Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE

Corso di Laurea in Matematica

TEORIA DEI MODELLI E TEOREMA DI AX-KOCHEN

Tesi di Laurea in Logica Matematica

Relatore:
Chiar.mo Prof.
MARTINO LUPINI

Presentata da:
MATTEO GABRIELLONI

Anno Accademico 2025-2026

A chi si è chiesto se ci
fosse un altro modo,
un'altra strada

Introduzione

La matematica si configura come l'insieme di simboli e formule che forniscono il linguaggio per esplorare e comprendere la realtà. L'approccio del ricercatore a essa, tuttavia, non è sempre il medesimo; l'Algebra, la Geometria e l'Analisi, le tre colonne portanti di questa disciplina, si differenziano infatti per gli strumenti utilizzati nel descrivere e analizzare gli oggetti di studio. Accade spesso, d'altronde, che approcci differenti si incontrino nello studio dello stesso oggetto: un esempio perfetto è l'insieme dei numeri reali $\mathbb{R}$. Nell'Algebra, esso è visto come un campo ordinato completo rispetto alle operazioni di somma e prodotto; nella Geometria, i reali diventano le coordinate dello spazio euclideo $\mathbb{R}^n$; nell'Analisi, infine, $\mathbb{R}$ è concepito come il prototipo dello spazio metrico completo, in cui, intuitivamente, "non esistono buchi". In questo elaborato vedremo come il cambio di prospettiva sia talvolta fondamentale: passeremo dalla formulazione algebrica di un problema alla sua riscrittura e risoluzione tramite gli strumenti di un'altra branca della matematica: la Logica.

Questa tesi è rivolta ad appassionati di matematica che abbiano già familiarità con le nozioni elementari dell'algebra dei campi finiti e della logica del primo ordine. Nel corso del testo introdurremo strumenti più avanzati di entrambe le discipline, omettendo alcune dimostrazioni puramente tecniche con l'unico scopo di evidenziare le intuizioni che hanno permesso, dapprima, a Emil Artin di formulare la sua celebre congettura e, in seguito, a James Ax e Simon Kochen di dimostrarla parzialmente.

Emil Artin (1898 – 1962) è stato uno dei più influenti algebristi del ventesimo secolo. In questa tesi ricordiamo in particolare i suoi studi sui polinomi omogenei (o forme), come, ad esempio, il polinomio $p(x, y) = 3x^2 - 2xy + 7y^2$, e sulla ricerca delle loro soluzioni non banali. Se in ambito fisico e ingegneristico la determinazione degli zeri

di un polinomio è cruciale per ottimizzare processi o analizzare la stabilità dei sistemi, in ambito teorico Artin si interessò a determinare sotto quali condizioni una forma di grado d in più di d^2 variabili ammetta soluzioni non banali all'interno del campo dei numeri p-adici $\mathbb{Q}_p$. Artin era a conoscenza del fatto che il campo delle serie formali di Laurent a coefficienti in un campo finito, $\mathbb{F}_p((t))$, godeva di tale proprietà (proprietà C_2, dimostrata dal suo allievo Serge Lang). Poiché i numeri p-adici $\mathbb{Q}_p$ condividono profonde analogie strutturali con $\mathbb{F}_p((t))$, Artin congetturò che anche $\mathbb{Q}_p$ fosse un campo C_2. Se la congettura fosse stata universalmente vera, avrebbe garantito l'esistenza di uno zero p-adico non banale per ogni forma di grado d in $n > d^2$ variabili. Tuttavia, a causa di sottili divergenze algebriche tra i due campi, Artin non riuscì a fornirne una dimostrazione generale, sebbene per i gradi $d = 1, 2, 3$ la congettura si fosse rivelata corretta. Solo anni più tardi, il contributo di due logici risultò fondamentale per sbloccare la questione.

James Ax (1937 – 2006) e Simon Kochen (1934) sono i due matematici che, a metà degli anni Sessanta, hanno impresso una svolta decisiva al problema. Essi intuirono che le analogie profonde tra $\mathbb{Q}_p$ e $\mathbb{F}_p((t))$ non risiedevano tanto nelle loro proprietà strettamente algebriche, quanto nelle loro proprietà elementari dal punto di vista logico. Attraverso la Teoria dei Modelli, la branca della logica matematica che studia le relazioni tra le strutture algebriche e i linguaggi formali, Ax e Kochen dimostrarono che ogni enunciato elementare valido in $\mathbb{Q}_p$ "per quasi tutti i primi p" (espressione che assumerà un significato matematico rigoroso tramite l'uso degli ultrafiltri) è valido anche in $\mathbb{F}_p((t))$ "per quasi tutti i primi p". Questo risultato, noto come Principio di Ax-Kochen, ha permesso di risolvere parzialmente la congettura di Artin, dimostrando che essa è vera "quasi sempre" (ovvero per tutti i primi superiori a un certo indice critico dipendente dal grado). La congettura, considerata nella sua totalità, è infatti falsa: lo mostreremo esplicitamente nell'ultimo capitolo riportando il celebre controesempio trovato dal matematico francese Guy Terjanian nel 1966.

Il controesempio di Terjanian (1966) arrivò "subito dopo" la dimostrazione di Ax-Kochen (1965/1966). Fu uno shock perché dimostrò che la logica avesse ragione laddove l'intuizione algebrica globale falliva. Questo lavoro intende quindi mostrare come la Logica Matematica non sia semplicemente uno strumento di fondazione, bensì un potente mezzo d'indagine capace di risolvere problemi aperti dell'Algebra e della Teoria dei

Numeri laddove i metodi classici si rivelano insufficienti.

L'elaborato è organizzato come segue: la prima sezione fornisce il retroscena algebrico necessario a enunciare formalmente la congettura di Artin e la proprietà C_2, riservando uno spazio centrale alla teoria dei campi finiti e a quella dei campi valutati. Successivamente, dopo un breve richiamo alla logica proposizionale e del primo ordine, verranno introdotti i concetti cardine della teoria dei modelli necessari alla dimostrazione: i filtri, gli ultraprodotti, gli n-tipi e i modelli saturi. Infine, previo l'enunciato di un lemma aritmetico essenziale, la tesi si conclude con la trattazione del Principio di Ax-Kochen e l'analisi del controesempio di Terjanian.

Indice

Capitolo 1

Introduzione alla Teoria dei Campi

Questo primo capitolo introduce quasi tutti gli strumenti algebrici che utilizzeremo, necessari per enunciare la congettura di Artin. Essa riguarda infatti concetti come quello di polinomio omogeneo, proprietà C_i, campi con valutazione e il campo dei numeri p-adici $\mathbb{Q}_p$.

1.1 Proprietà C_i

È noto che, fissato un campo F, la possibilità di trovare zeri per un polinomio dipende dal numero di variabili n coinvolte e il grado d del polinomio stesso. Intuitivamente, maggiore è il numero di variabili rispetto al grado, più lo "spazio" in cui cercare è ampio, aumentando la probabilità che il polinomio ammetta soluzioni non banali. Per formalizzare questa intuizione e classificare i campi in base alla loro "complessità aritmetica" rispetto alla risolubilità dei polinomi, Emil Artin introdusse negli anni '30 la nozione di campo quasi-algebricamente chiuso, successivamente generalizzata nella proprietà di tipo C_i. Questa proprietà fornisce un criterio quantitativo preciso: un campo è detto C_i se il numero di variabili necessarie a garantire l'esistenza di uno zero non banale è legato al grado del polinomio tramite una relazione di tipo polinomiale. Partiamo col definire una specifica classe di equazioni:

Definizione 1.1. Un polinomio f su un campo F si dice omogeneo di grado $d \geq 1$ in n variabili $x_1, \ldots, x_n$ se tutti i monomi di f hanno grado d, cioè se può essere scritto nella

forma

$$f(x_1, \ldots, x_n) = \sum_i a_i x_1^{b_{i,1}} \cdots x_n^{b_{i,n}},$$

tale che per ogni i si ha

$$\sum_{j=1}^{n} b_{i,j} = d.$$

Osservazione 1.2. Se f è un polinomio omogeneo di grado d in n variabili su F, allora per ogni $c \in F$ si ha

$$f(cx_1, \ldots, cx_n) = c^d f(x_1, \ldots, x_n).$$

Poiché un polinomio omogeneo non può avere termine costante, tutti i polinomi omogenei ammettono lo zero banale $(0, \ldots, 0)$. È interessante studiare quando i polinomi omogenei ammettono zeri non banali.

Esempio 1.3. Sia f_n il polinomio $x_1^2 + x_2^2 + \cdots + x_n^2$. Per ogni $n > 0$, f_n è un polinomio omogeneo di grado 2 in n variabili. Su $\mathbb{R}$, f_n ha solo lo zero banale per ogni n. Ma su $\mathbb{C}$, f_n ha zeri non banali (ad esempio $(1, i, 0, \ldots, 0)$) per ogni $n > 1$. È facile verificare che su $\mathbb{F}_7$, f_n ha zeri non banali per ogni $n > 2$, e (nel Corollario 1) mostreremo che ciò vale per tutti i campi finiti. Il 2 deriva dal grado di f_n.

Definizione 1.4. Un campo F si dice C_i, per $i \in \mathbb{N}$, se ogni polinomio omogeneo su F di grado d in n variabili tale che $n > d^i$ ammette uno zero non banale in F^n.

Possiamo caratterizzare facilmente i campi C_0:

Teorema 1.5. Un campo è algebricamente chiuso se e solo se è C_0.

Dimostrazione. Sia F un campo.

Supponiamo che F sia algebricamente chiuso. Sia $f(x_1, \ldots, x_n)$ un polinomio omogeneo su F di grado d in $n > d^0 = 1$ variabili. Scriviamo f come polinomio in una variabile, x_1, con coefficienti in $F[x_2, \ldots, x_n]$: $f = \sum_{i=0}^{d'} f_i(x_2, \ldots, x_n)\, x_1^i$. Il grado d' è la massima potenza di x_1 che compare in f.

Se $d' = 0$, allora nessuna potenza non nulla di x_1 compare in f, quindi $f(1, 0, \ldots, 0) = f(0, \ldots, 0) = 0$, e $(1, 0, \ldots, 0)$ è uno zero non banale di f.

Se invece $d' > 0$, consideriamo il coefficiente principale $f_{d'}(x_2, \ldots, x_n)$. Vogliamo trovare $(\alpha_2, \ldots, \alpha_n) \in F^{n-1}$ non banale tale che $f_{d'}(\alpha_2, \ldots, \alpha_n) \neq 0$. Poiché ogni campo algebricamente chiuso è infinito e un polinomio non nullo non può avere infiniti zeri, esiste $(\alpha_2, \ldots, \alpha_n)$ con almeno una coordinata non nulla e tale che $f_{d'}(\alpha_2, \ldots, \alpha_n) \neq 0$.

Definiamo $f(x_1) := f(x_1, \alpha_2, \ldots, \alpha_n)$. Abbiamo semplicemente valutato i coefficienti f_i in $(\alpha_2, \ldots, \alpha_n)$, e il coefficiente principale resta non nullo, quindi f è un polinomio in una variabile di grado $d' > 0$. Poiché F è algebricamente chiuso, f ha una radice α_1. Allora $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ è uno zero di f, ed è non banale perché almeno una $\alpha_j \neq 0$.

Viceversa, supponiamo che F sia C_0. Sia $f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0$ un polinomio di grado $d \geq 1$ su F. Vogliamo mostrare che f ha una radice in F.

Consideriamo il polinomio omogeneo $\tilde{f}(x_1, x_2) = a_d x_1^d + a_{d-1}x_1^{d-1}x_2 + \cdots + a_1 x_1 x_2^{d-1} + a_0 x_2^d$. Allora $\tilde{f}$ è un polinomio omogeneo di grado d in 2 variabili, e $2 > d^0 = 1$, quindi $\tilde{f}$ ha uno zero non banale $(\alpha_1, \alpha_2) \in F^2$.

Osserviamo che $\alpha_2 \neq 0$: infatti, se $\alpha_2 = 0$, allora $\tilde{f}(\alpha_1, 0) = a_d \alpha_1^d = 0$, da cui $\alpha_1 = 0$, contro il fatto che lo zero sia non banale.

Poiché $\tilde{f}(\alpha_1, \alpha_2) = 0$, usando l'Osservazione 1.2 otteniamo $\tilde{f}(\alpha_1 \alpha_2^{-1}, 1) = (\alpha_2^{-1})^d \tilde{f}(\alpha_1, \alpha_2) = 0$. Ma sostituendo $x_2 = 1$ si ha $\tilde{f}(x_1, 1) = f(x_1)$, quindi $f(\alpha_1 \alpha_2^{-1}) = 0$.

Dunque f ha una radice in F. Ne segue che ogni polinomio non costante su F ha una radice, cioè F è algebricamente chiuso. □

1.2 Campi finiti

In questa sezione considereremo K un campo finito di caratteristica p con $|K| = q$. Ricordiamo che:

- p è un numero primo;
- $q = p^v$ per qualche $v > 0$;
- il gruppo moltiplicativo $K^* = K \setminus \{0\}$ è ciclico di ordine $q - 1$.

Lemma 1.6. Per $m > 0$,

$$\sum_{a \in K} a^m = \begin{cases} -1 & \text{se } (q-1) \mid m \\ 0 & \text{altrimenti} \end{cases}$$

Dimostrazione. Supponiamo che $(q-1) \mid m$. Allora per ogni $a \in K^*$, $a^m = 1$, quindi

$$\sum_{a \in K} a^m = 0^m + \sum_{a \in K^*} a^m = \sum_{a \in K^*} 1 = q - 1 = -1 \in K.$$

Altrimenti, se $(q-1) \nmid m$, esiste y generatore del gruppo ciclico K^*. Allora $y^m \neq 1$ e la moltiplicazione per y permuta gli elementi di K^*, dunque:

$$\sum_{a \in K} a^m = \sum_{a \in K^*} a^m = \sum_{a \in K^*} (ya)^m = y^m \sum_{a \in K^*} a^m = y^m \sum_{a \in k} a^m$$

e quindi $(y^m - 1) \sum_{a \in K} a^m = 0$. Poiché $y^m - 1 \neq 0$, deve essere $\sum_{a \in K} a^m = 0$. □

Il teorema seguente implica che i campi finiti sono C_1, ma è in realtà un risultato più forte riguardante il numero di zeri di qualsiasi polinomio (non necessariamente omogeneo) con un numero di variabili superiore al suo grado.

Teorema 1.7 (Chevalley-Warning)**.** Sia f un polinomio su K di grado d in n variabili, $x_1, \ldots, x_n$. Se $n > d$, allora il numero di zeri di f in K^n è divisibile per p.

Dimostrazione. Per $(\alpha_1, \ldots, \alpha_n) \in K^n$:

$$1 - f(\alpha_1, \ldots, \alpha_n)^{q-1} = \begin{cases} 1 & \text{se } f(\alpha_1, \ldots, \alpha_n) = 0 \\ 0 & \text{altrimenti} \end{cases}$$

Contare il numero di zeri mod p di f equivale quindi a sommare i valori di questa espressione su tutti gli $(\alpha_1, \ldots, \alpha_n) \in K^n$. f^{q-1} è un polinomio di grado $d(q-1) < n(q-1)$ per ipotesi e può essere scritto come combinazione lineare di monomi di grado minore di $n(q-1)$. Allora per ogni monomio della forma $x_1^{d_1} x_2^{d_2} \ldots x_n^{d_n}$ esiste i tale che $d_i < p - 1$. Si ha quindi (prendendo ad esempio $i = 1$):

$$\sum_{(x_1, \ldots, x_n) \in K^n} x_1^{d_1} x_2^{d_2} \ldots x_n^{d_n} = \sum_{x_1 \in K} x_1^{d_1} \sum_{(x_2, \ldots, x_n)} x_2^{d_2} \ldots x_n^{d_n}.$$

Ora, se $d_1 = 0$ il primo fattore è $q = 0 \mod p$ Se invece è $d_1 \neq 0$, il primo fattore è comunque uguale a 0 per il Lemma 1.6 perché d_1 non è divisibile per $p-1$ essendo inferiore. Così il numero di zeri di f in K^n è $0 \pmod p$. □

Corollario 1.8. I campi finiti sono C_1.

Dimostrazione. Sia f un polinomio omogeneo su K di grado d in $n > d$ variabili. Per il Teorema 1.7, il numero di zeri è divisibile per p. Poiché f ha almeno lo zero banale, deve avere almeno p zeri ,e in particolare almeno $p-1$ zeri non banali. □

I prossimi teoremi servono a far capire al lettore che le proprietà C_i relative ai campi si preservano nelle estensioni. Omettiamo le loro dimostrazioni, che si rifanno a definizioni di norma e forma normica, che vanno oltre l'obiettivo di questa tesi.

Teorema 1.9 (Lang-Nagata)**.** Sia F un campo C_i. Siano $f_1, \ldots, f_r$ polinomi omogenei su F di grado d in n variabili. Se $n > rd^i$, allora essi hanno uno zero comune non banale in F^n.

Teorema 1.10. Se F è un campo C_i, allora ogni estensione algebrica di F è C_i.

Teorema 1.11. Se F è un campo C_i ed E è un'estensione di F di grado di trascendenza finito j, allora E è C_{i+j}.

1.3 Valutazioni e strutture associate

L'obiettivo di questa sezione è dimostrare che il campo delle serie di Laurent formali su un campo finito è C_2. Inoltre svilupperemo la teoria dei campi a valutazione discreta e i loro completamenti, che ci permetteranno di definire i campi p-adici. Iniziamo con le definizioni di gruppo abeliano e di valutazione.

Definizione 1.12. Un gruppo abeliano linearmente ordinato è un gruppo abeliano G, con una relazione d'ordine $\leq$, tale che $\forall a, b, c \in G$:

1. $\leq$ è un ordine lineare su G, cioè:
   (a) $a \leq b$ oppure $b \leq a$,

(b) se $a \leq b$ e $b \leq a$, allora $a = b$,

(c) se $a \leq b$ e $b \leq c$, allora $a \leq c$,

2. se $a \leq b$, allora $a + c \leq b + c$.

Scriveremo talvolta $b \geq a$ invece di $a \leq b$, e $a < b$ per indicare $a \leq b$ e $a \neq b$.

Definizione 1.13. Sia G un gruppo abeliano linearmente ordinato, dove estendiamo l'ordine e l'operazione a $G \cup \{\infty\}$ ponendo $b \leq \infty$ e $b + \infty = \infty \ \forall b \in G$. Dato un campo F e una funzione $v : F \to G \cup \{\infty\}$ tale che per ogni $a, b \in F$ vale che:

1. $v(a) = \infty$ se e solo se $a = 0$,
2. $v(ab) = v(a) + v(b)$,
3. $v(a + b) \geq \min(v(a), v(b))$,

diciamo che F è un campo valutato e v è una valutazione su F.

Esempio 1.14. Dato un campo F e un gruppo abeliano linearmente ordinato G, possiamo definire la valutazione banale $v : F \to G \cup \{\infty\}$ che manda 0 in ∞ e tutti gli altri elementi in 0.

Nei prossimi due esempi introduciamo rispettivamente la valutazione p-adica v_p e la valutazione t-adica v_t, necessarie per definire i campi ai fini di questa trattazione.

Esempio 1.15. Per ogni primo p, definiamo $v_p : \mathbb{Z} \setminus \{0\} \to \mathbb{N}$ ponendo $v_p(a) = k$, dove k è il massimo intero tale che $p^k \mid a$. Estendiamo v_p a $\mathbb{Q}$ ponendo:

$$v_p(0) = \infty, \quad v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b).$$

Esempio 1.16. Per ogni campo F, possiamo definire una valutazione simile a quella dell'Esempio 1.15 sul campo delle funzioni razionali su F. Per definirla partiamo da $f(t) \in F[t]$, dove i generici elementi di $F[t]$ sono della forma $f(t) = \sum_{n=0}^{+\infty} a_n t^n$. Definiamo

$$v_t(f(t)) = \min\{k \mid a_k \neq 0\},$$

Estendiamo tale valutazione a $F(t)$, i cui generici elementi sono della forma $f(t) = \sum_{n=N}^{+\infty} a_n t^n$, con $N \in \mathbb{Z}$ (anche negativo):

$$v_t\left(\frac{f}{g}\right) = v_t(f) - v_t(g).$$

È facile mostrare come le valutazioni definite sopra siano ben definite secondo la Definizione 1.13.

Lemma 1.17. Sia F un campo valutato con valutazione $v : F \to G \cup \{\infty\}$. Allora per ogni $a, b \in F$ vale che:

1. $v(1) = 0$,
2. $v(a^{-1}) = -v(a)$, se $a \neq 0$,
3. $v(-a) = v(a)$,
4. se $v(a) \neq v(b)$, allora $v(a + b) = \min(v(a), v(b))$.

Dimostrazione. Il punto (2) nella Definizione 1.13 ci dice che v è un omomorfismo tra F^* e G. Quindi mappa l'identità di F in quella di G: $v(1) = 0$, e manda l'inverso di un elemento di F nell'inverso di un elemento di G: $v(a^{-1}) = -v(a)$ (da ciò seguono i primi due asserti). Ora dalla proprietà (1a) della Definizione 1.12 abbiamo che $0 \leq v(-1)$ oppure $v(-1) \leq 0$. Supponiamo che $0 \leq v(-1)$, da cui segue:

$$0 \leq v(-1) \leq v(-1) + v(-1) = v(-1 \cdot -1) = v(1) = 0$$

cioè $v(-1) = 0$. Seguirbbe lo stesso risultato se supponessimo $v(-1) \leq 0$. Allora $v(-a) = v(-1 \cdot a) = v(-1) + v(a) = v(a)$ (da cui il terzo asserto). Infine supponiamo $v(a) \neq v(b)$, ad esempio $v(a) < v(b)$. Allora dal punto (3) della Definizione 1.13 seguono le seguenti disuguaglianze: $v(a + b) \geq \min(v(a), v(b)) = v(a) = v(a + b - b) \geq$
$\geq \min(v(a + b), v(-b)) = \min(v(a + b), v(b)) = v(a + b)$. Sono quindi tutte uguaglianze e ciò conclude la dimostrazione. □

Osservazione 1.18. Ogni campo valutato ha alcune strutture naturali:

- v è un omomorfismo da F^* a G, quindi $v(F^*)$ è un sottogruppo linearmente ordinato di G, chiamato Gruppo dei valori.

- Definiamo $\mathcal{O}_F = \{a \in F \mid v(a) \geq 0\}$. $\mathcal{O}_F$ contiene $1, 0$ ed è chiuso rispetto all'addizione, moltiplicazione e inverso additivo, è quindi un sottoanello di F, chiamato anello di valutazione. Osserviamo che $\forall a \in F, a \in \mathcal{O}_F \vee a^{-1} \in \mathcal{O}_F$, perché se $v(a) < 0$, allora segue che $v(a^{-1}) > v(a) + v(a^{-1}) = v(a \cdot a^{-1}) = v(1) = 0$. Quindi il campo delle frazioni di $\mathcal{O}_F$ è F. Se non c'è ambiguità denoteremo $\mathcal{O}_F$ con $\mathcal{O}$.

- Gli elementi invertibili in $\mathcal{O}$ sono gli elementi con valutazione 0. Infatti se un elemento $a \in \mathcal{O}$ è tale che $a^{-1} \in \mathcal{O}$ allora $0 \leq v(a) + v(a^{-1}) = v(a \cdot a^{-1}) = v(1) = 0$ ma dato che entrambi $v(a)$ e $v(a^{-1})$ sono positivi perché $a, a^{-1} \in \mathcal{O}$ si ha $0 = v(a) = v(a^{-1})$. Al contrario, se un elemento $a \in O_F$ ha valutazione nulla, allora $v(a^{-1}) = -v(a) = 0$, in particolare $a^{-1} \in \mathcal{O}$. Denotiamo quindi con $\mathcal{O}^*$ le unità in O.

- Definiamo $I_1 = \{a \in \mathcal{O} \mid v(a) > 0\}$. L'insieme I_1 è un ideale, dato che è chiuso per addizione e se $a \in I_1, b \in \mathcal{O}$, allora $v(ab) = v(a) + v(b) > 0$, cioè $ab \in I_1$. È inoltre un ideale massimale, in quanto se esiste I' ideale in $\mathcal{O}$ che contiene propriamente I_0, allora ha un elemento u tale che $v(u) = 0$, cioè contiene un elemento invertibile e quindi $I' = \mathcal{O}$.

- Dato che I_1 è un ideale massimale, il quoziente $\overline{F} = \mathcal{O}_F/I_1$ è un campo, detto campo residuo. Denotiamo la classe residuo di $a \in \mathcal{O}_F$ con $\overline{a}$.

1.4 Campi a valutazione discreta

Definizione 1.19. Un campo F con valutazione v è chiamato discreto se il suo gruppo dei valori $v(F^*)$ è isomorfo a $\mathbb{Z}$ con il suo usuale ordinamento. Chiamiamo l'isomorfismo ϕ. Un elemento $\pi \in F$ è detto elemento primo se $\phi(v(\pi)) = 1$.

Per facilitare la notazione indicheremo $(\phi \circ v)$ solamente con v. I campi $\mathbb{Q}$ e $F(t)$ con le valutazioni v_p e v_t (definite negli Esempi 1.15 e 1.16) sono due campi con valutazione discreta.

Lemma 1.20. Sia F un campo a valutazione discreta con valutazione v e sia π un elemento primo in F. Allora:

- Per ogni $a \in F^*$, se $v(a) = n \in \mathbb{Z}$, $a = u\pi^n$ per qualche $u \in \mathcal{O}_F^*$;
- $\forall n \geq 1$, l'insieme $I_n = \{a \in F \mid v(a) \geq n\}$ è un ideale principale di O, generato da π^n.

Dimostrazione. Per ogni $a \in F^*$ sia $n = v(a)$. Allora $v(a\pi^{-n}) = v(a) + v(\pi^{-n}) = n - n = 0$, quindi $u = a\pi^{-n}$ è un'unità in $\mathcal{O}$ per l'Osservazione 1.18. Da cui $a = u\pi^n$, con $u \in \mathcal{O}^*$. Ora $\forall n \geq 1$, I_n è chiuso per l'addizione, e se $a \in I_n$ e $y \in \mathcal{O}$, allora $v(ay) = v(a) + v(y) \geq n + 0 = n$, quindi $ay \in I_n$, da cui I_n è un ideale. $\forall a \in I_n$, $a = u\pi^{v(a)} = u\pi^n\pi^{v(a)-n}$, per qualche unità $u \in \mathcal{O}^*$ □

Per tutti gli $n \geq 0$, definiamo l'anello $\mathcal{O}_n = \mathcal{O}/I_{n+1}$ (quoziente modulo π^{n+1}). Osserviamo come $\mathcal{O}_0 = \mathcal{O}/I_1 = \overline{F}$. Scegliamo un insieme di rappresentanti $A = \{\alpha_i\} \subset \mathcal{O}$ di elementi di $\overline{F}$. Sia ora $a \in \mathcal{O}$; se $\overline{a} = \overline{\alpha}_{i_0}$, allora $a - \alpha_{i_0} \in I_1 = (\pi)$; quindi $a = \alpha_{i_0} + a_1\pi$ per qualche $a_1 \in \mathcal{O}$. Ripetendo il procedimento, se $\overline{a}_1 = \overline{\alpha}_{i_1}$ allora $a_1 = \alpha_{i_1} + a_2\pi$ per qualche $a_2 \in \mathcal{O}$, quindi $a = \alpha_{i_0} + \alpha_{i_1}\pi + a_2\pi^2$. Quindi $a \equiv \alpha_{i_0} + \alpha_{i_1}\pi \mod \pi^2$, e $\alpha_{i_0} + \alpha_{i_1}\pi$ è l'immagine di a in $\mathcal{O}_1$. Possiamo quindi rappresentare, iterando questo procedimento ogni elemento di $\mathcal{O}_n$ unicamente nella forma $\alpha_{i_0} + \alpha_{i_1}\pi + \cdots + \alpha_{i_n}\pi^n$ per qualche $\alpha_{i_0}, \ldots, \alpha_{i_n} \in A$. Nella prossima definizione consideriamo $\forall n > 0$ l'omomorfismo canonico $\phi_n : \mathcal{O}_n \to \mathcal{O}_{n-1}$ che mappa elementi di $\mathcal{O}_n$ nel loro resto modulo π^n. Secondo la rappresentazione degli elementi di $\mathcal{O}_n$ come sopra, ϕ_n omette semplicemente il termine $\alpha_{i_n}\pi^n$.

Definizione 1.21. Sia F un campo a valutazione discreta. Definiti $\mathcal{O}_n$ e ϕ_n come sopra, il completamento di $\mathcal{O}$, $\widehat{\mathcal{O}}$ è definito da:

$$\widehat{\mathcal{O}} = \{(a_0, a_1, \ldots) \in \prod_{n\geq 0} \mathcal{O}_n \mid \forall n > 0, \phi_n(a_n) = a_{n-1}\}$$

$\widehat{\mathcal{O}}$ è un sottoanello dell'anello prodotto $\prod_{n\geq 0} \mathcal{O}_n$. Il completamento di F, $\widehat{F}$ è definito come il campo delle frazioni di $\widehat{\mathcal{O}}$.

Per comodità esprimeremo gli elementi $a = (\alpha_{i_0}, \alpha_{i_0} + \alpha_{i_1}\pi, \alpha_{i_0} + \alpha_{i_1}\pi + \alpha_{i_2}\pi^2, \dots)$ come l'infinita somma $\alpha_{i_0} + \alpha_{i_1}\pi + \alpha_{i_2}\pi^2 + \cdots$, e tale rappresentazione è ben definita.

Osservazione 1.22. Il completamento di F, che abbiamo definito puramente in modo algebrico, è isomorfo al completamento "analitico" di F indotto dalla metrica $\|a\|_v = 2^{-v(a)}$ (non lo mostriamo).

Nei prossimi due esempi introduciamo i protagonisti del principio di Ax-Kochen, il campo delle serie formali di Laurent e il campo dei numeri p-adici. Entrambi sono ottenuti tramite il completamento di un altro spazio, secondo la definizione 1.21.

Esempio 1.23. Consideriamo $F(t)$ il campo delle funzioni razionali sul campo F con la valutazione v_t definita all'Esempio 1.16. Vedremo che il suo completamento è $f((t))$, il campo delle serie formali di Laurent su F. Dato che $v_t(t) = 1$ scegliamo $\pi = t$ come elemento primo. Scrivendo le frazioni ai minimi termini, abbiamo che $\mathcal{O} = \mathcal{O}_{F(t)} = \{\frac{f}{g} \in F(t) \mid t \nmid g\}$ con ideale massimale $I_1 = \{\frac{f}{g} \in F(t) \mid t | f, t \nmid g\}$. Mostriamo ora come $\mathcal{O}/I_1 = \overline{F(t)} \cong F$: sia $\frac{f}{g} \in \mathcal{O}$ e sia $h \in F$ l'inverso del termine costante di g, cioè tale che $hg \equiv 1 \mod t$). Sia inoltre $l = \frac{f(hg-1)}{t} \in F(t)$. Ebbene

$$\frac{f}{g} + \frac{tl}{g} = \frac{f + tl}{g} = \frac{f + f(hg-1)}{g} = \frac{fhg}{g} = fh \in F[t]$$

Osserviamo che $\frac{tl}{g} = t\frac{l}{g} \in I_1$ dato che I_1 è un ideale e $t \in I_1$, quindi le uguaglianze sopra mostrano come ogni elemento di $\mathcal{O}$ è congruente a un elemento di $F[t]$ mod I_1 e ricordando che $t \in I_1$, ogni elemento di $\mathcal{O}$ è congruente a un elemento di F mod I_1. Da ciò $\overline{F(t)} \cong F$, possiamo quindi scegliere come rappresentanti gli elementi di F. In generale gli elementi di $\widehat{\mathcal{O}}$, il completamento di $\mathcal{O}$, sono della forma $\alpha_{i_0} + \alpha_{i_1}\pi + \alpha_{i_2}\pi^2 + \cdots$ con π primo di F. In questo caso $\pi = t$, allora gli elementi sono della forma $\alpha_{i_0} + \alpha_{i_1}t + \alpha_{i_2}t^2 + \cdots$ con $\alpha_i \in F$, cioè $\widehat{\mathcal{O}} = F[[t]]$. Il suo campo delle frazioni sarà quindi $\widehat{F(t)}$. Sia $x = \frac{\alpha_0+\alpha_1 t+\cdots}{\beta_0+\beta_1 t+\cdots} \in \widehat{F(t)}$. Sia $k = \min\{j \mid \beta_j \neq 0\}$. Possiamo quindi esprimere $x = (\frac{1}{\beta_k t^k})(\frac{\alpha_0+\alpha_1 t+\cdots}{1+\gamma_1 t+\cdots})$, dove $\gamma_i = \beta_{k+1}\beta_k^{-1} \in F$ per ogni $i \geq 1$. Tramite la formula della serie geometrica abbiamo che:

$$\frac{1}{1 + \gamma_1 t + \cdots} = \frac{1}{1 - (-\gamma_1 t - \cdots)} = 1 + (-\gamma_1 t - \cdots) + (-\gamma_1 t - \cdots)^2 + \cdots$$

da cui $y = \frac{1}{1+\gamma t+\cdots} \in \mathbb{F}[[t]]$. Possiamo scrivere $x = \beta_k^{-1} t^{-k} y(\alpha_0 + \alpha_1 t + \cdots)$ e tale elemento ha quindi la forma $c_{-k}t^{-k} + \cdots + c_{-1}t^{-1} + c_0 + c_1 t + \cdots$ con $c_i \in F$. Tutti gli elementi di $\widehat{F(t)}$ possono quindi essere scritti in questa forma. Chiamiamo quindi il completamento il campo delle serie formali di Laurent su F e lo denotiamo con $F((t))$.

Esempio 1.24. Per ogni primo p, definiamo il campo dei numeri p-adici $\mathbb{Q}_p$ come il completamento di $\mathbb{Q}$ secondo la valutazione v_p definita all'Esempio 1.15. Osservando che $v_p(p) = 1$, scegliamo $\pi = p$ come elemento primo di $\mathbb{Q}$. Similarmente all'esempio precedente, scrivendo le frazioni ai minimi termini, abbiamo che $\mathcal{O} = \mathcal{O}_{\mathbb{Q}} = \{\frac{a}{b} \in \mathbb{Q} \mid p \nmid b\}$ con ideale massimale $I_1 = \{\frac{a}{b} \in \mathbb{Q} \mid p|a, p \nmid b\}$. Ora per ogni $\frac{a}{b} \in \mathcal{O}$ sia $d \in \mathbb{Z}$ tale che $db \equiv 1 \mod p$). Sia $c = \frac{a(db-1)}{p} \in \mathbb{Z}$. Seguono ora le uguaglianze:

$$\frac{a}{b} + \frac{pc}{b} = \frac{a+pc}{b} = \frac{a+a(db-1)}{b} = \frac{adb}{b} = ad \in \mathbb{Z}$$

Dato che $p \in I_1$ e I_1 è un ideale, abbiamo che $\frac{pc}{b} \in I_1$, Quindi ciò mostra che ogni elemento di $\mathcal{O}$ è congruente a un intero modulo I_1, e dato che ogni multiplo di p sta in I_1p, è congruente a un intero in $\{0, 1, \ldots, p-1\}$ mod I_1. Quindi il campo delle classi residuo ha p elementi, $\overline{\mathbb{Q}} \cong \mathbb{F}_p$, e prendiamo come rappresentanti delle classi l'insieme $A = \{1, 2, \ldots, p-1\}$. Prendiamo ora il completamento di $\mathcal{O}$. L'anello risultante è $\widehat{\mathcal{O}} = \mathbb{Z}_p$, gli interi p-adici. I suoi elementi possono essere unicamente nella forma $\alpha_0 + \alpha_1 p + \alpha_2 p^2 + \cdots$, con ogni $\alpha_i \in A$. Quindi il completamento di $\mathbb{Q}$ secondo la valutazione v_p è $\mathbb{Q}_p$, il campo delle frazioni di $\mathbb{Z}_p$. Con un argomento simile all'esempio sopra, ogni elemento di $\mathbb{Q}_p$ può essere rappresentato in modo unico nella forma $c_{-k}p^{-k} + \cdots + c_{-1}p^{-1} + c_0 + c_1 p + \cdots$, con ogni $c_i \in A$.

1.5 Congettura di Artin

Artin osservò che gli elementi di $\mathbb{Q}_p$ possono essere pensati come serie formali di Laurent in una singola "variabile" p con coefficienti in $\mathbb{F}_p$. Le somiglianze tra queste due strutture e la conoscenza del fatto che $\mathbb{F}_p((t))$ fosse C_2 sono stati i motivi della congettura di Artin del 1950 secondo cui $\mathbb{Q}_p$ è C_2. Tuttavia, i campi $\mathbb{Q}_p$ e $\mathbb{F}_p((t))$ non sono isomorfi, la loro aritmetica è molto diversa, in particolare il primo ha caratteristica 0, mentre il secondo caratteristica p. Solo gli strumenti logici che introdurremo nelle mani di James

Ax e Simon Kochen saranno in grado di dimostrare che la somiglianza tra questi campi non è solo una coincidenza. Ora mostreremo quindi in ordine:

- che $\mathbb{F}_p((t))$ è C_2;
- gli strumenti logici necessari;
- il Principio di Ax-Kochen, che afferma come, data una formula ben definita secondo dei formalismi che introduciamo nel prossimo capitolo (e tale formula sarà la proprietà di essere C_2), essa è vera in $\mathbb{F}_p((t))$ per tutti i primi p tranne un numero finito se e solo se è vera anche in $\mathbb{Q}_p$ per tutti i primi p tranne un numero finito.

Saltiamo ora la dimostrazione di alcuni teoremi che enunciamo solo, per dimostrare il primo asserto della lista.

Definizione 1.25. Per ogni campo a valutazione discreta F con anello di valutazione O, consideriamo l'omomorfismo $i : \mathcal{O} \to \widehat{\mathcal{O}}$ che mappa $x \in \mathcal{O}$ nell'immagine di x in $\mathcal{O}_n$ per ogni $n \geq 0$. L'unico elemento di $\mathcal{O}$ divisibile da tutte le potenze di π è 0, quindi i è iniettiva. Così consideriamo $\mathcal{O}$ come sottoanello di $\widehat{\mathcal{O}}$ e F come un sottocampo di $\widehat{F}$. Se i è anche suriettivo, allora $\mathcal{O} \cong \widehat{\mathcal{O}}$ e $F \cong \widehat{F}$. In tale caso diciamo che $\mathcal{O}$ e F sono completi.

Lemma 1.26. Il completamento di un campo a valutazione discreta è un campo a valutazione discreta completo.

Definizione 1.27. Sia f un polinomio omogeneo in n variabili su un campo a valutazione discreta F con elemento primo π, e supponiamo che ogni coefficiente di f sia nell'anello di valutazione $\mathcal{O}$. Diciamo che uno zero $(\alpha_1, \ldots, \alpha_n) \in \mathcal{O}^n$ di f è primitivo se per qualche j, $\pi \nmid \alpha_j$. Similarmente, per $m \geq 0$, diciamo che uno zero $(\overline{\alpha}_1, \ldots, \overline{\alpha}_n) \in O_m^n$ di $\overline{f}$ è primitivo se per qualche j, $\overline{\pi} \nmid \overline{\alpha}_j$, dove $\overline{\pi}$ è il resti di $\pi \mod \pi^{m+1}$.

Il nostro obiettivo è ridurre il problema di trovare zeri di f in $\mathcal{O}^n$ al problema d trovare zeri di $\overline{f}$ in $\mathcal{O}_m^n$ per ogni $m \geq 0$. Il vantaggio nel lavorare con zeri primitivi è che uno zero primitivo non può diventare triviale con la riduzione $\mod \pi^{m+1}$, infatti vale che:

Teorema 1.28. Sia F un campo a valutazione discreta completo con elemento primo π. Supponiamo che l campo delle classi residuo $\overline{F}$ è finito. Allora un polinomio omogeneo f in $\mathcal{O}$ di grado d in n variabili ha uno zero primitivo in $\mathcal{O}^n$ se e solo se $\overline{f}$ ha uno zero primitivo in $\mathcal{O}_m^n$ $\forall m \geq 0$

Teorema 1.29 (Teorema di Lang)**.** Se F è un campo finito, allora $F((t))$ è C_2.

Dimostrazione. È sufficiente considera il polinomio omogeneo a coefficienti in $F[[t]] = O_{F((t))}$, dato che possiamo elidere i denominatori. Infatti, dato $f \in F((t))[x_1, \ldots, x_n]$ omogeneo di grado d in n variabili, se c è la minima valutazione tra i coefficienti di f (se ad esempio $n = 2$, f sarà della forma $\sum_{k=0}^{d}(\sum_{i=N_k}^{+\infty} a_i t^i)x_1^k x_2^{d-k}$), allora $t^{cd}f \in F[[t]][x_1, \ldots, x_n]$ è anche omogeneo di grado d in n variabili. Se $(\alpha_1, \ldots, \alpha_n)$ è uno zero non triviale di $t^{cd}f$, allora $f(t^c\alpha_1, \ldots, t^c\alpha_n) = t^{cd}f(\alpha_1, \ldots, \alpha_n) = 0$ per l'osservazione 1.1, quindi $(t^c\alpha_1, \ldots, t^c\alpha_n)$ è uno zero non triviale di f.

Sia ora quindi f un polinomio omogeneo generico in $F[[t]]$ di grado d in n variabili, con $n > d^2$. Il campo delle classi residuo $\overline{F((t))} \cong F$ è finito, e $F((t))$ è completo per il Lemma 1.26, possiamo quindi applicare il Teorema 1.28 (con elemento primo $\pi = t$): dato che ogni zero primitivo in $F[[t]]^n$ è non triviale in $F((t))^n$, è sufficiente trovare uno zero primitivo di $\overline{f}$ nell'anello dei residui modulo t^{m+1} per ogni $m \geq 0$. Fissiamo $m \geq 0$, sia $\widetilde{f}$ il polinomio ottenuto ignorando i termini di grado maggiore di m in ogni coefficiente di f. Ogni coefficiente di $\widetilde{f}$ è quindi un polinomio in t di grado al più m.

Ora se $\widetilde{f}$ è il polinomio identicamente zero significa ogni coefficiente di f è divisibile da t^{m+1}, quindi riducendo modulo t^{m+1}, $\overline{f}$ è il polinomio zero, che ha banalmente uno zero primitivo, quindi in questo caso abbiamo finito.

Altrimenti consideriamo $\widetilde{f}$ come un polinomio omogeneo di grado d in n variabili in $F(t)$. Per il Corollario 1.8 e per ipotesi di finitezza F è C_1. Per il Teorema 1.11, $F(t)$ è C_2. Dato che $n > d^2$, per definizione di C_2, $\exists(\alpha_1, \ldots, \alpha_n) \in F(t)^n$ zero non triviale di $\widetilde{f}$ in $F(t)$. Sia j l'indice corrispondente all' $\alpha_j \in F(t)$ con valutazione minore e sia $c = v_t(\alpha_j)$. Sia ora $\beta_i := t^{-c}\alpha_i$ $\forall i \in [1, n]$ e osserviamo che $v_t(\beta_i) = v_t(t^{-c}) + v_t(\alpha_i) \geq -c + c = 0$, quindi $\beta_i \in F[t]$. Ora $t^{cd}\widetilde{f}(\beta_1, \ldots, \beta_n) = \widetilde{f}(t^c\beta_1, \ldots, t^c\beta_n) = \widetilde{f}(\alpha_1, \ldots, \alpha_n) = 0$. Dato che $F[t]$ è un dominio e che $t^{cd} \neq 0$, $\widetilde{f}(\beta_1, \ldots, \beta_n) = 0$. Inoltre, $v_t(\beta_j) = -c + c = 0$, quindi $t \nmid \beta_j$ da cui $(\beta_1, \ldots, \beta_n)$ è uno zero primitivo. Ora finalmente, dato che $\widetilde{f}(\beta_1, \ldots, \beta_n) = 0$ e $\widetilde{f}$ corrisponde a $\overline{f}$ mod t^{m+1}, considerando $\beta_1, \ldots, \beta_n$ come elementi di $F[[t]]$ dati

dall'inclusione naturale, $(\overline{\beta}_1, \ldots, \overline{\beta}_n)$ è uno zero di $\overline{f}$ mod t^{m+1}. Dato che lo zero è primitivo, anche la sua riduzione modulo t^{m+1} lo è, come volevasi dimostrare. □

Dato che il campo $\mathbb{F}_p$ è finito, dal teorema segue banalmente che il campo delle serie di Laurent $\mathbb{F}_p((t))$ su $\mathbb{F}_p$ è C_2 per ogni primo p.

Capitolo 2

Teoria dei Modelli

La teoria dei modelli studia le strutture matematiche attraverso gli strumenti della logica del primo ordine, analizzando quali proprietà possono essere espresse tramite tali strumenti e il loro comportamento nei modelli. Quindi, in questo capitolo abbandoniamo momentaneamente i polinomi per concentrarci sull'introdurre le nozioni di logica da applicare successivamente alle strutture algebriche definite nel capitolo precedente. In particolare, ora introdurremo le basi della logica del primo ordine, definendo linguaggi, strutture e nozioni di soddisfacibilità.

2.1 Richiamo di strumenti di Logica

Definizione 2.1. Un linguaggio $\mathcal{L}$ è l'unione di:

- $\mathcal{F}$, un insieme di simboli di funzione, con un intero $n_f \geq 0$ per ogni $f \in \mathcal{F}$;
- $\mathcal{R}$, un insieme di simboli di relazioni, con un intero $n_R > 0$ per ogni $R \in \mathcal{R}$

Gli interi n_f e n_R sono chiamate arietà delle corrispondenti funzioni e relazioni. Una funzione n-aria prende n argomenti e una relazione n-aria è una relazione fra n elementi. Sia $\mathcal{C} := \{f \in \mathcal{F} \mid n_f = 0\}$ e lo consideriamo come un insieme di simboli di costanti. Le funzioni e relazioni 1-arie e 2-arie, che useremo più frequentemente, vengono dette rispettivamente unarie e binarie.

Definizione 2.2. Sia $\mathcal{L} = \mathcal{F} \cup \mathcal{R}$ un linguaggio. Una $\mathcal{L}$-struttura $\mathcal{M}$ è:

- un insieme $M \neq \emptyset$, il dominio;
- una funzione $f^{\mathcal{M}} : M^{n_f} \to M$ per ogni $f \in \mathcal{F}$;
- una relazione $R^{\mathcal{M}} \subseteq M^{n_R}$ per ogni $R \in \mathcal{R}$.

$f^{\mathcal{M}}$ e $R^{\mathcal{M}}$ sono dette le interpretazioni degli $\mathcal{L}$-simboli in $\mathcal{M}$.

Definizione 2.3. Un campo F con valutazione v è chiamato campo valutato con *cross section* se $\exists\, i : v(F) \to F$ mappa iniettiva tale che i è un omomorfismo di gruppi tra $v(F^*)$ e F, e $\forall x \in F$ vale che $v(i(x)) = x$.

È possibile dare una *cross section* a ogni campo valutato dato un suo elemento primo π, definendo $i(n) := \pi^n \ \forall n \in \mathbb{Z}$, con $i(\infty) = 0$. Infatti $v(i(n)) = v(\pi^n) = n$, e $v(i(\infty)) = v(0) = \infty$. Grazie a questa definizione per il resto della tesi considereremo $v(F) = \{\pi^n \mid n \in \mathbb{Z}\}$ omettendo i.

Esempio 2.4. Per scrivere enunciati sui campi valutati (con *cross section*) abbiamo bisogno di simboli, consideriamo quindi il linguaggio $\mathcal{L}_{VF} = \{+, \cdot, -, 0, 1, V, \leq, v\}$, dove $+$ e $\cdot$ sono simboli di funzioni binarie, $-$ un simbolo di funzione unaria, 0 e 1 sono simboli di costante (funzioni con arietà 0), V è un simbolo di relazione unaria, $\leq$ simbolo di relazione binaria e v simbolo di funzione unaria.

La proprietà di *cross section* sarà utile per riferirsi a elementi del gruppo dei valori utilizzando il dominio della struttura relativa al campo valutato. Quando interpreteremo i simboli di $\mathcal{L}$ in una struttura, che sarà un campo valutato, useremo $+, \cdot, -, 0, 1, v, \leq$ per rappresentare rispettivamente le funzioni nel campo, l'inverso secondo l'addizione, gli elementi neutri per la somma e moltiplicazione, la valutazione, relazione d'ordine e infine consideriamo V per usare gli elementi del campo valutato, $x \in V$ se e solo se x è nel gruppo dei valori.

2.2 Termini, formule e soddisfacibilità

Da questa sezione in poi considereremo un insieme generico di variabili $\mathcal{V} = \{v_1, \ldots, v_n\}$, i connettivi booleani $\vee, \wedge, \neg$, i quantificatori $\forall, \exists$ e il simbolo $=$ come concetti già conosciuti dal lettore. Introduciamo ora i termini:

Definizione 2.5. Gli $\mathcal{L}$-termini sono espressioni ce rappresentano modi di combinare elementi della struttura.

- Le variabili sono termini.
- Se f è un simbolo di funzione e $t_1, \ldots, t_{n_f}$ sono $\mathcal{L}$-termini, allora $f(t_1, \ldots, t_{n_f})$ è un $\mathcal{L}$-termine.
- Se c è un simbolo di costante, allora è un $\mathcal{L}$-termine.

Definizione 2.6. Le $\mathcal{L}$-formule sono espressioni che rappresentano modi di esprimere delle proprietà che una struttura o suoi elementi possono avere. Si definiscono ricorsivamente come i termini a partire dalle $\mathcal{L}$-formule atomiche, che sono di due tipi:

- $R(t_1, \ldots, t_{n_R})$, con R simbolo di relazione in $\mathcal{L}$ e $t_1, \ldots, t_{n_R}$ $\mathcal{L}$-termini;
- $t_1 = t_2$, con t_1, t_2 $\mathcal{L}$-termini.

Otteniamo le $\mathcal{L}$-formule combinando formule atomiche e formule tra loro usando i quantificatori e i connettivi booleani.

Definizione 2.7. Sia ϕ una $\mathcal{L}$-formula con variabili libere da $v_1, \ldots, v_n$. Sia $\mathcal{M}$ una $\mathcal{L}$-struttura con dominio M, e siano $a_1, \ldots, a_n \in M^n$ elementi del dominio. Definiamo $\mathcal{M} \models \phi(a_1, \ldots, a_n)$ induttivamente come segue:

- Se ϕ è $t_1(v_1, \ldots, v_n) = t_2(v_1, \ldots, v_n)$, allora $\mathcal{M} \models \phi(a_1, \ldots, a_n)$ se e solo se $t_1^{\mathcal{M}}(a_1, \ldots, a_n) = t_2^{\mathcal{M}}(a_1, \ldots, a_n)$.
- Se ϕ è $R(t_1(v_1, \ldots, v_n), \ldots, t_{n_R}(v_1, \ldots, v_n))$, allora $\mathcal{M} \models \phi(a_1, \ldots, a_n)$ se e solo se $(t_1^{\mathcal{M}}(a_1, \ldots, a_n), \ldots, t_{n_R}^{\mathcal{M}}(a_1, \ldots, a_n)) \in R^{\mathcal{M}}$.
- Se ϕ è $\neg\psi(v_1, \ldots, v_n)$, allora $\mathcal{M} \models \phi(a_1, \ldots, a_n)$ se e solo se $\mathcal{M} \not\models \psi(a_1, \ldots, a_n)$.
- Se ϕ è $\psi(v_1, \ldots, v_n) \wedge \theta(v_1, \ldots, v_n)$, allora $\mathcal{M} \models \phi(a_1, \ldots, a_n)$ se e solo se $\mathcal{M} \models \psi(a_1, \ldots, a_n)$ e $\mathcal{M} \models \theta(a_1, \ldots, a_n)$.
- Se ϕ è $\psi(v_1, \ldots, v_n) \vee \theta(v_1, \ldots, v_n)$, allora $\mathcal{M} \models \phi(a_1, \ldots, a_n)$ se e solo se $\mathcal{M} \models \psi(a_1, \ldots, a_n)$ o $\mathcal{M} \models \theta(a_1, \ldots, a_n)$.

- Se ϕ è $\exists v\, \psi(v_1, \ldots, v_n, v)$, allora $\mathcal{M} \models \phi(a_1, \ldots, a_n)$ se e solo se esiste un $b \in M$ tale che $\mathcal{M} \models \psi(a_1, \ldots, a_n, b)$.
- Se ϕ è $\forall v\, \psi(v_1, \ldots, v_n, v)$, allora $\mathcal{M} \models \phi(a_1, \ldots, a_n)$ se e solo se per ogni $b \in M$, $\mathcal{M} \models \psi(a_1, \ldots, a_n, b)$.

Definizione 2.8. Un insieme di $\mathcal{L}$-formule S con variabili libere $v_1, \ldots, v_m$ è detto soddisfacibile se esiste una $\mathcal{L}$-struttura $\mathcal{M}$ con dominio M e elementi $a_1, \ldots, a_n \in M$ tale che $\mathcal{M} \models \phi(a_1, \ldots, a_n)$ per ogni formula $\phi \in S$.

Definizione 2.9. Una $\mathcal{L}$-sentenza è una $\mathcal{L}$-formula senza variabili libere.

Esempio 2.10. Per ogni primo p, consideriamo la $\mathcal{L}_{VF}$-sentenza

$$\mathrm{Char}_p : \underbrace{1 + 1 + \cdots + 1}_{\text{p volte}} = 0$$

che esprime la proprietà di una $\mathcal{L}_{VF}$-struttura di avere caratteristica p. Ad esempio $\mathbb{F}_7 \models \mathrm{Char}_7$ mentre $\mathbb{Q}_7 \not\models \mathrm{Char}_7$. Dato che le sentenze non hanno variabili, esse esprimono una proprietà della struttura, non di alcuni elementi. La proprietà di avere caratteristica zero si esprime affermando che la struttura non ha caratteristica p per ogni p, ma in una singola sentenza possiamo scrivere solo un numero limitato di $\neg\mathrm{Char}_p$. Ce ne servono infinite! Introduciamo quindi:

Definizione 2.11. Una $\mathcal{L}$-teoria T è un insieme di $\mathcal{L}$-sentenze, siano $\mathcal{M}$ una $\mathcal{L}$-struttura e T una $\mathcal{L}$-teoria. Diciamo che $\mathcal{M}$ è un modello di T se $\mathcal{M} \models \phi$ per ogni sentenza $\phi \in T$. In tal caso scriviamo $\mathcal{M} \models T$. Diciamo inoltre che T è soddisfacibile se esiste un tale modello $\mathcal{M}$ per T.

Per esprimere la proprietà di avere caratteristica zero definiamo allora la $\mathcal{L}_{VF}$-teoria $\mathrm{Char}_0 = \{\neg\mathrm{Char}_p \mid p \text{ primo}\}$. Allora $\mathbb{Q}_p \models \mathrm{Char}_0$ dato che $\mathbb{Q}_p \models \neg\mathrm{Char}_p$ per ogni p primo, mentre $\mathbb{F}_p \not\models \mathrm{Char}_0$ visto che $\mathbb{F}p \not\models \neg\mathrm{Char}_5$.

Definizione 2.12. Una classe di $\mathcal{L}$-strutture $\mathcal{K}$ è detta elementare se esiste una $\mathcal{L}$-teoria T tale che $\mathcal{K} = \{\mathcal{M} \quad \mathcal{L}\text{-struttura} \mid \mathcal{M} \models T\}$. La teoria T è detta un insieme di assiomi per $\mathcal{K}$.

Esempio 2.13. Mostriamo che la classe dei campi valutati con *cross section* è elementare, fornendo un insieme di assiomi nel linguaggio $\mathcal{L}_{VF}$. Denotiamo questa teoria con VF.

- Assiomi di Campo:
  1. $\forall v_1 \forall v_2 \forall v_3((v_1 + v_2) + v_3 = v_1 + (v_2 + v_3))$
  2. $\forall v_1 \ (v_1 + 0 = v_1)$
  3. $\forall v_1 \ (v_1 + -(v_1) = 0)$
  4. $\forall v_1 \forall v_2 (v_1 + v_2 = v_2 + v_1)$
  5. $\forall v_1 \forall v_2 \forall v_3((v_1 \cdot v_2) \cdot v_3 = v_1 \cdot (v_2 \cdot v_3))$
  6. $\forall v_1 (v_1 \cdot 1 = v_1)$
  7. $\forall v_1 (\neg(v_1 = 0) \to \exists v_2 \ (v_1 \cdot v_2 = 1))$
  8. $\forall v_1 \forall v_2 (v_1 \cdot v_2 = v_2 \cdot v_1)$
  9. $\forall v_1 \forall v_2 \forall v_3 (v_1 \cdot (v_2 + v_3) = v_1 \cdot v_2 + v_1 \cdot v_3)$
  10. $\neg(1 = 0)$
- Assiomi della valutazione:
  1. $\forall v_1 (v(v_1) = 0 \leftrightarrow v_1 = 0)$
  2. $\forall v_1 \forall v_2 (v(v_1 \cdot v_2) = v(v_1) \cdot v(v_2))$
  3. $\forall v_1 \forall v_2 (v(v_1) \leq v(v_2) \to v(v_1) \leq v(v_1 + v_2))$
- Il gruppo dei valori è un sottogruppo del gruppo moltiplicativo:
  1. $\forall v_1 \forall v_2 ((V(v_1) \wedge V(v_2)) \to V(v_1 \cdot v_2))$
  2. $\forall v_1 (V(v_1) \to \exists v_2 (V(v_2) \wedge v_1 \cdot v_2 = 1))$
- Assiomi di ordine lineare sul gruppo dei valori:
  1. $\forall v_1 \forall v_2 ((V(v_1) \wedge V(v_2)) \to (v_1 \leq v_2 \vee v_2 \leq v_1))$
  2. $\forall v_1 \forall v_2 \ ((V(v_1) \wedge V(v_2) \wedge v_1 \leq v_2 \wedge v_2 \leq v_1) \to v_1 = v_2)$

3. $\forall v_1 \forall v_2 \forall v_3((V(v_1) \wedge V(v_2) \wedge V(v_3) \wedge v_1 \leq v_2 \wedge v_2 \leq v_3) \rightarrow v_1 \leq v_3)$
4. $\forall v_1 \forall v_2 \forall v_3\ ((V(v_1) \wedge V(v_2) \wedge V(v_3) \wedge v_1 \leq v_2) \rightarrow v_1 \cdot v_3 \leq v_2 \cdot v_3)$

- Assiomi di *cross section*

1. $\forall v_1 V(v(v_1))$
2. $\forall v_1\ (V(v_1) \rightarrow v(v_1) = v_1)$

Definizione 2.14. Sia T una $\mathcal{L}$-teoria e ϕ una $\mathcal{L}$-sentenza. Diciamo che ϕ è una conseguenza logica di T scrivendo $T \models \phi$ se $\mathcal{M} \models \phi$ per ogni modello $\mathcal{M} \models T$. Una $\mathcal{L}$-teoria T è detta completa se per ogni $\mathcal{L}$-sentenza ϕ, si ha che $T \models \phi$ oppure $T \not\models \phi$.

Un risultato centrale nella teoria dei modelli è il teorema di compattezza, un potente strumento per costruire modelli.

Teorema 2.15 (Teorema di Compattezza)**.** Una $\mathcal{L}$-teoria T è soddisfacibile se e solo se ogni sottoinsieme finito di T è soddisfacibile.

2.3 Omomorfismi tra strutture

Definizione 2.16. Date due $\mathcal{L}$-strutture $\mathcal{M}$ e $\mathcal{N}$ con domini M e N, una $\mathcal{L}$-immersione da $\mathcal{M}$ a $\mathcal{N}$ è una mappa iniettiva $\eta : M \rightarrow N$ che preserva le interpretazioni degli $\mathcal{L}$-simboli, cioè tale che, se $\mathcal{L} = \mathcal{F} \cup \mathcal{R}$:

- $\forall f \in \mathcal{F}, \forall (a_1, \ldots, a_{n_f}) \in M^{n_f}$ vale che

$$\eta(f^{\mathcal{M}}(a_1, \ldots, a_{n_f})) = f^{\mathcal{N}}(\eta(a_1), \ldots, \eta(a_{n_f}))$$

- $\forall R \in \mathcal{R}, \forall (a_1, \ldots, a_{n_f}) \in M^{n_R}$, vale che

$$(a_1, \ldots, a_{n_R}) \in R^{\mathcal{M}} \text{ se e solo se } (\eta(a_1), \ldots, \eta(a_{n_R})) \in R^{\mathcal{N}}$$

.

Un $\mathcal{L}$-isomorfismo è una $\mathcal{L}$-immersione biunivoca. Se esiste un $\mathcal{L}$-isomorfismo tra $\mathcal{M}$ e $\mathcal{N}$ scriviamo che $\mathcal{M} \cong \mathcal{N}$.

L'esistenza di una $\mathcal{L}$-immersione tra due $\mathcal{L}$-strutture non ci dà informazioni su quali $\mathcal{L}$-formule sono soddisfatte in queste strutture. Nella prossima definizione introduciamo quindi uno strumento più forte:

Definizione 2.17. Una $\mathcal{L}$-immersione elementare è una $\mathcal{L}$-immersione $j : \mathcal{M} \to \mathcal{N}$ tra due $\mathcal{L}$-strutture $\mathcal{M}, \mathcal{N}$ tale che per ogni $\mathcal{L}$-formula $\phi(v_1, \ldots, v_n)$ ed elementi $a_1, \ldots, a_n$ nel dominio di $\mathcal{M}$, $\mathcal{M} \models \phi(a_1, \ldots, a_n)$ se e solo se $\mathcal{N} \models \phi(j(a_1), \ldots, j(a_n))$.

Definizione 2.18. Una $\mathcal{L}$-struttura $\mathcal{M}$ con dominio M è una sottostruttura di una $\mathcal{L}$-struttura $\mathcal{N}$ con dominio N se $M \subseteq N$ e la mappa di inclusione è una $\mathcal{L}$-immersione. Se $\mathcal{M}$ è una sottostruttura di $\mathcal{N}$ e la mappa di inclusione è elementare, allora $\mathcal{M}$ è una sottostruttura elementare di $\mathcal{N}$ e $\mathcal{N}$ è un'estensione elementare di $\mathcal{M}$.

Uno dei teoremi fondamentali della teoria dei modelli riguarda l'esistenza di estensioni e sottostrutture elementari. I Teoremi di Löwenheim-Skolem, qui riportati senza dimostrazione, affermano intuitivamente che, data una struttura infinita, esistono estensioni elementari e sottostrutture elementari di ogni cardinalità infinita.

Teorema 2.19 (Teorema di Löwenheim-Skolem "Up")**.** Sia $\mathcal{M}$ una $\mathcal{L}$-struttura infinita con dominio M, e sia κ un cardinale infinito tale che $\kappa \geq |M| + |\mathcal{L}|$. Allora esiste una $\mathcal{L}$-struttura $\mathcal{N}$ di cardinalità κ e un'immersione elementare $j : \mathcal{M} \to \mathcal{N}$, tale che $\mathcal{N}$ è un'estensione elementare di $j(\mathcal{M})$.

Teorema 2.20 (Teorema di Löwenheim-Skolem "Down")**.** Sia $\mathcal{M}$ una $\mathcal{L}$-struttura con dominio M, e sia $X \subseteq M$. Allora esiste una sottostruttura elementare $\mathcal{N}$ di $\mathcal{M}$ con dominio N tale che $X \subseteq N$ e $|N| \leq |X| + |\mathcal{L}| + \aleph_0$.

Definizione 2.21. Data una $\mathcal{L}$-struttura $\mathcal{M}$ definiamo la $\mathcal{L}$-teoria completa di $\mathcal{M}$, $\mathrm{Th}(\mathcal{M}) = \{\phi \mid M \models \phi\}$. Per definizione, se ϕ è una $\mathcal{L}$-sentenza, $\mathcal{M} \models \phi$, oppure $\mathcal{M} \not\models \phi$, quindi $\mathrm{Th}(\mathcal{M}) \models \phi$ oppure $\mathrm{Th}(\mathcal{M}) \models \neg\phi$, cioè $\mathrm{Th}(\mathcal{M})$ è completa.

Definizione 2.22. Siano $\mathcal{M}$ e $\mathcal{N}$ due $\mathcal{L}$-strutture. Diciamo che $\mathcal{M}$ e $\mathcal{N}$ sono elementarmente equivalenti, e scriviamo $\mathcal{M} \equiv \mathcal{N}$, se $\mathrm{Th}(\mathcal{M}) = \mathrm{Th}(\mathcal{N})$, cioè che per ogni $\mathcal{L}$-sentenza ϕ, $\mathcal{M} \models \phi$ se e solo se $\mathcal{N} \models \phi$.

Osservazione 2.23. L'esistenza di una $\mathcal{L}$-immersione elementare tra due $\mathcal{L}$-strutture $\mathcal{M}$ e $\mathcal{N}$ implica banalmente che $\mathcal{M} \equiv \mathcal{N}$. Il viceversa non è vero in generale, vale invece l'asserto del prossimo teorema, con ipotesi più forti:

Teorema 2.24. Date due $\mathcal{L}$-strutture $\mathcal{M}$ e $\mathcal{N}$, se $\mathcal{M} \cong \mathcal{N}$, allora $\mathcal{M} \equiv \mathcal{N}$.

Dimostrazione. Sia $j : \mathcal{M} \to \mathcal{N}$ un $\mathcal{L}$-isomorfismo che mappa M, il dominio di $\mathcal{M}$, biunivocamente in N, il dominio di $\mathcal{N}$. Se $\overline{a} = (a_1, \ldots, a_n) \in M^n$, poniamo $j(\overline{a}) = (j(a_1), \ldots, j(a_n)) \in N^n$.

Dimostreremo per induzione sui termini la seguente affermazione: se t è un $\mathcal{L}$-termine con variabili libere in $\overline{v} = (v_1, \ldots, v_n)$, allora per ogni $\overline{a} = (a_1, \ldots, a_n) \in M^n$, $j(t^{\mathcal{M}}(\overline{a})) = t^{\mathcal{N}}(j(\overline{a}))$.

- Se t è un simbolo di costante c, allora $j(t^{\mathcal{M}}(\overline{a})) = j(c^{\mathcal{M}}) = c^{\mathcal{N}} = t^{\mathcal{N}}(j(\overline{a}))$.
- Se t è una variabile v_i, allora $j(t^{\mathcal{M}}(\overline{a})) = j(a_i) = t^{\mathcal{N}}(j(\overline{a}))$.
- Se t è $f(t_1(v), \ldots, t_{n_f}(v))$, dove f è un simbolo di funzione e $t_1, \ldots, t_{n_f}$ sono $\mathcal{L}$-termini per i quali l'affermazione è vera, allora:

$$\begin{aligned} j(t^{\mathcal{M}}(\overline{a})) &= j(f^{\mathcal{M}}(t_1^{\mathcal{M}}(\overline{a}), \ldots, t_{n_f}^{\mathcal{M}}(\overline{a}))) \\ &= f^{\mathcal{N}}(j(t_1^{\mathcal{M}}(\overline{a})), \ldots, j(t_{n_f}^{\mathcal{M}}(\overline{a}))) \quad \text{poiché } j \text{ è una } \mathcal{L}\text{-immersione} \\ &= f^{\mathcal{N}}(t_1^{\mathcal{N}}(j(\overline{a})), \ldots, t_{n_f}^{\mathcal{N}}(j(\overline{a}))) \quad \text{per l'ipotesi induttiva} \\ &= t^{\mathcal{N}}(j(\overline{a})). \end{aligned}$$

Questo completa l'induzione sui termini e la prova dell'affermazione. Proveremo ora per induzione sulle formule che se ϕ è una $\mathcal{L}$-formula con variabili libere in $\overline{v} = (v_1, \ldots, v_n)$, allora per ogni $\overline{a} = (a_1, \ldots, a_n) \in M^n$, $\mathcal{M} \models \phi(\overline{a})$ se e solo se $\mathcal{N} \models \phi(j(\overline{a}))$.

Se $\phi(\overline{v})$ è $t_1(\overline{v}) = t_2(\overline{v})$, dove t_1 e t_2 sono $\mathcal{L}$-termini, allora:

$$\begin{aligned} \mathcal{M} \models \phi(\overline{a}) &\iff t_1^{\mathcal{M}}(\overline{a}) = t_2^{\mathcal{M}}(\overline{a}) \\ &\iff j(t_1^{\mathcal{M}}(\overline{a})) = j(t_2^{\mathcal{M}}(\overline{a})) \quad \text{(poiché } j \text{ è iniettiva)} \\ &\iff t_1^{\mathcal{N}}(j(\overline{a})) = t_2^{\mathcal{N}}(j(\overline{a})) \quad \text{(applicando l'affermazione sui termini)} \\ &\iff \mathcal{N} \models \phi(j(\overline{a})). \end{aligned}$$

Se $\phi(v)$ è $R(t_1(\overline{v}), \ldots, t_{n_R}(\overline{v}))$, dove R è un simbolo di relazione e $t_1, \ldots, t_{n_R}$ sono $\mathcal{L}$-termini, allora:

$$\begin{aligned}
\mathcal{M} \models \phi(\overline{a}) &\iff (t_1^{\mathcal{M}}(\overline{a}), \ldots, t_{n_R}^{\mathcal{M}}(\overline{a})) \in R^{\mathcal{M}} \\
&\iff (j(t_1^{\mathcal{M}}(\overline{a})), \ldots, j(t_{n_R}^{\mathcal{M}}(\overline{a}))) \in R^{\mathcal{N}} \quad \text{poiché } j \text{ è una } \mathcal{L}\text{-immersione} \\
&\iff (t_1^{\mathcal{N}}(j(\overline{a})), \ldots, t_{n_R}^{\mathcal{N}}(j(\overline{a}))) \in R^{\mathcal{N}} \quad \text{applicando l'affermazione} \\
&\iff \mathcal{N} \models \phi(j(\overline{a})).
\end{aligned}$$

Se $\phi(v)$ è $\neg\psi(v)$, dove ψ è una $\mathcal{L}$-formula per la quale l'asserzione è vera, allora:

$$\begin{aligned}
\mathcal{M} \models \phi(\overline{a}) &\iff \mathcal{M} \not\models \psi(\overline{a}) \\
&\iff \mathcal{N} \not\models \psi(j(\overline{a})) \quad \text{per ipotesi induttiva} \\
&\iff \mathcal{N} \models \phi(j(\overline{a})).
\end{aligned}$$

Se $\phi(v)$ è $\psi(v) \wedge \theta(v)$, dove ψ e θ sono $\mathcal{L}$-formule per le quali l'asserzione è vera, allora:

$$\begin{aligned}
\mathcal{M} \models \phi(\overline{a}) &\iff \mathcal{M} \models \psi(\overline{a}) \text{ e } \mathcal{M} \models \theta(\overline{a}) \\
&\iff \mathcal{N} \models \psi(j(\overline{a})) \text{ e } \mathcal{N} \models \theta(j(\overline{a})) \quad \text{per ipotesi induttiva} \\
&\iff \mathcal{N} \models \phi(j(\overline{a})).
\end{aligned}$$

Se $\phi(\overline{v})$ è $\exists w\, \psi(\overline{v}, w)$, dove w è una variabile e ψ è una $\mathcal{L}$-formula per la quale l'asserzione è vera, allora $\mathcal{M} \models \phi(\overline{a})$ se e solo se esiste un qualche $b \in M$ tale che $\mathcal{M} \models \psi(\overline{a}, b)$. Ora, se esiste tale b, allora per induzione $\mathcal{N} \models \psi(j(\overline{a}), j(b))$, quindi esiste $c \in N$ (si prenda $c = j(b)$) tale che $\mathcal{N} \models \psi(j(\overline{a}), c)$, e dunque $\mathcal{N} \models \phi(j(\overline{a}))$. Viceversa, se $\mathcal{N} \models \phi(j(\overline{a}))$, allora esiste $c \in N$ tale che $\mathcal{N} \models \psi(j(\overline{a}), c)$. Poiché j è suriettiva, esiste $b \in M$ tale che $j(b) = c$, e per induzione $\mathcal{M} \models \psi(\overline{a}, b)$.

Questo completa la prova per induzione sulle formule. Non è necessario considerare formule costruite usando $\vee$ o $\forall$, poiché queste possono essere riscritte utilizzando solo $\neg, \wedge$ e $\exists$. Questo completa anche la dimostrazione del teorema, poiché abbiamo mostrato che se ϕ è un $\mathcal{L}$-sentenza, allora $\mathcal{M} \models \phi$ se e solo se $\mathcal{N} \models \phi$. Pertanto $\mathcal{M} \equiv \mathcal{N}$. $\square$

2.4 Filtri, Ultrafiltri ed Equivalenza Elementare

I campi $\mathbb{F}_p((t))$ e $\mathbb{Q}_p$ non sono elementarmente equivalenti (ad esempio la sentenza Char_p è vera nel primo e falso nel secondo). Vedremo però come ciò sia invece vero per le $\mathcal{L}_{VF}$-sentenze per tutti i p eccetto un numero finito. Questo concetto di "tutte tranne un numero finito" è esprimibile tramite la nozione di filtro su di un insieme:

Definizione 2.25. Dato un insieme I, un filtro su I è un sottoinsieme dell'insieme delle parti $\mathcal{D} \subseteq \mathcal{P}(I)$ tale che:

- $\emptyset \notin \mathcal{D}$;
- $I \in \mathcal{D}$;
- se $A \in \mathcal{D}$ e $B \in \mathcal{D}$, allora $A \cap B \in \mathcal{D}$;
- se $A \in \mathcal{D}$ e $A \subseteq B \subseteq \mathcal{D}$, allora $B \in \mathcal{D}$.

Per l'ultima proprietà si può intuire che prendere un filtro significa prendere i sottoinsiemi dell'insieme I "abbastanza grandi", cioè rilevanti.

Esempio 2.26. I seguenti esempi sono filtri su di un insieme I:

- $\mathcal{D}_T = \{I\}$, il filtro banale;
- Per ogni $j \in I$, $\mathcal{D}_j = \{X \subseteq I \mid j \in X\}$ è detto il filtro principale generato da j;
- nel caso in cui I sia infinito, $\mathcal{D}_F = \{X \subseteq I \mid I \setminus X \text{ è finito}\}$ è un filtro ben definito ed è detto il filtro di Fréchet.

Definizione 2.27. Un filtro $\mathcal{D}$ su I è un ultrafiltro se per ogni $X \subseteq I$, $X \in \mathcal{D}$ oppure $I \setminus X \in \mathcal{D}$

Osservazione 2.28. Tutti i filtri principali sono ultrafiltri.

Il lemma e il teorema a seguire dimostrano che gli ultrafiltri non principali possono essere ottenuti estendendo il filtro di Fréchet con un insieme infinito.

Lemma 2.29. Dato un filtro $\mathcal{D}$ su di un insieme I e un sottoinsieme $X \subset I$ tale che $X \notin \mathcal{D}$, possiamo estendere $\mathcal{D}$ a un filtro $\mathcal{D}_X$ su I tale che $\mathcal{D} \subseteq \mathcal{D}_X$ e $I \setminus X \in \mathcal{D}_X$.

Dimostrazione. Sia $\mathcal{D}_X = \{Y \subseteq I \mid \exists Z_Y \in \mathcal{D} \text{ tale che } Z_Y \setminus X \subseteq Y\}$. Mostriamo che $\mathcal{D}_X$ è un filtro su I:

- se $\emptyset \in \mathcal{D}_X$, allora esiste $Z \in \mathcal{D}$ tale che $Z \setminus X = \emptyset$, cioè $Z \subseteq X$. Ma per definizione di filtro poiché $Z \subseteq X \subset I$, seguirebbe che $X \in \mathcal{D}$, andando contro le ipotesi;
- per ogni $Z \in \mathcal{D}$, $Z \setminus X \subseteq I$, quindi $I \in \mathcal{D}_X$;
- dati $A, B \in \mathcal{D}_X$, esistono $Z_A, Z_B \in \mathcal{D}$ tale che $Z_A \setminus X \subseteq A$ e $Z_B \setminus X \subseteq B$. Allora $(Z_A \cap Z_B) \setminus X \subseteq (A \cap B)$, quindi prendendo $Z_{A \cap B} = Z_A \cap Z_B$, si ha che $A \cap B \in \mathcal{D}_X$;
- Siano A, B tale che $A \in \mathcal{D}_x$ e $A \subseteq B \subset I$, allora esiste $Z_A \in \mathcal{D}$ tale che $B \in \mathcal{D}_X$

Per ogni $W \in \mathcal{D}$, prendendo $Z_W = W$ si ha che $Z_W \setminus X = Y \setminus X \subseteq Y$, allora $Y \in \mathcal{D}_X$. Da ciò $\mathcal{D} \subseteq \mathcal{D}_X$.

Prendendo $Z_{I \setminus X} = I$ si ha che $Z_{I \setminus X} \setminus X = I \setminus X \subseteq I \setminus X$ banalmente, quindi $I \setminus X \in \mathcal{D}_X$, che conclude la dimostrazione. □

Teorema 2.30. Per ogni filtro $\mathcal{D}$ su I, esiste un ultrafiltro $\mathcal{U}$ su I con $\mathcal{D} \subseteq \mathcal{U}$.

Dimostrazione. Sia $\mathcal{F} = \{C \text{ filtro di } I \mid \mathcal{D} \subseteq C\}$ insieme ordinato dalla relazione $\subseteq$. Vogliamo mostrare che esiste un elemento massimale per $\mathcal{F}$ applicando il lemma di Zorn. Prendiamo quindi una catena $(\mathcal{C}_\alpha : \alpha < \beta)$ in $\mathcal{F}$ e sia $\mathcal{C} = \bigcup_\alpha \mathcal{C}_\alpha$, mostriamo che $\mathcal{C} \in \mathcal{F}$:

- $\mathcal{C}$ è un filtro:
  - $\forall \alpha,\ \emptyset \notin \mathcal{C}_\alpha$, quindi $\emptyset \notin \mathcal{C}$;
  - $\forall \alpha,\ I \in \mathcal{C}_\alpha$, quindi $I \in \mathcal{C}$;
  - Se $A, B \in \mathcal{C}$, allora $A \in C_\alpha$ e $B \in C_\beta$ per qualche α e β. Allora dato che $(\mathcal{C}_\alpha : \alpha < \beta)$ è linearmente ordinato $A, B \in \mathcal{C}_{\max\{\alpha,\beta\}}$ e $A \cap B \in \mathcal{C}_{\max\{\alpha,\beta\}} \subseteq \mathcal{C}$, cioè $\mathcal{C}$ è chiuso per intersezioni;
  - Se $A \in \mathcal{C}$ e $A \subseteq B \subseteq I$, allora $A \in \mathcal{C}_\alpha$ per qualche α, quindi $B \in \mathcal{C}_\alpha \subseteq \mathcal{C}$.

- $\mathcal{C}$ estende $\mathcal{D}$ perché è unione di filtri che estendono $\mathcal{D}$.

Osservando che $\mathcal{C}$ è un maggiorante della catena perché $\mathcal{C}_\alpha \subseteq \mathcal{C}\ \forall\alpha$, $\mathcal{F}$ rispetta quindi le ipotesi del lemma di Zorn, sia quindi $\mathcal{U}$ l'elemento massimale di $\mathcal{F}$. Mostriamo ora che $\mathcal{U}$ è un ultrafiltro, cioè equivalentemente alla definizione, che se $X \subseteq I$ e $X \notin \mathcal{U}$, allora $I \setminus X \subseteq \mathcal{U}$.

Sia quindi $X \subseteq I$ con $X \notin \mathcal{U}$. Per il Lemma 2.29 possiamo estenderlo a un filtro $\mathcal{U}_X$ su I tale che $\mathcal{U} \subseteq \mathcal{U}_X$ e $I \setminus X \in \mathcal{U}_X$. Dato che $\mathcal{U}_X$ estende $\mathcal{U}$, estende anche $\mathcal{D}$, quindi $\mathcal{U}_X \in \mathcal{F}$, ma $\mathcal{U}$ è un elemento massimale di $\mathcal{F}$, allora $\mathcal{U}_X = \mathcal{U}$. Da ciò segue che $I \setminus X \in \mathcal{U}$, che era quello che volevamo mostrare. □

Osserviamo come nessun ultrafiltro $\mathcal{U}$ su I estenda il filtro di Fréchet è principale, dato che per ogni $j \in I$, $I \setminus \{j\} \in \mathcal{D}_F \subset \mathcal{U}$. Infatti, tutti gli ultrafiltri non principali sono estensioni del filtro di Fréchet:

Lemma 2.31. L'intersezione $\bigcap \mathcal{D}$ di tutti gli ultrafiltri non principali $\mathcal{D}$ su un insieme infinito I è il filtro di Fréchet $\mathcal{D}_F$.

Dimostrazione. Dimostriamo il doppio contenimento per $\mathcal{D}_F = \bigcap \mathcal{D}$:

$\subseteq$: Vogliamo mostrare che per ogni ultrafiltro non principale $\mathcal{D}$, si ha che $\mathcal{D}_F \subset \mathcal{D}$, da cui segue che $\mathcal{D}_F \subset \bigcap \mathcal{D}$. Sia quindi $\mathcal{D}$ un ultrafiltro non principale; per ogni $j \in I$, $\exists X_j \in \mathcal{D}$ tale che $j \notin X_j$ (altrimenti $\mathcal{D}$ sarebbe l'ultrafiltro principale generato da j). Sia $Y_j = I \setminus \{j\}$. Dato che $X_j \subseteq Y_j \subset I$, per definizione di filtro si ha che $Y_j \in \mathcal{D}$. Osserviamo che $\forall A \in \mathcal{D}_F$ si ha $A = I \setminus \{a_i\}_{i=1}^n$ per qualche insieme finito $\{a_i\}_{i=1}^n \subset I$. Allora $A = \bigcap_i^n Y_{a_i} \in \mathcal{D}$. Da cui $\mathcal{D}_F \subset \mathcal{D}$.

$\supseteq$: Per dimostrare il contrario, ci muoviamo per assurdo: sia $A \in \bigcap \mathcal{D}$ con $A \notin \mathcal{D}_F$. Per il Lemma 2.29 possiamo estendere $\mathcal{D}_F$ a un filtro $\mathcal{D}_A$ che contiene $I \setminus A$. Dal Teorema 2.30, possiamo estendere $\mathcal{D}_A$ a un ultrafiltro $\mathcal{U}$ che contiene $I \setminus A$. Questo filtro non è principale, dato che estende $\mathcal{D}_F$. Allora si ha che $I \setminus A \in \mathcal{U} \subset \bigcap \mathcal{D}$, e ciò implica che $A \notin \bigcap \mathcal{D}$. Ciò è assurdo perché va contro la nostra ipotesi iniziale. □

2.5 Ultraprodotti e Teorema di Łoś

Ora che abbiamo gli ultrafiltri a nostra disposizione, siamo pronti per introdurre gli ultraprodotti:

Definizione 2.32. Sia $\{\mathcal{M}_i\}_{i\in I}$ una collezione di $\mathcal{L}$-strutture indicizzate da un insieme infinito I, e sia $\mathcal{D}$ un ultrafiltro su I. Se M_i sono i domini degli $\mathcal{M}_i$, consideriamo il prodotto cartesiano $\prod M_i = \{f : I \to \bigcup M_i \mid \forall i \in I, f(i) \in M_i\}$. Definiamo la relazione $\sim_{\mathcal{D}}$ su $\prod M_i$ data da $f \sim_{\mathcal{D}} g$ se e solo se $\{i \in I \mid f(i) = g(i)\} \in \mathcal{D}$.

Definizione 2.33. Con $\{\mathcal{M}_i\}_{i\in I}$, $\mathcal{D}$, e $\sim_{\mathcal{D}}$ come sopra, l'ultraprodotto $\mathcal{M} = \prod \mathcal{M}_i/\mathcal{D}$ è una $\mathcal{L}$-struttura, definita come segue:

- il dominio di $\mathcal{M}$, denotato $\prod M_i/\mathcal{D}$, è l'insieme delle classi di equivalenza di $\sim_{\mathcal{D}}$ in $\prod M_i$. Denoteremo la classe di equivalenza di $f \in \prod M_i$ con $[f]$ o con $[f(i) \mid i \in I]$;
- Per ogni simbolo di funzione $f \in \mathcal{L}$, la sua interpretazione in $\mathcal{M}$ è:

$$f^{\mathcal{M}}([g_1], \ldots, [g_{n_f}]) = [f^{M_i}(g_1(i), \ldots, g_{n_f}(i)) \mid i \in I]$$

- Per ogni simbolo di relazione $R \in \mathcal{L}$, la sua interpretazione in $\mathcal{M}$ è:

$$([g_1], \ldots, [g_{n_R}]) \in R^{\mathcal{M}} \text{ se e solo se } \{i \in I \mid g_1(i), \ldots, g_{n_R}(i)) \in R^{\mathcal{M}_i}\} \in \mathcal{D}$$

Osservazione 2.34. Per $\mathcal{M}$ come sopra, le interpretazioni $f^{\mathcal{M}}$ e $R^{\mathcal{M}}$ sono ben definite per ogni simbolo di funzione f e di relazione R in $\mathcal{L}$. Mostriamolo:

Sia f un simbolo di funzione. Supponiamo che $\forall\ 1 \leq j \leq n_f$ si ha che $g_j, h_j \in \prod M_i$ con $g_j \sim_{\mathcal{D}} h_j$, cioè che $A_j := \{i \in I \mid g_j(i) = h_j(i)\} \in \mathcal{D}$. Se definiamo $g_f(i) = f^{\mathcal{M}_i}(g_1(i), \ldots, g_{n_f}(i))$ e $h_f(i) = f^{\mathcal{M}_i}(h_1(i), \ldots, h_{n_f}(i))$, il nostro obiettivo è mostrare che $g_f \sim_{\mathcal{D}} h_f$, cioè che $A_f := \{i \in I \mid g_f(i) = h_f(i)\} \in \mathcal{D}$. Banalmente g_f e h_f coincidono in tutti gli $i \in I$ in cui tutti i g_j e h_j sono uguali e ciò lo scriviamo con $\bigcap_{j=1}^{n} Aj \subseteq A_f$ $(\subseteq I)$. Per le proprietà nella definizione di filtro l'intersezione di tutti gli A_j sta in $\mathcal{D}$ e quindi anche A_f.

Sia ora R un simbolo di relazione. Supponiamo di nuovo che $\forall\ 1 \leq j \leq n_f$ si ha che $g_j, h_j \in \prod M_i$ con $g_j \sim_{\mathcal{D}} h_j$, cioè che $A_j := \{i \in I \mid g_j(i) = h_j(i)\} \in \mathcal{D}$. Definendo

$G = \{i \in I \mid (g_1(i), \ldots, g_{n_R}(i)) \in R^{\mathcal{M}_i}\}$ e $H = \{i \in I \mid (h_1(i), \ldots, h_{n_R}) \in R^{\mathcal{M}_i}\}$ vogliamo mostrare che $G \in \mathcal{D}$ se e solo se $H \in \mathcal{D}$. Supponiamo $G \in \mathcal{D}$. Banalmente se $(g_1(i), \ldots, g_{n_R}(i)) \in R^{\mathcal{M}_i}$ e $g_j(i) = h_j(i)\ \forall j$, allora $(h_j(i), \ldots, h_{n_R}(i)) \in R^{\mathcal{M}_i}$ e ciò lo scriviamo con $G \cap \bigcap_{j=1}^{n} A_j \subseteq H$. Ora, per le supposizioni fatte prima e le proprietà della definizione di filtro si ha che $H \in \mathcal{D}$ come volevasi dimostrare. Il verso opposto è analogo.

Il principale motivo per l'introduzione degli ultraprodotti è il teorema seguente, la cui dimostrazione è molto tecnica, che afferma come una formula valga nell'ultraprodotto di una collezione di $\mathcal{L}$-strutture se e solo se vale in "quasi tutte" le strutture della collezione.

Teorema 2.35 (Teorema di Łoś)**.** Sia $\mathcal{M}$ l'ultraprodotto $\prod \mathcal{M}_i/\mathcal{D}$ di $\mathcal{L}$-strutture con ultrafiltro $\mathcal{D}$ sull'insieme degli indici I e sia $\phi(\overline{v})$ una $\mathcal{L}$-formula con $\overline{v} = (v_1, \ldots, v_n)$. Allora se $\overline{[g]} = ([g_1], \ldots, [g_n]) \in (\prod M_i/\mathcal{D})^n$, $\prod M_i/\mathcal{D} \models \phi(\overline{[g]})$ se e solo se $\{i \in I \mid \mathcal{M}_i \models \phi(\overline{g(i)})\} \in \mathcal{D}$.

Dimostrazione. Come prima cosa mostriamo che se $t(\overline{v})$ è un $\mathcal{L}$-termine, allora $t^{\mathcal{M}}(\overline{[g]}) = [t^{\mathcal{M}_i}(\overline{g(i)}) \mid i \in I]$. Dividiamo quindi in casi:

- Se t è un simbolo di costante c, la tesi è vera per definizione: $c^{\mathcal{M}} = [c^{\mathcal{M}_i} \mid i \in I]$.
- se t è una variabile v_j, allora $t^{\mathcal{M}}(\overline{[g]}) = [g_j] = [g_j(i) \mid i \in I] = [t^{\mathcal{M}_i}(\overline{g(i)}) \mid i \in I]$.
- se t è $f(t_1(\overline{v}), \ldots, t_{n_f}(\overline{v}))$, dove f è simbolo di funzione e $t_1, \ldots, t_{n_f}$ sono $\mathcal{L}$-termini per i quali la tesi è vera, allora:

$$\begin{aligned} t^{\mathcal{M}}(\overline{[g]}) &= f^{\mathcal{M}}(t_1^{\mathcal{M}}(\overline{[g]}), \ldots, t_{n_f}^{\mathcal{M}}(\overline{[g]})) \\ &= f^{\mathcal{M}}([t_1^{\mathcal{M}_i}(\overline{g(i)}) \mid i \in I], \ldots, [t_{n_f}^{\mathcal{M}_i}(\overline{g(i)} \mid i \in I]) \text{ per induzione} \\ &= [f^{\mathcal{M}_i}(t_1^{\mathcal{M}_i}(\overline{g(i)}), \ldots, t_{n_f}^{\mathcal{M}_i}(\overline{g(i)})) \mid i \in I] \text{ interpretazione di } f \\ &= [t^{\mathcal{M}_i}(\overline{g(i)}) \mid i \in I]. \end{aligned}$$

Avendo stabilito che i termini si comportano come previsto sotto interpretazione, possiamo passare alla dimostrazione del teorema. Iniziamo con le formule atomiche:

Se $\phi(v)$ è $t_1(v) = t_2(v)$, dove t_1 e t_2 sono $\mathcal{L}$-termini, allora:

$$\begin{aligned}
\mathcal{M} \models \phi([g]) &\iff t_1^{\mathcal{M}}([g]) = t_2^{\mathcal{M}}([g]) \\
&\iff [t_1^{\mathcal{M}_i}(g(i)) \mid i \in I] = [t_2^{\mathcal{M}_i}(g(i)) \mid i \in I] \text{ applicando la tesi} \\
&\iff \{i \in I \mid t_1^{\mathcal{M}_i}(g(i)) = t_2^{\mathcal{M}_i}(g(i))\} \in D \\
&\iff \{i \in I \mid \mathcal{M}_i \models \phi(g(i))\} \in D.
\end{aligned}$$

Se $\phi(v)$ è $R(t_1(v), \ldots, t_{n_R}(v))$, dove R è un simbolo di relazione e $t_1, \ldots, t_{n_R}$ sono $\mathcal{L}$-termini, allora:

$$\begin{aligned}
\mathcal{M} \models \phi([g]) &\iff (t_1^{\mathcal{M}}([g]), \ldots, t_{n_R}^{\mathcal{M}}([g])) \in R^{\mathcal{M}} \\
&\iff ([t_1^{\mathcal{M}_i}(g(i)) \mid i \in I], \ldots, [t_{n_R}^{\mathcal{M}_i}(g(i)) \mid i \in I]) \in R^{\mathcal{M}} \text{ applicando la tesi} \\
&\iff \{i \in I \mid (t_1^{\mathcal{M}_i}(g(i)), \ldots, t_{n_R}^{\mathcal{M}_i}(g(i))) \in R^{\mathcal{M}_i}\} \in D \text{ interpretazione di } R \\
&\iff \{i \in I \mid \mathcal{M}_i \models \phi(g(i))\} \in D.
\end{aligned}$$

Se $\phi(v)$ è $\neg\psi(v)$, dove ψ è una $\mathcal{L}$-formula per la quale la nostra asserzione è vera, allora:

$$\begin{aligned}
\mathcal{M} \models \phi([g]) &\iff \mathcal{M} \not\models \psi([g]) \\
&\iff \{i \in I \mid \mathcal{M}_i \models \psi(g(i))\} \notin D \text{ per induzione} \\
&\iff I \setminus \{i \in I \mid \mathcal{M}_i \models \psi(g(i))\} \in D \text{ poiché } D \text{ è un ultrafiltro} \\
&\iff \{i \in I \mid \mathcal{M}_i \not\models \psi(g(i))\} \in D \\
&\iff \{i \in I \mid \mathcal{M}_i \models \phi(g(i))\} \in D.
\end{aligned}$$

Se $\phi(v)$ è $\psi(v) \wedge \theta(v)$, dove ψ e θ sono $\mathcal{L}$-formule per le quali la nostra asserzione è vera, allora:

$$\begin{aligned}
\mathcal{M} \models \phi([g]) &\iff \mathcal{M} \models \psi([g]) \text{ e } \mathcal{M} \models \theta([g]) \\
&\iff \{i \in I \mid \mathcal{M}_i \models \psi(g(i))\} \in D \text{ e } \{i \in I \mid \mathcal{M}_i \models \theta(g(i))\} \in D, \text{ per induzione.}
\end{aligned}$$

Siano $A = \{i \in I \mid \mathcal{M}_i \models \psi(g(i))\}$ e $B = \{i \in I \mid \mathcal{M}_i \models \theta(g(i))\}$. Se $A \in D$ e $B \in D$, allora $A \cap B \in D$. Viceversa, $A \cap B \subseteq A$ e $A \cap B \subseteq B$, quindi se $A \cap B \in D$,

allora $A \in D$ e $B \in D$. Ora:

$$\begin{aligned} A \cap B \in D &\iff \{i \in I \mid \mathcal{M}_i \models \psi(g(i)) \text{ e } \mathcal{M}_i \models \theta(g(i))\} \in D \\ &\iff \{i \in I \mid \mathcal{M}_i \models \phi(g(i))\} \in D. \end{aligned}$$

Se $\phi(v)$ è $\exists w\, \psi(v, w)$, dove w è una variabile e ψ è una $\mathcal{L}$-formula per la quale la nostra asserzione è vera, allora $\mathcal{M} \models \phi([g])$ se e solo se esiste $[h] \in \prod M_i/D$ tale che $\mathcal{M} \models \psi([g], [h])$, se e solo se (per induzione) esiste $[h]$ tale che $\{i \in I \mid \mathcal{M}_i \models \psi(g(i), h(i))\} \in D$. Siano $A_{[h]} = \{i \in I \mid \mathcal{M}_i \models \psi(g(i), h(i))\}$ e $B = \{i \in I \mid \mathcal{M}_i \models \phi(g(i))\}$. Vorremmo mostrare che esiste $[h]$ tale che $A_{[h]} \in D$ se e solo se $B \in D$.

Supponiamo che esista tale $[h]$. Allora $A_{[h]} \subseteq B$, poiché per $i \in A_{[h]}$, $\mathcal{M}_i \models \psi(g(i), h(i))$, quindi $\mathcal{M}_i \models \phi(g(i))$, dato che $h(i)$ soddisfa il quantificatore esistenziale in $\mathcal{M}_i$. Quindi $B \in D$. Viceversa, supponiamo $B \in D$. Sia $h \in \prod M_i$ tale che per ogni $i \in B$, $h(i) \in M_i$ è un elemento che soddisfa il quantificatore esistenziale, e per $i \notin B$, $h(i)$ è un elemento arbitrario. Allora $B \subseteq A_{[h]}$, quindi $A_{[h]} \in D$.

Questo completa la dimostrazione per induzione sulle formule. Non è necessario considerare formule costruite usando $\vee$ o $\forall$, poiché queste possono essere riscritte per usare solo $\neg, \wedge$ e $\exists$. □

Il Teorema di Łoś è prettamente semantico perché riguarda la verità nelle strutture. Esso afferma che una proprietà è vera in un ultraprodotto se e solo se è "frequentemente" vera nelle strutture componenti (cioè se l'insieme degli indici per cui vale appartiene all'ultrafiltro). Osserviamo invece che il Teorema di Compattezza (vedi Teorema 2.15) è "sintattico" perché si basa sulla coerenza interna delle formule. Il primo fornisce il modo algebrico per costruire i modelli che il secondo promette esistano.

Corollario 2.36. Se $\mathcal{K}$ è una classe elementare di $\mathcal{L}$-strutture e $\{M_i\}_{i \in I}$ è una collezione di $\mathcal{L}$-strutture in $\mathcal{K}$ indicizzate da un insieme infinito I, allora per ogni ultrafiltro $\mathcal{D}$ su I, $\prod \mathcal{M}_i/\mathcal{D}$ è in $\mathcal{K}$.

Dimostrazione. Sia T un insieme di assiomi per $\mathcal{K}$. Per ogni $\phi \in T, \{i \in I \mid \mathcal{M}_i \models \phi\} = I$, dato che $\mathcal{M}_i \in \mathcal{K}$ per ogni $i \in I$. Ora $I \in \mathcal{D}$, allora $\prod \mathcal{M}_i/\mathcal{D} \models \phi$ per il teorema di Łoś. Così $\prod \mathcal{M}_i/\mathcal{D} \models T$, e $\prod \mathcal{M}_i/\mathcal{D}$ è nella classe $\mathcal{K}$. □

Esempio 2.37. Sia $\mathcal{D}$ un ultrafiltro non principale sull'insieme di tutti i primi P. Per il Corollario 2.36, considerando $\mathcal{K}$ la classe elementare dei campi valutati con *cross section* (per l'Esempio 2.10), $\prod \mathbb{F}_p/\mathcal{D}$ e $\prod \mathbb{Q}_p$ sono campi valutati con *cross section*. Inoltre, $\prod \mathbb{Q}_p/\mathcal{D}$ ha caratteristica zero per il teorema di Łoś, dato che $\mathbb{Q}_p \models \mathrm{Char}_0$ per ogni primo p.

Studiamo invece la caratteristica di $\prod \mathbb{F}_p((t))/\mathcal{D}$. Per ogni primo p, $\mathbb{F}_q((t)) \models \mathrm{Char}_p$ se e solo se q=p, quindi $\{q \in P \mid \mathbb{F}_q((t)) \models \mathrm{Char}_p\} = \{p\}$. Questo è un insieme finito, quindi il suo complementare è nel filtro di Fréchet $\mathcal{D}_F$ su P. Ma per il Lemma 2.31 $\mathcal{D}$ contiene $\mathcal{D}_F$, quindi $P \setminus \{p\} \in \mathcal{D}$, cioè $\{p\} \notin \mathcal{D}$. Allora per il teorema di Łoś $\prod \mathbb{F}_p((t))/\mathcal{D} \models \neg\mathrm{Char}_p$ per tutti i $p \in P$, cioè $\prod \mathbb{F}_p((t))/\mathcal{D}$ ha caratteristica zero.

Lemma 2.38. Per ogni ultrafiltro non principale $\mathcal{D}$, vale che:

- $v((\prod \mathbb{Q}_p/\mathcal{D})^*) \cong \prod \mathbb{Z}/\mathcal{D} \cong v((\prod \mathbb{F}_p((t))/\mathcal{D})^*)$, cioè i gruppi di valutazioni sono isomorfi (come gurppi);
- $\overline{\prod \mathbb{Q}_p/\mathcal{D}} \cong \prod \mathbb{F}_p/\mathcal{D} \cong \overline{\prod \mathbb{F}_p((t))/\mathcal{D}}$, cioè i campi delle classi residuo sono isomorfi (come campi);
- $\mathrm{Char}(\prod \mathbb{F}_p/\mathcal{D}) = 0$.

Dimostrazione. Sia $\mathcal{M} = \prod \mathbb{Q}_p/\mathcal{D}$ e sia $[f] \in M$, il dominio di $\mathcal{M}$, con $[f] \neq 0$, che equivale a $f \not\sim_{\mathcal{D}} 0$, cioè $\{p \in P \mid f(p) = 0\} \in \mathcal{D}$ e dato che $\mathcal{D}$ è un ultrafiltro vi è il suo complementare, cioè $A := \{p \in P \mid f(p) \neq 0\} \in \mathcal{D}$. Definiamo allora $g \in \prod M_i$ con $g(p) := f(p)$ se $p \in A$ e $g(p) = 1$ se $p \notin A$. Allora $A \subseteq \{p \in P \mid g(p) = f(p)\}$, da cui $g \sim_{\mathcal{D}} f$. Abbiamo quindi mostrato che per ogni $f \in M$ con $[f] \neq 0$ esiste un rappresentante $[g] = [f]$ con $g(p) \neq 0$ per ogni p. Per definizione di ultraprodotto, $v^{\mathcal{M}}([f]) = [v^{\mathbb{Q}_p}(g(p)) \mid p \in P] = [p^{n_p} \mid p \in P]$ per qualche intero n_p poiché $g(p) \neq 0$. Il gruppo dei valori $v^{\mathcal{M}}(M)$ è quindi composto di classi di equivalenza di questa forma. Sia $\phi : v((\prod \mathbb{Q}_p/\mathcal{D})^*) \to \prod \mathbb{Z}/\mathcal{D}$ data da $\phi([p^{n_p} \mid p \in P]) = [n_p \mid p \in P] \in \prod \mathbb{Z}/\mathcal{D}$. Si mostra facilmente che ϕ è un isomorfismo di gruppi. Si può costruire un isomorfismo analogo per $v((\prod \mathbb{F}_p((t))/\mathcal{D})^*) \cong \prod \mathbb{Z}/\mathcal{D}$, con la differenza che $v((\prod \mathbb{F}_p((t))/\mathcal{D})^*)$ è composto da classi di equivalenza del tipo $[t^{n_p} \mid p \in P]$, con n_p intero. Ciò conclude il primo asserto.

Dati $\mathcal{O} = \mathcal{O}_{\mathcal{M}}$ e I_1, consideriamo $\overline{\mathcal{M}} = \mathcal{O}/I_1 = \mathcal{O}/\{[f] \in O \mid \mathcal{M} \models (1 < v([f]))\}$ e tale insieme per il teorema di Łoś è uguale a $\mathcal{O}/\{[f] \in \mathcal{O} \mid \{p \mid \mathbb{Q}_p \models (1 < v(f(p)))\} \in \mathcal{D}\}$. Mostriamo che l'insieme $R = \{[g] \in \mathcal{O} \mid \forall p \in P, g(p) \in \{0, 1, \ldots, p-1\}\}$ è un insieme completo di rappresentanti per il campo dei residui. Ogni classe di equivalenza $\mod I_1$ ha un rappresentante in R, preso infatti un qualsiasi rappresentante f di una classe e riducendo ogni coordinata $f(p) \mod p$ a un elemento in $\{0, 1, \ldots, p-1\}$ si costruisce una funzione in R che è equivalente ad $[f] \mod p$. Vediamo ora sia minimale prendendo per assurdo due elementi $[g], [h] \in R$, con $[g] \neq [h]$ e $[g] \equiv [h] \mod I_1$. Da tali ipotesi segue che $\{p \mid g(p) \neq g(p)\} \in \mathcal{D}$, e che $[g] + [f] = [h]$ per qualche $[f] \in I_1$. $[f] \in I_1$ equivale a $\{p \mid \mathbb{Q}_p \models (1 < v(f(p)))\} \in \mathcal{D}$. Ora dato che $g(p) \neq h(p)$ ed entrambi sono presi dall'insieme $\{0, 1, \ldots, p-1\}$ la loro differenza $g(p) - h(p)$ non può essere divisibile per p, in particolare $g(p) - h(p) \neq f(p)$ se $v(f(p)) > 1$. Ciò si può scrivere tramite l'inclusione

$$\{p \mid \mathbb{Q}_p \models (1 < v(f(p))\} \cap \{p \mid g(p) \neq h(p)\} \subseteq \{p \mid g(p) + f(p) \neq h(p)\}$$

e per le proprietà della definizione di ultrafiltro, siccome il primo membro di questa inclusione sta in $\mathcal{D}$, vi sta anche il secondo e quindi $g + f \not\sim_{\mathcal{D}} h$, che è una contraddizione.

Ogni elemento $[f] \in \overline{\mathcal{M}}$ ha quindi un unico rappresentante $[g]$ in R, cioè R è un insieme completo di rappresentanti per le classi $\mod I_1$. Immergendo ogni elemento $[g] \in R$ come un elemento di $\prod \mathbb{F}_p/\mathcal{D}$, è facile verificare come la mappa risultante da $\overline{\mathcal{M}}$ a $\prod \mathbb{F}_p/\mathcal{D}$ sia un isomorfismo di campi. Ripetendo lo stesso procedimento a $\prod \mathbb{F}_p((t))/\mathcal{D}$, considerando però che la differenza che tra due diversi $g(p)$ e $h(p)$ in $\{0, 1, \ldots, p-1\}$ non può essere divisibile per t, segue il secondo asserto dell'enunciato.

Infine, la classe residuo ha caratteristica zero per un argomento analogo all'Esempio 2.37: $\mathbb{F}_q \models \mathrm{Char}_p$ solo quando $q = p$, allora $\prod \mathbb{F}_p/\mathcal{D} \models \neg\mathrm{Char}_p$ per ogni p, da cui per il teorema di Łoś segue che $\mathrm{Char}(\prod \mathbb{F}_p/\mathcal{D}) = 0$. □

Grazie a tali teoremi è ora possibile enunciare un risultato fondamentale per la dimostrazione del principio di Ax-Kochen:

Teorema 2.39. Sia $\{\mathcal{M}_i\}_{i \in I}$ e $\{\mathcal{N}_i\}_{i \in I}$ collezioni di $\mathcal{L}$-strutture indicizzate dallo stesso insieme infinito I. Supponiamo che per ogni ultrafiltro non principale $\mathcal{D}$ vale che $\prod \mathcal{M}_i/\mathcal{D} \equiv \prod \mathcal{N}_i/\mathcal{D}$. Allora per ogni $\mathcal{L}$-sentenza ϕ, $\mathcal{M}_i \models \phi$ per tutti gli i eccetto un numero finito se e solo se $\mathcal{N}_i \models \phi$ per tutti gli i eccetto un numero finito.

Dimostrazione. Supponiamo che $\mathcal{M}_i \models \phi$ per tutti gli i tranne un numero finito. Allora $A = \{i \in I \mid \mathcal{M}_i \models \phi\} \in \mathcal{D}_F$, il filtro di Fréchet su I. Per il Lemma 2.31 $A \in \mathcal{D}$ per ogni ultrafiltro non principale $\mathcal{D}$. Per il teorema di Łoś $\prod \mathcal{M}_i/\mathcal{D} \models \phi$ e per ipotesi di equivalenza elementare vale analogamente che $\prod \mathcal{N}_i/\mathcal{D} \models \phi$. Ora, per l'altro verso del teorema di Łoś vale che $B = \{i \in I \mid \mathcal{N}_i \models \phi\} \in \mathcal{D}$ per tutti gli ultrafiltri non principali $\mathcal{D}$, allora $B \in \bigcap \mathcal{D} = \mathcal{D}_F$ sempre per il Lemma 2.31. Allora $\mathcal{N}_i \models \phi$ per tutti gli i eccetto un numero finito. Il viceversa segue simmetricamente. □

Per il Teorema 2.39 il principio di Ax-Kochen è provato se riusciamo a dimostrare l'equivalenza elementare degli ultraprodotti $\prod \mathbb{F}_p((t))/\mathcal{D}$ e $\prod \mathbb{Q}_p/\mathcal{D}$ per ogni ultrafiltro principale $\mathcal{D}$ sull'insieme di tutti i primi P. Per farlo ci serviranno però nuove nozioni come quella di n-tipo e di modello saturato, che introduciamo nella prossima sezione. Tali strumenti ci serviranno per scavare in profondità nelle proprietà algebriche di $\mathbb{F}_p((t))$ e $\mathbb{Q}_p$.

2.6 Cenni di Tipi e Modelli saturati

Definizione 2.40. Sia $\mathcal{M}$ una $\mathcal{L}$-struttura con dominio M. Dato $A \subseteq M$, definiamo $\mathcal{L}_A = \mathcal{L} \cup \{c_a \mid a \in A\}$, dove c_a è nuovo simbolo di costante. Possiamo vedere $\mathcal{M}$ come una $\mathcal{L}_A$-struttura interpretando $c_a^{\mathcal{M}} = a$ per ogni nuovo simbolo di costante.

Espandendo il linguaggio in questo modo possiamo scrivere sentenze che si riferiscono a elementi di $A \subseteq M$. Considereremo $\mathrm{Th}_A(\mathcal{M}) = \{\phi \mid \phi$ è una $\mathcal{L}_A$-sentenza, e $\mathcal{M} \models \phi\}$.

Definizione 2.41. Data una $\mathcal{L}$-struttura $\mathcal{M}$ con dominio M e un sottoinsieme $A \in M$, un n-tipo su A è un insieme P di $\mathcal{L}_A$-formule con variabili libere $v_1 \ldots, v_n$ tale che $\mathrm{Th}_A(\mathcal{M}) \cup P$ è soddisfacibile (secondo la Definizione 2.7). Se per ogni $\mathcal{L}_A$-formula ϕ in variabili libere $v_1, \ldots, v_n$ si ha che $\phi \in P$ oppure che $\neg\phi \in P$, allora P è detto completo.

La condizione di soddisfacibilità significa che esiste una $\mathcal{N}$ con dominio N che è un modello di $\mathrm{Th}_A(\mathcal{M})$, ed esistono $b_1, \ldots, b_n \in N$ tale che $\mathcal{N} \models \phi(b_1, \ldots, b_n)$ per ogni $\phi \in P$. Diciamo che se ciò accade gli elementi $b_1, \ldots, b_n$ realizzano P in $\mathcal{N}$. Se invece un insieme P' di $\mathcal{L}_A$-formule non è realizzato in $\mathcal{N}$ diciamo che $\mathcal{N}$ omette il tipo P'.

Esempio 2.42. Mostriamo alcuni esempi di tipi:

1. L'elemento $\sqrt{2}$ nel campo $\mathbb{C}$ dei complessi, considerato come struttura nel linguaggio $\mathcal{L} = \{0, 1, +, \cdot\}$ realizza il tipo $x^2 = 2$ (con le ovvie definizioni $x^2 = x \cdot x$ e $2 = 1 + 1$). Osserviamo come anche l'elemento $-\sqrt{2}$ realizza la stessa formula ed esiste infatti un automorfismo di $\mathbb{C}$ che manda $\sqrt{2}$ in $-\sqrt{2}$.

2. In $(\mathbb{Q}, +, <)$ vi sono solo tre "tipi" di elementi: positivi, negativi e zero. Ad esempio 2 e 3 soddisfano le stesse formule in questo linguaggio ed esiste infatti l'automorfismo $x \to \frac{3}{2}x$ che manda 2 in 3.

Da questi esempi è possibile intuire come questa nozione di n-tipo possa essere utile per mostrare isomorfismi.

Da qui in poi utilizzeremo la nozione di cardinale come un concetto già assimilato dal lettore. Il motivo del loro utilizzo è che la "difficoltà" dell'esistenza di un modello che realizza un tipo su A dipende dalla taglia dell'insieme A.

Definizione 2.43. Sia T una teoria completa con infiniti modelli in un linguaggio numerabile $\mathcal{L}$ e sia κ un cardinale infinito. Un modello $\mathcal{M} \models T$ con dominio M è detto κ-saturato se per ogni $A \subset M$ con $|A| < \kappa$, ogni tipo su A è realizzato in $\mathcal{M}$.

Esempio 2.44. $(\mathbb{R}, 0, 1, +, \cdot, <)$ non è ω-saturo in quanto non realizza il tipo $p(y) = \{n < y \mid n \in \mathbb{N}\}$, in quanto non esiste un elemento in $\mathbb{R}$ maggiore di ogni naturale.

La proprietà di essere saturato si mostrerà infatti fondamentale per trovare isomorfismi; vale infatti che:

Teorema 2.45. Se $\mathcal{M}$ e $\mathcal{N}$ sono modelli saturati di una teoria completa T, è hanno la stessa cardinalità κ, allora $\mathcal{M} \cong \mathcal{N}$.

Ora che l'utilità dei modelli saturati per mostrare isomorfismi è chiara, ci interessiamo alla loro esistenza, i prossimi teoremi ci informano quindi a tale proposito.

Teorema 2.46. Sia $\mathcal{L}$ un linguaggio numerabile e sia $\mathcal{M}$ una $\mathcal{L}$-struttura con dominio infinito M. Sia inoltre κ un cardinale infinito. Allora esiste una estensione elementare $\mathcal{N}$ di $\mathcal{M}$ con dominio N tale che $|N| \leq |M|^\kappa$, con $\mathcal{N}$ κ^+-saturato.

Teorema 2.47. Se assumiamo l'ipotesi del continuo ($2^{\aleph_0} = \aleph_1$), esiste un modello saturato di $\mathrm{Th}(\mathcal{M})$ con cardinalità $\aleph_1$.

L'importanza del primo teorema risiede nella capacità di espandere un modello arbitrario in una struttura "logicamente ricca" senza perdere le proprietà del primo ordine (grazie all'estensione elementare). Ci dice che, per quanto un modello iniziale possa essere povero di tipi realizzati, esiste sempre una sua estensione in cui ogni descrizione coerente di un elemento trova un riscontro reale. È lo strumento che permette di costruire i cosiddetti Modelli Mostro, strutture in cui ogni tipo "abbastanza piccolo" è già realizzato al suo interno.

Il secondo teorema sotto l'Ipotesi del Continuo mostra come la saturazione non è più solo una proprietà asintotica, ma diventa una caratteristica concreta di modelli di cardinalità accessibili ($\aleph_1$).

Capitolo 3

Soluzione asintotica della Congettura di Artin

Giunti all'ultimo capitolo della tesi siamo ora capaci di, dopo aver riassunto quanto provato precedentemente, enunciare e dimostrare il teorema di Ax-Kochen. Ci manca però un'ultima nozione che è quella di campo Henseliano, la cui definizione e utilità è spiegata nella prossima sezione.

3.1 Il Lemma di Hensel

Uno dei nostri strumenti chiave per stabilire il Principio di Ax-Kochen è il lemma di Hensel. Nei campi valutati in cui vale il lemma di Hensel, è possibile trarre informazioni sui polinomi definiti sull'anello di valutazione studiando i polinomi definiti sul campo residuo.

Definizione 3.1. Sia F un campo valutato. Diciamo che F è Henseliano se F possiede la seguente proprietà, che è una delle formulazioni del Lemma di Hensel:

> Siano $f, g_0, h_0 \in \mathcal{O}[x]$ polinomi monici. Se le immagini di g_0 e h_0 nel campo residuo $\overline{F}[x]$, denotate con $\overline{g}_0$ e $\overline{h}_0$, sono coprime, e se $\overline{g}_0\overline{h}_0 = \overline{f}$, allora esistono $g, h \in \mathcal{O}[x]$ tali che $\overline{g} = \overline{g_0}$, $\overline{h} = \overline{h}_0$ e $f = gh$.

Tale proprietà è utilizzata in teoria dei numeri per la fattorizzazione di un polinomio. Ci dice che se il polinomio ridotto nel campo residuo si spezza in due fattori coprimi

$(\overline{g}_0 \cdot \overline{h}_0)$, allora l'intero polinomio originale si spezza in due fattori $(g \cdot h)$ che "sollevano" quelli del campo residuo.

Esempio 3.2. Vediamo un esempio di applicazione del lemma. Prendiamo come F il campo valutato $\mathbb{Q}_7$ con valutazione v_7 (che vedremo essere Henseliano), con $\overline{\mathbb{Q}}_7 = \mathbb{F}_7$ e $\mathcal{O}_{\mathbb{Q}_7} = \mathbb{Z}_7$. Consideriamo il polinomio $f(x) = x^2 - 2$. Vogliamo vedere se possiamo spezzarlo nel prodotto di due polinomi di primo grado, ovvero se 2 ha una radice quadrata in $\mathbb{Q}_7$. Passaggio al campo residuo ($\mathbb{F}_7$): Riduciamo i coefficienti di $f(x)$ modulo 7. Otteniamo:

$$\overline{f}(x) = x^2 - 2 \pmod 7$$

In $\mathbb{F}_7$, notiamo che $3^2 = 9 \equiv 2$ e $4^2 = 16 \equiv 2$. Quindi:

$$\overline{f}(x) = (x-3)(x-4) \in \mathbb{F}_7[x]$$

Verifica delle ipotesi della definizione di Henseliano: poniamo $\overline{g}_0 = (x-3)$ e $\overline{h}_0 = (x-4)$.

- $\overline{g}_0$ e $\overline{h}_0$ sono coprimi: sì, perché hanno radici distinte (3 e 4) in $\mathbb{F}_7$.
- $\overline{g}_0\overline{h}_0 = \overline{f}$: sì, per costruzione.

Poiché $\mathbb{Q}_7$ è un campo Henseliano, la definizione garantisce che esistano due polinomi $g, h \in \mathbb{Z}_7[x]$ tali che:$f = gh$ (ovvero $x^2 - 2$ si fattorizza esattamente in $\mathbb{Q}_7$). Questo ci dice che esistono due numeri 7-adici, chiamiamoli α e $-\alpha$ in $\mathbb{Z}_7$, che sono le radici di $x^2 - 2$. Sappiamo inoltre che questi numeri, se scritti come sviluppo 7-adico, inizieranno rispettivamente con le cifre 3 e 4 (perchè riducendo modulo 7 dobbiamo ritrovare le radici di $\overline{g}_0$ e di $\overline{h}_0$:

$$\alpha = 3 + c_1 \cdot 7 + c_2 \cdot 7^2 + \cdots$$

$$-\alpha = 4 + d_1 \cdot 7 + d_2 \cdot 7^2 + \cdots$$

Ora dopo aver capito l'utilità di tale lemma, è importante che i nostri campi di interessa lo soddisfino. Tramite strumenti algebrici come il risultante di due polinomi e la definizione di completezza per i campi con valutazione discreta è possibile dimostrare il seguente teorema, che sarà utile ai nostri fini.

Teorema 3.3. Tutti i campi con valutazione discreta completi sono Henseliani.

Corollario 3.4. I campi $\mathbb{Q}_p$ e $\mathbb{F}_p((t))$, sono Henseliani.

Nell'Esempio 2.37 usando il Corollario 2.36 abbiamo mostrato come per ogni ultrafiltro non principale $\mathcal{D}$, $\prod \mathbb{Q}_p/\mathcal{D}$ e $\prod \mathbb{F}_p/\mathcal{D}$ sono campi con valutazioni con *cross section*. Facciamo quindi lo stesso ragionamento per i campi Henseliani grazie al prossimo lemma.

Lemma 3.5. La classe dei campi con valutazione Henseliani con *cross section* è elementare.

Con i Corollari 2.36 e 3.4, il Lemma 3.5 mostra che per ogni ultrafiltro $\mathcal{D}$, $\prod \mathbb{Q}_p/\mathcal{D}$ e $\prod \mathbb{F}_p((t))/\mathcal{D}$ sono Henseliani. Ciò si rivelerà molto utile: nel Lemma 2.38 abbiamo mostrato l'equivalenza tra i campi residui e gli anelli di valutazioni degli ultraprodotti. Dato che i campi Henseliani hanno la proprietà di ottenere informazioni sulle soluzioni di polinomi nel campo proprio attraverso le loro soluzioni proprio nelle strutture che accomunano gli ultraprodotti, tale proprietà ci servirà per costruire il ponte logico tra il campo più "difficile" da manipolare, il campo dei numeri p-adici $\mathbb{Q}_p$, e il campo più trattabile, il campo delle serie formali di Laurent $\mathbb{F}_p((t))$.

3.2 Il principio di Ax-Kochen

Siamo ora in grado di provare gli ultimi teoremi per risolvere la congettura di Artin. Abbiamo visto nel Teorema 2.39 che è sufficiente provare l'equivalenza elementare degli ultraprodotti $\prod \mathbb{Q}_p/\mathcal{D}$ e $\prod \mathbb{F}_p/\mathcal{D}$ per ogni ultrafiltro non principale $\mathcal{D}$ e per ogni insieme di primi P.

Mostriamo ora con due tabelle cosa differenzia e accomuna rispettivamente i due campi $\mathbb{F}_p((t))$ e $\mathbb{Q}_p$ e i due ultraprodotti $\prod \mathbb{F}_p((t))/\mathcal{D}$ e $\prod \mathbb{Q}_p/\mathcal{D}$:

Proprietà	Campo delle serie di potenze $\mathbb{F}_p((t))$	Campo dei numeri p-adici $\mathbb{Q}_p$
Caratteristica	p	0
Algebra dei polinomi	C_2	?
Campo Residuo	$\mathbb{F}_p$	$\mathbb{F}_p$
Gruppo dei valori	$\mathbb{Z}$	$\mathbb{Z}$
È Henseliano?	Sì	Sì

Il campo delle serie di potenze è C_2 per quanto dimostrato nel primo capitolo con il Teorema di Lang 1.29, mentre il fatto che anche Q_p lo sia era solo stato congetturato da Artin. La differenza algebrica tra le caratteristiche di questi campi ci è costato il passaggio agli ultraprodotti, riportiamo quindi in una tabella i risultati trovati nel Lemma 2.38:

Proprietà	Ultraprodotto di serie di potenze $\prod \mathbb{F}_p((t))/\mathcal{D}$	Ultraprodotto di numeri p-adici $\prod \mathbb{Q}_p/\mathcal{D}$
Caratteristica	0	0
Campo Residuo	$\prod \mathbb{F}_p/\mathcal{D}$	$\prod \mathbb{F}_p/\mathcal{D}$
Caratteristica residua	0	0
Gruppo dei valori	$\prod \mathbb{Z}/\mathcal{D}$	$\prod \mathbb{Z}/\mathcal{D}$
È Henseliano?	Sì	Sì

Le uguaglianze tra le proprietà degli ultraprodotti sono proprio le ipotesi del prossimo teorema:

Teorema 3.6. Supponiamo che F e G sono campi con valutazione Henseliani con valutazioni rispettivamente v_F e v_G tale che:

- $v_F(F^*) \equiv v_G(G^*)$ (come $\mathcal{L}_G$-strutture);
- $\overline{F} \equiv \overline{G}$ (come $\mathcal{L}_F$-strutture);
- $\mathrm{Char}(\overline{F}) = \mathrm{Char}(\overline{G}) = 0$

Allora $F \equiv G$.

In questa tesi si è scelto di omettere la trattazione dettagliata dei tipi, della saturazione dei modelli e dell'Ipotesi del Continuo. Sebbene tali strumenti siano fondamentali per dimostrare il Teorema 3.6, essi appartengono più alla logica pura che all'applicazione algebrica del teorema. Per gli scopi di questa tesi, si è scelto di adottare un approccio funzionale alla Teoria dei Modelli, privilegiando la sua importanza algebrica del risultato rispetto alla sua struttura logica più astratta.

Osservazione 3.7. Applicando il Teorema 3.6 ai campi con valutazione Henseliani $F = \prod \mathbb{F}_p((t))/\mathcal{D}$ e $G = \prod \mathbb{Q}_p/\mathcal{D}$ segue che essi sono effettivamente elementarmente equivalenti come volevamo dimostrare. Passare dallo studio dei campi $\mathbb{Q}_p$, $\mathbb{F}_p$ allo studio degli ultraprodotti è stato fondamentale per oltrepassare l'ostacolo algebrico, ma riportando le proprietà della logica del primo ordine ai campi iniziali si perdono però le proprietà che avevano tutti i $\mathbb{F}_p$ (come quella di essere C_2 per ogni p). Infatti mostreremo come tali proprietà varranno per $\mathbb{Q}_p$ solo per un numero finito di p:

Teorema 3.8 (Principio di Ax-Kochen)**.** Sia ϕ una $\mathcal{L}_{VF}$-sentenza. Allora $\mathbb{Q}_p \models \phi$ per tutti i primi p tranne un numero finito se e solo se $\mathbb{F}_p((t)) \models \phi$ per tutti i primi p tranne un numero finito.

Dimostrazione. La classe dei campi valutati Henseliani è elementare per il Lemma 3.5 e quindi chiusa rispetto agli ultraprodotti per il Corollario 2.36. Per ogni p, $\mathbb{Q}_p$ e $\mathbb{F}_p((t))$ sono campi valutati Henseliani per il Corollario 3.4. Pertanto, per ogni ultrafiltro $\mathcal{D}$ sull'insieme dei numeri primi, $\prod \mathbb{Q}_p/\mathcal{D}$ e $\prod \mathbb{F}_p((t))/\mathcal{D}$ sono campi valutati Henseliani.

Nel Lemma 2.38 abbiamo visto che per ogni ultrafiltro non principale $\mathcal{D}$, i campi residui $\overline{\prod \mathbb{Q}_p/D}$ e $\overline{\prod \mathbb{F}_p((t))/D}$ hanno caratteristica zero. Abbiamo anche mostrato che $v(\prod \mathbb{Q}_p/D) \cong \prod \mathbb{Z}/D \cong v(\prod \mathbb{F}_p((t))/D)$ e $\overline{\prod \mathbb{Q}_p/D} \cong \prod \mathbb{F}_p/D \cong \overline{\prod \mathbb{F}_p((t))/D}$. Per il Teorema 2.24, l'isomorfismo implica l'equivalenza elementare, quindi questi campi valutati Henseliani hanno gruppi dei valori e campi residui elementarmente equivalenti. Queste sono le condizioni del Teorema 3.6, pertanto:

$$\prod \mathbb{Q}_p/D \equiv \prod \mathbb{F}_p((t))/D$$

Poiché l'equivalenza elementare vale per ogni ultrafiltro non principale, l'applicazione del Teorema 2.39 completa la dimostrazione. □

Ora che abbiamo il Principio di Ax-Kochen ci basterebbe mostrare che la proprietà C_2 è elementare per provare che $\mathbb{Q}_p$ è C_2 per tutti i p eccetto un numero finito. Purtroppo non è possibile esprimere tale proprietà come una $\mathcal{L}$-sentenza perché non possiamo quantificare polinomi di ogni grado. Tuttavia se fissiamo il grado d possiamo esprimere una proprietà equivalente a $C_2(d)$ come una $\mathcal{L}_{VF}$-sentenza e quindi poter applicare il

principio di Ax-Kochen per provare che $\mathbb{Q}_p$ è $C_2(d)$ per tutti i p eccetto un numero finito. È da notare come l'insieme dei p per i quali $\mathbb{Q}_p$ non è $C_2(d)$ dipende dal grado d.

Teorema 3.9. Per ogni grado $d > 0$, esiste un insieme finito di numeri primi $P(d)$ tale che per tutti i $p \notin P(d)$, se f è un polinomio omogeneo su $\mathbb{Q}_p$ di grado d in n variabili con $n > d^2$, allora f ha uno zero non banale in $\mathbb{Q}_p^n$.

Dimostrazione. Sia $C_2(d)$ la proprietà che ogni polinomio omogeneo di grado d in n variabili tale che $n > d^2$ abbia uno zero non banale.

Mostriamo innanzitutto che $C_2(d)$ è equivalente alla proprietà che ogni polinomio omogeneo di grado d in precisamente $d^2 + 1$ variabili abbia uno zero non banale. Chiameremo questa proprietà ϕ_d. Chiaramente $C_2(d)$ implica ϕ_d. Viceversa, se $f(x_1, \dots, x_n)$ è un polinomio omogeneo di grado d con $n > d^2$, allora ponendo le variabili extra uguali a 0, $g(x_1, \dots, x_{d^2+1}) = f(x_1, \dots, x_{d^2+1}, 0, \dots, 0)$ è il polinomio nullo oppure un polinomio omogeneo di grado d in $d^2 + 1$ variabili. Nel primo caso, ogni scelta non banale di valori per $x_1, \dots, x_{d^2+1}$ è uno zero non banale di f. Nel secondo caso, se vale ϕ_d, allora g ha uno zero non banale $(\alpha_1, \dots, \alpha_{d^2+1})$, dunque $(\alpha_1, \dots, \alpha_{d^2+1}, 0, \dots, 0)$ è uno zero non banale di f.

Desideriamo esprimere la proprietà ϕ_d come una $\mathcal{L}_{VF}$-sentenza per poter applicare il Principio di Ax-Kochen. Per fare ciò, dobbiamo quantificare su tutti i possibili polinomi omogenei di grado d in $d^2 + 1$ variabili. Ogni monomio di un tale polinomio ha grado d, quindi corrisponde a una scelta di d^2+1 esponenti $n_1, \dots, n_{d^2+1} \in \mathbb{N}$ per le d^2+1 variabili, tali che $\sum_{i=1}^{d^2+1} n_i = d$. Sia $\theta(d)$ il numero totale di tali scelte; possiamo enumerare tutti i monomi possibili come $m_1, \dots, m_{\theta(d)}$. Allora ogni polinomio omogeneo di grado d in d^2+1 variabili è univocamente determinato da una scelta di $\theta(d)$ coefficienti $a_1, \dots, a_{\theta(d)}$, uno per ogni m_i, tali che almeno uno dei coefficienti sia non nullo.

Se m_i è il monomio $x_1^{n_1} \dots x_{d^2+1}^{n_{d^2+1}}$, definiamo il $\mathcal{L}_{VF}$-termine $m_i(x_1, \dots, x_{d^2+1})$ nelle variabili libere $(x_1, \dots, x_{d^2+1})$ come:

$$\underbrace{x_1 \cdot \dots \cdot x_1}_{n_1 \text{ volte}} \cdot \dots \cdot \underbrace{x_{d^2+1} \cdot \dots \cdot x_{d^2+1}}_{n_{d^2+1} \text{ volte}}$$

Useremo le variabili a_i e x_i per chiarezza. Formalmente, esse sono scelte di v_j dal nostro insieme infinito di variabili $V = \{v_1, v_2, \dots\}$. Possiamo esprimere la proprietà ϕ_d con la seguente $\mathcal{L}_{VF}$-sentenza:

$$\forall a_1 \ldots \forall a_{\theta(d)} \neg((a_1 = 0) \wedge \cdots \wedge (a_{\theta(d)} = 0)) \rightarrow$$
$$(\exists x_1 \ldots \exists x_{d^2+1} \neg((x_1 = 0) \wedge \cdots \wedge (x_{d^2+1} = 0)) \wedge$$
$$(a_1 \cdot m_1(x_1, \ldots, x_{d^2+1}) + \cdots$$
$$+ a_{\theta(d)} \cdot m_{\theta(d)}(x_1, \ldots, x_{d^2+1}) = 0)).$$

Ora, per un campo valutato F, $F \models \phi_d$ se e solo se F ha la proprietà $C_2(d)$. Per il Teorema 1.29, $\mathbb{F}_p((t))$ è C_2, e quindi ha la proprietà $C_2(d)$ per ogni numero primo p. Pertanto, per ogni primo p, $\mathbb{F}_p((t)) \models \phi_d$.

Applicando il Principio di Ax-Kochen, $\mathbb{Q}_p \models \phi_d$ per tutti i primi p tranne al più un numero finito, e dunque $\mathbb{Q}_p$ ha la proprietà $C_2(d)$ per quasi tutti i p. Sia $P(d)$ questo insieme eccezionale finito. Allora per ogni $p \notin P(d)$, $C_2(d)$ afferma che se f è un polinomio omogeneo su $\mathbb{Q}_p$ di grado d in n variabili con $n > d^2$, allora f ha uno zero non banale in $\mathbb{Q}_p^n$. □

Con questo teorema Ax e Kochen "dimostrano" parzialmente la congettura di Artin che afferma come $\mathbb{Q}_p$ sia C_2 per ogni p: lo hanno dimostrato definitivamente per primi p abbastanza grandi. Purtroppo il teorema non ci dice l'insieme dei p per i quali, fissato un grado d, $\mathbb{Q}_p$ non è $C_2(d)$. La congettura è infatti falsa, nella prossima breve sezione mostriamo come sia stato trovato una coppia p primo e d grado per i quali effettivamente non vale.

3.3 Il controesempio di Guy Terjanian

La congettura di Artin sulle forme p-adiche è stata dimostrata per i gradi $d = 1, 2, 3$ grazie ai seguenti contributi storici, qui brevemente richiamati:

1. Grado 1 ($d = 1$): Il caso lineare si riduce all'algebra lineare classica. Una forma omogenea in $n > 1$ variabili ammette sempre soluzioni non banali su qualsiasi campo.

2. Grado 2 ($d = 2$): Il caso quadratico è una conseguenza diretta del *Teorema di Hasse-Minkowski* sulle forme quadratiche, dimostrato da Helmut Hasse negli anni '20.

3. Grado 3 ($d = 3$): Dimostrato da Donald J. Lewis nel 1952.

Per i gradi d successivi per molti anni nessuno nè riuscì a dimostrare nè a confutare la congettura. La dimostrazione del teorema di James Ax e Simon Kochen che convalida la congettura in modo asintotico risale agli anni 1965 con la pubblicazione di *"Diophantine problems over local fields. I"*. L'anno dopo il matematico francese Guy Terjanian ha trovato un controesempio 2-adico per $d = 4$. Definito infatti

$$G(\overline{x}) = G(x_1, x_2, x_3) = (\sum_i x_i^4) - (\sum_{i<j} x_i^2 x_j^2) - x_1 x_2 x_3 (x_1 + x_2 + x_3),$$

G ha la proprietà che è 1 mod 4 se x_i è pari per qualche $i \in \{1, 2, 3\}$, altrimenti è 0 mod 16. Allora $f_G(\overline{x}, \overline{y}, \overline{z}, \overline{u}, \overline{s}, \overline{w}) = G(\overline{x}) + G(\overline{y}) + G(\overline{z}) + 4G(\overline{u}) + 4G(\overline{s}) + 4G(\overline{w})$ di grado $d = 4$ in $18 > 16 = d^2$ variabili non ha nessun zero non triviale in $\mathbb{Q}_2$.

Successivamente, Terjanian mostrò anche che per ogni numero primo p e per ogni grado $d > 2$ tale che $p(p-1)$ divida d, esiste un polinomio omogeneo in $\mathbb{Q}_p$ di grado d in $n > d^2$ variabili privo di zeri non banali. Di conseguenza, egli dimostrò che l'insieme $P(d)$ dei controesempi, definito nell'enunciato del teorema di Ax-Kochen, contiene tutti i numeri primi p per cui $p(p-1)$ divide d.

Bibliografia

[1] Kruckman, A.. The Ax-Kochen Theorem: an application of model theory to algebra.Arxiv: 1308.3897, 2013.

[2] James Ax and Simon Kochen. Diophantine problems over local fields. I. Amer. J. Math., 87:605–630, 1965.

[3] David Marker. Model theory, volume 217 of Graduate Texts in Mathematics. Springer-Verlag, New York, 2002.