NOTE INTRODUTTIVE DI ALGEBRA PER IL CORSO DI GEOMETRIA I DELL'UNIVERSITÀ DEGLI STUDI DI TRENTO

EMANUELE BOTTAZZI

Versione aggiornata al 9 dicembre 2014*

Indice

1. Introduzione

Lo scopo di queste note è di fornire alcuni elementi introduttivi di algebra che possono interessare agli studenti del corso di Geometria I. Le note non hanno alcuna pretesa di completezza, ma vogliono aiutare a fissare qualche idea. Ci saranno alcune definizioni, molti esempi (che si spera aiutino a suscitare interesse nei confronti degli oggetti definiti) e nessun "teorema".

1.1. **Consigli per la lettura e note tecniche.** Ai fini di godersi meglio il corso di Geometria I offerto dall'Università di Trento nell'anno accademico 2014/2015, l'unica sezione strettamente utile è la 2, dove viene data rapidamente la definizione di campo e viene fatto qualche esempio più e meno usuale. Le altre sezioni sono di lettura opzionale, in quanto costituiscono

*Eventuali versioni successive sono reperibili alla pagina `http://www.science.unitn.it/~bottazzi/geometria1415.html`.

una prima visita turistica alle meraviglie dell'algebra. Il loro scopo primario è di mostrare il cammino che un algebrista intraprende per definire il concetto di campo.

Qualsiasi sia l'uso che si voglia fare di queste note, mi preme sottolineare che esse *non costituiscono in alcun modo materiale d'esame* e nessuno studente verrà penalizzato per non averle lette.

Due note sulla simbologia:

- gli esempi segnati dal simbolo ♡ sono più complessi rispetto agli altri, e possono essere tranquillamente saltati;
- le affermazioni seguite dal simbolo (♠) sono vere ma non ovvie, quindi andrebbero dimostrate.

1.2. **Un avvertimento, una richiesta e il "paradosso dell'introduzione".** Leggendo queste note, vi prego di fare attenzione: certamente ci saranno alcuni errori. Se ne trovate qualcuno, vi chiederei la cortesia di segnalarmelo con una mail all'indirizzo `emanuele.bottazzi@unitn.it`, così che lo possa correggere.

Scrivendo la frase "certamente [queste note] contengono alcuni errori", mi sono deliberatamente esposto alla mia versione preferita del cosiddetto "paradosso dell'introduzione", che sostanzialmente consiste nel seguente argomento:

(1) se nelle note ci sono errori, allora l'affermazione è vera (questo è il caso noioso, che tristemente è anche il più probabile);
(2) se nelle note non ci sono errori, allora l'affermazione è falsa, ma quindi è un errore, e quindi è vera, e quindi non è un errore, e quindi è falsa...

2. Campi, la definizione veloce

Intuitivamente, un campo è un insieme sul quale sono definiti una "somma" ed un "prodotto", e dove si possono eseguire le "sottrazioni" e le "divisioni". Queste due ultime proprietà di solito vengono espresse richiedendo l'esistenza degli inversi additivi e moltiplicativi. Formalmente, abbiamo:

Definizione 2.1. Un *campo* è una 5-upla ordinata $(F, +, \cdot, 0, 1)$, dove:

- $F \neq \emptyset$ è un insieme;
- $0, 1 \in F$;
- $+ : F \times F \to F$ e $\cdot : F \times F \to F$ soddisfano le proprietà:
  (1) (Associatività) per ogni $x, y, z \in F$ valgono
  $$(x + y) + z = x + (y + z) \quad \text{e} \quad (x \cdot y) \cdot z = x \cdot (y \cdot z)$$
  (2) (Elemento neutro per la somma) per ogni $x \in F$ vale
  $$x + 0 = 0 + x = x$$
  (2') (Elemento neutro per il prodotto) per ogni $x \in F$ vale
  $$x \cdot 1 = 1 \cdot x = x$$

(3) (Esistenza dell'inverso additivo) per ogni $x \in F$ esiste $-x \in F$ che soddisfa
$$x + (-x) = (-x) + x = 0$$
(3') (Esistenza dell'inverso moltiplicativo) per ogni $x \in F$, se $x \neq 0$ esiste $x^{-1} \in F$ che soddisfa
$$x \cdot x^{-1} = x^{-1} \cdot x = 1$$
(4) (Commutatività della somma) per ogni $x, y \in F$
$$x + y = y + x$$
(4') (Commutatività del prodotto) per ogni $x, y \in F$
$$x \cdot y = y \cdot x$$
(5) (Distributività del prodotto rispetto alla somma) per ogni $x, y, z \in F$
$$x \cdot (y + z) = x \cdot y + x \cdot z$$
(in questa formula abbiamo usato la convenzione che il prodotto viene eseguito prima della somma).

Se le operazioni e i rispettivi elementi neutri sono famigliari, si usa anche dire che F è un campo. Quindi, ad esempio, diciamo che $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sono dei campi, e non c'è bisogno di dire esplicitamente "$(\mathbb{Q}, +, \cdot, 0, 1)$ è un campo" invece di "$\mathbb{Q}$ è un campo".

2.1. **Esempi di campi.** Oltre ai campi numerici $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, ci sono diversi altri campi di uso più o meno comune in matematica. Il primo esempio è decisamente banale, ma divertente.

Esempio 2.2 (Il campo banale)**.** Consideriamo $\{e\}$, un insieme con un solo elemento, e definiamo le operazioni in questo modo:
$$e + e = e \cdot e = e$$
È semplice verificare che $(\{e\}, +, \cdot, e, e)$ è un campo (♠). Questo è il campo più piccolo possibile: tutti gli altri campi hanno almeno due elementi. Questo è anche l'unico campo in cui la somma ed il prodotto coincidono (♠), ed è interessante cercare di scoprire il perchè.

I campi discussi nel prossimo esempio sono molto rilevanti per la teoria dei numeri e la crittografia.

Esempio 2.3 (Campi finiti)**.** Sia $p \in \mathbb{N}$ un numero primo. Consideriamo l'insieme $\mathbb{Z}_p = \{0, 1, \ldots, p-1\} \subset \mathbb{Z}$, e su questo insieme definiamo le operazioni $+_p, \cdot_p : \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p$ ponendo
$$a +_p b = \begin{cases} a + b & \text{se } a + b < p \\ a + b - p & \text{se } a + b \geq p \end{cases}$$
e
$$a \cdot_p b = \begin{cases} ab & \text{se } ab < p \\ ab - kp & \text{se } (k+1)p > ab \geq kp \text{ (con } k \geq 1) \end{cases}$$

Di solito queste operazioni si chiamano somma e prodotto *modulo* p, e si indicano così:

$$a +_p b = a + b \mod p$$

e

$$a \cdot_p b = ab \mod p$$

Si può verificare che $(\mathbb{Z}_p, +_p, \cdot_p, 0, 1)$ è un campo (♠). I campi della forma $\mathbb{Z}_p$ si chiamano *campi finiti* perchè, appunto, hanno un numero finito di elementi.

Osservazione 2.4. Le operazioni modulo n si possono definire per ogni $n \in \mathbb{N} \setminus \{0\}$[†], ma $(\mathbb{Z}_n, +_n, \cdot_n, 0, 1)$ è un campo se e solo se $n = 1$ o n è primo (♠). Gli studenti più appassionati possono provare a dimostrare quest'affermazione. Nell'esempio 4.4 approfondiremo le proprietà di $\mathbb{Z}_n$ con n composto.

Esempio 2.5 (♡ – Un'estensione di $\mathbb{R}$)**.** In questo esempio costruiremo un campo che estende il campo dei numeri reali. Prendiamo $\alpha \notin \mathbb{R}$ (possiamo pensare ad α come a un simbolo per un "nuovo numero") e definiamo l'insieme

$$R(\alpha) = \{p(\alpha)/q(\alpha) \mid p, q \in \mathbb{R}[x] \text{ e } q \neq 0\}$$

In altre parole, un generico oggetto di $R(\alpha)$ è un quoziente di polinomi "valutato" in α. Dato che i polinomi costanti sono elementi di $\mathbb{R}[x]$, è interessante osservare esplicitamente che $R(\alpha)$ contiene tutti i numeri reali, oltre a nuovi oggetti tra i quali ad esempio

$$\alpha \ ; \ \frac{\alpha^2 - 1}{\alpha - 1} \ ; \ -8\alpha + 12 - \alpha^{-57}$$

Tecnicamente, a questo punto è necessario definire su $R(\alpha)$ la relazione

$$\frac{p(\alpha)}{q(\alpha)} \simeq \frac{r(\alpha)}{s(\alpha)} \iff p(\alpha)s(\alpha) = q(\alpha)r(\alpha)$$

Questa relazione è analoga a quella definita sull'insieme delle frazioni di numeri interi per ottenere il campo dei numeri razionali. Infatti, si verifica che $\simeq$ è una *relazione di equivalenza* (♠). Chiamiamo $\mathbb{R}(\alpha)$ l'insieme delle classi di equivalenza di questa relazione:

$$\mathbb{R}(\alpha) = R(\alpha)/\simeq$$

I suoi elementi sono quozienti di polinomi coprimi (i.e. senza fattori comuni). In altre parole, se $p(\alpha)/q(\alpha) \in \mathbb{R}(\alpha)$, allora non esiste nessun polinomio $h(\alpha) \neq 1$ in $\mathbb{R}[\alpha]$ che soddisfa

$$p(\alpha) = h(\alpha)p'(\alpha) \quad \text{e} \quad q(\alpha) = h(\alpha)q'(\alpha)$$

[†]Anche se per $n = 1$ otteniamo nuovamente il campo banale visto nell'esempio 2.2 (♠).

per qualche p' e $q' \in \mathbb{R}[\alpha]$[‡]. Ad esempio, gli oggetti seguenti appartengono a $\mathbb{R}(\alpha)$:

$$1 \ ; \ 57 \ ; \ 57\alpha^9 \ ; \ \frac{57\alpha^9 - 2\alpha^7 + \pi}{\alpha - 7} \ ; \ -\alpha^{-2}$$

mentre invece

$$\frac{\alpha^2 - 1}{\alpha - 1}$$

è un elemento $R(\alpha)$ che non appartiene a $\mathbb{R}(\alpha)$. Dato che

$$\frac{\alpha^2 - 1}{\alpha - 1} \simeq \alpha + 1$$

e $\alpha + 1$ è "ridotto ai minimi termini", deduciamo che $\alpha + 1$ *rappresenta* $(\alpha^2 - 1)/(\alpha - 1)$ in $\mathbb{R}(\alpha)$ (analogamente a come 2 *rappresenta* 197252/9876 in $\mathbb{Q}$).

Su $\mathbb{R}(\alpha)$ possiamo definire le operazioni di somma e prodotto in analogia alla somma e prodotto tra quozienti di polinomi. Quindi, valgono le similitudini

$$\frac{p(\alpha)}{q(\alpha)} \cdot \frac{r(\alpha)}{s(\alpha)} \simeq \frac{p(\alpha)r(\alpha)}{q(\alpha)s(\alpha)}$$

e

$$\frac{p(\alpha)}{q(\alpha)} + \frac{r(\alpha)}{s(\alpha)} \simeq \frac{p(\alpha)s(\alpha) + r(\alpha)q(\alpha)}{q(\alpha)s(\alpha)}$$

Ad esempio,

$$57 + \frac{57\alpha^9 + \pi}{\alpha^2} - \alpha^{-2} = \frac{57\alpha^9 + 57\alpha^2 - 1 + \pi}{\alpha^2}$$

Con queste operazioni si può verificare che 0 è l'elemento neutro per la somma, 1 è l'elemento neutro per il prodotto,

$$-\left(\frac{p(\alpha)}{q(\alpha)}\right) = \frac{-p(\alpha)}{q(\alpha)}$$

e, se $p(\alpha) \neq 0$, allora

$$\left(\frac{p(\alpha)}{q(\alpha)}\right)^{-1} = \frac{q(\alpha)}{p(\alpha)}$$

Quindi $(\mathbb{R}(\alpha), +, \cdot, 0, 1)$ è un campo.

3. Gruppi

La strada che viene seguita in algebra per introdurre la definizione di campo è di solito lunga, tortuosa ed estremamente interessante. In queste note taglieremo tutte le deviazioni panoramiche e cercheremo di arrivare alla meta nel minor tempo possibile. La partenza comunque rimane la definizione di gruppo, uno degli oggetti algebrici più interessanti, versatili ed affascinanti.

Definizione 3.1. Un *gruppo* è una terna $(G, \circ, e)$, dove:

[‡]Attenzione: la differenza tra $\mathbb{R}(\alpha)$ e $\mathbb{R}[\alpha]$ qui gioca un ruolo cruciale.

- G è un insieme;
- $e \in G$;
- $\circ : G \times G \to G$ è una funzione che soddisfa le proprietà:
  (1) (Associatività) per ogni $x, y, z \in G$ vale
  $$x \circ (y \circ z) = (x \circ y) \circ z$$
  (e quindi le parentesi si possono omettere e si può semplicemente scrivere $x \circ y \circ z$);
  (2) (Elemento neutro) per ogni $x \in G$ vale
  $$x \circ e = e \circ x = x$$
  (3) (Esistenza dell'inverso) per ogni $x \in G$ esiste $x^\star \in G$ che soddisfa
  $$x \circ x^\star = x^\star \circ x = e$$

In generale, non è richiesta la proprietà di
(4) (Commutatività) per ogni $x, y \in G$
$$x \circ y = y \circ x$$

Quando l'operazione $\circ$ ha anche questa proprietà, il gruppo $(G, \circ, e)$ si dice *commutativo* o *abeliano*[§]. Di solito per i gruppi abeliani si usa indicare l'operazione con il simbolo "+" invece di "$\circ$".

3.1. **Esempi di gruppi.** Diversi oggetti matematici hanno in modo "naturale" una struttura di gruppo.

Esempio 3.2. $(\mathbb{Z}, +, 0)$ è un gruppo abeliano. Senza grosse sorprese, anche $(\mathbb{Q}, +, 0)$, $(\mathbb{R}, +, 0)$ e $(\mathbb{C}, +, 0)$ sono gruppi abeliani. Inoltre, $(\mathbb{Q} \setminus \{0\}, \cdot, 1)$, $(\mathbb{R} \setminus \{0\}, \cdot, 1)$, $(\mathbb{C} \setminus \{0\}, \cdot, 1)$ sono gruppi abeliani.

Al di là degli insiemi numerici, che si possono studiare sotto molti punti di vista, un altro esempio interessante è quello dei *gruppi di funzioni*.

Esempio 3.3. Sia X un insieme non vuoto. Chiamiamo $aut(X)$[¶] l'insieme
$$aut(X) = \{f : X \to X \mid f \text{ è biettiva}\}$$
Su $aut(X)$ definiamo una composizione $\circ : aut(X) \times aut(X) \to aut(X)$ in questo modo:
$$(f \circ g)(x) = f(g(x))$$
Si verifica facilmente che la funzione id_X definita da $id_X(x) = x$ per ogni $x \in X$ ha la proprietà
$$id_X \circ f = f \circ id_X = f$$
per ogni $f \in aut(X)$. Inoltre, dato che ogni funzione biettiva ammette un'inversa (♠), per ogni $f \in aut(X)$ è ben definita la sua funzione inversa $f^\star$, che di solito si indica con il simbolo f^{-1}. Deduciamo che per ogni insieme non vuoto X $(aut(X), \circ, id_X)$ è un gruppo.

[§]Da Niels Henrik Abel, matematico norvegese del XIX secolo.
[¶]Si pronuncia "gruppo degli automorfismi di X".

Osservazione 3.4. In generale, $aut(X)$ *non* è abeliano (♠), ed è interessante provare a trovare degli esempi espliciti di insiemi X per cui questa proprietà fallisce (ad esempio: cosa succede quando $X = \{\triangleleft, \triangle, \triangleright\}$?).

Il prossimo esempio è di natura squisitamente algebrica.

Esempio 3.5 (Il quadrigruppo di Klein[‖])**.** Il quadrigruppo di Klein è il gruppo $(V, \circ, e)$, dove:

- V ha quattro elementi, che per comodità denoteremo $V = \{a, b, c, e\}$;
- $\circ$ è definita da:

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Dalla definizione di $\circ$ si può verificare che l'operazione è associativa (♠) e che $a^2 = b^2 = c^2 = e$ (in altre parole: ogni elemento di V è l'inverso di se stesso), quindi V è un gruppo. In più, si può verificare (sempre usando la definizione di $\circ$) che V è abeliano.

Anche il prodotto cartesiano di gruppi è ancora un gruppo.

Esempio 3.6 (♡)**.** Se $(G, \circ, e)$ e $(J, \diamond, \eta)$ sono due gruppi, anche $(G \times J, \circ \times \diamond, (e, \eta))$, dove

$$(x, \alpha) \circ \times \diamond (y, \beta) = (x \circ y, \alpha \diamond \beta)$$

è ancora un gruppo (♠), e sarebbe opportuno provare a verificare che $\circ \times \diamond$ soddisfa tutte le proprietà della definizione.

3.2. **Non-esempi di gruppi.** In questa sezione raccogliamo qualche esempio di oggetto matematico interessante che però non è un gruppo. I primi due "non-esempi" dovrebbero essere molto famigliari.

Esempio 3.7. $(\mathbb{N}, +, 0)$ non è un gruppo. Infatti, ogni numero diverso da 0 non ha inverso additivo. Per un motivo analogo, anche $(\mathbb{Z} \setminus \{0\}, \cdot, 1)$ non è un gruppo.

Con gli insiemi numerici è possibile inventarsi i non-esempi più disparati.

Esempio 3.8 (♡)**.** Di seguito, alcuni bizzarri esempi di non-gruppi. Per ciascuno di essi, lo studente interessato potrebbe provare a scoprire quale o quali proprietà di gruppo non vengono soddisfatte.

- $(\mathbb{R}, \uparrow, 1)$, dove $l \uparrow m = l^m$;
- $(\mathbb{Q}, \odot, 1)$, dove $n \odot u = n^2 u^2$;
- $(\mathbb{R}, \oplus, 0)$, dove $x \oplus y = \sin(x + y)$;
- $(\mathbb{Z}, \otimes, 1)$, dove $r \otimes s = \max\{r, s\}$;
- $(\mathbb{C}, \wr, 0)$, dove $a \wr b = a$.

[‖]Oppure semplicemente "gruppo di Klein". In inglese: Klein four-group. In tedesco: Vierergruppe.

Esistono anche insiemi di funzioni che, pur essendo molto rilevanti per la pratica matematica, non sono un gruppo rispetto all'operazione di composizione.

Esempio 3.9 (Le funzioni continue da $\mathbb{R}$ a $\mathbb{R}$)**.** L'insieme

$$C^0(\mathbb{R}) = \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ è continua}\}$$

delle funzioni continue da $\mathbb{R}$ a $\mathbb{R}$ con l'operazione di composizione e l'elemento neutro dato dalla funzione identità non è un gruppo. Il motivo fondamentale è che le funzioni continue non sono sempre invertibili rispetto alla composizione (♠).

Osservazione 3.10 (♡). Nulla vieta all'insieme $C^0(\mathbb{R})$ di essere un gruppo, se lo equipaggiamo con un'altra operazione e di conseguenza con un altro elemento neutro. Ad esempio, cosa succede se consideriamo $(C^0(\mathbb{R}), +, c_0)$, dove la funzione $f + g$ è definita da

$$(f + g)(x) = f(x) + g(x)$$

e con c_0 indichiamo la funzione costante 0?

4. Anelli

Avvicinandosi alla definizione di campo, l'oggetto intermedio che si incontra sul cammino è quello di anello. Negli anelli ci sono già due operazioni, che chiameremo somma e prodotto. La somma negli anelli verifica le stesse proprietà delle operazioni dei gruppi ed in più è commutativa, come nei campi. A differenza di quello che succede nei campi, però, il prodotto negli anelli oltre ad essere associativo e ad avere un elemento neutro verifica solo una proprietà essenziale di compatibilità con la somma.

Definizione 4.1. Un *anello* è una 5-upla ordinata $(R, +, \cdot, 0, 1)$, dove:

- $R \neq \emptyset$ è un insieme;
- $0, 1 \in R$;
- $+ : R \times R \to R$ e $\cdot : R \times R \to R$ soddisfano le proprietà:
  - (1) (Associatività) per ogni $x, y, z \in R$ valgono
    $$(x + y) + z = x + (y + z) \quad \text{e} \quad (x \cdot y) \cdot z = x \cdot (y \cdot z)$$
  - (2) (Elemento neutro per la somma) per ogni $x \in R$ vale
    $$x + 0 = 0 + x = x$$
  - (2') (Elemento neutro per il prodotto) per ogni $x \in R$ vale
    $$x \cdot 1 = 1 \cdot x = x$$
  - (3) (Esistenza dell'inverso additivo) per ogni $x \in R$ esiste $-x \in R$ che soddisfa
    $$x + (-x) = (-x) + x = 0$$

(4) (Commutatività dell'addizione) per ogni $x, y \in R$

$$x + y = y + x$$

(5) (Distributività del prodotto rispetto alla somma) per ogni $x, y, z \in R$

$$x \cdot (y + z) = x \cdot y + x \cdot z$$

(in questa formula abbiamo usato la convenzione che il prodotto viene eseguito prima della somma).

In generale, non è richiesta la proprietà di

(3') (Esistenza dell'inverso moltiplicativo) per ogni $x \in R$, se $x \neq 0$ esiste $x^{-1} \in R$ che soddisfa

$$x \cdot x^{-1} = x^{-1} \cdot x = 1$$

Quando l'operazione $\cdot$ ha anche questa proprietà, l'anello $(R, +, \cdot, 0, 1)$ si dice *con divisione*.

Non è nemmeno richiesta la proprietà di

(4') (Commutatività del prodotto) per ogni $x, y \in G$

$$x \cdot y = y \cdot x$$

Quando l'operazione $\cdot$ ha anche questa proprietà, l'anello $(R, +, \cdot, 0, 1)$ si dice *commutativo*[**].

4.1. **Esempi di anelli.** A lezione abbiamo già visto un esempio di anello, anche se non lo abbiamo chiamato con questo nome.

Esempio 4.2. Per $n \in \mathbb{N} \setminus \{0\}$, consideriamo l'insieme

$$R^{n,n} = \{\text{matrici } n \times n \text{ a coefficienti reali}\}$$

con le operazioni di somma e prodotto tra matrici viste a lezione. Se chiamiamo 0_n la matrice $n \times n$ le cui componenti sono tutte uguali a 0 e se chiamiamo Id_n la matrice identità di ordine n, allora $(R^{n,n}, +, \cdot, 0_n, Id_n)$ è un anello per ogni $n \in \mathbb{N} \setminus \{0\}$.

Ci sono due grossi casi da distinguere: quello in cui $n = 1$ e quello in cui $n > 1$. Se $n = 1$, $(R^{1,1}, +, \cdot, 0_1, Id_1)$ è un campo che si comporta come il campo dei numeri reali[††].

Se $n > 1$, abbiamo visto a lezione che valgono

¬(3') $R^{n,n}$ non è un anello con divisione (cioè ci sono delle matrici $n \times n$ non invertibili), e

¬(4') il prodotto in $R^{n,n}$ non è commutativo (cioè esistono $A, B \in R^{n \times n}$ tali per cui $AB \neq BA$).

[**]L'aggettivo "abeliano" si usa solo per i gruppi, quindi non si dice che un anello è abeliano.

[††]Più precisamente, si può dimostrare che $(R^{1,1}, +, \cdot, 0_1, Id_1)$ e $(\mathbb{R}, +, \cdot, 0, 1)$ sono due campi *isomorfi*, qualsiasi cosa voglia dire questa parola. Intuitivamente, non c'è nessuna proprietà dei campi che riesce a distinguerli, quindi a tutti gli effetti possiamo pensare che siano lo stesso campo.

Osservazione 4.3 (♡). A lezione dovrebbe essere stato mostrato (se non dimostrato) che c'è una corrispondenza biunivoca tra le funzioni lineari $L : \mathbb{R}^n \to R^n$ e le matrici $n \times n$. Inoltre, questa corrispondenza trasforma la somma di matrici in somma di funzioni lineari e il prodotto tra matrici in composizione di funzioni (♠). Quindi, le stesse considerazioni viste nell'esempio precedente valgono per l'insieme delle funzioni lineari $L : \mathbb{R}^n \to R^n$ con le operazioni di somma e composizione.

L'esempio successivo riprende il 2.3, ma questa volta si concentra sulle operazioni modulo n con n composto.

Esempio 4.4. Consideriamo $(\mathbb{Z}_n, +_n, \cdot_n, 0, 1)$ come definito nell'esempio 2.3, ma questa volta con n composto (i.e. non primo e non uguale a 1). Si può verificare che le operazioni modulo n rendono $\mathbb{Z}_n$ un anello commutativo (♠).

Eppure $\mathbb{Z}_n$ non è un anello con divisione. Una dimostrazione può essere questa: dato che n è composto, possiamo scrivere $n = \prod_{i=1}^{k} p_i$ con p_i primi non necessariamente distinti. I numeri $p = \prod_{i=1}^{k-1} p_i$ e p_k appartengono entrambi a $\mathbb{Z}_n$ e sono diversi da 0, in quanto positivi e minori di n, ma, per definizione di prodotto in $\mathbb{Z}_n$, il loro prodotto è

$$pp_k = 0 \mod n$$

Questo implica che né p (né p_k) possono avere un inverso moltiplicativo. Infatti, se supponessimo per assurdo[‡‡] che p abbia un inverso moltiplicativo p^{-1}, potremmo moltiplicare l'equazione precedente per p^{-1} ed ottenere

$$p^{-1}pp_k = 0 \mod n$$

che implica

$$p_k = 0 \mod n$$

contraddicendo $p_k \neq 0 \mod n$, che avevamo stabilito poco fa.

Il prossimo esempio è molto interessante di per sé, ed è usato sia per descrivere alcuni fenomeni della fisica quantistica sia per ideare algoritmi di computer grafica.

Esempio 4.5 (♡ – I Quaternioni di Hamilton[*])**.** Definiamo l'insieme

$$\mathbb{H} = \{w + xi + yj + zk \mid w, x, y, z \in \mathbb{R}\}$$

Su $\mathbb{H}$ definiamo la somma componente per componente: esplicitamente

$$(w+xi+yj+zk)+(a+bi+cj+dk) = (w+a)+(x+b)i+(y+c)j+(z+d)k$$

[‡‡]La dimostrazione per assurdo si può sintetizzare nella seguente inferenza logica: $(A \to \bot) \to \neg A$. In altre parole: se da A deduciamo una contraddizione, allora la negazione di A è vera. Questa tecnica dimostrativa si basa sul principio del terzo escluso (in formula: $A \vee \neg A$, cioè o A è vera o A è falsa, e non ci sono ulteriori alternative) che è rifiutato dai matematici costruttivisti.

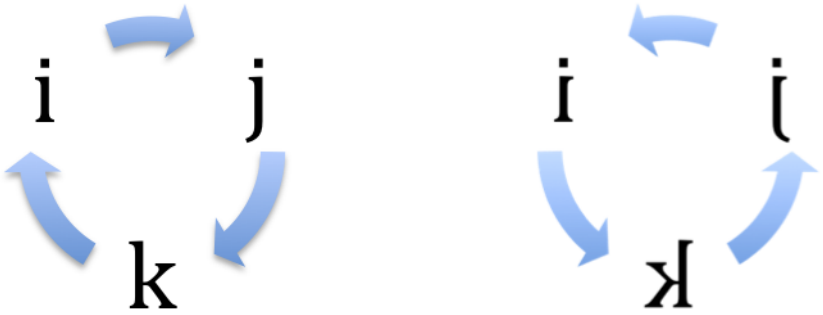
[*]Formalizzati da Sir William Rowan Hamilton intorno al 1840.

mentre il prodotto è l'usuale prodotto tra polinomi con in più le regole

$$i^2 = j^2 = k^2 = ijk = -1$$

$$\begin{array}{ll} ij = k & ji = -k \\ jk = i & kj = -i \\ ki = j & ik = -j \end{array}$$

Queste regole si possono ricordare più facilmente pensando a i, j, k disposti in ordine:



Il prodotto di due termini è sempre il terzo; il segno è "+" se i termini vengono moltiplicati in senso orario ed è "−" se i termini vengono moltiplicati in senso antiorario.

Con queste due operazioni, $\mathbb{H}$ è un anello con divisione (♠). Evidentemente non è commutativo, ma comunque estende il campo dei numeri complessi.

5. Campi, la definizione usuale

Dopo aver visto le definizioni di gruppo e anello, la definizione di campo diventa semplicemente:

Definizione 5.1. Un campo è un anello commutativo con divisione.

6. Conclusione

Sembra che con questo lungo cammino non abbiamo guadagnato nulla rispetto alla definizione della sezione 2. Eppure, lungo il percorso che ci ha portato dai gruppi ai campi abbiamo visto diverse strutture algebriche che soddisfano (e che non soddisfano) le più disparate proprietà. Spero che questo campionario di esempi possa aiutare ad intuire meglio tutta la ricchezza di richiedere che F (o $\mathbf{k}$, o $\daleth \dots$) "sia un campo" e, soprattutto, mi auguro che possa suscitare una scintilla di curiosità nei confronti delle meraviglie dell'algebra.

Riferimenti bibliografici

[1] I.N. Herstein (2003), *Algebra*, Editori Riuniti.
[2] R. Schoof e L. van Geemen (2001), *Algebra*, reperibile alla pagina `http://www-dimat.unipv.it/canonaco/notealgebra.pdf`
[3] Kiryl Tsishchanka (2003), *Groups, basic definitions and examples*, reperibile alla pagina `http://cims.nyu.edu/~kiryl/teaching/aa/review2.pdf`

Dipartimento di Matematica, Università di Trento, Italy.
E-mail address: `emanuele.bottazzi@unitn.it`