Università degli studi di Padova

Dipartimento di Matematica “Tullio Levi-Civita”

Corso di laurea magistrale in Matematica

Iperstrutture algebriche e applicazioni

RELATORE

Prof.ssa Alessandra Bertapelle

LAUREANDO

Elena Ferrarini
1179920

Anno Accademico 2018/2019

13 dicembre 2019

Indice

Introduzione

Le iperstrutture algebriche rappresentano una naturale generalizzazione delle classiche strutture algebriche. Se in una classica struttura algebrica la composizione di due elementi è un elemento, in una iperstruttura la composizione di due elementi è un insieme. Prima di trattare le iperstrutture, si deve innanzitutto definire cos'è una iperoperazione: un'iperoperazione è un'operazione che a due elementi di un insieme non vuoto H associa un sottoinsieme non vuoto di H. Un'iperstruttura è quindi data da un insieme non vuoto H e da una o più iperoperazioni.

In questa tesi abbiamo studiato alcune iperstrutture algebriche, confrontandole con le rispettive strutture dell'algebra classica; abbiamo poi esaminato diversi importanti risultati di algebra commutativa e geometria algebrica e li abbiamo riformulati in termini di iperstrutture algebriche. In seguito abbiamo analizzato lo spettro di un iperanello con le relative proprietà e infine abbiamo evidenziato, tramite alcuni esempi, l'esistenza di un legame tra iperstrutture algebriche, in particolare l'ipercampo tropicale $\mathbb{T}$, e la geometria tropicale, branca della geometria algebrica che ha riscosso notevole interesse negli ultimi anni.

In particolare, nel primo capitolo abbiamo riportato alcune definizioni e risultati di algebra commutativa e geometria algebrica classica confrontandoli successivamente con i corrispettivi nel caso "iper". Ad esempio, abbiamo considerato le definizioni di

gruppo, anello, campo e ideale; la costruzione dell'anello quoziente e il procedimento di localizzazione; il teorema degli zeri di Hilbert e la definizione di spettro primo di un anello. Alla fine del primo capitolo abbiamo, inoltre, richiamato alcune nozioni basilari riguardanti la teoria delle categorie, che ci serviranno nel capitolo successivo.
Nel secondo capitolo abbiamo introdotto ed esaminato alcune definizioni di base delle iperstrutture. In particolare, ci siamo occupati di ipergruppi canonici, iperanelli di Krasner e di ipercampi, fornendo esempi e analizzando alcune loro proprietà e mettendo in evidenza le analogie con il caso classico. Abbiamo, infatti, mostrato che alcuni risultati di Algebra Commutativa e di Geometria Algebrica possono essere riformulati in termini di iperanelli. Successivamente, abbiamo trattato lo spettro primo di un iperanello, anch'esso definito riformulando la nozione di spettro di un anello, descritta nel capitolo precedente, e abbiamo mostrato che, come nel caso classico, l'iperspettro è dotato della topologia di Zariski. Inoltre, abbiamo riportato un importante risultato di A. Connes e P. Consani riguardante la caratterizzazione dell'usuale spettro primo di un anello R come l'insieme degli omomorfismi di iperanelli $R \to \mathbb{K}$, dove R è dotato della naturale struttura di iperanello indotta dalla sua struttura di anello e $\mathbb{K}$ indica l'ipercampo di Krasner. Dopo aver esplicitato le nozioni di cono simmetrico, positivo e totale, abbiamo mostrato che esiste un omeomorfismo tra lo spettro primo di un anello e lo spettro di un iperanello. Alla fine del secondo capitolo, abbiamo riportato alcuni cenni storici riguardanti la nascita e lo sviluppo della Teoria delle iperstrutture algebriche.
Nell'ultimo capitolo, richiamando la definizione di ipercampo tropicale $\mathbb{T} := \mathbb{R} \cup \{\infty\}$ e di valutazione p-adica, abbiamo mostrato il legame tra varietà classiche e varietà tropicali mediante alcuni esempi. Infatti, abbiamo mostrato che la tropicalizzazione di varietà affini mediante la valutazione p-adica ha una naturale interpretazione in

termini di ipercampi, più precisamente, se x è definito da un polinomio $p(x)$ a coefficienti interi, la sua tropicalizzazione è il luogo degli “iperzeri” di $p(x)$ visto ora come un polinomio sull'ipercampo tropicale $\mathbb{T}$.

Capitolo 1

Nozioni di Algebra

In questa sezione si vogliono elencare alcune costruzioni e alcuni risultati di Algebra e di Algebra Commutativa, che saranno generalizzati nel prossimo capitolo ad iperstrutture, dove la somma è una multifunzione. Alla fine di questo capitolo verranno poi esplicitati alcuni risultati della teoria delle categorie.

1.1 Gruppi e Anelli

Definizione 1.1.1. Un **gruppo** è un insieme G dotato di un'operazione $*$ tale che ognuno dei seguenti assiomi sia soddisfatto:

1. Associatività $\quad a * (b * c) = (a * b) * c \quad \forall a, b, c \in G$;
2. Esistenza dell'elemento neutro $\quad$ Esiste un elemento $e \in G$ tale che $a * e = e * a = a \quad \forall a \in G$;
3. Esistenza dell'inverso $\quad \forall a \in G$ esiste un elemento $b \in G$ tale che $a * b = b * a = e$.

Definizione 1.1.2. Un gruppo G si dice **abeliano** se l'operazione di cui è dotato il gruppo è commutativa, ossia $a * b = b * a \quad \forall a, b \in G$.

Teorema 1.1.1. *Si assuma che G con l'operazione $*$ sia un gruppo.*

1. *L'elemento neutro di G è unico; ossia se e ed f sono elementi di G tali che:*

   $e * a = a * e = a \quad \forall a \in G$ *e* $f * a = a * f = a \quad \forall a \in G$ *allora* $e = f$.

2. *Ogni elemento di un gruppo ha un unico inverso; ossia se a, x e y sono elementi di G, e è l'elemento neutro di G, e $a * x = x * a = e$ e $a * y = y * a = e$ allora $x = y$.*

Dimostrazione. 1. Assumendo che e ed f soddisfino ciò che è stato asserito, allora $e * a = a$ per ciascuna $a \in G$ e quindi, $e * f = f$. In modo analogo, prendendo $a = e$ in $a * f = a$, si trova $e * f = e$. Quindi $f = e * f = e$ e quindi $e = f$.

2. Con a, x e y come sopra, si può scrivere:

$$\begin{array}{rcll} x & = & x * e & (e \text{ è l'identità}) \\ & = & x * (a * y) & \text{perché } (a * y = e) \\ & = & (x * a) * y & (\text{associatività}) \\ & = & e * y & (\text{perché } x * a = e) \\ & = & y & (\text{perché } e \text{ è l'identità}) \end{array}$$

□

Definizione 1.1.3. La cardinalità dell'insieme soggiacente il gruppo è detto **ordine** del gruppo e si denota con $|G|$. Un gruppo è detto *finito* o *infinito* se il suo ordine è finito o infinito.

Definizione 1.1.4. Un **semigruppo** è un insieme M con un'operazione binaria $*$ tale che:

$$a * (b * c) = (a * b) * c \quad \forall a, b, c \in M$$

Se $a * b = b * a \quad \forall a, b \in M$, M si dice **semigruppo commutativo**.

Se esiste un unico elemento $e \in M$ tale che $m * e = e * m = m \quad \forall m \in M$, allora M è detto **monoide**.

Osservazione 1.1.1. Un gruppo è un monoide in cui ogni elemento ammette inverso.

Definizione 1.1.5. Un **anello** A è un insieme con due operazioni binarie, che chiameremo addizione e moltiplicazione e indicheremo con $+$ e $\cdot$, tali che:

1. A è un gruppo abeliano rispetto all'addizione (sicché A possiede un elemento neutro, denotato con 0, e ogni elemento $x \in A$ ha un opposto, $-x$).

2. La moltiplicazione è associativa $(xy)z = x(yz)$ e distributiva rispetto all'addizione $x(y+z) = xy + xz, \quad (y+z)x = yx + zx$.

Se inoltre vale $xy = yx \quad \forall x, y \in A$ diremo che l'anello è **commutativo**.
Se l'anello possiede un **elemento unità** (denotato con 1), ossia

$$\exists 1 \in A \quad tale \quad che \quad x1 = 1x = x, \forall x \in A,$$

diremo che A è un **anello con unità**. Se esiste l'elemento unità, allora è unico.

Abbiamo per brevità scritto sopra $((xy)z = x(yz)$ al posto di $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, e così faremo d'ora in poi.

Notazione: Con il termine *"anello"* si indicherà d'ora in poi un anello commutativo con unità, ossia un anello che soddisfi gli assiomi da (1) a (4) indicati sopra.

Ricordiamo i seguenti fatti elementari sugli anelli:

Teorema 1.1.2. *Sia R un anello e siano $a, b, c \in R$.*

1. *L'elemento nullo di R è unico.*

2. *Ogni elemento di R ha un unico opposto.*

3. *Se $a + b = a + c$, allora $b = c$.*

4. *Se* $b + a = c + a$, *allora* $b = c$.

5. $0a = a0 = 0$.

6. $-(-a) = a$ *e* $-(a + b) = (-a) + (-b)$.

7. $a(-b) = (-a)b$.

8. $(-a)(-b) = ab$.

9. $a(b - c) = ab - ac$ *e* $(a - b)c = ac - bc$.

10. *Se* m *e* n *sono interi, allora* $(m + n)a = ma + na$, $m(a + b) = ma + mb$, *e* $m(na) = (mn)a$.

Definizione 1.1.6. Se A è un anello commutativo, allora $a \neq 0 \in A$ si dice **divisore dello zero** se esiste $b \in A, b \neq 0$ tale che $ab = 0$.

Esempio 1.1.1. In $A = \mathbb{Z}/6\mathbb{Z}$, 2 e 3 sono divisori dello zero.

Definizione 1.1.7. Un anello commutativo si dice **dominio di integrità** se non ha divisori dello zero.

Esempio 1.1.2. L'anello degli interi $\mathbb{Z}$ è un dominio di integrità e così anche ogni campo.

Definizione 1.1.8. Un anello si dice **anello di divisione** o *corpo* se i suoi elementi non nulli formano un gruppo rispetto alla moltiplicazione.

Osservazione 1.1.2. L'inverso di un elemento a rispetto alla moltiplicazione sarà indicato con a^{-1}.

Definizione 1.1.9. Un dominio di integrità si dice essere di **caratteristica 0** se la relazione $ma = 0$, dove $a \neq 0$ è un elemento di D e m è intero, sussiste solo nel caso $m = 0$.

Esempio 1.1.3. L'anello degli interi ha caratteristica 0 e così pure il campo dei numeri razionali.

Definizione 1.1.10. Un dominio di integrità si dice di **caratteristica finita** se esiste un intero positivo m tale che $ma = 0$ per ogni $a \in D$.

Osservazione 1.1.3. Se D ha caratteristica finita, si può definire la caratteristica di D come il più piccolo intero positivo p tale che $pa = 0$ per ogni $a \in D$ e si dimostra che p è un numero primo.

Definizione 1.1.11. Un **omomorifismo di anelli commutativi con unità** è un'applicazione f di un anello A in un anello B tale che:

1. $f(x + y) = f(x) + f(y)$ sicchè f è un omomorfismo di gruppi abeliani,
2. $f(xy) = f(x)f(y)$,
3. $f(1) = 1$.

Ossia f conserva l'addizione, la moltiplicazione e l'elemento unità.

Definizione 1.1.12. Se $f : R \to R'$ è un omomorfismo di anelli, si definisce **nucleo** di f l'insieme degli elementi $a \in R$ tali che $f(a) = 0$, dove 0 è l'elemento nullo di R' e lo si indica con $I(f)$ o $Kerf$.

Definizione 1.1.13. Un omomorfismo di R in R' si dice **isomorfismo** se è biiettivo e in tal caso diremo che R e R' sono isomorfi.

Definizione 1.1.14. Un sottoinsieme S di un anello A è un **sottoanello** di A, se S è un sottogruppo additivo di A chiuso rispetto alla moltiplicazione e contenente l'identità 1_A.

Osservazione 1.1.4.
1. Se $f\colon A \to B$, $g\colon B \to C$ sono omomorfismi di anelli, allora tale è la loro composizione $g \circ f\colon A \to C$.
2. Se S è un sottoanello di A, allora l'inclusione è un omomorfismo iniettivo.

1.2 Ideali

Definizione 1.2.1. Sia R un anello commutativo con unità. Un sottoinsieme $\mathfrak{a}$ di R si dice **ideale** di R se:

1. $\mathfrak{a}$ è sottogruppo additivo di R.
2. $r \in R, a \in \mathfrak{a}$ implicano $ra \in \mathfrak{a}$.

Osservazione 1.2.1. Dato un ideale $\mathfrak{a}$ in un anello R, sia $R/\mathfrak{a}$ l'insieme delle classi laterali di $\mathfrak{a}$ in R, ottenuto considerando $\mathfrak{a}$ come sottogruppo additivo di R. L'insieme $R/\mathfrak{a}$ consta delle classi laterali $a + \mathfrak{a}$, con $a \in R$ e si può dimostrare che $R/\mathfrak{a}$ è un gruppo rispetto all'addizione:

$$(a + \mathfrak{a}) \; + \; (b + \mathfrak{a}) = (a + b) + \mathfrak{a}.$$

Inoltre $R/\mathfrak{a}$ è dotato della struttura di anello definendo $(a+\mathfrak{a})\,(b+\mathfrak{a}) = ab+\mathfrak{a}$. Si nota che questa definizione non dipende dai rappresentanti scelti, ossia se $a + \mathfrak{a} = a' + \mathfrak{a}$ con $a = a' + \mathfrak{a}_1$ e $b + \mathfrak{a} = b' + \mathfrak{a}$ con $b = b' + \mathfrak{a}_2$, allora:

$$(a + \mathfrak{a})\,(b + \mathfrak{a}) = ab + \mathfrak{a} = (a' + \mathfrak{a}_1)\,(b' + \mathfrak{a}_2) + \mathfrak{a} = a'b' + \mathfrak{a} = (a' + \mathfrak{a})\,(b' + \mathfrak{a}).$$

Inoltre si verifica che $R/\mathfrak{a}$ è un anello commutativo, detto **anello quoziente**. Infatti,

$$(a+\mathfrak{a})\,(b+\mathfrak{a}) = \; ab+\mathfrak{a} = \; ba+\mathfrak{a} = \; (b+\mathfrak{a})\,(a+\mathfrak{a}).$$

Infine $1+\mathfrak{a}$ è l'elemento unità di $R/\mathfrak{a}$.

L'applicazione $f : R \to R/\mathfrak{a}$ data da $f(a) = a+\mathfrak{a}$, per ogni $a \in R$, è un omomorfismo di anelli, il cui nucleo è proprio $\mathfrak{a}$.

Osservazione 1.2.2.

- Se $\mathfrak{a}$ e $\mathfrak{b}$ sono ideali in un anello A, la `somma` di due ideali $\mathfrak{a}+\mathfrak{b}$ è definita come l'insieme di tutti gli elementi di A che si possono scrivere nella forma $x+y$, dove $x \in \mathfrak{a}$ e $y \in \mathfrak{b}$. Esso è il più piccolo ideale contenente $\mathfrak{a}$ e $\mathfrak{b}$.

- L'`intersezione` di una qualsiasi famiglia $(\mathfrak{a})_{i\in I}$ di ideali è ancora un ideale.

- Il `prodotto` di due ideali $\mathfrak{a}$ e $\mathfrak{b}$ in A è l'ideale indicato con $\mathfrak{ab}$ e generato da tutti i prodotti xy, dove $x \in \mathfrak{a}$ e $y \in \mathfrak{b}$. Esso consiste di tutte le somme finite $\sum_i x_i y_i$ dove $x_i \in \mathfrak{a}$ e $y_i \in \mathfrak{b}$.

- l'`unione` $\mathfrak{a} \cup \mathfrak{b}$ di ideali non è in generale un ideale.

Proposizione 1.2.1. *Se $\varphi : R \to A$ è un omomorfismo di anelli, e $J \subseteq A$ è un ideale di A, allora $\varphi^{-1}(J) = \{x \in R | \varphi(x) \in J\}$ è un ideale in R. In particolare il nucleo di φ, $I(\varphi) = \varphi^{-1}(0)$ è un ideale di R.*

Dimostrazione. Dato che J è un sottogruppo, lo stesso è $\varphi^{-1}(J)$. Inoltre per ogni $x \in R$ e per $y \in \varphi^{-1}(J)$ si avrà $\varphi(xy) = \varphi(x)\varphi(y) \in J$ poiché $\varphi(y) \in J$. $\square$

Osservazione 1.2.3. Esiste una corrispondenza biunivoca, che conserva l'ordinamento, tra gli ideali $\mathfrak{b}$ di A che contengono $\mathfrak{a}$ e gli ideali $\overline{\mathfrak{b}}$ di $A/\mathfrak{a}$ data da $\mathfrak{b} = \phi^{-1}(\overline{\mathfrak{b}})$.

Riassumiamo quanto fin qui visto.

Proposizione 1.2.2. *Siano R e R' anelli e f un omomorfismo di R su R' di nucleo I. Allora R' è isomorfo a R/I. Inoltre, esiste una corrispondenza biunivoca tra l'insieme degli ideali di R' e l'insieme degli ideali di R che contengono I.*

1.2.1 Ideali primi e ideali massimali

Definizione 1.2.2. Un ideale $\mathfrak{p} \neq (1)$ di R si dice **primo**, se $xy \in \mathfrak{p}$ implica $x \in \mathfrak{p}$ oppure $y \in \mathfrak{p}$.

Definizione 1.2.3. Un ideale $\mathfrak{m} \neq (1)$ di R si dice **massimale**, se non esiste alcun ideale proprio $\mathfrak{a}$ di R tale che $\mathfrak{m} \subsetneqq \mathfrak{a}$.

Si dimostra che:

$$\mathfrak{p} \text{ è primo} \iff R/\mathfrak{p} \text{ è un dominio di integrità.}$$
$$\mathfrak{m} \text{ è massimale} \iff R/\mathfrak{m} \text{ è un campo.}$$
$$\text{L'ideale nullo è primo} \iff R \text{ è dominio di integrità.}$$

Osservazione 1.2.4. Un ideale massimale è primo ma in generale non vale il viceversa.
Ad esempio (0) in $\mathbb{R}[x]$ è primo ma non massimale.

Discende come applicazione del *Lemma di Zorn* che ogni anello $A \neq 0$ possiede almeno un ideale massimale e di conseguenza ogni ideale proprio di A è contenuto in un ideale massimale di A. In particolare, ogni elemento non invertibile di A è contenuto in un ideale massimale.

1.3 Campi

Definizione 1.3.1. Un **campo** è un anello commutativo A in cui $1 \neq 0$ ed ogni elemento non nullo è invertibile. Essi sono particolari domini di integrità.

$$\text{campi} \subset \text{domini d'integrità} \subset \text{anelli commutativi} \subset \text{anelli}$$

Proposizione 1.3.1. *Sia A un anello non nullo. Allora le seguenti condizioni sono equivalenti:*

1. *A è un campo;*
2. *gli unici ideali di A sono 0 e (1);*
3. *ogni omomorfismo non nullo di anelli $A \to B$ è iniettivo.*

Dimostrazione. *1)* $\implies$ *2)* Sia $\mathfrak{a} \neq 0$ un ideale di A. Allora $\mathfrak{a}$ contiene un elemento non nullo x; poiché x è invertibile, si ha $\mathfrak{a} \supseteq (x) = (1)$, da cui $\mathfrak{a} = (1)$.
2) $\implies$ *3)* Sia $\phi : A \to B$ un omomorfismo di anelli. Allora $Ker(\phi)$ è un ideale $\neq (1)$ in A, sicché $Ker(\phi) = 0$, dunque ϕ è iniettivo.
3) $\implies$ *1)* Sia x un elemento non invertibile di A. Allora $(x) \neq (1)$, dunque $B = A/(x)$ non è l'anello nullo. Sia $\phi : A \to B$ l'omomorfismo naturale di A su B, con nucleo (x). Per ipotesi, ϕ è iniettivo, dunque $(x) = 0$, da cui $x = 0$. $\square$

Proposizione 1.3.2. *Siano R un anello e $\mathfrak{m} \subset R$ un ideale proprio. Le seguenti condizioni sono equivalenti:*

1. *$\mathfrak{m}$ è massimale;*
2. *$R/\mathfrak{m}$ è un campo.*

Definizione 1.3.2. Un sottoinsieme K di un campo F si dice **sottocampo** di F se K è un campo rispetto alle operazioni indotte da F.

1.4 Teoremi degli zeri di Hilbert

Si suppone in questa sezione che K sia un campo algebricamente chiuso, ossia un campo in cui ogni polinomio $f \in K[x]$ di grado maggiore di 0 ha un radice in K. Si consideri inoltre $\mathbb{A}^n_K$ lo spazio affine n-dimensionale su K. Indicheremo con $K[\underline{x}]$ l'anello dei polinomi nelle indeterminate $x_1, \ldots, x_n$.

Definizione 1.4.1. Se $I \subset K[\underline{x}]$ è un ideale, l'**insieme algebrico affine associato ad** I è

$$Z(I) = \Big\{ P \in \mathbb{A}^n_K : f(P) = 0 \quad \forall f \in I \Big\}.$$

Osservazione 1.4.1. Se $I \subset K[\underline{x}]$ è un ideale allora,

$$Z(I) = \Big\{ P \in \mathbb{A}^n_K : f(P) = 0 \quad \forall f \in I \Big\} = \bigcap_{f \in I} Z(f)$$

Inoltre, se I è ideale generato dai polinomi $g_1, \ldots g_r \in K[\underline{x}]$, si ha

$$Z(I) = \bigcap_{f \in I} Z(f) = Z(\{g_1, \ldots, g_r\}) = \bigcap_{i=1}^{r} Z(g_i).$$

Teorema 1.4.1 (*degli zeri di Hilbert forma debole*)**.** *Sia $I \subseteq K[\underline{x}]$ un ideale. Allora I è proprio $\iff$ $Z(I) \neq \emptyset$.*

Dimostrazione. Se $I = K[\underline{x}]$, $I = (1) \implies Z(I) = Z(1) = \emptyset$.

Sia $I \subset K[\underline{x}]$ un ideale proprio. Sia $\mathfrak{m} \supseteq I$ ideale massimale in $K[\underline{x}]$ che contiene I. È noto che $\mathfrak{m}$ è del tipo $(x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n)$, con $a_i \in K$. Dunque l'anello quoziente è $\frac{K[\underline{x}]}{\mathfrak{m}}$. Sia ϕ la proiezione che associa a_i a x_i:

$$\begin{tikzcd}
K[\underline{x}] \arrow[r, two heads, "\phi"] \arrow[d] & \frac{K[\underline{x}]}{\mathfrak{m}} \\
\frac{K[\underline{x}]}{I} \arrow[ur, dashed, "\psi"] &
\end{tikzcd}$$

La mappa ψ esiste perché $I \subset \mathfrak{m}$ e ϕ è un omomorfismo suriettivo di anelli. Se $f \in I$, allora $\phi(f) = f(a_1, \dots, a_n) = 0$ da cui segue che $(a_1, \dots, a_n) \in Z(f) \quad \forall f \in I$. Quindi $(a_1, \dots, a_n) \in (I) \neq \emptyset$.

$\square$

Definizione 1.4.2. Sia I un ideale in $K[\underline{x}]$, si definisce **radicale di** I l'insieme

$$\sqrt{I} := \{f \in K[\underline{x}] \,|\, f^n \in I \quad \exists n \in \mathbb{N}\}$$

Si dimostra che è un ideale in $K[\underline{x}]$ e che $I \subseteq \sqrt{I}$ ma in generale $I \neq \sqrt{I}$.

Definizione 1.4.3. Se I è un ideale, si definisce:

$$\mathcal{I}Z(I) := \{f \in K[\underline{x}] \,|\, f(P) = 0 \quad \forall P \in Z(I)\}$$

Osservazione 1.4.2. 1. $\mathcal{I}Z(I) \supseteq I$.

2. Se I e J sono ideali tali che $I \subseteq J$, allora $\mathcal{I}Z(I) \subseteq \mathcal{I}Z(J)$.

3. Sia I ideale in $K[\underline{x}]$. Vale $Z(I) = Z(\sqrt{I})$.

   L'inclusione $\subseteq$ è banale.

   Dimostriamo ora l'inclusione opposta. Prendiamo $P \in Z(I)$ e $g \in \sqrt{I}$ allora si ha $g^m \in I, \quad \exists m > 0$, ossia $g(P)^m = (g^m)(P) = 0$, che implica $g(P) = 0$, ossia $P \in Z(g)$ e per l'arbitrarietà di g si ha che $g \in Z(\sqrt{I})$.

Teorema 1.4.2 (degli zeri di Hilbert forma forte)**.** *Sia $I \subseteq K[x_1, \dots, x_n]$ un ideale. Allora:*

$$\mathcal{I}Z(I) = \sqrt{I}$$

Il risultato sopra dice che se f è un polinomio che si annulla in tutti i punti di $Z(I)$ allora una qualche potenza di f appartiene a I.

Dimostrazione. Grazie al punto 3 dell'Osservazione 1.4.2 si ha $Z(I) = Z(\sqrt{I})$ da cui si ricava

$$\mathcal{I}Z(I) = \mathcal{I}Z(\sqrt{I}) \supseteq \sqrt{I}.$$

Per l'inclusione opposta, prendiamo un generico $0 \neq h \in \mathcal{I}Z(I)$, si deve dimostrare che $h \in \sqrt{I}$, ossia $h^m \in I$ per un qualche $m \in \mathbb{N}$. Si consideri l'anello $K[x_1, \ldots, x_n, y]$ dove abbiamo aggiunto l'indeterminata y. Risulta

$$h \in K[x_1, \ldots, x_n,] \subset K[x_1, \ldots, x_n, y];$$

consideriamo inoltre il suo ideale J generato da I e dal polinomio $1 - hy$.

$$J := (I, 1 - hy) \subset K[\underline{x}, y]$$

Dal *teorema degli zeri di Hilbert in forma debole* discende che $J = K[\underline{x}, y]$. Infatti, come vediamo sotto, si ha, $Z(I) = \emptyset$. Se così non fosse, esisterebbe $(\overline{a}, b) = (a_1, \ldots a_n, b) \in K^{n+1}$ che annulla tutti gli elementi di I e $1 - hy$. Ma $(1 - hy)$ calcolato in $(\underline{a}, b)$ dà: $1 - h(\underline{a}) \cdot b = 1 \neq 0$. Pertanto $Z(J) = \emptyset$ e dunque $J = K[\underline{x}, y]$. In particolare posso scrivere $1 = q(x, y)(1-hy) + \sum_{i=1}^{s} q_i(x, y) r_i(x, y)$ con $(r_1, \ldots, r_n) \in I$ e $q_1, \ldots q_s \in K[\underline{x}, y]$. Si costruisca ora l'omomorfismo di anelli:

$$\psi : K[\underline{x}, y] \to K(\underline{x})$$

ponendo $\psi(x_i) = x_i$ e $\psi(y) = \frac{1}{h}$. Con $K(\underline{x})$ si indica il campo delle frazioni di $K[x_1, \ldots, x_n]$. In particolare

$$\psi(1) = \psi(\sum_{i=1}^{n} q_i(\underline{x}, y) r_i(x) + q(\underline{x}, y)(1 - hy)) = 1 =$$

$$= q(\underline{x}, 1/h)(1 - h \cdot 1/h) + \sum_{i=1}^{n} q_i(\underline{x}, 1/h) r_i(\underline{x}).$$

Dall'uguaglianza sopra, si ricava

$$1 = \sum_{i=1}^{n} q_i(\underline{x}, 1/h) r_i(x)$$

e potendo scrivere

$$q_i(\underline{x}, 1/h) = \frac{\widetilde{q_i}(\underline{x})}{h^{m_i}}$$

per opportuni $\widetilde{q_i}(x) \in K[\underline{x}]$, si ottiene:

$$1 = \sum_{i=1}^{n} \frac{\widetilde{q_i}(\underline{x})}{h^{m_i}} r_i(\underline{x}) = \sum_{i=1}^{n} \frac{\widetilde{\widetilde{q_i}}(\underline{x}) r_i(\underline{x})}{h^m}$$

dove $\widetilde{\widetilde{q_i}}(\underline{x}) \in K[\underline{x}]$.

In particolare

$$h^m = \sum_{i=1}^{n} \widetilde{\widetilde{q_i}}(\underline{x}) r_i(\underline{x}) \in I$$

da cui segue che $h \in \sqrt{I}$. □

1.5 Anelli di frazioni

In questa sezione descriveremo la formazione degli anelli di frazioni e il procedimento di localizzazione ad essa associato. Il procedimento con cui si costruisce il campo dei numeri razionali $\mathbb{Q}$ a partire dall'anello degli interi $\mathbb{Z}$, si può estendere a un qualsiasi dominio di integrità B e, con opportune restrizioni, ad un anello arbitrario.

Definizione 1.5.1. Sia A un anello commutativo con unità. Un **sottoinsieme moltiplicativamente chiuso** di A, o una **parte moltiplicativa** di A è un sottoinsieme S di A tale che $1 \in S$ e S è chiuso rispetto alla moltiplicazione.

Fissata una parte moltiplicativa $S \subseteq A$, si definisce una relazione $\equiv$ sull'insieme $A \times S$ ponendo:

$$(a,s) \equiv (b,t) \iff (at - bs)u = 0 \quad \text{per qualche } u \in S.$$

La relazione $\equiv$ è chiaramente *riflessiva* e *simmetrica* e si può dimostrare che è anche *transitiva*, infatti se $(a,s) \equiv (b,t)$ e $(b,t) \equiv (c,u)$, allora esistono $v, w \in S$ tali che $(at - bs)v = 0$ e $(bu - ct)w = 0$. Moltiplicando la prima per uw e la seconda per sv e sommando, si ottiene $(au - cs)tvw = 0$. Poiché S è chiuso rispetto alla moltiplicazione, si ha $tvw \in S$, da cui $(a,s) \equiv (c,u)$. Dunque $\equiv$ è una relazione di equivalenza e $\frac{a}{s}$ o $[(a,s)]$ denota la classe di equivalenza di (a,s). Inoltre si indicherà con $S^{-1}A$ l'insieme delle classi di equivalenza. Si definiscono poi su $S^{-1}A$ una **addizione** e una **moltiplicazione** allo scopo di dotarlo di una struttura di un *anello*. Si pone:

$$\frac{a}{s} + \frac{b}{t} = \frac{(at + bs)}{st},$$

$$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st},$$

e si dimostra che sono ben definite.

Proposizione 1.5.1. *$S^{-1}A$ è un anello commutativo con unità.*

Dimostrazione. Siano $a, c, e \in A$ e $b, d, f \in S$. Si deve verificare che $S^{-1}A$ soddisfa tutti gli assiomi di un anello commutativo con unità:

1. Si deve verificare che $S^{-1}A$ è un gruppo abeliano rispetto alla $+$:

   (i) $+$ è associativa, infatti: $\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} = \left(\frac{ad+cb}{bd}\right) + \frac{e}{f} = \frac{(ad+cb)f+e(bd)}{bdf} = \frac{adf+cbf+ebd}{bdf} = \left(\frac{adf}{bdf}\right) + \left(\frac{cbf+ebd}{bdf}\right) = \frac{a}{b} + \left(\frac{cf+ed}{df}\right) = \frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right)$;

   (ii) esiste l'elemento neutro $[(0,x)]$ con $x \in S$, infatti: $\frac{a}{b} + \frac{0}{x} = \frac{(a \cdot x + b \cdot 0)}{b \cdot x} = \frac{a \cdot x}{b \cdot x} = \frac{a}{b}$;

(iii) esiste l'inverso di $[(a,b)]$ detto *opposto*, ed è $[(-a,b)]$. Infatti: $\frac{a}{b}+\frac{-a}{b}=\frac{a\cdot b+(-a\cdot b)}{b\cdot b}=\frac{0}{b}$ con $b\in S$;

2. $\cdot$ è associativa, infatti: $\left(\frac{a}{b}\cdot\frac{c}{d}\right)\cdot\frac{e}{f}=\frac{ac}{bd}\cdot\frac{e}{f}=\frac{ace}{bdf}=\frac{a}{b}\cdot\frac{ce}{df}=\frac{a}{b}\cdot\left(\frac{c}{d}\cdot\frac{e}{f}\right)$;

   $\cdot$ è distributiva rispetto all'addizione:
   $\frac{a}{b}\cdot\left(\frac{c}{d}+\frac{e}{f}\right)=\frac{a}{b}\cdot\left(\frac{cf+ed}{df}\right)=\frac{a\cdot(cf+ed)}{bdf}=\frac{acf+aed}{bdf}=\frac{ac}{bd}+\frac{ae}{bf}=\frac{a}{b}\cdot\frac{c}{d}+\frac{a}{b}\cdot\frac{e}{f}$.

3. Vale la proprietà commutativa della moltiplicazione $\cdot$: $\frac{a}{b}\cdot\frac{c}{d}=\frac{c}{d}\cdot\frac{a}{b}$ infatti $\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}=\frac{ca}{db}=\frac{c}{d}\cdot\frac{a}{b}$;

4. Possiede un elemento unità $[(1,1)]$, infatti: $\frac{a}{b}\cdot\frac{1}{1}=\frac{a\cdot 1}{b\cdot 1}=\frac{1\cdot a}{1\cdot b}=\frac{a}{b}$.

□

Osservazione 1.5.1. ◇ Dato un anello A e una sua parte moltiplicativa S esiste un omomorfismo "canonico" di anelli $f: A\to S^{-1}A$ definito ponendo $f(x)=\frac{x}{1}$, che però non è iniettivo in generale. Ad esempio se $0\neq a\in A$ è divisore dello zero, ossia $ab=0$ con $b\neq 0$, e $S=\{a^n, n\geqslant 0\}$ allora $f(b)=\frac{b}{1}=\frac{ab}{a}=\frac{0}{a}=0$.

◇ Se A è un dominio di integrità e $S=A\setminus\{0\}$, allora $S^{-1}A$ è il campo delle frazioni di A.

L'anello $S^{-1}A$ è chiamato **anello delle frazioni** di A rispetto a S. La seguente proposizione descrive una sua proprietà universale:

Proposizione 1.5.2. *Sia S una parte moltiplicativa di A e sia $g: A\to B$ un omomorfismo di anelli tale che $g(s)$ è invertibile in B per ogni $s\in S$. Allora esiste un unico omomorfismo di anelli $h: S^{-1}A\to B$ tale che $g=h\circ f$.*

Dimostrazione. (i) *Unicità.* Se h soddisfa le condizioni richieste, allora $h(\frac{a}{1})=hf(a)=g(a)\quad\forall a\in A$. Dunque se $s\in S$, $h(\frac{1}{s})=h((\frac{s}{1})^{-1})=h(\frac{s}{1})^{-1}=g(s)^{-1}$

e quindi si ha $h(\frac{a}{s}) = h(\frac{a}{1})$ per $h(\frac{1}{s}) = g(a)g(s)^{-1}$; dunque h è univocamente determinato da g.

(ii) *Esistenza.* Si ponga $h(\frac{a}{s}) = g(a)g(s)^{-1}$. Da qui risulterà che h è sicuramente un omomorfismo di anelli purché sia ben definito. Si supponga $\frac{a}{s} = \frac{a'}{s'}$, allora esiste un elemento $t \in S$ tale che $(as' - a's)t = 0$ da cui si ha $(g(a)g(s') - g(a')g(s))g(t) = 0$. Dato che $g(t)$ è invertibile in B, si ha $g(a)g(s)^{-1} = g(a')g(s')^{-1}$.

□

Osservazione 1.5.2. L'anello $S^{-1}A$ e l'omomorfismo $f : A \to S^{-1}A$ possiedono le seguenti proprietà:

1. $s \in S \implies f(s)$ è invertibile in $S^{-1}A$;
2. $f(a) = 0 \implies as = 0$ per qualche $s \in S$;
3. Ogni elemento di $S^{-1}A$ è della forma $f(a)f(s)^{-1}$ per qualche $a \in A$ e qualche $s \in S$.

Inoltre, se I e J sono ideali di A, allora:

1. $S^{-1}(I + J) = S^{-1}I + S^{-1}J$;
2. $S^{-1}(IJ) = (S^{-1}I)(S^{-1}J)$;
3. $S^{-1}(I \cap J) = S^{-1}I \cap S^{-1}J$.

1.5.1 Localizzazione

Sia $\mathfrak{p}$ un ideale primo di A. Allora $S = A \smallsetminus \mathfrak{p}$ è una parte moltiplicativa e si scriverà $A_\mathfrak{p}$ al posto di $S^{-1}A$. Gli elementi $\frac{a}{s}$ con $a \in \mathfrak{p}$ formano un ideale $\mathfrak{m}$ in $A_\mathfrak{p}$. Se $\frac{b}{t} \notin \mathfrak{m}$, allora $b \notin \mathfrak{p}$, sicché $b \in S$ e quindi $\frac{b}{t}$ è invertibile in $A_\mathfrak{p}$. Da qui segue che se

$\mathfrak{a}$ è un ideale in $A_{\mathfrak{p}}$ e $\mathfrak{a} \nsubseteq \mathfrak{m}$, allora $\mathfrak{a}$ contiene un elemento invertibile che è, in realtà, l'intero anello. Quindi $\mathfrak{m}$ è l'unico ideale massimale in $A_{\mathfrak{p}}$; e pertanto, $A_{\mathfrak{p}}$ è un **anello locale**.

Il procedimento di passaggio da A ad $A_{\mathfrak{p}}$ prende il nome di **localizzazione**.

Se invece consideriamo un elemento $f \in A$ che non sia nilpotente e poniamo $S = \{f^n, n \geqslant 0\}$, $S^{-1}A$ verrà indicato con A_f.

Esempio 1.5.1. Sia $A = \mathbb{Z}$ e $\mathfrak{p} = (p)$ con p numero primo. Allora $A_{\mathfrak{p}}$ è l'insieme di tutti i numeri razionali $\frac{m}{n}$ dove n non è divisibile per p. Se $f \in \mathbb{Z}$ e $f \neq 0$, allora A_f è l'insieme di tutti i numeri razionali che si possono scrivere con denominatore una potenza di f.

Ad esempio $\frac{3}{2} = \frac{9}{6} \in \mathbb{Z}_f$ con $f = 6$.

Si può dimostrare che se $\mathfrak{p}$ è un ideale primo di A, gli ideali primi dell'anello locale $A_{\mathfrak{p}}$ sono in corrispondenza biunivoca con gli ideali primi di A contenuti in $\mathfrak{p}$.

1.6 Spettro primo di un anello

In questa sezione:

- con *anello* si intenderà un *anello commutativo con unità*;
- ogni omomorfismo di anelli $f : A \to B$ manderà l'unità di A nell'unità di B;
- gli ideali primi si intenderanno sempre *propri*;
- grazie al *Lemma di Zorn* ogni anello non nullo possiederà ideali massimali e ogni ideale massimale sarà *primo*;
- dato un anello R e $I \subseteq R$ un ideale, indicheremo con $V(I)$ l'insieme di tutti gli ideali primi in R che contengono I.

Si vuole definire lo *spettro primo di un anello* per poter associare ad un anello arbitrario A un oggetto geometrico che generalizzi la costruzione di varietà affini.

Definizione 1.6.1. ([11] p41) Sia A un anello,

$$Spec\ A := \{\mathfrak{p} \subset A; \quad \mathfrak{p} \quad \text{ideale primo proprio}\}$$

Si vuole dotare $Spec\ A$ della struttura di spazio topologico. Per ogni sottoinsieme $M \subset A$ sia $V(M)$ un **insieme degli ideali primi di** A **che contengono** M.

Notazione: Se x è un punto di $Spec\ A$, scriveremo spesso $\mathfrak{p}_x$ invece di x quando pensiamo a x come a un ideale primo di A.

Osservazione 1.6.1. (Cfr. [11])

- Se $\mathfrak{a}$ è l'ideale generato da M, allora $V(M) = V(\mathfrak{a})$.
- Per ogni $f \in A$ si scriverà $V(f)$ al posto di $V(\{f\})$ e sarà l'insieme degli ideali primi x tali che f diventa 0 in A/x (scriveremo anche $f(x) = 0$). Si definisce poi il **dominio di** f come il complementare di $V(f)$ in $Spec\ A$,

$$D(f) = Spec\ A - V(f) = \{x \in Spec\ A | f(x) \neq 0\}.$$

Osservazione 1.6.2. Chiaramente si ha $D(0) = \emptyset$, $D(1) = Spec\ A$ e, in generale si ha $D(u) = Spec\ A$ per ogni $u \in A$ invertibile. Sia $\mathfrak{p}$ un ideale primo e siano $f, g \in A$, si ha $fg \notin \mathfrak{p}$ se e solo se $f \notin \mathfrak{p}$ e $g \notin \mathfrak{p}$ e dunque si ha $D(f) \cap D(g) = D(fg)$.

Prima di enunciare il seguente lemma, si richiamano le definizioni di *radicale* e di *insieme degli zeri* di un sottoinsieme E di un anello A. Sia $\mathfrak{a} = (E) \subset A$ l'ideale generato da E in A, allora il radicale di $\mathfrak{a}$ o di E è:

$$\sqrt{E} = \sqrt{\mathfrak{a}} = \{f \in A : f^n \in \mathfrak{a} \text{ per qualche } n \in \mathbb{N}\},$$

mentre l'insieme degli zeri di E:

$$V(\mathfrak{a}) = V(E) = \{x \in SpecA : f(x) = 0 \ \forall f \in E\} = \{x \in Spec\ A : E \subset \mathfrak{p}_x\}$$

Lemma 1.6.1. *Si considerino sottoinsiemi E, E' e una famiglia di sottoinsiemi $(E_i)_{i \in I}$ di un anello A. Allora:*

1. $V(0) = Spec\ A\ , \quad V(1) = \emptyset$;
2. $E \subseteq E' \implies V(E) \supseteq V(E')$;
3. $V(\bigcup_{i \in I} E_i) = V(\sum_{i \in I}(E_i)) = \bigcap_{i \in I} V(E_i)$;
4. $V(EE') = V(E) \cup V(E') \qquad$ *dove* $EE' = \{ff' : f \in E, f' \in E'\}$;
5. $V(E) = V(\sqrt{E})$.

Dimostrazione. 1) e 2) sono ovvie.

3) L'insieme $V(\bigcup_{i \in I} E_i)$ consiste di tutti i punti $x \in SpecA$ tali che $\bigcup_{i \in I} E_i \subset \mathfrak{p}_x$ dove $\mathfrak{p}_x$ indica l'ideale corrispondente a x su A, quindi $E_i \subseteq \mathfrak{p}_x$ per ogni $i \in I$, e perciò coincide con $\bigcap_{i \in I} V(E_i)$. L'insieme $\bigcup_{i \in I} E_i$ è contenuto in $\mathfrak{p}_x$ per qualche $x \in SpecA$ se e solo se l'ideale $\sum_{i \in I}(E_i)$ generato da $\bigcup_{i \in I} E_i$ è contenuto in $\mathfrak{p}_x$. Si nota poi che $V(\bigcup_{i \in I} E_i)$ coincide con $V(\sum_{i \in I}(E_i))$.

4) Sia $x \in SpecA$ tale che $x \notin V(E)$ e $x \notin V(E')$. Allora si ha $E \not\subseteq \mathfrak{p}_x$ e $E' \not\subseteq \mathfrak{p}_x$ e ci sono elementi $f \in E$ e $f' \in E'$ tali che $f, f' \notin \mathfrak{p}_x$. Essendo $\mathfrak{p}_x$ un ideale primo, anche $ff' \notin \mathfrak{p}_x$ e perciò $x \notin V(EE')$, pertanto $V(EE') \subset V(E) \cup V(E')$. Per mostrare l'inclusione inversa, si prenda $x \in V(E)$, ossia $E \subseteq \mathfrak{p}_x$. Avremo $EE' \subseteq \mathfrak{p}_x$ e perciò $x \in V(EE')$. Questo prova che $V(E) \subseteq V(EE')$ e analogamente, $V(E') \subseteq V(EE')$.

5) È verificata poiché $E \subset \mathfrak{p}_x$ è equivalente a $\sqrt{E} \subset \mathfrak{p}_x$, dato che $\mathfrak{p}_x$ è un ideale primo. $\square$

Le proprietà elencate nel lemma precedente indicano che l'insieme di sottoinsiemi di *Spec* A, del tipo $V(\mathfrak{a})$, può essere visto come l'insieme dei chiusi di una topologia su *Spec* A.

Definizione 1.6.2. Sia A un anello. L'insieme *Spec* A di tutti gli ideali primi di A con la topologia in cui i chiusi sono gli insiemi $V(\mathfrak{a})$, al variare di $\mathfrak{a}$ tra gli ideali di A, è detto **spettro primo di A** o semplicemente **spettro di A**. La topologia così definita è detta **topologia di Zariski** su *Spec* A.

Lemma 1.6.2. *Sia A un anello e $X =$ Spec A il suo spettro. Esiste un'unica topologia su X, la topologia di Zariski, in cui gli insiemi chiusi sono costituiti dai sottoinsiemi del tipo $V(E) \subset X$ per qualche sottoinsieme $E \subset A$. Inoltre, ogni sottoinsieme di X è unione di insiemi del tipo $D(f)$. In particolare $D(f)$ forma una base della topologia di Zariski su X.*

Osserviamo che gli insiemi del tipo $D(f)$ sono sottoinsiemi aperti di X.

Dimostrazione. Le affermazioni 1), 3) e 4) del *Lemma 1.6.1* dimostrano le caratteristiche principali degli insiemi chiusi di una topologia. Gli insiemi $D(f)$ per funzioni $f \in A$ sono aperti e sono i complementari degli insiemi $V(f)$. Grazie al punto 4) del *Lemma 1.6.1* si ha $V(\bigcup_{i\in I} E_i) = \bigcap_{i\in I} V(E_i)$ per cui l'unione finita di insiemi $V(E)$ è ancora contenuta in X. Infine, un sottoinsieme aperto arbitrario $U \subset X =$ *Spec* A è il complementare di un insieme chiuso del tipo $V(E)$ per qualche $E \subset A$. Inoltre $V(E) = \bigcap_{f\in E} V(f)$ e quindi, $U = \bigcup_{f\in E} D(f)$, ossia ogni sottoinsieme aperto in X è unione di sottoinsiemi $D(f)$. Dunque $D(f)$ forma una base della topologia di Zariski su X. $\square$

Esempio 1.6.1. Se K è un campo, allora i suoi unici ideali sono quelli banali. Dunque *Spec* K è costituito dal singoletto $\{(0)\}$.

Proposizione 1.6.1. *Un omomorfismo di anelli $\phi : R \to A$ determina una mappa continua:*

$$\begin{array}{rcl} \phi^\sharp : Spec\ A & \to & Spec\ R \\ \mathfrak{q} & \mapsto & \phi^{-1}(\mathfrak{q}) \end{array}$$

In altre parole, Spec è un funtore controvariante dalla categoria degli anelli commutativi con unità a quella degli spazi topologici.

Dimostrazione. La mappa $\phi^\sharp$ è ben definita. Se $I \subseteq R$ è un ideale,

$$\begin{array}{rcl} (\phi^\sharp)^{-1}(V(I)) & = & \{\mathfrak{q} \in SpecA | \phi^\sharp(\mathfrak{q}) \in V(I)\} \\ & = & \{\mathfrak{q} \in SpecA | I \subseteq \phi^{-1}(\mathfrak{q})\} \\ & = & \{\mathfrak{q} \in SpecA | \phi(I) \subseteq \mathfrak{q}\} \\ & = & V(\phi(I)) \end{array}$$

Quindi $\phi^\sharp$ è continua.

□

Generalizzando la nozione di $\mathcal{I}V(I)$ enunciata nella sezione 1.4, si consideri ora lo spettro $X = SpecA$ di un anello arbitrario A, si vuole associare a un sottoinsieme $Y \subset X$ l'ideale:

$$\widetilde{I}(Y) = \{f \in A : f \in \mathfrak{p}_y \quad \forall y \in Y\} = \bigcap_{y \in Y} \mathfrak{p}_y$$

di tutti gli elementi in A che si annullano in Y. Si osservi poi che $f \in \mathfrak{p}_y$ implica $\mathcal{I}(\{y\}) = \mathfrak{p}_y$ per ogni $y \in X$.

Proposizione 1.6.2. *Sia A un anello.*

- *Siano $Y \subseteq Y' \subseteq Spec\ A$ due sottoinsiemi. Allora $\widetilde{I}(Y) \supseteq \widetilde{I}(Y')$.*
- $\widetilde{I}(\bigcup_{i \in I} Y_i) = \bigcap_{i \in I} \widetilde{I}(Y_i)$ *per ogni famiglia $(Y_i)_{i \in I}$ di sottoinsiemi in Spec A.*

1.7 Cenni di teoria delle categorie

La teoria delle categorie nasce con l'osservazione che alcune proprietà sono comuni a strutture matematiche di natura molto diversa. Nel contesto delle categorie, si possono discutere in modo naturale proprietà generali di strutture come i gruppi, gli anelli, gli insiemi o gli spazi topologici insieme alle loro rispettive trasformazioni, ossia gli omomorfismi, le funzioni o le mappe continue.

Definizione 1.7.1. Una **categoria** $\mathcal{C}$ consiste di tre dati:

1. una classe di *oggetti* $obj(\mathcal{C})$;
2. un insieme di *morfismi* $Hom_{\mathcal{C}}(A, B)$ per ogni coppia ordinata (A, B) di oggetti in $obj(\mathcal{C})$;
3. una *composizione* $Hom_{\mathcal{C}}(A, B) \times Hom_{\mathcal{C}}(B, C) \to Hom_{\mathcal{C}}(A, C)$ denotata con:
$$(f, g) \mapsto gf$$
per ogni terna ordinata A, B, C di oggetti in $obj(\mathcal{C})$;

che soddisfano i seguenti assiomi:

1. gli insiemi Hom sono a due a due disgiunti; ossia, ogni $f \in Hom_{\mathcal{C}}(A, B)$ ha un unico **dominio** A e un unico **codominio** B;
2. per ogni oggetto A, c'è un *morfismo identità* $1_A \in Hom_{\mathcal{C}}(A, A)$ tale che $f\ 1_A = f$ e $1_B\ f = f \quad \forall f \in Hom_{\mathcal{C}}(A, B)$;
3. la composizione è *associativa*: dati i morfismi $f \in Hom_{\mathcal{C}}(A, B)$, $g \in Hom_{\mathcal{C}}(B, C)$ e $h \in Hom_{\mathcal{C}}(C, D)$, allora
$$h(gf) = (hg)f$$
.

Notazione: D'ora in poi si scriverà $f : A \to B$ o $A \xrightarrow{f} B$ al posto di $f \in Hom_{\mathcal{C}}(A, B)$.

Esempio 1.7.1. Gli *insiemi* formano una categoria, indicata usualmente con **Sets**. Gli *oggetti* di questa categoria sono gli insiemi, i *morfismi* $Hom_{\mathcal{C}}(A, B)$ sono le funzioni $f : A \to B$ e la *composizione* è l'usuale composizione di funzioni.

Esempio 1.7.2. I *gruppi* formano una categoria, indicata con **Groups**: gli *oggetti* sono i gruppi, i *morfismi* sono gli omomorfismi di gruppi e la *composizione* è l'usuale composizione. Anche i *gruppi abeliani* formano una categoria: gli *oggetti* sono i gruppi abeliani, i *morfismi* sono gli omomorfismi e la *composizione* è l'usuale composizione.

Esempio 1.7.3. Gli *anelli* formano una categoria, indicata con **Rings**: gli *oggetti* sono gli anelli, i *morfismi* sono gli omomorfismi di anelli e la *composizione* è l'usuale composizione

Definizione 1.7.2. Una categoria $\mathcal{S}$ è una **sottocategoria** di una categoria $\mathcal{C}$ se:

- $obj(\mathcal{S}) \subseteq obj(\mathcal{C})$;
- $Hom_{\mathcal{S}}(A, B) \subseteq Hom_{\mathcal{C}}(A, B)$ per ogni $A, B \in obj(\mathcal{S})$;
- se $f \in Hom_{\mathcal{S}}(A, B)$ e $g \in Hom_{\mathcal{S}}(B, C)$, allora la composizione $gf \in Hom_{\mathcal{S}}(A, C)$ è uguale alla composizione $gf \in Hom_{\mathcal{C}}(A, C)$;
- se $A \in obj(\mathcal{S})$, allora l'identità $1_A \in Hom_{\mathcal{S}}(A, A)$ è uguale all'identità $1_A \in Hom_{\mathcal{C}}(A, A)$

Una sottocategoria $\mathcal{S}$ di $\mathcal{C}$ è una **sottocategoria piena** se, per ogni $A, B \in obj(\mathcal{S})$ si ha $Hom_{\mathcal{S}}(A, B) = Hom_{\mathcal{C}}(A, B)$.

Esempio 1.7.4. I gruppi abeliani sono una sottocategoria piena della categoria gruppi.

Si definisce ora la nozione di omomorfismi tra categorie, ossia i funtori.

Definizione 1.7.3. Se $\mathcal{C}$ e $\mathcal{D}$ sono categorie, allora un **funtore covariante** $T : \mathcal{C} \to \mathcal{D}$ è il dato di:

1. un $T(A) \in obj(\mathcal{D})$ per ogni $A \in obj(\mathcal{C})$;
2. un morfismo $T(f) : T(A) \to T(A')$ in $\mathcal{D}$ per ogni $f : A \to A'$ in $\mathcal{C}$;

che soddisfano i seguenti assiomi:

i) se $A \xrightarrow{f} A' \xrightarrow{g} A''$ sono morfismi in $\mathcal{C}$, allora $T(A) \xrightarrow{T(f)} T(A') \xrightarrow{T(g)} T(A'')$ in $\mathcal{D}$ soddisfano:
$$T(gf) = T(g)T(f);$$

ii) $T(1_A) = 1_{T(A)}$ per ogni $A \in obj(\mathcal{C})$.

Esempio 1.7.5. Se $\mathcal{C}$ è una categoria, allora il funtore identità $1_{\mathcal{C}} : \mathcal{C} \to \mathcal{C}$ è definito ponendo $1_{\mathcal{C}}(A) = A$ per ogni oggetto A e $1_{\mathcal{C}}(f) = f$ per ogni morfismo f.

Definizione 1.7.4. Siano $\mathcal{C}$ e $\mathcal{D}$ due categorie, un **funtore controvariante** $T : \mathcal{C} \to \mathcal{D}$, è il dato di:

1. un $T(C) \in obj(\mathcal{D})$ per ogni $C \in obj(\mathcal{C})$;
2. un morfismo $T(f) : T(C') \to T(C)$ in $\mathcal{D}$ per ogni $f : C \to C'$ in $\mathcal{C}$;

che soddisfi i seguenti assiomi:

i) se $C \xrightarrow{f} C' \xrightarrow{g} C''$ sono morfismi in $\mathcal{C}$, allora $T(C'') \xrightarrow{T(g)} T(C') \xrightarrow{T(f)} T(C)$ in $\mathcal{D}$ soddisfano:
$$T(gf) = T(f)T(g);$$

ii) $T(1_A) = 1_{T(A)}$ per ogni $A \in obj(\mathcal{C})$.

Osservazione 1.7.1. Se $\mathcal{B}$,$\mathcal{C}$ e $\mathcal{D}$ sono categorie e $F : \mathcal{B} \to \mathcal{C}$ e $G : \mathcal{C} \to \mathcal{D}$ sono funtori, allora si indica con $GF : \mathcal{B} \to \mathcal{D}$ il funtore che risulta dalla composizione del funtore F e del funtore G, ossia $GF(A) = G(F(A))$ e $GF(f) = G(F(f))$ per ogni $A \in Obj(\mathcal{B})$ e f morfismo in $\mathcal{B}$. Infatti si ha:

$$GF(1_A) = G(1_{F(A)}) = 1_{GF(A)} \quad \text{con } A \in Obj(\mathcal{B})$$

$$GF(fg) = G(F(f)F(g)) = GF(f)GF(g)$$

Si osservi che GF è covariante se entrambi i funtori sono simultaneamente co- o controvarianti. Se uno dei due funtori è covariante e l'altro è controvariante, allora GF è controvariante.

Esempio 1.7.6. $Id_{\mathcal{C}} : \mathcal{C} \to \mathcal{C}$ denota il funtore con le mappe identità come mappe identificative. $Id_{\mathcal{C}}$ è un funtore covariante. Infatti per funtori F e G si ha:

$$Id_{\mathcal{C}}F = F \quad \text{e} \quad GId_{\mathcal{C}} = G$$

Esempio 1.7.7. Un altro esempio di funtore covariante è il funtore "*dimenticanza*", che semplicemente "dimentica" alcune o tutte le strutture di un oggetto algebrico. Il funtore *forgetful* U: **Groups** $\to$ **Sets** assegna ad ogni gruppo G l'insieme UG dei suoi elementi ("dimenticando" la struttura di gruppo) e assegna ad ogni morfismo $f : G \to G'$ di gruppi la stessa funzione f, vista come funzione tra insiemi.

Esempio 1.7.8. Dato un qualsiasi anello, lo *spettro primo di un anello*, *Spec* è un funtore controvariante dalla categoria degli anelli alla categoria degli spazi affini.

$Spec$: Rings $\longrightarrow$ Spazi affini

$$\begin{array}{ccc} A & & SpecA \\ \downarrow & & \uparrow \\ B & & SpecB \\ \downarrow & & \uparrow \\ C & & SpecC \end{array}$$

Definizione 1.7.5. Se $\mathcal{C}$ è una categoria, si definisce la sua **categoria opposta** $\mathcal{C}^{op}$ la categoria tale che $obj(\mathcal{C}^{op}) = obj(\mathcal{C})$ e $Hom_{\mathcal{C}^{op}}(A, B) = Hom_{\mathcal{C}}(B, A)$. Si indicheranno con f^{op} i morfismi in $\mathcal{C}^{op}$, dove f è un morfismo in $\mathcal{C}$. La composizione in $\mathcal{C}^{op}$ è l'opposta di quella in $\mathcal{C}$ ossia $g^{op} f^{op} = (fg)^{op}$.

È noto che un funtore controvariante $\mathcal{C} \to \mathcal{D}$ corrisponde a un funtore covariante $\mathcal{C}^{op} \to \mathcal{D}$.

Definizione 1.7.6. Un morfismo $f : A \to B$ in una categoria $\mathcal{C}$ è un **isomorfismo** se esiste un morfismo $g : B \to A$ in $\mathcal{C}$ con

$$gf = 1_A \quad \text{e} \quad fg = 1_B$$

Il morfismo g è detto l'**inverso** di f.

Esempio 1.7.9. I morfismi *identità* in una categoria sono sempre isomorfismi.
Nella categoria **Sets**, gli isomorfismi sono biiezioni.
Nella categoria **Groups** e nella categoria **Rings**, gli isomorfismi sono isomorfismi nel senso usuale di gruppi (rispettivamente di anelli).

Capitolo 2

Iperstrutture algebriche

In questa sezione si vogliono esplicitare le definizioni e i maggiori risultati riguardanti le iperstrutture.

Definizione 2.0.1. Una **iperoperazione** su un insieme non vuoto H è una funzione:

$$\begin{aligned} \boxplus : H \times H &\rightarrow \mathcal{P}(H)^* \\ (x, y) &\mapsto x \boxplus y \end{aligned}$$

dove $\mathcal{P}(H)^*$ è l'insieme dei sottoinsiemi non vuoti di H.

Un'*iperoperazione* associa ad ogni coppia $(x, y) \in H \times H$ un sottoinsieme *non vuoto* di H denotato con $x \boxplus y \in \mathcal{P}(H)^*$, non necessariamente un singoletto.

Definizione 2.0.2. Una **iperstruttura** è un insieme non vuoto H dotato di una o più iperoperazioni.

Osservazione 2.0.1. Data una iperoperazione su $H \neq \emptyset$, definiamo per ogni coppia $A, B \subseteq H$ di sottoinsiemi non vuoti:

$$A \boxplus B := \bigcup_{a \in A, b \in B} (a + b).$$

Nel seguito, la notazione $(x \boxplus y) \boxplus z$ indicherà $A \boxplus \{z\}$ con $A := x \boxplus y$; inoltre dati $x, y \in H$ quando $x \boxplus y = \{z\}$, si scriverà $x \boxplus y = z$ per semplicità di notazione. Grazie a questa notazione, dati un sottoinsieme $A \subseteq H$ e un elemento $a \in H$ con $a \boxplus A$ si intenderà $\{a\} \boxplus A$.

2.1 Iperanelli e ipergruppi

Definizione 2.1.1. Un **ipergruppo canonico** $(H, \boxplus)$ è una coppia in cui H è un insieme non vuoto dotato di una iperoperazione $\boxplus$ che gode delle seguenti proprietà:

1. $\boxplus$ è `commutativa`: $x \boxplus y = y \boxplus x \quad \forall x, y \in H$.

2. $\boxplus$ è `associativa`: $(x \boxplus y) \boxplus z = x \boxplus (y \boxplus z) \quad \forall x, y, z \in H$.

3. Esiste l'elemento `neutro`: $\exists! 0_H \in H$ tale che $0_H \boxplus x = x = x \boxplus 0_H \quad \forall x \in H$.

4. Esiste un `unico inverso`: $\forall x \in H \ \exists! y \in H$ t.c. $0 \in x \boxplus y$; si scriverà $y = -x$.

5. `Reversibilità`: $x \in y \boxplus z \iff z \in x - y \quad \forall x, y, z \in H$.

In letteratura esistono definizioni più generali di *ipergruppi* ma noi ci occuperemo solo di quelli canonici e per brevità li chiameremo semplicemente *"ipergruppi"*.

Esempio 2.1.1. Sull'insieme $\{0, 1\}$, si definisce l'operazione $\boxplus$ data dalle formule:

$$0 \boxplus 0 = \{0\} \ , \quad 0 \boxplus 1 = \{1\} = 1 \boxplus 0 \ , \quad 1 \boxplus 1 = \{0, 1\}$$

Questo è un ipergruppo, dato che soddisfa le condizioni della *Definizione 3.1.1.* Questo è l'unico ipergruppo di due elementi, che non provenga da un gruppo. Infatti le prime tre condizioni sono fissate dell'essere ipergruppo. Resta da decidere $1 \boxplus 1$:

- ⋄ se vale $\{0\}$ proviene da un gruppo,

- $\diamond$ se vale $\{0,1\}$ è l'esempio dato,
- $\diamond$ se vale $\{1\}$ salta l'esistenza dell'inverso.

Osservazione 2.1.1. Ad ogni gruppo abeliano $(G, +_G)$ resta associato un ipergruppo canonico ponendo

$$\boxplus : G \times G \to \mathcal{P}(G)^*$$

$$(x, y) \mapsto \{x +_G y\}$$

Definizione 2.1.2. Un **iperanello commutativo di Krasner** è un insieme non vuoto R tale che:

1. $(R, \boxplus)$ è un ipergruppo con elemento neutro indicato con 0;
2. $(R, \cdot, 1)$ è un monoide commutativo, nel senso usuale, e sono soddisfatte le seguenti condizioni:
   (a) $\boxplus$ e $\cdot$ sono *compatibili*, ossia $\forall x, y, z \in R$ valgono $x(y \boxplus z) = xy \boxplus xz$ e $(x \boxplus y)z = xz \boxplus yz$.
   (b) 0 è un elemento "che assorbe" ossia $\forall x \in R$ vale $x \cdot 0 = 0 = 0 \cdot x$.
   (c) $0 \neq 1$.

Si noti che in (a) stiamo usando la notazione $xR = \{xa, a \in R\}$ per ogni $R \in \mathcal{P}(R)^*$.

Conseguenze 2.1.1. Dalla definizione di *iperanello di Krasner* si può dedurre che:

1. $-(-a) = a \quad \forall a \in R$.
2. 0 è l'unico elemento t.c. $\forall a \in R$ c'è un elemento $-a \in R$ con la proprietà $0 \in a \boxplus (-a)$.

3. $-0 = 0$.

4. $-(a \boxplus b) = -a \boxplus -b \quad \forall a, b \in R$.

5. $-A = (-1)A = \{-a | a \in A\}$

Osservazione 2.1.2.

- Ad ogni anello commutativo con unità $(R, +_R, \cdot_R)$ posso associare un iperanello di Krasner ponendo:

$$\boxplus : R \times R \to \mathcal{P}(R)^*$$

$$(x, y) \mapsto \{x +_R y\}$$

e tenendo $\cdot_R$ come moltiplicazione.

- Vi sono nozioni più generali di iperanello che però noi non considereremo.

- Vi sono inoltre iperanelli di Krasner non commutativi che però noi non considereremo.

Definizione 2.1.3. Un iperanello di Krasner R è detto **iperdominio** se $ab = \{0\}$ implica $a = 0$ o $b = 0$.

Esempio 2.1.2. Sia $\mathbf{R} := \{0, 1, 2\}$ con l'iperoperazione e la moltiplicazione date nelle seguenti tabelle:

$\boxplus$	0	1	2
0	$\{0\}$	$\{1\}$	$\{2\}$
1	$\{1\}$	$\{1\}$	R
2	$\{2\}$	R	$\{2\}$

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	2

Allora $(R, \boxplus, \cdot)$ è un iperanello di Krasner e anzi un iperdominio.

Esempio 2.1.3. Sia $(G, *)$ un gruppo abeliano finito con m elementi, $m > 3$, si definisca un'iperaddizione $\boxplus$ e una moltiplicazione $\cdot$ su $H = G \cup \{0\}$ date da:

- $a \boxplus 0 = 0 \boxplus a = \{a\}$ per ogni $a \in H$;
- $a \boxplus a = \{a, 0\}$ per ogni $a \in G$;
- $a \boxplus b = b \boxplus a = H \setminus \{a, b\}$ per ogni $a, b \in G$, $a \neq b$;
- $a \cdot 0 = 0$ per ogni $a, b \in H$;
- $a \cdot b = a * b$ per ogni $a, b \in G$:

Allora $(H, \boxplus, \cdot)$ è un iperanello di Krasner.

Osservazione 2.1.3. In generale, in un iperanello non è soddisfatta la proprietà distributiva doppia. Ossia, la seguente identità

$$(a \boxplus b)(c \boxplus d) = ac \boxplus ad \boxplus bc \boxplus bd$$

in generale non è soddisfatta. Invece, l'identità

$$(a \boxplus b)(c \boxplus d) \subseteq ac \boxplus ad \boxplus bc \boxplus bd$$

resta verificata. Infatti per ogni elemento $x \in (c \boxplus d)$ la distributività mi dà $(a \boxplus b)x = ax \boxplus bx$, e si ha $(a \boxplus b)(c \boxplus d) = \bigcup_{x \in (c \boxplus d)} (a \boxplus b)x = \bigcup_{x \in (c \boxplus d)} (ax \boxplus bx)$. Ma d'altra parte,

$$ac \boxplus ad \boxplus bc \boxplus bd = (ac \boxplus ad) \boxplus (bc \boxplus bd) = a(c \boxplus d) \boxplus b(c \boxplus d) \supseteq ax \boxplus bx$$

per ogni $x \in (c \boxplus d)$ e quindi:

$$ac \boxplus bc \boxplus ad \boxplus bd \supseteq \bigcup_{x \in (c \boxplus d)} (ax \boxplus bx) = (a \boxplus b)(c \boxplus d).$$

Definizione 2.1.4. Siano $(R_1, \boxplus_1, \cdot_1)$ e $(R_2, \boxplus_2, \cdot_2)$ iperanelli.

Un'applicazione $\varphi : R_1 \to R_2$ è detta **omomorfismo di iperanelli** se:

1. φ è un *omomorfismo di ipergruppi*, ossia

$$\varphi(a \boxplus_1 b) \subseteq \varphi(a) \boxplus_2 \varphi(b) \quad \forall a, b \in R_1 \quad \text{e} \quad \varphi(0) = 0$$

2. φ è un *omomorfismo di monoidi* rispetto alla moltiplicazione, ossia

$$\varphi(a \cdot_1 b) = \varphi(a) \cdot_2 \varphi(b) \quad \forall a, b \in R_1 \quad \text{e} \quad \varphi(1) = 1$$

Definizione 2.1.5. Sia R un iperanello. Con **estensione di un iperanello** R si intende un iperanello L tale che ci sia un omomorfismo iniettivo $i : R \to L$ di iperanelli. Un **sottoiperanello** H di R è un sottoinsieme di R tale che H sia esso stesso un iperanello con addizione e moltiplicazione indotte da quelle di R, ossia $a \boxplus_H b = (a \boxplus_R b) \cap H$ e $a \cdot_H b = a \cdot_R b$.

Osservazione 2.1.4. In generale, se H è un sotto-iperanello di un iperanello R, $\forall a, b \in H$ si avrà $(a \boxplus_H b) \subseteq (a \boxplus_R b)$.

Definizione 2.1.6. Sia $\phi : R_1 \to R_2$ un omomorfismo da un iperanello R_1 in un altro iperanello R_2. Allora l'insieme $\{x \in R_1 | \phi(x) = 0\}$ è detto **nucleo** di ϕ e si denota con $Ker\phi$. L'insieme $\{\phi(x) | x \in R_1\}$ è detto invece **immagine** di ϕ e si denota con $Im\phi$.

Osservazione 2.1.5. Si devono trattare con cautela le *estensioni di un iperanello* R quando l'omomorfismo iniettivo di anelli non sia stretto. Infatti, si avrà $(a \boxplus_R b) \subseteq (a \boxplus_L b)$ per $a, b \in R$, ma in generale non varrà l'uguaglianza.

Esempio 2.1.4. In questo esempio si vuole mostrare una via alternativa di costruire un *iperanello* attraverso l'algebra commutativa classica.
Sia A un anello commutativo con unità e indichiamo con $A^\times$ il **gruppo delle unità**

$$A^\times := \{a \in A | \exists b \in A \text{ tale che } ab = 1\}.$$

Sia G un sottogruppo moltiplicativo di $A^\times$, ossia $A/G = \{aG | a \in A\}$. Si noti che G agisce su A tramite l'operazione

$$G \times A \to A$$

$$(g, a) \mapsto ag.$$

Fissato $a \in A$, indichiamo con $aG = \{ag,\ g \in G\}$ e la chiameremo **orbita di** a **in** A. Indicheremo inoltre con A/G l'**insieme delle orbite**. Esso ha una naturale struttura di iperanello ponendo:

- Moltiplicazione:

$$m : A/G \times A/G \to A/G$$

$$(xG, yG) \mapsto xyG \quad \forall x, y \in A.$$

- Iperaddizione:

$$\boxplus : A/G \times A/G \to \mathcal{P}(A/G)^*$$

$$(xG, yG) \mapsto \{qG | q = xt + ys \text{ per qualche } t, s \in G\} \quad \forall x, y \in A.$$

Allora A/G è un iperanello detto *iperanello quoziente*.

Esempio 2.1.5. Sia $A = \mathbb{Z}/6\mathbb{Z}$. Il gruppo delle unità è:

$$A^\times = \{1, 5\}$$

e dunque l'insieme delle orbite è

$$A/G = \{0G, 1G, 2G, 3G\}.$$

A/G è un iperanello di Krasner con la moltiplicazione m e l'iperaddizione $\boxplus$ definite nell'*Esempio 2.1.4*, che qui sotto esplicitiamo:

m	$0G$	$1G$	$2G$	$3G$
$0G$	$0G$	$0G$	$0G$	$0G$
$1G$	$0G$	$1G$	$2G$	$3G$
$2G$	$0G$	$2G$	$4G$	$0G$
$3G$	$0G$	$3G$	$0G$	$3G$

$\boxplus$	$0G$	$1G$	$2G$	$3G$
$0G$	$0G$	$\{1G, 5G\}$	$\{2G, 4G\}$	$3G$
$1G$	$\{1G, 5G\}$	$\{2G, 4G\}$	$\{1G, 3G, 5G\}$	$\{2G, 4G\}$
$2G$	$\{2G, 4G\}$	$\{1G, 3G, 5G\}$	$\{2G, 4G\}$	$\{1G, 5G\}$
$3G$	$\{3G\}$	$\{2G, 4G\}$	$\{1G, 5G\}$	$0G$

2.2 Ipercampi

Come per *ipergruppi* e *iperanelli*, la nozione di *ipercampo* è l'immediata generalizzazione della nozione di campo.

Definizione 2.2.1. Sia $(R, \boxplus, \cdot)$ un iperanello (di Krasner). Se $(R \backslash \{0\}, \cdot)$ è un gruppo abeliano, allora $(R, \boxplus, \cdot, 0, 1)$ si dice **ipercampo**.

Esempio 2.2.1. Sia $\mathbf{K} := \{0, 1\}$ con l'iperoperazione e la moltiplicazione data da:

$\boxplus$	0	1
0	$\{0\}$	$\{1\}$
1	$\{1\}$	$\{0, 1\}$

$\cdot$	0	1
0	0	0
1	0	1

Allora $\mathbf{K}$ è un ipercampo ed è chiamato *ipercampo di Krasner*.

Esempio 2.2.2. Sia $\mathbf{S} := \{-1, 0, 1\}$ dotato di un'iperoperazione e una moltiplicazione, entrambe commutative:

$\boxplus$	-1	0	1
-1	-1	-1	$\{-1, 0, 1\}$
0	-1	0	1
1	$\{-1, 0, 1\}$	1	1

$\cdot$	-1	0	1
-1	1	0	-1
0	0	0	0
1	-1	0	1

Allora $\mathbf{S}$ è un ipercampo, detto *ipercampo dei segni* in quanto l'iperoperazione definita sopra segue la regola dei segni.

Esempio 2.2.3. Sia $\mathcal{T}\mathbb{R} := (\mathbb{R}, +_T, \cdot)$; dove l'insieme soggiacente è l'insieme dei numeri reali e la moltiplicazione è la solita moltiplicazione tra numeri reali. L'iperaddizione è data da:

$$x +_T y = \begin{cases} \{x\} & \text{se } |x| > |y| \\ \{y\} & \text{se } |x| < |y| \\ \{x\} & \text{se } x = y \\ [-|x|, |x|] \text{ ,un intervallo chiuso,} & \text{se } x = y \end{cases}$$

$\mathcal{T}\mathbb{R}$ è un ipercampo, detto *ipercampo di Viro.*

Esempio 2.2.4. Sia $\mathbb{T} := \mathbb{R} \cup \{\infty\}$ l'insieme dei numeri reali unito al simbolo di ∞. La moltiplicazione $\cdot$ è l'usuale addizione tra numeri reali tale per cui $a \cdot (\infty) = \infty$. L'iperaddizione $\boxplus$ è data da:

$$x \boxplus y = \begin{cases} \min\{x, y\} & \text{se } x \neq y \\ [x, +\infty] & \text{se } x = y \end{cases}$$

$\mathbb{T}$ è chiamato *ipercampo tropicale.*

Esempio 2.2.5. Grazie alla *Definizione 2.1.6*, si nota che $\mathcal{T}\mathbb{R}$ è un'estensione dall'ipercampo $\mathbf{S}$.

Proposizione 2.2.1. *In ogni estensione di iperanelli R dell'ipercampo di Krasner* $\mathbf{K}$ *si ha $x \boxplus x = \{0, x\}$ $\forall x \in R$ e inoltre*

$$a \in a \boxplus b \iff b \in \{0, a\}$$

In particolare, non ci sono estensioni dell'ipercampo $\mathbf{K}$ *di cardinalità* 3 *o* 4.

Dimostrazione. Dato che $1 \boxplus 1 = \{0, 1\}$ si ha $x \boxplus x = \{0, x\}$ grazie alla proprietà distributiva. Si assuma che $a \in a \boxplus b$ in R. Allora, se $a \boxplus a = \{0, a\}$ si ha $-a = a$ e, grazie alla condizione di reversibilità nella definizione di ipergruppo, si ha $b \in a - a = \{0, a\}$. Al contrario, se $b \in \{0, a\}$ segue che $a \in a \boxplus b = \{a, a + b\}$.

Se F è un'estensione dell'ipercampo $\mathbf{K}$ di cardinalità maggiore di 2, allora F contiene un elemento $\alpha \notin \{0, 1\}$. Se la cardinalità fosse 3, avrei $F = \{0, 1, \alpha\}$ e il sottoinsieme $1 \boxplus \alpha$ non potrebbe contenere 0 (dato che 1 è l'unico opposto di 1), o 1 o α grazie alla prima parte di questa proposizione. Infatti, se $1 \in 1 \boxplus \alpha$ allora $\alpha \in \{0, 1\}$ e se $\alpha \in 1 \boxplus \alpha$ allora $1 \in \{0, \alpha\}$. Se F fosse un'estensione dell'ipercampo $\mathbf{K}$ di cardinalità 4, scriviamolo come $F = \{0, \xi_1, \xi_2, \xi_3\}$ con $\xi_i = 1$. Dalla prima parte di questa proposizione, sappiamo che ciascun ξ_i coincide con il proprio opposto e che la somma $\xi_j \boxplus \xi_k$, per $j \neq k$ deve contenere il terzo elemento non nullo ξ_l di F e non contiene nè ξ_j, nè ξ_k. Inoltre non può contenere 0 perché ξ_j non è l'opposto di ξ_k, ma questo contraddice l'associatività dell'iperaddizione per $\sum \xi_i$. Infatti per $\{i, j, h\} = \{1, 2, 3\}$, avrei $(\xi_i \boxplus \xi_j) \boxplus \xi_h = \{\xi_h\} \boxplus \xi_h = \{0, \xi_h\}$, mentre $\xi_i \boxplus (\xi_j \boxplus \xi_h) = \xi_i \boxplus \{\xi_i\} = \{0, \xi_i\}$. $\square$

2.3 Iperideali

Definizione 2.3.1. Sia R un iperanello.

- Un sottoinsieme non vuoto I di R si dice **iperideale** se valgono le seguenti condizioni:

  1. $\forall a, b \in I$, si ha che $a \boxplus b \subseteq I$.
  2. $\forall r \in R$ e $a \in I$ si ha che $ra \in I$.
  3. $\forall a \in I$ si ha che $-a \in I$.

- Un iperideale $I \subset R$ si dice **primo** se I soddisfa la seguente proprietà:

$$\text{Se } xy \in I, \text{ allora} \quad x \in I \text{ o } y \in I, \quad \forall x, y \in I.$$

- Un iperideale $I \subsetneq R$ si dice **massimale** se I soddisfa la seguente proprietà:

se $J \subset R$ è un iperideale di R che contiene I , allora $I = J$.

Osservazione 2.3.1. $\diamond$ Si osserva che se $\phi : R_1 \to R_2$ è un omomorfismo di iperanelli, allora $Ker\phi$ è un iperideale di R_1.

$\diamond$ Si osservi poi se R è un anello e indichiamo con la stessa lettera l'iperanello associato, allora $I \subseteq R$ è un ideale primo se e solo se I è un iperideale primo.

Definizione 2.3.2. Siano A e B due sottoinsiemi non vuoti di un iperanello R.

1. La somma $A \boxplus B$ è l'ipersomma definita nella *Definizione 2.0.1*

$$A \boxplus B = \{x | x \in a \boxplus b \text{ per qualche } a \in A, b \in B\} = \bigcup_{a \in A, b \in B} a \boxplus b.$$

2. Il prodotto AB è definito da:

$$AB = \{x | x \in \sum_{i=1}^{n} a_i b_i \quad a_i \in A, b_i \in B, n \in \mathbb{Z}^+\}.$$

Se A e B sono iperideali di R, allora $A \boxplus B$ e AB sono ancora iperideali di R.

Osservazione 2.3.2. Un iperideale proprio M di R, ossia tale che $M \neq R$, è un iperideale massimale di R se gli unici iperideali di R che contengono M sono M stesso e R.

Definizione 2.3.3. Sia X un sottoinsieme di un iperanello R. Sia $A_i = \{A_i | i \in I\}$ la famiglia di tutti gli iperideali in R che contengono X. Allora $\bigcap_{i \in I} A_i$ è detto **iperideale generato da** X. Questo iperideale di denota con $< X >$; se $X = \{x_1, x_2, \ldots, x_n\}$, allora l'iperideale $< X >$ si denoterà con $< x_1, x_2, \ldots x_n >$.

Osservazione 2.3.3. Esiste una corrispondenza biunivoca che conserva l'ordinamento tra gli iperideali $\mathfrak{s}$ di R che contengono $\mathfrak{r}$ e gli iperideali $\bar{\mathfrak{s}}$ di $R/\mathfrak{r}$ data da $\mathfrak{s} = \phi^{-1}(\bar{\mathfrak{s}})$, dove ϕ è la mappa di proiezione da R in $R/\mathfrak{r}$.

Proposizione 2.3.1. *Sia R un iperanello.*

1. *Sia I un iperideale proprio di R. Allora, esiste un iperideale massimale $\mathfrak{m}$ tale che $I \subseteq \mathfrak{m}$.*

2. *Ogni iperideale massimale $\mathfrak{m}$ è primo.*

Dimostrazione.

1. Per prima cosa, dobbiamo dimostrare che ogni iperanello possiede almeno un iperideale massimale e per farlo si vuole utilizzare il *Lemma di Zorn.* Sia Δ l'insieme di tutti gli iperideali diversi da (1) in R. Δ è non vuoto dato che $(0) \in \Delta$. Ora si ordina Δ rispetto all'inclusione per poi mostrare che ogni catena in Δ possiede un maggiorante in Δ. Sia $(\mathfrak{m}_\alpha)$ una catena di ideali in Δ, per ogni coppia di indici α e β, assumiamo senza perdere di generalità $(\mathfrak{m}_\alpha) \subseteq (\mathfrak{m}_\beta)$. Sia poi $\mathfrak{m} = \bigcup_\alpha \mathfrak{m}_\alpha$; $\mathfrak{m}$ è un ideale e $1 \notin \mathfrak{m}$ dato che $1 \notin \mathfrak{m}_\alpha$ per ogni α. Perciò $\mathfrak{m} \in \Delta$ e $\mathfrak{m}$ è un maggiorante della catena da cui segue che Δ possiede un elemento massimale.
   Successivamente, consideriamo $I \subsetneq R$ un iperideale proprio di R, per dimostrare che esiste un iperideale massimale $\mathfrak{m}$ tale per cui $I \subseteq \mathfrak{m}$, si applica quanto affermato prima all'iperanello R/I, che sicuramente è non nullo poiché $I \subsetneq R$. Grazie all'*Osservazione 2.3.3*, si ha che la controimmagine di ogni ogni ideale massimale $\mathfrak{m}$ in R/I rispetto alla proiezione $R \to R/I$ è un ideale massimale in R contenente I.

2. Siano $x, y \in R$ elementi tali che $xy \in \mathfrak{m}$ e $x \notin \mathfrak{m}$. Allora l'insieme $\mathfrak{m} \boxplus xR = \bigcup\{a \boxplus b | a \in \mathfrak{m}, b \in xR\}$ è un iperideale di R contenente sia $\mathfrak{m}$ che xR, ma

diverso da $\mathfrak{m}$ perché si ha $x \in \mathfrak{m} \boxplus xR$ e $x \notin \mathfrak{m}$. Quindi $\mathfrak{m} \boxplus xR = R$ e dunque si conclude che $1 \in \mathfrak{m} \boxplus xR$. Pertanto $1 \in a \boxplus xr$ per qualche $a \in \mathfrak{m}$ e $r \in R$. In particolare si ottiene $y \in y(a \boxplus xr) = ya \boxplus yxr \subseteq \mathfrak{m} \boxplus \mathfrak{m} \subseteq \mathfrak{m}$. Quindi $y \in \mathfrak{m}$.

$\square$

2.4 Teorema degli zeri di Hilbert

In questa sezione R indicherà sempre un iperanello e $V(I)$ l'insieme degli iperideali primi di R contenenti un iperideale I.

Lemma 2.4.1. *Sia $I \subseteq R$ un iperideale. Allora il seguente insieme:*

$$\sqrt{I} := \{r \in R | \exists n \in \mathbb{N} \text{ tale che } r^n \in I\}$$

è un iperideale.

Dimostrazione. Sicuramente $0 \in \sqrt{I}$.
Sia $a \in \sqrt{I}$, ossia $a^n \in I$ per qualche $n \in \mathbb{N}$ e sia $r \in R$. Dato che I è un iperideale, si ha $r^n a^n = (ra)^n \in I$. Da cui segue che $ra \in \sqrt{I}$; dunque la proprietà 3 è soddisfatta.
Chiaramente, $(-a)^n$ potrebbe essere o a^n o $-a^n$. Ma, sia a^n sia $-a^n$ sono in I, da cui segue che $-a \in \sqrt{I}$; dunque $\sqrt{I}$ soddisfa la 2.
Infine siano $a, b \in \sqrt{I}$, ossia a^n, $b^m \in I$ per opportuni $n, m \in \mathbb{Z}^+$. Allora per $l \geq (n+m)$ si ha che $(a \boxplus b)^l \subseteq \sum \binom{l}{k} a^k b^{l-k} \subseteq I$, dove $\sum$ è da intendersi come ipersomma e così la moltiplicazione per $\binom{l}{k}$. Questo implica che $(a \boxplus b) \subseteq \sqrt{I}$; quindi sono soddisfatte le tre condizioni della definizione di *iperideale*, perciò $\sqrt{I}$ è un iperideale. $\square$

Lemma 2.4.2 (Nullstellensatz). *Sia R un iperanello e sia I un iperideale di R. Allora:*

$$\sqrt{I} = \bigcap_{\mathfrak{p}\in V(I)} \mathfrak{p}$$

Dimostrazione. Iniziamo dimostrando l'inclusione $\sqrt{I} \subseteq \bigcap_{\mathfrak{p}\in V(I)} \mathfrak{p}$. Si supponga che $a \in \sqrt{I}$, allora $a^n \in I \subseteq \mathfrak{p}$ per ogni $\mathfrak{p} \in V(I)$. Dato che $\mathfrak{p}$ è un iperideale primo, segue che $a \in \mathfrak{p}$; quindi, $\sqrt{I} \subseteq \mathfrak{p}$ per ogni $\mathfrak{p} \in V(I)$.

Viceversa, si supponga che $f \in \bigcap_{\mathfrak{p}\in V(I)} \mathfrak{p}$ e si supponga per assurdo che $f \notin \sqrt{I}$. Questo implicherebbe che:

$$S := \{1, f, f^2, \dots\} \cap I = \emptyset$$

Sia Σ l'insieme degli iperideali J di R tali che $S \cap J = \emptyset$ e $I \subseteq J$. Allora $\Sigma \neq \emptyset$, in quanto $I \in \Sigma$. Σ è non vuoto e lo si ordina rispetto all'inclusione; grazie al *Lemma di Zorn*, Σ ha un elemento massimale $\mathfrak{q}$. Infatti, data una catena $(\mathfrak{q}_\alpha)$ di iperideali in Σ; $\mathfrak{q} = \bigcup_\alpha \mathfrak{q}_\alpha$ è ancora un iperideale tale che $S \cap \mathfrak{q} = \emptyset$ e $I \subseteq \mathfrak{q}$. Dunque $\mathfrak{q} \in \Sigma$ e $\mathfrak{q}$ è un maggiorante della catena $(\mathfrak{q}_\alpha)$, pertanto si può concludere che Σ ha un elemento massimale $\mathfrak{q}$. Resta da dimostrare che $\mathfrak{q}$ è primo. Dato un $x \in R$ il seguente insieme:

$$\mathfrak{q} \boxplus xR := \bigcup \{a \boxplus b \mid a \in \mathfrak{q},\ b \in xR\}$$

è un iperideale in quanto somma di due iperideali e $\mathfrak{q}$ è primo grazie alla *Proposizione 2.3.1* poiché $\mathfrak{q}$ è massimale.

Se $x, y \notin \mathfrak{q}$ allora $\mathfrak{q}$ è contenuto propriamente negli iperideali $\mathfrak{q} \boxplus xR$ e $\mathfrak{q} \boxplus yR$. Pertanto, $\mathfrak{q} \boxplus xR, \mathfrak{q} \boxplus yR \notin \Sigma$ per la massimalità di $\mathfrak{q}$ in Σ. Da cui segue che $f^n \in \mathfrak{q} \boxplus xR$ e $f^m \in \mathfrak{q} \boxplus yR$ per qualche $n, m \in \mathbb{N}$. In altre parole, $f^n \in a_1 \boxplus xr_1$, $f^m \in a_2 \boxplus yr_2$ per qualche $a_1, a_2 \in \mathfrak{q}$ e $r_1, r_2 \in R$. Perciò si ha:

$$f^{n+m} \in (a_1 \boxplus xr_1)(a_2 \boxplus yr_2) \subseteq a_1a_2 \boxplus a_1yr_2 \boxplus a_2xr_1 \boxplus xyr_1r_2 \subseteq \mathfrak{q} \boxplus xyR$$

Questo implica che $xy \notin \mathfrak{q}$ perché se $xy \in \mathfrak{q}$ allora $f^{n+m} \in \mathfrak{q}$, ma si è assunto che $f^l \notin \mathfrak{q} \quad \forall l \in \mathbb{N}$. Segue che $\mathfrak{q}$ è un iperideale primo contenente I tale che $S \cap \mathfrak{q} = \emptyset$. Ma questo è impossibile se si prende $f \in \bigcap_{\mathfrak{p} \in V(I)} \mathfrak{p}$ in quanto $\bigcap \mathfrak{p} \subseteq \mathfrak{q}$. E questo conclude la dimostrazione. □

Proposizione 2.4.1. *Se I e J sono iperideali di R, le seguenti condizioni sono equivalenti:*

1. $V(I) \subseteq V(J)$*;*
2. $J \subseteq \sqrt{I}$ *e* $\sqrt{J} \subseteq \sqrt{I}$*.*

Dimostrazione. **1)** $\Longrightarrow$ **2)** ogni iperideale primo di R, contenente I contiene anche J, perciò $J \subseteq \sqrt{I}$ e $\sqrt{J} \subseteq \sqrt{I}$.

2) $\Longrightarrow$ **1)** Sia $\mathfrak{p} \in V(I)$ un ideale, allora $\mathfrak{p} \supseteq \sqrt{I}$ per il *Lemma 2.4.2*, da cui $\mathfrak{p} \supseteq J$ e $\mathfrak{p} \in V(J)$.

□

2.5 Iperanello delle frazioni

Definizione 2.5.1. (Cf. [21]) Un sottoinsieme S di un iperanello R si dice **parte moltiplicativa** $\iff$ $1 \in S$ e $\forall x, y \in S \quad xy \in S$.

Sia S un sottoinsieme moltiplicativo di un iperanello R con $0 \notin S$. Vogliamo costruire l'iperanello delle frazioni $S^{-1}R$ in modo analogo a quanto fatto per gli anelli usuali.

Si consideri la seguente relazione in $R \times S$:

$$(h, s) \sim (h', s') \iff \exists x \in S \text{ t.c. } xhs' = xh's$$

Questa è una relazione di equivalenza. Si indicherà con $S^{-1}R$ l'insieme $(R \times S/\sim)$ di classi di equivalenza. Denotiamo con $\frac{r}{s}$ o $[(r,s)]$ la classe di equivalenza di $(r,s) \in R \times S$ sotto la relazione di equivalenza definita sopra. Dunque $S^{-1}R$ è l'insieme di tutte le classi di equivalenza. Lo dotiamo ora di una struttura di iperanello.
In $(R \times S/\sim)$ si può definire un'**ipersomma** e un **prodotto**.
L'**ipersomma** è data data:

$$[(h,s)] \boxplus [(k,t)] = [(ht \boxplus ks, st)] = \{[(y,st)] : y \in ht \boxplus ks\}$$

e il **prodotto** è dato da:

$$[(h,s)] \cdot [(k,t)] = [(hk,st)]$$

Osservazione 2.5.1. Le due operazioni appena esplicitate sono ben definite; infatti se:

$$(h,s) \sim (h',s') \text{ allora } \exists x \in S \text{ t.c. } xhs' = xh's$$

e

$$(k,t) \sim (k',s') \text{ allora } \exists w \in S \text{ t.c. } wkt' = wk't$$

Perciò, $\forall [(y',s't')] \in [(h',s')] \boxplus [(k',t')]$ esiste $[(y,st)] \in [(h,s)] \boxplus [(k,t)]$ t.c. $[(y,st)] = [(y',s't')]$. Infatti:
$[(y',s't')] \in [(h',s')] \boxplus [(k',t')] \implies y' \in h't' \boxplus k's' \implies y'st \in h't'st \boxplus k's'st = h's(tt') \boxplus k't(ss') \implies xwy'st \in (ht \boxplus ks)xws't' \implies \exists y \in ht \boxplus ks : xwsty' = xws't'y \implies (y,st) \sim (y',s't')$ essendo $xw \in S$. L'ipersomma è quindi ben definita, e in modo analogo si dimostra che il prodotto è ben definito.

Proposizione 2.5.1. *$(S^{-1}R, \boxplus, \cdot)$ è un iperanello commutativo con unità, detto **iperanello delle frazioni rispetto a** S.*

Dimostrazione. Si deve dimostrare che $(S^{-1}R, \boxplus, \cdot)$ soddisfi tutte le proprietà della definizione di iperanello commutativo:

1. $\boxplus$ è associativa, ossia

$$\Big([(h,s)] \boxplus [(k,t)]\Big) \boxplus [(j,u)] = [(h,s)] \boxplus \Big([(h,s)] \boxplus [(k,t)]\Big)$$

   Infatti:
   $\Big([(h,s)] \boxplus [(k,t)]\Big) \boxplus [(j,u)] = [(ht \boxplus ks, st)] \boxplus [(j,u)] = \Big\{[(y,st)] : y \in ht \boxplus ks\Big\} \boxplus [(j,u)] = \bigcup_{y \in ht \boxplus ks}([(y,st)] \boxplus [(j,u)]) = \bigcup_{w \in ku \boxplus jt}\Big\{[(v,stu)] : v \in htu \boxplus ws\Big\} = \bigcup_{w \in ku \boxplus jt}\Big([(h,s)] \boxplus [(w,tu)]\Big) = [(h,s)] \boxplus \Big\{[(w,tu)] : w \in ku \boxplus jt\Big\} = [(h,s)] \boxplus \Big([(k,t)] \boxplus [(j,u)]\Big)$.

2. La proprietà commutativa di $\boxplus$ segue dalle analoghe proprietà di $\boxplus$ e $\cdot$ in R.

3. $[(0,w)]$ con $w \in S$ è l'elemento unità dell'ipersomma in $S^{-1}R$.

4. $\forall [(h,s)] \in S^{-1}R \; \exists! \; [(-h,s)] \in S^{-1}R$ t.c. $-[(h,s)] = [(-h,s)]$.

5. $[(h,s)] \in [(k,t)] \boxplus [(j,u)] \implies [(k,t)] \in [(h,s)] - [(j,u)]$ infatti: $[(h,s)] \in [(k,t)] \boxplus [(j,u)] \implies h \in tj \boxplus ku$ e $s = tu \implies ku \in h - tj \implies ku^2 \in hu - tju \implies [(ku^2, tu^2)] \in [(hu, tju, tu^2)] = [(h,tu)] - [(j,u)]$.

6. Le proprietà associativa e commutativa del prodotto in $S^{-1}R$ seguono dalle analoghe proprietà in R.

7.
   - $\Big([(h,s)] \boxplus [(k,t)]\Big) \cdot [(j,u)] = \Big\{[(y,st)] \cdot [(j,u)] : y \in ht \boxplus ks\Big\} = \Big\{[(yj, stu)] : y \in ht \boxplus ks\Big\}$;
   - $[(h,s)] \cdot [(j,u)] \boxplus [(k,t)] \cdot [(j,u)] = [(hj, su)] \boxplus [(kj, tu)] = \Big\{[(w, stu^2)] : w \in hjtu \boxplus kjsu\Big\} = \Big\{[(v, stu)] : v \in hjt \boxplus kjs\Big\}$

8. $S^{-1}R$ è unitario con $[(1,1)]$ elemento unità.

$\square$

Osservazione 2.5.2. Se $[(h,s)] \in S^{-1}R$ con $h \in S$, allora $[(h,s)] \in S^{-1}R$ e $[(s,h)] = [(h,s)]^{-1}$.

Proposizione 2.5.2. *(Cfr. [21] p77) La mappa di localizzazione i_R^S:*

$$i_R^S : R \to S^{-1}R$$

$$h \longmapsto [(h,1)] = \tfrac{h}{1}$$

*è un omomorfismo di iperanelli. Inoltre $Ker(i_R^S) = \{0\} \iff S$ non ha divisori dello zero. Perciò, se R è un iperdominio di integrità e $S = R \setminus \{0\}$, $S^{-1}R$ è un ipercampo, detto **ipercampo delle frazioni di** R e $i_R^S(R)$ è un subiperanello di $S^{-1}R$ isomorfo a R.*

Definizione 2.5.2. Se I è un iperideale,

$$S^{-1}I := \{\frac{i}{s} :\ i \in I, s \in S\} = i_R^S(I)$$

$S^{-1}I$ è detta **estensione di** I in $S^{-1}R$.

Si noti che $\frac{r}{s} \in S^{-1}I$ non implica per forza che $r \in I$, in quanto è possibile che $\frac{a}{s} = \frac{r}{s}$ con $a \in I$ e $r \notin I$.

Lemma 2.5.1. *Sia S un sottoinsieme moltiplicativo di un iperanello R. Se I e J sono ideali di R, allora:*

1. $S^{-1}(I \boxplus J) = S^{-1}I \boxplus S^{-1}J$;

2. $S^{-1}(IJ) = (S^{-1}I)(S^{-1}J)$;

3. $S^{-1}(I \cap J) = S^{-1}I \cap S^{-1}J$.

Lemma 2.5.2. *Sia I un iperideale di un iperanello R, allora $S \cap I \neq \emptyset$ se e solo se $S^{-1}I = S^{-1}R$.*

Proposizione 2.5.3. *Sia R un iperanello e S un sottoinsieme moltiplicativo di R.*

1. *Per un iperideale I di R, il seguente insieme:*

$$S^{-1}I := \{\frac{i}{s} : \ i \in I, s \in S\}$$

   è un iperideale di $S^{-1}R$.

2. *Se $\mathfrak{p}$ è un iperideale primo di R tale che $S \cap \mathfrak{p} = \emptyset$, allora $S^{-1}\mathfrak{p}$ è un iperideale primo di $S^{-1}R$.*

3. *Se $S = R \setminus \mathfrak{p}$ per qualche iperideale primo $\mathfrak{p}$ di R, allora $S = R \setminus \mathfrak{p}$ è un sottoinsieme moltiplicativo di R e $S^{-1}R$ ha un unico iperideale massimale dato da $S^{-1}\mathfrak{p}$.*

   L'iperanello delle frazioni $S^{-1}R$ è chiamato ***localizzazione*** *di R in $\mathfrak{p}$ e si denota con $R_\mathfrak{p}$. Se I è un iperideale di R, allora l'iperideale $S^{-1}I$ in $R_\mathfrak{p}$ si denota con $I_\mathfrak{p}$.*

Teorema 2.5.1. *Sia I un iperideale primo in un iperanello R.*

1. *C'è una corrispondenza biunivoca tra l'insieme degli iperideali primi di R che sono contenuti in I e l'insieme degli iperideali primi di $R_\mathfrak{p}$ data da $Q \mapsto Q_\mathfrak{p}$;*

2. *L'iperideale $I_\mathfrak{p}$ in $R_\mathfrak{p}$ è l'unico iperideale massimale di $R_\mathfrak{p}$.*

2.6 Spettro primo di un iperanello

Definizione 2.6.1. Sia R un iperanello. Si denota con *Spec* R, lo **spettro primo di un iperanello**, ossia l'insieme degli iperideali primi di R.
Si può dotare *Spec* R di una topologia, come nel caso classico. Avremo che

$$\text{un sottoinsieme } A \subseteq Spec\ R \text{ è chiuso } \iff A = V(I) \text{ per qualche iperideale } I \text{ di } R$$

dove $V(I) = \{J \in Spec\ R | I \subseteq J\}$. Infatti $\mathscr{C} := \{V(I),\ I \text{ iperideale di } J\}$ soddisfa tutti gli assiomi per essere la famiglia di insiemi chiusi per una topologia, detta *topologia di Zariski* su *Spec* R. Infine, $\mathscr{A} := \{A(I) : I \text{ iperideale di } R\}$ con $A(I) = Spec\ R \setminus V(I)$ è la famiglia degli insiemi aperti nello spazio topologico $(Spec\ R, \mathscr{C})$.

Mostriamo le due proprietà relative all'unione e all'intersezione dei chiusi.

Proposizione 2.6.1. *Sia R un iperanello e poniamo $X = Spec\ R$.*

1. *Sia $\{I_\lambda\}_{\lambda\in\Lambda}$ una famiglia di iperideali di R. Allora si avrà:*

$$\bigcap_{\lambda\in\Lambda} V(I_\lambda) = V(<\bigcup_{\lambda\in\Lambda} I_\lambda>)$$

   dove $<\bigcup_{\lambda\in\Lambda} I_\lambda>$ è il più piccolo iperideale contenente $\bigcup_{\lambda\in\Lambda} I_\lambda$.

2. *Siano I e I' iperideali di R, allora:*

$$V(I) \cup V(I') = V(I \cap I').$$

Dimostrazione. 1) $J \in \bigcap_{\lambda\in\Lambda} V(I_\lambda) \iff \forall\lambda \in \Lambda :\ J \in V(I_\lambda) \iff \forall\lambda \in \Lambda :\ I_\lambda \subseteq J \iff \bigcup_{\lambda\in\Lambda} I_\lambda \subseteq J \iff <\bigcup_{\lambda\in\Lambda} I_\lambda> \subseteq J \iff J \in V(<\bigcup_{\lambda\in\Lambda} I_\lambda>)$. Quindi $\bigcap_{\lambda\in\Lambda} V(I_\lambda) \in \mathscr{C}$.

2) Sia $J \in V(I) \cup V(I') \implies J \in V(I)$ o $J \in V(I') \implies I \subseteq J$ o $I' \subseteq J \implies I \cap I' \subseteq J \implies J \in V(I \cap I')$.

Viceversa, se $J \in V(I \cap I')$ allora $I \cap I' \subseteq J$. Sia $I \nsubseteq J$, $y \in I'$ e $x \in I \setminus J$. Allora $xy \in I \cap I'$ che implica $xy \in J$ con $x \notin J$. Essendo J iperideale primo di R, si ottiene $y \in J$. Dal fatto che y è un generico elemento di I' deduco $I' \subseteq J$, ossia $J \in V(I')$. $\square$

Osservazione 2.6.1. Si ha $V(R) = \emptyset$ in quanto gli elementi di *Spec* R sono tutti contenuti propriamente in R. D'altra parte, ogni iperideale primo di R contiene l'iperideale nullo, e dunque $V(\{0\}) =$ *Spec* R.

Esempio 2.6.1. Dato un anello A, lo spettro di un anello A, *Spec* A, coincide con lo spettro dell'iperanello associato all'anello A.

Proposizione 2.6.2. $\forall x \in R$ *si consideri l'insieme*

$$B(x) = A(<x>) = \{J \in Spec\ R : <x> \nsubseteq J\} = \{J \in Spec\ R :\ x \notin J\}.$$

La famiglia $\mathscr{B} = \{B(x) : x \in R\}$ *è una base per la topologia di Zariski di Spec B.*

Dimostrazione. Ogni $B(x) \in \mathscr{B}$ è aperto per costruzione. Inoltre $\forall A(I) \in \mathscr{A}$ e $\forall J \in A(I)$, $\exists B(x) \in \mathscr{B}$ t.c. $J \in B(x)$ e $B(x) \subseteq A(I)$. Infatti $J \in A(I) \implies I \nsubseteq J \implies \exists x \in I, x \notin J \implies J \in B(x)$. Inoltre $B(x) \subseteq A(I)$, infatti se $L \in B(x)$ allora $x \notin L$ da cui $I \nsubseteq L$ e dunque segue che $L \in A(I)$. $\square$

Osservazione 2.6.2. Se R e R' sono due iperanelli commutativi e $f : R \to R'$ è un omomorfismo di iperanelli, si ha che $f^{-1}(J') \in Spec\ R \quad \forall J' \in Spec\ R'$.

Proposizione 2.6.3. *Le mappe* $R \to Spec\ R$, $\quad f \to Spec\ f$ *dove* $Spec\ f(J') = f^{-1}(J')$ $\forall J' \in Spec\ R'$, *definiscono un* funtore controvariante *dalla categoria degli iperanelli, alla categoria degli spazi topologici.*

Dimostrazione. Si deve verificare che $Spec\ f$ è una mappa continua rispetto alla topologia di Zariski. Per ogni chiuso $V(I) \in \mathscr{C}$ si ha:

$$\begin{aligned}(Spec\ f)^{-1}(V(I)) &= \{J' \in Spec\ R' \ :\ f^{-1}(J') \in V(I)\}\\ &= \{J' \in Spec\ R' \ :\ f^{-1}(J') \supseteq I\}\\ &= \{J' \in Spec\ R' \ :\ f(I) \subseteq J'\}\\ &= V(f(I))\end{aligned}$$

allora $Spec\ f^{-1}(V(I))$ è un insieme chiuso in $Spec\ R'$. □

Diamo ora una importante caratterizzazione dello spettro di un iperanello come descritto in un articolo di A. Connes e P.Consani.

Teorema 2.6.1. *Sia R un iperanello e $\mathbf{K}$ l'ipercampo di Krasner $\{0,1\}$ dell'*esempio 3.2.1. *Allora la mappa:*

$$\varphi : Spec\ R \ \to \ Hom(R, \mathbf{K}), \quad \mathfrak{p} \mapsto \varphi_{\mathfrak{p}}$$

definita da:

$$\begin{aligned}\varphi_{\mathfrak{p}}(x) &= 0 \qquad \forall x \in \mathfrak{p}\\ \varphi_{\mathfrak{p}}(x) &= 1 \qquad \forall x \notin \mathfrak{p}\end{aligned}$$

determina una naturale biezione di insiemi.

Dimostrazione. L'applicazione $\varphi_{\mathfrak{p}} : R \to \mathbf{K}$ è moltiplicativa dato che il complementare di un qualsiasi ideale primo $\mathfrak{p}$ in R è un insieme moltiplicativo. Inoltre $\varphi_{\mathfrak{p}}$ è compatibile con l'iperaddizione. Dato che l'ipersomma di iperideali è ancora contenuta in un iperideale, l'opposto di un iperideale è a sua volta un ideale e grazie alla condizione di reversibilità data dalla definizione di ipergruppo, la mappa φ è ben definita. Per definire l'inversa di φ, assegniamo all'omomorfismo di iperanelli $\rho \in Hom(R, \mathbf{K})$ il suo nucleo, che è un ideale primo di R. Pertanto $Ker\rho$ determina univocamente ρ. □

Descriviamo ora gli elementi dell'insieme $Hom(R, \mathbf{S})$, dove $\mathbf{S}$ è l'ipercampo dei segni descritto nell' *Esempio 2.2.2.* Iniziamo richiamando le definizioni di *ordine totale*, di *cono positivo* e, *cono simmetrico* in R.

Definizione 2.6.2. Un **ordine totale**, $\leqslant$, è una relazione binaria su un insieme Y che gode di quattro proprietà, dati $x, y, z \in Y$:

1. è `riflessiva`, $x \leqslant x$;
2. è `antisimmetrica`, se $x \leqslant y$ e $y \leqslant x$ allora $x = y$
3. è `transitiva`, se $x \leqslant y$ e $y \leqslant z$ allora $x \leqslant z$
4. è `totale`, se $x \leqslant y$ e $y \leqslant x$.

Un insieme dotato di un ordine totale si dice **insieme totalmente ordinato**.

Osservazione 2.6.3. Le condizioni 1)-3) definiscono un *ordine parziale* e se in aggiunta a 1)-3) è verificata anche 4) allora l'ordine è *totale.*
La relazione $\leqslant$ è un ordine totale sugli insiemi $\mathbb{N}, \mathbb{Z}$ o $\mathbb{Q}$.

Definizione 2.6.3. Un **cono positivo** su un anello A è un sottoinsieme P di A tale che:

1. $P + P \subseteq P$;
2. $PP \subseteq P$;
3. $0 \notin P$.

Un **cono totale positivo** su A è un cono P su A tale per cui valgano le condizioni 1)-3) e inoltre

4. $P \cup \{0\} \cup -P = A$.

Definizione 2.6.4. Sia A un anello. Un **cono simmetrico** P in A è un sottoinsieme $P \subset A$ tale che:

1. $0 \notin P, \quad P + P \subset P, \quad PP \subset P, \quad$ (ossia è un cono positivo);

2. $P^c + P^c \subset P^c \quad$ dove P^c è il complementare di P in A;

3. $a \in P \quad \text{e} \quad ab \in P \implies b \in P$;

4. $P - P = A$.

Osservazione 2.6.4. Si può notare che ogni cono simmetrico è positivo e ogni cono totale è simmetrico.

Esempio 2.6.2. Se $R = \mathbb{R}$ allora $P = \mathbb{R}_{>0}$ è un cono simmetrico ed è pure totale. Inoltre se $R = \mathbb{Z}$ (oppure $R = \mathbb{Q}$) , allora $P = \mathbb{Z}_{>0}$ (rispettivamente $R = \mathbb{Q}_{>0}$) è un cono simmetrico ed è anche totale.

Esempio 2.6.3. Sia $\mathbb{C}$ il campo dei numeri complessi e sia P il cono positivo su $\mathbb{C}$ che consiste di tutti i numeri reali che sono positivi con l'ordine usuale sul campo dei numeri reali $\mathbb{R}$. Allora P non è un cono simmetrico poiché, per esempio, $1 + i \notin P$ e $1 - i \notin P$ ma $(1 + i) + (1 - i) \in P$. Dunque contraddice la condizione 2.

Esempio 2.6.4. Si consideri $R = \mathbb{R}[x]$. Allora un cono simmetrico è dato da $P = \{\text{polinomi del tipo } a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \text{ con } a_n > 0\}$ che è pure totale.

Esempio 2.6.5. Consideriamo ora un esempio di cono simmetrico ma non totale.
In $\mathbb{R}[x]$, prendiamo $P = \{\text{polinomi con termine noto positivo}\} = \{\text{polinomi del tipo } a_n x^n + a_{n-1}x^{n-1} + \ldots a_0 \quad \text{con } a_0 > 0\}$. Restano verificate:

- $P + P \subseteq P$;

- $P \cdot P \subseteq P$;
- $0 \notin P$.

Sia inoltre

$$P^c = \{\text{polinomi con termine noto} \leqslant 0\} = \{a_n x^n + a_{n-1}x^{n-1} + \ldots a_0 \quad \text{con } a_0 \leqslant 0\},$$

$$-P = \{\text{polinomi con termine noto} < 0\} = \{a_n x^n + a_{n-1}x^{n-1} + \ldots a_0 \quad \text{con } a_0 < 0\}.$$

È verificata inoltre

- $P - P = \mathbb{R}[x]$

ma $P \cup -P \cup \{0\} \subsetneqq \mathbb{R}[x]$ infatti mancano nell'unione ad esempio $x, x^2, x^3, \ldots$

Ora enunciamo un risultato riguardante i coni totali che sarà utile per dimostrare la proposizione successiva.

Teorema 2.6.2. *Sia R un anello. Se Q è un ideale primo in R e T è un cono totale su R/Q, allora $S = \{r \in R \mid r + Q \in T\}$ è un cono simmetrico su R. Viceversa, se S' è un cono simmetrico su R e $Q' = \{r \in R, r \notin S',\ -r \notin S'\}$, allora Q' è un ideale primo in R e l'immagine di S' in R/Q' è un cono totale su A/Q'.*

Per la dimostrazione si veda ([14])

La proposizione che segue mostra che la nozione di *cono simmetrico* in un anello è equivalente a quella di un elemento di $Hom(R, \mathbf{S})$. Se R è un anello ed S è un iperanello, si sta indicando con R pure l'iperanello associato ad R e Hom è da intendersi nella categoria degli iperanelli.

Proposizione 2.6.4. *1. Un omomorfismo di un anello R nell'iperanello $\mathbf{S}$ è determinato dal suo nucleo $\mathfrak{p} \in Spec\ R$ e da un ordine totale nel campo delle frazioni dal dominio d'integrità $R/\mathfrak{p}$.*

2. *Un omomorfismo da un anello R nell'iperanello $\mathbf{S}$ è determinato da un cono simmetrico di R.*

Dimostrazione. Sia $\rho \in Hom(R, \mathbf{S})$. Consideriamo la mappa del valore assoluto $\pi : \mathbf{S} \to \mathbf{K}, \quad \pi(x) = |x|$. π è un omomorfismo di anelli, pertanto anche $\pi \circ \rho$ è un omomorfismo di anelli. Quindi il nucleo di ρ, $Ker(\rho)$, è un ideale primo $\mathfrak{p} \subset R$ per quanto visto nella dimostrazione del *Teorema 2.6.1*. Inoltre la mappa ρ si fattorizza attraverso il quoziente $R/\mathfrak{p}$ che è un dominio d'integrità. Sia F il campo delle frazioni di $R/\mathfrak{p}$. Osserviamo che gli elementi di F sono frazioni $\frac{a}{b}$, con $a, b \in R/\mathfrak{p}$, e $\rho(b) \neq 0$ mentre $\rho(a) = 0$ se e solo se $a = 0$. Si ha $\rho(0) = 0$, $\rho(1) = 1$ e $\rho(-1) = -1$ dal momento che $0 \in \rho(1) + \rho(-1)$. Si prenda come $P \subset F$ l'insieme delle frazioni della forma $x = \frac{a}{b}$ con $\rho(a) = \rho(b) \neq 0$. Questo sottoinsieme di F è ben definito, infatti $\frac{a}{b} = \frac{c}{d}$ significa $ad = bc$ da cui segue che $\rho(c) = \rho(d) \neq 0$. Inoltre P è stabile rispetto all'addizione: presi $\frac{a}{b}$ e $\frac{c}{d}$ in P, se $c = 0$ o $a = 0$, è banale. Siano ora $\rho(a) \neq 0$ e $\rho(c) \neq 0$. Si noti che $\frac{a}{b} = \frac{-a}{-b}$ e dunque possiamo assumere $\rho(a) = \rho(b) = 1$ e analogamente per $\frac{c}{d}$. Ora $\frac{a}{b} + \frac{c}{d} = \frac{ad+cb}{bd}$ e si ha $\rho(d) = 1$, perciò $\rho(ad + bc) = \rho(cd) = \rho(c)$. In questo modo abbiamo provato $P + P \subseteq P$. Analogamente si mostra che $P \cdot P \subseteq P$. Inoltre dato $x \in F$ e $x \neq 0$, si prenda $x = \frac{a}{b}$ allora, o $x \in P$, ossia $\rho(a) = \rho(b) \neq 0$ oppure $\frac{-a}{b} = -\frac{a}{b} \in P$, ossia $-x \in P$. Quindi F è un campo ordinato, con ordine totale $\geqslant$ tale per cui il cono positivo dell'ordine sia $P = \{x \in F | \ x > 0\}$ e ρ è una composizione di un morfismo canonico $R \to F$ con la mappa $F \to F/F_+^\times \sim \mathbf{S}$. Viceversa, se viene dato un ordine al campo di frazioni del dominio di integrità $R/\mathfrak{p}$, si può utilizzare la naturale identificazione $F/F_+^\times \sim \mathbf{S}$ per ottenere il morfismo ρ.

2) segue da 1) e dal *Teorema 2.6.2* riguardante i coni totali. Infatti, dato un cono simmetrico $P \subset R$, le seguente formula definisce un elemento $\rho \in Hom(R, \mathbf{S})$:

$$\rho(x) = \begin{cases} 1, & \text{se } x \in P \\ -1, & \text{se } x \in -P \\ 0, & \text{altrimenti} \end{cases}$$

Inoltre, se $\rho \in Hom(R, \mathbf{S})$ allora $P = \rho^{-1}(1)$ è un cono simmetrico e si nota poi che $Ker\rho(x)$ è un ideale primo per quanto affermato nell' *Osservazione 3.3.1.* Dunque $\rho \in Hom(R, \mathbf{S})$ è determinato dal cono simmetrico P. $\square$

Dall' *Osservazione 2.3.1* sappiamo che se R è un anello, allora c'è una biiezione, in realtà un omeomorfismo, tra il suo spettro primo e l'iperspettro. Vediamo ora come quozientare per unità non alteri l'iperspettro.

Lemma 2.6.1. *Sia A un anello commutativo, $G \subseteq A^\times$ un sottogruppo moltiplicativo con $A^\times = \{a \in A | \ \exists b \in A$ tale che $ab = 1\}$ e sia A/G l'iperanello quoziente. Allora, $X = Spec\ A$ e $Y = Spec\ (A/G)$ sono omeomorfi dove entrambi sono dotati della topologia di Zariski.*

Dimostrazione. Se $G = \{1\}$ non c'è nulla da dimostrare.
Assumiamo $|G| \geqslant 2$ e definiamo l'applicazione

$$\begin{aligned} \sim: X &\rightarrow Y \\ \mathfrak{q} &\mapsto \widetilde{\mathfrak{q}} := \{\alpha G | \alpha \in \mathfrak{q}\} \end{aligned}$$

Questa applicazione è *ben definita*, infatti si ha

$$\begin{aligned} \alpha G = \beta G &\iff \alpha = \beta u \text{ con } u \in G \subseteq A^\times \\ &\iff \alpha, \beta \in \mathfrak{q} \text{ o } \alpha, \beta \notin \mathfrak{q}, \end{aligned}$$

perciò $\widetilde{\mathfrak{q}}$ è univocamente determinato da $\mathfrak{q}$. Inoltre $\widetilde{\mathfrak{q}}$ è un iperideale, infatti $0G \in \widetilde{\mathfrak{q}}$; se $aG \in \widetilde{\mathfrak{q}}$ allora $(-a)G = -(aG) \in \widetilde{\mathfrak{q}}$ e inoltre se per $rG \in A/G$ e $aG \in \widetilde{\mathfrak{q}}$, poiché

$(rG)(aG) = raG$ e $ra \in \mathfrak{q}$, si ha che $(rG)(aG) \in \widetilde{\mathfrak{q}}$. Supponiamo poi aG, $bG \in \widetilde{\mathfrak{q}}$. Osserviamo che $aG, bG \in \widetilde{\mathfrak{q}} \iff a, b \in \mathfrak{q}$ poiché $G \subseteq A^\times$ e $\mathfrak{q}$ è un ideale primo. Perciò se $zG \in aG + bG$, possiamo assumere che $z = at + bh$ per qualche $t, h \in G$ e $a, b \in \mathfrak{q}$, da cui segue che $z \in \mathfrak{q}$, quindi $zG \in \widetilde{\mathfrak{q}}$. Abbiamo quindi dimostrato che $\widetilde{\mathfrak{q}}$ è un *iperideale*.

Ora dimostriamo che è un iperideale *primo*. Supponiamo che $(aG)(bG) = (abG) \in \widetilde{\mathfrak{q}}$ e $aG \notin \widetilde{\mathfrak{q}}$. Questo implica che $ab \in \mathfrak{q}$ e $au \notin \mathfrak{q}$ per ogni $u \in G$, quindi $a \notin \mathfrak{q}$. Poiché $\mathfrak{q}$ è primo, questo implica che $b \in \mathfrak{q}$ e $bG \in \widetilde{\mathfrak{q}}$.

Ora mostriamo che l'applicazione $\sim$ è *continua*. Chiamiamo $\varphi := \sim$ per semplicità di notazione. Ci basta mostrare che $\varphi^{-1}(D(fG))$ è aperto, dove $D(fG)$ è aperto in Y per definizione della topologia di Zariski. Si ha che $\varphi^{-1}(D(fG)) = D(f)$. Infatti, se $\mathfrak{q} \in D(f)$, allora $\varphi(\mathfrak{q}) = \widetilde{\mathfrak{q}}$ non può contenere fG per definizione. Quindi, $D(f) \subseteq \varphi^{-1}(D(fG))$. Per l'inclusione consideriamo $\mathfrak{p} \in \varphi^{-1}(D(fG))$, ossia $\varphi(\mathfrak{p}) \in D(fG)$. Poiché $\varphi(\mathfrak{p}) = \widetilde{\mathfrak{p}} = \{\alpha G | \ \alpha \in \mathfrak{p}\}$ e $fG \notin \widetilde{\mathfrak{p}}$, segue che $f \notin \mathfrak{p}$ e dunque $\mathfrak{p} \in D(f)$. Quindi $\varphi^{-1}(D(fG)) \subseteq D(f)$.

Ora costruiamo l'*inversa* dell'applicazione $\varphi = \sim$. La proiezione canonica $\pi : A \to A/G$, che è un'applicazione tra insiemi, induce la seguente mappa:

$$\begin{aligned} \psi : Y &\to X \\ \mathfrak{p} &\mapsto \pi^{-1}(\mathfrak{p}). \end{aligned}$$

Osserviamo che ψ è continua poiché $\psi^{-1}(D(f)) = D(fG)$. Abbiamo affermato che φ e ψ sono una l'inversa dell'altra e poiché sono entrambe continue basta dimostrare che φ è biiettiva e che vale $\varphi \circ \psi = id_Y$.

Per prima cosa mostriamo che φ è *iniettiva*. Poniamo $\varphi(\mathfrak{q}) = \psi(\mathfrak{p})$ per $\mathfrak{q}, \mathfrak{p} \in X$. Per $x \in \mathfrak{q}$ si ha $y \in \mathfrak{p}$ tali che $xG = yG$ da cui segue che $x = yg$ per qualche $g \in G$, quindi

$x \in \mathfrak{p}$. Dato che vale la simmetria, si ha $\mathfrak{p} = \mathfrak{q}$.

Per mostrare la *suriettività* di φ, prendiamo un elemento $\wp \in Spec\,(A/G)$. Consideriamo αG come il sottoinsieme $\alpha G := \{\alpha g |\ g \in G\} \subseteq A$ e definiamo $\mathfrak{p} := \bigcup_{\alpha G \in \wp} \alpha G$. Ora dobbiamo dimostrare che $\mathfrak{p}$ è un ideale primo di A; innanzitutto $0 \in \mathfrak{p}$. Inoltre, $a \in \mathfrak{p} \iff a \in \alpha G$ per qualche $\alpha G \in \wp$, dunque, per $a \in \mathfrak{p}$ e $r \in A$, si ha $aG \in wp$ e $rG \in A/G$. Segue da $(rG)(aG) = (raG) \in \wp$ che $ra \in \mathfrak{p}$. Se $a, b \in \mathfrak{p}$, allora $aG, bG \in \wp$. Questo implica che $aG \boxplus bG \subseteq \wp$ e quindi $a + b \subseteq \mathfrak{p}$. Questo dimostra che $\mathfrak{p}$ è un ideale che non può essere A poiché implicherebbe $1 \in \mathfrak{p}$ e $1G \in wp$ ma $\wp \in A/G$. Osserviamo poi che $\mathfrak{p}$ è primo poiché per $ab \in \mathfrak{p}$ e $a \notin \mathfrak{p}$ si ha $(aG)(bG) \in \wp$ e $aG \notin \wp$. Questo implica che $bG \in \wp$, quindi $b \in \mathfrak{p}$. Ovviamente, si ha $\varphi(\mathfrak{p}) = \wp$. Questo mostra che φ è suriettiva infatti si ha $\mathfrak{p} = \psi(\wp)$. Perciò si ha $\varphi(\mathfrak{p}) = \varphi \circ \psi(\wp) = \wp$ e di conseguenza $\varphi \circ \psi = id_Y$.

□

2.7 Alcuni cenni storici

La teoria riguardante le iperstrutture ebbe inizio nel 1934 quando il matematico francese F. Marty, durante l'ottavo congresso dei matematici scandinavi tenutosi a Stoccolma, diede la prima nozione di *ipergruppo* (Cf.[16]) e ne illustrò alcune applicazioni per lo studio di gruppi non commutativi, funzioni algebriche e frazioni razionali. Intorno agli anni Quaranta del secolo scorso, furono studiati in Francia, in USA, in Russia, in Italia e in Giappone gli aspetti generici di questa teoria, i collegamenti con i gruppi classici e le applicazioni in geometria, da illustri matematici come M. Krasner, M. Kuntzmann, H. S. Wall, A. Vikhrov e Y. Utumi. La teoria progredì molto negli anni Settanta quando l'area di ricerca si allargò considerevolmente: in Francia M. Krasner, M. Koskas e Y. Sureau iniziarono a studiare i sottoipergruppi e

in particolare M. Krasner introdusse una specifica classe di iperanelli in [15], presentò quelli che ora sono detti *iperanelli di Krasner* insieme agli *iperanelli quoziente* e agli *ipercampi*. Dopo M. Krasner, D. Stratigopoulos si occupò nella tesi di dottorato, in seguito pubblicata in [22], degli *iperanelli artiniani*, e J. Mittas approfondì gli iperanelli di Krasner. Successivamente T. Vougiouklis e M. De Salvo studiarono gli *iperanelli generici* in [25] e infine R. Procesi e R. Rota introdussero la nozione di *iperanelli moltiplicativi* in [20] e in [19]. Gli iperanelli furono inoltre il punto di partenza per lo studio degli ipermoduli, analizzati da matematici come P. Corsini, C. G. Massouros e altri ancora. Sempre negli anni Settanta in Grecia, J. Mittas e i suoi studenti, oltre agli iperanelli di Krasner, approfondirono il concetto di ipergruppo canonico e iperreticolo in [18]; inoltre Ch. Massouros ottenne importanti risultati riguardo gli ipercampi e altre iperstutture ed alcune importanti applicazioni agli automi in [17].
Una figura che diede un contributo essenziale nello studio degli ipergruppi, in particolare ipergruppi regolari e ipergruppi completi, fu P. Corsini, matematico italiano, che insieme al suo gruppo di ricerca ottenne molteplici risultati anche riguardo agli omomorfismi di gruppi e alle applicazioni nel calcolo combinatorio e in geometria. Egli scrisse uno dei primi testi dedicati agli ipergruppi "*Prolegomena of hypergroup theory*"([6]) e fu seguito poi da T. Vougiouklis con "*Hyperstructures and their representations*"([26]).
In America le iperstrutture furono approfondite negli USA e in Canada specialmente da R. Roth che si servì degli ipergruppi canonici per risolvere alcuni problemi riguardanti la teoria dei gruppi finiti.
Le iperstrutture hanno molteplici applicazioni alla geometria, alle relazioni binarie, alla crittografia, all'intelligenza artificiale, alla probabilità e a molte altre. Tra le ultime applicazioni presentate vi è quella alla geometria tropicale che presentiamo nel

prossimo capitolo della tesi.

Capitolo 3

Applicazioni alla geometria tropicale

In questa sezione vogliamo mostrare un'applicazione della teoria degli iperanelli alla geometria tropicale; quest'ultima è una branca della geometria algebrica che si è molto sviluppata negli ultimi anni per le sue molteplici applicazioni. La geometria tropicale può essere pensata come una geometria algebrica costruita sul cosiddetto "semianello tropicale", ossia l'insieme $\mathbb{R} \cup \{\infty\}$ dotato di una moltiplicazione $\cdot$ ed una iperaddizione $\boxplus$. Molteplici lavori hanno mostrato come sia possibile introdurre i corrispettivi tropicali di molte costruzioni classiche e che queste godono di proprietà simili, per questo la geometria tropicale è talvolta utilizzata per risolvere problemi di geometria algebrica classica sul campo dei numeri complessi e reali. Tramite alcuni esempi, daremo un'idea della relazione tra varietà classiche e quelle tropicali tramite l'interpretazione della tropicalizzazione di varietà affini in termini di zeri di polinomi a coefficienti nell'ipercampo tropicale. Iniziamo introducendo la nozione di *valutazione p-adica* che sarà alla base del processo di tropicalizzazione.

3.1 Valutazione p-adica

Sia p un numero primo fissato.

Definizione 3.1.1. Si dice **valutazione p-adica** una funzione

$$v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$$

sul campo dei numeri razionali definita da

$$v\left(\frac{a}{b}\right) = r \quad \text{con } a, b \text{ numeri interi non nulli e } \frac{a}{b} = p^r \cdot \frac{a'}{b'} \quad \text{dove } a', b' \text{ sono coprimi con } p.$$

Si fissa $v_p(0) = \infty$. La valutazione p-adica soddisfa le seguenti:

1. $v_p(xy) = v_p(x) + v_p(y)$;
2. $v_p(x + y) \geqslant min\{v_p(x), v_p(y)\}$ e vale l'uguaglianza se $v_p(x) \neq v_p(y)$.

Osservazione 3.1.1. Data una valutazione p-adica v_p, grazie alle proprietà 1 e 2 di v_p si ha:

1. $v_p(1) = 0$;
2. $v_p(-1) = 0$;
3. $v_p\left(\frac{x}{y}\right) = v_p(x) - v_p(y)$;
4. $v_p(x + y) = v_p(x)$ se $v_p(x) > v_p(y)$. Infatti $v_p(x) = v_p(x + y - y) \geqslant min\{v_p(x + y), v_p(y)\}$. Poiché $v_p(x + y) \geqslant v_p(x)$ e $v_p(x) > v_p(y)$ per ipotesi, si ha che $min\{v_p(x + y), v_p(y)\} = v_p(x + y)$ e quindi $v_p(x + y) = v_p(x)$.

Definizione 3.1.2. Si dice **norma p-adica** $\|\cdot\|_p$ la norma definita da $\|x\|_p = p^{-v_p(x)}$, con $\|0\|_p = 0$. La norma p-adica soddisfa le seguenti proprietà:

1. $\|xy\|_p = \|x\|_p\|y\|_p$;
2. $\|x + y\|_p \leqslant max\{\|x\|_p, \|y\|_p\}$.

Osservazione 3.1.2. Segue dalla definizione di norma p-adica che

- ◇ $\|x\|_p \geqslant 0$ e vale 0 se e solo se $x = 0$;
- ◇ $\|-x\|_p = \|x\|_p$;
- ◇ $\|x+y\|_p \leqslant \|x\|_p + \|y\|_p$;
- ◇ $\|x\|_p \leqslant 1$ implica che $\|1+x\|_p \leqslant 1$.

Esempio 3.1.1. Sia $p = 3$,
$v_3(135) = 3$ poiché $135 = 3^3 \cdot 5^1$.
$\|135\|_3 = 3^{-3} = \frac{1}{3^3}$.

3.2 Esempi

Richiamiamo il concetto di *ipercampo tropicale* $\mathbb{T}$, definito nell'*Esempio 3.2.4*: l'**ipercampo tropicale** $\mathbb{T} = \mathbb{R} \cup \{\infty\}$ è definito come l'insieme dei numeri reali unito al simbolo di ∞.Esso è dotato di due operazioni: una moltiplicazione $\cdot$, che coincide con l'addizione tra due numeri reali, e inoltre vale $a \cdot \infty = \infty$ e un'iperaddizione $\boxplus$ definita da:

$$x \boxplus y = \begin{cases} \min\{x, y\} & \text{se } x \neq y \\ [x, +\infty] & \text{se } x = y. \end{cases}$$

In generale si ha:

- $0_{\mathbb{T}} = \infty$;
- $1_{\mathbb{T}} = 0_{\mathbb{R}}$;
- $-a = a$, se $a \in \mathbb{R}$.

Si può notare che in $\mathbb{T}$ il ruolo dell'elemento neutro per la $\boxplus$ è svolto da ∞, il ruolo dell'unità per la $\cdot$ è svolto da $0 \in \mathbb{R}$.
Per gli esempi che andremo a trattare ci serve anche estendere la *valutazione p-adica* $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$, definita nella sezione precedente alla chiusura algebrica di $\mathbb{Q}$, $\overline{\mathbb{Q}}$. Indicheremo sempre con v_p anche questa estensione $\overline{\mathbb{Q}} \to \mathbb{Q} \cup \{\infty\}$ e manterrà le proprietà elencate nella *Definizione 4.1.1.*
A titolo di esempio, se $x \in \overline{\mathbb{Q}}$ soddisfa $x^n = a$ con $a \in \mathbb{Q}$ allora $v_p(x) = \frac{1}{n} v_p(a)$.

A partire dagli zeri $(a, b) \in \overline{\mathbb{Q}}^2$ di un polinomio $f \in \mathbb{Z}[x, y]$ considereremo

$$trop(a, b) = (v_p(a), v_p(b)) \in \mathbb{T}^2$$

e successivamente prenderemo

$$\mathscr{T} = \{trop(a, b) | \ (a, b) \in V_{\overline{\mathbb{Q}}}(f)\}$$

l'insieme delle coppie $(v_p(a), v_p(b))$ al variare di $(a, b) \in \overline{\mathbb{Q}}^2$ tra gli zeri del polinomio f.

Definizione 3.2.1. Si dirà **tropicalizzazione** la chiusura di $\mathscr{T}$ in $\mathbb{R}^2$.

Essa sarà l'unione di semirette di $\mathbb{R}^2$ e di segmenti contenenti infiniti punti di $\mathscr{T}$ e aventi estremi in $\mathscr{T}$. Sia poi $f = \sum_{i,j} a_{ij} x^i y^j \in \mathbb{Z}[x, y]$ un polinomio a coefficienti interi. Il polinomio f può essere visto come una funzione

$$\begin{aligned} f : \mathbb{T} \times \mathbb{T} &\to \mathcal{P}(\mathbb{T})^* \\ (a, b) &\mapsto \boxplus_{ij}(a_{ij} \cdot a^i \cdot b^j) \end{aligned}$$

dove $\cdot$ indica il prodotto in $\mathbb{T}$ e dunque la scrittura $\boxplus_{ij}(a_{ij} \cdot a^i \cdot b^j)$ sta ad indicare in realtà l'iperaddizione $\boxplus$ al variare di i e j di $(a_{ij} + ia + jb)$.

Trattandosi di iperaddizione, affermare che $(a,b) \in \mathbb{T} \times \mathbb{T}$ è uno *zero* di f significa che $0_{\mathbb{T}} \in f(a,b)$, ma $0_{\mathbb{T}} = \infty$, e quindi $\infty \in f(a,b)$. Affinché poi ∞ appartenga a $f(a,b)$, almeno due degli addendi $a_{ij} + ia + jb$ devono coincidere; in questo modo se si svolge l'ipersomma $\boxplus_{ij}(a_{ij} + ia + jb)$ si otterranno delle semirette.

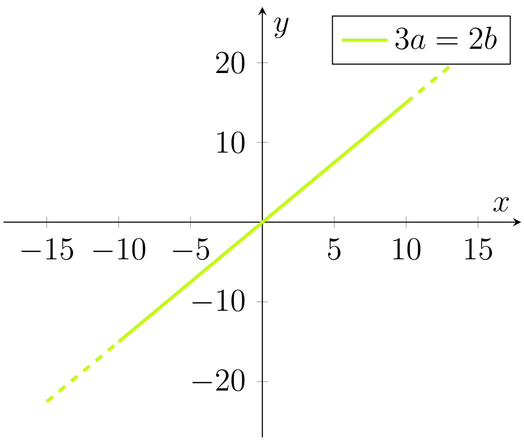
Negli esempi a seguire mostreremo che il luogo degli zeri di f in $\mathbb{T}$ imponendo $\infty = 0_{\mathbb{T}} \in f(a,b)$ con $(a,b) \in \mathbb{T} \times \mathbb{T}$ descrive figure che sono le stesse, a meno di traslazione, di quelle trovate tramite la valutazione p-adica degli zeri del polinomio $f \in \mathbb{Z}[x,y]$ in $\overline{\mathbb{Q}}^2$.

Esempio 3.2.1. Sia $f = x^3 - y^2$.

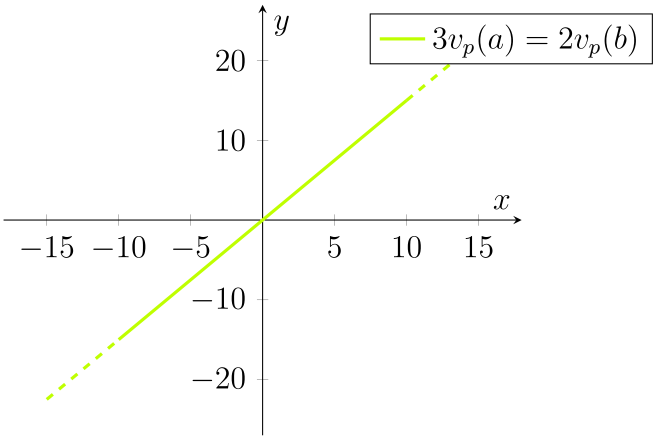
Allora f è la funzione

$$\begin{aligned} f : \mathbb{T} \times \mathbb{T} &\rightarrow \mathcal{P}(\mathbb{T})^* \\ (a,b) &\mapsto 3a \boxplus 2b. \end{aligned}$$

Affinché $(a,b) \in \mathbb{T}^2$ sia uno zero di f, si deve verificare $\infty \in 3a \boxplus 2b$ e questo accade se e solo se $3a = 2b$, ossia $b = \frac{3}{2}a$, quindi (a,b) appartengono alla retta disegnata in figura:



Analizzando la *controparte tropicale*, se $(a,b) \in \overline{\mathbb{Q}}^2$ è uno zero di $f : x^3 - y^2$, allora si ha $a^3 = b^2$ e applicando la valutazione p-adica, si ha $3v_p(a) = 2v_p(b)$. Se consideriamo $trop(a, b) = (v_p(a), v_p(b))$ troviamo lo stesso sottoinsieme del piano:



Esempio 3.2.2. Sia $f = x + y + 1$.

Possiamo vedere f come una funzione

$$\begin{aligned} f : \mathbb{T} \times \mathbb{T} &\rightarrow \mathcal{P}(\mathbb{T})^* \\ (a, b) &\mapsto a \boxplus b \boxplus 1. \end{aligned}$$

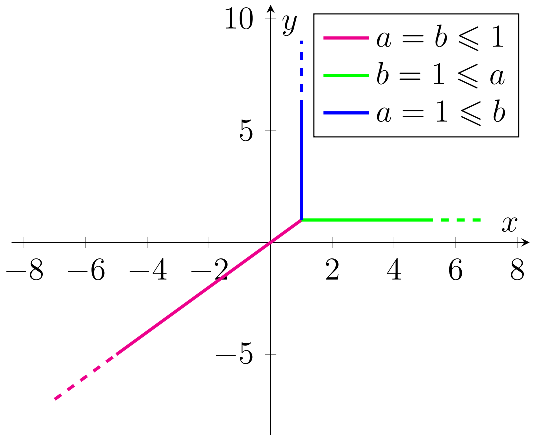
Affinché $(a, b) \in \mathbb{T}^2$ sia uno zero di f, si deve verificare $\infty \in a \boxplus b \boxplus 1$, ossia deve valere una delle seguenti condizioni:

(i) $a = b \leqslant 1$;

(ii) $b = 1 \leqslant a$;

(iii) $a = 1 \leqslant b$.

ossia:



Ora analizziamo la *controparte tropicale.*

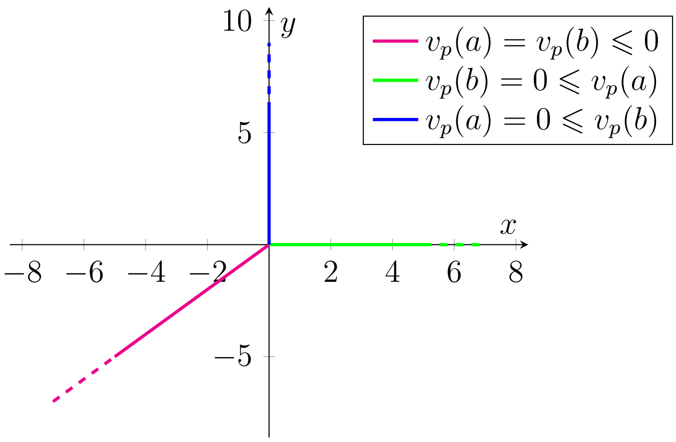
Se $(a, b) \in \overline{\mathbb{Q}}^2$ è uno zero di $f : x + y + 1 \in \mathbb{Z}[x, y]$, allora si ha $a + b + 1 = 0$. Consideriamo $trop(a, b) = (v_p(a), v_p(b))$, dove $v_p(a) = v_p(b + 1)$ e può assumere il valore $v_p(b)$ se questo è < 0, 0 se $v_p(b) > 0$ e valori arbitrari se $v_p(b) = v_p(1) = 0$. Quindi dobbiamo studiare $v_p(a), v_p(b)$ e $v_p(1) = 0$, quindi osserviamo che si possono presentare solo i seguenti casi:

(i) $v_p(a) = v_p(b) \leqslant v_p(1) = 0$;

(ii) $v_p(b) = v_p(1) = 0 \leqslant v_p(a)$;

(iii) $v_p(a) = v_p(1) = 0 \leqslant v_p(b)$.

La tropicalizzazione di f risulta quindi data da:



Si può osservare quindi che a meno di traslazioni, rappresentano lo stesso sottoinsieme del piano.

Per osservare figure più strutturate, inseriamo alcuni coefficienti a f. Si dovrà porre attenzione al valore di p nella valutazione p-adica delle soluzioni.

Esempio 3.2.3. Sia $f = 3x + 4y^2 + 1$.

Possiamo vedere f come una funzione

$$\begin{aligned} f : \mathbb{T} \times \mathbb{T} &\to \mathcal{P}(\mathbb{T})^* \\ (a, b) &\mapsto 3 + a \boxplus 4 + 2b \boxplus 1. \end{aligned}$$

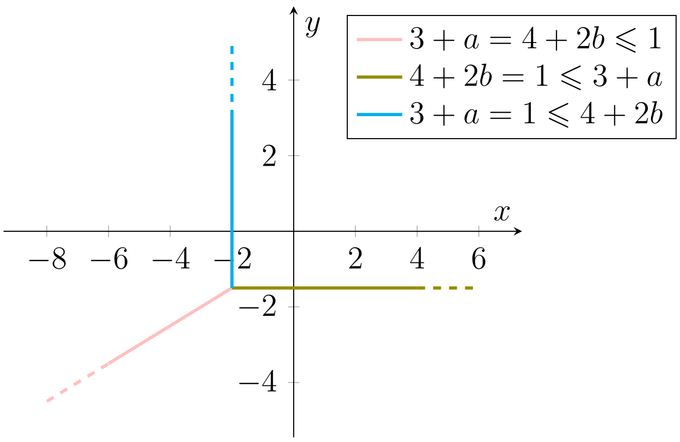
Affinché $(a, b) \in \mathbb{T}^2$ sia uno zero di f, si deve verificare $\infty \in 3 + a \boxplus 4 + 2b \boxplus 1$, ossia deve valere una delle seguenti condizioni:

(i) $3 + a = 4 + 2b \leqslant 1$;

(ii) $4 + 2b = 1 \leqslant 3 + a$;

(iii) $3 + a = 1 \leqslant 4 + 2b$.

ossia:



Ora analizziamo la controparte tropicale nel caso in cui $p \neq 2, 3$.

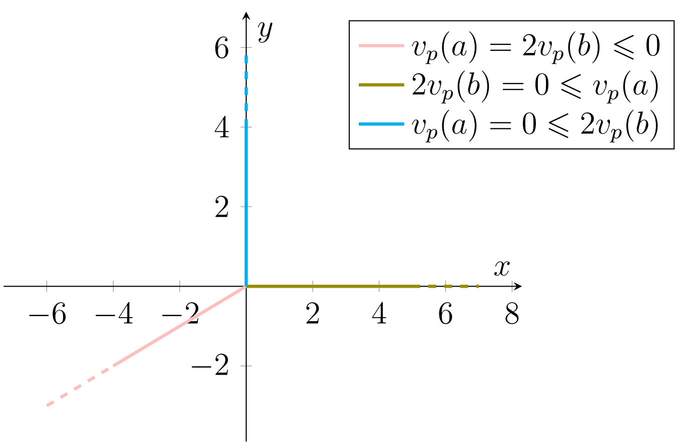
Se $(a, b) \in \overline{\mathbb{Q}}^2$ è uno zero di $f : 3x + 4y^2 + 1 \in \mathbb{Z}[x, y]$, allora si ha $3a + 4b^2 + 1 = 0$. Consideriamo $trop(a, b) = (v_p(a), v_p(b))$, con $p \neq 2, 3$ e quindi dobbiamo studiare $v_p(3) + v_p(a), v_p(4) + 2v_p(b)$ e $v_p(1)$, ma $v_p(3)$, $v_p(4)$ e $v_p(1)$ sono tutti nulli, e quindi analizziamo:

(i) $v_p(a) = 2v_p(b) \leqslant v_p(1) = 0$;

(ii) $2v_p(b) = v_p(1) = 0 \leqslant v_p(a)$;

(iii) $v_p(a) = v_p(1) = 0 \leqslant 2v_p(b)$.

La tropicalizzazione di f risulta quindi data da:



Si può osservare quindi che a meno di traslazioni, rappresentano lo stesso sottoinsieme del piano.

Se invece consideriamo:

- $\mathbf{p = 2}$.

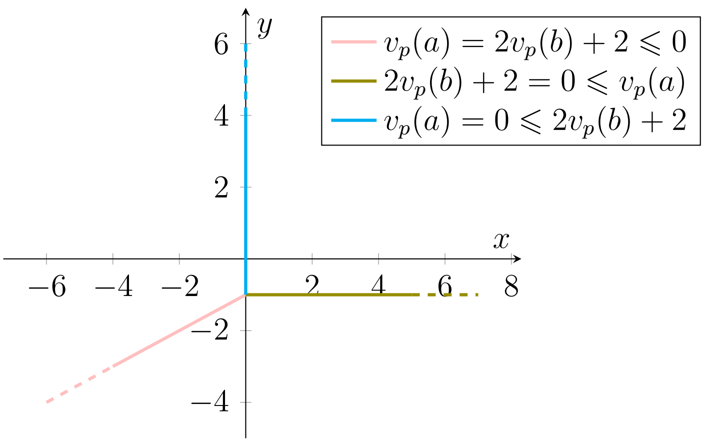
  Dobbiamo studiare $v_p(3) + v_p(a), v_p(4) + 2v_p(b)$ e $v_p(1)$, ma $v_p(4) = 2$ mentre $v_p(3)$ e $v_p(1)$ sono nulli, e quindi dovremmo analizzare:

  (i) $v_p(a) = 2v_p(b) + 2 \leqslant v_p(1) = 0$;

  (ii) $2v_p(b) + 2 = v_p(1) = 0 \leqslant v_p(a)$;

  (iii) $v_p(a) = v_p(1) = 0 \leqslant 2v_p(b) + 2$.

  ossia il sottoinsieme del piano è il seguente:



  Si nota quindi che l'origine delle semirette si è spostata dal punto $(0, 0)$ al punto $(0, -1)$.

- $\mathbf{p = 3}$.

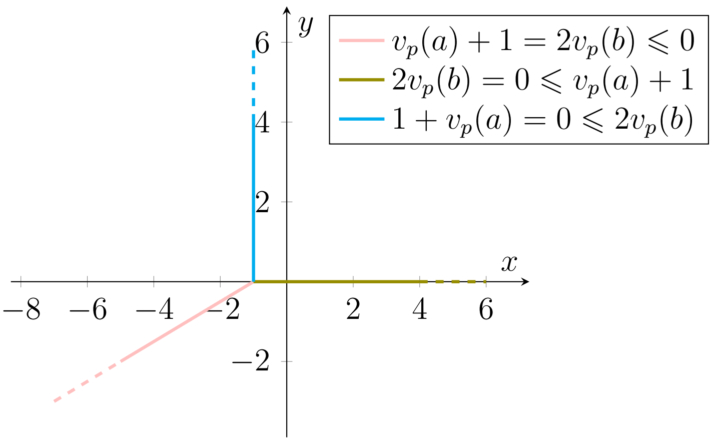
  Dobbiamo sempre studiare $v_p(3) + v_p(a), v_p(4) + 2v_p(b)$ e $v_p(1)$, ma $v_p(3) = 1$ mentre $v_p(4)$ e $v_p(1)$ sono nulli, e quindi dovremmo analizzare:

(i) $v_p(a) + 1 = 2v_p(b) \leqslant v_p(1) = 0$;

(ii) $2v_p(b) = v_p(1) = 0 \leqslant v_p(a) + 1$;

(iii) $1 + v_p(a) = v_p(1) = 0 \leqslant 2v_p(b)$.

ossia il sottoinsieme del piano è il seguente:



Si nota che l'origine delle semirette si è spostata al punto $(-1, 0)$.

Esempio 3.2.4. Sia $f = x - 2y^2 - 3xy$.

Possiamo vedere f come una funzione

$$\begin{aligned} f : \mathbb{T} \times \mathbb{T} &\rightarrow \mathcal{P}(\mathbb{T})^* \\ (a, b) &\mapsto a \boxplus 2 + 2b \boxplus 3 + a + b. \end{aligned}$$

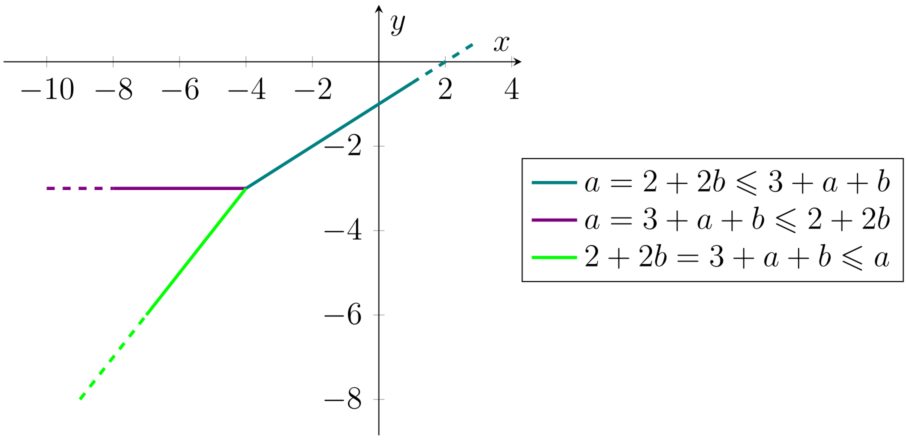
Affinché $(a, b) \in \mathbb{T}^2$ sia uno zero di f, si deve verificare $\infty \in a \boxplus 2 + 2b \boxplus 3 + a + b$ ossia devono valere le seguenti condizioni:

(i) $a = 2 + 2b \leqslant 3 + a + b$;

(ii) $a = 3 + a + b \leqslant 2 + 2b$;

(iii) $2 + 2b = 3 + a + b \leqslant a$.

ossia (a, b) appartengono al sottoinsieme disegnato in figura:



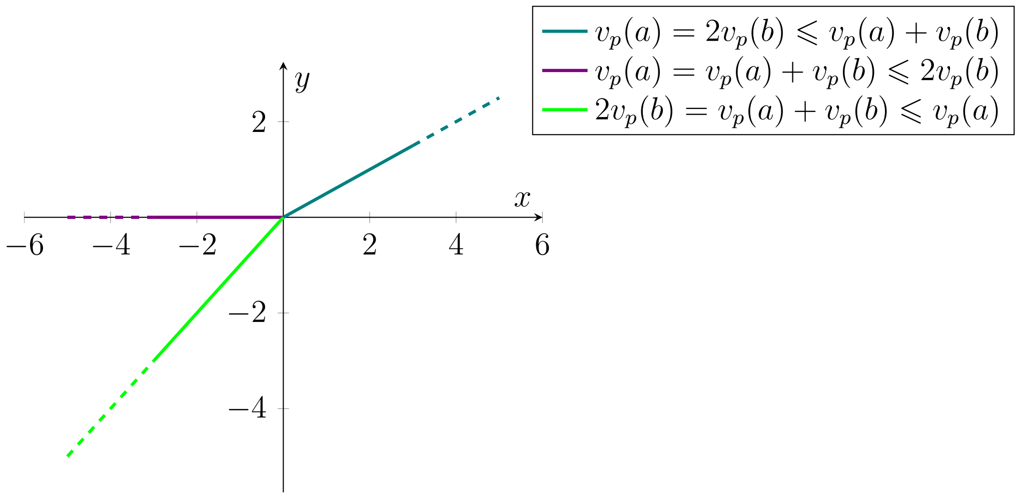
Analizzando la *controparte tropicale*, se $(a, b) \in \overline{\mathbb{Q}}^2$ è uno zero di $f : x - 2y^2 - 3xy \in \mathbb{Z}[x, y]$, allora si ha $a - 2b^2 - 3ab = 0$. Consideriamo $trop(a, b) = (v_p(a), v_p(b))$, e quindi dobbiamo studiare $v_p(a), v_p(2) + 2v_p(b)$ e $v_p(3) + v_p(a) + v_p(b)$, con $p \neq 2, 3$ quindi $v_p(2)$ e $v_p(3)$ sono entrambi nulli, e dunque analizziamo i casi:

(i) $v_p(a) = 2v_p(b) \leqslant v_p(a) + v_p(b)$;

(ii) $v_p(a) = v_p(a) + v_p(b) \leqslant 2v_p(b)$;

(iii) $2v_p(b) = v_p(a) + v_p(b) \leqslant v_p(a)$.

La tropicalizzazione di f risulta quindi data da:



Anche in questo caso l'origine delle semirette risulta traslata nel punto $(0, 0)$. Si nota infine che a meno di traslazioni, troviamo lo stesso sottoinsieme del piano. Se nella valutazione p-adica della parte tropicale consideriamo $p = 2$ o $p = 3$, troviamo ancora, a meno di traslazioni, lo stesso sottoinsieme del piano.

◇ Sia $\mathbf{p} = \mathbf{2}$.

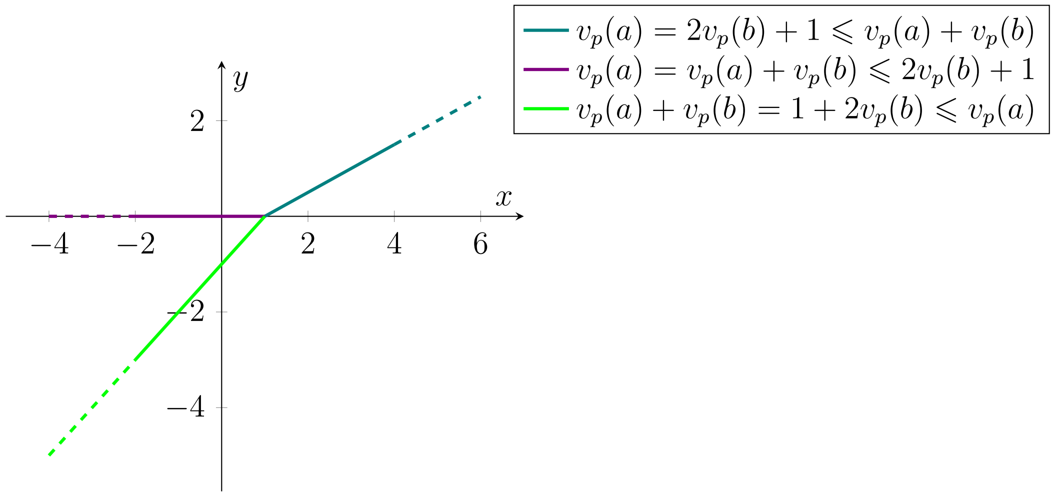
Dobbiamo studiare $v_p(a), v_p(2) + 2v_p(b)$ e $v_p(3) + v_p(a) + v_p(b)$, ma $v_p(2) = 1$ mentre $v_p(3)$ è nullo, e quindi dovremmo analizzare:

(i) $v_p(a) = 2v_p(b) + 1 \leqslant v_p(a) + v_p(b)$;

(ii) $v_p(a) = v_p(a) + v_p(b) \leqslant 2v_p(b) + 1$;

(iii) $v_p(a) + v_p(b) = 1 + 2v_p(b) \leqslant v_p(a)$.

ossia il sottoinsieme del piano è il seguente:



Si nota quindi che l'origine delle semirette si è spostata dal punto $(0, 0)$ al punto $(1, 0)$.

◇ Sia $\mathbf{p} = \mathbf{3}$.

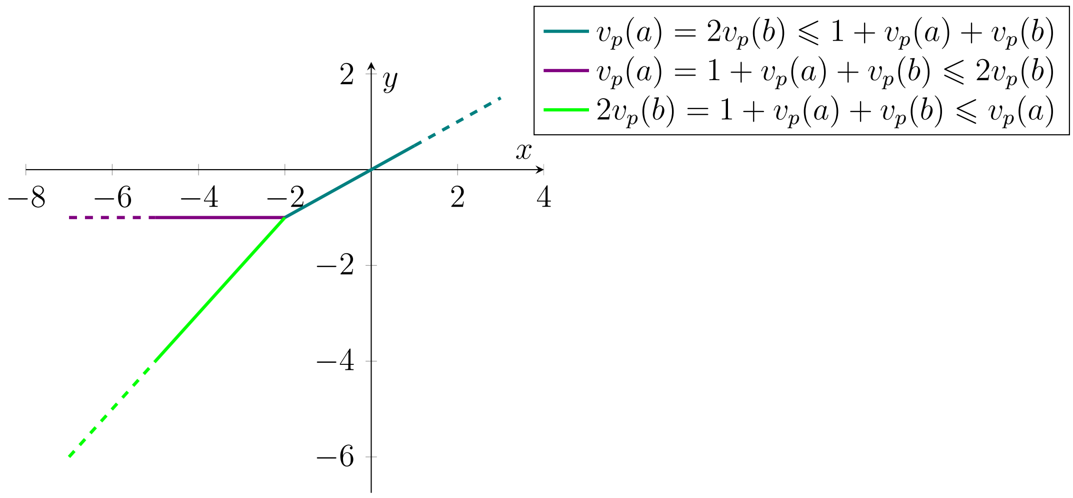
Dobbiamo sempre studiare $v_p(a)$, $v_p(2) + 2v_p(b)$ e $v_p(3) + v_p(a) + v_p(b)$, ma $v_p(3) = 1$ mentre $v_p(2)$ è nullo, e quindi dovremmo analizzare:

(i) $v_p(a) = 2v_p(b) \leqslant 1 + v_p(a) + v_p(b)$;

(ii) $v_p(a) = 1 + v_p(a) + v_p(b) \leqslant 2v_p(b)$;

(iii) $2v_p(b) = 1 + v_p(a) + v_p(b) \leqslant v_p(a)$.

ossia il sottoinsieme del piano è il seguente:



Possiamo dedurre che il sottoinsieme del piano è lo stesso a meno di traslazioni.

Con il seguente esempio mostriamo che la situazione in realtà è più complicata: non sempre è possibile notare che il sottoinsieme del piano resta lo stesso a meno di traslazioni. In alcuni casi si osserva che le pendenze delle semirette che descrivono la tropicalizzazione sono le stesse ma il sottoinsieme del piano non è lo stesso a meno di traslazioni.

Esempio 3.2.5. Sia $f = x^2 + xy + y + 2$.

Possiamo vedere f come una funzione

$$\begin{aligned} f : \mathbb{T} \times \mathbb{T} &\rightarrow \mathcal{P}(\mathbb{T})^* \\ (a, b) &\mapsto 2a \boxplus a + b \boxplus b \boxplus 2. \end{aligned}$$

Affinché $(a, b) \in \mathbb{T}^2$ sia uno zero di f, si deve verificare $\infty \in 2a \boxplus a + b \boxplus b \boxplus 2$, ossia deve valere una delle seguenti condizioni:

(i) $2a = a + b$ e $\begin{cases} a + b \leqslant b \\ a + b \leqslant 2 \end{cases}$

(ii) $2a = b$ e $\begin{cases} b \leqslant a + b \\ b \leqslant 2 \end{cases}$

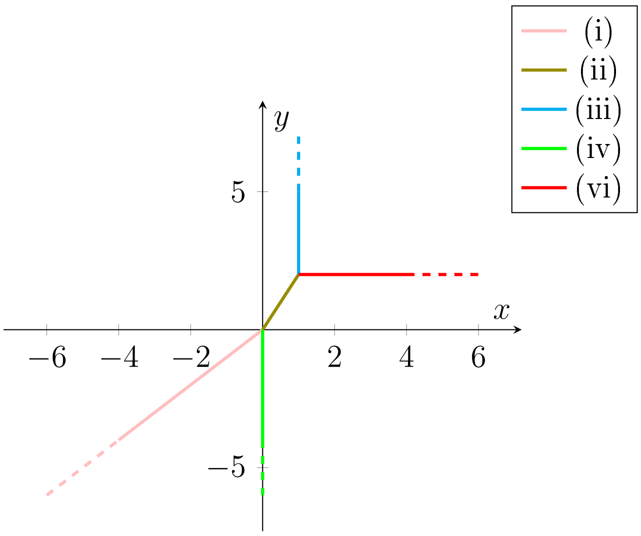
(iii) $2a = 2 \quad \text{e} \quad \begin{cases} 2 \leqslant a + b \\ 2 \leqslant b \end{cases}$

(iv) $a + b = b \quad \text{e} \quad \begin{cases} b \leqslant 2a \\ b \leqslant 2 \end{cases}$

(v) $a + b = 2 \quad \text{e} \quad \begin{cases} 2 \leqslant 2a \\ 2 \leqslant b \end{cases}$

(vi) $b = 2 \quad \text{e} \quad \begin{cases} 2 \leqslant 2a \\ 2 \leqslant a + b \end{cases}$

ossia:



Ora analizziamo la controparte tropicale nel caso in cui $p \neq 2$.

Se $(a, b) \in \overline{\mathbb{Q}}^2$ è uno zero di $f : x^2 + xy + y + 2 \in \mathbb{Z}[x, y]$, allora si ha $a^2 + ab + b + 2 = 0$. Consideriamo $trop(a, b) = (v_p(a), v_p(b))$, con $p \neq 2$ e quindi dobbiamo studiare $2v_p(a), v_p(a) + v_p(b), v_p(b)$ e $v_p(2)$, ma $v_p(2)$ è nullo, e quindi analizziamo:

(i) $2v_p(a) = v_p(a) + v_p(b) \quad \text{e} \quad \begin{cases} v_p(a) + v_p(b) \leqslant v_p(b) \\ v_p(a) + v_p(b) \leqslant 0 \end{cases}$

(ii) $2v_p(a) = v_p(b) \quad \text{e} \quad \begin{cases} v_p(b) \leqslant v_p(a) + v_p(b) \\ v_p(b) \leqslant 0 \end{cases}$

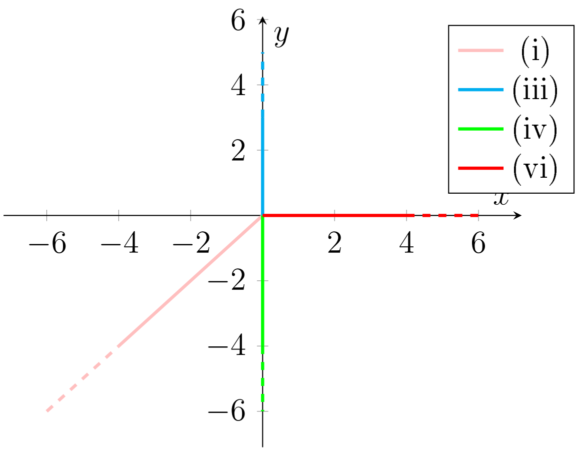
(iii) $2v_p(a) = 0 \quad \text{e} \quad \begin{cases} 0 \leqslant v_p(a) + v_p(b) \\ 0 \leqslant v_p(b) \end{cases}$

(iv) $v_p(a) + v_p(b) = v_p(b) \quad \text{e} \quad \begin{cases} v_p(b) \leqslant 2v_p(a) \\ v_p(b) \leqslant 0 \end{cases}$

(v) $v_p(a) + v_p(b) = 0 \quad \text{e} \quad \begin{cases} 0 \leqslant 2v_p(a) \\ 0 \leqslant v_p(b) \end{cases}$

(vi) $v_p(b) = 0 \quad \text{e} \quad \begin{cases} 0 \leqslant 2v_p(a) \\ 0 \leqslant v_p(a) + v_p(b) \end{cases}$

La tropicalizzazione di f risulta quindi data da:



Si può osservare quindi che le semirette mantengono le stesse pendenze e l'origine di tutte le semirette è ora nel punto $(0, 0)$.

Se invece consideriamo $\mathbf{p = 2}$.

Dobbiamo studiare $2v_p(a), v_p(a)+v_p(b), v_p(b)$ e $v_p(2)$, ma $v_p(2) = 1$, e quindi dovremo analizzare:

(i) $2v_p(a) = v_p(a) + v_p(b) \quad \text{e} \quad \begin{cases} v_p(a) + v_p(b) \leqslant v_p(b) \\ v_p(a) + v_p(b) \leqslant 1 \end{cases}$

(ii) $2v_p(a) = v_p(b) \quad \text{e} \quad \begin{cases} v_p(b) \leqslant v_p(a) + v_p(b) \\ v_p(b) \leqslant 1 \end{cases}$

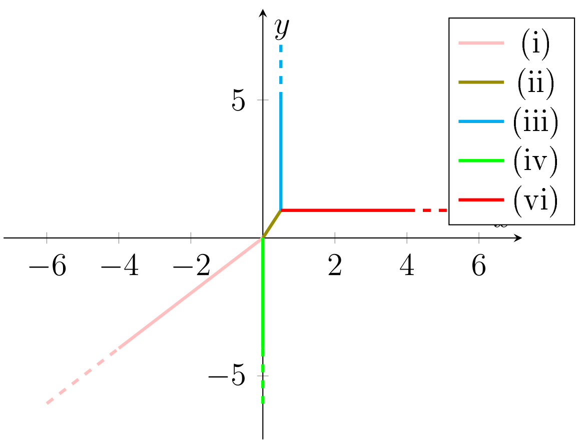
(iii) $2v_p(a) = 1$ e $\begin{cases} 1 \leqslant v_p(a) + v_p(b) \\ 1 \leqslant v_p(b) \end{cases}$

(iv) $v_p(a) + v_p(b) = v_p(b)$ e $\begin{cases} v_p(b) \leqslant 2v_p(a) \\ v_p(b) \leqslant 1 \end{cases}$

(v) $v_p(a) + v_p(b) = 1$ e $\begin{cases} 1 \leqslant 2v_p(a) \\ 1 \leqslant v_p(b) \end{cases}$

(vi) $v_p(b) = 1$ e $\begin{cases} 1 \leqslant 2v_p(a) \\ 1 \leqslant v_p(a) + v_p(b) \end{cases}$

ossia il sottoinsieme del piano è il seguente:



Osserviamo quindi che le pendenze di tutte le semirette restano inalterate, c'è una similitudine tra i sottoinsiemi del piano che però non sono gli stessi a meno di traslazioni. Si nota che l'origine delle semirette $y = 1$, $x = 1/2$ e $y = 2x$ nel tratto $x \in [0, 1/2]$, è traslata nel punto $(1/2, 1)$.

Bibliografia

[1] A. Asokkumar, M. Velrajan, *"A radical property of hyperrings"*, Italian journal of pure and applied mathematics, 2000.

[2] M.F. Atiyah, I.G. MacDonald, *"Introduzione all'algebra commutativa"*, Feltrinelli editore, Milano, 1981.

[3] G. Bachman, *"Introduction to p-Adic Numbers and Valuation Theory"*, Academic Press, New York, 1964.

[4] S. Bosch, *"Algebraic geometry and commutative algebra"*, Springer, 2012.

[5] A. Connes, C. Consani, *"The hyperring of adele classes"*, J. Number theory 131 (2), 2011, pp. 159-194.

[6] P. Corsini, *"Prolegomena of hypergroup theory"*, Second edition, Aviani editor, 1993.

[7] P. Corsini, V. Leoreanu, *"Applications of Hyperstructure Theory"*, vol 5, Springer, 2003.

[8] B. Davvaz, V. Leoreanu-Fotea, *" Hyperring Theory and Applications"*, Int. Acad. Press, USA, 2007.

[9] B. Davvaz, A. Salasi, *" A realization of Hyperrings"*, Communication in Algebra, 2007.

[10] J.R. Durbin, *"Modern Algebra, an Introduction"*, John Wiley & Jons, Inc, United States of America, 1981.

[11] U. Görtz ,T. Wedhorn, *"Algebraic Geometry I"* Vieweg+Teubner, 2010, pp.40,41.

[12] I. N. Hernstein, *"Algebra"*, Editori uniti, Roma, 1994.

[13] J. Jun, *"Algebraic geometry over hyperrings"*, Advances in Mathematics 323, 2018, pp. 142-192.

[14] C. Kohls, J. Reid, *"Orders on commutative rings"*, Duke Math.J. 33, 1966, pp. 657-666.

[15] M. Krasner, *"Approximation des corps valués complets de caractéristique* $p \neq 0$ *par ceux de caractéristique* 0*"*, Colloque d'Algébre Supérleure, Bruxelles, 1956.

[16] F. Marty, *"Sur une généralization de la notion de groupe"*, in 8^{th} Congress Math. Scandinaves, Stockholm, 1934, pp. 45-49.

[17] Ch. G. Massouros, *"On the theory of hyperrings and hyperfields"*, Algebra i Logika, 24, 1985, pp. 728-742.

[18] J.Mittas, *"Hypergroupes canoniques"*, Math. Balkanica, Beograd 2, 1972, pp. 165-172.

[19] R. Procesi, R. Rota, *"Le spectre premier d'un hyperanneau multiplicatif"*, Atti Conv. Ipergruppi, altre strutture moltiplicative e loro applicazioni, Udine, 1985.

[20] R. Rota, *"Sugli iperanelli moltiplicativi"*, Rend. Mat., Series VII(4), 2, 1982, pp.711-724.

[21] R. Procesi-Ciampi, R.Rota, *"The hyperring spectrum"*, Rivista di matematica pura e applicata, 1987.

[22] D. Stratigopoulos, *"Hyperanneaux non commutatifs: hyperanneaux artiniens, centralisateur dun hypermodule et théorème de densité"*, C.R. Acad. Sc. Paris, 269, Paris, 1969, pp.889-891.

[23] J.J. Rotman, *"An introduction to homological algebra"*, Springer, 2000.

[24] O. Viro, *"Hyperfields for tropical geometry I. Hyperfields and dequantization"*, preprint, arXiv:1006.3034, 2010.

[25] T. Vougiouklis, *"Representations of hypergroups. Hypergroup algebra"*, Atti Conv. Ipergruppi, altre strutture moltiplicative e loro applicazioni, Udine, 1985.

[26] T. Vougiouklis, *"Hyperstructures and their representations"*, Hadronic Press, Florida, 1994.