (per giunta, indipendentemente dal valore di verità del conseguente!). Lo scopo dei prossimi paragrafi è quello di mostrare che questa definizione non solo non è frutto di una scelta capricciosa di qualcuno, ma è l'unica coerente con l'uso 'intuitivo' che dell'implicazione siamo sempre stati abituati a fare.

L'obiezione che spesso, in aula, gli studenti sollevano è che 'quando si sa già che p è falso la frase "se p allora q" (o la formula "$p \Rightarrow q$") non ha senso', e quindi non dovrebbe essere definito il suo valore di verità. E, inoltre, molti ritengono che se anche si deve proprio attribuire a questa frase un valore di verità sia innaturale la scelta di porla vera.

Non è così: una delle caratteristiche specifiche dei linguaggi formalizzati è, per così dire, l'indifferenza rispetto ai contenuti. La correttezza sintattica di una formula (come "$p \Rightarrow q$"), ed il fatto che essa venga interpretata nella semantica (in parole semplici, il fatto che la formula 'abbia senso') deve poter essere stabilita una volta per tutte e non può dipendere da informazioni accessorie di cui possiamo disporre o meno, come il contenuto fattuale di p (e che sono magari soggette a cambiare col tempo e le circostanze[8]). Questo fatto è addirittura utile, altrimenti, a rigore, non potremmo neanche discutere di formule come "$p \Rightarrow q$" se avessimo il dubbio che si possa dimostrare la falsità di p; ad essere pignoli non sarebbero possibili in matematica le dimostrazioni per assurdo o per contrapposizione.

Detto ciò, perché le implicazioni con antecedente falso devono proprio essere vere? Spero che questo esempio chiarisca la ragione della definizione. Consideriamo la frase "per ogni numero intero x compreso tra 1 e 3 si ha che se $x > 2$ allora $x > 1$". Tutti concordiamo su fatto che questa frase è vera. Analizziamola; essa significa che tutte le implicazioni $x > 2 \Rightarrow x > 1$ ottenute sostituendo ad x uno dei numeri 1, 2, 3 sono vere. Dunque sono vere la proposizione Φ_1 : "$1 > 2 \Rightarrow 1 > 1$", la Φ_2 : "$2 > 2 \Rightarrow 2 > 1$" e la Φ_3 : "$3 > 2 \Rightarrow 3 > 1$". Vediamo che la Φ_3 è del tipo 'non contestato': una implicazione in cui sia antecedente che conseguente sono veri, quindi vera, come indica il primo rigo della nostra tavola di verità. Le altre due proposizioni hanno invece l'antecedente falso. La Φ_1 è del tipo descritto dal quarto rigo della tavola di verità ('falso implica falso'), dal momento che sia l'antecedente $(1 > 2)$ che il conseguente $(1 > 1)$ sono falsi; la Φ_2 è del tipo descritto dal terzo rigo ('falso implica vero'). Se siamo d'accordo che sia ragionevole sostenere che la frase da cui siamo partiti ("per ogni numero intero x compreso tra 1 e 3 si ha che se $x > 2$ allora $x > 1$") sia vera, allora dobbiamo essere d'accordo anche sul fatto che siano (ragionevolmente) vere Φ_1 e Φ_2, quindi che siano ragionevoli i valori di verità che appaiono nella nostra tabella e che abbiamo usato per definire l'implicazione.[9]

[7] con un piccolo, ma conveniente, abuso di linguaggio si usa chiamare implicazione sia il connettivo ($\Rightarrow$) che una formula come $\alpha \Rightarrow \beta$ (dove α e β siano a loro volta formule) in cui il connettivo appare. Similmente accade per gli altri connettivi: può capitare ad esempio di dire che la formula $\alpha \wedge \beta$ sia una congiunzione

[8] come caso limite, si pensi ad una formula che esprima una frase del tipo "se esiste un polinomio non nullo f a coefficienti razionali di cui il numero π è radice, allora ...". Accogliendo l'obiezione secondo cui una implicazione il cui antecedente sia (notoriamente) falso non ha senso, dovremmo concludere che questa frase aveva senso verso la metà dell'ottocento ma non lo ha più a partire dal 1882, anno in cui è stato dimostrato (da Ferdinand von Lindemann) che un polinomio come f non può esistere. O, peggio, non ha più senso per chi conosce il risultato di Lindemann, lo ha per chi non lo conosce. In un liguaggio formale non c'è posto per pasticci del genere.

[9] ad ulteriore conferma, se la frase di partenza fosse stata "per ogni numero intero x compreso tra 1 e 3 si ha che se $x > 1$ allora $x > 2$", la frase sarebbe stata falsa. Infatti, le tre proposizioni ottenute sostituendo ad x i numeri 1, 2, 3 non sono *tutte* vere: quella ottenuta ponendo 2 al posto di x, cioè "$2 > 1 \Rightarrow 2 > 2$" è falsa, in accordo col secondo rigo della tavola, avendo l'antecedente vero ed il conseguente falso. Su questi esempi torneremo più avanti per chiarirli, si spera, ulteriormente.

Dunque le implicazioni con antecedente falso sono vere; osserviamo anche che sono vere le implicazioni con conseguente vero. In effetti, possiamo dire, sinteticamente, che una *implicazione è vera precisamente quando il suo antecedente è falso o il suo conseguente è vero.*

Esercizi ed Esempi.

B.1. Scrivere le tavole di verità di ciascuna delle forme proposizionali: "$p \wedge (p \vee q)$", "$(p \wedge q) \wedge r$", "$(p \wedge q) \vee r$".

B.2. Scrivere le tavole di verità di ciascuna delle forme proposizionali: "$p \Rightarrow (p \vee q)$", "$(p \wedge q) \Rightarrow r$", "$(p \wedge q) \Leftrightarrow r$".

B.3. Stabilire i valori di verità delle formule e frasi (assumiamo nota la matematica elementare coinvolta): "$(1+1=0) \vee (0+0=0)$"; "$(1+1=0) \wedge (0+0=0)$"; "$(1+1=0) \Rightarrow (0+0=0)$"; "$\sqrt{2}$ è un numero razionale o un numero irrazionale"; "$2^5 = 32 \Rightarrow 47 - 1 = 46$".

B.4. È molto importante saper 'tradurre' espressioni del linguaggio ordinario (della lingua italiana che parliamo quotidianamente) in linguaggio 'semiformalizzato', riconoscendo la presenza ed il ruolo dei connettivi proposizionali contenuti nelle frasi. Ad esempio, se indichiamo con α la frase 'domani pioverà' e con β la frase 'domani prenderò l'ombrello', si può rendere con $\alpha \wedge \beta$ la frase 'domani pioverà e prenderò l'ombrello'. Fare lo stesso per le frasi:

(a) Il supermercato era aperto e non ci sono entrato.
(b) Il supermercato era aperto ma non ci sono entrato.
(c) Se vedo Nicola lo saluto.
(d) Se domenica non piove e vado a Roma, $2 > 1$, ma se Marco mangia la pizza allora certamente fioriranno le rose.

B.5. Come nell'esercizio precedente, che struttura logica ha la frase: 'Maria ha cucinato la torta, e Franco non l'ha vista oppure l'ha mangiata'? Scriviamo t per 'Maria ha cucinato la torta', v per 'Franco ha visto la torta' e m per 'Franco ha mangiato la torta'. Se facciamo attenzione alla virgola che appare nella frase, concludiamo che questa frase si può rendere con $t \wedge ((\neg v) \vee m)$. Bene, come possiamo rendere: 'Maria ha cucinato la torta e Franco non l'ha vista, oppure l'ha mangiata'? Le due frasi hanno necessariamente gli stessi valori di verità, oppure possono esserci circostanze in cui una è vera e l'altra falsa?

B.6. Spiegare la seguente (vecchia e non particolarmente esilarante) storiella: la moglie del logico chiede al marito: 'Caro, stasera usciamo o restiamo a casa?'. Il marito risponde: 'Sì'.

3. Tautologie

Interrompiamo la lista dei connettivi per introdurre alcune importanti nozioni. Consideriamo una forma proposizionale Φ e supponiamo che p, q, r, ... siano le variabili proposizionali che *possono* apparire in Φ (quest'ultimo fatto si può esprimere scrivendo $\Phi(p, q, r, \dots)$ per Φ). Se attribuiamo un valore di verità (V o F) a ciascuna delle variabili in Φ (in modo consistente, ovviamente: ad esempio sempre lo stesso valore per ogni occorrenza della p) possiamo calcolare il valore di verità di Φ in funzione di quelli attribuiti a p, q, r, ...: è quello che facciamo quando scriviamo una tavola di verità. Si dice che Φ è una tautologia se e solo se il valore di verità di Φ così calcolato è V, indipendentemente dai valori attribuiti alle variabili che appaiono in Φ. In altri termini, Φ è una tautologia se e solo se, nella tavola di verità che la descrive, la colonna intestata da Φ contiene esclusivamente V. Alcuni esempi banali di tautologie sono le forme "$p \Rightarrow p$" e "$p \Leftrightarrow p$"; un altro, che esprime il *principio del terzo escluso*, di cui qualcuno potrebbe avere memoria scolastica, è la forma "$p \vee (\neg p)$". Per quanto facile, verifichiamo questa tautologia usando una tavola di verità:

terzo escluso

p	$\neg p$	$p \vee (\neg p)$
V	F	V
F	V	V

Come già minacciato, abbiamo qui una tavola di verità in cui la parte destra contiene più di una colonna: la prima contiene i valori di verità della sottoformula $\neg p$, usati come passaggio intermedio nel calcolo:

prima si è calcolata questa colonna a partire dalla colonna di p ed usando la descrizione di $\neg$, poi si è ottenuta la terza colonna applicando la disgiunzione alle prime due.

Dualmente, esistono forme proposizionali Φ per le quali, calcolando come detto sopra il valore di verità, si ottiene sempre il valore F. Queste si chiamano *contraddizioni*. Dovebbe essere chiaro che Φ è una contraddizione se e solo se $\neg\Phi$ è una tautologia. Un famoso esempio di contraddizione (lo si verifichi per esercizio) è la forma $p \wedge (\neg p)$, quindi la sua negazione $\neg(p \wedge (\neg p))$ è una tautologia, il *principio di non contraddizione*. Una forma proposizionale che non sia né una tautologia né una contraddizione si dice *contingente*. Ad esempio, la forma $p \Rightarrow q$ è contingente perché può assumere, in dipendenza dei valori sostituiti a p e a q, sia il valore V che il valore F.

Se α e β sono due forme proposizionali, si dice che α e β sono *logicamente equivalenti* (o, semplicemente, equivalenti) se e solo se la forma $\alpha \Leftrightarrow \beta$ è una tautologia. Naturalmente, questa condizione vuol dire che per qualsiasi scelta dei valori di verità attribuiti alle variabili che appaiono o in α o in β, α e β hanno lo stesso valore di verità. O, ancora in altri termini: α e β sono logicamente equivalenti se e solo in una tavola di verità in cui appaiano entrambe, ad esse corrisponda la stessa colonna di valori di verità. Vediamo un esempio molto semplice: questa tabella mostra che p e $\neg(\neg p)$ sono logicamente equivalenti.

tautologia della doppia negazione

p	$\neg p$	$\neg(\neg p)$
V	F	V
F	V	F

Detto diversamente, $p \Leftrightarrow (\neg(\neg p))$ è una tautologia, quella della *doppia negazione*.

Se una forma α appare come componente (o *sottoformula*) di una forma proposizionale Φ e se β è una forma logicamente equivalente ad α, è chiaro che sostituendo in Φ la sottoformula α con β si ottiene una forma Φ' che sarà logicamente equivalente a Φ. Ad esempio, se in Φ appare una sottoformula come $\neg(\neg\varphi)$, possiamo cancellare le due negazioni e quindi sostituire φ a $\neg(\neg\varphi)$ ottenendo una forma equivalente a Φ. Manipolazioni di questo genere sono spesso utili per calcolare valori di verità senza dover necessariamente far ricorso a tavole di verità.

Alcune tautologie elementari. Abbiamo già visto qualche esempio di tautologia. Ne elenchiamo ora altre, in modo più sistematico, spesso attribuendo loro, per nostra comodità, dei nomi che serviranno a poterle richiamare più avanti. La maggior parte di quelle che stiamo per vedere non necessitano di particolari commenti, risultando spesso addirittura ovvie. Chi legge è però caldamente invitato ad esercitarsi verificando che quelle elencate sono effettivamente tautologie. Le prime che incontriamo ricordano, anche nel nome, proprietà abitualmente definite per operazioni algebriche.

$$(p \wedge p) \Leftrightarrow p \qquad (p \wedge q) \Leftrightarrow (q \wedge p) \qquad \big((p \wedge q) \wedge r\big) \Leftrightarrow \big(p \wedge (q \wedge r)\big)$$
$$(p \vee p) \Leftrightarrow p \qquad (p \vee q) \Leftrightarrow (q \vee p) \qquad \big((p \vee q) \vee r\big) \Leftrightarrow \big(p \vee (q \vee r)\big)$$
$$(p \Leftrightarrow q) \Leftrightarrow (q \Leftrightarrow p) \qquad \big((p \Leftrightarrow q) \Leftrightarrow r\big) \Leftrightarrow \big(p \Leftrightarrow (q \Leftrightarrow r)\big)$$

idempotenza — commutatività — associatività

Sull'associatività di $\wedge$ e $\vee$, osserviamo che $(p \wedge q) \wedge r$ risulta vera se e solo se sono contemporaneamente vere sia p che q che r (lo stesso vale per $p \wedge (q \wedge r)$, altrimenti non avremmo una tautologia), mentre $(p \vee q) \vee r$ (ovvero, $p \vee (q \vee r)$) è vera se e solo se è vera almeno una tra p, q ed r. Più in generale (come accade in algebra), a partire da queste tautologie è possibile (ma noioso) provare che, qualunque sia l'intero positvo k le forme proposizionali in cui appaiano tutte e sole le le variabili $p_1, p_2, \ldots, p_k$, delle parentesi e, tra i connettivi, solo $\wedge$ sono equivalenti tra loro, indipendentemente dall'ordine in cui appaiano le variabili, dalle eventuali ripetizioni e dal modo in cui esse sono raggruppate (cioè da come sono disposte le parentesi).[10] Per queste forme si può allora rinunciare all'uso delle parentesi e scrivere semplicemente $p_1 \wedge p_2 \wedge p_3 \wedge \cdots \wedge p_k$ (omettendo, magari, anche le ripetizioni) o $\bigwedge_{i=1}^{k} p_i$ per indicare una qualunque di queste forme. Questa forma assume il valore V se e solo e valgono V tutte le p_i. Simile

[10] ad esempio, per $k = 4$, le forme $(p_1 \wedge p_2) \wedge (p_3 \wedge p_4)$, $p_1 \wedge ((p_2 \wedge p_3) \wedge p_4)$, $((p_2 \wedge p_4) \wedge (p_1 \wedge p_3)) \wedge p_4$ ed infinite altre sono tra loro equivalenti

enunciato vale per $\vee$ e giustifica l'uso di scritture come $p_1 \vee p_2 \vee p_3 \vee \cdots \vee p_k$ o $\bigvee_{i=1}^{k} p_i$, questa forma vale V se e solo se almeno una tra le p_i vale V.

Anche a proposito dell'associatività di $\Leftrightarrow$ qualche commento può essere utile. La verifica del fatto che tratti di una tautologia, cioè del fatto che $(p \Leftrightarrow q) \Leftrightarrow r$ e $p \Leftrightarrow (q \Leftrightarrow r)$ sono logicamente equivalenti, è contenuta nella tavola di verità (la cui verifica è lasciata a chi legge):

associatività della equivalenza

p	q	r	$(p \Leftrightarrow q) \Leftrightarrow r$	$p \Leftrightarrow (q \Leftrightarrow r)$
V	V	V	V	V
V	V	F	F	F
V	F	V	F	F
V	F	F	V	V
F	V	V	F	F
F	V	F	V	V
F	F	V	V	V
F	F	F	F	F

Si noti che $(p \Leftrightarrow q) \Leftrightarrow r$ vale vera se e solo se esattamente uno o tutti e tre tra p, q e r valgono vero.

Distributività. Altre tautologie che ricordano da vicino proprietà algebriche sono le *leggi distributive* (di $\wedge$ rispetto a $\vee$ e viceversa):

$$p \wedge (q \vee r) \iff (p \wedge q) \vee (p \wedge r)$$
$$p \vee (q \wedge r) \iff (p \vee q) \wedge (p \vee r),$$

Verifichiamo la prima delle due utilizzando una tavola di verità, questa volta con tutti i passaggi intermedi:

p	q	r	$q \vee r$	$p \wedge (q \vee r)$	$p \wedge q$	$p \wedge r$	$(p \wedge q) \vee (p \wedge r)$
V	V	V	V	V	V	V	V
V	V	F	V	V	V	F	V
V	F	V	V	V	F	V	V
V	F	F	F	F	F	F	F
F	V	V	V	F	F	F	F
F	V	F	V	F	F	F	F
F	F	V	V	F	F	F	F
F	F	F	F	F	F	F	F

Confrontando la quinta e l'ottava colonna, che coincidono in tutto tranne che nell'intestazione, si ottiene il risultato.

Esercizi.
C.1. Verificare la seconda delle tautologie appena enunciate (cioè la distributività della disgiunzione rispetto alla congiunzione).
C.2. La forma proposizionale $(p \wedge q) \Rightarrow (p \vee q)$ è una tautologia, mentre $(p \vee q) \Rightarrow (p \wedge q)$ non lo è. Scrivere la tavola di verità di quest'ultima. È possibile scrivere una forma proposizionale più breve (nel senso ovvio) di $(p \vee q) \Rightarrow (p \wedge q)$ e che sia equivalente a questa?
C.3. Verificare la tautologia $\big(p \Rightarrow (q \Rightarrow r)\big) \iff \big((p \Rightarrow q) \Rightarrow (p \Rightarrow r)\big)$ (distributività da sinistra della implicazione rispetto a se stessa).

Leggi di De Morgan. Quando è che una proposizione della forma $p \wedge q$ è falsa? Risposta: quando (e solo quando) è falsa *almeno una* tra p e q. Questo è evidente dalla tavola di verità che descrive la congiunzione. La risposta che qualche volta capita di ricevere: 'quando sia p che q sono false' è sbagliata: la proposizione è sicuramente falsa in questo caso, ma lo è anche in altri. Ad esempio, perché non sia vero che io abbia preso il treno e sia arrivato a Firenze non è necessario che io non abbia preso il treno *e* non sia arrivato a Firenze, la frase è falsa anche se io ho preso il treno e mi sono fermato a Roma, ad esempio, o anche se io sono andato a Firenze, ma in auto.

Dualmente, una proposizione della forma $p \vee q$ è falsa precisamente quando *sia p che q* sono false (come mostra la tavola di verità della disgiunzione), quindi la negazione di 'prendo l'auto o vado a piedi' è 'non prendo l'auto *e* non vado a piedi'. Tutto questo è espresso da due tautologie molto importanti, note come *leggi di De Morgan*:

$$\begin{aligned} \big(\neg(p \wedge q)\big) &\iff \big((\neg p) \vee (\neg q)\big) \\ \big(\neg(p \vee q)\big) &\iff \big((\neg p) \wedge (\neg q)\big) \end{aligned} \qquad \text{(De Morgan)}$$

Dunque, una disgiunzione (o una congiunzione) si negano negando i due termini che stiamo disgiungendo (o congiungendo) e, contemporaneamente, scambiando tra loro i simboli $\wedge$ e $\vee$.

Esercizi.
D.1. Negare ciascuna delle frasi: "Mario corre e Maria nuota"; "La bottiglia è vuota oppure tappata".
D.2. Negare la frase: 'Alice ha i capelli biondi ricci'. (Si chiede che anche la negazione inizi con 'Alice ha i capelli ...'. Attenzione: quale connettivo proposizionale è nascosto nella frase?)
D.3. Usando le leggi di De Morgan, negare $p \vee (\neg(q \wedge (\neg p)))$. Ciò che si chiede è scrivere una formula che sia equivalente alla negazione di quella data e che non abbia $\neg$ come primo simbolo.
D.4. Come per l'esercizio precedente, negare ciascuna delle due formule: "$p \wedge q \wedge r$" e "$(p \vee q) \wedge ((p \vee r) \wedge (q \vee s))$".

Tautologie sulla implicazione. Le tautologie sulla implicazione hanno grande importanza: il carattere meno intuitivo di questo connettivo le rende meno ovvie di quelle che abbiamo incontrato finora, ma l'uso frequentissimo che si fa in matematica del connettivo di implicazione rende queste tautologie uno strumento utilissimo. Vale dunque la pena di soffermarsi con una certa attenzione su di esse.

In primo luogo, il connettivo "$\Rightarrow$", a differenza degli altri connettivi binari analizzati finora, non è commutativo; vale a dire: le forme "$p \Rightarrow q$" e "$q \Rightarrow p$" non sono equivalenti tra loro. Basta una tavola di verità per convincersene:

p	q	$p \Rightarrow q$	$q \Rightarrow p$
V	V	V	V
V	F	F	V
F	V	V	F
F	F	V	V

Prendiamo nota del fatto che spesso si scrive "$p \Leftarrow q$" per "$q \Rightarrow p$". Si può considerare questo simbolo "$\Leftarrow$" come un ulteriore connettivo binario (*implicazione inversa*), definito appunto dall'essere $p \Leftarrow q$ logicamente equivalente a $q \Rightarrow p$.

Come chi legge queste note certamente già sa, la congiunzione di una implicazione e della corrispondente implicazione inversa equivale alla doppia implicazione, cioè vale la tautologia:

$$\big(p \Leftrightarrow q\big) \iff \big((p \Rightarrow q) \wedge (p \Leftarrow q)\big), \qquad \text{(tautologia della doppia implicazione)}$$

come mostrato dalla tavola di verità:

p	q	$p \Leftrightarrow q$	$p \Rightarrow q$	$p \Leftarrow q$	$(p \Rightarrow q) \wedge (p \Leftarrow q)$
V	V	V	V	V	V
V	F	F	F	V	F
F	V	F	V	F	F
F	F	V	V	V	V

Non basteranno mai gli avvertimenti e le preghiere rivolte agli studenti perché facciano attenzione a non confondere tra loro implicazione, implicazione inversa ed equivalenza. Si tratta, lo abbiamo visto in dettaglio, di connettivi che hanno funzioni logiche ben diverse; confonderli porta quasi certamente ad errori di ragionamento, spesso molto gravi.[11]

Forse questo è un punto adatto per elencare alcune delle tante espressioni che vengono utilizzate in matematica per rendere nel linguaggio ordinario i connettivi di implicazione, implicazione inversa ed equivalenza. In ciascuna colonna si possono leggere frasi che traducono la formula nell'intestazione:

$p \Rightarrow q$	$p \Leftarrow q$	$p \Leftrightarrow q$
Se p allora q		
p solo se q	p se q	p se e solo se q
p è condizione sufficiente per q	p è condizione necessaria per q	p è condizione necessaria e sufficiente per q

Come si è visto, dunque, il connettivo di equivalenza può essere ridotto a quelli di implicazione e congiunzione. Anche il connettivo di implicazione può essere espresso in termini di altri connettivi (disgiunzione e negazione). Si ha infatti questa tautologia:

$$\big(p \Rightarrow q\big) \iff \big((\neg p) \vee q\big), \qquad \text{(implicazione come disgiunzione)}$$

che segue direttamente dalle tavole di verità di implicazione e disgiunzione e che avevamo sostanzialmente già osservato nelle ultime righe della sezione in cui è stata introdotta l'implicazione, dove abbiamo notato che una una implicazione è vera se e solo se il suo antecedente è falso o il suo conseguente è vero. Da questa tautologia se ne può facilmente dedurre un'altra, la *legge di contrapposizione*:

$$\big((p \Rightarrow q)\big) \iff \big((\neg q) \Rightarrow (\neg p)\big). \qquad \text{(legge di contrapposizione)}$$

Il passaggio è il seguente: $p \Rightarrow q$ equivale a $(\neg p) \vee q$, ovvero a $q \vee (\neg p)$ (per la commutatività di $\vee$), ovvero a $(\neg(\neg q)) \vee (\neg p)$ (per la tautologia della doppia negazione), ma quest'ultima, per la tautologia dell'implicazione come disgiunzione, equivale a $(\neg q) \Rightarrow (\neg p)$.

Molto importante, ed anch'essa immediata dalla tavola di verità della implicazione, è la tautologia che mostra come negare una implicazione: questa è falsa precisamente quando l'antecedente è vero ed il conseguente è falso.

$$\big(\neg(p \Rightarrow q)\big) \iff \big(p \wedge (\neg q)\big). \qquad \text{(negazione dell'implicazione)}$$

Un'altra tautologia di uso frequentissimo è quella della *transitività dell'implicazione*:

$$\big((p \Rightarrow q) \wedge (q \Rightarrow r)\big) \Rightarrow \big(p \Rightarrow r\big). \qquad \text{(transitività dell'implicazione)}$$

Piuttosto che scrivere una (noiosa e lunga) tavola di verità, verifichiamo questa tautologia utilizzando un metodo che è spesso molto conveniente quando si ha a che fare con le implicazioni. Per provare che la formula risulti vera, indipendentemente dal valore di verità attribuito a p, q, r, poveremo che in nessun caso essa può risultare falsa. Perché la formula sia falsa occorre che sia vero l'antecedente $((p \Rightarrow q) \wedge (q \Rightarrow r))$ e falso il conseguente $(p \Rightarrow r)$. La prima condizione significa che sono vere $p \Rightarrow q$ e $q \Rightarrow r$, la seconda che sia vera p e falsa r. Ora, assumendo queste condizioni, sono in particolare vere p e $p \Rightarrow q$; da ciò segue subito che q è vera (se p è vera ma q è falsa, allora $p \Rightarrow q$ è falsa!). Quindi, se la nostra formula è falsa, risultano vere p e q, ma falsa r. Tuttavia, in questo caso, $q \Rightarrow r$ è falsa, mentre avevamo detto che, perché la formula sia falsa, $q \Rightarrow r$ deve essere vera. Questo ragionamento mostra che

[11] come quello del contadino che, sapendo che se piove si esce con l'ombrello, pensa che sia sufficiente prendere l'ombrello per garantire un po' di pioggia ai suoi campi.

la formula considerata, cioè $\big((p \Rightarrow q) \wedge (q \Rightarrow r)\big) \Rightarrow \big(p \Rightarrow r\big)$, non può essere falsa in nessun caso, quindi è una tautologia.

L'idea esemplificata da questa dimostrazione consiste in questo: imporre che una implicazione sia falsa fornisce immediatamente due informazioni: i valori di verità di antecedente e conseguente. Dunque può essere conveniente, nello studiare una implicazione, analizzare subito le conseguenze dell'ipotesi che essa sia falsa.

È chiaro che dalla transitività dell'implicazione (e dalla tautologia della doppia implicazione si possono dedurre molte altre tautologie che coinvolgano i connettivi $\Rightarrow$, $\Leftarrow$ e $\Leftrightarrow$, come ad esempio la *transitività della equivalenza*: $\big((p \Leftrightarrow q) \wedge (q \Leftrightarrow r)\big) \Rightarrow \big(p \Leftrightarrow r\big)$ o altre come $\big((p \Leftrightarrow q) \wedge (q \Rightarrow r) \wedge (r \Rightarrow t)\big) \Rightarrow \big(p \Rightarrow t\big)$.

Concludiamo accennando a una notazione abbreviata, molto intuitiva e di uso comune, quella delle cosiddette catene di implicazioni, che esprimono congiunzioni tra formule che sono a loro volta implicazioni, implicazioni inverse o equivalenze. Dovrebbe bastare qualche esempio: espressioni come $\alpha \Rightarrow \beta \Leftrightarrow \gamma$ oppure $\alpha \Leftarrow \beta \Rightarrow \gamma \Rightarrow \delta$ (senza parentesi), vengono usate al posto di $(\alpha \Rightarrow \beta) \wedge (\beta \Leftrightarrow \gamma)$ e $(\alpha \Leftarrow \beta) \wedge (\beta \Rightarrow \gamma) \wedge (\gamma \Rightarrow \delta)$ rispettivamente. Dunque, la transitività della implicazione si può riscrivere come $(p \Rightarrow q \Rightarrow r) \Rightarrow (p \Rightarrow r)$.

Esercizi ed Osservazioni.

E.1. Torniamo sull'Esercizio B.5. La prima frase proposta in quell'esercizio si potrebbe rendere, in modo equivalente, con $t \wedge (v \Rightarrow m)$? Oppure con $t \wedge (m \Rightarrow v)$?

E.2. Studiare la forma $(p \Rightarrow q) \vee (p \Leftarrow q)$. Confrontarla col secondo membro (il termine a destra di "$\Leftrightarrow$") nella tautologia della doppia implicazione.

E.3. Utilizzando le leggi di De Morgan, si determini la negazione di $(\neg p) \vee q$. Si confronti quanto ottenuto con le tautologie della implicazione come disgiunzione e con quella della negazione dell'implicazione.

E.4. La legge di contrapposizione è alla base di una tecnica dimostrativa di uso molto frequente. Per dimostrare una tesi T partire da una ipotesi H, cioè per dimostrare l'implicazione $H \Longrightarrow T$, si può assumere falsa T e dedurre da questa assunzione la falsità di H. In altri termini, ciò che si fa in questo modo è dimostrare l'implicazione $(\neg T) \Longrightarrow (\neg H)$. Per la legge di contrapposizione, questa formula equivale ad $H \Longrightarrow T$, quella che si voleva dimostrare. Dimostrazioni condotte in questo modo si chiamano *dimostrazioni per contrapposizione*.

E.5. Si provi che le forme proposizionali "$(p \wedge q) \Rightarrow r$", "$p \Rightarrow (q \Rightarrow r)$" e "$q \Rightarrow (p \Rightarrow r)$" sono tra loro logicamente equivalenti. Si consiglia di non utilizzare, a questo scopo, tavole di verità ma di ragionare come fatto per la transitività dell'implicazione. Questo consiglio si estende anche agli esercizi che seguono.

E.6. Verificare la tautologia "$\big(p \wedge (p \Rightarrow q)\big) \Rightarrow q$", nota come *legge dell'inferenza*.

E.7. Tornare all'Esercizio C.3 (se lo si è svolto) e ripetere (o farla ex-novo) la verifica senza usare tavole di verità. La forma "$\big((p \Rightarrow q) \Rightarrow r\big) \Leftrightarrow \big((p \Rightarrow r) \Rightarrow (q \Rightarrow r)\big)$" è una tautologia?

E.8. Verificare le tautologie "$\big(p \Rightarrow (q \wedge r)\big) \Leftrightarrow \big((p \Rightarrow q) \wedge (p \Rightarrow r)\big)$" e "$\big(p \Rightarrow (q \vee r)\big) \Leftrightarrow \big((p \Rightarrow q) \vee (p \Rightarrow r)\big)$" (distributività da sinistra di $\Rightarrow$ rispetto a $\wedge$ e a $\vee$). Suggerimento: si usi la tautologia della implicazione come disgiunzione per trasformare tutte le implicazioni in disgiunzioni che coinvolgano $\neg p$.

Le forme "$\big((q \wedge r) \Rightarrow p\big) \Leftrightarrow \big((q \Rightarrow p) \wedge (r \Rightarrow p)\big)$" e "$\big((q \vee r) \Rightarrow p\big) \Leftrightarrow \big((q \Rightarrow p) \vee (r \Rightarrow p)\big)$" sono tautologie?

4. Altri connettivi binari

Per completare la nostra discussione sul calcolo proposizionale vanno ancora menzionati alcuni connettivi binari, che hanno interesse di per sé e sono spesso utilizzati in informatica. Il più importante tra questi è la *disgiunzione esclusiva* ($\dot\vee$, o XOR), a cui abbiamo già fatto cenno. Altri due sono le negazioni della congiunzione e della disgiunzione, rispettivamente NAND e NOR (da leggere come not-and e not-or), che sono anche noti, rispettivamente, come operazione di Sheffer (o *stroke*, indicata con $|$ o $\uparrow$) e operazione di Pierce (e indicata con $\downarrow$). Le tavole di verità sono:

p	q	$p \dot\vee q$ p XOR q
V	V	F
V	F	V
F	V	V
F	F	F

p	q	$p \mid q$ p NAND q
V	V	F
V	F	V
F	V	V
F	F	V

p	q	$p \downarrow q$ p NOR q
V	V	F
V	F	F
F	V	F
F	F	V

È chiaramente giustificato quanto abbiamo appena detto su NAND e NOR: questi connettivi negano $\wedge$ e $\vee$, nel senso che "$(p \text{ NAND } q) \Leftrightarrow (\neg(p \wedge q))$" e "$(p \text{ NOR } q) \Leftrightarrow (\neg(p \vee q))$" sono tautologie. Allo stesso modo, XOR nega $\Leftrightarrow$. Si ha infatti una utilissima serie di tautologie, che si possono esprimere come catena di equivalenze:

$$\big(\neg(p \Leftrightarrow q)\big) \iff \big((\neg p) \Leftrightarrow q\big) \iff \big(p \Leftrightarrow (\neg q)\big) \iff \big(p \text{ XOR } q\big). \qquad \text{(negazione dell'equivalenza)}$$

Ricordiamo cosa significa: le quattro forme proposizionali elencate sono a due a due logicamente equivalenti. Che lo siano si vede subito: ciascuna di esse è vera quando e solo quando p e q hanno diversi valori di verità, cioè una vale 'vero', l'altra vale 'falso'. Notiamo che queste tautologie ci mostrano come possiamo importare ed esportare (portare 'dentro' o 'fuori' a nostro piacimento) il simbolo di negazione da una equivalenza a ciascuno dei termini che vi appaiono. Usando questo fatto possiamo dimostrare una proprietà molto importante: l'associatività del connettivo XOR.[12]

Consideriamo infatti la forma p XOR $(p$ XOR $r)$. La catena di equivalenze appena osservata mostra che p XOR $(q$ XOR $r)$ equivale a $\neg(p \Leftrightarrow (q \text{ XOR } r))$ e questa (importando la negazione al secondo termine dell'equivalenza), equivale a $p \Leftrightarrow (\neg(q \text{ XOR } r))$, cioè a $p \Leftrightarrow (q \Leftrightarrow r)$. Abbiamo dunque la tautologia

$$\big(p \text{ XOR } (q \text{ XOR } r)\big) \iff \big(p \Leftrightarrow (q \Leftrightarrow r)\big).$$

Allo stesso modo (oppure usando quest'ultima tautologia insieme alla *commutatività*, ovvia, di XOR[13] e a quella di $\Leftrightarrow$) si verifica la tautologia

$$\big((p \text{ XOR } q) \text{ XOR } r\big) \iff \big((p \Leftrightarrow q) \Leftrightarrow r\big).$$

Da queste due, e dall'associatività di $\Leftrightarrow$ si ricava la tautologia che volevamo provare:

$$\big(p \text{ XOR } (q \text{ XOR } r)\big) \iff \big((p \text{ XOR } q) \text{ XOR } r\big). \qquad \text{(associatività di XOR)}$$

Altre due facili tautologie che riguardano XOR sono espresse in questa catena di equivalenze:

$$(p \text{ XOR } q) \iff \big((p \wedge (\neg q)) \vee (q \wedge (\neg p))\big) \iff \big((p \vee q) \wedge (\neg(p \wedge q))\big). \qquad \text{(esplicitazione di XOR)}$$

Anche queste equivalenze si provano facilmente osservando che, evidentemente, sia $\big((p \wedge (\neg q)) \vee (q \wedge (\neg p)\big)$ che $\big((p \vee q) \wedge (\neg(p \wedge q)\big)$ sono vere se e solo esattamente uno tra p e q è vero, ma si veda a questo riguardo anche l'Esercizio F.1. È poi importante (per lo studio delle strutture booleane) la tautologia

$$\big(p \wedge (q \text{ XOR } r)\big) \iff \big((p \wedge q) \text{ XOR } (p \wedge r)\big), \qquad \text{(distributività di } \wedge \text{ rispetto a XOR)}$$

di verifica diretta.

L'ultima osservazione che facciamo prima di chiudere con il calcolo proposizionale evidenzia una particolarità che rende interessanti i connettivi NAND e NOR. Sappiamo che la nostra lista di connettivi è piuttosto ridondante. Non avremmo avuto bisogno, ad esempio, di definire in modo indipendente il connettivo di equivalenza, ma avremmo potuto considerare la scrittura "$p \Leftrightarrow q$" come una semplice abbreviazione di "$(p \Rightarrow q) \wedge (q \Rightarrow p)$", dal momeno che la tautologia della doppia implicazione ci dice che le due formule sono equivalenti. Similmente, la tautologia della implicazione come disgiunzione mostra come sia possibile fare a meno anche del connettivo $\Rightarrow$ ed esprimere tutte le implicazioni (e le implicazioni inverse) utilizzando $\neg$ e $\vee$; in modo ancora più immediato NAND e NOR si ottengono da $\neg$, $\vee$ e $\wedge$, che

[12] il fatto che XOR sia associativo permette, tra l'altro, di definire in modo sintetico le strutture booleane, che hanno enorme importanza nell'informatica teorica.

[13] cioè la tautologia $(p \text{ XOR } q) \iff (q \text{ XOR } p)$. Anche NOR e NAND sono commutative; tutto ciò è evidente dalle descrizioni che abbiamo dato di questi connettivi.

certamente bastano per esprimere anche XOR. Dunque possiamo esprimere tutto il calcolo proposizionale usando solo i connettivi $\neg$, $\vee$ e $\wedge$. Meglio ancora: dalle leggi di De Morgan (e dalla tautologia della doppia negazione) seguono le tautologie

$$\big(p \vee q\big) \Leftrightarrow \big(\neg((\neg p) \wedge (\neg q))\big) \qquad \text{e} \qquad \big(p \wedge q\big) \Leftrightarrow \big(\neg((\neg p) \vee (\neg q))\big),$$

che mostrano come la disgiunzione si possa esprimere utilizzando $\neg$ e $\wedge$, mentre la congiunzione si può esprimere utilizzando $\neg$ e $\vee$. Dunque tutte le formule del calcolo proposizionale possono essere espresse (a meno di equivalenze) usando solo due connettivi: $\neg$ ed uno a scelta tra $\wedge$ e $\vee$. Se siamo davvero interessati a ridurre il numero dei connettivi usati, si può addirittura fare di meglio: basta un solo connettivo, uno a scelta tra NAND e NOR. Abbiamo infatti due tautologie (di semplicissima verifica):

$$(p \text{ NOR } p) \iff (\neg p) \iff (p \text{ NAND } p)$$

che garantiscono come l'uso della negazione possa sempre essere sostituito dall'uso di una qualsiasi tra NAND e NOR. Dunque, il connettivo NAND permette di esprimere $\neg$, e quindi $\wedge$ (perché $p \wedge q$ equivale a $\neg(p \text{ NAND } q)$, cioè a $(p \text{ NAND } q)$ NAND $(p \text{ NAND } q)$). Per quanto visto sopra, possiamo concludere che *ogni formula del calcolo proposizionale equivale ad una formula in cui l'unico connettivo che appaia è* NAND. Allo stesso modo, dal momento che NOR basta per esprimere la negazione e quindi la disgiunzione (tramite la tautologia $(p \vee q) \Leftrightarrow (\neg(p \text{ NOR } q))$, *anche* NOR *ha la stessa proprietà.* È questo il motivo che rende le porte NAND e le porte NOR così utili per la progettazione di circuiti elettronici.

Esercizi.

F.1. Usando le leggi distributive e le leggi di De Morgan, verificare direttamente che la forma proposizionale $(p \wedge (\neg q)) \vee (q \wedge (\neg p))$ è equivalente a $(p \vee q) \wedge ((\neg q) \vee (\neg p))$ e quindi a $(p \vee q) \wedge (\neg(p \wedge q))$. Utilizzando le tautologie della doppia implicazione e della implicazione come disgiunzione verificare poi che anche $(\neg p) \Leftrightarrow q$ è equivalente a $(p \vee q) \wedge ((\neg q) \vee (\neg p))$. Questo fornisce una dimostrazione alternativa per le due tautologie cha abbiamo chiamato esplicitazione di XOR.

F.2. Verificare in dettaglio la distributività della congiunzione rispetto a XOR. Basta usare una tavola di verità, ma si può ragionare in modo più sintetico così: se p vale 'falso' entrambi i membri della equivalenza sono falsi, se p vale 'vero', entrambi sono equivalenti a q XOR r. Completare il ragionamento verificando tutti i passaggi.

F.3. Vale la tautologia "$\big(p \vee (q \text{ XOR } r)\big) \iff \big((p \vee q) \text{ XOR } (p \vee r)\big)$" (distributività della disgiunzione rispetto a XOR)?

F.4. Scrivere una forma proposizionale equivalente a $p \Rightarrow q$ in cui appaiano solo le variabili p e q, il connettivo NAND e, eventualmente, parentesi.

5. Quantificatori

Consideriamo la formula "$x > 1$" del linguaggio dell'aritmetica che abbiamo già (informalmente) introdotto nella prima sezione di queste note. In accordo con quanto scritto lì, questa formula non ha un valore di verità, perché non è una proposizione. Abbiamo però a disposizione una idea intuitiva di 'sostituzione'[14] che ci permette di estendere la nostra nozione di verità, valutando la formula per ciascuno dei numeri che possono essere sostituiti alla variabile x.[15] In termini semplici, non abbiamo difficoltà a dire che la formula è vera "per $x = 10$" (cioè sostituendo ad x il numero 10) ed è falsa per $x = 0$. Se chiamiamo φ, o $\varphi(x)$, la nostra formula, possiamo indicare con $\varphi(10)$ e $\varphi(0)$, rispettivamente, le formule "ottenute da φ sostituendo ad x i numeri 10 e 0", nell'ordine, quindi $\varphi(10)$ è la formula (chiusa! e vera) $10 > 1$ mentre $\varphi(0)$ è la formula (chiusa e falsa) $0 > 1$.

Può capitare che una formula risulti vera per ogni possibile sostituzione delle variabili. In questo caso diremo che la formula è *valida.*[16] Ad esempio, sono valide le formule $x = x$ o anche le formule ricavate

[14] idea che naturalmente, ma con qualche fatica, si potrebbe formalizzare. A qualcosa in più accenneremo tra poche pagine, dopo aver discusso di variabili libere e vincolate

[15] scriviamo 'numeri' perché il linguaggio che stiamo usando è quello dell'aritmetica e quindi implicitamente assumiamo che le variabili possano indicare solo oggetti che chiamiamo numeri interi, qualsiasi cosa essi siano.

[16] Ancora una volta dobbiamo sottolineare che stiamo fornendo una trattazione molto semplificata della materia. Quella di validità di una formula è in realtà una nozione più ricca di quanto risulta qui, ma la sua definizione completa dipende da concetti che non ci è necessario toccare e non toccheremo.

da tautologie, come ad esempio $\varphi \vee (\neg\varphi)$, per qualsiasi formula φ, che si ottiene rimpiazzando p con φ nella tautologia principio del terzo escluso. Useremo espressioni come 'vale l'implicazione $\varphi \Rightarrow \psi$' per dire che la formula $\varphi \Rightarrow \psi$ è valida, oppure 'φ e ψ sono equivalenti' per dire che $\varphi \Leftrightarrow \psi$ è valida; questo per *arbitrarie* (cioè non necessariamente chiuse) formule φ e ψ.

Torniamo al nostro discorso. La nozione di sostituzione ci premette di introdurre due nuovi simboli logici, che svolgono un ruolo centrale in un capitolo della logica chiamato *calcolo dei predicati*. Questi simboli sono il *quantificatore universale* $\forall$ ed il *quantificatore esistenziale* $\exists$.[17] La sintassi è semplice: se φ è una una formula ed x è una variabile allora anche "$\forall x(\varphi)$" e "$\exists x(\varphi)$" sono formule; per maggior leggibilità si può anche scrivere "$(\forall x)(\varphi)$" e "$(\exists x)(\varphi)$" o, come al solito, scrivere $\varphi(x)$ al posto di φ per evidenziare la possibilità che x appaia in φ.

La prima formula, $\forall x(\varphi)$, è quella che si chiama una *formula universale*[18] e si legge 'per ogni x, φ'. Questa formula esprime la contemporanea affermazione di tutte le formule $\varphi(a)$ ottenute sostituendo ad x ogni possibile valore a. Può aiutare pensare a questa formula come ad una versione generalizzata della congiunzione: la congiunzione tra tutte le formule $\varphi(a)$ ottenute da φ per sostituzione di x con a, per ogni possibile scelta di a.[19] Nel caso in cui ciascuna delle formule $\varphi(a)$ così ottenute sia chiusa (cioè una proposizione), la formula $\forall x(\varphi)$ esprime il fatto che ciascuna delle $\varphi(a)$ è vera. Ad esempio, usando come φ la formula $x = x$ otteniamo la formula $\forall x(x = x)$, che è una proposizione (vedremo come mai) vera perché qualsiasi sia l'oggetto che sostituiamo ad x, questo oggetto è uguale e se stesso. Invece, se partiamo dalla formula $x > 1$ dell'aritmetica usata come esempio nel paragrafo precedente, otteniamo $\forall x(x > 1)$, che è ancora una proposizione ma è falsa, perché non tutti i numeri interi verificano la condizione di essere maggiori di uno.

Se le formule universali possono essere pensate come una sorta di congiunzione generalizzata, le *formule esistenziali*, cioè quelle introdotte dal quantificatore $\exists$, possono invece essere pensate come disgiunzioni generalizzate. Se x è una variabile e $\varphi = \varphi(x)$ una formula, $\exists x(\varphi)$ (che si può leggere: "esiste un x tale che φ") esprime l'affermazione di *almeno una* tra le formule $\varphi(a)$ ottenute sostituendo ad x ogni possibile valore a. Ad esempio, nel linguaggio dell'aritmetica la formula $\exists x(x > 1)$ è una proposizione (lo vedremo) ed è vera perché, ad esempio, è vera la formula "$3 > 1$" ottenuta sostituendo 3 ad x in "$x > 1$". Invece la formula $\exists x(x \neq x)$ è falsa.

Oltre a $\forall$ ed $\exists$ esistono altri quantificatori. Quello di uso più frequente è "$\exists!$". Se φ è una formula ed x è una variabile, la formula "$\exists! x(\varphi)$" si legge "esiste uno ed un solo x tale che φ" ed afferma $\varphi(a)$ per uno dei possibili valori a che possono essere sostituiti ad x, negando $\varphi(b)$ per ogni b diverso da a; in termini più semplici: φ è verificata da a e solo da a. In modo sintetico e più formale, se y è una variabile (diversa da x) che non appare in φ, questo quantificatore è definito dall'equivalenza:[20]

$$\exists! x(\varphi(x)) \iff \exists x(\forall y(\varphi(y) \Leftrightarrow y = x)). \qquad \text{(descrizione di } \exists!)$$

È un utile esercizio comprendere questa equivalenza, cioè il fatto che il suo membro a destra (vale a dire $\exists x(\forall y(\varphi(y) \Leftrightarrow y = x))$) esprime proprio ciò che vogliamo esprima il membro a sinistra ($\exists! x(\varphi(x))$). Commenti a questo proposito sono nell'Osservazione G.1.

Variabili libere e vincolate. In una formula come $\forall x(\varphi)$ o come $\exists x(\varphi)$ (anche se queste appaiono come sottoformule di formule più complesse) si dice che le occorrenze di x sono *vincolate* (dal quantificatore $\forall$ o dal quantificatore $\exists$). Dunque sono vincolate le (occorrenze delle) variabili che appaiano nel 'raggio d'azione' di un quantificatore (si intende però che ogni quantificatore può vincolare solo le occorrenze della variabile che lo segue immediatamente: in $\forall x(x = y)$, il quantificatore vincola la x, non la y). In una qualsiasi formula, le (occorrenze delle) variabili che non sono vincolate si dicono *libere*. Ad esempio, sono vincolate le occorrenze di x in "$(\forall x(x + 1 > x)) \wedge (\exists x(x > y))$", mentre nella stessa formula è libera l'occorrenza di y. Attenzione: è possibile che nella stessa formula la stessa variabile abbia sia occorrenze libere che occorrenze vincolate: ad esempio, in "$(\forall x(x + 1 > x)) \vee (x = 0)$" l'ultima occorrenza di x è libera, le altre sono vincolate (si noti però che tutte le occorrenze di x in "$\forall x((x + 1 > x) \vee (x = 0))$" sono vincolate; attenzione alle parentesi!).

[17] l'origine del simbolo $\exists$ è ovvia: richiama la 'E' iniziale della parola 'Esiste' o delle sue varianti in diverse lingue. Il simbolo $\forall$ richiama invece la 'A' iniziale dell'inglese 'All' (o meglio, del tedesco 'Alle') che sta per 'tutti'.

[18] cioè: introdotta da un quantificatore universale.

[19] non si tratta effettivamente di una congiunzione, perché si possono congiungere, usando il connettivo $\wedge$, solo un numero finito di formule per volta, invece le formule $\varphi(a)$ sono, in generale, in numero infinito.

[20] questa frase vuol dire: $\exists!$ è definito dal fatto che scelti comunque la formula φ e le variabili (distinte) x e y in modo che y non appaia in x la formula che segue è *valida*, nel senso indicato sopra.

Benché le nozioni di occorrenze libere e vincolate siano qui state presentate solo per grandi linee, è bene farci attenzione per almeno due motivi. Il primo è che la (già promessa) definizione di formula chiusa dipende proprio dalle nozioni appena introdotte: *una formula è chiusa se e solo se non contiene variabili con occorrenze libere*. Vediamo così che formule come "$\forall x(x > 1)$" e "$\forall x((x+1 > x) \vee (x = 0))$", che abbiamo incontrato poco sopra, sono proposizioni: in entrambe l'unica variabile che appare, x, ha solo occorrenze vincolate. Invece, la formula "$\exists x(x > y)$" non è una proposizione, a causa dell'occorrenza libera di y. Possiamo modificare questa formula perché diventi chiusa? Certamente, il modo ovvio di farlo è quello di premettere un quantificatore che vincoli la variabile y: "$\exists y(\exists x(x > y))$" e "$\forall y(\exists x(x > y))$" sono proposizioni. Cosa significa tutto ciò in termini più semplici? Che *se una formula contiene variabili che non sono state introdotte da quantificatori* (in tutte le loro occorrenze) *allora questa formula non ha un valore di verità* e non ha senso stare a discutere sul fatto che sia vera o falsa. Per poterle attribuire un valore di verità dobbiamo prima 'quantificare', come si dice, le variabili libere che vi appaiono. Ovviamente abbiamo più modi di farlo, che portano, in genere, a formule molto diverse tra loro, come nel caso delle due formule $\exists y(\exists x(x > y))$ e $\forall y(\exists x(x > y))$ appena viste.

È bene insistere su questo punto: i quantificatori sono essenziali per la corretta espressione ed interpretazione delle formule in logica e più generalmente in matematica, ed è quindi importantissimo che siano sempre espressi, ed in modo non ambiguo.[21] Si invita chi legge a prendere la sana abitudine di farlo; la pratica di omettere o sottintendere quantificatori è una delle più frequenti cause di errori di ragionamento e, cosa forse più grave, di completa incomprensione di concetti matematici.

La seconda ragione per cui è bene cercare di familiarizzarsi con la nozione di occorrenza libera o vincolata di una variabile è che, nell'interpretazione di una formula, variabili libere e variabili vincolate giocano ruoli molto diversi. La questione è molto delicata e non facile da afferrare, non mi stupirei se il contenuto dei paragrafi seguenti risultasse poco comprensibile a chi legge, ma invito per lo meno a provare a rifletteci sopra.

Guardiamo alle sostituzioni. Non abbiamo potuto dare più che una idea intuitiva di come si effettui una sostituzione di un termine ad una variabile in una formula, ma una cosa che possiamo dire è che *nelle sostituzioni si opera solo sulle occorrenze libere delle variabili*. Se ci fermiamo a pensarci un attimo, questo non è strano. Infatti a nessuno (spero) verrebbe mai in mente di sostituire, ad esempio, 0 alla variabile x in "$\forall x(x > y)$" ottenendo "$\forall 0(0 > y)$", o magari "$\forall x(0 > y)$". Qualche esempio: nel linguaggio dell'aritmetica, consideriamo le tre formule φ, $\bar{\varphi}$ e ψ:

$$\varphi\colon\ \text{“}x > 1\text{”}; \qquad \bar{\varphi}\colon\ \text{“}\forall x(x > 1)\text{”}; \qquad \psi\colon\ \text{“}\forall x(x > 1) \wedge x = 7\text{”}.$$

Sostituendo ad x il numero 3 in ciascuna delle formule otteniamo le formule

$$\varphi(3)\colon\ \text{“}3 > 1\text{”}; \qquad \bar{\varphi}(3) = \bar{\varphi}(x)\colon\ \text{“}\forall x(x > 1)\text{”}; \qquad \psi(3)\colon\ \text{“}\forall x(x > 1) \wedge 3 = 7\text{”}.$$

Cosa è successo? In ciascuna delle formule abbiamo sostituito 3 alle occorrenze libere di x, ma non a quelle vincolate; è questa la regola generale. Nelle formule chiuse non appaiono variabili libere, quindi non c'è nulla da sostituire e per questo le sostituzioni lasciano invariate le formule chiuse. Come si vede, questo è il caso che si è verificato per la formula (chiusa) $\bar{\varphi}(x)$. In $\psi(x)$ l'unica occorrenza libera di x è l'ultima, quella che appare in "$x = 7$", quindi solo questa è stata sostituita.

Per dirla in modo grossolano ma comprensibile, una variabile libera è qualcosa che, nella formula, "rappresenta" un oggetto (e quindi può essere sostituita da un oggetto), una variabile vincolata invece no. Non per niente, per indicare una variabile con occorrenza vincolata si usa anche l'espressione 'variabile muta'.

Infine, un po' di terminologia. Un *predicato unario* nella variabile x è formula che non contenga occorrenze libere di variabili diverse di x. Quindi, se φ è una formula e x è una variabile, $\forall x(\varphi)$ è una proposizione esattamente quando φ è un predicato unario in x; lo stesso vale per $\exists x(\varphi)$ e $\exists! x(\varphi)$. Similmente, si dice che la formula φ è un predicato binario quando in essa appaiono al più due variabili con occorrenze libere[22], un predicato ternario è una formula in cui appaiono al più tre variabili con occorrenze libere, e così via.

---

[21] ad esempio, andrebbero evitate espressioni del tipo: "$f(x) < 4$, con $x > 0$" dove chi legge deve, per bene che vada, tirare ad indovinare se quel "con" rappresenta un quantificatore esistenziale o uno universale. Analogamente, in "…, per $x > 0$", non sempre è chiaro se quel "per" vada inteso come "per ogni" o "per almeno un". Il senso logico delle frasi, come si vede, cambia se si cambia l'interpretazione.

[22] attenzione: non due *occorrenze*, ma due variabili, con un numero arbitrario di occorrenze. Ad esempio, la formula "$(x < y) \vee ((x = y) \Rightarrow (x > 7))$", in cui x appare tre volte, è un predicato binario in x e y (nel linguaggio dell'aritmetica).

Osservazioni.

G.1. Torniamo sulla equivalenza che abbiamo dato come descrizione del quantificatore $\exists!$. Siano φ una formula e x, y due variabili, e assumiamo che y non appaia in φ. Se chiamiamo $\psi(x, y)$ la formula $\varphi(y) \Leftrightarrow y = x$, possiamo riscrivere l'equivalenza come $\exists! x(\varphi(x)) \iff \exists x(\forall y(\psi(x, y))$. Vogliamo esaminare il membro a destra di questa equivalenza. Per semplificare il discorso, supponiamo che φ sia un predicato unario in x, quindi che $\exists x(\forall y(\psi(x, y))$ sia una proposizione; il ragionamento è analogo nel caso generale. Quando è che questa proposizione è vera? Esattamente quando esiste *almeno* un a per il quale sia vera la formula (che è anch'essa chiusa) $\forall y(\psi(a, y))$; come sappiamo questo equivale a dire che è vera $\psi(a, b)$, cioè la formula $\varphi(b) \Leftrightarrow b = a$, per ogni possibile scelta di b. Tra le possibili scelte per b c'è anche a; la formula diventa in questo caso particolare $\varphi(a) \Leftrightarrow a = a$. Poiché $a = a$ è vera, questa equivale a $\varphi(a)$. Se invece scegliamo come b un qualsiasi oggetto diverso da a, allora $b = a$ è falsa, quindi $\varphi(b) \Leftrightarrow b = a$ equivale alla negazione di $\varphi(b)$.

In definitiva, abbiamo mostrato che la formula $\exists x(\forall y(\psi(x, y))$ è vera se e solo se esiste un a per il quale è vera $\varphi(a)$ e, contemporaneamente, è falsa $\varphi(b)$ per ogni b diverso da a. Questo è precisamente quello che volevamo esprimere col quantificatore $\exists!$; è quindi giustificata l'idea di descrivere formalmente questo quantificatore come abbiamo fatto.

G.2. Non abbiamo descritto in dettaglio le sostituzioni, abbiamo solo avvertito che la nozione è solo ingannevolmente semplice. Un esempio può dare l'idea delle difficoltà che possono sorgere (ma, niente paura, si risolvono). È lecito sostituire a variabili altre variabili. Consideriamo la formula $\exists x(x \neq y)$ nella variabili x (vincolata) e y (libera). Cosa succederebbe se sostituissimo 'meccanicamente' y con x in questa formula?

G.3. Questa osservazione fornisce un suggerimento pratico, mirato a semplificare la scrittura delle formule. Una regola (molto intuitiva) del calcolo dei predicati afferma che se si "cambia nome" alle variabili vincolate in una formula si ottiene una formula equivalente. Più precisamente, data una formula φ in cui appare una variabile x, se y è una variabile che non appare in φ, la formula ottenuta scrivendo y al posto di x in ogni occorrenza vincolata di x in φ è equivalente a φ. Per esempio, "$\forall x(x + 1 > x)$" e "$\forall y(y + 1 > y)$" sono equivalenti. Usando questa regola, è possibile riscrivere in modo equivalente qualsiasi formula in modo da evitare che la stessa variabile appaia sia libera che vincolata, con gran vantaggio per la chiarezza. Ad esempio, la già menzionata formula "$(\forall x(x + 1 > x)) \vee (x = 0)$" dell'aritmetica si potrebbe equivalentemente riscrivere come "$(\forall y(y + 1 > y)) \vee (x = 0)$", sicuramente più facile da leggere.

Quantificatori ristretti. Nella pratica matematica si incontrano con gran frequenza espressioni del tipo "$(\forall x \in S)(\varphi)$" o "$(\exists x > 0)(\varphi)$" (le parentesi non sono tutte necessarie, ma rendono le formule più facili da leggere; come si sarà immaginato qui φ è una formula e x una variabile, e S è un insieme), in cui il quantificatore è accompagnato da una condizione che limita l'ambiente in cui la variabile possa assumere i suoi valori. Queste espressioni hanno ovvie interpretazioni, ma è bene sapere che sono semplicemente abbreviazioni di formule in cui i quantificatori sono usati nel modo indicato nella sezione precedente, ed è bene sapere di quali formule sono abbreviazioni. La prima formula può essere definita in questo modo:

$$(\forall x \in S)(\varphi) : \iff \forall x(x \in S \Rightarrow \varphi)$$

(i due punti che precedono $\iff$ ci ricordano solo che questa equivalenza, o meglio l'affermazione che vale questa equivalenza, è stabilita come definizione dell'espressione a sinistra). Come spesso accade, non essersi accontentati di una idea intuitiva ma aver cercato una definizione precisa non è un atto di pignoleria fine a se stesso, ma comporta un utile vantaggio. In questo caso, ci permette di chiarire in modo molto semplice un punto che spesso sfugge agli studenti: cosa accade quando S è l'insieme vuoto? La risposta è:

per ogni predicato unario φ nella variabile x, la proposizione $(\forall x \in \varnothing)(\varphi)$ è vera.[23]

Come mai? Stando alla nostra definizione "$(\forall x \in \varnothing)(\varphi)$" significa "$\forall x(x \in \varnothing \Rightarrow \varphi)$". Ora, qualunque sia l'oggetto a, la formula $a \in \varnothing$ è falsa (l'insieme vuoto non ha elementi: è questa la sua definizione) quindi l'implicazione "$a \in \varnothing \Rightarrow \varphi(a)$" ha l'antecedente falso e quindi è vera. Dunque, se sostituiamo a ad x in "$x \in \varnothing \Rightarrow \varphi$" otteniamo certamente una formula vera. Pertanto "$\forall x(x \in \varnothing \Rightarrow \varphi)$", ovvero

[23] ricordiamo che se la formula φ non fosse un predicato unario in x, cioè se φ contenesse una variabile libera diversa da x, allora $(\forall x \in \varnothing)(\varphi)$ non sarebbe una proposizione, quindi non sarebbe né vera né falsa.

"$(\forall x \in \varnothing)(\varphi)$", è vera, come si voleva dimostrare. Possiamo a questo punto dire che, a meno che non esistano cavalli[24] verdi, la frase "ogni cavallo verde ha otto zampe" è vera.

Discorso analogo vale per altre restrizioni che possono essere imposte alla variabile quantificata. Ad esempio, $(\forall x > 0)(\varphi)$ significa $\forall x(x > 0 \Rightarrow \varphi)$.

Se cambiamo quantificatore la definizione è diversa:

$$(\exists x \in S)(\varphi) : \iff \exists x((x \in S) \wedge \varphi)$$

e qui non ci dovrebbero essere difficoltà: "esiste x in S tale che ..." significa proprio "esiste x tale che x sia in S e ..." . Ovviamente, nella solita ipotesi che φ sia un predicato unario in x, questa formula è sicuramente una proposizione falsa quando $S = \varnothing$.

Abbiamo introdotto i quantificatori $\forall$ ed $\exists$ suggerendo un'analogia tra essi ed i connettivi $\wedge$ e $\vee$, cioè che i quantificatori in qualche modo corrispondano a forme più generali di congiunzione (nel caso del quantificatore universale) e disgiunzione (per quello esistenziale). Questa analogia si può effettivamente rendere precisa e verificare nel caso dei quantificatori ristretti ad insiemi finiti e non vuoti. Se S è appunto un insieme finito e $S \neq \varnothing$, se φ è una formula e x una variabile, è chiaro che la formula $(\forall x \in S)(\varphi(x))$ è equivalente a $\bigwedge_{a \in S} \varphi(a)$, cioè a $\varphi(a_1) \wedge \varphi(a_2) \wedge \cdots \wedge \varphi(a_k)$, dove $a_1, \ldots a_k$ sono gli elementi di S, mentre $(\exists x \in S)(\varphi(x))$ è equivalente a $\bigvee_{a \in S} \varphi(a)$.[25]

Si può, a questo punto, tornare all'esempio della frase "per ogni numero intero x compreso tra 1 e 3 si ha che se $x > 2$ allora $x > 1$" discussa nella sezione in cui è stato introdotto il connettivo di implicazione. Come si può ora riconoscere, questa frase non è altro che un modo per rendere verbalmente la formula $(\forall x \in \{1, 2, 3\})(x > 2 \Rightarrow x > 1)$; questa è una formula introdotta da un quantificatore universale ristretto ad un insieme di tre elementi, quindi si riduce ad una congiunzione tra tre formule, e sotto questo aspetto l'avevamo studiata.

6. Qualche regola d'uso

Esiste un gran numero di regole del calcolo dei predicati che permettono di manipolare formule contenenti quantificatori. Si tratta per lo più di regole estremamente intuitive; una è quella data nell'Osservazione G.3, ne vedremo altre. Spesso queste regole sono enunciate dichiarando la validità di determinate implicazioni. Anche in questa sezione, ma non lo ripeteremo ogni volta, le lettere x, y e z indicano sempre variabili, φ e ψ sono invece formule.

Quantificatori multipli. Innanzitutto, può capitare di avere più quantificatori consecutivi; un esempio lo abbiamo già visto con la formula a secondo membro della equivalenza che descrive formalmente $\exists!$. Abbiamo formule del tipo $\forall x(\forall y(\cdots(\varphi)\cdots)$ o $\exists x(\exists y(\cdots(\varphi)\cdots)$, in cui è lo stesso quantificatore a ripetersi; in questi casi l'ordine in cui appaiono i quantificatori è irrilevante nel senso che, ad esempio, $\forall x(\forall y(\varphi))$ e $\forall y(\forall x(\varphi))$ sono equivalenti. Si usa scrivere, per brevità, $\forall x, y, \ldots, z\,(\varphi)$ invece di $\forall x(\forall y(\cdots \forall z(\varphi)\cdots)$ e $\exists x, y, \ldots, z\,(\varphi)$ invece di $\exists x(\exists y(\cdots \exists z(\varphi)\cdots)$. Diverso è il caso in cui appaiono sia il quantificatore esistenziale che quello universale. Le formule "$\forall x(\exists y(\varphi))$" e "$\exists y(\forall x(\varphi))$" non sono in generale equivalenti. La prima afferma che, scelto comunque un termine a, ne esiste almeno uno, b, dipendente, in generale, dalla scelta di a, per il quale si abbia $\varphi(a, b)$. La seconda formula dice qualcosa in più: che si ha la stessa situazione ma, questa volta, si può scegliere b indipendentemente dalla scelta di a: esiste un particolare b per il quale si abbia $\varphi(a, b)$ per ogni possibile scelta di a. Dunque, vale sempre l'implicazione

$$\exists y(\forall x(\varphi)) \Longrightarrow \forall x(\exists y(\varphi))$$

ma, in generale, non vale l'implicazione inversa. Un esempio può aiutare: nel linguaggio dell'aritmetica, sia $\varphi(x, y)$ la formula $x < y$. La prima delle nostre formule diventa

$$\forall x(\exists y(x < y)),$$

[24] si intende: cavalli *vivi*.

[25] per una convenzione di uso universale, se S ha un solo elemento, cioè $k = 1$ e $S = \{a_1\}$, sia $\bigwedge_{a \in S} \varphi(a)$ che $\bigvee_{a \in S} \varphi(a)$ valgono $\varphi(a_1)$. In verità la stessa convenzione permette di estendere questa notazione anche al caso in cui $S = \varnothing$, stabilendo che $\bigwedge_{a \in \varnothing} \varphi(a)$ e $\bigvee_{a \in \varnothing} \varphi(a)$ indicano una formula vera ed una falsa, rispettivamente. Con questa ulteriore convenzione le equivalenze $((\forall x \in S)(\varphi(x))) \Leftrightarrow \bigwedge_{a \in S} \varphi(a)$ e $((\exists x \in S)(\varphi(x))) \Leftrightarrow \bigvee_{a \in S} \varphi(a)$ continuano a valere, anche nel caso in cui $S = \varnothing$.

che afferma che per ogni numero esiste un numero più grande. Questa è una proposizione vera: se a è un numero intero, $a+1$ è un numero intero maggiore di a, quindi $\varphi(a, a+1)$ è vera.[26] La seconda formula è invece

$$\exists y(\forall x(x < y)),$$

che afferma che esiste un intero (quello che andrebbe sostituito ad y) maggiore di tutti gli interi; questa è una proposizione falsa.

Negazione di quantificatori. Come si nega una formula universale? E come si nega una formula esistenziale? Dovrebbe bastare il buon senso a suggerirlo: per stabilire che sia falsa la frase "ogni cittadino italiano si chiama Mario" basta osservare che esiste qualche cittadino italiano che non si chiama Mario; anche se ce ne sono alcuni che effettivamente si chiamano Mario la frase è ugualmente falsa, perché *non tutti* hanno quel nome. Sarebbe un errore pensare che per rendere falsa la frase in questione bisognerebbe che *nessuno* dei cittadini italiani si chiamasse Mario. Questo esempio suggerisce che la negazione di una frase universale sia una frase esistenziale (dove è negata la formula oggetto della quantificazione). È proprio così; per ogni formula φ ed ogni variabile x vale:

$$\big(\neg(\forall x(\varphi))\big) \iff \big(\exists x(\neg\varphi)\big).^{27} \qquad \text{(negazione di formule universali)}$$

Simmetricamente, pensiamo che la frase "esiste un cittadino italiano di nome Xwas" sia falsa, non perché esiste un cittadino italiano che non si chiama Xwas, ma perché *nessun* cittadino italiano si chiama Xwas, o, per dirla in modo più utile ai nostri scopi, anche se meno naturale, *ogni* cittadino italiano *non* si chiama Xwas.[28] La regola di negazione per le formule esistenziali è, infatti:

$$\big(\neg(\exists x(\varphi))\big) \iff \big(\forall x(\neg\varphi)\big). \qquad \text{(negazione di formule esistenziali)}$$

Vale la pena di osservare che questa regola segue dalla precedente e dalle tautologie della negazione e della commutatività dell'equivalenza. Infatti, "$\big(\neg(\exists x(\varphi))\big) \iff \big(\forall x(\neg\varphi)\big)$" equivale, per queste tautologie, a "$\big(\exists x(\varphi)\big) \iff \big(\neg(\forall x(\neg\varphi))\big)$" e quindi a "$\big(\neg(\forall x(\neg\varphi))\big) \iff \big(\exists x(\varphi)\big)$". Questa (per la tautologia della doppia negazione) non è altro che la regola per la negazione delle formule universali applicata con $\neg\varphi$ al posto di φ.

Se torniamo all'analogia tra i quantificatori $\forall$ ed $\exists$ ed i connettivi $\wedge$ e $\vee$, possiamo pensare a queste regole di negazione come all'analogo delle leggi di De Morgan.

Notiamo che queste regole di negazione stabiliscono anche l'interdipendeza di $\forall$ ed $\exists$, nel senso che mostrano come l'uno dei due si possa definire in termini dell'altro; ad esempio, potremmo assumere dato $\forall$ e definire $\exists$ usando l'equivalenza $\big(\exists x(\varphi)\big) \Leftrightarrow \big(\neg(\forall x(\neg\varphi))\big)$. La situazione, come si vede, è simile a quella dei connettivi proposizionali: abbiamo introdotto due simboli ($\forall$ e $\exists$) ma ci siamo accorti che, volendo, potremmo fare a meno di uno dei due.

Non sorprendentemente, per formule con quantificatori ristretti abbiamo regole di negazione simili a quelle per i quantificatori non ristretti (le notazioni sono quelle solite; in particolare, S indica un insieme):

$$\neg(\forall x \in S)(\varphi) \iff \exists(x \in S)(\neg\varphi) \qquad \text{e} \qquad \neg(\exists x \in S)(\varphi) \iff \forall(x \in S)(\neg\varphi).$$

Il senso è chiaro, ma è utile e istruttivo verificare queste formule. Per la prima: $(\forall x \in S)(\varphi)$ significa $\forall x(x \in S \Rightarrow \varphi)$, la cui negazione è $\exists x(\neg(x \in S \Rightarrow \varphi))$. Ricordiamo come si nega un'implicazione: affermando l'antecedente e contemporaneamente negando il conseguente. Quindi $\neg(\forall x \in S)(\varphi)$ equivale a $\exists x((x \in S) \wedge (\neg\varphi))$. Ma questa formula, come abbiamo visto sopra, è proprio quella che viene abbreviata con $\exists(x \in S)(\neg\varphi)$. La verifica è così completa. La seconda formula si può dimostrare dalla prima (analogamente a quanto fatto nel caso dei quantificatori non ristretti) oppure in modo diretto, come si suggerisce di fare in uno dei prossimi esercizi.

---

[26] seguiamo qui una convenzione standard: avendo indicato la formula φ come $\varphi(x, y)$, abbiamo specificato l'ordine in cui consideriamo le variabili. Dunque $\varphi(a, a+1)$ sarà la formula ottenuta sostituendo a ad x e $a+1$ ad y, non viceversa.

[27] stiamo facendo largo uso di parentesi, sperando che questo aiuti nella lettura. Potremmo però anche farne a meno. Ad esempio, questa formula si potrebbe anche scrivere $\neg\forall x(\varphi) \iff \exists x(\neg\varphi)$, senza nessuna ambiguità; si vedano le tautologie della negazione dell'equivalenza per il ruolo di $\neg$ nella sua prima occorrenza.

[28] spero di non essere smentito, su questo punto, da un'indagine anagrafica.

Un errore da evitare. Qualunque sia il termine a, due (ovvie) regole[29] stabiliscono la catena di implicazioni:

$$\big(\forall x(\varphi(x))\big) \Longrightarrow \varphi(a) \Longrightarrow \big(\exists x(\varphi(x))\big),$$

da cui segue $\big(\forall x(\varphi(x))\big) \Rightarrow \big(\exists x(\varphi(x))\big)$ (a condizione che si ammetta, come in genere si fa, che esista almeno un oggetto a cui il linguaggio si riferisce). Nel caso in cui i quantificatori siano ristretti la situazione può essere diversa. L'implicazione $\big((\forall x \in S)(\varphi(x))\big) \Rightarrow \big((\exists x \in S)(\varphi(x))\big)$ vale certamente se S è un insieme non vuoto, *ma non se S è l'insieme vuoto.* Per convincercene, consideriamo il caso in cui φ sia un predicato unario in x. Se $S = \varnothing$ l'antecedente $(\forall x \in \varnothing)(\varphi(x))$ della nostra implicazione è vero (si veda la discussione su queste formule nella sezione sui quantificatori ristretti) ed il conseguente $(\exists x \in \varnothing)(\varphi(x))$ è falso, quindi l'implicazione è falsa.

Capita non tanto di rado di trovare errori di ragionamento dovuti proprio a questa disattenzione: dal fatto che tutti gli elementi di un insieme abbiano una certa proprietà si deduce l'esistenza di almeno un elemento con quella proprietà. Questo passaggio non è lecito a meno di non essersi assicurati che l'insieme in questione non è vuoto. Per esempio, abbiamo detto che ogni cavallo verde ha otto zampe, da questo non possiamo certamente dedurre che esistano cavalli verdi con otto zampe!

Esercizi.

H.1. Vero o falso? E perché? Questo è un esercizio di corretta lettura ed interpretazione di formule.

(a) $(\forall x \in \mathbb{N})(x + 1 < x \Rightarrow x^2 = 1)$.
(b) $\exists x \in \mathbb{N}(\forall y \in \mathbb{N}(x \leq y))$.
(c) $\forall x \in \mathbb{N}(\exists y \in \mathbb{N}(x < y))$.
(d) $\forall x \in \mathbb{N}(\exists y \in \mathbb{N}((x = y + 1) \Rightarrow (x < y)))$.
(e) $\exists x \in \mathbb{N}(\forall y \in \mathbb{N}((x < y) \vee (y < x) \vee (y = 11)))$.
(f) $\exists x \in \mathbb{N}(\forall y \in \mathbb{Z}((x \neq y) \Rightarrow (x < y)))$.
(g) Ogni numero reale il cui quadrato sia negativo è maggiore di 10^{327}.

H.2. Una regola (molto intuitiva) del calcolo dei predicati stabilisce l'equivalenza

$$\big(\forall x(\varphi \wedge \psi)\big) \iff \big((\forall x(\varphi)) \wedge (\forall x(\psi))\big),$$

qualsiasi siano le formule φ e ψ (ovviamente x indica una variabile). Oppure mi sbaglio? Anche questo è un esercizio di lettura! Può essere utile pensare a frasi come "ogni giorno mangio una pizza e vado al cinema" e "ogni giorno mangio una pizza e ogni giorno vado al cinema". Con le stesse notazioni, confrontare tra loro le formule "$\forall x(\varphi \vee \psi)$" e "$(\forall x(\varphi)) \vee (\forall x(\psi))$".

Ripetere l'esercizio sostituendo, in tutte le formule, "$\forall$" con "$\exists$".

H.3. Verificare (in modo diretto) la formula $\neg(\exists x \in S)(\varphi) \iff \forall(x \in S)(\neg\varphi)$.

H.4. Si scriva la negazione di $\exists! x(\varphi)$. Sono possibili più risposte, diverse nella forma ma equivalenti tra loro.

H.5. Si neghi ciascuna delle le formule (le notazioni sono le solite):

(a) $\forall x(\exists y(\varphi(x, y) \Rightarrow \psi(x, y)))$;
(b) $\exists x(\varphi(x) \wedge \forall y(\neg\psi(x, y)))$;
(c) $\forall x, y(\exists z(z \neq y \wedge \varphi(x, z)))$;

H.6. Si neghi ciascuna delle frasi:

(a) Ogni volta che vedo Astolfo, litighiamo.
(b) Una volta ho visto Astolfo ed ho bevuto un caffé.
(c) Tutti i giorni della prossima settimana andrò al cinema, ed uno di quei giorni andrò in pizzeria.

7. Insiemi

Sia $\varphi = \varphi(x)$ un predicato unario nella variabile x. Si indica col simbolo $\{x \mid \varphi\}$ la totalità (potremmo anche dire: la collezione, la classe; stiamo usando questi termini in modo del tutto informale) degli oggetti a che, sostituiti ad x in φ, rendono φ vera (vale a dire: tali che $\varphi(a)$ sia una formula vera). Questa totalità si chiama anche l'*estensione* di φ. Si può pensare a φ come espressione di una 'proprietà' che un oggetto può soddisfare oppure no, allora la sua estensione $\{x \mid \varphi\}$ è la totalità degli oggetti che soddisfano (verificano, hanno) la proprietà espressa da φ. Ad esempio, la formula "$(x \in \mathbb{N}) \wedge (x < 3)$",

[29] la prima delle quali si chiama *regola di specializzazione*

esprime la proprietà di "essere un numero naturale minore di 3", e $\{x \mid (x \in \mathbb{N}) \wedge (x < 3)\}$ è costituito dai numeri 0, 1 e 2.

La teoria degli insiemi tratta di enti matematici, appunto gli insiemi, che formalizzano l'idea intuitiva di 'aggregato di oggetti'; gli assiomi di questa teoria regolano in modo preciso il modo in cui su questi enti si può operare. Un tentativo (quello del logico tedesco Gottlob Frege) di fondare l'intera teoria sull'idea che l'estensione di ogni predicato unario si possa considerare come insieme fallì molto presto, non appena si scoprì che questa assunzione porta necessariamente a contraddizioni.[30] In altri termini: non sempre l'estensione $\{x \mid \varphi(x)\}$ di un predicato φ (unario, in x) è un insieme. Detto in modo ancora diverso, esistono 'proprietà' perfettamente ragionevoli e ben definite (cioè espresse da un predicato unario) tali che, sfortunatamente, non esista l'*insieme* degli oggetti che le verificano. Ad esempio, tutti gli studenti che sono stati sottoposti ad una qualche infarinatura di teoria degli insiemi (come questa!) dovrebbero sapere che *non esiste l'insieme di tutti gli insiemi*; si vedano a questo proposito l'Esempio I.2 e l'Esercizio I.3.

Qualcosa dell'idea di Frege, però, si salva. Dato un predicato unario φ, se proviamo a selezionare tutti gli oggetti che verificano φ è possibile, lo abbiamo appena detto, che non si ottenga un insieme; ma se noi abbiamo già a disposizione un insieme S e limitiamo la selezione ai soli elementi di S (lasciando perdere tutto ciò che non appartenga ad S), allora sicuramente otteniamo un insieme: l'insieme degli elementi di S che verificano φ. Ce lo assicura uno degli assiomi della teoria degli insiemi, l'*assioma di separazione* (o di *comprensione*; più precisamente, si tratta di uno schema di assiomi, ma non entriamo in questa sottigliezza). In modo più esplicito: dati un insieme S ed un predicato unario φ nella variabile x, la formula "$(x \in S) \wedge \varphi$" è ancora un predicato unario in x;[31] l'assioma di separazione dice che, in queste circostanze, l'estensione $\{x \mid (x \in S) \wedge \varphi(x)\}$ di questo predicato è un insieme. Per indicare questo insieme si usa, in genere, una notazione più compatta: $\{x \in S \mid \varphi(x)\}$. L'insieme così ottenuto è ovviamente una parte di S.

Un altro assioma che conviene menzionare è l'assioma di *estensionalità*. Questo assioma stabilisce che gli insiemi sono completamente determinati dai loro elementi, ovvero: dati un insieme A ed un insieme B, si ha $A = B$ se e solo se A e B hanno esattamente gli stessi elementi—si veda l'Esercizio I.5. Abbiamo implicitamente fatto uso di questo assioma quando abbiamo descritto $\{x \mid \varphi(x)\}$ (quando è un insieme) e $\{x \in S \mid \varphi(x)\}$ specificando solo quali sono i loro elementi.

Torniamo sul significato di queste espressioni. Trattiamo come oggetti matematici 'veri e propri' gli insiemi, ma non le estensioni di predicati che non siano insiemi. Quindi, continuando ad usare le notazioni che abbiamo introdotto nei paragrafi precedenti, per noi $\{x \mid \varphi(x)\}$ esiste come oggetto della matematica se è un insieme, non esiste altrimenti. In effetti, più in generale, nella teoria degli insiemi standard si assume abitualmente che *non esistano enti matematici che non siano insiemi*.[32] Scriviamo dunque formule come $A = \{x \mid \varphi(x)\}$ solo nel caso in cui $\{x \mid \varphi(x)\}$ sia un insieme. In questo caso,

$$\text{l'uguaglianza} \qquad A = \{x \mid \varphi(x)\} \qquad \text{equivale a:} \qquad \forall x(x \in A \Leftrightarrow \varphi(x)).$$

Invece la formula $A = \{x \in S \mid \varphi(x)\}$ ha sempre senso, perché il secondo membro è un insieme, e

$$\text{l'uguaglianza} \qquad A = \{x \in S \mid \varphi(x)\} \qquad \text{equivale a:} \qquad \forall x(x \in A \Leftrightarrow ((x \in S) \wedge \varphi(x))).$$

Esempi, Osservazioni, Esercizi (alcuni non facili).

I.1. Usando l'assioma di estensionalità verificare che esiste solo un insieme vuoto.

I.2. Abbiamo detto che se φ è un predicato unario, non necessariamente esiste l'insieme $\{x \mid \varphi(x)\}$ degli oggetti che verificano φ. Per convincerci di questo fatto, esaminiamo un esempio. Scegliamo come φ la formula $x \notin x$ e supponiamo che esista l'insieme $\{x \mid x \notin x\}$, che possiamo chiamare R. Stando al significato che abbiamo stabilito per questa notazione, abbiamo: $\forall x(x \in R \Leftrightarrow x \notin x)$. La regola di specializzazione, applicata sostituendo di R a x, fornisce allora $R \in R \Leftrightarrow R \notin R$. Questa è evidentemente una contraddizione; dobbiamo concludere che l'insieme $\{x \mid x \notin x\}$ non esiste.

Questo esempio contiene la cosidetta *Antinomia* (o *Paradosso*) *di Russell* (da ciò l'uso della lettera R) ed ha una bella ed istruttiva storia alle spalle (anzi, almeno due).

[30] Stiamo rendendo breve una storia che è molto più lunga e complessa. In particolare, il primo sistema di assiomi per la teoria degli insiemi, quello di Zermelo (1908), è storicamente successivo all'emersione delle contraddizioni a cui stiamo accennando.

[31] come già capitato in casi analoghi, ci stiamo prendendo una piccola libertà: trattiamo in questa formula S come un simbolo di costante. Per una versione meglio formulata dell'assioma di separazione si veda l'Esercizio I.4.

[32] Esistono teorie degli insiemi alternative, un po' più sofisticate, nelle quali le cose non stanno così e si può dare un significato matematico preciso a $\{x \mid \varphi(x)\}$ anche nel caso in cui questo non sia un insieme.

I.3. Usando l'osservazione precedente (I.2) e l'assioma di separazione, dimostrare che non esiste l'insieme di tutti gli insiemi. Cosa sappiamo dire su $\{x \mid x = x\}$?
I.4. Sia φ un predicato unario in x. La formula $\forall y \exists z \forall x\big((x \in z) \Leftrightarrow \big((x \in y) \wedge \varphi\big)\big)$ è uno dei modi per esprimere l'assioma di separazione 'applicato' a φ (per meglio dire: l'istanza dell'assioma di separazione per φ). Verificarlo; è un ulteriore esercizio di lettura.
I.5. Assumendo che non esistano oggetti che non siano insiemi l'assioma di estensionalità è invece espresso dalla formula: $(\forall y, z)(y = z \iff (\forall x(x \in y \Leftrightarrow x \in z)))$. Verificarlo.

Formule insiemistiche. La vaga ed imperfetta corrispondenza tra predicati unari ed insiemi, di cui abbiamo parlato nella sezione precedente, può essere comunque usata per tradurre risultati del calcolo proposizionale (come la validità di tautologie) in formule della teoria degli insiemi. Questa sorta di traduzione si può ottenere facendo corrispondere relazioni o operazioni insiemistiche a connettivi proposizionali, come vedremo con diversi esempi.

Come punto di partenza, osserviamo che l'idea di estensione di un predicato, discussa nella sezione precedente, si può in un certo senso invertire. Infatti, ogni insieme A si può considerare come l'estensione del predicato "$x \in A$", vale a dire: $A = \{x \mid x \in A\}$.[33] Ora, se A e B sono insiemi, l'assioma di estensionalità ci dice che vale:

$$A = B \iff \forall x(x \in A \Leftrightarrow x \in B),$$

mentre, per definizione di inclusione,

$$A \subseteq B \iff \forall x(x \in A \Rightarrow x \in B).$$

Queste due formule suggeriscono che, nello stesso senso, informale in cui facciamo corrispondere (ovvero 'traduciamo') i predicati "$x \in A$" e "$x \in B$" con A e B, possiamo far corrispondere i connettivi $\Leftrightarrow$ e $\Rightarrow$ ai simboli di uguaglianza e di inclusione tra insiemi. Ci vuole poco a convincersi di come, nella stessa ottica, la tautologia della doppia implicazione si traduca nella ben nota regoletta insiemistica della doppia inclusione. A titolo di esempio, verifichiamolo in dettaglio, senza timore di essere troppo pignoli. La tautologia assicura che "$x \in A \Leftrightarrow x \in B$" sia equivalente a "$(x \in A \Rightarrow x \in B) \wedge (x \in B \Rightarrow x \in A)$". Inoltre, una delle tante regole del calcolo dei predicati (si veda l'Esercizio H.2) stabilisce l'equivalenza

$$\big(\forall x(\varphi \wedge \psi)\big) \iff \big((\forall x(\varphi)) \wedge (\forall x(\psi))\big). \qquad (*)$$

qualsiasi siano le formule φ e ψ. Abbiamo allora le equivalenze (alcune scritte in verticale, questa volta, e giustificate da un commento a destra):

$$\begin{aligned}
A = B &\iff \forall x(x \in A \Leftrightarrow x \in B) \\
&\qquad\Updownarrow \qquad\qquad\qquad\qquad\qquad\qquad \text{(tautologia)} \\
&\forall x\big((x \in A \Rightarrow x \in B) \wedge (x \in B \Rightarrow x \in A)\big) \\
&\qquad\Updownarrow \qquad\qquad\qquad\qquad\qquad\qquad \text{(regola } (*)\text{)} \\
&\big(\forall x(x \in A \Rightarrow x \in B)\big) \wedge \big(\forall x(x \in B \Rightarrow x \in A)\big) \\
&\qquad\Updownarrow \qquad\qquad\qquad\qquad\qquad\qquad \text{(definizione di inclusione)} \\
&(A \subseteq B) \wedge (B \subseteq A).
\end{aligned}$$

Quindi, e non è una sorpresa, $A = B$ se e solo se $A \subseteq B$ e $B \subseteq A$; questa è la regola della doppia inclusione. In modo analogo, la tautologia della transitività dell'implicazione fornisce la *transitività dell'inclusione*:

$$(\forall A, B, C)\big(((A \subseteq B) \wedge (B \subseteq C)) \Rightarrow (A \subseteq C)\big);$$

è un utile esercizio verificarlo in dettaglio.

Abbiamo fatto corrispondere i simboli di uguaglianza e inclusione ai connettivi di equivalenza e di implicazione; è chiaro cosa si possa far corrispondere ai connettivi di congiunzione e disgiunzione: le operazioni di intersezione e di unione (binarie). Questo perché, scelti comunque gli insiemi A e B, si ha

$$\forall x\big(x \in A \cap B \iff ((x \in A) \wedge (x \in B))\big) \qquad \text{e} \qquad \forall x\big(x \in A \cup B \iff ((x \in A) \vee (x \in B))\big),$$

[33] ovviamente questa non sarebbe accettata come una vera e propria descrizione di A. Il discorso su questo punto andrebbe approfondito, ma così si andrebbe molto al là dei nostri scopi. Osserviamo ancora (vedi la nota 31) che nella formula "$x \in A$" trattiamo A come una costante, similmente faremo in formule analoghe, dove altri insiemi appaiono al posto di A.

quindi il predicato di appartenenza ad $A \cap B$ equivale alla congiunzione del predicato di appartenenza ad A e di quello di appartenenza ad B, mentre il predicato di appartenenza ad $A \cup B$ equivale alla disgiunzione di questi due.[34] Dalle tautologie di idempotenza, commutatività e associatività (pag. 7) e dalle leggi distributive (pag. 8) per $\wedge$ e $\vee$ si ottengono dunque le analoghe proprietà per le operazioni di unione e intersezione tra insiemi: per ogni A, B, C si ha:

$$A = A \cap A, \qquad A \cap B = B \cap A, \qquad A \cap (B \cap C) = (A \cap B) \cap C,$$
$$A = A \cup A, \qquad A \cup B = B \cup A, \qquad A \cup (B \cup C) = (A \cup B) \cup C$$

e

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

Ad esempio, per la commutatività di $\wedge$ abbiamo $\big((x \in A) \wedge (x \in B)\big) \iff \big((x \in B) \wedge (x \in A)\big)$; ma in questa equivalenza il primo membro equivale a $x \in A \cap B$, il predicato da appartenenza ad $A \cap B$, il secondo membro equivale a $x \in B \cap A$, il predicato da appartenenza ad $B \cap A$. Quindi questi due predicati sono equivalenti e così $A \cap B = B \cap A$ per l'assioma di estensionalità. In modo analogo si ragiona per le altre uguaglianze.

Il connettivo di negazione presenta invece una difficoltà: se A è un insieme allora $\{x \mid x \notin A\}$, l'estensione della negazione del predicato di appartenenza ad A, non è un insieme (si veda l'Esercizio J.3). Dunque, non abbiamo a disposizione una immediata 'traduzione' insiemistica di $\neg$. Assegnati comunque due insiemi A e B, abbiamo però l'insieme $A \smallsetminus B = \{x \in A \mid x \notin B\}$, e questo ci permette comunque di tradurre in formule insiemistiche tautologie sulla negazione.

Ancora De Morgan. Vediamo il caso delle leggi di De Morgan. Siano A, B e C insiemi, e chiamiamo α, β e γ i corrispondenti predicati di appartenenza nella variabile x: α è "$x \in A$", β è "$x \in B$" e γ è "$x \in C$". Allora "$x \in A \smallsetminus (B \cap C)$" equivale ad $\alpha \wedge (\neg(\beta \wedge \gamma))$. Ora, utilizzando la prima delle leggi di De Morgan e poi una delle leggi distributive, abbiamo:

$$\big(\alpha \wedge (\neg(\beta \wedge \gamma))\big) \iff \big(\alpha \wedge ((\neg\beta) \vee (\neg\gamma))\big) \iff \big((\alpha \wedge (\neg\beta)) \vee (\alpha \wedge (\neg\gamma))\big).$$

Ricordando le definizioni di α, β e γ, vediamo che l'ultima formula in questa catena equivale a "$x \in (A \smallsetminus B) \cup (A \smallsetminus C)$". Quindi "$x \in A \smallsetminus (B \cap C)$" e "$x \in (A \smallsetminus B) \cup (A \smallsetminus C)$" sono equivalenti. Similmente, "$x \in A \smallsetminus (B \cup C)$" equivale ad $\alpha \wedge ((\neg\beta) \wedge (\neg\gamma))$, quindi ad $(\alpha \wedge (\neg\beta)) \wedge (\alpha \wedge (\neg\gamma))$, cioè a "$x \in (A \smallsetminus B) \cap (A \smallsetminus C)$". Abbiamo così due importanti formule, che, analogamente alle tautologie, sono note come *formule di De Morgan*: scelti comunque gli insiemi A, B e C,

$$A \smallsetminus (B \cap C) = (A \smallsetminus B) \cup (A \smallsetminus C)$$
$$A \smallsetminus (B \cup C) = (A \smallsetminus B) \cap (A \smallsetminus C). \qquad \text{(De Morgan)}$$

Differenza simmetrica. Definiamo l'operazione insiemistica $\triangle$ di *differenza simmetrica* come l'operazione corrispondente alla disgiunzione esclusiva; poniamo dunque, per ogni A e B,

$$A \triangle B := \{x \mid (x \in A) \text{ XOR } (x \in B)\}.$$

Questa operazione ha proprietà algebriche notevoli che non sono evidenti a prima vista; per questo essa assume un ruolo centrale per lo studio di strutture importanti in informatica, come gli anelli booleani.

Le tautologie che abbiamo chiamato esplicitazione di XOR:

$$(p \text{ XOR } q) \iff \big((p \wedge (\neg q)) \vee (q \wedge (\neg p))\big) \iff \big((p \vee q) \wedge (\neg(p \wedge q))\big)$$

dànno facilmente (chi legge è invitato a verificarlo):

$$A \triangle B = (A \smallsetminus B) \cup (B \smallsetminus A) = (A \cup B) \smallsetminus (B \cap A),$$

mentre la commutatività e l'associatività di XOR e la distributività di $\wedge$ rispetto a XOR forniscono, ancora più direttamente, la commutatività e l'associatività di $\triangle$ e la distributività di $\cap$ rispetto a $\triangle$. Per ogni A, B, C, abbiamo, cioè:

$$A \triangle B = B \triangle A; \qquad A \triangle (B \triangle C) = (A \triangle B) \triangle C; \qquad A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C).$$

[34] va aggiunto che $A \cap B = \{x \mid (x \in A) \wedge (x \in B)\} = \{x \in A \mid x \in B\}$ e $A \cup B = \{x \mid (x \in A) \vee (x \in B)\}$ sono effettivamente insiemi se lo sono A e B; nel primo caso ciò segue dall'assioma di separazione, nel secondo invece da un altro, apposito assioma della teoria degli insiemi, che si chiama, guarda caso, *assioma dell'unione*.

Parti di un fissato insieme. La difficoltà che abbiamo incontrato con la 'traduzione' del connettivo di negazione scompare se limitiamo le nostre formule a parti di un prefissato insieme anziché ad insiemi arbitrari. Vediamo come. Fissiamo un insieme S. Se A è una parte di S, come abbiamo detto non esiste l'insieme degli oggetti che non appartengono ad A, ma invece esiste (per l'assioma di separazione) l'insieme degli elementi di S che non appartengono ad A; questo insieme è $S \smallsetminus A$. Possiamo dunque considerare l'operazione (unaria) di scelta del complemento in S come 'traduzione' insiemistica del connettivo di negazione (nel prefissato ambiente S). Le 'traduzioni' degli altri connettivi logici ($\Leftrightarrow$, $\Rightarrow$, $\wedge$, $\vee$, XOR) che avevamo a disposizione nel caso generale continuano ad essere valide senza sostanziali modifiche (ad esempio, per arbitrarie *parti* A e B di S vale: $A = B \iff (\forall x \in S)(x \in A \Leftrightarrow x \in B)$) e possiamo, come sopra, ottenere rapidamente formule della teoria degli insiemi da tautologie.

Ad esempio, la tautologia della doppia negazione si traduce nella formula

$$S \smallsetminus (S \smallsetminus A) = A \qquad \text{per ogni } A \subseteq S$$

(bisogna fare attenzione: questa formula vale nell'ipotesi $A \subseteq S$; se A ed S sono insiemi arbitrari si ha $S \smallsetminus (S \smallsetminus A) = S \cap A$; vedi l'Esercizio J.4).

Cosa ricaviamo di nuovo dalle tautologie sulla implicazione? Se A e B sono parti di S, sappiamo che $A \subseteq B$ equivale a $(\forall x \in S)(x \in A \Rightarrow x \in B)$. La tautologia della implicazione come disgiunzione e la legge di contrapposizione (ricordiamo: $\big(p \Rightarrow q\big) \iff \big((\neg p) \vee q\big) \iff \big((\neg q) \Rightarrow (\neg p)\big)$) mostrano che "$x \in A \Rightarrow x \in B$" equivale da una parte a "$(x \notin A) \vee (x \in B)$", dall'altra a "$x \notin B \Rightarrow x \notin A$". La conclusione è che, per ogni insieme S e per arbitrarie parti A e B di S,

$$A \subseteq B \iff S = (S \smallsetminus A) \cup B \iff S \smallsetminus B \subseteq S \smallsetminus A.$$

Osservazioni ed Esercizi.

J.1. Quello descritto nell'ultima sezione di queste note è solo uno dei tanti metodi per provare formule insiemistiche. Esistono tanti altri metodi, ad esempio quello dei diagrammi di Euler-Venn; a seconda dei casi (e dei gusti) può essere conveniente usare i metodi descritti qui o uno degli altri.

Si incoraggia chi legge a verificare le formule dimostrate in quest'ultima sezione *anche* utilizzando i diagrammi di Euler-Venn.

J.2. Siano φ e ψ due predicati unari nella variabile x. Nell'ipotesi che le loro estensioni $A_\varphi = \{x \mid \varphi\}$ e $A_\psi = \{x \mid \psi\}$ siano insiemi, si ha: $A_\varphi = A_\psi \iff (\forall x(\varphi \Leftrightarrow \psi))$ e $A_\varphi \subseteq A_\psi \iff (\forall x(\varphi \Rightarrow \psi))$.

J.3. Dimostrare che, come detto nel testo, se A è un insieme allora non esiste l'insieme degli oggetti che non appartengono ad A. Suggerimento: se esistesse questo insieme, allora la sua unione con A sarebbe ...

J.4. Provare, per *arbitrari* insiemi S ed A che $S \smallsetminus (S \smallsetminus A) = S \cap A$. Suggerimento: una volta che si sia osservato che $S \cap A \subseteq S$ e $S \smallsetminus A = S \smallsetminus (S \cap A)$, la dimostrazione è quasi completa.

J.5. Anche il principio del terzo escluso e quello di non contraddizione hanno una traduzione insiemistica: per ogni insieme S ed ogni sua parte A si ha $A \cup (S \smallsetminus A) = S$ e $A \cap (S \smallsetminus A) = \varnothing$. Verificarlo. Queste formule restano valide senza l'ipotesi che A sia contenuto in S?

J.6. Dedurre da una delle tautologie proposte nell'Esercizio E.8 la formula:

$$(\forall A, B, C)\big((A \subseteq B \cap C) \iff ((A \subseteq B) \wedge (A \subseteq C))\big).$$

La formula analoga, con $\cup$ e $\vee$ al posto di $\cap$ e $\wedge$, non vale. Come mai? (Riguardare *tutto* l'Esercizio E.8).

Sezioni e Retrazioni

Come sappiamo bene, la composta di due applicazioni iniettive è necessariamente iniettiva, la composta di due applicazioni suriettive è necessariamente suriettiva. Inoltre:

1. *Siano $f\colon A \to B$ e $g\colon B \to C$ due applicazioni componibili.*

(i) *se fg è iniettiva, f è iniettiva;*
(ii) *se fg è suriettiva, g è suriettiva;*
(iii) *se fg è biettiva, f è iniettiva e g è suriettiva.*

Dimostrazione. Iniziamo col provare (i). Sia fg iniettiva; per ogni $x, y \in A$, se $x^f = y^f$ allora $x^{fg} = (x^f)^g = (y^f)^g = y^{fg}$. Ma allora, poiché fg è iniettiva, si ha $x = y$. Abbiamo così dimostrato: $(\forall\, x, y \in A)(x^f = y^f \Rightarrow x = y)$, cioè: f è iniettiva, come richiesto dalla (i).

Proviamo (ii). Sia fg suriettiva. Per ogni $c \in C$ esiste $a \in A$ tale che $c = a^{fg}$. Posto $b = a^f$ abbiamo dunque $c = b^g$. È così provato che ogni elemento di C è immagine mediante g di un elemento di B, ovvero che g è suriettiva. Anche la (ii) è così dimostrata; la (iii) è immediata conseguenza delle prime due. □

Sia $f\colon A \to B$ un'applicazione. Per definizione, un'applicazione $g\colon B \to A$ si dice:

sezione	di f	se $gf = \mathrm{id}_B$
retrazione	di f	se $fg = \mathrm{id}_A$
inversa	di f	se g è sia una sezione che una retrazione di f.

Come è evidente dalle definizioni, dire che un'applicazione g è una sezione di un'applicazione f equivale a dire che f è una retrazione di g. Una semplice dimostrazione algebrica mostra che se un'applicazione ha sia una sezione che una retrazione, queste devono coincidere. Ciò prova, in particolare, l'unicità della (eventuale) inversa di un'applicazione.

2. *Sia $f\colon A \to B$ un'applicazione e supponiamo che f abbia una sezione g ed una retrazione h. Allora $g = h$, in particolare g è un'inversa di f. Inoltre g è sia l'unica sezione che l'unica retrazione di f.*

Dimostrazione. Poiché g è una sezione di f si ha $gf = \mathrm{id}_B$, poiché h è una retrazione di f si ha $fh = \mathrm{id}_A$. Allora $g = g\,\mathrm{id}_A = g(fh) = (gf)h = \mathrm{id}_B h = h$. Dunque, g è sia una sezione che una retrazione di f, quindi ne è una inversa. Se g_1 è una qualsiasi sezione di f, applicando a g_1 e h la prima parte dell'enunciato, appena dimostrata, si ottiene $g_1 = h$, quindi $g_1 = g$. Per lo stesso motivo, se h_1 è una retrazione di f si deve avere $g = h_1$. Ciò prova l'unicità di g come sezione e come retrazione di f. □

Dunque, un'applicazione è *invertibile* (cioè ha un'inversa) se e solo se ha sia una sezione che una retrazione. Come segue subito da (**2**), di inversa ce n'è al massimo una:

3. *Sia f un'applicazione invertibile. Allora f ha un'unica inversa.*

L'unica inversa di un'applicazione invertibile f viene indicata come f^{-1}. Come vedremo, un'applicazione non invertibile può avere più di una sezione o più di una retrazione. Iniziamo a studiare le sezioni.

4. *Sia $f\colon A \to B$ un'applicazione. Esistono sezioni di f se e solo se f è suriettiva.*

Dimostrazione. Se f ha una sezione g, allora $gf = \mathrm{id}_B$. Poiché id_B è suriettiva (in effetti è biettiva), da (**1**) segue che f è suriettiva. Viceversa, se f è suriettiva possiamo definire una sezione di f nel modo che stiamo per descrivere. Per ogni $b \in B$ l'antiimmagine A_b di $\{b\}$ mediante f (definita come $A_b = \{a \in A \mid a^f = b\}$) non è vuota; si può dunque scegliere, in modo arbitrario, un elemento $b^* \in A_b$.[(‡)] Effettuata questa scelta, poniamo $g\colon b \in B \mapsto b^* \in A$. Possiamo ora dimostrare che g è una sezione di f, cioè che $gf = \mathrm{id}_B$. Sappiamo che gf e id_B hanno lo stesso dominio e lo stesso codominio (B in entrambi i casi), quindi dobbiamo solo provare che $b^{gf} = b^{\mathrm{id}_B}$, cioè $b^{gf} = b$ per ogni $b \in B$. Per ogni tale b abbiamo $b^g \in A_b$, per la definizione di g, e quindi $b^{gf} = (b^g)^f = b$, come si voleva. Dunque g è effettivamente una sezione di f, e così l'enunciato è provato. □

Si può approfondire l'argomentazione svolta nella parte finale dell'ultima dimostrazione per descrivere esplicitamente l'insieme di tutte le sezioni di un'assegnata applicazione suriettiva $f\colon A \twoheadrightarrow B$. Sia g un'applicazione da B ad A. Ponendo $A_b = \{a \in A \mid a^f = b\}$ per ogni $b \in B$, abbiamo infatti, come osservato nella dimostrazione,

---

[(‡)] qui stiamo sorvolando su una seria difficoltà, alla quale facciamo solo un cenno. Il fatto che si possano effettuare *in simultanea* le scelte degli elementi b^*, anche, ad esempio, quando gli insiemi coinvolti siano infiniti e non abbiamo a disposizione alcun criterio di selezione per gli elementi di A non è affatto scontato. Per poter effettuare questa scelta, e costruire quindi la sezione g come stiamo qui facendo, è necessario un potente assioma della teoria degli insiemi, l'*assioma di scelta*. Senza questo assioma, non è possibile dimostrare l'enunciato (**4**), che si può anzi provare essere una forma equivalente dell'assioma di scelta.

che g è una sezione di f se e solo se $(b^g)^f = b$ per ogni $b \in B$, ma questa condizione equivale a richiedere $b^g \in A_b$ per ogni $b \in B$. Ciò mostra che le sezioni di f costruite col metodo della dimostrazione di (**4**) sono le uniche esistenti, quindi f ha tante sezioni quanti sono i modi di scegliere un elemento da ciascuno degli insiemi A_b.

Esempio 1. Poniamo $A = \{1,2,3,4,5,6\}$ e $B = \{u,v,w\}$, dove $|B| = 3$ (cioè: u, v e w sono a due a due distinti) e sia $f\colon A \to B$ definita da

$$f\colon \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ u & v & u & w & v & u \end{pmatrix}.$$

Chiaramente f è suriettiva. Volendo costruire sezioni di f, consideriamo le antiimmagini mediante f dei singleton degli elementi di B: $A_u = \{1,3,6\}$ (antiimmagine di $\{u\}$), $A_v = \{2,5\}$ (antiimmagine di $\{v\}$) e $A_w = \{4\}$ (antiimmagine di $\{w\}$). Un'applicazione $g\colon B \to A$ è una sezione di f se e solo se manda u in un elemento di A_u, v in un elemento di A_v e w in un elemento di A_w. Quindi abbiamo a disposizione tre possibili scelte (1, 3 o 6) per u^g, due per v^g (2 o 5) ed una sola per w^g: dobbiamo porre necessariamente $w^g = 4$. Esistono dunque esattamente $3 \cdot 2 \cdot 1 = 6$ sezioni di f. Esse sono le applicazioni da B ad A qui descritte:

$$\begin{pmatrix} u & v & w \\ 1 & 2 & 4 \end{pmatrix} \quad \begin{pmatrix} u & v & w \\ 1 & 5 & 4 \end{pmatrix} \quad \begin{pmatrix} u & v & w \\ 3 & 2 & 4 \end{pmatrix} \quad \begin{pmatrix} u & v & w \\ 3 & 5 & 4 \end{pmatrix} \quad \begin{pmatrix} u & v & w \\ 6 & 2 & 4 \end{pmatrix} \quad \begin{pmatrix} u & v & w \\ 6 & 5 & 4 \end{pmatrix}.$$

In generale, il numero delle sezioni di un'applicazione suriettiva $f\colon A \twoheadrightarrow B$ è il prodotto delle cardinalità degli insiemi A_b, definiti come sopra, al variare di b in B. Si osservi che l'insieme $\{A_b \mid b \in B\}$ non è altro che $\operatorname{coim} f$ (e $A_b \neq A_{b'}$ se b e b' sono elementi distinti di B). Quindi:

5. *Il numero delle sezioni di un'applicazione suriettiva f è il prodotto $\prod_{X \in \operatorname{coim} f} |X|$ delle cardinalità degli elementi della coimmagine di f.*

Almeno nel caso finito, il seguente enunciato si può vedere come caso particolare del precedente.

6. *Se un'applicazione $f\colon A \to B$ ha una ed una sola sezione allora essa è biettiva.*

Dimostrazione. Affinché f abbia almeno una sezione, f deve essere suriettiva. Se poi f è suriettiva, essa ha una sola sezione se e solo se, con le notazioni adoperate sinora, $|A_b| = 1$ per ogni $b \in B$ (per ogni $b \in B$ deve esistere una sola possibile scelta per l'immagine per b mediante una sezione di f). Ma questa condizione implica che f è anche iniettiva: se $x, y \in A$ e $x^f = y^f$ allora $x, y \in A_{x^f}$; supponendo $|A_{x^f}| = 1$ si ha quindi $x = y$. È così provato che f è biettiva. □

Vedremo tra poco che, viceversa, le applicazioni biettive sono invertibili, quindi, per (**2**), hanno una ed una solo sezione.

Passiamo ora allo studio delle retrazioni. Solo nel caso degli insiemi non vuoti vale per le retrazioni l'analogo della (**4**).

7. *Sia $f\colon A \to B$ un'applicazione e supponiamo $A \neq \varnothing$. Esistono retrazioni di f se e solo se f è iniettiva.*

Dimostrazione. Se f ha una retrazione g, allora $fg = \mathrm{id}_A$, quindi, poiché id_A è iniettiva, anche f è iniettiva per (**1**). Viceversa, supponiamo f iniettiva e costruiamo una retrazione di f. Fissiamo un elemento $u \in A$; lo possiamo fare perché, per ipotesi, $A \neq \varnothing$. Per ogni $b \in \operatorname{im} f$ esiste uno ed un solo $b^* \in A$ tale che $(b^*)^f = b$, questo perché f è iniettiva. Definiamo g in questo modo:

$$g\colon b \in B \longmapsto \begin{cases} b^* & \text{se } b \in \operatorname{im} f \\ u & \text{se } b \notin \operatorname{im} f \end{cases} \in A.$$

Vogliamo provare che g è effettivamente una retrazione di f, cioè che $fg = \mathrm{id}_A$. Ovviamente $fg\colon A \to A$, inoltre, per ogni $a \in A$, abbiamo $a^f \in \operatorname{im} f$ e $(a^f)^* = a$, quindi $a^{fg} = (a^f)^g = a$. Ciò mostra che $fg = \mathrm{id}_A$, come si voleva. □

Cosa succede nel caso in cui il dominio A dell'applicazione $f\colon A \to B$ considerata sia l'insieme vuoto? In questo caso f è certamente iniettiva (ogni applicazione di dominio vuoto è trivialmente iniettiva), ma ha una retrazione se e solo se $B = \varnothing$. Infatti, se $B = \varnothing$ allora $f = \mathrm{id}_\varnothing$, ed è facile concludere che $f = f^{-1}$, dunque f è inversa, e quindi retrazione, di se stessa; se invece $B \neq \varnothing$ allora f non ha retrazioni per l'ottimo motivo che non esistono applicazioni da B ad $A = \varnothing$ (come mai?). Notiamo infine una forma equivalente dell'enunciato (**7**): *un'applicazione è iniettiva se e solo se o ha retrazioni o ha dominio vuoto.*

8. *Sia f un'applicazione. Sono equivalenti:*

(*i*) *f è biettiva;*
(*ii*) *f ha una sezione ed una retrazione;*
(*iii*) *f è invertibile.*

Dimostrazione. Che (*iii*) implichi (*ii*) è ovvio, che (*ii*) implichi (*iii*) è stato dimostrato in (**2**). Nel caso in cui il dominio di f non sia vuoto, l'equivalenza tra (*i*) e (*ii*) segue immediatamente da (**4**) e (**7**). Nel caso in cui il dominio sia vuoto, come abbiamo osservato subito prima di questo enunciato, f è invertibile se e solo se anche il codominio di f è vuoto; d'altra parte è chiaro che quest'ultima condizione è necessaria e sufficiente affinché f sia biettiva. Dunque, anche in questo caso (*i*) e (*iii*), e quindi (*ii*), sono equivalenti. □

Chiarita la situazione per quanto riguarda le inverse delle applicazioni, ritorniamo sulle retrazioni delle applicazioni iniettive allo scopo di ottenerne una descrizione esplicita (e quindi, nel caso finito, anche contarle).

9. *Sia $f\colon A \rightarrowtail B$ un'applicazione iniettiva e sia $f_0\colon A \to \operatorname{im} f$ la ridotta di f alla sua immagine.*[♮] *Allora un'applicazione $g\colon B \to A$ è una retrazione di f se e solo se la restrizione di g a $\operatorname{im} f$ è f_0^{-1}.*

Dimostrazione. Il fatto che g sia una retrazione di f significa, per definizione, che $fg = \mathrm{id}_A$. Poiché, fg ha lo stesso dominio, A, e codominio, ancora A, di id_A, ciò equivale all'essere $a^{fg} = a^{\mathrm{id}_A}$, cioè $a^{fg} = a$, per ogni $a \in A$. Sia ora g_0 la restrizione di g a $\operatorname{im} f$. Allora, per ogni $a \in A$, poiché $a^f \in \operatorname{im} f$, si ha $a^{fg} = (a^f)^g = (a^f)^{g_0}$; inoltre $a^{f_0} = a^f$, quindi $a^{fg} = a^{f_0 g_0}$. In conclusione g è una retrazione di f se e solo se $a^{f_0 g_0} = a$ per ogni $a \in A$, cioè se e solo se $f_0 g_0 = \mathrm{id}_A$. Dal momento che f_0 è biettiva, f_0 ha una sola retrazione (come visto in (**2**)), cioè f_0^{-1}. Pertanto $f_0 g_0 = \mathrm{id}_A$ se e solo se $g_0 = f_0^{-1}$. In questo modo è provato che g è una retrazione di f se e solo se $g_0 = f_0^{-1}$, che è quanto affermato dall'enunciato.[!] □

Possiamo esprimere lo stesso enunciato anche in questa forma: con le notazioni fissate,

le retrazioni di f sono tutti e soli i prolungamenti di f_0^{-1} a B.

La questione ora diventa: quali e quanti sono i prolungamenti f_0^{-1} a B? Esaminiamo il problema da un punto di vista più generale. Se $h\colon S \to T$ è un'applicazione e X è un insieme contenente S, come possiamo descrivere i prolungamenti di h a X? Intuitivamente è chiaro che un tale prolungamento si ottiene mandando ogni elemento x di S in x^h ed assegnando arbitrarie immagini (in T) agli elementi di $X \smallsetminus S$. Precisando questa idea, per ogni applicazione $k\colon X \smallsetminus S \to T$ definiamo

$$h_k\colon x \in X \longmapsto \begin{cases} x^h & \text{se } x \in S \\ x^k & \text{se } x \notin S \end{cases} \in T,$$

è chiaro che h_k è un prolungamento di h a X. Si ha:

10. *Con le notazioni appena stabilite, indicando con $\mathcal{P}$ l'insieme dei prolungamenti di h a X, l'applicazione $p\colon k \in \operatorname{Map}(X \smallsetminus S, T) \mapsto h_k \in \mathcal{P}$ è biettiva; la sua inversa è $q\colon t \in \mathcal{P} \mapsto t_{|X \smallsetminus S} \in \operatorname{Map}(X \smallsetminus S, T)$.*[♭]

Dimostrazione. Sia $k \in \operatorname{Map}(X \smallsetminus S, T)$. Allora $k^{pq} = (k^p)^q$ è la restrizione $X \smallsetminus S$ di $k^p = h_k$. Questa restrizione è ovviamente k. Dunque $k^{pq} = k$, quindi $pq = \mathrm{id}_{\operatorname{Map}(X \smallsetminus S, T)}$. Sia ora $t \in \mathcal{P}$. Allora $t^{qp} = h_{t^q}$ è l'applicazione da X a T che manda ogni elemento x di S in x^h ed ogni elemento y di $X \smallsetminus S$ in y^{t^q}; ora, poiché h e t^q sono restrizioni di t, si ha $x^h = x^t$ e $y^{t^q} = y^t$. Quindi t^{qp} manda ogni elemento di X nella sua immagine mediante t dunque $t^{qp} = t$, sicché $qp = \mathrm{id}_{\mathcal{P}}$. In questo modo è provato che q è l'inversa di p e quindi, per (**8**), che p è biettiva. □

Otteniamo a questo punto un'altra utile descrizione delle retrazioni di un'assegnata applicazione iniettiva. Questa descrizione è forse meno immediata di quella fornita in (**9**), ma più esplicita. Riprendiamo le notazioni di (**9**) per l'applicazione $f\colon A \rightarrowtail B$ e la sua ridotta f_0, e indichiamo con $\mathcal{R}$ l'insieme delle retrazioni di f, dunque $\mathcal{R} = \{g \in \operatorname{Map}(B, A) \mid fg = \mathrm{id}_A\}$.

11. *Con le notazioni appena fissate, per ogni applicazione $k\colon B \smallsetminus \operatorname{im} f \to A$ si ponga:*

$$g_k\colon b \in B \longmapsto \begin{cases} b^{f_0^{-1}} & \text{se } b \in \operatorname{im} f \\ b^k & \text{se } b \notin \operatorname{im} f \end{cases} \in A.$$

Allora l'applicazione $\theta\colon k \in \operatorname{Map}(B \smallsetminus \operatorname{im} f, A) \longmapsto g_k \in \mathcal{R}$ è biettiva.

Dimostrazione. La dimostrazione segue immediatamente da (**9**) e da (**10**). □

[♮] quindi f_0 è l'applicazione: $a \in A \mapsto a^f \in \operatorname{im} f$; chiaramente f_0 è biettiva.

[!] non si faccia assolutamente confusione su questo punto: in questa dimostrazione abbiamo potuto dedurre $g_0 = f_0^{-1}$ da $f_0 g_0 = \mathrm{id}_A$ *soltanto perché già sapevamo che f_0 è biettiva.* In generale, se $h\colon X \to Y$ e $k\colon Y \to X$ sono applicazioni e sappiamo che $hk = \mathrm{id}_X$ ciò non ci basta per dedurre che k sia l'inversa di h. Otteniamo questa informazione se sappiamo anche che $kh = \mathrm{id}_Y$, come richiesto dalla definizione di applicazione inversa, oppure, come nella dimostrazione, se sappiamo che almeno una tra h e k è biettiva, potendo in questo caso fare uso di (**2**).

[♭] si ricorda che $t_{|X \smallsetminus S}$ indica la restrizione di t a $X \smallsetminus S$.

Sintetizzando, per costruire una retrazione $g\colon B \twoheadrightarrow A$ di un'applicazione iniettiva $f\colon A \rightarrowtail B$ basta fare in modo che ogni elemento di $\operatorname{im} f$ venga mandato da g nella sua unica controimmagine mediante f, mentre la scelta delle immagini mediante g degli elementi di $B \setminus \operatorname{im} f$ è del tutto arbitraria. Può essere istruttivo ritornare alla dimostrazione di (**7**) ed osservare come quella dimostrazione sia una versione semplificata di quella svolta per (**9**). È poi importante capire bene il significato di (**11**). Questo enunciato mostra che le retrazioni dell'applicazione f sono tutte e sole le applicazioni g_α, e che queste sono a due a due distinte, nel senso che, se α e β sono applicazioni distinte da $B \setminus \operatorname{im} f$ ad A, allora $g_\alpha \neq g_\beta$.

12. *Sia $f\colon A \rightarrowtail B$ un'applicazione iniettiva tra insiemi finiti. Se $|A| = a$ e $|B| = b$, il numero delle retrazioni di f è a^{b-a}.*

Dimostrazione. Abbiamo visto in (**11**) che l'insieme delle retrazioni di f è equipotente a $\operatorname{Map}(B \setminus \operatorname{im} f, A)$. Poiché $|\operatorname{im} f| = |A| = a$ e quindi $|B \setminus \operatorname{im} f| = b - a$, la cardinalità di $\operatorname{Map}(B \setminus \operatorname{im} f, A)$ è a^{b-a}, il che prova l'asserto. □

Conseguenza di (**11**), e nel caso finito anche di (**12**), è:

13. *Sia A un insieme tale che $|A| > 1$. Un'applicazione $f\colon A \to B$ ha una ed una sola retrazione se e solo se è biettiva (in questo caso l'unica retrazione di f è f^{-1}).*

Dimostrazione. Se f ha una retrazione, allora f è iniettiva, come mostra (**7**). Se ciò accade, per (**11**), la retrazione è unica se e solo se $\operatorname{Map}(B \setminus \operatorname{im} f, A)$ ha un solo elemento. Siccome A ha almeno due elementi, ciò accade se solo se $B \setminus \operatorname{im} f = \varnothing$.[(†)] Dire che $B \setminus \operatorname{im} f = \varnothing$ significa esattamente dire che f è suriettiva, dunque biettiva. Tenendo presenti anche (**3**) e (**8**), ciò prova l'asserto. □

Si può confrontare (**13**) con (**6**). Come nel caso di (**7**), il risultato per le applicazioni iniettive è perfettamente analogo a quello per le applicazioni suriettive solo se un'ipotesi aggiuntiva (in questo caso $|A| > 1$) garantisce che il dominio non sia 'troppo piccolo'. Abbiamo già discusso il caso delle applicazioni con dominio vuoto, vediamo cosa accade se il dominio A ha cardinalità 1 (cioè è un singleton). Se $|A| = 1$, qualunque sia l'insieme B, ogni applicazione f da A a B è iniettiva; affinché una tale applicazione esista deve essere $B \neq \varnothing$. Purché, appunto, $B \neq \varnothing$ si ha però $|\operatorname{Map}(B, A)| = 1$, quindi f ha una ed una sola retrazione, ma f non è suriettiva se $|B| > 1$. Ciò spiega perché è stato necessario inserire nell'enunciato l'ipotesi che A abbia più di un elemento.

Esempio 2. Elenchiamo tutte le retrazioni dell'applicazione iniettiva $f\colon A \rightarrowtail B$ definita da

$$\begin{pmatrix} u & v & w \\ 2 & 5 & 3 \end{pmatrix},$$

dove $A = \{u, v, w\}$ ha cardinalità 3 e $B = \{1, 2, 3, 4, 5\}$. Si ha chiaramente $\operatorname{im} f = \{2, 3, 5\}$. La (**9**) e la (**11**) mostrano come costruire (tutte) le retrazioni di f. L'immagine di ciascuno dei tre elementi di $\operatorname{im} f$ mediante una qualsiasi retrazione g di f è determinata: si deve avere $2^g = u$, $3^g = w$ e $5^g = v$, cioè: ciascuno dei tre elementi di $\operatorname{im} f$ deve essere mandato da g nell'unico elemento del quale è immagine mediante f. In altri termini, questo fa sì che la restrizione di g a $\operatorname{im} f$ sia l'inversa della ridotta di f alla sua immagine, come richiesto da (**9**). Agli altri elementi di B, cioè 1 e 4, possiamo far corrispondere arbitrari elementi di A. Nella maniera più precisa indicata in (**11**), consideriamo le nove applicazioni da $B \setminus \operatorname{im} f$ ad A:

$$\begin{cases} 1 \mapsto u \\ 4 \mapsto u \end{cases} \quad \begin{cases} 1 \mapsto u \\ 4 \mapsto v \end{cases} \quad \begin{cases} 1 \mapsto u \\ 4 \mapsto w \end{cases} \quad \begin{cases} 1 \mapsto v \\ 4 \mapsto u \end{cases} \quad \begin{cases} 1 \mapsto v \\ 4 \mapsto v \end{cases} \quad \begin{cases} 1 \mapsto v \\ 4 \mapsto w \end{cases} \quad \begin{cases} 1 \mapsto w \\ 4 \mapsto u \end{cases} \quad \begin{cases} 1 \mapsto w \\ 4 \mapsto v \end{cases} \quad \begin{cases} 1 \mapsto w \\ 4 \mapsto w \end{cases}$$

da queste, come mostra la biezione θ di (**11**), si ottengono le nove retrazioni di f:

$$\begin{cases} 1 \mapsto u \\ 2 \mapsto u \\ 3 \mapsto w \\ 4 \mapsto u \\ 5 \mapsto v \end{cases} \quad \begin{cases} 1 \mapsto u \\ 2 \mapsto u \\ 3 \mapsto w \\ 4 \mapsto v \\ 5 \mapsto v \end{cases} \quad \begin{cases} 1 \mapsto u \\ 2 \mapsto u \\ 3 \mapsto w \\ 4 \mapsto w \\ 5 \mapsto v \end{cases} \quad \begin{cases} 1 \mapsto v \\ 2 \mapsto u \\ 3 \mapsto w \\ 4 \mapsto u \\ 5 \mapsto v \end{cases} \quad \begin{cases} 1 \mapsto v \\ 2 \mapsto u \\ 3 \mapsto w \\ 4 \mapsto v \\ 5 \mapsto v \end{cases} \quad \begin{cases} 1 \mapsto v \\ 2 \mapsto u \\ 3 \mapsto w \\ 4 \mapsto w \\ 5 \mapsto v \end{cases} \quad \begin{cases} 1 \mapsto w \\ 2 \mapsto u \\ 3 \mapsto w \\ 4 \mapsto u \\ 5 \mapsto v \end{cases} \quad \begin{cases} 1 \mapsto w \\ 2 \mapsto u \\ 3 \mapsto w \\ 4 \mapsto v \\ 5 \mapsto v \end{cases} \quad \begin{cases} 1 \mapsto w \\ 2 \mapsto u \\ 3 \mapsto w \\ 4 \mapsto w \\ 5 \mapsto v \end{cases}$$

Esercizi.

1. Si indichi come costruire un numero arbitariamente grande di retrazioni dell'immersione di $\mathbb{N}$ in $\mathbb{Z}$ e di sezioni dell'applicazione $n \in \mathbb{Z} \mapsto |n| \in \mathbb{N}$.
2. Quante sono le retrazioni dell'applicazione $n \in \{-2, -1, 0, 1, 2\} \mapsto n^2 \in \{0, 1, 2, 3, 4\}$?
3. Provare che se $f\colon A \twoheadrightarrow B$ e $g\colon B \twoheadrightarrow C$ sono applicazioni suriettive componibili e se $\bar{f}$ e $\bar{g}$ sono sezioni di f e g rispettivamente, allora $\bar{g}\bar{f}$ è una sezione di fg. Enunciare e provare l'analoga proposizione per le retrazioni.
4. L'inversa dell'inversa di un'applicazione invertibile è l'applicazione stessa.

[(†)] se $b \in B \setminus \operatorname{im} f$ e u, v sono due elementi distinti di A, esistono almeno due applicazioni da $B \setminus \operatorname{im} f$ ad A: una che manda b in u e tutti gli altri elementi di $B \setminus \operatorname{im} f$ in v, l'altra che manda ogni elemento di $B \setminus \operatorname{im} f$ in v.

Il Teorema di Omomorfismo per Insiemi

Sia $f\colon A \to B$ un'applicazione dall'insieme A all'insieme B. Ad f possiamo associare una relazione di equivalenza nel dominio A di f, detta il *nucleo di equivalenza* di f (o, come nel testo di Facchini, equivalenza associata ad f) e che indicheremo con $\sim_f$. Essa è definita ponendo, per ogni x e y in A,

$$x \sim_f y \iff x^f = y^f.$$

Si veda Facchini (pagine 61 e seguenti) per tutti gli (importantissimi) dettagli.

L'insieme quoziente $A/\sim_f$ prende il nome di *coimmagine* di f e si indica abitualmente come $\operatorname{coim} f$. Quali sono i suoi elementi? Si può facilmente mostrare che $\operatorname{coim} f$ consiste precisamente delle antiimmagini dei singleton degli elementi di $\operatorname{im} f$ mediante f, cioè che:

$$\operatorname{coim} f = A/\sim_f = \left\{\{b\}^{\overleftarrow{f}} \mid b \in \operatorname{im} f\right\} \tag{1}$$

(ricordiamo che, per ogni $b \in B$, per definizione di antiimmagine si ha

$$\{b\}^{\overleftarrow{f}} = \left\{x \in A \mid x^f \in \{b\}\right\} = \{x \in A \mid x^f = b\};$$

questo insieme è diverso da $\varnothing$ se e solo se $b \in \operatorname{im} f$). Per provare la (1) osserviamo che, per ogni $a \in A$ la classe di equivalenza di a modulo $\sim_f$ è $\{x \in A \mid x^f = a^f\}$, l'insieme degli elementi di A che hanno, mediante f, la stessa immagine di a. Evidentemente questo insieme è $\{a^f\}^{\overleftarrow{f}}$. Pertanto $\operatorname{coim} f \subseteq \left\{\{b\}^{\overleftarrow{f}} \mid b \in \operatorname{im} f\right\}$. Viceversa, se $b \in \operatorname{im} f$ esiste $a \in A$ tale che $b = a^f$. Allora, per quanto appena visto, $\{b\}^{\overleftarrow{f}} = \{a^f\}^{\overleftarrow{f}} = [a]_{\sim_f} \in \operatorname{coim} f$. La (1) è così provata. Prima di proseguire con la discussione, vediamo un esempio (a colori).

Esempio 1. Supponiamo che A sia l'insieme dei numeri naturali minori di 10 e B sia un insieme di colori, poniamo $B = \{\text{rosso, verde, blu, marrone, giallo}\}$. Sia f un'applicazione da A a B; dunque f associa a ciascuno dei numeri in A uno dei colori in B. Supponiamo che f sia definita in questo modo: a 1, 5 e 7 è associato il colore rosso, a 0, 3, 6 e 8 il verde, a 2 e 9 il blu e a 4 il marrone:

$$A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}.$$

Allora, rispetto a $\sim_f$, due elementi di A sono equivalenti se e solo se hanno lo stesso colore, e $\operatorname{coim} f$ è costituita da quattro classi di equivalenza: quella degli elementi di colore rosso: $\{1, 5, 7\}$, che è l'antiimmagine di $\{\text{rosso}\}$ mediante f, quella degli elementi verdi: $\{0, 3, 6, 8\}$, quella degli elementi blu: $\{2, 9\}$ e quella degli elementi marroni: $\{4\}$; dunque

$$\operatorname{coim} f = \left\{\{1, 5, 7\}, \{0, 3, 6, 8\}, \{2, 9\}, \{4\}\right\}.$$

Si noti che, benché B abbia tra i suoi elementi il colore giallo, questo colore non determina nessun elemento di $\operatorname{coim} f$. Ciò è in accordo con la (1): $\operatorname{coim} f$ è l'insieme delle antiimmagini dei singleton degli elementi di $\operatorname{im} f$ (cioè rosso, verde, blu e marrone), mentre giallo è in B ma non in $\operatorname{im} f$.

Torniamo ora alla discussione generale. Per un'arbitraria applicazione f, rifacendoci a (1) ed alle osservazioni immediatamente successive, possiamo osservare che l'applicazione

$$\alpha\colon b \in \operatorname{im} f \longmapsto \{b\}^{\overleftarrow{f}} \in \operatorname{coim} f$$

è suriettiva. D'altra parte, è evidente che α è anche iniettiva: se $b, c \in \operatorname{im} f$ e $b \neq c$ allora certamente $b^\alpha = \{b\}^{\overleftarrow{f}} \neq \{c\}^{\overleftarrow{f}} = c^\alpha$, perché gli elementi di b^α vengono mandati da f in b mentre quelli di c^α vengono mandati in c. Dunque, α è biettiva, e possiamo considerare la sua inversa, che indichiamo con $\tilde{f}$. Questa è

$$\tilde{f}\colon [a]_{\sim_f} \in \operatorname{coim} f \longmapsto a^f \in \operatorname{im} f, \tag{2}$$

infatti, come abbiamo visto sopra, per ogni $a \in A$ la classe $[a]_{\sim_f}$ è proprio $\{a^f\}^{\overleftarrow{f}}$, che è l'immagine di a^f mediante α.

Anche se in senso stretto è inutile farlo, osserviamo che avremmo potuto definire direttamente $\tilde{f}$ tramite la (2) senza utilizzare α; in questo caso però sarebbe stato necessario verificare che $\tilde{f}$ è ben definita. Per far questo avremmo dovuto prima osservare che ogni elemento di $\operatorname{coim} f$ si può rappresentare nella forma $[a]_{\sim_f}$ per un opportuno $a \in A$. Questa rappresentazione non è unica, ma l'applicazione è comunque ben posta perché, per ogni $x, y \in A$,

$$[x]_{\sim_f} = [y]_{\sim_f} \iff x \sim_f y \iff x^f = y^f,$$

quindi, effettivamente, ogni elemento di $\operatorname{coim} f$ ha un solo corrispondente mediante $\tilde{f}$, anzi, questa catena di equivalenze, letta da destra verso sinistra, mostra anche l'iniettività di $\tilde{f}$ (la suriettività è ovvia).

Qualunque sia il modo preferito per definire di $\tilde{f}$, è importante comprendere bene questo: che scelto comunque $X \in \operatorname{coim} f$, tutti gli elementi di X hanno, mediante f la stessa immagine, vale a dire: $(\forall\, x, y \in X)(x^f = y^f)$, e $\tilde{f}$ è l'applicazione da $\operatorname{coim} f$ a $\operatorname{im} f$ che associa ad ogni tale X questa immagine comune.

Utilizziamo l'applicazione $\tilde{f}$ per costruire un diagramma commutativo:

$$\begin{array}{ccc} A & \xrightarrow{\quad f \quad} & B \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle\iota} \\ \operatorname{coim} f & \xrightarrow[\quad \tilde{f} \quad]{\sim} & \operatorname{im} f \end{array} \tag{3}$$

dove π è la proiezione canonica: $a \mapsto [a]_{\sim_f}$ e ι è l'immersione di $\operatorname{im} f$ in B. Che il diagramma (3) sia commutativo significa, naturalmente, che $\pi\tilde{f}\iota = f$ ed è piuttosto facile da provare. Infatti, per ogni $a \in A$, abbiamo

$$a^{\pi\tilde{f}\iota} = ([a]_{\sim_f})^{\tilde{f}\iota} = \big(([a]_{\sim_f})^{\tilde{f}}\big)^{\iota} = (a^f)^{\iota} = a^f.$$

Questo risultato, di grande importanza, è noto come Teorema fondamentale di omomorfismo per insiemi. Il suo contenuto è perfettamente reso dalla commutatività del diagramma (3). Lo possiamo comunque enunciare in questa forma:

Teorema. *Sia $f\colon A \to B$ un'applicazione. Allora:*

(*i*) *l'applicazione $\tilde{f}\colon [a]_{\sim_f} \in \operatorname{coim} f \longmapsto a^f \in \operatorname{im} f$ è biettiva;*

(*ii*) *se π è la proiezione canonica da A a $\operatorname{coim} f$ e ι è l'immersione di $\operatorname{im} f$ in B, si ha $f = \pi\tilde{f}\iota$.*

Vediamo due importanti conseguenze del teorema. In primo luogo, poiché $\tilde{f}$ è biettiva si ha

$$|\operatorname{im} f| = |\operatorname{coim} f|.$$

In secondo luogo il teorema mostra che ogni applicazione f ha una fattorizzazione nel prodotto di una applicazione suriettiva (π), un'applicazione biettiva ($\tilde{f}$) ed una iniettiva (ι). Questa fattorizzazione $f = \pi\tilde{f}\iota$ è nota come *fattorizzazione canonica* di f.

Esempio 2. La signora Pacchetti è addetta allo smistamento delle lettere all'ufficio postale del paese di Rocca Insiemistica. Il suo lavoro consiste nel suddividere la corrispondenza in partenza secondo la città di destinazione. Nella giornata in cui si svolge questa storia sono state consegnate all'ufficio postale diverse lettere, alcune destinate a Roma, altre a Milano, altre ancora a Palermo, a Torino, a Verona, a Bari. Come procede la signora Pacchetti? Raccoglie tutte le lettere destinate a Roma in un apposita cassetta, quelle per Milano in un'altra cassetta e così via; su ciascuna cassetta appone un'etichetta con il nome della città di destinazione delle lettere lì contenute. Queste cassette saranno poi portate all'ufficio spedizioni, in modo che il loro contenuto sia inviato alle rispettive destinazioni.

Possiamo descrivere tutto ciò in termini del teorema di omomorfismo per insiemi; vediamo in che modo. Chiamiamo L l'insieme delle lettere che vengono spedite oggi da Rocca Insiemistica (passano tutte per l'ufficio postale), e chiamiamo D l'insieme di tutte le possibili destinazioni (possiamo dire che D sia l'insieme di tutte le città del mondo). Ogni lettera, cioè ogni elemento di L, ha una ed una sola destinazione, quindi abbiamo un'applicazione $d\colon L \to D$, quella che ad ogni lettera associa la sua città di destinazione. L'immagine $\operatorname{im} d$ dell'applicazione d è l'insieme delle destinazioni alle quali, nella nostra giornata, è stata effettivamente spedita almeno una lettera da Rocca Insiemistica, dunque $\operatorname{im} d = \{\text{Roma, Milano, Palermo, Torino, Verona, Bari}\}$. Due lettere sono in relazione rispetto al nucleo di equivalenza di d se e solo se hanno la stessa destinazione. Ad esempio, la classe di equivalenza di una lettera per Torino è l'insieme di tutte le lettere per Torino, cioè l'insieme di tutte le lettere che la signora Pacchetti ha infilato in una certa cassetta, quella a cui ha poi apposto l'etichetta "Torino". Quindi le cassette che la signora Pacchetti ha preparato rappresentano le classi di equivalenza; di conseguenza l'insieme di queste cassette rappresenta la coimmagine di d. È chiaro che ci ritroviamo con esattamente una cassetta per ciascuna città di destinazione (dunque, nel nostro esempio, la signora Pacchetti ha preparato sei cassette). In altri termini, a ciascuna di queste cassette corrisponde una città di destinazione (quella indicata dall'etichetta) e, viceversa, a ciascuna delle sei destinazioni in $\operatorname{im} d$ corrisponde una cassetta. Questa corrispondenza non è altro che l'applicazione biettiva $\tilde{d}\colon \operatorname{coim} d \to \operatorname{im} d$ data dal teorema: ad ogni elemento X di $\operatorname{coim} d$ (cioè ad ogni cassetta) associamo l'immagine mediante d (cioè la città di destinazione) di un qualsiasi elemento di X (cioè di una qualsiasi lettera che la signora Pacchetti ha infilato nella cassetta X). Possiamo, in un certo senso dire che la nostra signora Pacchetti ha applicato prima la proiezione canonica $\pi\colon x \in L \mapsto [x]_{\sim_d} \in \operatorname{coim} d$ quando ha messo ciascuna lettera nella sua cassetta, poi l'applicazione biettiva $\tilde{d}\colon [x]_{\sim_d} \in \operatorname{coim} d \mapsto x^d \in \operatorname{im} d$ quando ha apposto un etichetta con il nome della città di destinazione a ciascuna delle cassette. Cosa significa, nel nostro esempio, il fatto che il diagramma (3) sia commutativo, cioè che $\pi\tilde{d}\iota = d$ dove ι è l'immersione di $\operatorname{im} d$ in D? Semplicemente che (per fortuna!) la procedura seguita nell'ufficio postale di Rocca Insiemistica fa sì che ogni lettera arrivi effettivamente alla città alla quale era destinata. Infatti questa procedura avrà per risultato la spedizione di ogni lettera x alla città $x^{\pi\tilde{d}\iota}$, che, per il teorema, coincide con x^d, la destinazione indicata dal mittente. Ad esempio, una lettera x per Palermo viene prima messa nella cassetta di tutte le lettere per Palermo (l'insieme di queste lettere è x^π), a questa cassetta viene messa un'etichetta con su scritto "Palermo", e tutto il contenuto della cassetta viene spedito a Palermo (quindi $(x^\pi)^{\tilde{d}} = \text{Palermo}$). Dunque $x^{\pi\tilde{d}\iota} = \text{Palermo}$, sicché x viene spedita a Palermo. Tutto è andato a buon fine, perché Palermo ($= x^d$) era proprio la destinazione della lettera.

Coefficienti binomiali

Sia S un insieme. Per ogni numero naturale k si definisce $\mathcal{P}_k(S)$ come l'insieme delle parti di S che abbiano (esattamente) k elementi, dunque:

$$\mathcal{P}_k(S) = \{X \subseteq S \;\big|\; |X| = k\}.$$

Gli elementi di $\mathcal{P}_k(S)$ si chiamano anche *k-parti* di S (con una terminologia un pò vecchia ma ancora corrente, queste sono anche chiamate *combinazioni* di n oggetti di classe k). Ad esempio, l'unica 0-parte di un insieme S è l'insieme vuoto, mentre le 1-parti di S sono i singleton degli elementi di S, quindi

$$\mathcal{P}_0(S) = \{\varnothing\} \qquad \text{e} \qquad \mathcal{P}_1(S) = \big\{\{x\} \mid x \in S\big\}$$

qualsiasi sia S; se poi $S = \{1,2,3,4\}$ allora $\mathcal{P}_2(S) = \big\{\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\}\big\}$.

Non è difficile verificare che se $f\colon S \to T$ è un'applicazione biettiva, per ogni $k \in \mathbb{N}$ l'applicazione

$$\alpha\colon X \in \mathcal{P}_k(S) \longmapsto X^{\vec{f}} \in \mathcal{P}_k(T),$$

che ad ogni k-parte di S associa la sua immagine tramite f, è ben posta ed è biettiva: se g è l'inversa di f allora l'inversa di α è l'applicazione data da $Y \in \mathcal{P}_k(T) \longmapsto Y^{\vec{g}} \in \mathcal{P}_k(S)$. Pertanto, scelti comunque due insiemi S e T ed un numero naturale k, se $|S| = |T|$ allora $|\mathcal{P}_k(S)| = |\mathcal{P}_k(T)|$.

Supponiamo ora che S sia un insieme finito e sia $n = |S|$. Per ogni $k \in \mathbb{N}$ poniamo, per definizione,

$$\binom{n}{k} := |\mathcal{P}_k(S)|.$$

Il simbolo $\binom{n}{k}$ così definito si chiama *coefficiente binomiale*. La correttezza di questa definizione va giustificata. Infatti abbiamo definito un termine (il coefficiente binomiale), che deve dipendere solo dai numeri naturali k ed n, come il numero delle k-parti di un *particolare* insieme S di n elementi. In linea di principio si potrebbe pensare che, sostituendo ad S un altro insieme con lo stesso numero n di elementi, il numero delle k-parti di questo secondo insieme possa risultare diverso da $|\mathcal{P}_k(S)|$; se così fosse non avremmo correttamente definito $\binom{n}{k}$. Come abbiamo dimostrato sopra, però, ciò non accade: se T è un insieme e $|T| = n = |S|$ allora $|\mathcal{P}_k(T)| = |\mathcal{P}_k(S)|$. In altri termini, il valore di $|\mathcal{P}_k(S)|$ non dipende dalla particolare scelta di S tra gli insiemi con n elementi; è questo che rende accettabile la definizione data per il coefficiente binomiale.

Alcuni coefficienti binomiali sono immediati da calcolare: per ogni $n \in \mathbb{N}$ si ha

$$\binom{n}{0} = \binom{n}{n} = 1; \qquad \binom{n}{1} = n; \qquad (\forall\, k \in \mathbb{N})\ \Big(k > n \Rightarrow \binom{n}{k} = 0\Big).$$

Infatti, se S è un insieme di n elementi, abbiamo $\mathcal{P}_0(S) = \{\varnothing\}$ e $\mathcal{P}_n(S) = \{S\}$, quindi $\binom{n}{0} = \binom{n}{n} = 1$; inoltre $\mathcal{P}_1(S)$, l'insieme dei singleton degli elementi di S, ha tanti elementi quanto S, dunque n, quindi $\binom{n}{1} = n$. Infine, se $k > n$ allora certamente $\mathcal{P}_k(S) = \varnothing$ (S non ha parti che abbiano più elementi dello stesso S) e quindi $\binom{n}{k} = 0$. Un'altra proprietà molto semplice da verificare è:

1. *Per ogni $n \in \mathbb{N}$ si ha* $\displaystyle\sum_{k=0}^{n} \binom{n}{k} = 2^n$.

Dimostrazione — Sia S un insieme tale che $|S| = n$. È chiaro che $\mathcal{P}(S)$ è unione disgiunta degli insiemi $\mathcal{P}_k(S)$ al variare dell'intero k tra 0 e n; in altri termini $\{\mathcal{P}_k(S) \mid k \in \mathbb{N} \wedge k \leq n\}$ è una partizione di $\mathcal{P}(S)$. Pertanto $|\mathcal{P}(S)| = \sum_{k=0}^{n} |\mathcal{P}_k(S)|$; poiché $|\mathcal{P}(S)| = 2^n$ e, per ogni scelta di k, $|\mathcal{P}_k(S)| = \binom{n}{k}$, otteniamo così l'asserto. □

Si può pensare al coefficiente binomiale $\binom{n}{k}$ in questi termini: $\binom{n}{k}$ è il numero di modi in cui si possono scegliere k oggetti da un insieme di n oggetti (infatti scegliere k oggetti significa in sostanza scegliere una k-parte se, come qui stiamo facendo, non consideriamo importante l'ordine in cui questi oggetti siano stati scelti). Ora, selezionare k oggetti da un insieme di n è concettualmente equivalente a sceglierne $n-k$ da scartare (ad esempio, per essere sicuro di restare con due carte in mano se ne ho cinque, posso sceglierne due da "tenere" oppure sceglierne tre da "scartare": $3 = 5 - 2$). Dunque

dovrebbe esser facile comprendere che il coefficiente binomiale $\binom{n}{n-k}$ coincide con $\binom{n}{k}$. Questa idea intuitiva è facile da formalizzare:

2. *Siano $n, k \in \mathbb{N}$ e supponiamo $k \leq n$. Allora* $\displaystyle\binom{n}{n-k} = \binom{n}{k}$.

Dimostrazione — Fissato un insieme S con (esattamente) n elementi, consideriamo l'applicazione

$$c\colon X \in \mathcal{P}(S) \longmapsto S \smallsetminus X \in \mathcal{P}(S)$$

che ad ogni parte di S associa il suo complemento in S. Poiché il complemento del complemento di una qualsiasi parte X di S è X stessa (vale a dire: $S \smallsetminus (S \smallsetminus X) = X$ per ogni $X \subseteq S$), è chiaro che c^2 è l'applicazione identica di $\mathcal{P}(S)$, cioè che c è l'applicazione inversa di se stessa. Dunque c è biettiva. L'immagine di $\mathcal{P}_k(S)$ mediante c è costituita dai complementi in S delle parti di S di cardinalità k, ma queste sono precisamente le parti di S di cardinalità $n-k$. Dunque, l'immagine di $\mathcal{P}_k(S)$ mediante c è $\mathcal{P}_{n-k}(S)$. Pertanto l'applicazione (indotta da c, nel senso che è una restrizione di c ridotta alla sua immagine)

$$c_k\colon X \in \mathcal{P}_k(S) \longmapsto S \smallsetminus X \in \mathcal{P}_{n-k}(S)$$

è anch'essa biettiva. Ciò dimostra che $|\mathcal{P}_k(S)| = |\mathcal{P}_{n-k}(S)|$, ovvero, in altri termini, $\binom{n}{k} = \binom{n}{n-k}$, come si voleva dimostrare. □

La proprietà espressa dal precedente enunciato viene talvolta chiamata proprietà di simmetria dei coefficienti binomiali. Un'altra notevolissima proprietà è quella rappresentata nel cosiddetto *triangolo di Tartaglia-Pascal*. Si tratta essenzialmente di questa formula:

3. *Siano $n, k \in \mathbb{N}$ e supponiamo $k \leq n$. Allora* $\displaystyle\binom{n+1}{k+1} = \binom{n}{k+1} + \binom{n}{k}$.

Dimostrazione — Diamo questa dimostrazione in una versione poco formalizzata ma più facile da seguire di quanto sarebbe in una stesura più rigorosa.

Supponiamo di avere un insieme S costuito da $n+1$ palline bianche. Ovviamente $S \neq \varnothing$, perché $n+1 > 0$, quindi possiamo selezionare una delle palline e colorarla, diciamo, di nero. Il coefficiente binomiale che vogliamo calcolare, $\binom{n+1}{k+1}$, è il numero delle $(k+1)$-parti di S. Possiamo distinguere tra due tipi di $(k+1)$-parti di S: quelle costituite da sole palline bianche e quelle costituite dalla pallina nera e da k palline bianche. Ovviamente $\binom{n+1}{k+1}$ è la somma tra il numero delle parti del primo tipo ed il numero delle parti del secondo tipo. Quante sono le parti del primo tipo? Esse sono precisamente le $(k+1)$-parti dell'insieme delle palline bianche. Poiché il numero delle palline bianche è n (le palline erano in origine $n+1$, ne abbiamo colorato una di nero, restano bianche $n = (n+1)-1$ palline), questo numero sarà $\binom{n}{k+1}$. Quante sono invece le parti del secondo tipo? Ciascuna di esse si ottiene aggiungendo la pallina nera ad una k-parte dell'insieme delle palline bianche, e da ciò è facile dedurre che il numero delle parti del secondo tipo è uguale a quello delle k-parti dell'insieme delle palline bianche, dunque $\binom{n}{k}$. Pertanto $\binom{n+1}{k+1}$, che come detto è uguale alla somma tra il numero delle parti del primo tipo ed il numero delle parti del secondo tipo, è proprio $\binom{n}{k+1} + \binom{n}{k}$, come volevamo dimostrare. □

Vediamo come la formula appena dimostrata si visualizza nel triangolo di Tartaglia-Pascal. Questo triangolo è costruito secondo lo schema:

$$\begin{array}{ccccccccccccccccc}
 & & & & & & \binom{0}{0} & & & & & & & & & & \\
 & & & & & \binom{1}{0} & & \binom{1}{1} & & & & & & & & & \\
 & & & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & & & & & & & \\
 & & & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & & & & & & & \\
 & & \binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} & & & & & & \\
 & & & & & & \ddots & & & & & & & & & &
\end{array}$$

in cui il coefficiente binomiale $\binom{n}{k}$ appare come $(k+1)$-esimo termine della riga $(n+1)$-esima. A parte i coefficienti che appaiono sui lati del triangolo (quelli della forma $\binom{n}{0}$ oppure $\binom{n}{n}$, che sappiamo essere uguali a 1), la formula provata in (**3**) mostra che ciascun coefficiente è la somma dei due che gli sono sopra, cioè, nel rigo superiore, uno immediatamente a sinistra, l'altro immediatamente a destra. Ciò permette di calcolare in modo relativamente semplice i coefficienti binomiali: quelli sui lati sono già noti (sono tutti 1), quindi conosciamo già le prime due righe, il termine centrale della terza riga, cioè $\binom{2}{1}$ lo ricaviamo come somma tra i due termini della prima, quindi $\binom{2}{1} = 1+1 = 2$, come in effetti già sapevamo. Essendo ora nota la terza riga possiamo calcolare la quarta: $\binom{3}{1} = 1+2 = 3$ (i due primi termini della terza riga sono, appunto, 1 e 2) e, similmente, $\binom{3}{2} = 2+1 = 3$; dalla quarta riga ricaviamo la quinta … e così via. Iterando il procedimento possiamo calcolare (ricorsivamente) ciascun coefficiente binomiale a cui siamo interessati; per questo procedimento è solo necessario eseguire delle addizioni. Le prime righe sono dunque:

$$\begin{array}{ccccccccccccccc}
 & & & & & & 1 & & & & & & & & \\
 & & & & & 1 & & 1 & & & & & & & \\
 & & & & 1 & & 2 & & 1 & & & & & & \\
 & & & 1 & & 3 & & 3 & & 1 & & & & & \\
 & & 1 & & 4 & & 6 & & 4 & & 1 & & & & \\
 & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & & & \\
1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 & & \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & .
\end{array}$$

Ad esempio, nella settima riga il terzo termine è 15, ottenuto come $5+10$, dunque $\binom{6}{2} = 15$. Si può anche notare come questo triangolo sia simmetrico rispetto al suo asse verticale (ciascuno dei numeri che appare coincide con quello che occupa la posizione simmetrica rispetto a quest'asse); questa proprietà è precisamente quella espressa in (**1**).

Oltre al metodo offerto dal triangolo di Tartaglia-Pascal, esiste una maniera diretta di calcolare i coefficienti binomiali:

4. *Siano $n, k \in \mathbb{N}$ e supponiamo $k \leq n$. Allora* $\displaystyle\binom{n}{k} = \frac{n!}{k!(n-k)!}$.

Dimostrazione — Non è difficile dimostrare questa formula per induzione, utilizzando a questo scopo la relazione ricorsiva stabilita in (**3**). Possiamo però anche procedere in modo del tutto indipendente e diretto.

Sia S un insieme costituito da n elementi, e sia I un qualsiasi insieme costituito da k elementi. Sappiamo che esistono esattamente $n^{\underline{k}} = n!/(n-k)!$ applicazioni iniettive da I a S. Ciascuna di queste applicazioni iniettive ha per immagine una k-parte di S. Viceversa, ogni k-parte X di S è immagine di qualche applicazione iniettiva da I a S; più precisamente possiamo osservare che le applicazioni iniettive da I ad S che hanno X come immagine sono tante quante le applicazioni biettive $I \to X$, quindi $k!$. Da questo segue subito che il numero $n^{\underline{k}}$ delle applicazioni iniettive da I a S è pari al prodotto tra $\binom{n}{k}$, il numero delle k-parti di S e $k!$, il numero delle applicazioni iniettive che hanno per immagine una qualsiasi prefissata k-parte di S. Dunque,

$$\frac{n!}{(n-k)!} = n^{\underline{k}} = k!\binom{n}{k},$$

da cui segue la formula nell'enunciato.

Tutto questo dovrebbe essere sufficientemente chiaro, ma possiamo anche verificare in maggior dettaglio il fatto che l'insieme F_X delle applicazioni iniettive da I ad S che hanno X come immagine ha cardinalità uguale a quella dell'insieme B_X delle applicazioni biettive da I a X. Se $\iota\colon X \hookrightarrow S$ è l'immersione di X in S, ad ogni $f \in B_X$ possiamo associare l'applicazione $f\iota$, che appartiene certamente a F_X; in questo modo definiamo l'applicazione $f \in B_X \mapsto f\iota \in F_X$, che si vede facilmente essere biettiva. Dunque $|F_X| = |B_X|$. Essendo $|X| = |I| = k$, sappiamo che $|B_X| = k!$, quindi $|F_X| = k!$. □

Il lettore può divertirsi a verificare che sarebbe stata possibile una impostazione differente da quella qui seguita: provare prima (**4**) e poi dedurre da questa formula esplicita tutte le proprietà dei coefficienti binomiali che noi abbiamo invece ricavato in precedenza.

Perché i coefficienti binomiali sono chiamati proprio così? Perché appaiono nell'espressione delle potenze di quello che tradizionalmente veniva (e viene) chiamato un binomio, un'espressione del tipo $a+b$. Ad esempio, siamo abituati a calcolare $(a+b)^2 = a^2+2ab+b^2$, in cui i coefficienti nel secondo termine, 1, 2 e 1, sono proprio quelli che appaiono alla terza riga del triangolo di Tartaglia-Pascal; $(a+b)^3 = a^3+3a^2b+3ab^2+b^3$, e qui i coefficienti, 1, 3, 3 e 1 descrivono la quarta riga dello stesso triangolo. Il risultato generale che spiega questo fenomeno è la cosiddetta *formula del binomio di Newton*:

5. *Siano a e b due elementi di un anello, e supponiamo che valga $ab = ba$. Allora, per ogni intero positivo n:*

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i}b^i.$$

Dimostrazione — Anche in questo caso possiamo scegliere tra diverse possibili dimostrazioni, tra cui una dimostrazione per induzione che si invita a svolgere per esercizio. Diamo una dimostrazione quanto più possibile diretta. Partiamo da un esempio: supponiamo di voler calcolare $(a+b)^3$, cioè $(a+b)(a+b)(a+b)$. Utilizzando più volte la proprietà distributiva abbiamo

$$\begin{aligned}(a+b)^3 = (a+b)(a+b)(a+b) &= a(a+b)(a+b) + b(a+b)(a+b)\\ &= a\big(a(a+b)+b(a+b)\big) + b\big(a(a+b)+b(a+b)\big)\\ &= a\big((aa+ab)+(ba+bb)\big) + b\big((aa+ab)+(ba+bb)\big)\\ &= aaa+aab+aba+abb+baa+bab+bba+bbb.\end{aligned}$$

Come si vede, la terza potenza di $a+b$ si ottiene sommando tutti i possibili prodotti con tre fattori scelti tra a e b (tenendo conto dell'ordine dei fattori). A questo punto possiamo usare il fatto che a e b commutano e quindi, ad esempio, $aab = aba = baa = a^2b$, per raccogliere addendi uguali e riscrivere l'uguaglianza in forma più compatta: $(a+b)^3 = a^3+3a^2b+3ab^2+b^3$.

Passiamo ora alla dimostrazione vera e propria. Qualunque sia l'intero positivo n, segue dalla proprietà distributiva che $(a+b)^n$ è la somma di tutti i possibili prodotti $u_1u_2u_3\dots u_n$ con n fattori ciascuno dei quali sia o a oppure b. Poiché $ab = ba$, ciascuno di questi prodotti si può riscrivere riordinando gli n fattori in modo da far apparire prima tutti i fattori a e poi i fattori b. Supponiamo che il numero di questi ultimi sia i; poiché il numero totale dei fattori è n, ci saranno allora esattamente $n-i$ fattori a; il prodotto sarà dunque $a^{n-i}b^i$ (ad esempio, se $n=5$, il prodotto $abaab$ si può scrivere come a^3b^2). A questo punto sappiamo che $(a+b)^n$ è somma di prodotti della forma $a^{n-i}b^i$, ci serve solo scoprire quante volte appare ciascuno di essi in questa somma. In altri termini, fissato un intero i compreso tra 0 e n, dobbiamo calcolare in quanti modi possiamo scrivere prodotti del tipo $u_1u_2u_3\dots u_n$ (descritti come sopra) con fattori a o b in modo che il fattore b appaia esattamente i volte. Se questa proprietà è realizzata, allora l'insieme $\big\{\lambda \in \{1,2,\dots,n\} \mid u_\lambda = b\big\}$ è una i-parte di $\{1,2\dots,n\}$, viceversa, se X è una qualsiasi i-parte di $\{1,2,\dots,n\}$, allora ponendo $u_\lambda = b$ se $\lambda \in X$ e $u_\lambda = a$ se $\lambda \in \{1,2,\dots,n\} \smallsetminus X$ si ha che $u_1u_2u_3\dots u_n$ è uno dei prodotti del tipo descritto in cui b appare precisamente i volte. Dunque, il numero di tali prodotti è uguale al numero delle i-parti di $\{1,2,\dots,n\}$, cioè $\binom{n}{i}$. Questo vuol dire che si ottiene $(a+b)^n$ come una somma in cui appare una volta a^n (essendo $1 = \binom{n}{0}$), $n = \binom{n}{1}$ volte $a^{n-1}b$, $\binom{n}{2}$ volte $a^{n-2}b^2$, …, $n = \binom{n}{n-1}$ volte ab^{n-1} e una volta b^n, perché $1 = \binom{n}{n}$. Questa è proprio la formula che stavamo cercando di dimostrare. □

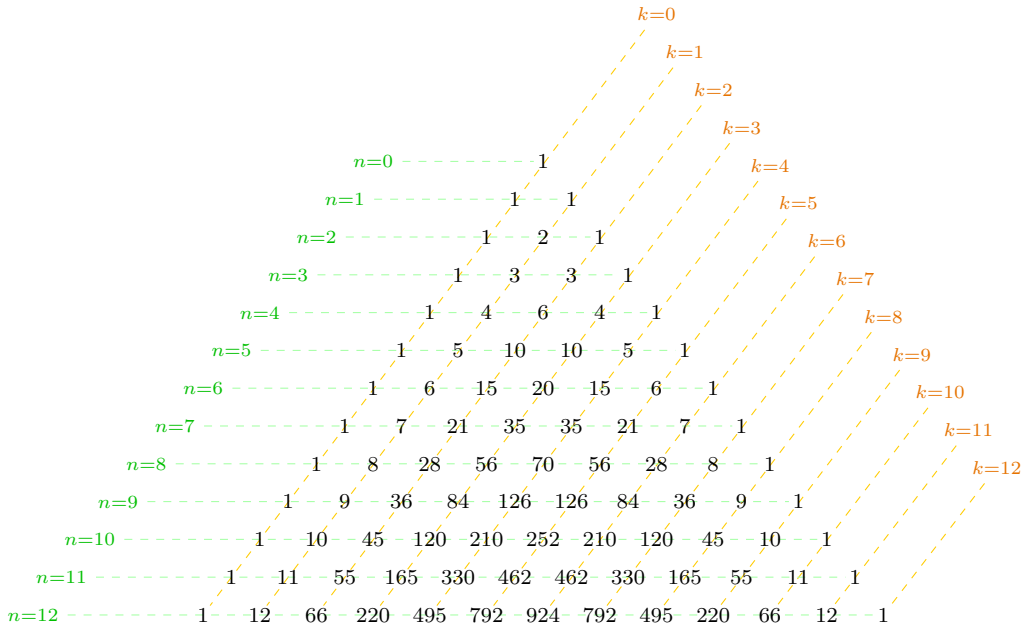
La formula di Newton vale, in particolare, per qualsiasi coppia di elementi a, b di un anello commutativo. È bene però osservare esplicitamente che essa non vale (in anelli non commutativi) nel caso in cui i due elementi a e b non commutino. Ad esempio, calcolando il quadrato di $a+b$ potremo certamente osservare che $(a+b)^2 = a^2+ab+ba+b^2$, ma se $ab \neq ba$ questo elemento sarà certamente diverso da $a^2+2ab+b^2$.

Il triangolo di Tartaglia-Pascal

(i coefficienti binomiali non nulli)

$$\forall\, n, k \in \mathbb{N} \left(\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1} \right)$$

$$\begin{array}{c}
\binom{0}{0} \\
\binom{1}{0}\ \binom{1}{1} \\
\binom{2}{0}\ \binom{2}{1}\ \binom{2}{2} \\
\binom{3}{0}\ \binom{3}{1}\ \binom{3}{2}\ \binom{3}{3} \\
\binom{4}{0}\ \binom{4}{1}\ \binom{4}{2}\ \binom{4}{3}\ \binom{4}{4} \\
\binom{5}{0}\ \binom{5}{1}\ \binom{5}{2}\ \binom{5}{3}\ \binom{5}{4}\ \binom{5}{5} \\
\binom{6}{0}\ \binom{6}{1}\ \binom{6}{2}\ \binom{6}{3}\ \binom{6}{4}\ \binom{6}{5}\ \binom{6}{6} \\
\binom{7}{0}\ \binom{7}{1}\ \binom{7}{2}\ \binom{7}{3}\ \binom{7}{4}\ \binom{7}{5}\ \binom{7}{6}\ \binom{7}{7} \\
\binom{8}{0}\ \binom{8}{1}\ \binom{8}{2}\ \binom{8}{3}\ \binom{8}{4}\ \binom{8}{5}\ \binom{8}{6}\ \binom{8}{7}\ \binom{8}{8} \\
\binom{9}{0}\ \binom{9}{1}\ \binom{9}{2}\ \binom{9}{3}\ \binom{9}{4}\ \binom{9}{5}\ \binom{9}{6}\ \binom{9}{7}\ \binom{9}{8}\ \binom{9}{9} \\
\binom{10}{0}\ \binom{10}{1}\ \binom{10}{2}\ \binom{10}{3}\ \binom{10}{4}\ \binom{10}{5}\ \binom{10}{6}\ \binom{10}{7}\ \binom{10}{8}\ \binom{10}{9}\ \binom{10}{10} \\
\binom{11}{0}\ \binom{11}{1}\ \binom{11}{2}\ \binom{11}{3}\ \binom{11}{4}\ \binom{11}{5}\ \binom{11}{6}\ \binom{11}{7}\ \binom{11}{8}\ \binom{11}{9}\ \binom{11}{10}\ \binom{11}{11} \\
\binom{12}{0}\ \binom{12}{1}\ \binom{12}{2}\ \binom{12}{3}\ \binom{12}{4}\ \binom{12}{5}\ \binom{12}{6}\ \binom{12}{7}\ \binom{12}{8}\ \binom{12}{9}\ \binom{12}{10}\ \binom{12}{11}\ \binom{12}{12}
\end{array}$$



Cancellabilità

A livello di linguaggio informale, la parola "cancellabile" ha in algebra lo stesso significato che ha nella lingua italiana di ogni giorno: "cancellabile" significa "che si può cancellare", intendendo con questo che chiamiamo a cancellabile quando possiamo dedurre da ogni uguaglianza della forma $ax = ay$ (oppure $xa = ya$) l'uguaglianza $x = y$.

Diamo una definizione più precisa. Sia S un insieme dotato di un'operazione binaria interna $*$, e sia $a \in S$. Diciamo che a è *cancellabile a sinistra* in $(S, *)$ se e solo se si ha:

$$(\forall\, b, c \in S)(a * b = a * c \Rightarrow b = c).$$

Si può riformulare questa definizione in modo anche più sintetico: per ogni $a \in S$ si considera la *traslazione sinistra* determinata da a in $(S, *)$, cioè l'applicazione

$$\sigma_a \colon x \in S \longmapsto a * x \in S;$$

dovrebbe essere chiaro che a è cancellabile a sinistra se e solo se σ_a è iniettiva.

Esiste ovviamente anche la nozione, analoga, di cancellabilità a destra. Fissati a e S come sopra, diciamo che a è *cancellabile a destra* in $(S, *)$ se e solo se $(\forall\, b, c \in S)(b * a = c * a \Rightarrow b = c)$, ovvero se e solo se la *traslazione destra* determinata da a in $(S, *)$:

$$\delta_a \colon x \in S \longmapsto x * a \in S$$

è iniettiva. Si dice infine che a è *cancellabile* in $(S, *)$ se e solo se a è cancellabile sia a sinistra che a destra in $(S, *)$.

Va tenuto presente che se l'operazione $*$ è commutativa non ha senso distinguere tra cancellabilità a sinistra, cancellabilità a destra e cancellabilità: le tre proprietà sono in questo caso equivalenti.

È anche il caso di osservare esplicitamente in che modo va negata la cancellabilità: un elemento a di S non è cancellabile a sinistra in $(S, *)$ se e solo se esistono b e c in S tali che $a * b = a * c$ ma $b \neq c$; in modo analogo si nega la cancellabilità a destra.

Esempi. Ogni numero intero è cancellabile in $(\mathbb{Z}, +)$ (se a, b e c sono interi, da $a + b = a + c$ segue senz'altro $b = c$); allo stesso modo ogni intero diverso da 0 è cancellabile in $(\mathbb{Z}, \cdot)$, invece il numero 0 non è cancellabile in $(\mathbb{Z}, \cdot)$: infatti $0 \cdot 5 = 0 \cdot 2$ ma $5 \neq 2$. Similmente, in $(\mathcal{P}(\mathbb{Z}), \cup)$, $\mathbb{N}$ non è cancellabile perché, ad esempio, $\mathbb{N} \cup \{2\} = \mathbb{N} \cup \varnothing$.

Proposizione 1. *Sia $(S, *, e)$ un monoide e sia $a \in S$. Se a è simmetrizzabile a sinistra (risp. simmetrizzabile a destra, simmetrizzabile) rispetto a $*$, allora a è cancellabile a sinistra (risp. cancellabile a destra, cancellabile) rispetto a $*$.*

Dimostrazione — Consideriamo il caso in cui a è simmetrizzabile a sinistra. Esiste $a' \in S$ tale che $a' * a = e$. Per ogni $b, c \in S$, se $a * b = a * c$ abbiamo:

$$b = e * b = (a' * a) * b = a' * (a * b) = a' * (a * c) = (a' * a) * c = e * c = c.$$

In accordo con la definizione, ciò prova che a è cancellabile a sinistra rispetto a $*$. Per il caso della cancellabilità a destra la dimostrazione è analoga. Infine, se a è simmetrizzabile (cioè simmetrizzabile sia a sinistra che a destra), esso è cancellabile sia a sinistra che a destra (cioè cancellabile), come segue dalla simultanea applicazione dei due casi (sinistro e destro) appena considerati. □

L'enunciato precedente fornisce un modo molto semplice per giustificare il fatto che, come osservato nell'esempio precedente, tutti i numeri interi sono cancellabili in $(\mathbb{Z}, +)$: essi sono tutti simmetrizzabili. Invece gli interi diversi da 0, che pure sono cancellabili in $(\mathbb{Z}, \cdot)$ non sono simmetrizzabili in questo monoide. Concludiamo dunque che, in generale, mentre la simmetrizzabilità implica la cancellabilità, l'implicazione inversa può non valere: la cancellabilità non implica necessariamente la simmetrizzabilità. Questa implicazione vale però nel caso dei monoidi (ed in un certo senso, più generalmente, per i semigruppi) *finiti*, come ora dimostreremo.

Lemma 2. *Sia a un elemento del semigruppo finito $(S, *)$. Se σ_a è definita come sopra, sono equivalenti:*
(i) a è cancellabile a sinistra in $(S, *)$;
(ii) σ_a è iniettiva;
(iii) σ_a è suriettiva;
(iv) σ_a è biettiva.
Inoltre, se a è cancellabile a sinistra allora esistono un elemento s neutro a sinistra in $(S, *)$ ed un elemento $a' \in S$ tale che $a * a' = s$.

Dimostrazione — Abbiamo già osservato che, in generale, a è cancellabile a sinistra se e solo se σ_a è iniettiva, vale a dire: $(i) \iff (ii)$. D'altra parte σ_a è un'applicazione da S ad S, e, poiché S è finito, una tale applicazione è iniettiva se e solo se è suriettiva, dunque se e solo se è biettiva. Ciò prova che (ii), (iii) e (iv) sono tra loro equivalenti.

Resta da dimostrare l'ultima frase dell'enunciato, quella più importante. Se a è cancellabile a sinistra in $(S, *)$ allora σ_a è suriettiva. Esiste, in particolare, $s \in S$ tale che $s^{\sigma_a} = a$, ovvero $a * s = a$. Per ogni $x \in S$ abbiamo $(s * x)^{\sigma_a} = a * (s * x) = (a * s) * x = a * x = x^{\sigma_a}$. Allora, dal momento che σ_a è iniettiva, $s * x = x$. Ciò prova che s è neutro a sinistra in $(S, *)$. Infine, ancora per la suriettività di σ_a, esiste $a' \in S$ tale che $(a')^{\sigma_a} = s$, dunque $a * a' = s$. Il lemma è così dimostrato. □

Allo stesso modo possiamo provare un enunciato duale, in cui la sinistra è stata scambiata con la destra.

Lemma 3. *Sia a un elemento del semigruppo finito $(S, *)$. Se δ_a è definita come sopra, sono equivalenti:*
(i) a è cancellabile a destra in $(S, *)$;
(ii) δ_a è iniettiva;
(iii) δ_a è suriettiva;
(iv) δ_a è biettiva.
Inoltre, se a è cancellabile a destra allora esistono un elemento d neutro a destra in $(S, *)$ ed un elemento $a'' \in S$ tale che $a'' * a = d$.

Arriviamo infine al risultato annunciato:

Teorema 4. *Sia $(S, *)$ un semigruppo finito. Se S possiede elementi cancellabili allora esso è un monoide ed ogni suo elemento cancellabile è simmetrizzabile.*

Dimostrazione — Sia a un elemento cancellabile in $(S, *)$. Per i due lemmi precedenti, S possiede un elemento neutro a sinistra ed un elemento neutro a destra, quindi un elemento neutro. Dunque, $(S, *)$ è un monoide. Inoltre, per gli stessi due lemmi, a possiede un simmetrico sinistro ed un simmetrico destro, quindi è simmetrizzabile. □

Esercizio. L'enunciato del Lemma 2 si può arricchire provando che l'elemento a' lì determinato è a sua volta cancellabile a sinistra in $(S, *)$.

Cancellabilità negli anelli

La nozione di cancellabilità, come quella di invertibilità, ha una grande importanza in teoria degli anelli. In questo contesto una prima precisazione, per quanto ovvia, è necessaria: ogni elemento di un anello è simmetrizzabile, quindi anche cancellabile, rispetto all'operazione additiva, dunque quando si parla di elementi cancellabili o simmetrizzabili in un anello è all'operazione moltiplicativa che si fa riferimento (l'informazione sarebbe inutile se riferita all'addizione). Ad esempio, riprendendo un'osservazione fatta sopra, nell'anello degli interi diciamo che 3 è cancellabile ma non simmetrizzabile, nel dire questo stiamo intendendo cancellabile ma non simmetrizzabile in $(\mathbb{Z}, \cdot)$. In verità, trattandosi di anelli, come spesso quando si usa la notazione moltiplicativa, si preferisce dire 'invertibile' piuttosto che 'simmetrizzabile'; così faremo nel resto di questa nota.

Dai risultati esposti in precedenza, validi in ogni monoide, sappiamo che la nozione di cancellabilità è legata, in ogni anello unitario, a quella di invertibilità: se R è un anello unitario ogni elemento

invertibile a sinistra (risp. a destra) in R è anche cancellabile a sinistra (risp. a destra) in R; abbiamo anche dimostrato che queste due proprietà sono addirittura equivalenti nel caso degli anelli finiti (ma non in generale).

In realtà la nozione di cancellabilità in teoria degli anelli è ancora più strettamente legata ad un'altra nozione, quella di divisore dello zero.

Sia $(R, +, \cdot)$ un anello. Un elemento $a \in R$ si dice *divisore sinistro dello zero* in R se esiste $b \in R \setminus \{0\}$ tale che $ab = 0$. Analogamente, si dice che a e un *divisore destro dello zero* in R se esiste un elemento b diverso da zero in R tale che $ba = 0$. Si dice semplicemente che a è un divisore dello zero se a è o un divisore sinistro o un divisore destro dello zero (si noti la differenza, in questo, rispetto alle definizioni di elemento cancellabile e di elemento simmetrizzabile, in cui è richiesto che la proprietà sia verificata sia a sinistra che a destra). Allo scopo di evitare confusione, osserviamo che molti autori preferiscono richiedere in queste definizione anche che a sia diverso da zero (quindi non considerano 0 un divisore dello zero); noi non lo stiamo facendo, quindi consideriamo (in ogni anello con almeno due elementi) 0 un divisore dello zero. Per maggior chiarezza chiamiamo divisore proprio (o, nel caso, divisore sinistro, o destro, proprio) dello zero un divisore dello zero che sia diverso da zero. Il nesso tra queste nozioni e quella di cancellabilità è dato da:

Proposizione 5. *Sia a un elemento dell'anello R. Allora, in R, a è cancellabile a sinistra (risp. cancellabile a destra, cancellabile) se e solo se a non è un divisore sinistro (risp. divisore destro, divisore) dello zero.*

Dimostrazione — Dimostriamo l'equivalenza delle due proprietà facendo vedere che sono equivalenti le loro negazioni. Supponiamo che a sia un divisore sinistro dello zero. Allora esiste $b \in R$ tale che $b \neq 0 = ab$. Dunque $a0 = ab$ ma $0 \neq b$, quindi a non è cancellabile a sinistra. Viceversa, se a non è cancellabile a sinistra esistono in R due elementi distinti, b e c tali che $ab = ac$. Allora $a(b - c) = ab - ac = 0$, inoltre $b - c \neq 0$, dunque a è un divisore sinistro dello zero.

Abbiamo così mostrato che la proprietà di essere cancellabile a sinistra equivale alla proprietà di non essere un divisore sinistro dello zero, in modo analogo (oppure per dualità) si prova l'enunciato corrispondente per la destra che sostituisce la sinistra. A questo punto possiamo anche dire che un elemento a di R è cancellabile se e solo se non è un divisore sinistro dello zero né un divisore destro dello zero, per una delle leggi di De Morgan ciò equivale a dire che a non è un divisore dello zero. □

Un anello si dice *integro* se in esso vale la *legge di annullamento del prodotto*:

$$(\forall\, a, b \in R)\big(ab = 0 \Rightarrow (a = 0 \vee b = 0)\big),$$

ovvero: se un prodotto è zero allora almeno uno dei suoi fattori è zero; in forma contrapposta ciò si può anche esprimere dicendo che il prodotto di due qualsiasi elementi diversi da zero è diverso da zero. Con la terminologia appena introdotta, possiamo riformulare questa condizione in questo modo: un anello è integro se e solo se non ha divisori propri dello zero (infatti, se $ab = 0$ e $a \neq 0 \neq b$, allora a e b sono divisori propri dello zero). Per quanto appena dimostrato, ciò equivale anche a dire che nell'anello in questione ogni elemento diverso da zero è cancellabile.

Il caso più importante è quello dei domini di integrità, che sono gli anelli integri commutativi. Possiamo formularne la definizione in uno qualsiasi dei seguenti modi, tra loro equivalenti: un *dominio di integrità* è:

- un anello commutativo integro;
- un anello commutativo in cui vale la legge di annullamento del prodotto;
- un anello commutativo privo di divisori propri dello zero;
- un anello commutativo in cui ogni elemento diverso da zero è cancellabile.

Esempi di domini di integrità sono i campi (in cui ogni elemento non nullo è addirittura invertibile) e l'anello degli interi, che invece non è un campo. Va osservato che se R è un anello integro, quindi, in particolare, se è un dominio di integrità, allora $R^{\#} := R \setminus \{0\}$ è una parte stabile del semigruppo $(R, \cdot)$ (questa è, chiaramente, una delle formulazioni della legge di annullamento del prodotto) quindi è esso stesso un semigruppo; per la Proposizione 5 risulta addirittura che $(R^{\#}, \cdot)$ è un semigruppo regolare, cioè un semigruppo in cui tutti gli elementi sono cancellabili.

Una conseguenza del Teorema 4 è poi questa: se R è un anello finito, allora ogni suo elemento cancellabile è invertibile (intendendo con questo anche che l'anello è unitario se ha almeno un elemento cancellabile). Un esempio di questa situazione si ha tra i quozienti propri di $\mathbb{Z}$: questi sono anelli

finiti e, infatti, in ciascuno di essi gli elementi cancellabili sono precisamente gli invertibili; i restanti elementi sono i divisori dello zero. Più in particolare, se R è un dominio di integrità finito, allora ogni elemento non nullo di R è cancellabile e dunque, sempre per il Teorema 4, invertibile (risultando R unitario). Pertanto R è un campo. Abbiamo così provato:

6. *Ogni dominio di integrità finito è un campo.*

Questo stesso ragionamento mostra che ogni anello integro finito è un corpo. Solo a titolo di notizia, aggiungiamo che vale anche un teorema, di natura meno elementare di quelli che sono qui trattati, secondo il quale *ogni corpo finito è commutativo* (cioè è un campo); si può dunque concludere, più in generale, che ogni anello integro finito è un campo.

Partizioni ed equivalenze

GIOVANNI CUTOLO

In queste pagine vengono presentate due nozioni insiemistiche di grande importanza e strettamente collegate tra loro, quella di partizione e quella di relazione di equivalenza. Come vedremo le due nozioni sono di fatto interscambiabili.

1. Partizioni

Sia A un insieme. Per definizione, una partizione di A è un insieme $\mathcal{F}$ di parti non vuote di A con la proprietà che ciascun elemento di A appartenga ad uno ed un solo elemento di $\mathcal{F}$, vale a dire:

$$\mathcal{F} \subseteq \mathcal{P}(A) \smallsetminus \{\varnothing\} \qquad \wedge \qquad \forall x \in A \left(\exists! y \in \mathcal{F}(x \in y)\right).$$

Ad esempio, se A è l'insieme $\{1,2,3\}$, allora una delle partizioni di A è l'insieme $\big\{\{1\},\{2,3\}\big\}$. Non vanno confuse tra loro le nozioni di partizione e quella di parte, che sono molto diverse tra loro benché abbiano nomi simili: quasi sempre una parte (cioè un sottoinsieme) di un insieme non ne è una partizione ed una partizione non ne è una parte. Gli elementi di una partizione vengono qualche volta chiamati anche *blocchi* della partizione.

Una semplice caratterizzazione delle partizioni è data dalla seguente proposizione.

Proposizione 1. *Siano A e $\mathcal{F}$ due insiemi. Allora $\mathcal{F}$ è una partizione di A se e solo se valgono le seguenti tre proprietà:*

(i) $\bigcup \mathcal{F} = A$;
(ii) $\forall b, c \in \mathcal{F}\ (b \neq c \Rightarrow b \cap c = \varnothing)$;
(iii) $\forall b \in \mathcal{F}\ (b \neq \varnothing)$.

Dimostrazione. Supponiamo in primo luogo che $\mathcal{F}$ sia una partizione di A e proviamo che valgono (i), (ii) e (iii). Per definizione di partizione, $\varnothing \notin \mathcal{F}$, quindi è certamente verificata la condizione (iii). Inoltre, ogni elemento di $\mathcal{F}$ è una parte di A, quindi $\bigcup \mathcal{F} \subseteq A$ e, viceversa, sempre per definizione di partizione, ogni elemento di A appartiene ad un elemento di $\mathcal{F}$, quindi $A \subseteq \bigcup \mathcal{F}$ e possiamo concludere che vale (i)[(1)]. Dimostriamo (ii) ragionando per assurdo. Supponiamo che (ii) sia falsa, cioè che esistano $b, c \in \mathcal{F}$ tali che $b \neq c$ e $b \cap c = \varnothing$.[(2)] Fissati tali b e c, allora esiste $x \in b \cap c$; dunque x è un elemento di A che appartiene a due elementi distinti di $\mathcal{F}$ (a b ed a c), in contraddizione con la definizione di partizione. Questa contraddizione mostra che così come (i) e (iii), anche (ii) è vera se $\mathcal{F}$ è una partizione di A.

Abbiamo dimostrato che la condizione espressa nell'enunciato è necessaria affinché $\mathcal{F}$ sia una partizione; proviamone la sufficienza. Supponiamo dunque che valgano (i), (ii) e (iii). Sia b un elemento di $\mathcal{F}$. Ovviamente $b \subseteq \bigcup \mathcal{F}$, quindi, per (i), b è una parte di A e, per (iii), $b \neq \varnothing$. Sia ora $x \in A$. Allora, per (i), x appartiene ad almeno un elemento, chiamiamolo ancora b, di $\mathcal{F}$. Se x appartenesse anche ad un elemento c di $\mathcal{F}$ diverso da b, allora avremmo $x \in b \cap c$, quindi $b \cap c \neq \varnothing$ e, poiché $b \neq c$, sarebbe contraddetta (ii). Dunque $\mathcal{F}$ è un insieme di parti non vuote di A ed ogni elemento di A appartiene ad esattamente un elemento di $\mathcal{F}$, quindi $\mathcal{F}$ è una partizione di A, come richiesto. □

In termini più sintetici (ma meno espliciti), la proposizione ci dice che una partizione di un insieme A è un insieme di parti non vuote di A, a due a due disgiunte, la cui unione sia A.

Spesso viene usata la condizione richiesta da questa caratterizzazione come definizione della nozione di partizione. Ovviamente questo approccio è perfettamente equivalente al nostro.

Indicheremo con $\mathrm{Partz}(A)$ l'insieme delle partizioni dell'insieme A. Segue facilmente dalla definizione che l'unica partizione dell'insieme vuoto è l'insieme vuoto stesso (vale a dire: $\mathrm{Partz}(\varnothing) = \{\varnothing\}$). Se A è un insieme non vuoto, tra le sue partizioni ci sono certamente le cosiddette *partizioni banali*, che sono quella costituita dai singleton degli elementi di A, vale a dire $\mathcal{P}_1(A) = \big\{\{x\} \mid x \in A\big\}$, e quella che ha A stesso come unico elemento, vale a dire $\{A\}$. A titolo di esercizio, può essere utile verificare le affermazioni appena fatte e le seguenti:

- L'unica partizione dell'insieme vuoto è l'insieme vuoto stesso.
- Se A è un singleton, allora $\{A\}$ è l'unica partizione di A (in questo caso, quindi le partizioni banali di A coincidono. Ovviamente, se $A = \{x\}$, allora $\{A\} = \big\{\{x\}\big\}$);
- Se $|A| = 2$, allora A ha esattamente due partizioni, quelle banali, che in questo caso non coincidono. Ad esempio, se $A = \{1,2\}$, allora $\mathrm{Partz}(A)$ ha due elementi: la partizione $\mathcal{P}_1(A) = \big\{\{1\},\{2\}\big\}$ e la partizione $\big\{\{A\}\big\}$.

[(1)] ricordiamo che $\bigcup \mathcal{F}$, anche scritto $\bigcup_{b \in \mathcal{F}} b$, è l'insieme $\{x \mid \exists b \in \mathcal{F}\,(x \in b)\}$ degli oggetti che appartengano ad almeno un elemento di $\mathcal{F}$.

[(2)] la negazione di (ii) è espressa da: $\exists b, c \in \mathcal{F}\ (b \neq c \wedge b \cap c \neq \varnothing)$.

- Se $|A| = \{1, 2, 3\}$, allora A ha esattamente cinque partizioni: le due banali, $\mathcal{P}_1(A) = \big\{\{1\}, \{2\}, \{3\}\big\}$ e $\big\{\{A\}\big\}$, ed inoltre le tre partizioni $\big\{\{1\}, \{2, 3\}\big\}$, $\big\{\{2\}, \{1, 3\}\big\}$, $\big\{\{3\}, \{2, 3\}\big\}$ costituite da un singleton ed un insieme di due elementi.
- Per ogni insieme A ed ogni suo sottoinsieme x tale che $\varnothing \neq x \neq A$, l'insieme $\{x, A \smallsetminus x\}$ è una partizione di A. Questo non resta vero se non si richiede la condizione $\varnothing \neq x \neq A$, come mai? Verificare che ogni partizione $\mathcal{F}$ di A tale che $|\mathcal{F}| = 2$ ha questa stessa forma, infatti se x ne è un elemento, allora l'altro elemento di $\mathcal{F}$ è $A \smallsetminus x$.

La penultima affermazione può essere giustificata (anche) facendo uso di questa osservazione davvero elementare:

- Sia A un insieme finito e sia $\mathcal{F} \in \mathrm{Partz}(A)$. Allora $|A| = \sum_{b \in \mathcal{F}} |b|$.

Infine, dalla definizione di partizione segue che per ogni insieme A ed ogni sua partizione $\mathcal{F}$ è ben definita l'applicazione $\pi_{\mathcal{F}} \colon A \to \mathcal{F}$ che a ciascun $x \in A$ associa l'unico $b \in \mathcal{F}$ tale che $x \in b$. Chiamiamo $\pi_{\mathcal{F}}$ la *proiezione* di A su $\mathcal{F}$. Abbiamo:

Lemma 2. *Per ogni A ed ogni $\mathcal{F} \in \mathrm{Partz}(A)$ la proiezione $\pi_{\mathcal{F}}$ di A su $\mathcal{F}$ è suriettiva.*

Dimostrazione. Dobbiamo provare che ogni elemento di $\mathcal{F}$ è nell'immagine di $\pi_{\mathcal{F}}$. Sia $b \in \mathcal{F}$. Poiché, per definizione di partizione, $b \neq \varnothing$, esiste $x \in b$. Fissato un tale x, allora b è l'unico elemento di $\mathcal{F}$ a cui x appartiene, dunque $b = \pi_{\mathcal{F}}(x)$ e $b \in \operatorname{im} \pi_{\mathcal{F}}$. Pertanto, $\pi_{\mathcal{F}}$ è suriettiva. □

2. Relazioni di equivalenza

Fissiamo un insieme A. Una relazione binaria $\sim$ in A è, come ben noto, una *relazione di equivalenza* se e solo se verifica ciascuna delle tre proprietà:

riflessiva: $\forall x \in A\ (x \sim x)$;
simmetrica: $\forall x, y \in A\ (x \sim y \Rightarrow y \sim x)$;
transitiva: $\forall x, y, z \in A\ \big((x \sim y \wedge y \sim z) \Rightarrow x \sim z\big)$.

Indichiamo con $\mathrm{Eq}(A)$ l'insieme delle relazioni di equivalenza in A. Vediamo alcuni esempi; è importante che chi legge sia in grado di giustificare pienamente tutte le affermazioni che seguono:

(1) Per ogni insieme A, come è facile verificare (farlo!) sono relazioni di equivalenza la relazione di uguaglianza in A (rispetto alla quale due qualsiasi elementi x e y di A sono in relazione se e solo $x = y$) e la relazione universale in A (cioè la relazione binaria τ in A tale che $x\ \tau\ y$ per ogni $x, y \in A$). La relazione di uguaglianza in A ha per grafico l'insieme $\Delta_A := \{(x, x) \mid x \in A\}$, mentre la relazione universale ha per grafico $A \times A$.
(2) Sia ρ la relazione binaria in $\mathbb{Z}$ definita da: $\forall x, y \in \mathbb{Z}\ (x\ \rho\ y \iff x + y$ è pari). Verifichiamo che ρ è di equivalenza. Per ogni $x \in \mathbb{Z}$, il numero $x + x = 2x$ è pari, quindi $x\ \rho\ x$; dunque vale la proprietà riflessiva. Per ogni $x, y \in \mathbb{Z}$ abbiamo $x\ \rho\ y \iff x + y$ è pari $\iff y + x$ è pari $\iff y\ \rho\ x$; vale quindi anche la proprietà simmetrica. Infine, verifichiamo la proprietà transitiva: siano $x, y, z \in \mathbb{Z}$ ed assumiamo $x\ \rho\ y$ e $y\ \rho\ z$. Allora $x + y$ e $y + z$ sono pari, quindi è pari la loro somma $x + 2y + z$ e quindi anche $x + z = (x + y) + (y + z) - 2y$, dunque $x\ \rho\ z$. Pertanto $\rho \in \mathrm{Eq}(A)$.
(3) Modifichiamo l'esempio precedente considerando la relazione binaria ρ_3 definita in modo analogo alla precedente ma sostituendo la nozione di numero pari (cioè multiplo di 2) con quella di numero multiplo di 3. Dunque ρ_3 è la relazione binaria in $\mathbb{Z}$ definita da: $\forall x, y \in \mathbb{Z}\ (x\ \rho_3\ y \iff x+y$ è multiplo di 3). La relazione ρ_3 non è riflessiva (infatti, ad esempio, $1 \not\rho_3 1$), quindi non è di equivalenza. Cambiando ancora relazione, definiamo ρ_3^*, ancora una relazione binaria in $\mathbb{Z}$, ponendo: $\forall x, y \in \mathbb{Z}\ \big(x\ \rho_3^*\ y \iff (x = y \vee x\ \rho_3\ y)\big)$. A differenza della precedente, ρ_3^* è riflessiva, inoltre essa è simmetrica, ma non è transitiva, ad esempio perché $1\ \rho_3^*\ 2$ e $2\ \rho_3^*\ 4$, ma $1 \not\rho_3^* 4$. Dunque, neanche ρ_3^* è una relazione di equivalenza.
(4) Sia σ la relazione binaria definita in $\mathcal{P}(\mathbb{Z})$ ponendo, per ogni $x, y \in \mathcal{P}(\mathbb{Z})$, $x\ \sigma\ y \iff x \cap \mathbb{N} = y \cap \mathbb{N}$. Per ogni $x \in \mathcal{P}(\mathbb{Z})$ si ha $x \cap \mathbb{N} = x \cap \mathbb{N}$, ovvero $x\ \sigma\ x$, quindi σ è riflessiva; per ogni $x, y \in \mathcal{P}(\mathbb{Z})$, se $x\ \sigma\ y$, cioè $x \cap \mathbb{N} = y \cap \mathbb{N}$, allora $y \cap \mathbb{N} = x \cap \mathbb{N}$, ovvero $y\ \sigma\ x$, quindi σ è simmetrica; per ogni $x, y, z \in \mathcal{P}(\mathbb{Z})$, se $x\ \sigma\ y$ e $y\ \sigma\ z$, cioè $x \cap \mathbb{N} = y \cap \mathbb{N}$ e $y \cap \mathbb{N} = z \cap \mathbb{N}$, allora $x \cap \mathbb{N} = z \cap \mathbb{N}$, cioè $x\ \sigma\ z$. Abbiamo verificato anche la proprietà transitiva per σ, quindi $\sigma \in \mathrm{Eq}(\mathcal{P}(\mathbb{Z}))$.

In modo particolare, l'ultimo degli esempi ammette un'importante generalizzazione, che andiamo ora a discutere.

Sia $f \colon A \to B$ una qualsiasi applicazione di dominio l'insieme A. Si chiama *nucleo di equivalenza di f* la relazione binaria $\mathfrak{K}_f$ definita ponendo, per ogni $x, y \in A$, $x\ \mathfrak{K}_f\ y \iff f(x) = f(y)$. Ad esempio, la relazione di equivalenza σ considerata nell'ultimo degli esempi appena visti è il nucleo di equivalenza dell'applicazione $x \in \mathcal{P}(\mathbb{Z}) \mapsto x \cap \mathbb{N} \in \mathcal{P}(\mathbb{Z})$ (ma anche, ad esempio, della sua ridotta $x \in \mathcal{P}(\mathbb{Z}) \mapsto x \cap \mathbb{N} \in \mathcal{P}(\mathbb{N})$). Non solo in questo caso, ma sempre, i nuclei di equivalenza sono relazioni di equivalenza; verifichiamolo:

Proposizione 3. *Siano $f \colon A \to B$ un'applicazione e $\mathfrak{K}_f$ il suo nucleo di equivalenza. Allora $\mathfrak{K}_f \in \mathrm{Eq}(A)$.*

Dimostrazione. La verifica, molto semplice, segue la falsariga dell'esempio già visto. Per ogni $x \in A$ si ha ovviamente $f(x) = f(x)$, ovvero $x\ \mathfrak{K}_f\ x$, quindi $\mathfrak{K}_f$ è riflessiva; per ogni $x, y \in A$, abbiamo $x\ \mathfrak{K}_f\ y \iff f(x) = f(y) \iff f(y) = f(x) \iff y\ \mathfrak{K}_f\ x$, quindi $\mathfrak{K}_f$ è simmetrica; per ogni $x, y, z \in A$, se $x\ \mathfrak{K}_f\ y$ e $y\ \mathfrak{K}_f\ z$, cioè $f(x) = f(y)$ e $f(y) = f(z)$, allora $f(x) = f(z)$, cioè $x\ \mathfrak{K}_f\ z$; quindi $\mathfrak{K}_f$ è transitiva. □

In alcuni testi il nucleo di equivalenza di un'applicazione viene chiamato *equivalenza associata* (all'applicazione). La costruzione del nucleo di equivalenza fornisce immediatamente un gran numero di esempi di relazioni di equivalenza: per ottenere una relazione di equivalenza in un insieme A basta considerare una qualsiasi applicazione che abbia A come dominio ed il nucleo di equivalenza di questa. Non solo: questa costruzione permette di verificare in modo diretto che alcune relazioni binarie sono di equivalenza. Ad esempio, consideriamo la relazione binaria $\sim$ in $\mathbb{N}$ definita ponendo, per ogni $x, y \in \mathbb{N}$, $x \sim y \iff x^2 - 3x = y^2 - 3y$. Si può verificare che $\sim$ è di equivalenza procedendo, come fatto per gli esempi presentati sopra, a verificare le proprietà riflessiva, simmetrica e transitiva, ma anche, più rapidamente ed in un colpo solo, osservando che $\sim$ è il nucleo di equivalenza dell'applicazione $n \in \mathbb{N} \mapsto n^2 - 3n \in \mathbb{Z}$, e quindi $\sim \in \mathrm{Eq}(\mathbb{N})$ per la proposizione 3.

Un punto molto importante, che discuteremo più avanti (corollario 10), è che quella dei nuclei di equivalenza non è semplicemente una costruzione che fornisce esempi di relazioni di equivalenza, ma è l'esempio più generale possibile, nel senso che le fornisce tutte: vedremo infatti che ogni relazione di equivalenza è il nucleo di equivalenza di qualche applicazione.

Esercizio 4. Determinare le applicazioni f tali che...

i) ...il nucleo di equivalenza di f sia la relazione di uguaglianza nel dominio di f;
ii) ...il nucleo di equivalenza di f sia la relazione universale nel dominio di f.

3. Classi di equivalenza ed insieme quoziente

Forse la più importante nozione legata alle relazioni di equivalenza è quella di classe di equivalenza. Siano A un insieme, x un suo elemento e $\sim \in \mathrm{Eq}(A)$. La *classe di equivalenza* di x rispetto a $\sim$ (si dice anche: "modulo $\sim$") è l'insieme

$$[x]_\sim := \{y \in A \mid y \sim x\},$$

che è ovviamente una parte di A. Osserviamo subito che, per ogni $x \in A$, $x \in [x]_\sim$, per la proprietà riflessiva di $\sim$ (dunque $[x]_\sim \neq \varnothing$), e $[x]_\sim = \{y \in A \mid x \sim y\}$, dal momento che, per la proprietà simmetrica, scelti comunque x e y in A si ha $y \sim x \iff x \sim y$.

Con queste stesse notazioni, si chiama *insieme quoziente* (di A rispetto a $\sim$, o modulo $\sim$) l'insieme

$$A/\sim = \{[x]_\sim \mid x \in A\}$$

di tutte le classi di equivalenza rispetto a $\sim$ degli elementi di A.

Facciamo un esempio: se ρ è la relazione di equivalenza in $\mathbb{Z}$ presentata all'esempio (2) di pagina 2, allora $[0]_\rho = \{n \in \mathbb{Z} \mid n + 0 \text{ è pari}\}$, quindi $[0]_\rho$ è l'insieme $P = 2\mathbb{Z}$ dei numeri interi pari. Similmente $[1]_\rho = \{n \in \mathbb{Z} \mid n + 1 \text{ è pari}\}$ è l'insieme $D = \mathbb{Z} \setminus 2\mathbb{Z}$ dei numeri interi dispari. Seguirà dai prossimi risultati che ci accingiamo a provare che $\mathbb{Z}/\rho$ è una partizione di $\mathbb{Z}$, e di conseguenza, poiché $\mathbb{Z} = P \cup D$, si ha $\mathbb{Z}/\rho = \{P, D\}$.

Le proprietà principali delle classi di equivalenza sono raccolte nella proposizione 7; per comodità di esposizione ne verifichiamo prima un caso particolare:

Lemma 5. *Siano A un insieme, $\sim \in \mathrm{Eq}(A)$ e $x, y \in A$. Sono allora equivalenti:*

(i) $x \sim y$;
(ii) $x \in [y]_\sim$;
(iii) $[x]_\sim = [y]_\sim$.

Dimostrazione. Per definizione di classe d'equivalenza, certamente (i) $\iff$ (ii). Supponiamo ora che valga (i). Per ogni $z \in [x]_\sim$ si ha, sempre per la stessa definizione, $z \sim x$, quindi, per la proprietà transitiva, $z \sim y$, cioè $z \in [y]_\sim$. Dunque, se vale (i), allora $[x]_\sim \subseteq [y]_\sim$. Ma, se vale (i) si ha anche $y \sim x$, per la proprietà simmetrica, quindi, scambiando i ruoli di x e di y, abbiamo anche $[y]_\sim \subseteq [x]_\sim$. Abbiamo così provato che (i) implica (iii). Infine, se assumiamo (iii), poiché, come sappiamo, $x \in [x]_\sim$ per la proprietà riflessiva, concludiamo $x \in [y]_\sim$. Dunque (iii) implica (ii). A questo punto la dimostrazione è completa. □

Proposizione 6. *Siano A un insieme e $\sim \in \mathrm{Eq}(A)$. Allora $A/\sim$ è una partizione di A. Inoltre, per ogni $x \in A$, l'unica classe di equivalenza rispetto a $\sim$ a cui x appartenga è $[x]_\sim$.*

Dimostrazione. Per ogni $x \in A$, sappiamo che vale $x \in [x]_\sim$. Se $y \in A$ è tale che $x \in [y]_\sim$, allora, per il lemma precedente, $[y]_\sim = [x]_\sim$. Possiamo concludere che $[x]_\sim$ è l'unica classe di equivalenza rispetto a $\sim$ a cui x appartenga (giustificando così l'ultima parte dell'enunciato). Abbiamo anche provato che $A/\sim$ è un insieme di parti non vuote di A con la proprietà che ogni elemento di A appartenga ad uno ed un solo elemento di $A/\sim$, quindi $A/\sim \in \mathrm{Partz}(A)$, come richiesto dalla prima parte dell'enunciato. □

Proposizione 7. *Siano A un insieme, $\sim \in \mathrm{Eq}(A)$ e $x, y \in A$. Sono allora equivalenti:*

(i) $x \sim y$;
(ii) $y \sim x$;
(iii) $x \in [y]_\sim$;
(iv) $y \in [x]_\sim$;
(v) $[x]_\sim = [y]_\sim$;
(vi) $[x]_\sim \cap [y]_\sim \neq \varnothing$.

Dimostrazione. (i) e (ii) sono equivalenti tra loro per la proprietà simmetrica, e, per il lemma 5, sono anche equivalenti a (iii), (iv) e (v). Se queste valgono, allora, ovviamente, $[x]_\sim \cap [y]_\sim = [x]_\sim \neq \varnothing$, e quindi vale (vi). Infine, $[x]_\sim$ e $[y]_\sim$ sono due elementi di $A/\!\sim$, che è una partizione per la proposizione 6, quindi, come segue dalla proposizione 1, se $[x]_\sim \neq [y]_\sim$, allora $[x]_\sim \cap [y]_\sim = \varnothing$. Questo vuol dire che (vi) implica (v); a questo punto la dimostrazione è completata.[3] □

Possiamo aggiungere un semplice esercizio: nelle ipotesi della proposizione 7, anche la condizione $[x]_\sim \subseteq [y]_\sim$ equivale a $x \sim y$.

È utile fissare l'attenzione su questo punto stabilito nella proposizione 7: scelti comunque due elementi x e y di un insieme A sul quale sia assegnata una relazione di equivalenza $\sim$, si verifica necessariamente una delle due: o $x \sim y$ e $[x]_\sim = [y]_\sim$, oppure $x \nsim y$ e $[x]_\sim \cap [y]_\sim = \varnothing$.

La proposizione 6 garantisce che ogni insieme quoziente è una partizione. Vale anche l'inverso: ogni partizione è l'insieme quoziente rispetto ad una relazione di equivalenza; più precisamente rispetto ad una ed una sola relazione di equivalenza. Questo è il contenuto del teorema fondamentale su partizioni e relazioni di equivalenza.

Teorema 8. *Per ogni insieme A, l'applicazione $\sim \in \mathrm{Eq}(A) \longmapsto A/\!\sim \in \mathrm{Partz}(A)$ è biettiva.*

Dimostrazione. Chiamiamo α l'applicazione $\sim \in \mathrm{Eq}(A) \mapsto A/\!\sim \in \mathrm{Partz}(A)$ considerata nell'enunciato. Innanzitutto, osserviamo che α è ben definita per la proposizione 6. Per verificare che α è iniettiva, supponiamo che ρ e σ siano relazioni di equivalenza in A tali che $\alpha(\rho) = \alpha(\sigma)$, cioè $A/\rho = A/\sigma$, e proviamo che di conseguenza $\rho = \sigma$. Per ogni $x \in A$, si ha ovviamente $[x]_\rho \in A/\rho$, ma anche $A/\rho = A/\sigma$, quindi $[x]_\rho \in A/\sigma$, vale a dire: $[x]_\rho$ è una classe di equivalenza rispetto a σ. L'unico elemento di A/σ a cui x appartenga è $[x]_\sigma$ (ancora per la proposizione 6), pertanto $[x]_\sigma = [x]_\rho$. Questo vale per ogni $x \in A$. Ora, per ogni $x, y \in A$ abbiamo:

$$x \,\rho\, y \iff [x]_\rho = [y]_\rho \iff [x]_\sigma = [y]_\sigma \iff x \,\sigma\, y,$$

per via del lemma 5 e della coincidenza, appena osservata, tra le classi modulo σ e quelle modulo ρ. La conclusione è che σ e ρ coincidono. Abbiamo così provato che α è iniettiva.

Proviamo ora che α è suriettiva. Sia $\mathcal{F} \in \mathrm{Partz}(A)$, e sia $\pi = \pi_{\mathcal{F}}$ la proiezione di A su $\mathcal{F}$, cioè, ricordiamo, l'applicazione che ad ogni $x \in A$ fa corrispondere quell'unico elemento di $\mathcal{F}$ a cui x appartiene. Sia ora $\sim$ il nucleo di equivalenza di π. Per ogni $x \in A$ la classe $[x]_\sim$ è l'insieme degli $y \in A$ tali che $\pi(y) = \pi(x)$. Come dovrebbe essere chiaro, si ha $\pi(y) = \pi(x)$ se e solo se $y \in \pi(x)$, quindi $[x]_\sim = \pi(x)$. Allora

$$A/\!\sim = \{[x]_\sim \mid x \in A\} = \{\pi(x) \mid x \in A\} = \operatorname{im}\pi = \mathcal{F},$$

per il lemma 2. Abbiamo appena provato che $\mathcal{F}$ è l'immagine di $\sim$ mediante α. Con questo è verificato che α è suriettiva, dunque biettiva. □

La dimostrazione appena esposta fornisce anche una descrizione dell'inversa dell'applicazione α. Se, nelle notazioni del teorema, $\mathcal{F}$ è una partizione di A, allora l'immagine di $\mathcal{F}$ mediante α^{-1} è la relazione di equivalenza $\sim$ in A descritta nella dimostrazione come nucleo di equivalenza di π, cioè quella definita da: $\forall x, y \in A\ (x \sim y \iff \pi(x) = \pi(y))$, o, per darne una descrizione ancora più esplicita, da:

$$\forall x, y \in A\ \big(x \sim y \iff (\exists\, b \in \mathcal{F}(x \in b \wedge y \in b))\big),$$

infatti, se $x \in A$ e $b \in \mathcal{F}$ sono tali che $x \in b$, allora $b = \pi(x)$ (perché $\pi(x)$ è *l'unico* blocco di $\mathcal{F}$ a cui x appartenga), quindi se x e y sono due elementi di A, dire che essi appartengono ad uno stesso blocco di $\mathcal{F}$ equivale a dire: $\pi(x) = \pi(y)$.

Il teorema 8 è di grande importanza: esso stabilisce che il problema di descrivere le relazioni di equivalenza in un dato insieme è essenzialmente lo stesso che quello (generalmente più facile da affrontare direttamente) dello studio delle partizioni dello stesso insieme. Per descrivere le prime basta descrivere le seconde ed usare la biezione che abbiamo chiamato α^{-1} per 'tradurre' le partizioni in relazioni di equivalenza. Facciamo qualche esempio:

(1) Sia $A = \{n \in \mathbb{N} \mid n < 10\}$ e consideriamo la partizione $\mathcal{F} = \big\{\{0, 2, 4\}, \{1\}, \{3, 9\}, \{5, 6, 7, 8\}\big\}$ di A (è una partizione, vero?). Qual è la relazione di equivalenza $\sim$ di A che corrisponde ad $\mathcal{F}$? In accordo con quanto appena stabilito, è quella descritta dalla proprietà che due arbitrari elementi di A siano in relazione se e solo se appartengono allo stesso blocco di $\mathcal{F}$. Dunque sono equivalenti tra loro 0, 2 e 4 (che però non sono equivalenti ad altri elementi di A), 1 è equivalente solo a sé stesso;[4] sono equivalenti tra loro 3 e 9 ed infine sono equivalenti tra loro (ma non equivalenti a 1, 3 e 9) i rimanenti elementi: 5, 6, 7 e 8. Per essere ancora più espliciti, il grafico di $\sim$ è l'insieme

$$(\{0, 2, 4\} \times \{0, 2, 4\}) \cup \{(1, 1)\} \cup (\{3, 9\} \times \{3, 9\}) \cup (\{5, 6, 7, 8\} \times \{5, 6, 7, 8\}),$$

[3] A titolo di esercizio, o di ulteriore chiarificazione, mostriamo anche in che modo si può dedurre che (vi) implica (v) per via diretta. Assumiamo che valga (vi). Allora esiste $z \in [x]_\sim \cap [y]_\sim$, dunque z appartiene sia a $[x]_\sim$ che a $[y]_\sim$. Ma, per la proposizione 6, $[z]_\sim$ è l'unica classe rispetto a $\sim$ a cui z appartenga, dunque $[x]_\sim = [z]_\sim = [y]_\sim$ e quindi $[x]_\sim = [y]_\sim$.

[4] chi avesse perplessità sull'ortografia può consultare il sito dell'Accademia della Crusca, ad esempio 1, 2 o 3

cioè l'insieme

$$\{(0,0),(1,1),(2,2),(3,3),(4,4),(5,5),(6,6),(7.7),(8,8),(9,9),$$
$$(0,2),(2,0),(2,4),(4,2),(0,4),(4,0),(3,9),(9,3),$$
$$(5,6),(6,5),(5,7),(7,5),(5,8),(8,5),(6,7),(7,6),(6,8),(8,6),(7,8),(8,7)\}$$

che può essere rappresentato, in modo molto meno pesante, dalla tabella (ogni cella della tabella rappresenta una elemento di $A \times A$, quelle marcate da un pallino rappresentano gli elementi del grafico):

	0	1	2	3	4	5	6	7	8	9
0	●		●		●					
1		●								
2	●		●		●					
3				●						●
4	●		●		●					
5						●	●	●	●	
6						●	●	●	●	
7						●	●	●	●	
8						●	●	●	●	
9				●						●

(2) le due relazioni di equivalenza banali in un insieme $A \neq \varnothing$, cioè la relazione di uguaglianza e la relazione universale, corrispondono alle due partizioni banali di A, infatti il quoziente di A rispetto alla relazione di uguaglianza è $\mathcal{P}_1(A) = \{\{x\} \mid x \in A\}$ (ogni classe di equivalenza è un singleton), quello rispetto alla relazione universale è $\{A\}$ (poiché tutti gli elementi di A sono in relazione tra loro, A costituisce una classe di equivalenza). Cosa cambia se A è l'insieme vuoto?

(3) Dal teorema fondamentale (il teorema 8), segue che, per ogni insieme A, ci sono tante relazioni di equivalenza in A quante sono le partizioni di A. Ad esempio, se $|A| = 2$, poiché, come abbiamo visto sopra, A ha esattamente due partizioni (quelle banali), A ha anche esattamente due relazioni di equivalenza (quelle banali). Quante sono le relazioni di equivalenza in A se $|A| < 2$?

(4) Descriviamo le relazioni di equivalenza in un insieme di tre elementi: $A = \{1,2,3\}$. Per farlo ci basta elencare le partizioni di A e quindi applicare il teorema 8. Le partizioni già le conosciamo: come abbiamo visto in un esempio precedente sono in tutto cinque, le due partizioni banalie e poi le tre partizioni $F_1 = \big\{\{1\},\{2,3\}\big\}$, $F_2 = \big\{\{2\},\{1,3\}\big\}$ ed $F_3 = \big\{\{3\},\{1,2\}\big\}$. Allora le relazioni di equivalenza in A saranno anch'esse cinque: le due banali (quella di uguaglianza e quella universale) e le tre relazioni di equivalenza σ_1, σ_2 e σ_3 che corrispondono, nell'ordine, a F_1, F_2 ed F_3. Le rappresentiamo in tabella:

σ_1	1	2	3
1	●		
2		●	●
3		●	●

σ_2	1	2	3
1	●		●
2		●	
3	●		●

σ_3	1	2	3
1	●	●	
2	●	●	
3			●

(5) Abbiamo usato il teorema 8 per elencare le relazioni di equivalenze in un insieme, vediamo ora un esempio di in cui lo stesso teorema viene usato per elencare tutte le relazioni di equivalenza (sempre in un assegnato insieme) con assegnate proprietà, traducendo questo problema in un problema espresso in termini di partizioni. Sia $A = \{n \in \mathbb{N} \mid n < 9\}$. Proviamo a descrivere l'insieme E di tutte le relazioni di equivalenza $\sim$ in A tali che $0 \sim 1 \nsim 2$, $3 \in [1]_\sim \subseteq [5]_\sim$, $4 \in [2]_\sim \cap [6]_\sim$ e $7 \sim 8$. Usando la proposizione 7 (ed il piccolo esercizio che segue), possiamo verificare (farlo in dettaglio) che la condizione equivale al richiedere $7 \sim 8$, che gli elementi di $X := \{0,1,3,5\}$ siano equivalenti tra loro e quelli di $Y := \{2,4,6\}$ siano equivalenti tra loro ma non a quelli di X. In altri termini la condizione significa precisamente questo: che X sia contenuto in una classe di equivalenza in $A/\!\sim$ ed Y sia contenuto in una classe di equivalenza in $A/\!\sim$ diversa da quella contenente X, ed infine che $7 \sim 8$. Usiamo il teorema 8 per tradurre il nostro problema in termini di partizioni di A: dobbiamo cercare le partizioni di A costituite da almeno due blocchi distinti, uno contenente X ed uno contenente Y, ed in cui 7 ed 8 appartengono allo stesso blocco; siccome $A = X \cup Y \cup \{7,8\}$ questo implica che i blocchi di una tale partizione sono al massimo tre. È facile riconoscere che le partizioni che soddisfano le condizioni sono tre: una con tre blocchi distinti: $F_1 := \{X, Y, \{7,8\}\}$, e due con soli due blocchi: $F_2 := \{X \cup \{7,8\}, Y\}$ e $F_3 := \{X, Y \cup \{7,8\}\}$. Quindi, per il teorema 8, l'insieme E che volevamo descrivere ha esattamente tre elementi, le tre relazioni corrispondenti a F_1, F_2 e F_3, descritte come segue. Come già avevamo osservato, rispetto a tutte e tre gli elementi di X sono equivalenti tra loro, e quelli di Y pure, ma quelli di X non sono equivalenti a quelli di Y, inoltre 7 ed 8 sono equivalenti tra loro. Rispetto alla prima relazione di equivalenza (quella corrispondente a F_1) 7 ed 8 non sono equivalenti a nessun elemento di X o di Y, rispetto alla seconda (quella corrispondente a F_2) 7 ed 8 sono equivalenti agli elementi di X, rispetto alla terza (quella corrispondente a F_3) 7 ed 8 sono equivalenti agli elementi di Y.

4. Ancora sui nuclei di equivalenza

Sia $\sim$ una relazione di equivalenza in un insieme A. Si chiama *proiezione canonica* (di A su $A/\!\sim$, oppure definita da $\sim$) l'applicazione

$$\pi_\sim \colon x \in A \longmapsto [x]_\sim \in A/\!\sim.$$

È evidente dalla definizione di insieme quoziente che $\pi_\sim$ è suriettiva, ma in realtà questo è già noto dal lemma 2, dal momento che $\pi_\sim$ non è altro che la proiezione di A su $A/\!\sim$ visto come partizione di A. Da questo e dalla dimostrazione del teorema 8 si potrebbe fare seguire la proposizione seguente, di cui però forniamo una dimostrazione diretta.

Proposizione 9. *Sia $\sim$ una relazione di equivalenza. Allora $\sim$ è il nucleo di equivalenza della proiezione canonica che definisce.*

Dimostrazione. Continuiamo ad usare la notazioni appena introdotte; sia $\sim \in \mathrm{Eq}(A)$ e sia $\pi_\sim \colon A \to A/\!\sim$ la proiezione canonica. Sia ρ il nucleo di equivalenza di $\pi_\sim$. Allora, per ogni x, $y \in A$, abbiamo:

$$x \,\rho\, y \iff \pi_\sim(x) = \pi_\sim(y) \iff [x]_\sim = [y]_\sim \iff x \sim y,$$

per il lemma 5. Dunque, $\rho = \sim$ e l'enunciato è provato. □

È davvero importante questa conseguenza, che avevamo già annunciato:

Corollario 10. *Ogni relazione di equivalenza è il nucleo di equivalenza di qualche applicazione.*

In maggior dettaglio, se A è un insieme e $\sim$ è una relazione di equivalenza in A, esiste almeno un'applicazione f *di dominio* A tale che $\sim$ sia il nucleo di equivalenza di f. Non dimostriamo qui (ma non è difficile farlo) che è possibile scegliere f in modo che A sia anche il codominio di f.

Notiamo che applicazioni diverse possono avere lo stesso nucleo di equivalenza. Ad esempio, segue dall'esercizio 4 che le relazioni di equivalenza banali in un, qualsiasi, fissato insieme non vuoto sono nuclei di equivalenza di infinite applicazioni. Per fare un esempio diverso, le applicazioni $n \in \mathbb{Z} \mapsto |n| \in \mathbb{N}$, $n \in \mathbb{Z} \mapsto |n| \in \mathbb{Z}$, $n \in \mathbb{Z} \mapsto n^2 \in \mathbb{Z}$ e tante altre hanno lo stesso nucleo di equivalenza: la relazione binaria in $\mathbb{Z}$ che dichiara equivalenti due numeri interi se e solo se essi hanno lo stesso valore assoluto.

Abbiamo così che le relazioni di equivalenza si possono riguardare da almeno tre punti di vista: come particolari relazioni binarie, secondo la definizione, come concetto associato a quello di partizione (attraverso il teorema 8) e come nozione collegata a quella di applicazione: le relazioni di equivalenza sono i nuclei di equivalenza delle applicazioni. Mentre però il teorema 8 mostra che la corrispondenza tra relazioni di equivalenza e partizioni in un dato insieme è descritta da un'applicazione biettiva, e per questo studiare le partizioni dell'insieme equivale a studiarne le relazioni di equivalenza, lo stesso non vale nel caso delle applicazioni e dei corrispondenti nuclei di equivalenza.

Studiamo ora in maggior dettaglio i nuclei di equivalenza ed i corrispondenti quozienti.

Lemma 11. *Siano $f \colon A \to B$ un'applicazione e τ il suo nucleo di equivalenza. Allora, per ogni $x \in A$, si ha $[x]_\tau = \overleftarrow{f}\big(\{f(x)\}\big)$*

Dimostrazione. Sia $x \in A$. Allora $[x]_\tau = \{y \in A \mid y \,\tau\, x\} = \{y \in A \mid f(y) = f(x)\}$. Ora, per ogni $y \in A$, la condizione $f(y) = f(x)$ è equivalente a $f(y) \in \{f(x)\}$, cioè alla condizione che y appartenga all'antiimmagine $\overleftarrow{f}\big(\{f(x)\}\big)$ di $\{f(x)\}$ mediante f. Pertanto $[x]_\tau = \big\{y \in A \mid y \in \overleftarrow{f}\big(\{f(x)\}\big)\big\} = \overleftarrow{f}\big(\{f(x)\}\big)$. □

Teorema 12 (teorema di omomorfismo per insiemi)**.** *Siano $f \colon A \to B$ un'applicazione e τ il suo nucleo di equivalenza. Allora, l'applicazione*

$$y \in \operatorname{im} f \longmapsto \overleftarrow{f}\big(\{y\}\big) \in A/\tau$$

è biettiva ed ha per inversa l'applicazione

$$\tilde{f} \colon [x]_\tau \in A/\tau \longmapsto f(x) \in \operatorname{im} f.$$

Di conseguenza, $|A/\tau| = |\operatorname{im} f|$.

Dimostrazione. Ricordiamo che $\operatorname{im} f$ è, per definizione, l'insieme $\{f(x) \mid x \in A\}$, quindi per ogni $y \in \operatorname{im} f$ esiste $x \in A$ tale che $y = f(x)$ e così, per il lemma 11, $\overleftarrow{f}\big(\{y\}\big) = [x]_\tau \in A/\tau$. Questo mostra che l'applicazione $\alpha \colon y \in \operatorname{im} f \mapsto \overleftarrow{f}\big(\{y\}\big) \in A/\tau$ è ben definita. Verifichiamo che essa è suriettiva. Per ogni $c \in A/\tau$ esiste $x \in A$ tale che $c = [x]_\tau$, e $[x]_\tau = \overleftarrow{f}\big(\{f(x)\}\big)$ ancora per il lemma 11, inoltre $f(x) \in \operatorname{im} f$, dunque $c = \alpha(f(x))$. Pertanto α è suriettiva. Per verificare che α è iniettiva siano ora $u, v \in \operatorname{im} f$ tali che $\alpha(u) = \alpha(v)$. Dal momento che $u \in \operatorname{im} f$, esiste $x \in A$ tale che $u = f(x)$. Per tale x si ha così $x \in \overleftarrow{f}\big(\{u\}\big) = \alpha(u)$. Ma abbiamo assunto $\alpha(u) = \alpha(v)$, quindi si ha anche $x \in \alpha(v) = \overleftarrow{f}\big(\{v\}\big)$, cioè $f(x) = v$. Pertanto $u = f(x) = v$. Abbiamo così mostrato che α è iniettiva, quindi anche biettiva. Vogliamo infine descrivere α^{-1}. A questo scopo, sia c un qualsiasi elemento di A/τ. Naturalmente $c = [x]_\tau$ per un opportuno $x \in A$, e $\alpha(f(x)) = \overleftarrow{f}\big(\{f(x)\}\big) = [x]_\tau$ per il lemma 11, quindi $f(x) = \alpha^{-1}([x]_\tau) = \alpha^{-1}(c)$. In questo modo abbiamo verificato che l'inversa di α è, come richiesto dall'enunciato, l'applicazione $\tilde{f} \colon [x]_\tau \in A/\tau \mapsto f(x) \in \operatorname{im} f$, provando così anche che quest'applicazione è ben definita. □

La situazione descritta nel teorema precedente può essere descritta da questo diagramma

$$\begin{array}{ccc} A & \xrightarrow{\ f\ } & B \\ {\scriptstyle \pi_\tau}\downarrow & & \uparrow{\scriptstyle \iota} \\ A/\tau & \xrightarrow{\ \tilde f\ } & \operatorname{im} f \end{array}$$

in cui π_τ è la proiezione canonica definita dal nucleo di equivalenza τ dell'applicazione f, $\tilde f$ è definita come nell'enunciato del teorema e ι è l'immersione di $\operatorname{im} f$ in B, ed $\tilde f$ è biettiva per il teorema 12. Risulta $f = \iota \circ \tilde f \circ \pi_\tau$, infatti per ogni $x \in A$ si ha $(\iota \circ \tilde f \circ \pi_\tau)(x) = \iota(\tilde f(\pi_\tau(x))) = \iota(\tilde f([x]_\tau)) = \iota(f(x)) = f(x)$. Siccome π_τ è suriettiva, $\tilde f$ è biettiva e ι è iniettiva, vediamo così che *ogni applicazione è ottenibile come composta tra un'applicazione iniettiva ed una suriettiva*: $f = (\iota \circ \tilde f) \circ \pi_\tau$.[(5)]

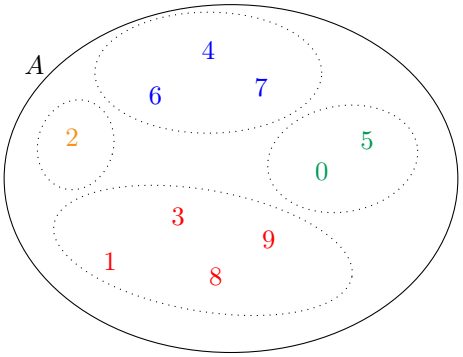
Vediamo qualche esempio:

(1) Siano $A = \{n \in \mathbb{Z} \mid -3 \leq n \leq 5\}$ e $f\colon n \in A \mapsto n^2 \in \mathbb{N}$. Sia poi τ il nucleo di equivalenza di f. Per descrivere il quoziente A/τ possiamo partire dalla descrizione di $\operatorname{im} f$. Dovrebbe essere chiaro che $\operatorname{im} f = \{n^2 \mid n \in A\} = \{0, 1, 4, 9, 16, 25\}$. Allora $\operatorname{im} f$ ha sei elementi, quindi, per il teorema 12 abbiamo $|A/\tau| = 6$; in altri termini in A ci sono esattamente sei classi di equivalenza rispetto a τ, che corrispondono ai sei elementi di $\operatorname{im} f$. Le classi, cioè gli elementi di A/τ sono dunque, sempre per lo stesso teorema: $\overleftarrow{f}(\{0\}) = \{0\}$, $\overleftarrow{f}(\{1\}) = \{1, -1\}$, $\overleftarrow{f}(\{4\}) = \{2, -2\}$, $\overleftarrow{f}(\{9\}) = \{3, -3\}$, $\overleftarrow{f}(\{16\}) = \{4\}$ e $\overleftarrow{f}(\{25\}) = \{5\}$.

(2) Utilizziamo lo stesso insieme A dell'esempio precedente, e studiamo il nucleo di equivalenza σ dell'applicazione $g\colon x \in \mathcal{P}(A) \mapsto x \cap \mathbb{N} \in \mathcal{P}(\mathbb{N})$. Iniziamo con l'identificare $\operatorname{im} f$. Posto $B = A \cap \mathbb{N}$, per ogni $x \in \mathcal{P}(B)$ si ha evidentemente $g(x) = x \cap \mathbb{N} \subseteq B$. Viceversa, per ogni $y \in \mathcal{P}(B)$ abbiamo $y = y \cap \mathbb{N} = g(y)$, quindi $y \in \operatorname{im} g$. Pertanto $\operatorname{im} g = \mathcal{P}(B)$ e quindi, come mostra il teorema 12, $|\mathcal{P}(A)/\sigma| = |\operatorname{im} g| = |\mathcal{P}(B)| = 2^{|B|} = 32$. Come sono fatte le singole classi di equivalenza rispetto a σ? Sempre per lo stesso teorema esse corrispondono agli elementi di $\operatorname{im} g = \mathcal{P}(B)$, sono cioè gli insiemi $\overleftarrow{g}(\{y\})$ al variare di $y \in \mathcal{P}(B)$. Ad esempio, l'elemento $\varnothing$ di $\mathcal{P}(B)$ corrisponde alla classe $\overleftarrow{g}(\{\varnothing\}) = \{x \in \mathcal{P}(A) \mid g(x) = \varnothing\} = \{x \in \mathcal{P}(A) \mid x \cap \mathbb{N} = \varnothing\}$. Non è difficile vedere che questo insieme è $\mathcal{P}(A \smallsetminus B) = \mathcal{P}(\{-3, -2, -1\})$, un insieme di otto elementi. Chi legge può provare a dimostrare che, per ogni $y \in \mathcal{P}(B)$ si ha $\overleftarrow{g}(\{y\}) = \{x \in \mathcal{P}(A) \mid g(x) = y\} = \{y \cup z \mid z \in \mathcal{P}(A \smallsetminus B)\}$ e questo insieme ha esattamente otto elementi. Come ulteriore esempio, dal momento che $g(\{1, -1\}) = \{1\}$, il lemma 11 mostra che $[\{1, -1\}]_\sigma = \overleftarrow{g}(g(\{1, -1\})) = \overleftarrow{g}(\{1\}) = \{\{1\} \cup z \mid z \in \mathcal{P}(A \smallsetminus B)\}$.

Per un esempio conclusivo, che illustri i diversi punti di vista presentati in queste note, facciamo ancora una volta riferimento allo stesso insieme A, attribuendo un colore ad i suoi elementi, come indicato qui: $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Con riferimento ad A ed a questi colori possiamo . . . :

- . . . definire una relazione di equivalenza $\rho \in \operatorname{Eq}(A)$ dichiarando, per ogni $x, y \in A$, $x \,\rho\, y$ se e solo se x e y hanno lo stesso colore;
- . . . definire un'applicazione $c\colon A \to C$, dove C è un insieme di colori contenente (almeno) i quattro colori utilizzati, ad esempio $C = \{$*verde, rosso, giallo, arancione, blu, grigio*$\}$. Come la nostra rappresentazione suggerisce, c manda 0 e 5 in *verde*, 1, 3, 8 e 9 in *rosso*, 4, 6 e 7 in *blu* e 2 in *arancione*.
- . . . "raggruppare" gli elementi di A per colore, come nel diagramma che segue. Questo significa definire una partizione $\mathcal{F}$ di A costituita da quattro blocchi, uno per ciascuno dei colori utilizzati, ciascuno dei quali è l'insieme degli elementi di A del colore dato, quindi $\mathcal{F} = \big\{\{0, 5\}, \{1, 3, 8, 9\}, \{4, 6, 7\}, \{2\}\big\}$:



Vediamo (e se non lo vediamo immediatamente riflettiamoci sopra sino a convincercene) che ρ non è altro che il nucleo di equivalenza di c, e che $\mathcal{F}$ è precisamente A/ρ. Come sappiamo dal teorema 8, $\mathcal{F}$ è determinata univocamente da ρ e ρ è determinata univocamente da $\mathcal{F}$, quindi assegnare ρ equivale ad assegnare $\mathcal{F}$. In accordo con il teorema 12, $\mathcal{F} = A/\rho$ ha esattamente $4 = |\operatorname{im} c|$ elementi (le quattro classi rispetto a ρ, ovvero i quattro colori utilizzati). Notiamo infine che, mentre $\mathcal{F}$ e ρ sono determinate da c, c non è univocamente determinata da $\mathcal{F}$ e ρ. Infatti, se proviamo a cambiare l'insieme C (il codominio di c) aggiungendo ad esempio un nuovo colore (come *viola*), oppure cancellando da esso uno dei colori non usati (come *grigio*), l'applicazione c cambia, ma il suo nucleo

(5) o, se si preferisce, $f = \iota \circ (\tilde f \circ \pi_\tau)$.

di equivalenza resta ρ. Ancora più radicalmente, possiamo scambiare tra loro i colori, o sostituirne alcuni con altri in modo che l'applicazione c cambi senza che cambi il suo nucleo di equivalenza. Ad esempio, se ripetiamo l'intera discussione a partire da una colorazione di A come questa: $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, otteniamo un insieme C ed un'applicazione c sicuramente diversi da quelli presentati sopra ma, come si invita chi legge a verificare, la relazione d'equivalenza e la partizione risultanti (quelle che sopra erano ρ ed $\mathcal{F}$) non cambieranno.

Algoritmo euclideo, massimo comun divisore ed equazioni diofantee

Se a e b sono numeri interi, si dice che a divide b, in simboli: $a \mid b$, se e solo se esiste $c \in \mathbb{Z}$ tale che $b = ac$. Si può subito notare che:

- 1 e -1 sono gli unici interi che dividano ogni intero;
- 0 è l'unico intero che sia diviso da ogni intero.
- $\forall\, a, b \in \mathbb{Z}\ \big(a \mid b \iff -a \mid b \iff a \mid -b \iff -a \mid -b\big)$

L'insieme dei divisori (in $\mathbb{Z}$) di un intero n si indica come $\mathrm{D}(n)$. Dunque, per ogni $n \in \mathbb{Z}$,

$$\mathrm{D}(n) := \{a \in \mathbb{Z} : a \mid n\},$$

ad esempio, $\mathrm{D}(6) = \{1, -1, 2, -2, 3, -3, 6, -6\}$.

Un *massimo comun divisore* tra a e b è poi un intero d per il quale valgano le due condizioni:

$$\begin{aligned} &\text{i.)} \quad d \mid a \ \wedge\ d \mid b; \qquad \text{e} \\ &\text{ii.)} \quad \forall\, c \in \mathbb{Z}\big((c \mid a \ \wedge\ c \mid b) \Rightarrow c \mid d\big); \end{aligned}$$

ovvero, in modo equivalente:

$$\begin{aligned} &\text{i.)} \quad d \in \mathrm{D}(a) \cap \mathrm{D}(b); \qquad \text{e} \\ &\text{ii.)} \quad \forall\, c \in \mathrm{D}(a) \cap \mathrm{D}(b),\ \ c \mid d. \end{aligned}$$

Dunque, un massimo comun divisore tra a e b è un divisore comune ad a e b che sia diviso da ogni altro divisore comune ad a e b.

Alcune osservazioni immediate sulla nozione di massimo comun divisore sono le seguenti:

- Se d è un massimo comun divisore tra a e b allora d e $-d$ sono gli unici massimi comun divisori tra a e b,

dunque: calcolare un massimo comun divisore tra due interi equivale a calcolarli tutti;

- per ogni $a, b \in \mathbb{Z}$, i divisori comuni ad a e b sono tutti e soli i divisori comuni ad $|a|$ e $|b|$; quindi i massimi comun divisori tra a e b sono tutti e soli i massimi comun divisori tra $|a|$ e $|b|$.

Quest'ultima osservazione mostra che nel calcolare massimi comun divisori tra numeri interi è sempre possibile ridursi a calcolare massimi comun divisori tra interi non negativi. Ad esempio, i massimi comun divisori tra -7811 e 8456985 sono precisamente i massimi comun divisori tra 7811 e 8456985, così come quelli tra -7811 e -8456985 o quelli tra 7811 e -8456985. Inoltre, il calcolo dei massimi comun divisori tra 0 ed un arbitrario intero è immediato, come segue da queste altre due osservazioni:

- se a e b sono interi e $a \mid b$, allora a è un massimo comun divisore tra a e b;
- in particolare, per ogni $a \in \mathbb{Z}$, si ha che a è un massimo comun divisore tra a e 0.

Pertanto:

> *Il problema di calcolare un massimo comun divisore tra numeri interi si riduce sempre al problema di calcolare un massimo comun divisore tra numeri interi positivi.*

Sino a questo momento non si è ancora stabilito se questo problema abbia sempre soluzione, cioè se, assegnati comunque due interi a e b esista un massimo comun divisore tra a e b.

Il teorema fondamentale dell'aritmetica suggerisce un metodo per calcolare un massimo comun divisore tra a e b, quello che viene insegnato sin dalla scuola elementare: supponendo, come lecito, a e b positivi, basta esprimere sia a che b come prodotti di potenze di numeri primi (positivi) a due a due distinti, con esponenti positivi:

$$\begin{aligned} a &= p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_s^{\lambda_s} \\ b &= q_1^{\mu_1} q_2^{\mu_2} \cdots q_t^{\mu_t}; \end{aligned}$$

si ottiene un massimo comun divisore tra a e b come prodotto di tutti i primi che appaiono in entrambe le fattorizzazioni (i *fattori comuni* ...), ciascuno elevato al minimo degli esponenti con cui

---

Avvertenza: Queste note integrano, ma non sostituiscono, le corrispondenti parti del libro di testo.

appare (*... col minimo esponente*). Ciò è facile da verificare (lo si faccia per esercizio) e mostra che la risposta alla domanda formulata sopra è positiva. Grazie anche alle osservazioni precedenti possiamo concludere che:

> *Se a e b sono interi allora:*
> — *se $a = b = 0$, l'unico massimo comun divisore tra a e b è 0;*
> — *altrimenti, se almeno uno tra a e b è diverso da zero, a e b hanno esattamente due massimi comun divisori, uno opposto dell'altro.*
> *In ogni caso, dunque, esiste uno ed un solo massimo comun divisore non negativo tra a e b.*

Il massimo comun divisore non negativo tra due interi a e b viene spesso indicato con il simbolo $\mathrm{MCD}(a, b)$.

Il metodo di calcolo di un massimo comun divisore tra due interi a e b appena ricordato è molto rapido ed efficace nel caso in cui a e b siano numeri di valore assoluto sufficientemente piccolo da renderne semplice la scomposizione in fattori primi. Quando si ha a che fare con numeri più grandi questo metodo risulta invece spesso impraticabile, dal momento che non sono noti metodi che permettano di scomporre in tempi ragionevolmente brevi numeri interi arbitrari; anzi, il calcolo dei fattori primi di un intero può rivelarsi di estrema complessità computazionale.

Per questo è molto importante disporre di un metodo alternativo, quello fornito dall'algoritmo euclideo, che ora illustreremo e che si dimostra essere invece molto efficiente. Per semplificare la discussione, introduciamo una definizione. Per ogni $a, b \in \mathbb{Z}$ chiamiamo *combinazione lineare di a e b a coefficienti in $\mathbb{Z}$* ogni numero intero che si possa scrivere come $\alpha a + \beta b$ per opportuni $\alpha, \beta \in \mathbb{Z}$. In altri termini, una combinazione lineare di a e b (a coefficienti in $\mathbb{Z}$; talvolta lasceremo sottintesa questa specificazione) è la somma di un multiplo di a per un multiplo di b. Ad esempio, sono combinazioni lineare di a e b i numeri $3a + 7b$, $15a - 2b$, $-19b$.

Lemma 1. *Siano $a, b, c \in \mathbb{Z}$. Se c divide a e b allora c divide ogni combinazione lineare di a e b a coefficienti in $\mathbb{Z}$.*

Dimostrazione — Se $c \mid a$ e $c \mid b$, esistono interi h e k tali che $a = hc$ e $b = kc$. Scelti comunque $\alpha, \beta \in \mathbb{Z}$ si ha allora $\alpha a + \beta b = \alpha(hc) + \beta(kc) = (\alpha h + \beta k)c$, dunque c divide $\alpha a + \beta b$. □

Un caso particolare del precedente lemma è il punto centrale del ragionamento che suggerisce e giustifica l'algoritmo euclideo:

Lemma 2. *Siano $a, b, q, r \in \mathbb{Z}$ tali che $a = bq + r$. Allora i divisori comuni ad a e b sono tutti e soli i divisori comuni a b e r. In particolare, i massimi comun divisori tra a e b sono precisamente i massimi comun divisori tra b e r.*

Dimostrazione — Sia c un divisore comune a b e r. Poiché a è combinazione lineare di b e r, allora $c \mid a$ per il Lemma 1. Dunque c è un divisore comune ad a e b. Abbiamo così provato l'inclusione

$$\mathrm{D}(a) \cap \mathrm{D}(b) \supseteq \mathrm{D}(b) \cap \mathrm{D}(r).$$

Per provare l'inclusione opposta, osserviamo che $r = a - bq$ è combinazione lineare di a e b, quindi, come per il passaggio precedente, ogni divisore comune ad a e b divide r ed è così un divisore comune a b e r. Abbiamo ora dimostrato l'uguaglianza $\mathrm{D}(a) \cap \mathrm{D}(b) = \mathrm{D}(b) \cap \mathrm{D}(r)$, cioè che a e b da una parte e b ed r dall'altra hanno gli stessi divisori comuni, quindi anche gli stessi massimi comun divisori. □

Supponiamo ora di voler calcolare un massimo comun divisore tra due interi a e b; come visto sopra possiamo supporre che essi siano entrambi positivi. Possiamo ovviamente anche supporre $a \geq b$, infatti se $a < b$ basta scambiare tra loro a e b, dal momento che $\mathrm{MCD}(a, b) = \mathrm{MCD}(b, a)$.

Come sappiamo, si può effettuare la divisione aritmetica (con resto) di a per b. Esistono dunque (e sono univocamente determinati) due numeri naturali q (il quoziente) e r (il resto) tali che

$$a = bq + r \qquad \text{e} \qquad r < b.$$

Il Lemma 2 mostra che vale l'uguaglianza $\mathrm{MCD}(a, b) = \mathrm{MCD}(b, r)$. Possiamo dunque tradurre il nostro problema originale (calcolare un massimo comun divisore tra a e b) con il problema, simile,

di calcolare un massimo comun divisore tra b e r. Il vantaggio di questa riformulazione consiste in questo, che se consideriamo la "grandezza" dei due numeri a e b come misura (grossolana!) della difficoltà del nostro problema (nel senso che è, probabilmente, più facile calcolare un massimo comun divisore tra due numeri più piccoli piuttosto che tra due numeri più grandi), allora l'aver sostituito la coppia (b, r) alla coppia (a, b) ha semplificato il problema, perché $b < a$ e $r < b$.

È possibile che si abbia $r = 0$. In questo caso, $b \mid a$ e quindi b è un massimo comun divisore tra a e b. Se invece $r > 0$, possiamo ripetere per b e r il procedimento effettuato per a e b: dividendo b per r otteniamo,

$$b = rq_1 + r_1 \qquad \text{e} \qquad r_1 < r,$$

dove, ancora, $q_1, r_1 \in \mathbb{N}$ e i massimi comun divisori tra r e r_1 sono i massimi comun divisori tra b e r, quindi tra a e b. Se $r_1 = 0$ (cioè se $r \mid b$), allora r è un massimo comun divisore tra a e b, in caso contrario possiamo effettuare un'altra divisione, quella tra r e r_1, ottenendo $q_2, r_2 \in \mathbb{N}$ tali che:

$$r = r_1q_2 + r_2 \qquad \text{e} \qquad r_2 < r_1,$$

se $r_2 = 0$ allora r_1 è il massimo comun divisore cercato, altrimenti si proseguirà dividendo r_1 per r_2.

Dovrebbe essere a questo punto chiaro il procedimento: ad ogni passo si verifica se il resto r_t dell'ultima divisione effettuata: $r_{t-2} = r_{t-1}q_t + r_t$, è 0; in questo caso il penultimo resto r_{t-1} (vale a dire, l'ultimo resto diverso da 0, o, ancora, l'ultimo divisore) è il massimo comun divisore positivo tra a e b, se invece $r_t \neq 0$ si effettua un'altra divisione, tra il divisore r_{t-1} ed il resto r_t della divisione precedente.

È ancora da chiarire un solo punto, cioè se questo procedimento termina, ovvero se, iterando questo procedimento, si perviene ad una divisione con resto 0. La risposta è affermativa. Infatti, la sequenza dei resti ottenuti nelle successive divisioni è strettamente decrescente:

$$b > r > r_1 > r_2 > r_3 > \cdots \geq 0$$

e una sequenza strettamente decrescente di numeri naturali minori di b può avere al più b termini, dal momento che l'insieme $\{n \in \mathbb{N} \mid b \geq n\}$ ha b elementi. Dunque $r_t = 0$ per qualche $t < b$. Pertanto l'algoritmo termina, fornendo un massimo comun divisore tra a e b, dopo al più b divisioni (ad essere pedanti, si dovrebbe specificare che, affinché tutto ciò che è stato appena scritto abbia senso in ogni caso, si devono sottintendere le posizioni $r_0 := r$ e $r_{-1} := b$).

Notiamo che l'algoritmo euclideo appena descritto fornisce un'altra dimostrazione, costruttiva, dell'esistenza di un massimo comun divisore tra due arbitrari interi.

Possiamo riassumere la discussione precedente e schematizzare l'algoritmo euclideo per la ricerca di un massimo comun divisore come segue:

Assegnati due numeri interi a e b, si intende calcolare un massimo comun divisore d tra a e b.

① se uno tra a e b è 0, si pone d uguale all'altro e l'algoritmo termina. Altrimenti:

② si sostituiscono a e b con $|a|$ e $|b|$, nell'ordine;

③ se $a < b$ si scambiano tra loro a e b;

④ a partire dalla divisione di a per b si effettuano divisioni aritmetiche successive, come sopra specificato, finché non si ottenga 0 come resto:

$$\begin{aligned}
a &= bq + r \\
b &= rq_1 + r_1 \\
r &= r_1q_2 + r_2 \\
r_1 &= r_2q_3 + r_3 \\
&\vdots \\
r_{t-3} &= r_{t-2}q_{t-1} + r_{t-1} \\
r_{t-2} &= r_{t-1}q_t + r_t \\
r_{t-1} &= r_tq_{t+1} + 0
\end{aligned}$$

dove $b > r > r_1 > r_2 > \cdots > r_t > 0$. A questo punto, si pone $d = r_t$ e l'algoritmo termina.

Anche se non essenziali per la comprensione dell'algoritmo, si possono fare alcune osservazioni marginali. Innanzitutto, il passo ② non è necessario in senso stretto, dal momento che è possibile effettuare divisioni aritmetiche anche tra interi negativi, o tra un positivo e un negativo. Tuttavia, è consigliabile eseguirlo per evitare inutili complicazioni di calcolo. Anche il passo ③ si sarebbe potuto omettere dalla descrizione dell'algoritmo, per un motivo di tipo diverso. Infatti, se a e b sono positivi e $a < b$, allora la divisione aritmetica di a per b fornisce quoziente 0 e resto a. Dunque se eseguiamo il passo ④ dell'algoritmo senza aver prima scambiato tra loro a e b, la prima divisione (di a per b) fornisce $r = a$ e quindi la seconda, quella tra b e $r = a$, è precisamente quella da cui saremmo partiti se avessimo eseguito il passo ③. Ciò mostra che l'unico scopo del passo ③ è quello di evitare una divisione inutile (ancorché banale).

Osservazione più rilevante, a proposito del passo ④, è che, come abbiamo già detto, l'algoritmo terminerà dopo al più $|b|$ divisioni.

Come esempio di applicazione dell'algoritmo euclideo, supponiamo di voler calcolare il massimo comun divisore positivo d tra 2547 e -7431. Passando ai valori assoluti dei due numeri considerati, e tenendo conto che $2547 < 7431$, procediamo come al passo ④ dopo aver posto $a = 7431$ e $b = 2547$. Eseguiamo dunque le divisioni:

$$
\begin{aligned}
7431 &= 2547[2] + 2337 \\
2547 &= 2337[1] + 210 \\
2337 &= 210[11] + 27 \\
210 &= 27[7] + 21 \\
27 &= 21[1] + 6 \\
21 &= 6[3] + 3 \\
6 &= 3[2]
\end{aligned}
$$

Come evidenziato dalle frecce in colore, ogni divisione successiva alla prima ha per dividendo e per divisore il divisore ed il resto della divisione precedente. Come si può capire, è importante, eseguendo l'algoritmo, non confondere i ruoli tra i successivi divisori (indicati sopra come $b, r, r_1, \ldots$) ed i successivi quozienti (indicati come $q, q_1, q_2, \ldots$). I primi vanno riutilizzati nella divisione seguente, i secondi no. Allo scopo di evitare questa possibile confusione può essere utile adottare qualche artificio grafico. In questo caso, i quozienti sono stati scritti tra parentesi quadre.

Tornando al nostro specifico esempio, poiché l'ultimo resto non nullo è 3, concludiamo che 3 è un massimo comun divisore tra 2562 e -7491.

Un'ulteriore osservazione su questo algoritmo è che esso può essere reso ancora più efficace da una piccola modifica. Infatti, l'algoritmo si basa su una ripetuta applicazione del Lemma 2, e nell'enunciato del Lemma 2 non è richiesto che gli interi q ed r siano proprio il quoziente ed il resto della divisione aritmetica di a per b. Ora, è possibile effettuare un altro tipo di divisione tra interi che rispetti la condizione "$a = bq + r$" dell'ipotesi del Lemma 2:

Lemma 3 (Divisione euclidea). *Siano $a, b \in \mathbb{Z}$. Se $b \neq 0$ esistono $q, r \in \mathbb{Z}$ tali che $a = bq + r$ e $|r| \leq |b|/2$.*

Dimostrazione — Assegnati a e b come richiesto dall'enunciato, effettuiamo la divisione aritmetica tra a e b. Otteniamo così $\bar{q}, \bar{r} \in \mathbb{Z}$ tali che $a = b\bar{q} + \bar{r}$ e $0 \leq \bar{r} < |b|$. Se $\bar{r} \leq |b|/2$, allora abbiamo concluso la ricerca di q e r: basterà porre $r = \bar{r}$ e $q = \bar{q}$, a questo punto avremo $a = bq + r$ e $|r| = r \leq |b|/2$, come richieso dall'enunciato.

Se invece $\bar{r} > |b|/2$, allora si ha $|b| - \bar{r} < |b| - \big(|b|/2\big) = |b|/2$. In questo caso, poniamo $r := \bar{r} - |b|$. Poiché $\bar{r} < |b|$ si ha allora $r < 0$, e quindi $|r| = -r = |b| - \bar{r} < |b|/2$. Dunque la condizione $|r| \leq |b|/2$ è soddisfatta. Inoltre $\bar{r} = |b| + r$, dunque

$$a = b\bar{q} + \bar{r} = b\bar{q} + \big(|b| + r\big) = bq + r,$$

avendo posto $q = \bar{q} + 1$ se $b > 0$ (e quindi se $|b| = b$) e $q = \bar{q} - 1$ se $b < 0$. Con questa scelta di q e r le condizioni richieste dall'enunciato sono soddisfatte, e così il lemma è dimostrato. □

Ad esempio la divisione aritmetica di 14 per 5 dà quoziente 2 e resto 4; la divisione euclidea appena introdotta dà quoziente 3 (aumentato di 1 rispetto al precedente, perché il divisore 5 è positivo) e resto -1: infatti $14 = 5[3] + (-1)$.

Possiamo eseguire l'algoritmo euclideo per la ricerca di un massimo comun divisore effettuando quest'ultimo tipo di divisioni anziché quelle aritmetiche. Uno svantaggio (se così si può dire, anche questo sarebbe evitabile) è che eseguiremo divisioni anche tra numeri negativi, un significativo vantaggio è che la successione dei resti r, r_1, $r_2, \dots$ verificherà le condizioni:

$$|r| \leq |b|/2; \quad |r_1| \leq |r|/2 \leq |b|/4; \quad |r_1| \leq |r_2|/2 \leq |b|/8; \dots,$$

che, per dirla in termini informali, garantiscono che la successione dei resti decrescerà, nella maggior parte dei casi, più rapidamente di quanto non accadeva con la versione originaria dell'algoritmo. Ciò significa che possiamo aspettarci di dover effettuare meno divisioni, e quindi di terminare più rapidamente l'algoritmo.

A titolo di esempio, si possono confrontare il procedimento seguito prima per il calcolo del massimo comun divisore tra 7431 e 2547 con una versione dello stesso calcolo eseguito effettuando divisioni euclidee anziché aritmetiche:

$$\begin{aligned}
7431 &= 2547[2] + 2337 \\
2547 &= 2337[1] + 210 \\
2337 &= 210[11] + 27 \\
210 &= 27[7] + 21 \\
27 &= 21[1] + 6 \\
21 &= 6[3] + 3 \\
6 &= 3[2]
\end{aligned}
\qquad\qquad
\begin{aligned}
7431 &= 2547[3] + (-210) \\
2547 &= (-210)[-12] + 27 \\
-210 &= 27[-8] + 6 \\
27 &= 6[4] + 3 \\
6 &= 3[2]
\end{aligned}$$

Esercizio. Si sarebbero potute eseguire le divisioni nella colonna di sinstra, senza alterare il risultato finale, tralasciando i segni 'meno' dei divisori, e quindi assicurando che tutte le divisioni fossero tra numeri positivi. Ad esempio, dopo la prima divisione: $7431 = 2547[3] + (-210)$, la seconda avrebbe potuto essere $2547 = 210[12] + 27$. Basandosi sul Lemma 2 e su osservazioni precedenti, spiegare perché questa procedura è sempre lecita.

Equazioni diofantee

Oltre al calcolo dei massimi comun divisori, l'algoritmo euclideo permette di risolvere un altro importante problema. Un'equazione diofantea è un'equazione in cui appaiano solo indeterminate e numeri interi che si intenda risolvere in $\mathbb{Z}$, cioè per la quale siano ammesse come soluzioni solo numeri interi.

Ci occupiamo qui di un particolare tipo di equazione diofantea: quella cosiddetta lineare a due indeterminate, cioè una equazione diofantea della forma

$$ax + by = c, \tag{‡}$$

dove a, b e c sono numeri interi. Risolvere l'equazione (‡) significa dunque trovare le coppie di *interi* (u, v), che rendano vera l'uguaglianza se sostituiti a x e y, cioè tali che $au + bv = c$. Osserviamo subito che è possibile che la (‡) non ammetta soluzioni. Ad esempio, per $a = b = 0$ e $c = 1$ otteniamo l'equazione $0x + 0y = 1$ che, ovviamente, non ammette soluzioni. Facendo uso della terminologia introdotta sopra, è chiaro che (‡) ammette soluzioni (intere) se e solo se c è combinazione lineare di a e b a coefficienti in $\mathbb{Z}$. Ciò permette di dimostrare la prima importante osservazione su questo genere di equazioni.

Lemma 4. *Siano $a, b, c \in \mathbb{Z}$, e sia d un massimo comun divisore tra a e b. Se d non divide c, allora l'equazione diofantea $ax + by = c$ non ammette soluzioni.*

Dimostrazione — Supponiamo che l'equazione abbia soluzioni. Allora esistono $u, v \in \mathbb{Z}$ tali che $au + bv = c$, dunque c è combinazione lineare di a e b a coefficienti in $\mathbb{Z}$. Dal Lemma 1 segue allora che d divide c. Dunque, se supponiamo che d non divida c dobbiamo trarre la conclusione che la nostra equazione non ha soluzioni. □

Ad esempio, l'equazione diofantea $2x + 6y = 3$ non ha soluzioni. Ovviamente ciò significa che l'equazione non ha soluzioni intere; essa ha ovviamente soluzioni razionali (cioè in $\mathbb{Q}$), ad esempio $(0, 1/2)$ o $(1, 1/6)$, ma nessuna di esse è data da due numeri interi.

Vedremo come l'algoritmo euclideo permette non solo di dimostrare che vale anche l'implicazione inversa di quella stabilita nel Lemma 4, cioè, nelle stesse notazioni, che se d divide c, allora l'equazione diofantea $ax + by = c$ ammette soluzioni, ma anche di trovare queste soluzioni.

A questo scopo, iniziamo a considerare un caso banale, quello in cui almeno uno tra i coefficienti a e b è 0. Se $a = 0$, allora l'equazione (‡) si riduce a $by = c$. Dire che questa ha una soluzione intera equivale a dire che b divide c. Inoltre, b è un massimo comun divisore tra $a(= 0)$ e b, quindi è vero, in questo caso, che l'equazione data ammette soluzioni se (e solo se, in accordo col Lemma 4) un massimo comun divisore tra a e b divide c. Naturalmente, sempre in questo caso, è semplicissimo determinare le soluzioni, qualora ne esistano: se $b \neq 0$ esse sono tutte (e sole) le coppie $(n, c/b)$ al variare di n in $\mathbb{Z}$, mentre ogni coppia di numeri interi è soluzione se $b = 0$.

In modo analogo si ragiona se $b = 0$.

Supponiamo allora che sia a che b siano diversi da zero. Eseguiamo le divisioni successive previste dall'algoritmo euclideo:

$$\begin{aligned}
a &= bq + r \\
b &= rq_1 + r_1 \\
r &= r_1q_2 + r_2 \\
r_1 &= r_2q_3 + r_3 \\
&\vdots \\
r_{t-3} &= r_{t-2}q_{t-1} + r_{t-1} \\
r_{t-2} &= r_{t-1}q_t + r_t \\
r_{t-1} &= r_tq_{t+1}
\end{aligned}$$

Allora r_t è uno dei due massimi comun divisori tra a e b; poniamo $d := r_t$. Per risolvere l'equazione diofantea (‡) proveremo prima a risolvere l'equazione diofantea

$$ax + by = d. \tag{†}$$

Come già osservato, risolvere quest'ultima equivale ad esprimere d come combinazione lineare di a e b a coefficienti in $\mathbb{Z}$. La divisione in cui $d = r_t$ appare come resto permette di esprimere d come combinazione lineare dei due resti precedenti, r_{t-1} e r_{t-2}, infatti da $r_{t-2} = r_{t-1}q_t + d$ traiamo $d = r_{t-2} + [-q_t]r_{t-1}$. La divisione precedente, $r_{t-3} = r_{t-2}q_t + r_{t-1}$, fornisce poi r_{t-1} come combinazione lineare di r_{t-3} e r_{t-2}, dando $r_{t-1} = r_{t-3}+[-q_{t-1}]r_{t-2}$. Se sostituiamo questa espressione per r_{t-1} nella espressione trovata prima per d otteniamo $d = r_{t-2} + [-q_t]r_{t-1} = r_{t-2} + [-q_t]\big(r_{t-3} + [-q_{t-1}]r_{t-2}\big) = [-q_t]r_{t-3} + [1 + q_tq_{t-1}]r_{t-2}$, ed esprimiamo così d come combinazione lineare di r_{t-2} e r_{t-3}, i due resti precedenti r_{t-1}. Questi passaggi dovrebbero essere sufficienti a comprendere l'intero procedimento. Per comodità di espressione poniamo $r_0 := r$, $r_{-1} := b$ e $r_{-2} := a$. Ad ogni passo d è espresso come combinazione lineare (a coefficienti in $\mathbb{Z}$) di due "resti" con pedici consecutivi, diciamo r_i e r_{i+1}; dalla divisione di r_{i-1} per r_i si ottiene $r_{i+1} = r_{i-1} + [-q_{i+1}]r_i$. Sostituendo nell'espressione di d r_{i+1} con, appunto, $r_{i-1} + [-q_{i+1}]r_i$ si può scrivere d come combinazione lineare di r_{i-1} e r_i, i due "resti" precedenti, nell'ordine, r_i e r_{i+1}. Questo passaggio può essere reiterato finché non si ottenga un'espressione di d come combinazione lineare di $a = r_{-2}$ e $b = r_{-1}$, cioè due interi α e β tali che $\alpha a + \beta b = d$. Allora α e β forniscono una soluzione dell'equazione (†). Da questa si trae facilmente una soluzione per l'equazione (‡). Infatti, avendo assunto per ipotesi che d divida c, si ha $c = dh$ per un opportuno $h \in \mathbb{Z}$. Allora, ponendo $u := h\alpha$ e $v := h\beta$, si ha

$$au + bv = ah\alpha + bh\beta = h(\alpha a + \beta b) = hd = c,$$

quindi u e v forniscono una soluzione di (‡).

Abbiamo in questo modo provato che l'equazione diofantea (‡) ammette soluzioni se $d \mid c$. Ricordandoci del Lemma 4 possiamo dunque concludere col seguente teorema:

Teorema 5 (Teorema di Bézout). *Siano $a, b \in \mathbb{Z}$, e sia $d = \mathrm{MCD}(a, b)$. Allora l'equazione diofantea $ax + by = c$ ammette soluzioni (in $\mathbb{Z}$) se e solo se d divide c.*

Il Teorema di Bézout è spesso citato, in modo equivalente, anche in questa forma:

Teorema 5*. *Siano $a, b \in \mathbb{Z}$, e sia $d = \mathrm{MCD}(a, b)$. Allora l'insieme $\{\alpha a + \beta b \mid \alpha, \beta \in \mathbb{Z}\}$ delle combinazioni lineari di a e b a coefficienti in $\mathbb{Z}$ coincide con l'insieme $d\mathbb{Z} = \{dk \mid k \in \mathbb{Z}\}$ dei multipli di d in $\mathbb{Z}$.*

Come già per la ricerca di un massimo comun divisore, grazie all'algoritmo euclideo, non solo abbiamo stabilito esattamente quando un'equazione diofantea del tipo a noi considerato ammette soluzioni, ma abbiamo anche individuato un metodo (piuttosto efficace) per determinarne una nel caso esista.

Ad esempio, supponiamo di voler trovare soluzioni dell'equazione diofantea

$$74x + 22y = 10.$$

In questo caso è evidente che $\mathrm{MCD}(74, 22) = 2$; poiché 2 divide 10 siamo certi che l'equazione ammette soluzioni. Benché già conosciamo il massimo comun divisore 2, per trovare una soluzione mediante l'algoritmo euclideo bisogna eseguire le divisioni successive:

$$\begin{aligned} 74 &= 22[3] + 8 \\ 22 &= 8[2] + 6 \\ 8 &= 6[1] + 2 \\ 6 &= 2[3] \end{aligned}$$

sino ad ottenere 2 come ultimo resto non nullo. Da queste uguaglianze ricaviamo:

$$\begin{aligned} 8 &= 74 + 22[-3] \\ 6 &= 22 + 8[-2] \\ 2 &= 8 + 6[-1] \ . \end{aligned}$$

A questo punto possiamo esprimere 2 come combinazione lineare di 74 e 22, mediante successive sostituzioni:

$$\begin{aligned} 2 &= 8 + 6[-1] \\ &= 8 + \big(22 + 8[-2]\big)[-1] && \text{(sostituendo 6)} \\ &= 8 + 22[-1] + 8[2] && \text{(eseguendo i calcoli \dots)} \\ &= 8[3] + 22[-1] && \text{(\dots e raccogliendo i coefficienti di 8 e 22)} \\ &= \big(74 + 22[-3]\big)[3] + 22[-1] && \text{(sostituendo 8)} \\ &= 74[3] + 22[-9] + 22[-1] && \text{(eseguendo i calcoli \dots)} \\ &= 74[3] + 22[-10] && \text{(\dots e raccogliendo i coefficienti di 22 e 74).} \end{aligned}$$

Abbiamo così ottenuto l'espressione di 2 cercata. Questa mostra che la coppia $(3, -10)$ è soluzione dell'equazione diofantea $74x + 22y = 2$. Moltiplicando per 5 (cioè per $10/2$) si ottiene $74[15] + 22[-50] = 10$, dunque la coppia $(15, -50)$ è soluzione della nostra equazione diofantea $74x + 22y = 10$.

Alcune annotazioni: come è chiaro, il procedimento effettuato si sarebbe potuto semplificare in almeno due modi:

- avremmo potuto effettuare divisioni euclidee anziché aritmetiche, risparmiando qualche passaggio. In questo caso specifico, dividendo 22 per 8 avremmo potuto scrivere $22 = 8[3] + (-2)$ piuttosto che $22 = 8[2] + 6$, risparmiando sia una divisione che una sostituzione nella seconda parte dell'algoritmo. Per quest'ultima avremmo infatti ottenuto: $-2 = 22 + 8[-3] = 22 + \big(74 + 22[-3]\big)[-3] = 22[10] + 74[-3]$ e quindi $10 = 22[-50] + 74[15]$, moltiplicando per $-5 = 10/(-2)$.
- avendo osservato che 2 divide 74, 22 e10, avremmo potuto semplificare l'equazione dividendo tutti i coefficienti per 2 e ottenendo $37x + 11y = 5$, un'equazione equivalente alla precedente. Avremmo poi proceduto con calcoli analoghi a quelli effettuati sopra, ma facilitati perché applicati a numeri già divisi per due.

Una cosa molto importante da chiarire è che la soluzione trovata non è l'unica. Infatti, come è immediato verificare, per ogni intero k si ha $74(15 + 22k) + 22(-50 - 74k) = 10$, il che fornisce infinite soluzioni alla nostra equazione. In effetti, in generale, *ogni equazione diofantea del tipo che stiamo considerando (cioè lineare a due indeterminate) ha infinite soluzioni se ne ha almeno una.* Detto in altri termini: ha nessuna o infinite soluzioni. Ciò si può far seguire dalla teoria delle equazioni congruenziali lineari ad una indeterminata, che viene trattata in altre note. Ci limitiamo qui a stabilire il nesso tra equazioni diofantee e equazioni congruenziali:

Lemma 6. *Siano $a, b, c, u \in \mathbb{Z}$. Allora u è soluzione dell'equazione congruenziale $ax \equiv c \pmod{b}$ se e solo se esiste $v \in \mathbb{Z}$ tale che (u, v) sia soluzione dell'equazione diofantea $ax + by = c$.*

Dimostrazione — Se u è soluzione di $ax \equiv c \pmod{b}$, allora b divide $au - c$, quindi $au - c = bk$ per un opportuno $k \in \mathbb{Z}$. Ma allora $au - bk = c$, dunque, ponendo $v = -k$, si ha $au + bv = c$, il che significa che (u, v) è soluzione di $ax + by = c$. Viceversa, se esiste $v \in \mathbb{Z}$ tale che (u, v) sia soluzione di $ax + by = c$, cioè tale che $au + bv = c$, allora b divide $bv = au - c$, dunque $au \equiv c \pmod{b}$ e u è soluzione di $ax \equiv c \pmod{b}$. □

Possiamo concludere, grazie al Lemma 6, che il problema di risolvere l'equazione diofantea $ax + by = c$ è equivalente al problema di risolvere l'equazione congruenziale $ax \equiv c \pmod{b}$. Infatti, ogni soluzione (u, v) della prima fornisce immediatamente la soluzione u della seconda; viceversa, se u è soluzione della seconda, allora non solo esiste $v \in \mathbb{Z}$ tale che (u, v) sia soluzione della prima, ma tale v è facile da determinare: basta risolvere l'equazione (ad una sola indeterminata) $au + by = c$.

A titolo di esempio, torniamo alla nostra equazione $74x + 22y = 10$. Come abbiamo visto, la coppia $(15, -50)$ ne fornisce una soluzione. Allora 15 è soluzione dell'equazione congruenziale $74x \equiv 10 \pmod{22}$. Utilizzando questa informazione, dalla teoria delle equazioni congruenziali deduciamo che l'insieme di tutte le soluzioni di $74x \equiv 10 \pmod{22}$ è $[15]_{11} = [4]_{11} = 4 + 11\mathbb{Z} = \{4 + 11k \mid k \in \mathbb{Z}\}$. Pertanto le soluzioni (intere) di $74x + 22y = 10$ saranno tutte e sole le coppie (u, v) tali che $u = 4 + 11k$ e v sia soluzione di $74u + 22y = 10$, vale a dire: $v = (10 - 74u)/22$. Svolgendo tutti i calcoli, si ottiene $(10 - 74u)/22 = \big(5 - 37(4 + 11k)\big)/11 = -13 - 37k$, quindi l'insieme delle soluzioni della nostra equazione è

$$\big\{(4 + 11k, -13 - 37k) \,\big|\, k \in \mathbb{Z}\big\}.$$

Per $k = 0$ troviamo così la soluzione $(4, -13)$, mentre la soluzione $(15, -50)$ che avevamo calcolato sopra si ottiene per $k = 1$.

Va infine menzionata una importante applicazione del Teorema di Bézout. Due interi a e b si dicono *coprimi* se e solo se $1 = \mathrm{MCD}(a, b)$. È evidente che questa condizione equivale a richiedere che non esista alcun numero primo che divida sia a che b. Il Teorema di Bézout ha questo caso particolare (anch'esso talvolta chiamato Teorema di Bézout, in effetti il Teorema 5 si può dedurre da questo enunciato):

Corollario 7. *Siano $a, b \in \mathbb{Z}$. Allora a e b sono coprimi se e solo se esistono $u, v \in \mathbb{Z}$ tali che $au + bv = 1$.*

Dimostrazione — Per il Teorema 5, esistono $u, v \in \mathbb{Z}$ tali che $au + bv = 1$ se e solo se $\mathrm{MCD}(a, b)$ divide 1. Poiché i soli divisori di 1 sono 1 e -1, questa condizione equivale a $\mathrm{MCD}(a, b) = 1$, cioè a richiedere che a e b siano coprimi. □

Proposizione 8. *Siano a e b due interi coprimi. Per ogni $c \in \mathbb{Z}$, se $a \mid bc$ allora $a \mid c$.*

Dimostrazione — Per il Teorema di Bézout (o per il Corollario 7) si ha $1 = au + bv$ per opportuni $u, v \in \mathbb{Z}$. Moltiplicando per c otteniamo $c = acu + bcv$. Dunque c è combinazione lineare di a e bc; poiché a divide a e, per ipotesi, bc allora il Lemma 1 prova che a divide c. □

La funzione di Eulero

La funzione φ di Eulero (o funzione di Euler-Gauss) è l'applicazione di $\mathbb{N}^{\#}$ in sé definita ponendo, per ogni $n \in \mathbb{N}^{\#}$,

$$\varphi(n) = \big|\{a \in \mathbb{N}^{\#} \mid a \leq n \wedge a \text{ e } n \text{ sono coprimi}\}\big|.$$

Ad esempio, poiché tra gli interi positivi 1, 2, 3, 4, 5 e 6 ad essere coprimi con 6 sono (solo) 1 e 5 si ha $\varphi(6) = 2$.

La funzione di Eulero esprime le cardinalità del gruppo degli invertibili dei quozienti di $\mathbb{Z}$. Infatti, per ogni $n \in \mathbb{N}^{\#}$, sappiamo che gli elementi dell'anello $\mathbb{Z}_n$ corrispondono precisamente ai numeri interi positivi a tali che $a \leq n$, nel senso che

$$\mathbb{Z}_n = \{[a]_n \mid a \in \mathbb{N}^{\#} \wedge a \leq n\}$$

e se a e b sono interi positivi minori o uguali a n si ha $[a]_n = [b]_n$ se e solo se $a = b$. Sappiamo inoltre che, con queste stesse notazioni, $[a]_n$ è invertibile in $\mathbb{Z}_n$ se e solo se a e n sono coprimi. Dunque

$$\mathcal{U}(\mathbb{Z}_n) = \{[a]_n \mid a \in \mathbb{N}^{\#} \wedge a \leq n \wedge a \text{ e } n \text{ sono coprimi}\}$$

e quindi

$$\big|\mathcal{U}(\mathbb{Z}_n)\big| = \varphi(n).$$

Calcolo dei valori della funzione di Eulero. Sia p un numero (naturale) primo, e sia $n \in \mathbb{N}^{\#}$. Se $a \in \mathbb{Z}$ è chiaro che se a e p^n non sono coprimi, dunque se a e p hanno un fattore primo positivo in comune, questo fattore non potrà che essere p, l'unico divisore positivo primo di p^n. Da ciò segue facilmente che gli interi non coprimi con p^n sono tutti e soli i multipli p. Abbiamo allora:

$$\varphi(p^n) = \big|\{a \in \mathbb{N}^{\#} \mid a \leq n \wedge p \nmid a\}\big|.$$

Per ottenere $\varphi(p^n)$ basta dunque sottrarre a p^n (il numero degli interi positivi minori o uguali a p^n) il numero dei multipli positivi di p minori o uguali a p^n. Questi multipli sono $p, 2p, 3p, \ldots, p^{n-1}p = p^n$, e sono evidentemente p^{n-1} in tutto. Pertanto:

$$\varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1). \qquad (*)$$

Un caso particolare, per $n = 1$, è $\varphi(p) = p - 1$, cosa che si può verificare anche direttamente (tutti gli interi positivi minori di p sono coprimi con p).

Il calcolo di $\varphi(n)$ per un arbitrario intero positivo n si esegue utilizzando $(*)$ e la prossima informazione, di cui si omette la dimostrazione:

$$\textit{se } s \textit{ e } t \textit{ sono interi positivi } \underline{\textit{coprimi}} \textit{ si ha } \varphi(st) = \varphi(s)\varphi(t). \qquad (**)$$

Da una applicazione ripetuta di questo risultato si ottiene un enunciato (apparentemente) più generale: *se $t_1, t_2, \ldots, t_r$ sono interi positivi a due a due coprimi, si ha* $\varphi(t_1 t_2 \cdots t_r) = \varphi(t_1)\varphi(t_2)\cdots\varphi(t_r)$.

Sia ora assegnato $n \in \mathbb{N}^{\#}$, e supponiamo di voler calcolare $\varphi(n)$. Scomponiamo n in prodotto di potenze di primi, dunque $n = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_r^{\lambda_r}$ per opportuni primi $p_1, p_2, \ldots, p_r$ a due a due distinti e interi positivi $\lambda_1, \lambda_2, \ldots, \lambda_r$. Allora $\varphi(n) = \varphi(p_1^{\lambda_1})\varphi(p_2^{\lambda_2})\cdots\varphi(p_r^{\lambda_r})$, che sappiamo calcolare grazie a $(*)$.

Esempio. Calcoliamo $\varphi(360)$. Si ha $360 = 2^3 3^2 5$. Ora, $\varphi(2^3) = 2^3 - 2^2 = 8 - 4 = 4$, inoltre $\varphi(3^2) = 3^2 - 3 = 6$ e $\varphi(5) = 5 - 1 = 4$. Pertanto

$$\varphi(360) = \varphi(2^3)\varphi(3^2)\varphi(5) = 4 \cdot 6 \cdot 4 = 96.$$

Notare che $\varphi(360) = \varphi(36 \cdot 10) \neq \varphi(36)\varphi(10) = \varphi(4)\varphi(9)\varphi(2)\varphi(5) = 2 \cdot 6 \cdot 1 \cdot 4 = 48$; più semplicemente $2 = \varphi(4) = \varphi(2 \cdot 2) \neq \varphi(2)\varphi(2) = 1 \cdot 1 = 1$. Ciò mostra come in $(**)$ sia importante l'ipotesi che i fattori s e t siano tra loro coprimi.

Polinomi su un anello commutativo unitario

GIOVANNI CUTOLO

1. Definizione e terminologia essenziale

Sia A un anello commutativo unitario. Per definizione, un *anello di polinomi* a coefficienti in A nell'indeterminata x è un anello commutativo unitario $A[x]$ che verifichi le condizioni:

- (P_1) A è un sottoanello unitario di $A[x]$;[1]
- (P_2) $x \in A[x]$;
- (P_3) per ogni $f \in A[x]$ esiste una ed una sola successione $\underline{a} = (a_i)_{i\in\mathbb{N}}$ di elementi di A con la proprietà che esista $n \in \mathbb{N}$ tale che:
  - (i) $f = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$, e
  - (ii) $a_i = 0_A$ per ogni intero $i > n$.

È possibile dimostrare, ma non lo faremo qui, che per ogni anello commutativo unitario A esiste un anello di polinomi $A[x]$ come qui specificato; vedremo più avanti che, fissato A, questi anelli di polinomi sono tutti isomorfi tra loro. Vengono chiamati *polinomi* (a coefficienti in A) gli elementi di un tale anello $A[x]$.

Lasciando fisse le notazioni per A e x appena stabilite, facciamo alcune osservazioni che dovrebbero aiutare a comprendere meglio la definizione di anello di polinomi, introducendo nel contempo un po' di terminologia.

Come mostra (P_1), gli elementi di A sono anch'essi polinomi; in questo contesto chiameremo spesso *polinomi costanti* gli elementi di A. Tra essi c'è 0_A (che è ovviamente anche lo zero di $A[x]$), chiamato anche *polinomio nullo*.

Per ogni $f \in A[x]$, la successione $\underline{a} := (a_i)_{i\in\mathbb{N}}$ descritta in (P_3) in relazione ad f viene chiamata la *successione dei coefficienti* di f e, per ciascun $i \in \mathbb{N}$, ci si riferisce talvolta ad a_i come al coefficiente di posto i (o coefficiente i-esimo) di f. Quanto richiesto al punto (ii) in (P_3) mostra che l'insieme $S_f := \{i \in \mathbb{N} \mid a_i \neq 0_A\}$ è finito (tutti gli elementi di S_f sono compresi tra 0 ed il numero che in (P_3) appare come n). Se $f \neq 0_A$ si ha ovviamente $S_f \neq \varnothing$, quindi S_f, essendo un sottoinsieme finito non vuoto di $\mathbb{N}$, ha massimo; questo massimo è chiamato il *grado* di f, denotato col simbolo νf (o anche con altri simboli, tra i quali $\nu(f)$, $\deg f$ e $\delta(f)$). Il coefficiente $a_{\nu f}$ di posto νf si chiama *coefficiente direttore* di f e verrà indicato con $\operatorname{cd} f$. In altri termini, se f è un polinomio non nullo, il grado di f è il massimo intero i tale che il coefficiente i-esimo di f non sia nullo, e questo stesso coefficiente è il coefficiente direttore di f. Ad esempio, in un anello $\mathbb{Z}[x]$ di polinomi a coefficienti in $\mathbb{Z}$ nell'indeterminata x c'è il polinomio $h = 1 + 3x - 2x^3$; la successione dei coefficienti di h è la successione $(a_i)_{i\in\mathbb{N}}$ di numeri interi definita ponendo $a_0 = 1$, $a_1 = 3$, $a_3 = -2$ e $a_i = 0$ per ogni $i \in \mathbb{N} \smallsetminus \{0, 1, 3\}$. Allora $S_h = \{0, 1, 3\}$, quindi il grado di h è 3 ed il coefficiente direttore di h è $a_3 = -2$. Un altro esempio: se $0_A \neq a \in A$ (cioè: se a è un polinomio costante non nullo) la successione $(a_i)_{i\in\mathbb{N}}$ dei coefficienti di a è quella definita da $a_0 = a$ ed $a_i = 0_A$ per ogni $i \in \mathbb{N}^*$, dunque $S_a = \{0\}$, quindi a ha grado 0 e coefficiente direttore a.

Tornando al caso generale, le definizioni appena date di grado e di coefficiente direttore per un polinomio non nullo non si possono direttamente adattare al polinomio nullo $0_A = 0_{A[x]}$ su un anello commutativo unitario A. Infatti, come si verifica immediatamente, il polinomio nullo ha la successione costante 0_A (cioè la successione $(a_i)_{i\in\mathbb{N}}$ in cui $a_i = 0_A$ per ogni $i \in \mathbb{N}$) come successione dei coefficienti. In altri termini: questo polinomio non ha coefficienti non nulli. Si conviene di estendere al polinomio nullo di $A[x]$ le definizioni di coefficiente direttore e grado ponendo $\operatorname{cd} 0_A = 0_A$ e $\nu 0_A = -\infty$, dove $-\infty$ è un simbolo, appunto, convenzionale al quale non attribuiamo uno specifico significato; richiediamo solo $-\infty \notin \mathbb{N}$ ed estendiamo a $\mathbb{N} \cup \{-\infty\}$ sia l'ordinamento che l'addizione usualmente definiti in $\mathbb{N}$, ponendo, per ogni $n \in \mathbb{N} \cup \{-\infty\}$, $-\infty \leq n$ e $(-\infty) + n = n + (-\infty) = -\infty$.

Osserviamo che, allora, i polinomi costanti sono tutti e soli i polinomi in $A[x]$ di grado minore di 1: quelli non nulli hanno grado 0, mentre il polinomio nullo è l'unico che abbia grado $-\infty$; tutti i polinomi non costanti hanno invece grado positivo. Inoltre, il polinomio nullo è l'unico polinomio con coefficiente direttore 0_A.

Riassumendo: per ogni polinomio non nullo $f \in A[x]$, la proprietà (P_3) garantisce che f si può scrivere in unico modo nella forma $\sum_{i=0}^{n} a_i x^i$ dove $n \in \mathbb{N}$, per ogni $i \in \{0, 1, 2, \ldots, n\}$ si ha $a_i \in A$ e $a_n \neq 0_A$; questo accade se si pone $n = \nu f$ e gli elementi a_i sono i primi $n+1$ termini della successione dei coefficienti di f (e quindi $a_n = \operatorname{cd} f$); i termini rimanenti della successione dei coefficienti di f sono poi tutti uguali a 0_A.[2]

Aggiungiamo ancora della terminologia: diremo che un polinomio è *monico* se e solo se il suo coefficiente direttore è 1_A. Si usa infine chiamare *termine noto* di un polinomio il suo coefficiente di posto 0.

Completiamo questa sezione introduttiva notando esplicitamente una facile conseguenza dalla proprietà (P_3). Se A è un anello commutativo unitario *non nullo* (cioè tale che $A \neq \{0_A\}$), per ogni $n \in \mathbb{N}$ il polinomio x^n ha

[1] si ricorda cosa questo significhi: A è un sottoanello di $A[x]$ e l'unità 1_A di A appartiene ad $A[x]$, quindi è anche l'unità di $A[x]$.

[2] possiamo anche aggiungere che, invece, verificano le proprietà richieste per n in (i) e (ii) di (P_3) tutti e soli i numeri naturali $n \geq \nu f$.

grado n (perché il suo coefficiente n-esimo è 1_A mentre tutti gli altri coefficienti sono uguali a 0_A), quindi $x^n \notin A$ se $n > 0$ (in particolare, $x \notin A$) e se m è un numero naturale diverso da n, allora $x^n \neq x^m$. In altri termini: se $|A| \neq 1$ le potenze di x in $A[x]$ con esponente un numero naturale sono a due a due distinte, quindi: *se A è un anello commutativo unitario non nullo, l'anello di polinomi $A[x]$ è infinito.*[3]

Approfondimenti.[4] Abbiamo un modo più preciso per chiarire la relazione che intercorre tra un polinomio e la sua successione dei coefficienti. Chiamiamo supporto di una successione $\underline{a} := (a_i)_{i\in\mathbb{N}}$ di elementi di A l'insieme $\{i \in \mathbb{N} \mid a_i \neq 0_A\}$, e indichiamo con A_ω l'insieme delle successioni di elementi di A con supporto finito. Le successioni dei coefficienti dei polinomi hanno supporto finito; abbiamo così l'applicazione $\sigma\colon A[x] \to A_\omega$ che ad ogni polinomio in $A[x]$ associa la sua successione dei coefficienti. *Questa applicazione è biettiva.* Infatti, sia $\underline{a} = (a_i)_{i\in\mathbb{N}} \in A_\omega$. Se $\{i \in \mathbb{N} \mid a_i \neq 0_A\}$ non è vuoto sia n il suo massimo, altrimenti poniamo $n = 0$. In entrambi i casi, è chiaro che il polinomio $f_{\underline{a}} := \sum_{i=0}^n a_i x^i$ ha $\underline{a}$ come successione dei coefficienti. È altrettanto chiaro che, per ogni $f \in A[x]$, se $\underline{a}$ è la successione dei coefficienti di f, allora $f = f_{\underline{a}}$. Dunque, l'applicazione $\underline{a} \in A_\omega \mapsto f_{\underline{a}} \in A[x]$ è l'inversa di σ.

Menzioniamo il fatto che una delle possibili costruzioni di un anello dei polinomi su A si ottiene proprio definendo due operazioni (di addizione e moltiplicazione) nell'insieme A_ω che rendano questo un anello commutativo unitario in cui si può immergere A, in modo che A_ω risulti un anello di polinomi ad una indeterminata a coefficienti in A.

2. Proprietà universale

La proprietà più importante degli anelli di polinomi è la seguente:

Proprietà universale per anelli di polinomi ad una indeterminata. *Sia $A[x]$ un anello di polinomi nell'indeterminata x sull'anello commutativo unitario A. Si fissino un anello commutativo unitario B ed un omomorfismo $\theta\colon A \to B$ di anelli unitari*[5] *e $b \in B$. Allora esiste uno ed un solo omomorfismo $\theta^*\colon A[x] \to B$ di anelli unitari tale che $x^{\theta^*} = b$ e θ sia la restrizione di θ^* ad A.*[6]

In altre parole, assegnati omomorfismi (di anelli commutativi unitari) come nel diagramma a sinistra (l'omomorfismo $A \hookrightarrow A[x]$ è l'immersione di A in $A[x]$) ed un arbitrario $b \in B$, esiste uno ed un solo omomorfismo θ^* che renda commutativo il diagramma a destra mandando x in b:

Diamo solo un cenno alla dimostrazione, che si può completare per esercizio. Dalla definizione di omomorfismo di anelli segue subito che θ^* non può essere altro che l'applicazione

$$\theta^*\colon \sum_{i=0}^n a_i x^i \in A[x] \longmapsto \sum_{i=0}^n a_i^\theta b^i \in B$$

(qui gli a_i rappresentano elementi di A); è da osservare che ogni elemento di $A[x]$ si scrive nella forma indicata, e segue dalla (P_3) che l'applicazione θ^* è ben definita; si può poi verificare che essa è effettivamente un omomorfismo di anelli unitari e che manda x in b. In questo modo la proprietà universale è provata.

Vediamo alcune importanti applicazioni della proprietà universale:

- *Unicità dell'anello dei polinomi, a meno di isomorfismi.* Supponiamo che $A[x]$ e $A[y]$ siano anelli di polinomi ad una indeterminata sullo stesso anello (commutativo unitario) A, con indeterminate, rispettivamente, x e y. Applichiamo la proprietà universale scegliendo come θ l'immersione $A \hookrightarrow A[y]$ e, come b, l'elemento y. Otteniamo così un (unico) omomorfismo $\alpha\colon A[x] \to A[y]$ tale che $x^\alpha = y$ e la restrizione di α ad A sia l'immersione, cioè $a^\alpha = a$ per ogni $a \in A$. Poiché anche $A[y]$ è un anello dei polinomi, possiamo ripetere la stessa costruzione scambiando i ruoli di $A[x]$ (ed x) e $A[y]$ (ed y),

  ottenendo un omomorfismo $\beta\colon A[y] \to A[x]$ tale che $y^\beta = x$ e $a^\beta = a$ per ogni $a \in A$. È facile verificare che α e β sono l'uno l'inverso dell'altro. Infatti, per ogni elemento $f = \sum_{i=0}^n a_i x^i$ di $A[x]$ si ha $f^{\alpha\beta} = (\sum_{i=0}^n a_i y^i)^\beta = \sum_{i=0}^n a_i x^i = f$ e, similmente, $g^{\beta\alpha} = g$ per ogni $g \in A[y]$. Ciò prova che α è un isomorfismo.

---

[3] segue invece facilmente da (P_1) che se A è l'anello nullo, cioè se $|A| = 1$, allora $A[x] = A$.

[4] non richiesti ai fini dell'esame.

[5] si intende con questo che θ è un omomorfismo di anelli che manda l'unità di A nell'unità di B.

[6] in queste note le immagini di elementi mediante applicazioni sono generalmente indicate con la notazione esponenziale, quindi, ad esempio, x^{θ^*} è l'immagine di x mediante θ^*.

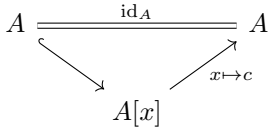
Dunque, assegnati due anelli di polinomi ad una indeterminata su A esiste un isomorfismo tra questi due anelli di polinomi che manda l'indeterminata del primo nell'indeterminata del secondo e manda in se stesso ogni elemento di A. Con le notazioni appena usate, questo isomorfismo è l'applicazione

$$\alpha\colon \sum_{i=0}^{n} a_i x^i \in A[x] \longmapsto \sum_{i=0}^{n} a_i y^i \in A[y],$$

osserviamo esplicitamente che essa manda ogni polinomio f di $A[x]$ nel polinomio di $A[y]$ che ha la stessa successione dei coefficienti di f.

Possiamo dunque dire, in modo un pò approssimativo ma efficace, che due anelli di polinomi sullo stesso anello commutativo unitario A possono solo differire per il nome dell'indeterminata; in questo senso, a meno di isomorfismi, ne esiste solo uno. Per questo motivo possiamo decidere di aver fissato, per ogni scelta di A, un anello dei polinomi $A[x]$ ad una indeterminata su A e chiamare questo *l'*anello dei polinomi ad una indeterminata su A (con l'articolo determinativo).

- L'applicazione più frequente della proprietà universale si ha per il caso in cui $B = A$ e θ è l'applicazione identica di A. In questo caso la proprietà ci dice che per ogni $c \in A$ esiste uno ed un solo omomorfismo di anelli unitari $A[x] \to A$ che manda ogni elemento di A in sé e x in c:

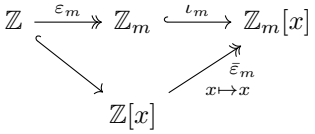


È facile descrivere esplicitamente questo omomorfismo. Per ogni $f = \sum_{i=0}^{n} a_i x^i \in A[x]$ poniamo $f(c) = \sum_{i=0}^{n} a_i c^i$. L'omomorfismo di cui stiamo parlando è allora l'applicazione:

$$f \in A[x] \longmapsto f(c) \in A,$$

che chiamiamo *omomorfismo di sostituzione*.

- Un'applicazione più specifica: per ogni intero positivo m, sia $\varepsilon_m\colon n \in \mathbb{Z} \mapsto [n]_m \in \mathbb{Z}_m$, la proiezione canonica $\mathbb{Z} \twoheadrightarrow \mathbb{Z}_m$ (il simbolo di freccia a doppia punta ci ricorda il fatto che ε_m è un omomorfismo suriettivo). Componendo questa con l'immersione $\iota_m\colon \mathbb{Z}_m \hookrightarrow \mathbb{Z}_m[x]$ otteniamo l'omorfismo di anelli unitari[7] $\varepsilon_m\iota_m\colon n \in \mathbb{Z} \mapsto [n]_m \in \mathbb{Z}_m[x]$ (come di consueto, usiamo lo stesso simbolo, x, per l'indeterminata di diversi anelli di polinomi). La proprietà universale fornisce l'omomorfismo $\bar{\varepsilon}_m$ qui descritto:



(è facile verificare che $\bar{\varepsilon}_m$ è effettivamente suriettivo). Più esplicitamente, l'immagine mediante $\bar{\varepsilon}_m$ di $f = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ è il polinomio $f_m = \sum_{i=0}^{n} [a_i]_m x^i$. Per indicare questo polinomio scriveremo spesso $\sum_{i=0}^{n} \bar{a}_i x^i \in \mathbb{Z}_m[x]$; (è ovviamente essenziale indicare sempre il modulo m, per evitare ambiguità) o anche, ancora più semplicemente, $\sum_{i=0}^{n} a_i x^i \in \mathbb{Z}_m[x]$. Si dice che f_m è *il polinomio f riguardato come polinomio a coefficienti in $\mathbb{Z}_m$* (o anche *... modulo m*). Ad esempio, se $f = 14x^3 - 3x + 1 \in \mathbb{Z}[x]$, il polinomio f riguardato come polinomio a coefficienti in $\mathbb{Z}_5$ è $\bar{4}x^3 - \bar{3}x + \bar{1} \in \mathbb{Z}_5[x]$, che possiamo anche scrivere come $-x^3 + \bar{2}x + \bar{1} \in \mathbb{Z}_5[x]$, o in infiniti altri modi.

Possiamo riferirci a quest'ultima costruzione per illustrare con qualche esempio le nozioni introdotte nella sezione precedente e vedere come grado e coefficiente direttore possono cambiare nel passaggio da un polinomio a coefficienti in $\mathbb{Z}$ al corrispondente polinomio riguardato modulo un intero positivo. Il polinomio $f = 15x^4 + 6x^2 + 2 \in \mathbb{Z}[x]$ ha grado 4 e coefficiente direttore 15. Invece f_5, cioè f riguardato come polinomio a coefficienti in $\mathbb{Z}_5$ ha grado 2 (il suo quarto coefficiente è $[15]_5 = [0]_5 = 0_{\mathbb{Z}_5}$ e coefficiente direttore $[6]_5 = [1]_5 = 1_{\mathbb{Z}_5}$, dunque f_5 è monico; possiamo scrivere $f_5 = x^2 + \bar{2} \in \mathbb{Z}_5[x]$. Invece f_3, cioè f riguardato come polinomio a coefficienti in $\mathbb{Z}_3$, ha grado 0 e si ha $f_3 = \operatorname{cd} f_3 = [2]_3 = -1_{\mathbb{Z}_3}$; dunque f_3 è un polinomio costante.

3. Grado di somme e prodotti di polinomi

Siano, ancora, A un anello commutativo unitario, e siano $f, g \in A[x]$, con successioni dei coefficienti, rispettivamente, $(a_n)_{n\in\mathbb{N}}$ e $(b_n)_{n\in\mathbb{N}}$. Supponiamo anche $f \neq 0_A \neq g$ e poniamo $n = \nu f$, $m = \nu g$; dunque $f = \sum_{i=0}^{n} a_i x^i$ e $g = \sum_{i=0}^{m} b_i x^i$; inoltre $a_n = \operatorname{cd} f \neq 0_A$ e $b_m = \operatorname{cd} g \neq 0_A$. Allora, posto $M = \max\{n, m\}$,

$$f + g = \sum_{i=0}^{M} (a_i + b_i) x^i; \qquad f - g = \sum_{i=0}^{M} (a_i - b_i) x^i; \qquad fg = (a_0 b_0) + (a_0 b_1 + a_1 b_0) x + \cdots + (a_n b_m) x^{n+m}.$$[8]

[7] In conformità all'uso della notazione esponenziale per le immagini di elementi del dominio di un'applicazione, la composizione di applicazioni è indicata in queste note nell'ordine naturale, scrivendo a sinistra l'applicazione che agisce per prima, quindi fg piuttosto che $g \circ f$ se f e g sono applicazioni componibili. Ad esempio, $\varepsilon_m\iota_m = \iota_m \circ \varepsilon_m$

[8] più precisamente: $fg = \sum_{i=0}^{n+m} c_i x^i$, dove, per ogni i, si ha $c_i = \sum_{j=0}^{i} a_j b_{i-j} = a_0 b_i + a_1 b_{i-1} + a_2 b_{i+2} + \cdots + a_{i-1} b_1 + a_i b_0$.

Cosa possiamo dire sui gradi di questi tre polinomi? Consideriamo in primo luogo $f+g$. Nella sua espressione non appaiono potenze di x con esponente superiore a M, quindi certamente $\nu(f+g) \leq M$, e $\nu(f+g) = M$ se e solo se il coefficiente di posto M in $f+g$ (cioè $a_M + b_M$) è diverso da zero. Distinguiamo tre casi: se $n < m$ allora $M = m$ e $a_m = 0_A$, quindi $a_M + b_M = b_m \neq 0_A$. In questo caso, dunque, $\nu(f+g) = m = M$, inoltre $\operatorname{cd}(f+g) = b_m = \operatorname{cd} g$. Ad esempio: se $A = \mathbb{Z}$, $f = 2x+1$ e $g = 3x^4 + 2x + 2$ (quindi $n = 1 < m = 4$) allora $f + g = 3x^4 + 4x + 3$ ha grado $4 = m$. Similmente, se $n > m$, vediamo che $f + g$ ha grado n e coefficiente direttore $a_n = \operatorname{cd} f$. Nel terzo caso, quello in cui $n = m$, bisogna fare una distinzione ulteriore: se $a_n + b_n \neq 0_A$ abbiamo $\nu(f+g) = n = M$ e $\operatorname{cd}(f+g) = a_n + b_n$, ma se invece $a_n + b_n = 0_A$ (cioè $a_n = -b_n$) allora certamente $\nu(f+g) < n$, perché per ogni intero $i > n-1$ il coefficiente i-esimo di $f+g$ è 0_A. Possiamo riassumere così ciò che abbiamo provato sino a questo punto:

Proposizione 1. *Se A è un anello commutativo unitario e $f, g \in A[x] \smallsetminus \{0_A\}$, allora $\nu(f+g) = \max\{\nu f, \nu g\}$ a meno che $\nu f = \nu g$ e $\operatorname{cd} f = -\operatorname{cd} g$. In questo secondo caso $\nu(f+g) < \nu f = \nu g$.*

Ripetendo il ragionamento per $f - g$, oppure applicando la Proposizione 1 a f e $-g$ (perché $f - g = f + (-g)$) si ha:

Proposizione 2. *Se A è un anello commutativo unitario e $f, g \in A[x] \smallsetminus \{0_A\}$, allora $\nu(f-g) = \max\{\nu f, \nu g\}$ a meno che $\nu f = \nu g$ e $\operatorname{cd} f = \operatorname{cd} g$. In questo secondo caso $\nu(f-g) < \nu f = \nu g$.*

Vediamo qualche altro esempio, ancora in $\mathbb{Z}[x]$. Se $f = 3x^2 + x + 1$ e $g = 2x^2 + x + 2$ (quindi $n = m = 2$) allora $f - g = x^2 - 1$ ha anch'esso grado 2 (f e g hanno lo stesso grado, ma coefficienti direttori diversi); se invece $g = 3x^2 + x + 2$ allora $\nu f = \nu g$ e $\operatorname{cd} f = \operatorname{cd} g$, quindi $f - g$ non ha grado 2, infatti $f - g = -1$ ha grado 0.

Passiamo ora a considerare il grado di fg. Il ragionamento è simile: poiché nell'espressione di fg non appaiono potenze di x con esponente superiore a $n+m$ certamente $\nu(fg) \leq n+m$ e vale $\nu(fg) = n+m$ se e solo se $a_n b_m$ (il coefficiente $(n+m)$-esimo di fg) è diverso da zero. Abbiamo allora:

Proposizione 3. *Se A è un anello commutativo unitario e $f, g \in A[x] \smallsetminus \{0\}$, posto $a = \operatorname{cd} f$ e $b = \operatorname{cd} g$ si ha:*

(i) *se $ab \neq 0_A$, allora $\operatorname{cd}(fg) = ab$ e $\nu(fg) = \nu f + \nu g$. In particolare, $fg \neq 0_A$;*
(ii) *se $ab = 0_A$, allora $\nu(fg) < \nu f + \nu g$.*

Se si verifica $\nu(fg) = \nu f + \nu g$, come nel caso (i) di questa proposizione, si dice che per i polinomi f e g vale la *regola di addizione dei gradi*. Ovviamente questa regola vale sempre nel caso in cui uno tra f e g è il polinomio nullo: se, ad esempio, $f = 0_A$, allora $\nu(fg) = \nu(0_A) = -\infty = (-\infty) + \nu g = \nu f + \nu g$.

Alcune importanti conseguenze della Proposizione 3 sono:

Corollario 4. *Sia A un anello commutativo unitario e sia $f \in A[x]$. Se $\operatorname{cd} f$ è cancellabile in A allora f è cancellabile in $A[x]$ e, per ogni $g \in A[x]$, si ha $\nu(fg) = \nu f + \nu g$.*

Dimostrazione. Sia $g \in A[x] \smallsetminus \{0_A\}$ e siano $a = \operatorname{cd} f$ e $b = \operatorname{cd} g$. Poiché a è cancellabile in A, quindi non un divisore dello zero, e $b \neq 0_A$ allora $ab \neq 0_A$. Per la Proposizione 3, allora $fg \neq 0_A$ e, inoltre, $\nu(fg) = \nu f + \nu g$. La prima informazione ci dice che f non è un divisore dello zero, e quindi è cancellabile, in $A[x]$. Con questo (ricordando che la regola di addizione dei gradi vale banalmente se uno dei polinomi coinvolti è quello nullo) la dimostrazione è completa. □

Proposizione 5. *Sia A un anello commutativo unitario. Sono allora equivalenti:*

(i) *A è un dominio di integrità;*
(ii) *per ogni coppia di polinomi $A[x]$ vale la regola di addizione dei gradi (cioè: $\forall f, g \in A[x](\nu(fg) = \nu f + \nu g)$);*
(iii) *$A[x]$ è un dominio di integrità.*

Inoltre, se A è un dominio di integrità allora $\mathcal{U}(A[x]) = \mathcal{U}(A)$.[(9)]

Dimostrazione. Supponiamo che A sia un dominio di integrità, e siano $f, g \in A[x]$. Se $f = 0_A$, allora vale banalmente $\nu(fg) = \nu(0_A) = -\infty = \nu f + \nu g$. Se invece $f \neq 0_A$, allora $\operatorname{cd} f \neq 0_A$, quindi, poiché A è un dominio di integrità, $\operatorname{cd} f$ è cancellabile in A e $\nu(fg) = \nu f + \nu g$ per il Corollario 4. Abbiamo provato che (i) implica (ii).

Che (ii) implichi (iii) è ovvio: se $f, g \in A[x] \smallsetminus \{0_A\}$ e in $A[x]$ vale la regola di addizione dei gradi, allora, come per la Proposizione 3, si ha $\nu(fg) = \nu f + \nu g \geq 0$, quindi $fg \neq 0_A$; questo significa che in $A[x]$ vale la legge di annullamento del prodotto e dunque $A[x]$ è un dominio di integrità.

Anche l'implicazione (iii) $\Rightarrow$ (i) è banale: se $A[x]$ è un dominio di integrità e a e b sono elementi di $A \smallsetminus \{0_A\}$, allora $ab \neq 0_A$, perché altrimenti a sarebbe un divisore dello zero in $A[x]$.[(10)]

Resta solo da provare che $\mathcal{U}(A[x]) = \mathcal{U}(A)$ se valgono le condizioni (i), (ii) e (iii). Se $a \in \mathcal{U}(A)$ e b è l'inverso di a in A, allora $ab = 1_A = 1_{A[x]}$, quindi b è anche l'inverso di a in $A[x]$, dunque $a \in \mathcal{U}(A[x])$. Pertanto $\mathcal{U}(A) \subseteq \mathcal{U}(A[x])$.[(11)] Nell'ipotesi che A sia un dominio di integrità sia, viceversa, $f \in \mathcal{U}(A[x])$ e sia g l'inverso di f in $A[x]$. Allora $fg = 1_A$ e, ovviamente, $f \neq 0_A \neq g$. Poiché in $A[x]$ vale la regola di addizione dei gradi,

(9) ricordiamo che, per ogni anello unitario R, con $\mathcal{U}(R)$ si indica il gruppo moltiplicativo degli elementi invertibili di R.

(10) in sostanza, ciò che stiamo osservando è che i sottoanelli non nulli dei domini di integrità sono essi stessi domini di integrità.

(11) anche in questo caso l'argomentazione mostra qualcosa che vale in contesti più generali: se A è un sottoanello *unitario* di un anello unitario R, allora $\mathcal{U}(A) \subseteq \mathcal{U}(R)$.

$\nu f + \nu g = \nu(fg) = \nu(1_A) = 0$. Dunque, νf e νg sono due numeri naturali la cui somma è 0; di conseguenza $\nu f = \nu g = 0$. Ciò mostra che $f \in A$ e $g \in A$, quindi sia f che il suo inverso sono elementi di A, dunque $f \in \mathcal{U}(A)$. Abbiamo così provato anche l'inclusione $\mathcal{U}(A[x]) \subseteq \mathcal{U}(A)$; a questo punto la dimostrazione è completa. □

Vediamo così che la regola di addizione dei gradi non vale per polinomi su anelli che non siano domini di integrità, ed è importante osservare che per tali anelli può non valere neanche la conclusione finale della Proposizione 5: non è detto che i polinomi invertibili siano costanti. Se ad esempio scegliamo come A l'anello $\mathbb{Z}_4$ e poniamo $f = \bar{2}x + \bar{1} \in \mathbb{Z}_4[x]$, allora $f^2 = \bar{4}x^2 + \bar{4}x + \bar{1} = \bar{1} = 1_{\mathbb{Z}_4}$, quindi non solo $0 = \nu(f \cdot f) < \nu f + \nu f$ e non vale in questo caso la regola di addizione dei gradi, ma addirittura abbiamo $f \in \mathcal{U}(\mathbb{Z}_4[x])$ (si ha $f^{-1} = f$) pur non essendo f un polinomio costante. Quindi $\mathcal{U}(\mathbb{Z}_4[x]) \neq \mathcal{U}(\mathbb{Z}_4)$, anzi $\mathcal{U}(\mathbb{Z}_4[x]) \not\subseteq \mathbb{Z}_4$.

Un ragionamento simile a quello svolto nella dimostrazione della Proposizione 5 utilizzando la regola di addizione dei gradi mostra che i polinomi monici di grado maggiore di zero non sono mai invertibili. Ad esempio, qualunque sia l'anello commutativo unitario non nullo A, l'indeterminata x non è invertibile in $A[x]$. Infatti, se x fosse invertibile, detto g il suo inverso, avremmo $1_A = xg$ e quindi $\nu(xg) = 0$, ma, per il Corollario 4, vale per x e g la regola di addizione dei gradi, quindi $\nu(xg) = \nu x + \nu g = 1 + \nu g$, in contraddizione con quanto appena detto.[12] Di conseguenza, *qualsiasi sia l'anello commutativo unitario non nullo* A, in $A[x]$ esistono elementi non invertibili e diversi dallo zero, quindi $A[x]$ *non è un campo.*[13]

4. Divisione con resto tra polinomi

Se f e g sono due polinomi su un anello commutativo unitario A, con $g \neq 0_A$, diciamo che in $A[x]$ è possibile effettuare la divisione di f (il *dividendo*) per g (il *divisore*) se e solo se esistono $q, r \in A[x]$ (che chiamiamo rispettivamente *quoziente* e *resto*) tali che $f = gq + r$ e $\nu r < \nu g$.

Un'osservazione banale è che se, nella situazione appena descritta, $\nu f < \nu g$ allora è sicuramente possibile effettuare la divisione di f per g: basta porre $q = 0$ e $r = f$. Il teorema che segue garantisce non solo la possibilità di effettuare la divisione, ma anche l'unicità di quoziente e resto in un caso importante.

Teorema 6. *Siano A un anello commutativo unitario e $f, g \in A[x]$. Supponiamo $\operatorname{cd} g \in \mathcal{U}(A)$. Allora esiste una ed una sola coppia $(q, r) \in A[x] \times A[x]$ tale che $f = gq + r$ e $\nu r < \nu g$.*

Dimostrazione. Iniziamo a provare l'esistenza di (q, r). Come appena osservato, se $\nu f < \nu g$ una coppia con le proprietà richieste si ottiene ponendo $q = 0$ e $r = f$. Possiamo allora supporre $n := \nu f \geq m := \nu g$; osserviamo che l'ipotesi su $\operatorname{cd} g$ garantisce $\operatorname{cd} g \neq 0_A$ e quindi $n, m \in \mathbb{N}$. Ragioniamo per induzione su n, quindi supponiamo che, per ogni $h \in A[x]$ tale che $\nu h < n$, sia possibile effettuare la divisione di h per g. Siano $a = \operatorname{cd} f$ e $b = \operatorname{cd} g$. Consideriamo il polinomio $k = ab^{-1}x^{n-m}g$. È chiaro che per $ab^{-1}x^{n-m}$ e g vale la regola di addizione dei gradi, in quanto il prodotto dei coefficienti direttori di questi due polinomi è $(ab^{-1})\operatorname{cd}(g) = ab^{-1} \cdot b = a \neq 0_A$ (vedi Proposizione 3). Dunque $\nu k = \nu(ab^{-1}x^{n-m}) + \nu g = (n - m) + m = n = \nu f$ e $\operatorname{cd} k = a = \operatorname{cd} f$. Allora f e k hanno lo stesso grado, n, e lo stesso coefficiente direttore, quindi la Proposizione 2 mostra che $h := f - k$ ha grado minore di n. A questo punto l'ipotesi induttiva garantisce che è possibile effettuare la divisione di h per g, dunque esistono $q_1, r_1 \in A[x]$ tali che $h = gq_1 + r_1$ e $\nu r_1 < \nu g$. Ora, $f = k + h = ab^{-1}x^{n-m}g + gq_1 + r_1 = g(ab^{-1}x^{n-m} + q_1) + r_1$, quindi, la coppia (q, r), definita ponendo $q = ab^{-1}x^{n-m} + q_1$ e $r = r_1$, soddisfa le condizioni richieste. L'esistenza della coppia (q, r) è così provata.

Dobbiamo ora verificarne l'unicità. Siano (q, r) e $(\bar{q}, \bar{r})$ due coppie con le proprietà richieste per quoziente e resto, dunque $f = gq + r = g\bar{q} + \bar{r}$, inoltre $\nu r, \nu\bar{r} < m$. Da $gq + r = g\bar{q} + \bar{r}$ segue $g(q - \bar{q}) = \bar{r} - r$. Dalla Proposizione 2 segue $\nu(\bar{r} - r) < m$. D'altra parte, poiché $\operatorname{cd} g$ è invertibile, quindi cancellabile, vale per g e $q - \bar{q}$ la regola di addizione dei gradi, dunque $\nu\big(g(q - \bar{q})\big) = m + \nu(q - \bar{q})$. Abbiamo così $m + \nu(q - \bar{q}) = \nu(\bar{r} - r) < m$. Di conseguenza $\nu(q - \bar{q}) = -\infty$, quindi $q - \bar{q} = 0_A$, ovvero $\bar{q} = q$ e, quindi, poiché $\bar{r} - r = g(q - \bar{q}) = 0_A$, $\bar{r} = r$. L'unicità della coppia (q, r) è così dimostrata. □

Un caso molto importante è quello dei polinomi a coefficienti in un campo. Infatti, se A è un campo e $0_A \neq g \in A[x]$ allora $\operatorname{cd} g$ è invertibile, come ogni elemento non nullo di A. Dunque, in questo caso, l'ipotesi $\operatorname{cd} g \in \mathcal{U}(A)$ nel Teorema 6 può essere sostituita da $g \neq 0_A$. Abbiamo così:

Corollario 7. *Siano K un campo e $f, g \in K[x]$. Se $g \neq 0_K$ esiste una ed una sola coppia $(q, r) \in K[x] \times K[x]$ tale che $f = gq + r$ e $\nu r < \nu g$.*

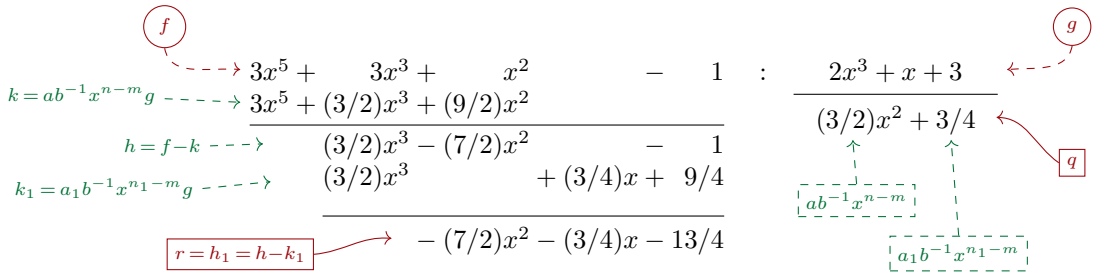
Notiamo che, con la notazione e nelle ipotesi del Teorema 6, g divide f se e solo se il resto (unicamente determinato) della divisione di f per g è 0_A.

Osserviamo poi che la dimostrazione del Teorema 6 fornisce un algorimo per il calcolo di quoziente e resto. Questo algoritmo non è altro che il procedimento comunemente insegnato anche nelle scuole per la divisione tra polinomi. Un esempio dovrebbe bastare a rendere questo punto chiaro. In $\mathbb{Q}[x]$ consideriamo i polinomi $f = 3x^5 + 3x^3 + x^2 - 1$ e $g = 2x^3 + x + 3$, e procediamo a dividere f per g. In accordo con le notazioni della dimostrazione del Teorema 6, poniamo $n = \nu f = 5$, $m = \nu g = 3$, $a = \operatorname{cd} f = 3$ e $b = \operatorname{cd} g = 2$. Abbiamo

[12] più in generale si può verificare, e si consiglia di farlo per esercizio, che lo stesso ragionamento mostra che se f è un polinomio non costante a coefficienti in un anello commutatativo unitario A e $\operatorname{cd} f$ è cancellabile in A, allora f non è invertibile in $A[x]$.

[13] Abbiamo anche accennato in una nota precedente al fatto che se A è nullo, allora anche $A[x]$ è nullo e quindi non è un campo. Dunque, qualsiasi sia l'anello commutativo unitario non nullo A, $A[x]$ non è un campo.

$ab^{-1}x^{n-m} = (3/2)x^2$ (che scriviamo sotto la linea al di sotto di g, perché sarà un addendo del quoziente) e $k = ab^{-1}x^{n-m}g = 3x^5 + (3/2)x^3 + (9/2)x^2$; seguendo la procedura descritta nella dimostrazione del teorema calcoliamo $h = f - k$. Se si avesse $\nu h < m$ allora la divisione sarebbe terminata: h sarebbe il resto, mentre il quoziente sarebbe $ab^{-1}x^{n-m}$.



Nel nostro esempio si ha invece $h = (3/2)x^3 - (7/2)x^2 - 1$, quindi $\nu h \geq m$ (in questo esempio, $\nu h = m$). La divisione va allora continuata, ripetendo la procedura dopo aver sostituito h ad f: posto $a_1 = \operatorname{cd} h$ e $n_1 = \nu h$ calcoliamo $a_1b^{-1}x^{n_1-m}$ (che scriviamo come secondo addendo del quoziente) e poi $k_1 = a_1b^{-1}x^{n_1-m}g$ e $h_1 = h - k_1$. Nel nostro esempio abbiamo $a_1 = 3/2$ e $n_1 = 3$, otteniamo dunque $a_1b^{-1}x^{n_1-m} = 3/4$, $k_1 = (3/2)x^3 + (3/4)x + 9/4$ e $h_1 = -(7/2)x^2 - (3/4)x - 13/4$. Poiché $\nu h_1 < m$ la divisione è terminata: h_1 è il resto, il quoziente è la somma $q = ab^{-1}x^{n-m} + a_1b^{-1}x^{n_1-m}$ dei suoi addendi calcolati fino a questo punto. In altri casi avremmo potuto avere ancora $h_1 \neq 0$ e $\nu h_1 \geq m$ e la divisione non sarebbe terminata qui, ma la procedura avrebbe dovuto essere ancora ripetuta, dopo aver sostituito h_1 ad f, calcolando, come nei passi precedenti, un polinomio h_2, di grado minore di νh_1, ed iterando ancora il procedimento fino ad ottenere un polinomio di grado minore di m: il resto della divisione; nello stesso tempo questo procedimento fornisce il quoziente come somma degli addendi calcolati ad ogni iterazione.

Il fatto che, nell'anello dei polinomi su un campo sia sempre possibile fare la divisione per un polinomio non nullo rende possibile, in questo caso, eseguire l'*algoritmo euclideo* delle divisioni successive per la ricerca del massimo comun divisore, esattamente allo stesso modo che nell'anello degli interi. Se K è un campo e $f, g \in K[x]$, se $g \neq 0_K$ dividiamo f per g ottenendo un quoziente q ed un resto r, se $r \neq 0_K$ dividiamo g per r ottenendo un resto r_1, se $r_1 \neq 0_K$ dividiamo r per r_1; se il resto r_2 così ottenuto non è zero dividiamo r_1 per r_2 e così via. Questo procedimento termina dopo un numero finito di passi perché i successivi resti, finché sono diversi da 0_K, hanno gradi strettamente decrescenti: $\nu g > \nu r > \nu r_1 > \nu r_2 > \cdots (\geq 0)$; dunque questa successione non può essere infinita. Così come per l'algoritmo euclideo in $\mathbb{Z}$ (ed esattamente per lo stesso motivo) l'ultimo resto non nullo è un massimo comun divisore tra f e g. E, sempre come per $\mathbb{Z}$, si può estendere l'algoritmo e dimostrare (costruttivamente) il teorema di Bézout per i polinomi su campi:

Teorema 8 (Teorema di Bézout)**.** *Sia K un campo e siano $f, g \in K[x]$. Sia d un massimo comun divisore in $K[x]$ tra f e g. Allora $\{uf + vg \mid u, v \in K[x]\}$ coincide con l'insieme dei multipli di d in $K[x]$.*

Esempio 9. In $\mathbb{Q}[x]$ consideriamo i polinomi $f = 2x^5 - x^3 + 2x^2 - 1$ e $g = x^5 + x^4 + x^3 + x^2 + x + 1$. Eseguiamo l'algoritmo euclideo per calcolare un massimo comun divisore tra f e g. La divisione di f per g fornisce quoziente 2 e resto $r = -2x^4 - 3x^3 - 2x - 3$, infatti $f = 2 \cdot g + r$. Dividendo g per r otteniamo poi $g = \big(-(1/2)x + 1/4\big) \cdot r + \big((7/4)x^3 + 7/4\big)$, qui $q_1 = -(1/2)x + 1/4$ è il quoziente e $r_1 = (7/4)x^3 + 7/4 = (7/4)(x^3 + 1)$ è il resto. La divisione successiva fornisce resto nullo, infatti $r = \big(-(8/7)x - 12/7\big)r_1$. Quindi r_1, l'ultimo resto non nullo, è un massimo comun divisore tra f e g. La teoria generale della divisibilità in monoidi commutativi ci dice che l'insieme dei massimi comuni divisori tra f e g è l'insieme dei polinomi associati a r_1; come vedremo nelle prossime sezioni questo è l'insieme di tutti i polinomi della forma cr_1 dove c è un numero razionale diverso da zero; tra questi massimi comuni divisori ne esiste dunque esattamente uno monico, precisamente $(4/7)r_1 = x^3 + 1$.

Come stabilito dal teorema di Bézout, possiamo scrivere r_1 nella forma $uf + gv$ per opportuni $u, v \in \mathbb{Q}[x]$. Possiamo calcolare una tale coppia (u, v) (ma sappiamo che ne esistono infinite) in questo modo: da $g = q_1 \cdot r + r_1$ segue $r_1 = g - q_1 r$; inoltre da $f = 2g + r$ segue $r = f - 2g$. Sostituendo questa espressione per r nell'uguaglianza precedente abbiamo $r_1 = g - q_1(f - 2g) = (-q_1)f + (1 + 2q_1)g$. Dunque, ponendo $u = -q_1 = (1/2)x - 1/4$ e $v = 1 + 2q_1 = -x + 3/2$, l'uguaglianza $r_1 = uf + gv$ è soddisfatta.

È bene tenere presente che l'algoritmo euclideo non può essere sempre utilizzato (almeno, non senza modifiche) per polinomi su anelli che non siano campi, come, ad esempio, in $\mathbb{Z}[x]$. Questo perché in questo caso non è sempre possibile effettuare la divisione tra polinomi non nulli; ad esempio, in $\mathbb{Z}[x]$ non si può dividere $2x^4 - 1$ per $3x^2 + 1$ (perché?). È possibile (ma non lo facciamo qui) verificare che *il teorema di Bézout non vale nell'anello* $\mathbb{Z}[x]$, dunque è essenziale, nel suo enunciato, richiedere che K sia un campo.

5. Applicazioni polinomiali e radici

Sia $f \in A[x]$, dove A è un anello commutativo unitario. Ricordiamo che se $f = \sum_{i=0}^{n} a_i x^i$ e $c \in A$ con $f(c)$ si indica l'elemento $\sum_{i=0}^{n} a_i c^i$ di A. L'applicazione

$$\tilde{f} \colon c \in A \longmapsto f(c) \in A$$

si chiama *applicazione polinomiale* determinata da f in A. A differenza dell'omomorfismo di sostituzione, definito nella Sezione 2, quest'applicazione non è, in generale, un omomorfismo. Osserviamo che se $f \in A$ allora $f(c) = f$ per ogni $c \in A$, quindi l'applicazione $\tilde{f}$ è costante. È per questo motivo che gli elementi di A vengono chiamati polinomi costanti (ma, attenzione!, è possibile che l'applicazione polinomiale $\tilde{f}$ sia costante anche in casi in cui il polinomio f non è costante; vedremo più avanti qualche esempio di questo tipo).

Sampre nelle stesse notazioni, diciamo che c è una *radice* di f se e solo se $f(c) = 0_A$.

Lemma 10. *Siano A un anello commutativo unitario e $f, g \in A[x]$. Allora:*

(i) *se, in $A[x]$, f divide g, ogni radice di f in A è radice di g;*
(ii) *se, in $A[x]$, f e g sono associati, f e g hanno le stesse radici in A;*
(iii) *se A è un dominio di integrità, allora le radici di fg in A sono tutti e soli gli elementi di A che sono radici di f o di g.*

Dimostrazione. (i): se $f|_{A[x]}\, g$, esiste $h \in A[x]$ tale che $g = fh$. Allora, applicando l'omomorfismo di sostituzione definito da g, abbiamo $g(c) = f(c)h(c) = 0_A h(c) = 0_A$, dunque c è radice di f.[(14)]

(ii) segue subito da (i): se f e g sono associati, f divide g e g divide f, quindi le radici di f sono radici di g e viceversa.

(iii): Per la (i), gli elementi di A che sono radici di f o di g sono radici anche di fg, multiplo di entrambi. Viceversa, se c è una radice in A di fg, allora $0_A = (fg)(c) = f(c)g(c)$. Poiché, per la Proposizione 5, $A[x]$ è un dominio di integrità, questo implica che uno tra $f(c)$ e $g(c)$ è 0_A, quindi c è radice di uno tra f e g. □

Esistono algoritmi che utilizzano questo semplice risultato per calcolare in modo efficiente valori di applicazioni polinomiali:

Teorema 11 (Teorema del resto)**.** *Sia A un anello commutativo unitario e siano $f \in A[x]$ e $c \in A$. Allora $f(c)$ è il resto della divisione di f per $x - c$.*

Dimostrazione. La prima cosa da osservare è che si può certamente effettuare la divisione di f per $x - c$, perché quest'ultimo polinomio è monico, quindi il suo coefficiente direttore è invertibile. Effettuata questa divisione, otteniamo $q, r \in A[x]$ tali che $f = (x - c)q + r$ e $\nu r < \nu(x - c) = 1$. Quest'ultima condizione equivale a dire che r è un polinomio costante, quindi $r(c) = r$. Applichiamo l'omomorfismo di sostituzione: $f(c) = \big((x - c)q + r\big)(c) = (c - c)q(c) + r(c) = 0_A q(c) + r = r$. È così provato che $f(c) = r$. □

Dal teorema del resto si ottiene immediatamente:

Teorema 12 (Teorema di Ruffini)**.** *Sia A un anello commutativo unitario e siano $f \in A[x]$ e $c \in A$. Allora c è una radice di f se e solo se $x - c$ divide f in $A[x]$.*

Dimostrazione. Per il teorema del resto, c è radice di f se e solo se il resto della divisione di f per $x - c$ è zero, cioè se e solo se $x - c$ divide f. □

Ad esempio, una conseguenza del teorema di Ruffini è:

Corollario 13. *Sia A un anello commutativo unitario e siano $f, g \in A[x]$ e $c \in A$. Supponiamo che f e g abbiano in $A[x]$ un massimo comun divisore d. Allora le radici comuni a f e g in A sono tutte e solo le radici di d in A: $\{c \in A \mid f(c) = 0_A = g(c)\} = \{c \in A \mid d(c) = 0_A\}$.*

Dimostrazione. Sia $c \in A$. Per il teorema di Ruffini, dire che c è radice di f e di g equivale a dire che $x - c$ è un divisore comune ad f e g. Per la definizione di massimo comun divisore, ciò equivale a dire che $x - c$ divide d, quindi, ancora per il teorema di Ruffini, a dire che c è radice di d. □

Per polinomi su domini di integrità vale una versione più generale del teorema di Ruffini:

Teorema 14 (Teorema di Ruffini generalizzato)**.** *Sia A un dominio di integrità unitario e siano $f \in A[x]$, $n \in \mathbb{N}^*$ e $c_1, c_2, \dots, c_n$ elementi di A a due a due distinti. Allora si ha che ciascuno degli elementi c_i è radice di f se e solo se $\prod_{i=1}^n (x - c_i)$ divide f in $A[x]$.*

Dimostrazione. Una delle due implicazioni è ovvia: se $\prod_{i=1}^n (x - c_i)$ divide f allora ciascuno degli elementi c_i è radice di f, in quanto $x - c_i$ divide f. Dimostriamo l'implicazione inversa per induzione su n. Supponiamo che gli elementi $c_1, c_2, \dots, c_n$ siano tutti radici di f. Se $n = 1$ allora $\prod_{i=1}^n (x - c_i) = x - c_1$ divide f per il teorema di Ruffini. Supponiamo allora $n > 1$ e, come ipotesi di induzione, che l'enunciato valga per insiemi di $n - 1$ elementi (distinti) di A ed arbitrari polinomi in $A[x]$. Poiché $f(c_n) = 0_A$, per il teorema di Ruffini esiste $q \in A[x]$ tale che $f = (x - c_n)q$. Sia ora i un intero tale che $1 \le i < n$. Poiché c_i è radice di f e A è un dominio di integrità, segue dal Lemma 10 (iii) che c_i è radice di uno tra $x - c_n$ e q. Ma $c_i \neq c_n$, per ipotesi, dunque $(x - c_n)(c_i) = c_i - c_n \neq 0_A$; allora c_i non è radice di $x - c_n$ e così c_i è radice di q. Dunque ciascuno degli elementi $c_1, c_2, \dots, c_{n-1}$ è radice di q. Possiamo allora applicare l'ipotesi di induzione e concludere che $\prod_{i=1}^{n-1} (x - c_i)$ divide q, quindi esiste $h \in A[x]$ tale che $q = h \prod_{i=1}^{n-1} (x - c_i)$. Allora $f = q \cdot (x - c_n) = h\big(\prod_{i=1}^{n-1} (x - c_i)\big) \cdot (x - c_n) = h \prod_{i=1}^{n} (x - c_i)$. Pertanto $\prod_{i=1}^n (x - c_i)$ divide f; la dimostrazione è così completa. □

[(14)] in alternativa, si potrebbe dedurre la (i) dal teorema di Ruffini. Come?

Il teorema di Ruffini generalizzato ha due importantissime conseguenze. La prima è una limitazione al numero di radici che un polinomio non nullo su un dominio di integrità può avere.

Teorema 15. *Sia A un dominio di integrità unitario e sia $0_A \neq f \in A[x]$. Allora il numero delle radici di f in A non supera νf.*

Dimostrazione. Se f ha esattamente n radici, siano esse $c_1, c_2, \dots, c_n$, allora f è multiplo di $g := \prod_{i=1}^{n}(x - c_i)$, per il teorema di Ruffini generalizzato, quindi $f = gq$ per opportuno $q \in A[x]$. Essendo $f \neq 0_A$ si ha anche $q \neq 0_A$. Ma $\nu g = n$ e per g e q vale la regola di addizione dei gradi (perché A è un dominio di integrità, o, in alternativa, perché g è monico, quindi ha coefficiente direttore invertibile). Quindi $\nu f = \nu g + \nu q = n + \nu q \geq n$. □

Sia per il teorema di Ruffini generalizzato che per il Teorema 15 è essenziale l'ipotesi che A sia un dominio di integrità. Consideriamo, ad esempio, il polinomio $f = \bar{2}x \in \mathbb{Z}_6[x]$. Sia $[0]_6$ che $[3]_6$ sono radici di f, quindi f ha più radici in $\mathbb{Z}_6$ di quanto sia il suo grado, che è 1. Come imposto dal teorema di Ruffini sia $x = x - [0]_6$ che $x - [3]_6$ dividono f (infatti $f = x \cdot [2]_6 = (x - [3]_6) \cdot [2]_6$), ma $x(x - [3]_6)$ non divide f, quindi la conclusione del teorema di Ruffini generalizzato non vale per f.

L'altra conseguenza del teorema di Ruffini generalizzato riguarda le applicazioni polinomiali e ci dice che nel caso dei domini di integrità infiniti ogni polinomio è identificato univocamente dalla sua applicazione polinomiale.

Teorema 16 (Principio di identità dei polinomi)**.** *Sia A un dominio di integrità infinito. Allora, per ogni $f, g \in A[x]$ si ha: $\tilde{f} = \tilde{g} \iff f = g$.*

Dimostrazione. Ovviamente $\tilde{f} = \tilde{g}$ se $f = g$. Supponiamo, viceversa, $\tilde{f} = \tilde{g}$. Allora $f(c) = g(c)$ per ogni $c \in A$. Sia $h = f - g$. Allora per ogni $c \in A$ abbiamo $h(c) = (f - g)(c) = f(c) - g(c) = 0_A$, vale a dire: ogni elemento di A è radice di h. Dunque h ha un numero infinito di radici. Ma il Teorema 15 assicura che se $h \neq 0_A$ allora il numero delle radici di h non supera νh, quindi è finito. Di conseguenza deve essere $h = 0_A$, vale a dire: $f = g$. □

È a causa del principio di identità dei polinomi che in alcuni casi vengono identificati i polinomi con le applicazioni polinomiali. Ad esempio, nei corsi di analisi matematica si definiscono i polinomi come particolari funzioni da $\mathbb{R}$ a $\mathbb{R}$, quelle che per noi sono le applicazioni polinomiali definite dai polinomi in $\mathbb{R}[x]$. Questo è lecito perché, essendo $\mathbb{R}$ un campo (quindi un dominio di integrità) infinito, il principio di identità dei polinomi assicura che i polinomi in $\mathbb{R}[x]$ corrispondono esattamente alle loro applicazioni polinomiali (in corsi di analisi più avanzati i polinomi sono definiti con riferimento al campo complesso, anziché a quello reale; il discorso è analogo: anche per il campo complesso vale il principio di identità dei polinomi). D'altra parte, non è lecito identificare polinomi ed applicazioni polinomiali in contesti in cui non valga il principio di identità dei polinomi, cioè quando l'anello A considerato sia finito oppure non sia integro.

Nel caso degli anelli finiti è certo che il principio di identità dei polinomi non può valere. Infatti, se A è un anello commutativo unitario finito, il numero delle applicazioni da A ad A, e quindi il numero delle applicazioni polinomiali in A, è finito, mentre $A[x]$ è comunque infinito. Dunque, in questo caso, è impossibile che ci sia una corrispondenza biunivoca tra polinomi e applicazioni polinomiali (ciò che il principio di identità dei polinomi afferma è che, se A è un dominio di integrità infinito, l'applicazione $f \in A[x] \mapsto \tilde{f} \in \mathrm{Map}(A, A)$ è iniettiva; ciò è impossibile nel caso che stiamo considerando ora, in cui il dominio $A[x]$ è infinito ma il codominio $\mathrm{Map}(A, A)$ è finito). Possiamo fare esempi più espliciti: il polinomio $x(x - \bar{1})(x - \bar{2}) = x^3 - x \in \mathbb{Z}_3[x]$ ha tutti gli elementi del campo $\mathbb{Z}_3$ come radici, questo significa che $\tilde{f}$ è l'applicazione costante $c \in \mathbb{Z}_3 \mapsto \bar{0} \in \mathbb{Z}_3$, ma allora $\tilde{f}$ coincide con l'applicazione polinomiale $\tilde{0}_{\mathbb{Z}_3}$ definita dal polinomio nullo, pur essendo $f \neq 0_{\mathbb{Z}_3}$. Più in generale, se se F è un campo finito, di cardinalità q, il polinomio $f = \prod_{c \in F}(x - c)$ ha grado q ed ha tutti gli elementi di F come radici, quindi $\tilde{f} = \tilde{0}_F$. È possibile dimostrare che due polinomi in $F[x]$ definiscono la stessa applicazione polinomiale se e solo se la loro differenza è un multiplo di questo polinomio f.

Anche nel caso degli anelli infiniti, che però non siano integri, il principio di identità dei polinomi può non valere. Ad esempio, se A è un anello booleano e $f = x^2 - x \in A[x]$ allora, poiché ogni elemento c di A è idempotente e quindi verifica $c^2 - c = 0_A$, ovvero $f(c) = 0_A$, tutti gli elementi di A sono radici di f. Allora $\tilde{f} = \tilde{0}_A$, anche se $f \neq 0_A$. Nel caso in cui A sia infinito, f è un esempio di polinomio di secondo grado con infinite radici.

6. Fattorizzazione

Ricordiamo che un monoide commutativo cancellativo (cioè ad elementi tutti cancellabili) si dice *fattoriale* se e solo se ogni suo elemento non invertibile è prodotto di elementi irriducibili e tali decomposizioni in irriducibili sono essenzialmente uniche.[15] Se A è un dominio di integrità unitario, allora $A^{\#} := A \setminus \{0_A\}$ è chiuso rispetto

[15] quest'ultima frase vuol dire che se $r, s \in \mathbb{N}^*$ e $p_1, p_2, \dots, p_r, q_1, q_2, \dots, q_s$ sono elementi irriducibili tali che $p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ allora $r = s$ ed esiste una permutazione $\sigma \in \mathbb{S}_r$ tale che, per ogni $i \in \{1, 2, \dots, r\}$ gli elementi p_i e q_{i^σ} siano associati. Detto in modo più facile (ma più ambiguo): il numero dei fattori nei prodotti $p_1 p_2 \cdots p_r$ e $q_1 q_2 \cdots q_s$ è lo stesso, ed i fattori nel secondo prodotto possono essere riordinati in modo che fattori corrispondenti nei due prodotti (p_1 con q_1, p_2 con q_2 etc.) siano associati tra loro. Già che ci siamo, ricordiamo anche che un elemento p si dice *irriducibile* se e solo se non è invertibile ed i suoi unici divisori sono quelli banali, cioè gli elementi invertibili e quelli associati a p. Un elemento non invertibile né irriducibile è invece *riducibile*. Due elementi a e b di un monoide commutativo S sono, per definizione, *associati* se e solo se a divide b e b divide a (in S); se poi S è anche un cancellativo si dimostra che a e b sono associati in S se e solo se $b = au$ per un opportuno elemento invertibile u di S. In ogni caso, la relazione 'essere elementi associati' è di equivalenza in S ed elementi tra loro associati hanno esattamente gli stessi divisori e gli stessi multipli.

alla moltiplicazione (questa affermazione è esattamente la legge di annullamento del prodotto: il prodotto tra due elementi di A diversi da zero è diverso da zero), quindi, con la moltiplicazione indotta da quella dell'anello, $A^\#$ è un monoide, cancellativo perché sono cancellabili in A tutti i suoi elementi. Si dice che A è un *anello fattoriale* se e solo se questo monoide $A^\#$ è fattoriale. Il motivo per cui questa nozione è importante nello studio degli anelli di polinomi è il seguente teorema, che non dimostreremo:

Teorema 17. *Se A è un anello fattoriale allora $A[x]$ è fattoriale.*

Ora, sono certamente fattoriali i campi ed è fattoriale, per il Teorema Fondamentale dell'Aritmetica, l'anello $\mathbb{Z}$ degli interi. Quindi è fattoriale $\mathbb{Z}[x]$ e, per ogni campo K, anche $K[x]$ (che, come già osservato, non può essere un campo). Dunque, sia per i polinomi a coefficienti in $\mathbb{Z}$ che per quelli a coefficienti in un campo vale un teorema di fattorizzazione essenzialmente unica in prodotto di polinomi irriducibili: ogni polinomio non invertibile e non nullo è prodotto di polinomi irriducibili e tale fattorizzazione è unica a meno dell'ordine dei fattori e della sostituzione di alcuni fattori con polinomi associati.

Nell'ipotesi che A sia fattoriale, una delle conseguenze del fatto che $A[x]$ è fattoriale è che (in analogia con ciò che accade in $\mathbb{Z}$), nota una fattorizzazione in prodotto di irriducibili di un polinomio f è facile determinare l'insieme dei divisori di f. Diamo un rapido cenno, tutto funziona come nell'aritmetica in $\mathbb{Z}$: posto $f = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_n^{\lambda_n}$, dove ciascuno dei polinomi p_i è irriducibile, se $i \neq j$ allora p_i e p_j non sono associati e $\lambda_i \in \mathbb{N}$ per ogni i, i divisori di f sono tutti e soli i polinomi della forma $p_1^{\sigma_1} p_2^{\sigma_2} \cdots p_n^{\sigma_n}$ ed i loro associati, dove, per ogni i, valga $\sigma_i \in \mathbb{N}$ e $\sigma_i \leq \lambda_i$. Usando questa osservazione è possibile anche notare che, scelti comunque $f, g \in A[x]$, esistono un massimo comun divisore d ed un minimo comune multiplo m tra f e g, e dm è associato a fg. Infatti, escluso il caso banale in cui uno tra f e g è il polinomio nullo, f e g si possono fattorizzare nella forma $f = up_1^{\lambda_1} p_2^{\lambda_2} \cdots p_n^{\lambda_n}$ e $g = vp_1^{\mu_1} p_2^{\mu_2} \cdots p_n^{\mu_n}$, dove, come sopra i p_i sono irriducibili a due a due non associati, $u, v \in \mathcal{U}(A[x]) = \mathcal{U}(A)$ e $\lambda_i, \mu_i \in \mathbb{N}$ per ogni i (notare che non è escluso che alcuni dei λ_i o μ_i siano 0). Si verifica allora che, ponendo $\sigma_i = \min\{\lambda_i, \mu_i\}$ e $\tau_i = \max\{\lambda_i, \mu_i\}$ per ogni i, si ha che $d := p_1^{\sigma_1} p_2^{\sigma_2} \cdots p_n^{\sigma_n}$ è un massimo comun divisore e $m := p_1^{\tau_1} p_2^{\tau_2} \cdots p_n^{\tau_n}$ è un minimo comune multiplo tra f e g; inoltre dm è associato a fg perché $\sigma_i + \tau_i = \lambda_i + \mu_i$ per ogni i, quindi $fg = uvdm$.

Nella pratica, è spesso molto più difficile calcolare una fattorizzazione in irriducibili di un polinomio che eseguire l'algoritmo euclideo, quindi risulta in genere conveniente questo secondo metodo quando si ricerca un massimo comun divisore tra due polinomi. È bene però notare che la discussione appena svolta mostra che anche nei casi in cui l'algoritmo euclideo non si può eseguire, come ad esempio in $\mathbb{Z}[x]$, la fattorialità garantisce comunque l'esistenza di un massimo comun divisore e di un minimo comune multiplo tra due polinomi.

Passiamo ora a discutere in maggior dettaglio le fattorizzazioni in polinomi irriducibili. Iniziamo a stabilire: quando è che due polinomi sono associati? Se A è un dominio di integrità unitario e $f \in A[x]$, i polinomi associati ad f sono tutti e soli quelli della forma uf, dove u è un polinomio invertibile in $A[x]$.[16] Come sappiamo (Proposizione 5), $\mathcal{U}(A[x]) = \mathcal{U}(A)$, quindi i polinomi associati ad f sono tutti e soli i polinomi della forma uf, dove u è un invertibile di A. In questo caso, quindi, *polinomi (non nulli) associati hanno necessariamente lo stesso grado*. Ad esempio, poiché $\mathcal{U}(\mathbb{Z}) = \{1, -1\}$, gli associati in $\mathbb{Z}[x]$ di un $f \in \mathbb{Z}[x]$ sono f stesso (cioè $1f$) e $-f$ (cioè $(-1)f$). Se invece K è un campo $\mathcal{U}(K[x]) = \mathcal{U}(K) = K^\# := K \setminus \{0_K\}$, quindi, l'insieme di tutti i polinomi associati ad un $f \in K[x] \setminus \{0_K\}$ è $\{cf \mid 0_K \neq c \in K\}$. Se $a = \operatorname{cd} f$ si ha $\operatorname{cd}(cf) = ca$ per ogni $c \in K^\#$. Allora, qualunque sia $k \in K^\#$, il nostro polinomio f ha esattamente un associato con coefficiente direttore k, precisamente $(ka^{-1})f$ (infatti, per ogni $c \in K^\#$, abbiamo che $\operatorname{cd}(cf) = ca = k$ se e solo se $c = ka^{-1}$). Il caso più importante è quello in cui scegliamo $k = 1_K$. In questo caso ciò che otteniamo è che f ha un unico associato con coefficiente direttore 1_K, ovvero monico, precisamente $a^{-1}f$. Otteniamo così:

Proposizione 18. *Sia K un campo. In ogni classe di elementi associati di polinomi non nulli in $K[x]$ esiste uno ed un solo polinomio monico.*

Ci riferiamo a questo polinomio come al *rappresentante monico* della classe. A titolo di esempio, in $\mathbb{Q}[x]$ il polinomio monico associato a $f := 3x^2 + x - 6$ è $(1/3)f = x^2 + (1/3)x - 2$; ma anche $-6x^2 - 2x + 12$ e $(1/100)x^2 + (1/300)x - 1/50$ (e infiniti altri polinomi, tutti quelli della forma cf, dove $0 \neq c \in \mathbb{Q}$) sono associati a f. L'esistenza di un unico rappresentante monico in ogni classe di polinomi non nulli associati permette di esprimere le fattorizzazioni in irriducibili dei polinomi a coefficienti in un campo in una forma spesso più conveniente:

Proposizione 19. *Sia K un campo. Allora ogni polinomio non nullo in $K[x]$ è prodotto di un elemento di K e di polinomi monici irriducibili in $K[x]$. Tale fattorizzazione è unica a meno dell'ordine dei fattori.*

Dimostrazione. L'unicità della fattorizzazione segue dal fatto che $K[x]$ è fattoriale e dal fatto che ogni classe di polinomi associati non nulli contiene un solo rappresentante monico. L'esistenza della decomposizione è ovvia nel caso dei polinomi costanti, va provata per polinomi non costanti. Sia, allora, $f \in K[x] \setminus K$. Sia $f = p_1 p_2 \cdots p_n$ una fattorizzazione di f in prodotto di polinomi irriducibili. Per ogni $i \in \{1, 2, \ldots, n\}$ sia $a_i = \operatorname{cd}(p_i)$; allora $p_i = a_i q_i$, dove $q_i = a_i^{-1} p_i$ è associato a p_i (quindi è irriducibile) ed è monico. Posto $a = a_1 a_2 \cdots a_n$ abbiamo $f = a q_1 q_2 \cdots q_n$; questa è la decomposizione cercata. □

Si noti che, nella fattorizzazione appena descritta, $a = \operatorname{cd} f$.

[16] questo è vero se $f \neq 0_A$, perché in questo caso f è cancellabile, ma è anche banalmente vero se $f = 0_A$.

Ci vogliamo ora occupare di descrivere, per quanto possibile, la proprietà di essere o meno irriducibile per un polinomio a coefficienti in un campo. Vedremo in che modo questo proprietà è collegata alla presenza di radici. Iniziamo con una importante caratterizzazione, che, quando la trattazione è limitata ad anelli di polinomi su campi, è talvolta utilizzata per definire la nozione di polinomio irriducibile. Va tenuto ben presente che, come vedremo, questo teorema non si applica a polinomi su anelli che non siano campi.

Teorema 20. *Siano K un campo e $f \in K[x]$. Se $n = \nu f$ allora f è irriducibile in $K[x]$ se e solo se $n > 0$ e vale una delle due proprietà equivalenti:*

(a) *non esistono $g, h \in K[x]$ tali che $f = gh$ e sia g che h abbiano grado minore di n;*
(b) *non esistono $g, h \in K[x]$ tali che $f = gh$ e sia g che h abbiano grado maggiore di 0.*

Dimostrazione. Ricordiamo che f è irriducibile se e solo se, in $K[x]$, non è invertibile e non ha divisori se non quelli banali. Possiamo subito osservare che i polinomi costanti non sono irriducibili. Infatti i polinomi costanti non nulli sono invertibili per la Proposizione 5, mentre il polinomio nullo ha tutti gli elementi di $K[x] \smallsetminus K$ come divisori non banali. Abbiamo così che l'asserto è corretto nel caso in cui f sia costante: f non è irriducibile e non è vero che $n = \nu f > 0$, quindi la condizione all'enunciato non è soddisfatta. Possiamo allora assumere $f \notin K$, cioè: $n > 0$. Supponiamo dunque $n > 0$. Osserviamo che, se $g, h \in K[x]$ e $f = gh$, per la regola di addizione dei gradi (che vale perché K è un campo) si ha $\nu g + \nu h = \nu f = n$, quindi $(\nu g < n \wedge \nu h < n) \iff (\nu g > 0 \wedge \nu h > 0)$, vale a dire: (a) e (b) sono equivalenti. Se f è irriducibile, scelti comunque $g, h \in K[x]$ tali che $f = gh$, allora g è un divisore di f, quindi un divisore banale perché f è irriducibile. Allora o g è invertibile, nel qual caso $g \in K \smallsetminus \{0_K\}$ e $\nu g = 0$, oppure g è associato a f, nel qual caso $\nu g = \nu f = n$. Ciò mostra che, se f è irriducibile, sono verificate (a) e (b). Se, invece, f non è irriducibile, f ha un divisore non banale g; allora $g \neq 0_K$ (altrimenti $f = 0_K$) e g non è invertibile, quindi $\nu g > 0$, ed esiste $h \in K[x]$ tale che $f = gh$. Ovviamente $h \neq 0_K$, e h non è invertibile perché g non è associato ad f, quindi abbiamo anche $\nu h > 0$. In questo caso, dunque, non vale (b), e quindi neanche (a). □

Un'ovvia conseguenza di questa caratterizzazione è che *i polinomi di primo grado a coefficienti in un campo K sono certamente irriducibili in $K[x]$*, dal momento che i prodotti tra polinomi di grado minore di 1 sono certamente costanti.

Se, ancora, K è un campo, ogni polinomio di primo grado $ax+b \in K[x]$ ha una radice in K (precisamente $-a^{-1}b$: essendo il polinomio di grado 1 si ha $a \neq 0_K$ quindi ha senso considerare a^{-1}), dunque un polinomio f che sia divisibile per un polinomio di primo grado ha almeno una radice in K, per il Lemma 10. Viceversa, se f ha una radice allora f ha un divisore di primo grado, per il teorema di Ruffini. Dunque:

Proposizione 21. *Sia K un campo e sia $f \in K[x]$. Allora f ha radici in K se e solo se ha almeno un divisore di primo grado in $K[x]$.*

Siccome una della due implicazioni, quella stabilita dal teorema di Ruffini, vale per polinomi su anelli commutativi unitari qualsiasi, possiamo anche osservare:

Proposizione 22. *Sia A un dominio di integrità unitario e sia $f \in A[x]$. Se $\nu f > 1$ e f ha radici in A, allora f è riducibile in $A[x]$.*

Dimostrazione. Per il teorema di Ruffini, f ha un divisore h di primo grado. Allora h non è invertibile (per la Proposizione 5) e poiché, come già osservato, due polinomi in $A[x]$ che siano associati devono avere lo stesso grado, mentre $\nu h = 1 < \nu f$, allora h non è associato a f. Pertanto h è un divisore non banale di f, quindi f non è irriducibile. □

In un caso molto particolare, ma importante, vale anche il viceversa:

Proposizione 23. *Siano K un campo e f un polinomio in $K[x]$ di grado 2 o 3. Allora f è irriducibile in $K[x]$ se e solo se è privo di radici in K.*

Dimostrazione. Poiché $\nu f > 0$, certamente f non è invertibile. Se f è irriducibile allora è privo di radici, per la Proposizione 22. Viceversa, se f è riducibile allora per il Teorema 20 dobbiamo avere $f = gh$ per opportuni $g, h \in K[x]$ tali che $\nu g, \nu h < \nu f$, e naturalmente $\nu g + \nu h = \nu f$. Se $\nu f = 2$ abbiamo una sola possibilità: $\nu g = \nu h = 1$; se $\nu f = 3$ abbiamo invece due casi possibili: $\nu g = 1$ e $\nu h = 2$ oppure, viceversa, $\nu g = 2$ e $\nu h = 1$. In tutti e tre i casi, comunque, f ha un divisore di grado 1, quindi una radice. Con questo l'enunciato è dimostrato. □

Possiamo schematizzare come segue le informazioni ottenute sulle proprietà di un polinomio a coefficienti in un campo di essere o meno irriducibile ed di avere o meno radici.

Se K è un campo e $0_K \neq f \in K[x]$, posto $n = \nu f$ si ha:

$n = 0$	$\implies$	f è invertibile e privo di radici
$n = 1$	$\implies$	f è irriducibile ed ha una radice
$n \in \{2, 3\}$	$\implies$	(f è irriducibile $\iff$ f non ha radici)
$n > 3$	$\implies$	(f è irriducibile $\implies$ f non ha radici)

(Ovviamente qui per 'irriducibile' si intente 'irriducibile in $K[x]$' e per 'radice' si intende 'radice in K').

Osserviamo che l'implicazione all'ultimo rigo di questa tabella, in generale, non si inverte. Ad esempio, un polinomio di grado 4 può essere il prodotto di due polinomi irriducibili di grado 2; in questo caso il polinomio è riducibile (ovviamente ...) ma privo di radici (perché privo di divisori di primo grado; oppure per questo motivo: una radice dovrebbe necessariamente essere radice di uno dei fattori di grado due, ma essendo irriducibili questi sono privi di radici). Un esempio di questo tipo è il polinomio $(x^2+1)(x^2+2)$ in $\mathbb{Q}[x]$.

Non va poi dimenticato che tutti questi risultati valgono nel caso dei polinomi a coefficienti in un campo, ma (ad eccezione della Proposizione 22) non in casi più generali. Ad esempio, in $\mathbb{Z}[x]$ il polinomio (costante) 2 è irriducibile (non invertibile!) in $\mathbb{Z}[x]$, pur avendo grado 0; il polinomio $2x$, che è irriducibile in $\mathbb{Q}[x]$ perché $\mathbb{Q}$ è un campo e $\nu(2x)=1$, è invece riducibile in $\mathbb{Z}[x]$, perché è diviso da 2 che, in $\mathbb{Z}[x]$ non è invertibile né associato a $2x$, quindi è un divisore non banale di $2x$. Come si vede, la differenza sta nel fatto che 2 è invertibile in $\mathbb{Q}[x]$ ma non in $\mathbb{Z}[x]$. Inoltre, in $\mathbb{Z}[x]$ il polinomio di primo grado $2x+1$ è privo di radici, quindi anche la Proposizione 21 non vale per arbitrari polinomi su $\mathbb{Z}$.

7. Metodi ed esempi di fattorizzazione per polinomi su un campo

Supponiamo di voler fattorizzare un polinomio (in un fissato anello di polinomi) in prodotto di polinomi irriducibili. Per farlo abbiamo bisogno:

- di saper trovare divisori non banali dei polinomio dato, se ne esistono;
- di saper riconoscere quali tra questi divisori sono irriducibili.

Limitiamoci al caso dei polinomi su un campo. Usando la tabella nella sezione precedente, sappiamo, in linea di massima, rispondere al secondo punto nel caso di divisori di grado minore di quattro. I polinomi di grado uno sono sempre irriducibili, quelli di grado due o tre lo sono se e solo se sono privi di radici. In due casi notevoli queste informazioni sono addirittura più di quanto non sia necessario. Infatti valgono questi teoremi (che non dimostriamo) per polinomi in $\mathbb{C}[x]$ ed in $\mathbb{R}[x]$ (come di consueto, $\mathbb{C}$ indica il campo dei numeri complessi ed $\mathbb{R}$ il campo dei numeri reali).

Teorema 24. *Ogni polinomio non costante in $\mathbb{C}[x]$ ha qualche radice in $\mathbb{C}$. Di conseguenza, gli unici polinomi irriducibili in $\mathbb{C}[x]$ sono quelli di grado uno.*

Teorema 25. *Ogni polinomio irriducibile in $\mathbb{R}[x]$ ha grado minore di 3.*

Dunque, i polinomi irriducibili in $\mathbb{R}[x]$ sono precisamente quelli di grado 1 e quelli di grado 2 privi di radici. Come è noto dalle scuole superiori, un polinomio $ax^2+bx+c \in \mathbb{R}[x]$ di grado 2 ha radici in $\mathbb{R}$ se e solo se $b^2-4ac \geq 0$. Dunque, è molto facile riconoscere se un polinomio in $\mathbb{C}[x]$ o in $\mathbb{R}[x]$ è irriducibile. A proposito dei polinomi in $\mathbb{R}[x]$ vale anche questo risultato, che si può provare con metodi elementari dell'analisi (è una conseguenza del teorema di Bolzano):

Teorema 26. *Ogni polinomio di grado dispari in $\mathbb{R}[x]$ ha qualche radice in $\mathbb{R}$.*

Osserviamo che quest'ultimo teorema di potrebbe anche dedurre dal precedente, se si supponesse di aver dimostrato quello. Infatti, se f è un polinomio di grado dispari in $\mathbb{R}[x]$ e $f=p_1p_2\cdots p_r$ è una sua fattorizzazione in prodotto di polinomi irriducibili in $\mathbb{R}[x]$, allora, dal momento che ciascuno dei polinomi p_i ha grado 1 o 2, ma non tutti possono avere grado 2, altrimenti $\nu f = \sum_{i=1}^{r} \nu(p_i)$ sarebbe $2r$, che è pari, almeno uno dei fattori p_i deve avere grado 1, quindi f ha un divisore di primo grado e così ha una radice.

La situazione è molto più complessa (ed interessante) nel caso di polinomi in $\mathbb{Q}[x]$. Lo studio dei polinomi in $\mathbb{Q}[x]$ si può ridurre al caso dei polinomi a coefficienti interi. Infatti, se $f=a_0+a_1x+a_2x^2+\cdots+a_nx^n \in \mathbb{Q}[x]$, ciascuno dei coefficienti a_i sarà una frazione, che possiamo scrivere come $a_i=u_i/v_i$, dove $u_i, v_i \in \mathbb{Z}$ e $v_i \neq 0$. Se m è un multiplo comune a $v_0, v_1, \ldots, v_n$ e $m \neq 0$ allora $\bar{f} := mf \in \mathbb{Z}[x]$; poiché $m \in \mathcal{U}(\mathbb{Q}[x])$, inoltre, $\bar{f}$ è associato a f in $\mathbb{Q}[x]$. Pertanto:

Lemma 27. *Ogni polinomio $f \in \mathbb{Q}[x]$ è associato, in $\mathbb{Q}[x]$, ad un polinomio $\bar{f} \in \mathbb{Z}[x]$.*

Ora, polinomi tra loro associati hanno esattamente le stesse proprietà rispetto alla fattorizzazione. Ad esempio, i polinomi f e $\bar{f}$ di questo lemma hanno gli stessi divisori in $\mathbb{Q}[x]$, f è irriducibile in $\mathbb{Q}[x]$ se e solo se lo è $\bar{f}$, inoltre f e $\bar{f}$ hanno esattamente le stesse radici in $\mathbb{Q}$ (Lemma 10, ad esempio). In questo senso lo studio di $\bar{f}$ equivale allo studio di f. Bisogna però fare attenzione, ci stiamo riferendo a $\bar{f}$ riguardato come polinomio in $\mathbb{Q}[x]$. Detto diversamente, ci interessano le proprietà di fattorizzazione di $\bar{f}$ in $\mathbb{Q}[x]$, non in $\mathbb{Z}[x]$. Come sappiamo già da esempi visti in precedenza, anche per polinomi in $\mathbb{Z}[x]$ le proprietà di essere irriducibile in $\mathbb{Z}[x]$ o di essere irriducibile in $\mathbb{Q}[x]$ non sono equivalenti; $\bar{f}$ potrebbe essere irriducibile in $\mathbb{Q}[x]$ pur non essendolo in $\mathbb{Z}[x]$.

A differenza di quanto accade in $\mathbb{C}[x]$ ed in $\mathbb{R}[x]$, esistono in $\mathbb{Q}[x]$ polinomi irriducibili di grado arbitrariamente grande. Questo segue dal prossimo teorema, che fornisce un utile criterio sufficiente a dimostrare l'irriducibilità di alcuni polinomi.

Teorema 28 (Criterio di irriducibilità di Eisenstein)**.** *Sia $f=a_0+a_1x+a_2x^2+\cdots+a_nx^n \in \mathbb{Z}[x]$. Se esiste un primo p tale che:*

(1) *p divide $a_0, a_1, \ldots, a_{n-1}$,*

(2) *p non divide a_n,*
(3) *p^2 non divide a_0,*

allora f è irriducibile in $\mathbb{Q}[x]$.

Ad esempio, per ogni intero positivo n e per ogni primo p, il polinomio $x^n - p$ è irriducibile in $\mathbb{Q}[x]$. Infatti possiamo applicare il criterio di Eisenstein con il primo p: il coefficiente direttore del nostro polinomio, cioè 1, non è divisibile per p, ma tutti gli altri coefficienti lo sono, inoltre p^2 non divide il termine noto $-p$. Dunque le ipotesi del criterio sono soddisfatte e $x^n - p$ è irriducibile. Vediamo così che per ogni intero positivo n esistono in $\mathbb{Q}[x]$ polinomi irriducibili di grado n.

Altri esempi di polinomi la cui irriducibilità segue dal criterio di Eisenstein sono $3x^{10} - 15x^7 + 20x^5 + 5x^2 - 10$ (si può applicare il criterio ponendo $p = 5$) e $7x^4 + 6x^3 + 12x - 30$ (si può applicare il criterio ponendo $p = 2$ o anche ponendo $p = 3$). Naturalmente il fatto che non si possa applicare il criterio di Eisenstein ad un polinomio f non comporta affatto che f sia riducibile. Ad esempio, al polinomio $x^3 + 2x + 1$ non si può applicare il criterio di Eisenstein, perché nessun primo ne divide il termine noto, ma ciononostante questo polinomio è irriducibile in $\mathbb{Q}[x]$ (vedi più avanti l'Esempio 32, per una giustificazione di questo fatto).

Torniamo ora al primo dei due punti considerati all'inizio di questa sezione: in che modo possiamo cercare divisori di un polinomio? Il metodo più semplice, quando è applicabile, è quello fornito dal teorema di Ruffini. Se di un polinomio f conosciamo una radice c allora f è divisibile per $x - c$. Dividendo f per $x - c$ otteniamo un polinomio f_1 tale che $f = (x - c)f_1$. Se stiamo ricercando una fattorizzazione in irriducibili di f basterà allora trovare una fattorizzazione in irriducibili di f_1 ed aggiungere a questa il fattore $x-c$. Ad esempio, $f = x^3-1 \in \mathbb{Q}[x]$ ha chiaramente 1 come radice; possiamo allora dividere f per $x - 1$ ottenendo il quoziente $x^2 + x + 1$, allora $f = (x-1)(x^2+x+1)$. Poiché x^2+x+1 non ha radici in $\mathbb{Q}$ (non ne ha neanche in $\mathbb{R}$) ed ha grado due, x^2+x+1 è irriducibile in $\mathbb{Q}[x]$ per la Proposizione 23; dunque la fattorizzazione ottenuta è la fattorizzazione in irriducibili monici di f in $\mathbb{Q}[x]$.

La ricerca di radici (in $\mathbb{Q}$) di polinomi in $\mathbb{Q}[x]$ è semplificata enormemente da questo semplice risultato:

Proposizione 29. *Sia $f = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in \mathbb{Z}[x]$, con $a_n \neq 0$. Allora ogni radice di f in $\mathbb{Q}$ si scrive come frazione u/v, dove u e v sono interi coprimi, u divide a_0 e v divide a_n.*

Dimostrazione. Ogni numero razionale si può scrivere come frazione ridotta, quindi nella forma u/v, dove u e v sono interi coprimi (e $v \neq 0$). Se una tale frazione u/v è radice di f allora $0 = f(u/v) = \sum_{i=0}^{n} a_i(u/v)^i$. Moltiplicando per v^n otteniamo:

$$a_0v^n + a_1uv^{n-1} + a_2u^2v^{n-2} + \cdots + a_{n-2}u^{n-2}v^2 + a_{n-1}u^{n-1}v + a_nu^n = 0.$$

Ora, escluso (per il momento) il primo, tutti gli addendi a primo membro sono multipli di u. Ma, poiché la loro somma vale 0, il primo addendo a_0v^n è l'opposto della somma dei rimanenti: $a_0v^n = -\sum_{i=1}^{n} a_iu^iv^{n-i}$, quindi anch'esso è multiplo di u. Dunque u divide a_0v^n. Ma u è coprimo con v, quindi con v^n, dunque u divide a_0, come richiesto dall'enunciato. In modo analogo si dimostra che v divide a_n: nella somma considerata sopra, escluso l'ultimo addendo a_nu^n tutti gli altri sono multipli di v, ma a_nu^n è l'opposto della somma degli addendi rimanenti, quindi v divide a_nu^n e, dal momento che v e u^n sono coprimi, v divide a_n. □

Ricordiamo che ogni polinomio in $\mathbb{Q}[x]$ è associato (in $\mathbb{Q}[x]$) ad un polinomio in $\mathbb{Z}[x]$, che avrà le sue stesse radici (in $\mathbb{Q}$). Dunque, volendo ricercare le radici razionali (cioè in $\mathbb{Q}$) di un polinomio $f \in \mathbb{Q}[x]$ possiamo procedere in questo modo: sostituiamo innanzitutto il polinomio con un suo associato a coefficienti in $\mathbb{Z}$, di questo consideriamo il coefficiente direttore a_n ed il termine noto a_0; le radici di f andranno cercate tra le frazioni ridotte con numeratore divisore di a_0 e denominatore divisore di a_n. È chiaro che (escluso il caso, banalmente semplificabile, in cui $a_0 = 0$) esiste solo un numero finito di tali frazioni, possiamo allora verificare per ciascuna di esse se è o meno radice del nostro polinomio.

Esempio 30. Consideriamo il polinomio $f = x^4 - 4x^2 + (3/2)x + 3 \in \mathbb{Q}[x]$. Un suo associato a coefficienti interi è $2f = 2x^4 - 8x^2 + 3x + 6$, con coefficiente direttore 2 e termine noto 6. Le frazioni della forma u/v con u e v interi coprimi tali che u divida 6 e v divida 2 sono: $1 = 1/1$, $1/2$, 2, 3, $3/2$, 6 ed i loro opposti -1, $-1/2$, -2, -3, $-3/2$, -6. Per cercare tutte le radici razionali di f non dobbiamo fare altro che controllare quali di questi dodici numeri sono radici di f. Nel nostro caso la verifica diretta mostra che solo -2, tra questi dodici, è radice. Concludiamo che -2 è l'unica radice di f in $\mathbb{Q}[x]$. Possiamo proseguire lo studio di questo polinomio cercando di fattorizzarlo in prodotto di irriducibili. Usiamo il teorema di Ruffini; dividendo f per $x + 2$ (cioè $x - (-2)$) otteniamo $f = (x+2)(x^3 - 2x^2 + 3/2)$. Il secondo fattore f_1 di questo prodotto è associato a $2f_1 = 2x^3 - 4x^2 + 3$. Ora, applicando direttamente la Proposizione 29 concluderemmo che le radici di f_1 sono da cercare tra le frazioni ridotte della forma u/v dove $u, v \in \mathbb{Z}$, u divide 3 e v divide 2. In realtà non è necessario esaminare tutte queste frazioni (sono in tutto otto: 1, $1/2$, 3, $3/2$ ed i loro opposti), perché ogni radice di f_1 è anche radice di f e di tutte queste frazioni, tranne -2, sappiamo che non sono radici di f, quindi nemmeno di f_1. Dobbiamo allora esaminare solo -2; si ha $f_1(-2) = (-2)^3 - 2(-2)^2 + 3/2 \neq 0$, quindi -2 non è radice di f_1. Pertanto f_1 non ha radici in $\mathbb{Q}$; poiché $\nu f_1 = 3$ concludiamo, per la Proposizione 23, che f_1 è irriducibile in $\mathbb{Q}[x]$. Dunque una fattorizzazione (l'unica a meno dell'ordine) di f in prodotto di irriducibili monici in $\mathbb{Q}[x]$ è $f = (x + 2)(x^3 - 2x^2 + 3/2)$.

Una situazione in cui la Proposizione 29 è particolarmente utile è quella in cui il polinomio f che appare nell'enunciato è monico. In questo caso, infatti, il denominatore v di una radice u/v di f in $\mathbb{Q}$ deve dividere 1, quindi $v = 1$ o $v = -1$; ciò comporta che la radice u/v è un numero intero. Abbiamo allora:

Corollario 31. *Sia f un polinomio monico in $\mathbb{Z}[x]$. Allora ogni radice razionale di f è intera.*

Esempio 32. Poco fa abbiamo detto, ma non giustificato, che il polinomio $f = x^3 + 2x + 1$ è irriducibile in $\mathbb{Q}[x]$. Sappiamo che questa affermazione equivale al fatto che f (che ha grado 3) è privo di radici in $\mathbb{Q}$, per la Proposizione 23. In effetti, ogni (eventuale) radice razionale di f deve essere intera, per il Corollario 31, inoltre, ancora per la Proposizione 29, essa deve dividere il termine noto di f, che è 1. Dunque gli unici due numeri razionali che potrebbero essere radici di f sono i divisori interi di 1, cioè 1 e -1. Ma $f(1) = 4$ e $f(-1) = -2$, quindi nessuno di questi due numeri è radice di f e così f è privo di radici. Per questo motivo f è irriducibile in $\mathbb{Q}[x]$.

Un'altra applicazione del Corollario 31 ha a che fare con le radici dei numeri interi. Se $a \in \mathbb{N}$ e $n \in \mathbb{N}^*$, la radice n-esima di a, $\sqrt[n]{a}$, è un numero reale la cui n-esima potenza sia a (precisamente, l'unico tale numero, se n è dispari, quello non negativo se n è pari). Quindi $\sqrt[n]{a}$ è una radice del polinomio monico $x^n - a \in \mathbb{Z}[x]$. Le radici razionali di questo polinomio sono intere, quindi $\sqrt[n]{a}$ è o intera (ad esempio, se $n = 2$ e $a = 4$) oppure irrazionale. Questo è un modo per dimostrare che numeri come $\sqrt{2}$, $\sqrt{3}$ o $\sqrt[11]{37}$, che certamente non sono interi, sono irrazionali.

Esempio 33. Fattorizziamo in prodotti di invertibili e irriducibili in $\mathbb{Q}[x]$ i polinomi $f = 2x^5 - x^3 + 2x^2 - 1$ e $g = x^5 + x^4 + x^3 + x^2 + x + 1$ dell'Esempio 9. Sappiamo che un loro massimo comun divisore è $(7/4)(x^3 + 1)$, quindi $d = x^3 + 1$ è il loro massimo comun divisore monico. Per fattorizzare f, conviene iniziare con lo sfruttare questa informazione, che fornisce un divisore non banale, per l'appunto d, di f. Dividendo f per d abbiamo $f = df_1$, dove $f_1 = 2x^2 - 1$. Per fattorizzare in irriducibili f basta dunque fattorizzare separatamente d e f_1. Iniziamo con $d = x^3 + 1$; poiché ha grado 3 esso è irriducibile se e solo se non ha radici in $\mathbb{Q}$, per la Proposizione 23. La Proposizione 29 (ed il Corollario 31) ci dicono che le radici razionali di d sono intere e dividono 1, quindi le sole possibili radici razionali di d sono 1 e -1. Ora, $d(1) = 2$ e $d(-1) = 0$, quindi 1 non è radice di d, ma -1 lo è. Allora, per il teorema di Ruffini, d è divisibile per $x - (-1) = x + 1$. Si ha $d = (x+1)(x^2 - x + 1)$. Le radici razionali di $h = x^2 - x + 1$ sono radici di d, la cui unica radice razionale è -1; quindi -1 è l'unica possibile radice razionale di h in $\mathbb{Q}$. Ma -1 non è radice di h, infatti $h(-1) = 3$, quindi h non ha radici in $\mathbb{Q}$ ed è così irriducibile per la Proposizione 23. Ovviamente avremmo anche potuto osservare, in alternativa, che h non ha radici reali, quindi non ha radici razionali, perché il suo discriminante è $-3 < 0$. Abbiamo così la fattorizzazione di d in irriducibili monici: $d = (x + 1)(x^2 - x + 1)$. Passiamo ora a $f_1 = 2x^2 - 1 = 2(x^2 - 1/2)$. Le radici di f_1 in $\mathbb{R}$ sono $1/\sqrt{2}$ e $-1/\sqrt{2}$, che sono irrazionali (se $1/\sqrt{2}$ fosse razionale sarebbe razionale anche il suo reciproco $\sqrt{2}$, ma sappiamo che $\sqrt{2} \notin \mathbb{Q}$). Quindi f_1 non ha radici razionali e, essendo di secondo grado, è quindi irriducibile. Mettendo insieme le fattorizzazioni di d e di f_1 otteniamo così la fattorizzazione di f come prodotto di un invertibile (il suo coefficiente direttore 2) ed irriducibili monici: $f = 2(x + 1)(x^2 - x + 1)(x^2 - 1/2)$. Questa fattorizzazione è unica a meno dell'ordine dei fattori (vedi Proposizione 19).

Fattorizziamo ora g. Come per f, iniziamo col dividere g per il suo divisore non banale d, ottenendo $g = dg_1$, dove $g_1 = x^2 + x + 1$. Abbiamo già la fattorizzazione completa di d; non è difficile verificare che g_1 è irriducibile, perché ha secondo grado ed è privo di radici. Quest'ultimo fatto si può verificare o osservando che il discriminante di g è negativo (quindi g non ha radici in $\mathbb{R}$), oppure che, per la Proposizione 29, le radici razionali di g sono da cercare tra 1 e -1, ma queste non sono radici di g. La fattorizzazione di g in prodotto di polinomi irriducibili monici in $\mathbb{Q}[x]$ è quindi $g = (x + 1)(x^2 - x + 1)(x^2 + x + 1)$.

Possiamo anche fattorizzare f e g in $\mathbb{R}[x]$. Conviene partire dalle fattorizzazioni in invertibili e irriducibili ottenute in $\mathbb{Q}[x]$. Nella fattorizzazione $f = 2(x + 1)(x^2 - x + 1)(x^2 - 1/2)$ il fattore di primo grado $x + 1$ è ovviamente irriducibile in $\mathbb{R}[x]$, i due fattori di secondo grado sono irriducibili in $\mathbb{R}[x]$ se e solo se sono privi di radici reali. Come già detto, $h = x^2 - x + 1$ non ha radici reali, quindi h è irriducibile in $\mathbb{R}$, mentre $x^2 - 1/2$ ha due radici reali, $1/\sqrt{2} = 2/\sqrt{2}$ e $-1/\sqrt{2}$, quindi $x^2 - 1/2 = (x - 1/\sqrt{2})(x + 1/\sqrt{2})$ per il teorema di Ruffini generalizzato. I due fattori appena trovati hanno grado uno e quindi sono irriducibili in $\mathbb{R}[x]$. La fattorizzazione in un invertibile e irriducibili monici di f in $\mathbb{R}[x]$ è dunque $f = 2(x+1)(x^2 - x + 1)(x - 1/\sqrt{2})(x + 1/\sqrt{2})$. Invece, entrambi i fattori di secondo grado nella fattorizzazione $g = (x + 1)(x^2 - x + 1)(x^2 + x + 1)$ di g sono privi di radici reali, quindi irriducibili anche in $\mathbb{R}[x]$, pertanto la stessa fattorizzazione è la fattorizzazione di g in prodotto di irriducibili monici in $\mathbb{R}[x]$.

A proposito del'uso del teorema di Ruffini per ottenere fattorizzazioni in $\mathbb{Q}[x]$, $\mathbb{R}[x]$ o $\mathbb{C}[x]$, menzionamo per completezza il fatto che, così come esiste una formula che fornisce la radici di un polinomio di secondo grado (in cui appare l'estrazione di una radice quadrata), esistono formule simili, ma un pò più complicate, che forniscono le radici dei polinomi di terzo e quarto grado (in cui appaiono estrazioni di radici terze o quarte, rispettivamente) ma non esistono (meglio: non possono esistere) formule dello stesso tipo che forniscano le radici di polinomi di grado superiore al quarto.

I due esempi conclusivi riguardano polinomi su campi finiti. Soprattutto quando la cardinalità del campo finito F è piccola il metodo più efficace per la ricerca delle radici di un polinomio $f \in F[x]$ è spesso la verifica diretta eseguita per ogni elemento, vale a dire il calcolo di $f(c)$ per ogni elemento c del campo.

Esempio 34. Per alcuni valori del primo p fattorizziamo f_p, il polinomio $f = 2x^5 - x^3 + 2x^2 - 1$ dell'esempio precedente riguardato come polinomio a coefficienti in $\mathbb{Z}_p$. Tra le applicazioni della proprietà universale viste

nella Sezione 2 ricordiamo l'omomorfismo suriettivo $\bar{\varepsilon}_p$ che ad ogni polinomio in $\mathbb{Z}[x]$ associa il polinomio stesso riguardato come polinomio a coefficienti in $\mathbb{Z}_p[x]$. Il fatto che $\bar{\varepsilon}_p$ sia un omomorfismo permette di 'tradurre' fattorizzazioni di un polinomio in $\mathbb{Z}[x]$ in fattorizzazioni della sua immagine in $\mathbb{Z}_p[x]$: per il nostro f, se $g, h \in \mathbb{Z}[x]$ sono tali che $f = gh$, allora $f^{\bar{\varepsilon}_p} = g^{\bar{\varepsilon}_p} h^{\bar{\varepsilon}_p}$.

Scriviamo allora f come prodotto di polinomi a coefficienti interi e irriducibili in $\mathbb{Z}[x]$, utilizzando quanto ottenuto nell'esempio precedente: $f = (x+1)(x^2-x+1)(2x^2-1)$. Per ogni primo p abbiamo $f_p = (x+1)^{\bar{\varepsilon}_p}(x^2-x+1)^{\bar{\varepsilon}_p}(2x^2-1)^{\bar{\varepsilon}_p}$. Per ottenere una fattorizzazione in prodotto di polinomi irriducibili in $\mathbb{Z}_p[x]$ si devono allora ulteriormente fattorizzare in prodotto di irriducibili (in $\mathbb{Z}_p[x]$) i tre fattori $h_{p,1} = (x+1)^{\bar{\varepsilon}_p}$, $h_{p,2} = (x^2-x+1)^{\bar{\varepsilon}_p}$ e $h_{p,3} = (2x^2-1)^{\bar{\varepsilon}_p}$. Non c'è nessun problema per il primo fattore, che è di primo grado e quindi irriducibile qualsiasi sia il primo p, vanno invece considerati con maggiore attenzione gli altri due fattori, che vanno studiati considerando separatamente i valori di p a cui siamo interessati. Qui consideriamo i primi minori o uguali a 7:

$p = 2$: $f_2 = x^3 + \bar{1} \in \mathbb{Z}_2[x]$ ha grado 3. Il terzo dei fattori appena presi in esame, infatti, in questo caso si riduce a $[1]_2$: $h_{2,3} = (\bar{2}x^2 - \bar{1})^{\bar{\varepsilon}_p} = \bar{1}$. Il secondo fattore $h_{2,2} = x^2 + x + \bar{1}$ è privo di radici in $\mathbb{Z}_2[x]$, infatti $h_{2,2}([0]_2) = h_{2,2}([1]_2) = [1]_2 \neq [0]_2$. Quindi, per la Proposizione 23, $h_{2,2}$ è irriducibile in $\mathbb{Z}_2[x]$ (vedi anche l'esempio successivo). La fattorizzazione di f_2 in prodotto di irriducibili in $\mathbb{Z}_2[x]$ è dunque $f_2 = (x + \bar{1})(x^2 + x + \bar{1})$.

$p = 3$: Se $p > 2$, quindi anche nel caso $p = 3$ che consideriamo ora, $\nu f_p = 5$. Sia $h_{3,2}$ che $h_{3,3}$ hanno grado 2, ricerchiamone le (eventuali) radici in $\mathbb{Z}_3$. Gli elementi di $\mathbb{Z}_3$ sono $[0]_3$, $[1]_3$, e $[-1]_3$, abbiamo $h_{3,2}([0]_3) = h_{3,2}([1]_3) = [1]_3 \neq [0]_3 = h_{3,2}([-1]_3)$, quindi $[-1]_3$ è l'unica radice di $h_{3,2}$ in $\mathbb{Z}_3$. Dal momento che $\nu h_{3,2} = 2$, allora $h_{3,2}$ è riducibile (è divisibile per $x + \bar{1}$, per il teorema di Ruffini) ed è il prodotto di due polinomi di primo grado, che possiamo anche scegliere monici perché $h_{3,2}$ è monico, dunque $h_{3,2} = (x + \bar{1})(x - c)$ dove c è una radice di $h_{3,2}$. Ma $[-1]_3$ è l'unica radice di $h_{3,2}$ in $\mathbb{Z}_3$ quindi $c = [-1]_3$ ed allora $h_{3,2} = (x + \bar{1})^2 \in \mathbb{Z}_3[x]$ (cosa che, ovviamente si può anche verificare direttamente: in $\mathbb{Z}_3[x]$ si ha $(x+\bar{1})^2 = x^2 + \bar{2}x + \bar{1} = x^2 - x + \bar{1} = h_{3,2}$). Consideriamo ora $h_{3,3} = -(x^2 + \bar{1})$; questo non ha radici in $\mathbb{Z}_3$, infatti $h_{3,3}([0]_3) = [-1]_3$ e $h_{3,3}([1]_3) = h_{3,3}([-1]_3) = [1]_3$. Dunque $h_{3,3}$ è irriducibile e la fattorizzazione di f_3 nel prodotto di un invertibile ed irriducibili monici è $f_3 = (-\bar{1})(x + \bar{1})^3(x^2 + \bar{1})$.

$p = 5$: Calcolando $h_{5,2}(c) = c^2 - c + [1]_5$ per ogni $c \in \mathbb{Z}_5$ verifichiamo rapidamente che $h_{5,2}([0]_5) = h_{2,5}([1]_5) = [1]_5$, $h_{5,2}([-1]_5) = [3]_5 = [-2]_5 = h_{5,2}([2]_5)$ e $h_{5,2}([-2]_5) = [2]_5$. Quindi $h_{5,2}$ non ha radici in $\mathbb{Z}_5$ e la Proposizione 23 ne garantisce l'irriducibilità. Per quanto riguarda $h_{5,3}$ abbiamo poi $h_{5,3} = \bar{2}x^2 - \bar{1} = \bar{2}x^2 + \bar{4} = \bar{2}(x^2 + \bar{2}) = \bar{2}(x^2 - \bar{3})$. Come si verifica subito, $[3]_5$ non è un quadrato in $\mathbb{Z}_5$ (infatti $[0]_5^2 = [0]_5$, $[1]_5^2 = [-1]_5^2 = [1]_5$ e $[2]_5^2 = [-2]_5^2 = [4]_5$), quindi anche $h_{5,3}$ è privo di radici in $\mathbb{Z}_5$ ed è così irriducibile in $\mathbb{Z}_5[x]$. Dunque, la fattorizzazione di f_5 nel prodotto di un invertibile ed irriducibili monici è $f_5 = \bar{2}(x + \bar{1})(x^2 - x + \bar{1})(x^2 + \bar{2})$.

$p = 7$: Ragionando come nei casi precedenti, cerchiamo le radici di $h_{7,2}$. Scopriamo che $[-2]_7$ e $[3]_7$ sono radici di $h_{7,2}$. Abbiamo poi $h_{7,3} = \bar{2}x^2 - \bar{1} = \bar{2}x^2 + \bar{6} = \bar{2}(x^2 + \bar{3}) = \bar{2}(x^2 - \bar{4}) = \bar{2}(x + \bar{2})(x - \bar{2})$ (quindi $h_{7,3}$ ha radici $[2]_7$ e $[-2]_7$). Allora tutti i fattori irriducibili di f_7 hanno primo grado; la fattorizzazione nel prodotto di un invertibile ed irriducibili monici è $f_7 = \bar{2}(x + \bar{1})(x - \bar{3})(x + \bar{2})^2(x - \bar{2})$.

Esempio 35. Possiamo usare i risultati di queste due ultime sezioni per elencare, uno per uno, tutti i polinomi irriducibili di assegnato grado in $\mathbb{Z}_2[x]$. Per qualsiasi campo K e per ogni $n \in \mathbb{N}$ i polinomi di grado n in $K[x]$ sono tutti quelli della forma $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ dove $a_0, a_1, \ldots, a_{n-1} \in K$ e $a_n \in K \smallsetminus \{0_K\}$. Nel nostro caso, in cui $K = \mathbb{Z}_2$, richiedere $a_n \in \mathbb{Z}_2 \smallsetminus \{0_{\mathbb{Z}_2}\}$ significa richiedere $a_n = [1]_2$, dunque tutti i polinomi non nulli in $\mathbb{Z}_2[x]$ sono monici. Abbiamo allora:

- esattamente due polinomi di grado uno: $x = x + \bar{0}$ e $x + \bar{1}$. Essendo di grado uno, questi sono irriducibili.
- I polinomi di grado due sono quelli della forma $x^2 + a_1 x + a_0$, dove a_1 e a_0 possono essere $\bar{0}$ o $\bar{1}$. Abbiamo dunque quattro polinomi di grado due: x^2, $x^2 + x$, $x^2 + \bar{1}$, $x^2 + x + \bar{1}$. Tra questi sono irriducibili tutti e soli quelli privi di radici. I primi due hanno $\bar{0}$ come radice, il terzo ha $\bar{1}$ come radice, il quarto non ha né $\bar{0}$ né $\bar{1}$ come radice, quindi è privo di radici ed è così irriducibile in $\mathbb{Z}_2[x]$, l'unico irriducibile di grado 2.
- Passiamo ai polinomi di grado tre: questi hanno la forma $x^3 + a_2x^2 + a_1x + a_0$, dove a_2, a_1 e a_0 possono essere scelti tra $\bar{0}$ e $\bar{1}$. Abbiamo così otto polinomi di grado tre; tra questi quelli privi di radici in $\mathbb{Z}_2$, cioè irriducibili in $\mathbb{Z}_2[x]$, sono: $x^3 + x^2 + \bar{1}$, $x^3 + x + \bar{1}$ e nessun altro.
- Per i polinomi di grado due o tre abbiamo usato la Proposizione 23; questa non può essere più utilizzata nel caso dei polinomi di quarto grado. Dei sedici polinomi di quarto grado esattamente quattro sono privi di radici in $\mathbb{Z}_2$, essi sono: $x^4+x^3+x^2+x+\bar{1}$, $x^4+x^3+\bar{1}$, $x^4+x^2+\bar{1}$ e $x^4+x+\bar{1}$. Un polinomio f di quarto grado (su un campo qualsiasi) che sia riducibile ma non abbia radici deve avere una fattorizzazione non banale del tipo $f = gh$ in cui $4 = \nu g + \nu h$ ma $\nu g \neq 1 \neq \nu h$, perché se f avesse un fattore di grado 1 allora avrebbe una radice (Proposizione 21), quindi deve aversi $\nu g = \nu h = 2$ Inoltre, poiché f è privo di radici anche g ed h sono privi di radici, quindi irriducibili. Dunque, un polinomio di quarto grado a coefficienti in un campo è irriducibile se e solo se è privo di radici e non è il prodotto di due polinomi irriducibili di grado due. Nel caso del campo $\mathbb{Z}_2$, che stiamo considerando, abbiamo visto che esiste solo un polinomio irriducibile di grado due: $x^2+x+\bar{1}$. Allora i polinomi irriducibili di grado quattro in $\mathbb{Z}_2[x]$ sono tutti e soli quelli privi radici ad eccezione di $(x^2+x+\bar{1})^2$. Poiché, come si vede rapidamente, $(x^2+x+\bar{1})^2 = x^4+x^2+\bar{1}$,

concludiamo che i polinomi irriducibili di grado quattro in $\mathbb{Z}_2[x]$ sono: $x^4+x^3+x^2+x+\bar{1}$, $x^4+x^3+\bar{1}$ e $x^4+x+\bar{1}$.

Abbiamo così stabilito che in $\mathbb{Z}_2[x]$ esistono esattamente due polinomi irriducibili di grado 1, uno di grado 2, due di grado 3, tre di grado 4. Si potrebbe continuare, con lo stesso metodo, ad elencare i polinomi irriducibili in $\mathbb{Z}_2[x]$ di gradi maggiori. Ad esempio, osservando che i polinomi irriducibili di grado cinque a coefficienti in un campo sono quelli privi di radici che non siano prodotto di un polinomio di grado due ed uno di grado tre si può arrivare a concludere che i polinomi irriducibili di grado cinque in $\mathbb{Z}_2[x]$ sono esattamente sei.

Si può anche ripetere l'esercizio per altri campi finiti. In questo caso non è più vero che i polinomi non nulli sono tutti monici, ma per trovare tutti quelli irriducibili basta comunque trovare gli irriducibili monici ed aggiungere poi alla lista i loro associati. Ad esempio, i polinomi irriducibili di secondo grado in $\mathbb{Z}_3[x]$ sono $x^2+\bar{1}$, $x^2+x-\bar{1}$, $x^2-x-\bar{1}$ (che sono i polinomi monici di grado due privi di radici) ed i loro opposti, che sono i loro altri associati.

Strutture booleane

GIOVANNI CUTOLO

Lo scopo di queste note è quello di presentare in modo unitario anelli booleani, reticoli booleani e algebre di Boole, senza entrare in troppi dettagli ma spiegando come e perché lo studio di ciascuna di queste strutture è equivalente a quello delle altre. Il riquadro che segue contiene un riassunto di questi contenuti; sia bene inteso che questo riassunto non è di per sé sufficiente per la loro comprensione, ma la sua lettura è un utile preliminare a quella del resto di queste note. Nella sezione finale delle note faremo poi qualche osservazione su come si possano inquadrare in questa teoria esempi di algebre di Boole che chi legge ha probabilmente incontrato, o sta per incontrare, in altri corsi.

In sintesi

Si definiscono tre tipi di strutture che fanno riferimento nel loro nome a quello di George Boole. Abbiamo gli *anelli booleani*, che sono per definizione gli anelli unitari i cui elementi sono tutti idempotenti, i *reticoli booleani*, che sono invece i reticoli distributivi e complementati, le *algebre di Boole*, che sono particolari strutture algebriche la cui definizione è riportata più avanti, nella terza sezione di queste note.

Ciò che lega queste strutture tra loro è che definire su un insieme una struttura di uno di questi tre tipi (anello booleano, reticolo booleano, algebra di Boole) equivale definirne una di ciascuno degli altri due tipi; in modo che risulti del tutto equivalente lo studio degli anelli booleani, quello delle algebre di Boole e quello dei reticoli booleani.

L'esempio da avere come riferimento è quello dell'insieme $\mathcal{P}(S)$ delle parti di un insieme S. Come dovrebbe essere ben noto, $(\mathcal{P}(S), \subseteq)$, cioè l'insieme $\mathcal{P}(S)$ ordinato per inclusione, è un reticolo, che risulta essere un reticolo booleano. Lo stesso insieme, munito delle operazioni di differenza simmetrica ed intersezione, $(\mathcal{P}(S), \triangle, \cap)$, è un anello booleano. Infine, $\mathcal{P}(S)$ si può struttuare come algebra di Boole mediante le operazioni di unione, intersezione e l'operazione unaria di complemento ${}^c\colon X \in \mathcal{P}(S) \mapsto S \smallsetminus X \in \mathcal{P}(S)$; l'algebra di Boole così ottenuta è $(\mathcal{P}(S), \cup, \cap, \varnothing, S, {}^c)$.

Questo esempio è particolarmente importante per almeno due motivi. Uno di tipo pratico: il modo in cui si può, in $\mathcal{P}(S)$, passare da uno dei tre tipi di struttura booleana a ciascuno degli altri due illustra molto bene come si può effettuare l'analogo passaggio a partire da una struttura booleana arbitraria; questo esempio può essere quindi di grande aiuto nello studio della situazione generale. Il secondo motivo, di carattere teorico e di importanza ancora maggiore, è che quello fornito dagli insiemi $\mathcal{P}(S)$ non è un esempio particolare ma, in qualche modo, quello tipico. Infatti un importante teorema (dovuto a M.H. Stone) mostra che ogni anello booleano finito è isomorfo a $(\mathcal{P}(S), \triangle, \cap)$ per un opportuno insieme S (per gli anelli infiniti il teorema è un po' più debole: ogni anello booleano è isomorfo ad un sottoanello unitario di $(\mathcal{P}(S), \triangle, \cap)$, per un opportuno insieme S). Analoghi enunciati valgono per i reticoli booleani e per le algebre di Boole. Questo vuol dire, ad esempio, che se sappiamo descrivere il reticolo delle parti degli insiemi finiti, conosciamo, a meno di isomorfismi, tutti i reticoli booleani finiti. Una conseguenza del teorema di Stone è che gli anelli booleani finiti (ma lo stesso vale per i reticoli booleani finiti o per le algebre di Boole finite) hanno per cardinalità una potenza di 2, e che due anelli booleani finiti con lo stesso numero di elementi sono necessariamente isomorfi.

Avvertenza. Alcune parti di questo file, in cui appaiono di regola dimostrazioni o verifiche, sono indentate e marcate da un segnale di pericolo. Questo indica che i loro contenuti vanno considerati approfondimenti per chi fosse ad essi interessato ma non fanno parte del programma del corso e non sono richiesti ai fini dell'esame. Altre osservazioni e dimostrazioni possono essere o non essere parte effettiva del programma, a seconda che siano o non siano state trattate a lezione.

1. Anelli booleani

Per definizione un *anello booleano* è un anello unitario in cui ogni elemento è *idempotente*, cioè coincide col proprio quadrato.

Ad esempio, l'anello $\mathbb{Z}_2$ degli interi modulo 2 è un anello booleano: è unitario e i suoi due elementi, $\bar{0} = [0]_2$ e $\bar{1} = [1]_2$ sono idempotenti: $\bar{0}^2 = \bar{0}$ e $\bar{1}^2 = \bar{1}$. Un altro esempio significativo è quello dell'anello $(\mathcal{P}(S), \triangle, \cap)$ delle parti di un (arbitrario) insieme S. Infatti quest'anello è unitario (di unità S) e, dal momento che l'operazione di moltiplicazione nell'anello $\mathcal{P}(S)$ è quella di intersezione, per ogni $X \in \mathcal{P}(S)$ si ha $X^2 = X \cap X = X$.

Prima di dimostrare una semplice proprietà degli anelli booleani è opportuno un richiamo sulla nozione di caratteristica di un anello unitario. Se R è un anello unitario e l'unità 1_R di R, ha periodo finito c nel gruppo additivo $(R, +)$, si dice che c è la *caratteristica* di R. Detto in modo più esplicito, se esiste qualche intero positivo n tale che $n1_R$ (che è la somma $1_R + 1_R + \cdots + 1_R$ con n addendi) è uguale a 0_R (lo zero di R), allora la caratteristica

di R è il minimo tale intero n.[1] Dovrebbe essere chiaro che R ha caratteristica 1 se e solo $1_R = 0_R$; si verifica facilmente che in questo caso $R = \{0_R\}$. Il caso immediatamente successivo è quello degli anelli di caratteristica 2: sono quelli in cui $1_R \neq 0_R$ ma $2 \cdot 1_R = 1_R + 1_R = 0_R$. Notiamo che l'anello $(\mathcal{P}(S), \triangle, \cap)$ ha questa proprietà se $S \neq \varnothing$. Infatti in questo anello l'unità è S, lo zero è $\varnothing$, l'addizione è l'operazione di differenza simmetrica e si ha $2 \cdot S = S \triangle S = \varnothing$. Quindi l'anello $\mathcal{P}(S)$ ha caratteristica 2.

Dimostriamo ora che quanto appena visto per $(\mathcal{P}(S), \triangle, \cap)$ vale per tutti gli anelli booleani; verificando inoltre che questi anelli sono sempre commutativi.

Proposizione 1. *Sia R un anello booleano. Allora R è commutativo e, se $|R| > 1$, R ha caratteristica 2.*

Dimostrazione. Per ogni $a, b \in R$ si ha $a^2 = a$, $b^2 = b$ e $(a+b)^2 = a + b$, perché R è booleano. D'altra parte, come in ogni anello,

$$(a+b)^2 = (a+b)(a+b) = a(a+b) + b(a+b) = a^2 + ab + ba + b^2$$

e quindi

$$a + b = (a+b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b.$$

Da ciò, cancellando a e b, si ricava $ab + ba = 0_R$. Dunque:

$$(\forall a, b \in R)\ (ab = -ba). \tag{$*$}$$

Applicando la $(*)$ nel caso in cui $a = b$ si ottiene, per ogni $a \in R$, $a^2 = -a^2$. Ma $a^2 = a$, quindi:

$$(\forall a \in R)\ (a = -a); \qquad \text{ovvero:} \qquad (\forall a \in R)\ (2a = 0_R). \tag{$**$}$$

In particolare, $2 \cdot 1_R = 0_R$, quindi o $1_R = 0_R$ e $R = \{0_R\}$ ha un solo elemento, oppure $|R| > 1$ e la caratteristica di R è 2.

Infine, per ogni $a, b \in R$, applicando la $(**)$ all'elemento ba otteniamo $-ba = ba$, quindi la $(*)$ prova $ab = ba$. È così dimostrato che R è commutativo. □

Enunciamo ma non dimostriamo il teorema di Stone, che è il risultato fondamentale nella teoria degli anelli booleani.

Teorema di Stone. *Sia R un anello booleano. Allora:*

(i) *esiste un insieme S tale che R sia isomorfo ad un sottoanello unitario di $(\mathcal{P}(S), \triangle, \cap)$;*
(ii) *se R è finito, esiste un insieme S tale che R sia isomorfo a $(\mathcal{P}(S), \triangle, \cap)$.*

Va notato, a proposito del punto (i), che tutti i sottoanelli unitari di $(\mathcal{P}(S), \triangle, \cap)$ sono booleani. Infatti:

Esercizio 2. Se R è un anello booleano ogni sottoanello unitario di R è booleano.

Il teorema di Stone ha un'importante conseguenza:

Corollario 3. *Sia R un anello booleano finito. Allora:*

(i) *$|R|$ è un potenza di 2;*
(ii) *se A è un anello booleano e $|A| = |R|$, allora $A \simeq R$.*

Dimostrazione. Per il teorema di Stone, esiste un insieme S, ovviamente finito, tale che R sia isomorfo a $(\mathcal{P}(S), \triangle, \cap)$. Posto $n = |S|$, allora $|R| = |\mathcal{P}(S)| = 2^n$, il che giustifica la (i). Se poi A è un anello booleano, anch'esso di cardinalità 2^n, ancora per il teorema di Stone abbiamo $A \simeq (\mathcal{P}(T), \triangle, \cap)$ per un opportuno insieme T. Ma allora $|\mathcal{P}(T)| = |A|$, quindi $|\mathcal{P}(T)| = 2^n$ e deduciamo così $|T| = n$. Dunque, $|T| = |S|$; questo comporta (vedi l'esercizio che segue) $(\mathcal{P}(T), \triangle, \cap) \simeq (\mathcal{P}(S), \triangle, \cap)$, quindi $A \simeq R$. □

Esercizio 4. Verificare che se $f\colon S \to T$ è un'applicazione biettiva, allora l'applicazione immagine $\vec{f}\colon \mathcal{P}(S) \to \mathcal{P}(T)$ è un isomorfismo di anelli da $(\mathcal{P}(S), \triangle, \cap)$ a $(\mathcal{P}(T), \triangle, \cap)$.

È bene notare che, nel teorema di Stone il caso degli anelli booleani infiniti differisce effettivamente dal caso degli anelli finiti. Esistono infatti anelli booleani infiniti che non sono isomorfi a $(\mathcal{P}(S), \triangle, \cap)$ per alcun insieme S. Un esempio è fornito dall'insieme P costituito da tutti i sottoinsiemi X di $\mathbb{N}$ tali che uno tra X e $\mathbb{N} \smallsetminus X$ sia finito.[2] Non è difficile verificare (ed è un buon esercizio farlo) che P è un sottoanello unitario di $(\mathcal{P}(\mathbb{N}), \triangle, \cap)$ e di conseguenza è un anello booleano. Si può però dimostrare (ma non si tratta in questo caso di un esercizio) che per ogni insieme S non esistono applicazioni biettive da P a $\mathcal{P}(S)$, quindi P, come anello, non può essere isomorfo a $(\mathcal{P}(S), \triangle, \cap)$.

---

[1] Se invece non esiste nessun $n \in \mathbb{N}^*$, tale che $n1_R = 0_R$, cioè: se 1_R non è periodico in $(R, +)$, allora R ha per definizione caratteristica 0.

[2] una parte X di un insieme Y si dice cofinita in Y se e solo se $Y \smallsetminus X$ è un insieme finito. Dunque, P è l'insieme costituito dalle parti finite e dalle parti cofinite di $\mathbb{N}$.

2. Reticoli booleani

Ricordiamo[3] che un reticolo è un insieme ordinato non vuoto $(L, \leq)$ tale che, per ogni $a, b \in L$ esistano l'estremo inferiore $\inf_{(L,\leq)}\{a, b\}$ e l'estremo superiore $\sup_{(L,\leq)}\{a, b\}$ di $\{a, b\}$ in $(L, \leq)$.

Ricordiamo anche che si può, in modo equivalente, riguardare i reticoli anche come strutture algebriche. Infatti, se $(L, \leq)$ è un reticolo, si definiscono in L le due *operazioni reticolari* $\vee$ e $\wedge$, ponendo, per ogni $a, b \in L$,

$$a \vee b = \sup_{(L,\leq)}\{a, b\} \qquad \text{e} \qquad a \wedge b = \inf_{(L,\leq)}\{a, b\}$$

e valgono, per $\vee$ e $\wedge$ queste proprietà algebriche:

(1) $\vee$ e $\wedge$ sono commutative;
(2) $\vee$ e $\wedge$ sono associative;
(3) valgono le leggi di assorbimento: per ogni $a, b \in L$,
   - $a \vee (a \wedge b) = a$;
   - $a \wedge (a \vee b) = a$.

Vale anche per $\vee$ e $\wedge$ una quarta proprietà, l'iteratività: per ogni $a \in L$, $a \vee a = a = a \wedge a$ (vale a dire: ogni elemento di L è idempotente sia rispetto a $\vee$ che rispetto a $\wedge$). Se, viceversa, $(L, \vee, \wedge)$ è una struttura algebrica in cui $\vee$ e $\wedge$ sono due operazioni binarie che verificano (1), (2) e (3), allora si può definire in L una relazione binaria $\preceq$ ponendo, per ogni $a, b \in L$,

$$a \preceq b \iff a = a \wedge b$$

e si verifica che $\preceq$ è una relazione d'ordine che rende $(L, \preceq)$ un reticolo. Inoltre, per ogni $a, b \in L$ si ha $a \vee b = \sup_{(L,\preceq)}\{a, b\}$ e $a \wedge b = \inf_{(L,\preceq)}\{a, b\}$. Dunque, $\vee$ e $\wedge$ risultano essere le operazioni reticolari in $(L, \preceq)$. Allo stesso modo, se $\vee$ e $\wedge$ sono le operazioni reticolari definite in un reticolo $(L, \leq)$, è chiaro che la relazione $\preceq$ definita sopra coincide con $\leq$.

In sintesi, fissato un insieme non vuoto L, se $\mathcal{A}$ è l'insieme delle relazioni d'ordine $\leq$ tali che $(L, \leq)$ sia un reticolo e $\mathcal{B}$ è l'insieme delle coppie $(\vee, \wedge)$ di operazioni binarie in L che verificano le condizioni (1), (2) e (3), abbiamo definito due applicazioni tra $\mathcal{A}$ e $\mathcal{B}$. La prima è $\alpha\colon \mathcal{A} \to \mathcal{B}$, che ad una relazione d'ordine $\leq \in \mathcal{A}$ associa la coppia ordinata $(\vee, \wedge) \in \mathcal{B}$, dove $\vee$ e $\wedge$ sono le operazioni reticolari di estremo superiore ed estremo inferiore in $(L, \leq)$. La seconda applicazione è $\beta\colon \mathcal{B} \to \mathcal{A}$, che ad ogni $(\vee, \wedge) \in \mathcal{B}$ associa la relazione d'ordine $\preceq \in \mathcal{A}$ definita come sopra. Quello che abbiamo evidenziato è che α e β sono l'una inversa dell'altra, quindi sono biettive.

L'esistenza di queste biezioni fa sì che sia del tutto equivalente lo studio dei reticoli (intesi come particolari insiemi ordinati) e quello delle strutture algebriche $(L, \vee, \wedge)$ per le quali valgano le condizioni (1), (2) e (3). Per questo motivo si fa riferimento a queste strutture chiamandole 'reticoli come strutture algebriche'. D'ora in avanti, dunque, per indicare un reticolo faremo indifferentemente riferimento alla strutture di insieme ordinato (indicando, ad esempio, il reticolo come $(L, \leq)$) o alla struttura algebrica (indicando il reticolo, con un abuso di terminologia, come $(L, \vee, \wedge)$; conveniamo che la prima operazione indicata è quella di estremo superiore, la seconda quella di estremo inferiore). Può essere conveniente, e lo faremo, indicare un reticolo come $(L, \leq, \vee, \wedge)$ per specificare in modo sintetico sia la relazione d'ordine che le operazioni reticolari.

Ricordiamo che anche le due possibili nozioni di isomorfismo per i reticoli (come insiemi ordinati) ed i reticoli come strutture algebriche coincidono. Va però osservato che la nozione di *sottoreticolo* è algebrica, nel senso che può essere definita solo in termini delle operazioni reticolari.

Infatti, se $(L, \leq)$ è un reticolo, un sottoreticolo di $(L, \leq)$ è per definizione un sottoinsieme non vuoto K di L che sia chiuso rispetto alle operazioni reticolari $\vee$ e $\wedge$ di L. Le operazioni indotte in K da $\vee$ e $\wedge$ continuano a verificare le condizioni (1), (2) e (3) e quindi rendono K un reticolo rispetto alla relazione d'ordine indotta da $\leq$ su K (quest'ultima osservazione è garantita dal fatto che la relazione d'ordine del reticolo è determinata dalle operazioni reticolari: per ogni $a, b \in L$ si ha $a \leq b \iff a = a \wedge b$).

Se a e b sono elementi di un insieme ordinato $(S, \leq)$, si chiama intervallo chiuso di estremi a e b, e si indica con $[a, b]_{(S,\leq)}$ (o semplicemente $[a, b]$ se il riferimento a $(S, \leq)$ può essere sottinteso) l'insieme $\{x \in S \mid a \leq x \leq b\}$, che è diverso dal vuoto se e solo se $a \leq b$ e in questo caso ha a come minimo e b come massimo.

Lemma 5. *Siano a e b elementi del reticolo $(L, \leq)$.*

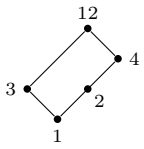
(i) *l'insieme $\{x \in L \mid a \leq x\}$ è un sottoreticolo di $(L, \leq)$;*
(ii) *l'insieme $\{x \in L \mid x \leq b\}$ è un sottoreticolo di $(L, \leq)$;*
(iii) *se $a \leq b$, l'intervallo chiuso $[a, b]$ è un sottoreticolo di $(L, \leq)$.*

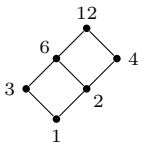
Dimostrazione. Sia $X = \{x \in L \mid a \leq x\}$. Certamente $X \neq \varnothing$, perché $a \in X$. Siano x e y elementi di X. Allora $a \leq x$ e $a \leq y$, quindi a è un minorante di $\{x, y\}$ in $(L, \leq)$. Dunque $a \leq \inf_{(L,\leq)}\{x, y\} = x \wedge y$ e possiamo concludere $x \wedge y \in X$. Inoltre $a \leq x \leq x \vee y$, quindi $x \vee y \in X$. Abbiamo così provato che X è chiuso rispetto a $\vee$ e $\wedge$, quindi è un sottoreticolo di $(L, \leq)$. È così provata la (i). Per dualità, anche $Y := \{x \in L \mid x \leq b\}$ è un sottoreticolo, quindi anche la (ii) è vera. Infine, si ha ovviamente $[a, b] = X \cap Y$, quindi $[a, b]$ è chiuso rispetto a $\vee$ e $\wedge$, in quanto intersezione di parti chiuse. Se $a \leq b$, allora $[a, b] \neq \varnothing$ e $[a, b]$ è un sottoreticolo di L; vale così anche (iii). □

[3] per tutto ciò che qui viene 'ricordato' e non giustificato o comunque spiegato in dettaglio, si rimanda al libro di testo o alle altre fonti a disposizione.

Ad esempio, per ogni $n \in \mathbb{N}$ sia l'insieme $\mathrm{Div}_{\mathbb{N}}(n)$ dei divisori di n che quello, $n\mathbb{N}$, dei multipli di n (in $\mathbb{N}$) costituiscono sottoreticoli di $(\mathbb{N}, |\,)$. Similmente, se S è un insieme e $T \subseteq S$, allora sia $\mathcal{P}(T)$ che l'insieme delle parti di S contenenti T costituiscono sottoreticoli di $(\mathcal{P}(S), \subseteq)$.

Esempio 6. Sia $L = \mathrm{Div}_{\mathbb{N}}(12)$ il reticolo dei divisori di 12, rappresentato dal diagramma di Hasse a destra. Il sottoinsieme $K = L \smallsetminus \{6\}$ non è un sottoreticolo di L, infatti K non è chiuso rispetto all'operazione reticolare $\vee$, dal momento che 2 e 3 appartengono a K ma $6 = 2 \vee 3 \notin K$. Se però consideriamo K come insieme ordinato dall'ordinamento indotto da quello di L, quindi ordinato per divisibilità, non è difficile verificare che, rispetto a questo ordinamento, K è un reticolo; il suo diagramma di Hasse è rappresentato a sinistra.





Questo esempio mostra che anche se un sottoinsieme ordinato di un reticolo L è, rispetto all'ordinamento indotto, a sua volta un reticolo, non è detto che esso sia un sottoreticolo di L.

Anche le nozioni di minimo e massimo hanno un'interpretazione algebrica.

Lemma 7. *Sia $(L, \leq, \vee, \wedge)$, un reticolo. Per ogni $a \in L$, a è il minimo in L se e solo se a è elemento neutro rispetto a $\vee$; a è il massimo in L se e solo se a è elemento neutro rispetto a $\wedge$.*

Dimostrazione. Si ha $a = \min L$ se e solo se $a \leq b$ per ogni $b \in L$; ma $a \leq b$ equivale a $a \vee b = b$. Dunque, $a = \min L$ se e solo se, per ogni $b \in L$ si ha $a \vee b = b$, cioè: se e solo se a è neutro in $(L, \vee)$. È così provata la prima parte dell'enunciato. La seconda è duale. □

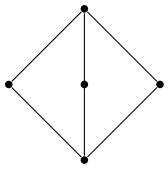
Dunque, se $(L, \leq, \vee, \wedge)$ è un un reticolo limitato (cioè dotato di minimo e massimo) sia $(L, \vee)$ che $(L, \wedge)$ sono monoidi commutativi.

Ad esempio, il reticolo $(\mathcal{P}(S), \subseteq)$ delle parti di un insieme S ha minimo e massimo, rispettivamente $\varnothing$ e S, ed operazioni reticolari $\cup$ e $\cap$. In effetti, $\varnothing$ è l'elemento neutro del monoide $(S, \cup)$, S è l'elemento neutro del monoide $(S, \cap)$.

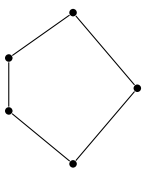
Definizione. Sia $(L, \leq, \vee, \wedge)$ un reticolo limitato e sia $a \in L$. Per ogni $b \in L$, b è un *complemento* di a in L se e solo se $a \vee b = \max L$ e $a \wedge b = \min L$.

Dovrebbe essere chiaro che, con le notazioni della definizione, dire che b è un complemento di a equivale a dire che a è un complemento di b. Altrettanto ovvio è che $\min L$ e $\max L$ sono l'uno complemento dell'altro (anzi, $\min L$ è l'unico complemento di $\max L$ in L e, dualmente, $\max L$ è l'unico complemento di $\min L$ in L.) Altri esempi:

- nel reticolo $(\mathcal{P}(S), \subseteq)$ delle parti di un insieme S, ogni elemento ha uno ed un solo complemento. Infatti, per ogni $X \in \mathcal{P}(S)$, $X \cup (S \smallsetminus X) = S = \max \mathcal{P}(S)$ e $X \cap (S \smallsetminus X) = \varnothing = \min \mathcal{P}(S)$, quindi $S \smallsetminus X$ è un complemento di X in $\mathcal{P}(S)$. L'unicità è facile da verificare direttamente, ma segue anche da considerazioni che faremo più avanti (Proposizione 9).
- Nel reticolo dei divisori di 12, visto nell'Esempio 6, gli elementi 1 e 12 (minimo e massimo del reticolo) sono l'uno complemento dell'altro, 3 e 4 sono l'uno complemento dell'altro ma né 2 né 6 hanno complemento.
- Come si vede facilmente, se L è un insieme non vuoto totalmente ordinato (e quindi un reticolo) limitato, in L gli unici elementi che hanno complemento sono il minimo ed il massimo.
- Anche in $(\mathbb{N}, |\,)$, gli unici elementi che hanno complemento sono il minimo, 0, ed il massimo, 1. Sia infatti $a \in \mathbb{N}$ e sia b un complemento di a in $(\mathbb{N}, |\,)$. Ricordando che le operazioni reticolari in $(\mathbb{N}, |\,)$ sono descritte dal minimo comune multiplo e dal massimo comun divisore, abbiamo $0 = \mathrm{mcm}(a, b)$ e $1 = \mathrm{MCD}(a, b)$. Se $a \neq 0$, allora da $\mathrm{mcm}(a, b) = 0$ segue $b = 0$, ma se $b = 0$ allora $1 = \mathrm{MCD}(a, b) = \mathrm{MCD}(a, 0) = a$. Dunque, se $a \notin \{0, 1\}$, a non ha complementi in $(\mathbb{N}, |\,)$.
- Un elemento in un reticolo (limitato) può anche avere più di un complemento. Questi due esempi sono di grande importanza:



reticolo trirettangolo



reticolo pentagonale

Come si vede immediatamente, nel reticolo trirettangolo ciascuno dei tre elementi diversi dal minimo e dal massimo ha gli altri due come complementi; nel reticolo pentagonale l'elemento rappresentato più a destra ha due complementi.

Ovviamente è possibile modificare questi esempi in modo da ottenenere reticoli finiti (e quindi limitati) con elementi dotati di un numero arbitrario di complementi. (Come?)

Definizione. Un reticolo L si dice *complementato* se e solo se ogni suo elemento ha in L almeno un complemento.

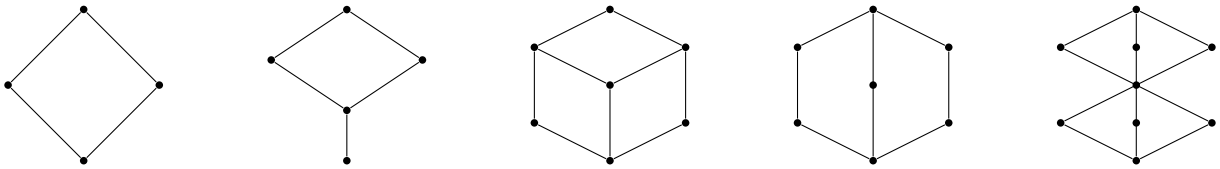
È chiaro che un reticolo, per essere complementato deve essere, in primo luogo, limitato, altrimenti in esso non possono esistere elementi dotati di complementi. Dagli esempi forniti a proposito della nozione di complemento vediamo subito che:

- per ogni insieme S, il reticolo $(\mathcal{P}(S), \subseteq)$ è complementato;
- un insieme non vuoto totalmente ordinato è complementato se e solo se ha al massimo due elementi;
- né $(\mathbb{N}, |\,)$ né il reticolo dei divisori di 12 sono complementati;
- il reticolo trirettangolo e quello pentagonale sono complementati.

Esercizio 8. Per ogni $n \in \mathbb{N}$, sia D_n il reticolo dei divisori di n in $\mathbb{N}$ (che è, ricordiamo, un sottoreticolo di $(\mathbb{N}, |\,)$). Lo scopo di questo esercizio è riconoscere che D_n è complementato se e solo se n è un intero *libero da quadrati*, cioè un intero non divisibile per il quadrato di alcun primo.[(4)]

(i) Sia d un divisore (in $\mathbb{N}$) di n. Se d e n/d sono coprimi, allora n/d è un complemento di d in D_n. [*Suggerimento: basta calcolare MCD e mcm tra d e n/d.*]
(ii) Dedurre dal punto precedente che se n è libero da quadrati allora D_n è complementato. [*Suggerimento: pensare alla scomposizione di n in fattori primi e descrivere i divisori di n.*]
(iii) Supponiamo che esista un primo p tale che p^2 divida n. Allora p non ha complemento in D_n. [*Suggerimento: se a è un complemento di p, p divide o non divide a?*]
(iv) A questo punto la conclusione è facile: D_n è complementato se e solo se n è libero da quadrati.

Ulteriori esempi: dei reticoli qui rappresentati sono complementati il primo, ed il quarto, non gli altri tre.



Un'altra proprietà di natura algebrica riferita a reticoli è la distributività.

Definizione. Un reticolo $(L, \leq, \vee, \wedge)$ si dice *distributivo* se e solo ciascuna delle due operazioni reticolari $\vee$ e $\wedge$ è distributiva rispetto all'altra.

In termini più espliciti, $(L, \leq, \vee, \wedge)$ è distributivo se e solo se, per ogni $a, b, c \in L$ si ha:

(d_1): $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$; e
(d_2): $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$.

In realtà è possibile dimostrare che se, in un reticolo L, è verificata almeno una delle due condizioni (d_1) e (d_2) *per ogni terna (a, b, c) di elementi di L*, allora anche l'altra è verificata e quindi L è distributivo.

Ad esempio, l'operazione insiemistica di unione binaria è distributiva rispetto all'intersezione, e viceversa l'intersezione è distributiva rispetto all'unione, quindi, per ogni insieme S, il reticolo $(\mathcal{P}(S), \subseteq)$ è distributivo.

Non è difficile verificare (è un utile esercizio di aritmetica) che anche il reticolo $(\mathbb{N}, |\,)$ è distributivo, così come sono distributivi i reticoli totalmente ordinati (quest'ultimo fatto segue anche dal criterio di distributività di Birkhoff, che incontreremo tra poco).

Invece, non sono distributivi né il reticolo trirettangolo né il reticolo pentagonale. Questo fatto segue dal prossimo risultato, perché come abbiamo visto, in questi due reticoli esistono elementi con più complementi.

Proposizione 9. *Sia $(L, \leq, \vee, \wedge)$ un reticolo distributivo. Allora ogni elemento di L ha al più un complemento in L.*

Dimostrazione. Sia $a \in L$, e siano x e y complementi di a in L. Per provare l'enunciato occorre (e basta) verificare che $x = y$.

Indicando con 1 e 0, nell'ordine, il massimo e il minimo di L, si ha $a \wedge x = a \wedge y = 0$ e $a \vee x = a \vee y = 1$. Usando la proprietà distributiva abbiamo:

$$x = x \vee 0 = x \vee (a \wedge y) = (x \vee a) \wedge (x \vee y) = 1 \wedge (x \vee y) = x \vee y.$$

Analogamente, scambiando i ruoli tra x e y, possiamo ottenenere $y = y \vee x$. Ma allora $y = y \vee x = x \vee y = x$. □

Dovrebbe essere evidente dalla definizione che ogni sottoreticolo di un reticolo distributivo è a sua volta distributivo. Di conseguenza, un reticolo distributivo non può avere sottoreticoli che siano isomorfi al reticolo trirettangolo o quello pentagonale. Un risultato notevole della teoria dei reticoli, che non dimostreremo, mostra che vale anche il viceversa: l'assenza di tali sottoreticoli basta a provare che un reticolo è distributivo.

Criterio di distributività di Birkhoff. *Sia L un reticolo. L è distributivo se e solo se non ha sottoreticoli isomorfi a uno tra il reticolo trirettangolo e il reticolo pentagonale.*

(4) i numeri naturali liberi da quadrati sono dunque 1 ed i numeri naturali che si possono scrivere come prodotti di primi a due a due distinti.

Vediamo qualche esempio di applicazione del criterio di Birkhoff. Poiché i sottoreticoli dei reticoli totalmente ordinati sono certamente totalmente ordinati, e nessuno dei due reticoli trirettangolo o pentagonale lo è, il criterio di Birkhoff fornisce una maniera per dimostrare che i reticoli totalmente ordinati sono distributivi. Siccome sia il reticolo trirettangolo che quello pentagonale sono costituiti da cinque elementi, il criterio di Birkhoff mostra anche che i reticoli con meno di cinque elementi sono sicuramente distributivi, quelli di cardinalità cinque sono distributivi se e solo se non sono isomorfi né al reticolo trirettangolo né al pentagonale. Se torniamo ai cinque reticoli esaminati come esempi dopo l'Esercizio 8, vediamo così che i primi due sono distributivi, gli altri tre no. Evidenziamo sottoreticoli trirettangoli (in blu) o pentagonali (in rosso) nei tre reticoli non distributivi:

È necessario fare attenzione al fatto che il criterio di Birkhoff esclude l'esistenza di sottoreticoli isomorfi al reticolo trirettangolo o a quello pentagonale in un reticolo distributivo L, ma non esclude che un sottoinsieme di L, munito dell'ordinamento indotto, possa essere un reticolo di uno di questi due tipi. Consideriamo il reticolo L dei divisori di 12 ed il suo sottoinsieme $K = L \smallsetminus \{6\}$ discusso nell'Esempio 6. Come sappiamo, L è un reticolo distributivo (è un sottoreticolo di $(\mathbb{N}, |\,)$) e, come si può vedere, K è isomorfo al reticolo pentagonale. Questo non contraddice il criterio di Birkhoff, perché K non è un sottoreticolo di L.

Definizione. Un reticolo si dice *booleano* se e solo se è distributivo e complementato.

Ad esempio, per ogni insieme S, il reticolo $(\mathcal{P}(S), \subseteq)$ è booleano. In conseguenza della definizione e della Proposizione 9, *se L è un reticolo booleano, ogni elemento di L ha uno ed un solo complemento in L.*

Osserviamo che un reticolo L è complementato, distributivo o booleano, allora anche il duale di L ha la stessa proprietà. Quindi vale per i reticoli con queste proprietà il principio di dualità: se una certa affermazione è verificata da ogni reticolo complementato, allora anche l'affermazione duale varrà in ogni reticolo complementato. Lo stesso è vero se nella frase precedente sostituiamo "complementato" con "distributivo" o con "booleano".

3. Algebre di Boole

Come sappiamo, si può dare la nozione di reticolo in termini puramente algebrici, cioè esclusivamente in termini di operazioni, senza fare riferimento a relazioni d'ordine: stiamo parlando dei reticoli 'come strutture algebriche'. Sia $(L, \wedge, \vee)$ una struttura algebrica di reticolo; vediamo quali condizioni sulle operazioni dobbiamo imporre affinché il reticolo L sia booleano. Oltre alle proprietà commutativa, associativa ed alle leggi di assorbimento, che già conosciamo, devono valere le proprietà distributive (di $\vee$ rispetto a $\wedge$ e di $\wedge$ rispetto a $\vee$), che fanno sì che il reticolo L sia distributivo. Sappiamo poi dal Lemma 7 che il fatto che L sia limitato equivale all'esistenza di elementi neutri per $\vee$ e $\wedge$. Infine, come abbiamo visto, in un reticolo booleano ogni elemento ha un unico complemento; possiamo allora considerare l'applicazione $'\colon L \to L$ che ad ogni $a \in L$ associa il suo complemento a' in L. Queste considerazioni suggeriscono la seguente definizione:

Definizione. Si dice *algebra di Boole* una struttura algebrica $(L, \vee, \wedge, 0, 1, ')$, dove $\vee$ e $\wedge$ sono operazioni binarie, 0 e 1 operazioni nullarie e $'$ un'operazione unaria, tale che:

(1) $(L, \vee, 0)$ e $(L, \wedge, 1)$ siano monoidi commutativi;
(2) valgano le leggi di assorbimento: per ogni $a, b \in L$, $a \vee (a \wedge b) = a = a \wedge (a \vee b)$;
(3) $\vee$ sia distributiva rispetto a $\wedge$ e $\wedge$ sia distributiva rispetto a $\vee$;
(4) per ogni $a \in L$, $a \vee a' = 1$ e $a \wedge a' = 0$,

dove abbiamo indicato con a' l'immagine di a rispetto a $'$.

Per quanto detto sopra, ogni reticolo booleano dà luogo ad un'algebra di Boole, viceversa un'algebra di Boole si può sempre riguardare come reticolo booleano. Infatti, la (1) e la (2) esprimono esattamente il fatto che $(L, \wedge, \vee)$ è un reticolo limitato, con minimo 0 e massimo 1, come segue dal Lemma 7; la (3) dice che questo reticolo è distributivo e la (4) garantisce che ogni elemento a di L ha un complemento: a'.

Possiamo dunque dire che la nozione di algebra di Boole è la versione 'puramente algebrica' della nozione di reticolo booleano.

Abbiamo, come per tutti tipi di strutture algebriche, una nozione di isomorfismo tra algebre di Boole: un'isomorfismo da un'algebra di Boole $(L_1, \vee_1, \wedge_1, 0_1, 1_1, ')$ ad un'algebra di Boole $(L_2, \vee_2, \wedge_2, 0_2, 1_2, '')$ è un'applicazione biettiva $f\colon L_1 \to L_2$ che 'conservi le operazioni', tale cioè che, per ogni $a, b \in L_1$ si abbia

i.) $f(a \vee_1 b) = f(a) \vee_2 f(b)$ e $f(a \wedge_1 b) = f(a) \wedge_2 f(b)$;
ii.) $f(0_1) = 0_2$ e $f(1_1) = 1_2$;
iii.) $f(a') = (f(a))''$.

Ora, la i.), cioè il proprietà che f conservi le operazioni reticolari, equivale al fatto che la biezione f sia un isomorfismo di reticoli. Se questa proprietà è verificata valgono però anche la ii.) e la iii.). Infatti, se f è un isomorfismo di reticoli da L_1 a L_2, allora f deve mandare il minimo 0_1 di L_1 nel minimo 0_2 di L_2 e, analogamente, $1_1 = \max L_1$ in $1_2 = \max L_2$. Vale così la ii.). Inoltre, per ogni $a \in L_1$, poiché a' è un complemento di a in L_1,

la sua immagine $f(a')$ deve essere un complemento di $f(a)$ in L_2. Ma, poiché L_2 è booleano, $(f(a))''$ è l'unico complemento di $f(a)$ in L_2, quindi $f(a') = (f(a))''$. Quello che abbiamo verificato è che gli isomorfismi di algebre di Boole da L_1 a L_2 sono tutti e soli gli isomorfismi di reticoli da L_1 a L_2. In particolare due algebre di Boole sono isomorfe (come algebre di Boole) se e solo se sono isomorfe come reticoli. A questo punto possiamo davvero concludere che lo studio delle algebre di Boole equivale allo studio dei reticoli booleani.

Definizione. Sia $(L, \vee, \wedge, 0, 1, ')$ un'algebra di Boole. Una parte non vuota K di L ne costituisce una *sottoalgebra di Boole* se e solo se K è un sottomonoide sia di $(L, \vee)$ che di $(L, \wedge)$ e contiene il complemento in L di ogni suo elemento.

In modo più esplicito, K costituisce una sottoalgebra di Boole di $(L, \vee, \wedge, 0, 1, ')$ se e solo se $K \subseteq L$ e sono verificate queste condizioni: per ogni $a, b \in K$,

- $a \vee b \in K$ e $a \wedge b \in K$;
- $0 \in K$ e $1 \in K$;
- $a' \in K$.

È evidente che in queste condizioni K, munita delle operazioni indotte da quelle di L è a sua volta un'algebra di Boole.

La nozione di sottoalgebra di Boole differisce da quella di sottoreticolo. Infatti, un sottoreticolo K di un reticolo booleano L deve essere chiuso rispetto alle due operazioni reticolari (quindi deve verificare la prima delle tre condizioni appena elencate), ma non contiene necessariamente il massimo o il minimo del reticolo né, tanto meno, i complementi dei suoi elementi.

Esempio 10. Dato un insieme $S \neq \varnothing$, consideriamo il reticolo booleano $(\mathcal{P}(S), \subseteq)$. Questo si struttura come algebra di Boole nella forma $(\mathcal{P}(S), \cup, \cap, \varnothing, S, ^c)$, dove ^{c} è l'applicazione "complemento" che manda ogni $X \in \mathcal{P}(S)$ in $X^c = S \smallsetminus X \in \mathcal{P}(S)$. Se T è una parte propria di S, allora $\mathcal{P}(T)$ costituisce un sottoreticolo di $\mathcal{P}(S)$ (ad esempio, per il Lemma 5), ma non una sottoalgebra di Boole di $\mathcal{P}(S)$, dal momento che $S \notin \mathcal{P}(T)$.

Nel caso appena considerato, $(\mathcal{P}(T), \subseteq)$ è comunque un reticolo booleano, quindi si struttura come algebra di Boole. Ma in altri casi la situazione puo' essere diversa. Ad esempio, se supponiamo $\varnothing \neq T \subset S$, allora $\{\varnothing, T, S\}$ forma un sottoreticolo di $(\mathcal{P}(S), \subseteq)$ che non è complementato e quindi non è booleano.

Esercizio 11. Provare che un parte di un'algebra di Boole ne è una sottoalgebra di Boole se e solo se è un sottoreticolo che contenga il complemento di ogni suo elemento.

Il prossimo enunciato elenca alcune identità che valgono nelle algebre di Boole. La terza si esprime dicendo che l'operazione di complemento è involutoria, cioè coincide con l'applicazione inversa di sé stessa (e, in particolare, è biettiva); le ultime due sono le note come leggi di De Morgan per algebre di Boole.

Proposizione 12. *Sia $(L, \vee, \wedge, 0, 1, ')$ un'algebra di Boole. Allora, per ogni $a, b \in L$,*

(i) $1 \vee a = 1$ *e* $0 \wedge a = 0$;
(ii) $1' = 0$ *e* $0' = 1$;
(iii) $(a')' = a$;
(iv) $(a \vee b)' = a' \wedge b'$;
(v) $(a \wedge b)' = a' \vee b'$.

Dimostrazione. La (i) e la (ii) sono immediate: visto L come reticolo, e quindi come insieme ordinato, 1 e 0 ne sono il massimo e il minimo e le operazioni $\vee$ e $\wedge$ forniscono estremi superiori e inferiori, dunque $1 \vee a = \sup\{1, a\} = 1$ e $0 \wedge a = \inf\{0, a\} = 0$;[(5)] inoltre, come sappiamo, minimo e massimo sono sempre l'uno il complemento dell'altro.

Anche la (iii) è pressoché ovvia: essendo a' un complemento di a, a è un complemento di a'. Anche $(a')'$ è un complemento di a'; l'unicità dei complementi nei reticoli booleani comporta $a = (a')'$.

Sempre per l'unicità del complemento, per provare la (iv) basterà mostrare che $a' \wedge b'$ è un complemento di $a \vee b$, cioè $(a \vee b) \vee (a' \wedge b') = 1$ e $(a \vee b) \wedge (a' \wedge b') = 0$. Usando la distributività e la (i), abbiamo $(a \vee b) \vee (a' \wedge b') = (a \vee b \vee a') \wedge (a \vee b \vee b') = (a \vee a' \vee b) \wedge (a \vee b \vee b') = (1 \vee b) \wedge (a \vee 1) = 1 \wedge 1 = 1$ e, in modo simmetrico, $(a \vee b) \wedge (a' \wedge b') = (a \wedge a' \wedge b') \vee (b \wedge a' \wedge b') = (a \wedge a' \wedge b') \vee (b \wedge b' \wedge a') = (0 \wedge b') \vee (0 \wedge a') = 0 \vee 0 = 0$. È così provata la (iv). La (v) segue per dualità. □

Ad illustrazione della Proposizione 12, leggiamo le identità appena provate nel caso in cui l'algebra di Boole L che appare nell'enunciato sia l'algebra delle parti di un insieme S, cioè $(\mathcal{P}(S), \cup, \cap, \varnothing, S, ^c)$, dove, come nell'Esempio 10 ^{c}: $X \in \mathcal{P}(S) \mapsto S \smallsetminus X \in \mathcal{P}(S)$. In questo caso la Proposizione 12 esprime cinque ben note formule insiemistiche elementari: per ogni $a, b \in \mathcal{P}(S)$, (i): $S \cup a = S$ e $\varnothing \cap a = \varnothing$; (ii): $S \smallsetminus S = \varnothing$ e $S \smallsetminus \varnothing = S$; (iii): $S \smallsetminus (S \smallsetminus a) = a$; (iv): $S \smallsetminus (a \cup b) = (S \smallsetminus a) \cap (S \smallsetminus b)$ e (v): $S \smallsetminus (a \cap b) = (S \smallsetminus a) \cup (S \smallsetminus b)$.

Esercizio 13. Sia $(L, \vee, \wedge, 0, 1, ')$ un'algebra di Boole. Allora anche $(L, \wedge, \vee, 1, 0, ')$ è un'algebra di Boole, quella costruita a partire dal reticolo booleano $(L, \wedge, \vee)$, il duale di $(L, \vee, \wedge)$. Verificare che l'applicazione $'$ è un isomorfismo tra queste due algebre di Boole. Questa è una riformulazione della Proposizione 12. Notare la conseguenza: ogni reticolo booleano è isomorfo al suo duale.

[(5)] oppure, per via algebrica: dal momento che 1 è neutro rispetto a $\wedge$, $1 \wedge a = a$, quindi, per una delle leggi di assorbimento, $1 = 1 \vee (1 \wedge a) = 1 \vee a$; analogamente si procede per 0.

4. Anelli booleani e algebre di Boole

In questa sezione arriveremo a provare che le nozioni di anello booleano e di reticolo booleano (ovvero di algebra di Boole) sono in sostanza interscambiabili, nel senso che si può costruire una struttura di reticolo booleano su ogni anello booleano e, viceversa, una struttura di anello booleano su ogni reticolo booleano, in modo che queste due costruzioni siano l'una inversa dell'altra.

In primo luogo, partendo da un anello booleano $(R, +, \cdot)$ vogliamo definire una struttura di reticolo booleano su R. L'esempio dell'anello delle parti di un insieme può suggerirci in che modo procedere. Fissato un insieme S, infatti, $(\mathcal{P}(S), \triangle, \cap)$ è un anello booleano ma $\mathcal{P}(S)$ è anche un reticolo booleano, con operazioni reticolari $\cup$ e $\cap$. La seconda operazione reticolare è proprio l'operazione di moltiplicazione nell'anello. Anche la prima operazione reticolare si può esprimere in termini delle operazioni dell'anello: per ogni $A, B \in \mathcal{P}(S)$ abbiamo infatti $A \cup B = (A \triangle B) \cup (A \cap B) = (A \triangle B) \triangle (A \cap B)$. Inoltre il minimo ed il massimo del reticolo sono $\varnothing$ e S, cioè lo zero e l'unità dell'anello, e ciascun $A \in \mathcal{P}(S)$ ha come complemento, nel reticolo $(\mathcal{P}(S), \subseteq)$, l'insieme $S \smallsetminus A = S \triangle A = 1_{\mathcal{P}(S)} \triangle A$.

Passando ora ad un arbitrario anello booleano $(R, +, \cdot, 0_R, 1_R)$, dove 0_R e 1_R sono lo zero l'unità dell'anello, l'esempio di $\mathcal{P}(S)$ suggerisce di definire in R l'operazione binaria $\vee$ ponendo, per ogni $a, b \in R$,

$$a \vee b := a + b + ab$$

e l'applicazione $'\colon a \in R \mapsto 1_R + a \in R$ da utilizzare come operazione unaria di complemento.

Proposizione 14. *Con le notazioni appena fissate, $(R, \vee, \cdot, 0_R, 1_R, ')$ è un'algebra di Boole.*

Dimostrazione. Dobbiamo verificare che $(R, \vee, 0_R)$ e $(R, \cdot, 1_R)$ siano monoidi commutativi, che valgano per $\vee$ e $\cdot$ le leggi di assorbimento e le proprietà distributive,[(6)] ed infine che l'applicazione $'$ verifichi la condizione richiesta dalla definizione di complemento.

Che $\vee$ sia commutativa è evidente, ed è anche chiaro che $a \vee 0_R = a + 0_R + a0_R = a$ per ogni $a \in R$, quindi 0_R è neutro rispetto a $\vee$. Proviamo l'associatività di $\vee$: per ogni $a, b, c \in R$ si ha $(a \vee b) \vee c = (a + b + ab) \vee c = (a+b+ab)+c+(a+b+ab)c = a+b+c+ab+ac+bc+abc$. Si ha quindi $a \vee (b \vee c) = (b \vee c) \vee a = b+c+a+bc+ba+ca+bca$; dunque $(a \vee b) \vee c = a \vee (b \vee c)$. È così provato che $\vee$ è associativa; $(R, \vee, 0_R)$ è quindi un monoide commutativo. Che lo sia anche $(R, \cdot, 1_R)$ è già noto in partenza, dal momento che R è un anello booleano.

Verifichiamo le leggi di assorbimento. Per ogni $a, b \in R$, $a \vee (ab) = a + ab + a(ab)$. Dal momento che R è booleano, $a(ab) = a^2b = ab$ e $ab + ab = 0_R$, quindi $a \vee (ab) = a + ab + ab = a$. Inoltre $a(a \vee b) = a(a + b + ab) = a^2 + ab + a^2b = a + ab + ab = a$. Le leggi di assorbimento sono così provate. A questo punto già possiamo concludere che $(R, \vee, \cdot)$ è un reticolo limitato.

Verifichiamo ora che $\cdot$ è distributiva rispetto a $\vee$. Per ogni $a, b, c \in R$ si ha $a(b \vee c) = a(b+c+bc) = ab+ac+abc$ e $(ab) \vee (ac) = ab + ac + (ab)(ac) = ab + ac + abc$, dunque $a(b \vee c) = (ab) \vee (ac)$. Pertanto, utilizzando anche la proprietà commutativa, possiamo concludere che $\cdot$ è distributiva rispetto a $\vee$.

Anche se non è strettamente necessario, verifichiamo anche che $\vee$ è distributiva rispetto a $\cdot$. Per ogni $a, b, c \in R$ abbiamo $a \vee (bc) = a+bc+abc$ e $(a \vee b)(a \vee c) = (a+b+ab)(a+c+ac) = a+ac+ac+ab+bc+abc+ab+abc+abc = a + bc + abc = a \vee (bc)$. Dunque, $\vee$ è distributiva rispetto a $\cdot$.

Resta infine da dimostrare che, per ogni $a \in R$, l'immagine di a mediante l'applicazione $'$, vale a dire $a' := 1_R + a$, verifica le condizioni $a \vee (1_R + a) = 1_R$ e $aa' = 0_R$. Questo è molto facile: per ogni $a \in R$ si ha $aa' = a(1_R + a) = a + a = 0_R$ e $a \vee a' = a + a' + aa' = a + (1_R + a) + 0_R = 1_R$, come richiesto. Con questo la dimostrazione è completa □

Descriviamo ora la costruzione inversa: quella di un anello booleano a partire da un'algebra di Boole. Anche in questo caso ci facciamo guidare dall'esempio dell'algebra $(\mathcal{P}(S), \cup, \cap, \varnothing, S, ^c)$ delle parti di un insieme S (come nell'Esempio 10, il simbolo ^{c} rappresenta l'operazione unaria di complemento in S). Delle due operazioni binarie dell'anello (booleano) $(\mathcal{P}(S), \triangle, \cap)$, quella di moltiplicazione, $\cap$, è già tra le operazioni dell'algebra di Boole. Per esprimere l'altra, la differenza simmetrica, utilizzando le operazioni dell'algebra di Boole ci è utile osservare che se A e B sono parti di S, allora $A \smallsetminus B = A \cap (S \smallsetminus B) = A \cap B^c$. Dunque $A \triangle B$ può essere scritta come $(A \smallsetminus B) \cup (B \smallsetminus A) = (A \cap B^c) \cup (B \cap A^c)$ o anche come $(A \cup B) \smallsetminus (A \cap B) = (A \cup B) \cap (A \cap B)^c$. Queste esempio suggerisce due possibili modi per definire, in un'arbitraria algebra di Boole $(L, \vee, \wedge, 0, 1, ')$, un'operazione binaria di addizione $+$ analoga alla differenza simmetrica in $\mathcal{P}(S)$. Il prossimo lemma mostra che queste due possibilità portano allo stesso risultato.

Lemma 15. *Sia $(L, \vee, \wedge, 0, 1, ')$ un'algebra di Boole. Allora, per ogni $a, b \in L$ si ha $(a \wedge b') \vee (a' \wedge b) = (a \vee b) \wedge (a \wedge b)'$.*

Dimostrazione. Usando la proprietà distributiva di $\vee$ rispetto a $\wedge$, abbiamo:

$$(a \wedge b') \vee (a' \wedge b) = (a \vee a') \wedge (a \vee b) \wedge (b' \vee a') \wedge (b' \vee b) = 1 \wedge (a \vee b) \wedge (b' \vee a') \wedge 1 = (a \vee b) \wedge (a' \vee b') = (a \vee b) \wedge (a \wedge b)',$$

avendo utilizzato, per l'ultimo passaggio, una delle leggi di De Morgan (Proposizione 12 (v)). □

(6) in realtà, per un'osservazione fatta a margine della definizione di reticolo distributivo, basterebbe dimostrare una sola delle due proprietà distributive.

Anche quest'altra osservazione può essere utile:

Lemma 16. *Sia $(L, \vee, \wedge, 0, 1, ')$ un'algebra di Boole. Allora, per ogni $a, b \in L$ si ha $(a \wedge b)' \wedge (a \wedge c) = a \wedge b' \wedge c$.*

Dimostrazione. Utilizzando una delle formule di De Morgan, $(a \wedge b)' \wedge (a \wedge c) = (a' \vee b') \wedge a \wedge c = \big((a' \wedge a) \vee (b' \wedge a)\big) \wedge c = \big(0 \vee (b' \wedge a)\big) \wedge c = a \wedge b' \wedge c$. □

Proposizione 17. *Sia $(L, \vee, \wedge, 0, 1, ')$ un'algebra di Boole. Se $+$ è l'operazione binaria definita in L ponendo, per ogni $a, b \in L$, $a + b = (a \wedge b') \vee (a' \wedge b)$, allora $(L, +, \wedge)$ è un anello booleano, con zero 0 e unità 1.*

Dimostrazione. Iniziamo col verificare che $(L, +)$ è un gruppo abeliano. Poiché $\vee$ e $\wedge$ sono commutative, è evidente che $+$ è commutativa. Per ogni $a, b, c \in L$ abbiamo:

$$\begin{aligned}
(a+b)+c &= \big((a \wedge b') \vee (a' \wedge b)\big) + c \\
&= \big(\big((a \wedge b') \vee (a' \wedge b)\big) \wedge c'\big) \vee \big(\big((a \wedge b') \vee (a' \wedge b)\big)' \wedge c\big) \\
&= \big(\big((a \wedge b') \vee (a' \wedge b)\big) \wedge c'\big) \vee \big(\big((a \vee b) \wedge (a \wedge b)'\big)' \wedge c\big) && \text{[usando il Lemma 15]} \\
&= \big(\big((a \wedge b') \vee (a' \wedge b)\big) \wedge c'\big) \vee \big(\big((a' \wedge b') \vee (a \wedge b)\big) \wedge c\big) && \text{[usando la Proposizione 12]} \\
&= \big((a \wedge b' \wedge c') \vee (a' \wedge b \wedge c')\big) \vee \big((a' \wedge b' \wedge c) \vee (a \wedge b \wedge c)\big) \\
&= (a \wedge b' \wedge c') \vee (a' \wedge b \wedge c') \vee (a' \wedge b' \wedge c) \vee (a \wedge b \wedge c).
\end{aligned}$$

Poiché $+$ è commutativa, abbiamo quindi anche $a+(b+c) = (b+c)+a = (b \wedge c' \wedge a') \vee (b' \wedge c \wedge a') \vee (b' \wedge c' \wedge a) \vee (b \wedge c \wedge a)$ ed allora, per la commutatività di $\wedge$ e $\vee$, $a + (b + c) = (a + b) + c$. Pertanto $+$ è associativa. Per ogni $a \in L$ vale $a + 0 = (a \wedge 0') \vee (a' \wedge 0) = (a \wedge 1) \vee 0 = a \vee 0 = a$, quindi 0 è neutro rispetto a $+$. Inoltre, sempre per ogni $a \in L$, $a + a = (a \wedge a') \vee (a' \wedge a) = 0 \vee 0 = 0$, quindi ogni elemento di L, rispetto a $+$, è il simmetrico di sé stesso. Dunque $(L, +)$ è un gruppo abeliano, con elemento neutro 0.
Sappiamo dalla definizione di algebra di Boole che $(L, \wedge, 1)$ è un monoide commutativo. Verifichiamo la distributività di $\wedge$ rispetto a $+$. Per ogni $a, b, c \in L$ abbiamo:

$$a \wedge (b + c) = a \wedge \big((b \wedge c') \vee (b' \wedge c)\big) = (a \wedge b \wedge c') \vee (a \wedge b' \wedge c)$$

e, utilizzando due volte il Lemma 16,

$$(a \wedge b) + (a \wedge c) = \big((a \wedge b) \wedge (a \wedge c)'\big) \vee \big((a \wedge b)' \wedge (a \wedge c)\big) = (a \wedge b \wedge c') \vee (a \wedge b' \wedge c),$$

quindi $a \wedge (b + c) = (a \wedge b) + (a \wedge c)$.
A questo punto abbiamo dimostrato che $(L, +, \wedge)$ è un anello (commutativo) unitario, con 0 e 1 come zero e unità. Per ogni $a \in L$ vale $a^2 = a \wedge a = a$, quindi questo anello è booleano. La dimostrazione è così completa. □

Abbiamo così visto che ogni anello booleano $(R, +, \cdot)$ determina una struttura di algebra di Boole sul suo stesso sostegno: $(R, \vee, \cdot, 0_R, 1_R, ')$, definita come nella Proposizione 14. Per la Proposizione 17, questa definisce a sua volta un anello booleano, indichiamolo come $(R, \oplus, \cdot)$, con operazione additiva $\oplus$ definita da: per ogni $a, b \in R$

$$a \oplus b = (ab') \vee (a'b) \in R.$$

Ora, scelti comunque $a, b \in R$, poiché, in accordo con la Proposizione 14, per ogni $u, v \in R$, abbiamo $u' = 1_R + u$ (e $uu' = 0_R$) e $u \vee v = u + v + uv$,

$$(ab') \vee (a'b) = (ab') + (a'b) + (ab')(a'b) = (ab') + (a'b) + aa'bb' = a(1_R + b) + (1_R + a)b + 0_R = a + ab + b + ab = a + b,$$

ricordando che $ab + ab = 0_R$. Dunque, l'operazione additiva $\oplus$ dell'anello booleano costruito a partire da $(R, \vee, \cdot, 0_R, 1_R, ')$ non è altro che l'originale addizione in $(R, +, \cdot)$.

Questo significa che, dato un anello booleano R, se si costruisce un'algebra di Boole su R come indicato nella Proposizione 14 e poi, a partire da quest'ultima, si costruisce un anello booleano come indicato nella Proposizione 17, questo anello è precisamente l'anello R da cui si era partiti.

Lo stesso vale se si fa il discorso inverso. Se, partendo da un'algebra di Boole $(L, \vee, \wedge, 0, 1, ')$, si definisce l'anello booleano $(L, +, \wedge)$ come nella Proposizione 17 e poi si usa la Proposizione 14 per costruire un'algebra di Boole $(L, \curlyvee, \wedge, 0, 1, '')$ a partire da questo anello, l'algebra così ottenuta è quella originaria. Per provarlo, basta verificare che l'operazione $\curlyvee$ coincide con $\vee$. Infatti, una volta stabilito ciò, si ha che le due strutture di reticolo booleano su L, l'originale $(L, \vee, \wedge)$ e la "nuova" $(L, \curlyvee, \wedge)$, coincidono, quindi lo stesso è vero per le corrispondenti algebre di Boole.

⚠ Verifichiamo $\curlyvee = \vee$. Scelti comunque $a, b \in L$, le costruzioni in Proposizione 17 e Proposizione 14 dànno $a + b = (a \wedge b') \vee (a' \wedge b)$ e $a \curlyvee b = a + b + (a \wedge b)$. Ma $b = 1 \wedge b$ e, usando la proprietà distributiva di $\wedge$ rispetto a $+$,

$$\begin{aligned} a \curlyvee b &= a + (1 \wedge b) + (a \wedge b) = a + \big((1 + a) \wedge b\big) \\ &= a + (a' \wedge b) && \text{[perché } a' = 1 + a\text{]} \\ &= \big(a \wedge (a' \wedge b)'\big) \vee \big(a' \wedge a' \wedge b\big) \\ &= \big(a \wedge (a \vee b')\big) \vee \big(a' \wedge b\big) && \text{[legge di De Morgan]} \\ &= a \vee (a' \wedge b) && \text{[legge di assorbimento]} \\ &= (a \vee a') \wedge (a \vee b) = 1 \wedge (a \vee b) = a \vee b. \end{aligned}$$

Quindi, effettivamente, $\curlyvee$ coincide con $\vee$. Possiamo sintetizzare quanto abbiamo dimostrato nel seguente teorema.

Teorema 18. *Sia L un insieme. Sia $\mathcal{A}$ l'insieme delle coppie ordinate $(\vee, \wedge)$ di operazioni binarie in L che strutturano L come algebra di Boole, e sia $\mathcal{B}$ l'insieme delle coppie ordinate $(+, \cdot)$ di operazioni binarie in L che strutturano L come anello booleano. Allora le costruzioni descritte dalla Proposizione 14 e dalla Proposizione 17 definiscono due applicazioni, da $\mathcal{B}$ a $\mathcal{A}$ e da $\mathcal{A}$ a $\mathcal{B}$, che sono l'una inversa dell'altra, quindi biettive.*

Questa corrispondenza tra algebre di Boole e anelli booleani conserva la nozione di isomorfismo.

Proposizione 19. *Siano $(L_1, \vee_1, \wedge_1, 0_1, 1_1, ')$ e $(L_2, \vee_2, \wedge_2, 0_2, 1_2, '')$ algebre di Boole e $(L_1, +_1, \wedge_1)$ e $(L_2, +_2, \wedge_2)$ i corrispondenti (nel senso del Teorema 18) anelli booleani. Sia poi $f \colon L_1 \to L_2$ un'applicazione biettiva. Allora f è un isomorfismo di algebre di Boole se e solo se è un isomorfismo di anelli booleani.*

Dimostrazione. Sia f un isomorfismo di algebre di Boole. Allora, per ogni $a, b \in L_1$ si ha

$$f(a +_1 b) = f\big((a \vee_1 b') \wedge_1 (a' \vee_1 b)\big) = \big(f(a) \vee_2 f(b)''\big) \wedge_2 \big(f(a)'' \vee_2 f(b)\big) = f(a) +_2 f(b)$$

e, ovviamente, $f(a \wedge_1 b) = f(a) \wedge_2 f(b)$. Quindi f è un isomorfismo di anelli booleani. Viceversa, se f è un isomorfismo di anelli booleani, allora, per ogni $a, b \in L_1$ si ha $f(a \wedge_1 b) = f(a) \wedge_2 f(b)$ e

$$f(a \vee_1 b) = f\big(a +_1 b +_1 (a \wedge_1 b)\big) = f(a) +_2 f(b) +_2 \big(f(a) \wedge_2 f(b)\big) = f(a) \vee_2 f(b).$$

Dunque f conserva le operazioni reticolari ed è quindi un isomorfismo di reticoli da L_1 a L_2. Come già sappiamo dalla sezione 4, da ciò segue che f è un isomorfismo di algebre di Boole. □

A questo punto possiamo concludere che lo studio degli anelli booleani equivale a quello delle algebre di Boole, e quindi a quello dei reticoli booleani. Vediamo anche che le sottoalgebre di Boole corrispondono precisamente ai sottoanelli unitari.

Proposizione 20. *Sia $(L, \vee, \wedge, 0, 1, ')$ un'algebra di Boole e sia $(L, +, \wedge)$ il corrispondente anello booleano (nel senso del Teorema 18). Sia $K \subseteq L$. Allora K è una sottoalgebra di Boole di $(L, \vee, \wedge, 0, 1, ')$ se e solo se è un sottoanello unitario di $(L, +, \wedge)$.*

Dimostrazione. Sia K una sottoalgebra di Boole. Allora, per ogni $a, b \in K$, si ha $a + b = (a \wedge b') \vee (a' \wedge b) \in K$, quindi K è chiusa rispetto a $+$. Dal momento che $(L, +, \wedge)$ è booleano, ogni elemento di L coincide col suo opposto. Da ciò segue che K è un sottogruppo di $(L, +)$. Ovviamente, poiché K è una sottoalgebra, K è un sottomonoide di $(K, \wedge, 1)$. Dunque, K è un sottoanello unitario di $(L, +, \wedge)$.

Viceversa, se K è un sottoanello unitario di $(L, +, \wedge)$, allora K è un sottomonoide di $(L, \wedge, 1)$. Inoltre $0 \in K$, per ogni $a \in K$ si ha $a' = 1 + a \in K$ e dunque, per ogni $a, b \in K$, $a \vee b = (a \wedge b') + (a' \wedge b) \in K$. Concludiamo che K è anche un sottomonoide di $(L, \vee, 0)$ e contiene il complemento in L di ogni suo elemento. Dunque, K è una sottoalgebra di Boole di $(L, \vee, \wedge, 0, 1, ')$. □

Da questi ultimi risultati e dal teorema di Stone per anelli booleani seguono subito i teoremi di Stone per algebre di Boole e per reticoli booleani.

Teorema di Stone (per algebre di Boole)**.** *Sia L un'algebra di Boole. Allora:*

(i) *esiste un insieme S tale che L sia isomorfa ad una sottoalgebra di Boole dell'algebra delle parti $(\mathcal{P}(S), \cup, \cap, \varnothing, S, ^c)$ di S;*
(ii) *se L è finita, esiste un insieme S tale che L sia isomorfa all'algebra delle parti $(\mathcal{P}(S), \cup, \cap, \varnothing, S, ^c)$ di S.*

Teorema di Stone (per reticoli booleani)**.** *Sia L un reticolo booleano. Allora:*

(i) *esiste un insieme S tale che L sia isomorfo ad un sottoreticolo del reticolo $(\mathcal{P}(S), \subseteq)$ delle parti di S;*
(ii) *se L è finito, esiste un insieme S tale che L sia isomorfo al reticolo $(\mathcal{P}(S), \subseteq)$ delle parti di S.*

Naturalmente, in conseguenza di questi teoremi, valgono anche per le algebre di Boole finite ed i reticoli booleani finiti le conseguenze osservate nel Corollario 3 per gli anelli booleani: tutte le algebre di Boole finite e tutti i reticoli booleani finiti hanno per cardinalità una potenza di 2; se due algebre di Boole finite sono equipotenti (cioè hanno lo stesso numero di elementi) allora esse sono isomorfe; se due reticoli booleani finiti sono equipotenti allora essi sono isomorfi.

5. Anelli booleani, stringhe di zeri e uno ed operazioni bit a bit

In questa sezione faremo alcune osservazioni ed esempi su una delle situazioni in cui, in informatica, capita di incontrare strutture booleane.

Iniziamo da un accenno ad una costruzione generale. Fissiamo un anello R ed un intero positivo n. L'insieme R^n delle n-ple di elementi di R si può strutturare come anello definendo operazioni binarie di addizione e moltiplicazione "componente per componente", cioè in questo modo: per ogni $\underline{a} = (a_1, a_2, \dots, a_n)$ e $\underline{b} = (b_1, b_2, \dots, b_n)$ appartenenti a R si pone

$$\underline{a} + \underline{b} = (a_1 + b_1, a_2 + b_2, \dots, a_n + b_n) \qquad \text{e} \qquad \underline{a} \cdot \underline{b} = (a_1 b_1, a_2 b_2, \dots, a_n b_n); \tag{$*$}$$

abbiamo indicato con $+$ e $\cdot$ sia le operazioni in R che quelle in R^n. È un semplice esercizio la verifica del fatto che in questo modo R^n si struttura come anello (con $(0_R, 0_R, \dots, 0_R)$ come zero e, se R è unitario, $(1_R, 1_R, \dots, 1_R)$ come unità) e che R^n è booleano se R è booleano.

Consideriamo il caso in cui R è l'anello $\mathbb{Z}_2$ degli interi modulo 2. Dal momento che $\mathbb{Z}_2$ è booleano, anche $\mathbb{Z}_2^n$ è booleano. I suoi elementi sono le n-ple di elementi di $\mathbb{Z}_2$, quindi le n-ple $(a_1, a_2, \dots, a_n)$ dove ciascuno degli a_i è uno dei due elementi di $\mathbb{Z}_2$: o $[0]_2$ oppure $[1]_2$. Ovviamente $|\mathbb{Z}_2^n| = 2^n$. Per semplificare la notazione possiamo scrivere 0 e 1 per $[0]_2$ e $[1]_2$ e rappresentare le n-ple come stringhe di lunghezza n, vale a dire, se, ad esempio, $n = 5$, scriviamo '$a_1a_2a_3a_4a_5$' piuttosto che $(a_1, a_2, a_3, a_4, a_5)$. Per esempio, sempre per $n = 5$, la stringa '10100' sta per $([1]_2, [0]_2, [1]_2, [0]_2, [0]_2) \in \mathbb{Z}_2^5$.

Con queste notazioni, dette $\underline{a} =$ '$a_1a_2 \dots a_n$' e $\underline{b} =$ '$b_1b_2 \dots b_n$' due stringhe appartenenti a $\mathbb{Z}_2^n$, abbiamo $\underline{a} + \underline{b} =$ '$s_1s_2 \dots s_n$' e $\underline{a} \cdot \underline{b} =$ '$p_1p_2 \dots p_n$', dove, per ogni $i \in \{1, 2, \dots, n\}$, s_i è la somma e p_i il prodotto di a_i e b_i in $\mathbb{Z}_2$, quindi $s_i = 0$ se $a_i = b_i$ e $s_i = 1$ se $a_i \neq b_i$, mentre $p_i = 1$ se $a_i = b_i = 1$ e $p_i = 0$ negli altri casi.

Molto probabilmente, chi legge riconosce in queste regole di calcolo le operazioni 'bit a bit' su "stringhe di zeri e uno" di fissata lunghezza con cui funzionano gli elaboratori elettronici, associate ai connettivi (operatori) logici XOR e AND. Quello che stiamo qui dicendo è che

queste operazioni 'bit a bit' non sono altro che le due operazioni binarie dell'anello booleano $\mathbb{Z}_2^n$.

Naturalmente lo stesso discorso si può estendere alle operazioni che, ai sensi della Proposizione 14, strutturano $\mathbb{Z}_2^n$ come algebra di Boole. Indicando con $\underline{1}$ la stringa '$11 \dots 1$' (di lunghezza n), che è l'unità di $\mathbb{Z}_2^n$, il complemento di $\underline{a} =$ '$a_1a_2 \dots a_n$' in $\mathbb{Z}_2^n$ sarà $\underline{1} + \underline{a}$ che, come si verifica subito, è la stringa ottenuta sostituendo in $\underline{a}$ ogni 0 con 1 ed ogni 1 con 0; quello che abbiamo descritto è l'operatore NOT. Se poi $\underline{b} =$ '$b_1b_2 \dots b_n$' $\in \mathbb{Z}_2^n$, è facile verificare che $\underline{a} \vee \underline{b} =$ '$l_1l_2 \dots l_n$', dove, per ogni i, $l_i = 0$ se $a_i = b_i = 0$ e $l_i = 1$ altrimenti; un modo per farlo è osservare che per le leggi di De Morgan (Proposizione 12) $\underline{a} \vee \underline{b} = \underline{1} + \big((\underline{1} + \underline{a})(\underline{1} + \underline{b})\big)$. Dunque $\vee$ coincide con l'operatore OR bit a bit.

Esercizio 21. Verificare la correttezza della definizione dell'anello R^n data all'inizio di questa sezione e le proprietà di R^n lì indicate.

Più in generale, siano n un intero positivo e $(R_1, +_1, \cdot_1)$, $(R_2, +_2, \cdot_2), \dots, (R_n, +_n, \cdot_n)$ anelli. Sia P il prodotto cartesiano $R_1 \times R_2 \times \cdots \times R_n$ e definiamo in P due operazioni binarie $+$ e $\cdot$ ponendo, per ogni $\underline{a} = (a_1, a_2, \dots, a_n), \underline{b} = (b_1, b_2, \dots, b_n) \in P$, come in $(*)$, $\underline{a} + \underline{b} = (a_1 +_1 b_1, a_2 +_2 b_2, \dots, a_n +_n b_n)$ e $\underline{a} \cdot \underline{b} = (a_1 \cdot_1 b_1, a_2 \cdot_2 b_2, \dots, a_n \cdot_n b_n)$. Verificare che $(P, +, \cdot)$ è un anello e che questo anello è unitario (rispettivamente, commutativo, booleano) se ciascuno degli anelli R_i ha la stessa proprietà.

Infine, vediamo cosa di altro possiamo dire sull'anello $\mathbb{Z}_2^n$ alla luce del teorema di Stone. Innanzitutto, (continuando a indicare con n un intero positivo fissato) cosa sono le n-ple di elementi di $\mathbb{Z}_2$? Una maniera per rispondere è assumere che, per definizione, una n-pla di elementi di $\mathbb{Z}_2$ sia un'applicazione da $S := \{1, 2, \dots, n\}$ a $\mathbb{Z}_2$: la n-pla $\underline{a} =$ '$a_1a_2 \dots a_n$' è l'applicazione $i \in S \mapsto a_i \in \mathbb{Z}_2$. Quindi l'insieme $\mathbb{Z}_2^n$ è l'insieme $\mathbb{Z}_2^S$ delle applicazioni da S a $\mathbb{Z}_2$.

A questo punto ci viene in aiuto la nozione insiemistica di funzione caratteristica. Se X è una parte di S, la funzione caratteristica di X in S (a valori in $\mathbb{Z}_2$) è l'applicazione

$$\chi_{X,S} \colon i \in S \longmapsto \begin{cases} 1, & \text{se } i \in X \\ 0, & \text{se } i \notin X \end{cases} \in \mathbb{Z}_2.$$

Si ricorda che l'applicazione $X \in \mathcal{P}(S) \mapsto \chi_{X,S} \in \mathbb{Z}_2^S$ è biettiva; l'applicazione inversa è quella che associa, ad ogni applicazione $f \colon S \to \mathbb{Z}_2$, l'antiimmagine di $\{1\}$ mediante f. Dunque, ricordano anche che $\mathbb{Z}_2^S = \mathbb{Z}_2^n$ e continuando a scrivere gli elementi di questo insieme come stringhe di lunghezza n, la stringa (funzione) caratteristica di una parte di S è la stringa '$a_1a_2 \dots a_n$', dove per ogni $i \in S$ si ha $a_i = 1$ se $i \in X$ e $a_i = 0$ se $i \notin X$; viceversa, una stringa '$a_1a_2 \dots a_n$' corrisponde all'insieme degli $i \in S$ tali che $a_i = 1$.

Facciamo un esempio per chiarire ulteriormente questa coppia di applicazioni biettive. Assumendo $n = 7$,

la stringa	è	la 7-pla	e corrisponde a	l'insieme
'1011010'		$([1]_2, [0]_2, [1]_2, [1]_2, [0]_2, [1]_2, [0]_2)$		$\{1, 3, 4, 6\}$

Ora, per il teorema di Stone l'anello $(\mathbb{Z}_2^n, +, \cdot)$ è isomorfo all'anello delle parti di un insieme. Poiché $|\mathbb{Z}_2^n| = 2^n$ e $|S| = n$, dobbiamo avere $\mathbb{Z}_2^n \simeq (\mathcal{P}(S), \triangle, \cap)$. In effetti, possiamo verificare che l'applicazione biettiva appena descritta è un isomorfismo.

Proposizione 22. *Siano n un intero positivo e $S = \{1, 2, \dots, n\}$. L'applicazione φ che ad ogni parte X di S associa la stringa che rappresenta la funzione caratteristica di X in S è un isomorfismo di anelli booleani da $(\mathcal{P}(S), \triangle, \cap)$ a $(\mathbb{Z}_2^n, +, \cdot)$.*

Dimostrazione. Siano A e B parti di S, e siano $\underline{a} = `a_1 a_2 \dots a_n' = \varphi(A)$ e $\underline{b} = `b_1 b_2 \dots b_n' = \varphi(B)$. Allora, per ogni $i \in S$, $a_i = 1$ se e solo se $i \in A$ (risultando $a_i = 0$ altrimenti); similmente $b_i = 1$ se e solo se $i \in B$. Sia $\underline{c} = `c_1 c_2 \dots c_n' = \varphi(A \cap B)$. Allora, per ogni $i$, $c_i = 1$ se e solo se $i \in A \cap B$, cioè se e solo se $a_i = b_i = 1$. Da ciò è chiaro che $\underline{c} = \underline{a} \cdot \underline{b}$. Sia poi $d = `d_1 d_2 \dots d_n' = \varphi(A \triangle B)$. Allora, per ogni $i \in S$, $d_i = 1$ se e solo se $i \in A \triangle B$, cioè se e solo se vale esattamente una tra $i \in A$ e $i \in B$, cioè se e solo se, tra a_i e b_i uno è 1 e l'altro è 0. Se ne ricava: $\underline{d} = \underline{a} + \underline{b}$. Abbiamo così provato che φ è un isomorfismo. □

Possiamo in definitiva concludere che lavorare su stringhe di zeri e uno di fissata lunghezza n utilizzando le operazioni 'bit a bit' è del tutto equivalente a lavorare nell'anello (booleano) delle parti dell'insieme S. La moltiplicazione 'bit a bit' (operatore AND) corrisponde all'operazione di intersezione, l'addizione (modulo 2, operatore XOR) corrisponde all'operazione di differenza simmetrica.

Ad esempio, se, come sopra, $n = 7$ e $\underline{a} =$ '1011010', ed inoltre $\underline{b} =$ '0011100', allora $\underline{a}$ e $\underline{b}$ corrispondono ai sottoinsiemi $A = \{1, 3, 4, 6\}$ e $B = \{3, 4, 5\}$ di $\{1, 2, 3, 4, 5, 6, 7\}$, e possiamo completare come segue una tabella in cui le stringhe al primo rigo corrispondono ad insiemi al secondo rigo:

$\underline{a} =$ '1011010'	$\underline{b} =$ '0011100'	$\underline{a} + \underline{b} =$ '1000110'	$\underline{a} \cdot \underline{b} =$ '0011000'
$A = \{1, 3, 4, 6\}$	$B = \{3, 4, 5\}$	$A \triangle B = \{1, 5, 6\}$	$A \cap B = \{3, 4\}$