# 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 $\sigma_a$ 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 $\sigma_a$ è definita come sopra, sono equivalenti:*
*(i) $a$ è cancellabile a sinistra in $(S, *)$;*
*(ii) $\sigma_a$ è iniettiva;*
*(iii) $\sigma_a$ è suriettiva;*
*(iv) $\sigma_a$ 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 $\sigma_a$ è iniettiva, vale a dire: $(i) \iff (ii)$. D'altra parte $\sigma_a$ 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 $\sigma_a$ 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 $\sigma_a$ è iniettiva, $s * x = x$. Ciò prova che $s$ è neutro a sinistra in $(S, *)$. Infine, ancora per la suriettività di $\sigma_a$, 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 $\delta_a$ è definita come sopra, sono equivalenti:*
*(i) $a$ è cancellabile a destra in $(S, *)$;*
*(ii) $\delta_a$ è iniettiva;*
*(iii) $\delta_a$ è suriettiva;*
*(iv) $\delta_a$ 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.