POLITECNICO DI TORINO

Corso di Laurea
in Matematica per l'Ingegneria

Tesi di Laurea

Algebra Commutativa: Anelli di Noether e di Artin

Relatori
prof. Francesco Malaspina
firma dei relatori

. . . . . .
. . . . . .

Candidato
Enrico Chiavassa
firma del candidato

. . . . . .

Anno Accademico 2020-2021

Sommario

Emmy Noether e Emil Artin sono stati tra le figure più importanti ed influenti dell'algebra astratta del 20° secolo. Durante la loro vita hanno approfondito aspetti molto diversi dell'algebra commutativa, tuttavia entrambi hanno ottenuto risultati fondamentali per lo sviluppo di questo ramo della matematica. In questo elaborato verrà presentata in primo luogo la teoria delle catene ascendenti, discussa da Noether nel paper *"Idealtheorie in Ringbereichen"* (Ideal Theory in Rings), e come questa definisca la condizione di **finitezza** che caratterizza gli anelli noetheriani. In seguito si approfondiranno alcune proprietà di questa famiglia di anelli, tra cui il teorema delle basi di Hilbert il quale mostra come la condizione di noetherianità si trasmette ad un anello di polinomi. Successivamente l'attenzione sarà spostata sulla condizione della catena discendente e quindi sugli anelli di Artin. Si studieranno le loro similitudini e le loro differenze con gli anelli di Noether, senza tralasciare alcune loro proprietà uniche. Tutto questo si concluderà con il teorema di Akizuki-Hopkins-Levitzki (e la sua dimostrazione) che mostra come gli anelli artiniani altro non sono che un particolare tipo di anelli noetheriani. Tuttavia per poter arrivare ai grandi teoremi appena citati sarà necessario enunciare e dimostrare un buon numero di proposizioni preliminari, che in alcuni casi saranno affrontate anche in modo più generale rispetto a quanto sarebbe sufficiente. Nell'ultimo capitolo invece verrà fatta un'introduzione alla geometria algebrica: per prima cosa si andrà definire le varietà algebriche, che sono di fatto l'oggetto di studio di questa disciplina, e verrà presentato il cosiddetto *Nullstellensatz* di Hilbert, che in italiano prende il nome di teorema degli zeri di Hilbert. Il tutto sarà anticipato da un capitolo dedicato alla ripresa dei concetti di base del corso di Istituzioni di Algebra e Geometria e all'introduzione del concetto di modulo su un anello, oltre ad alcune nuove proprietà riguardanti gli ideali.

Indice

Introduzione

This paper aims to convert the decomposition theorems for the integers or the decomposition of ideals in algebraic number fields into theorems for ideals in arbitrary integral domains (and rings in general). Così inizia l'articolo *Idealtheorie in Ringbereichen (Theory of Ideals in Ring Domains)* di Emmy Noether, dove per la prima volta si è fatto uso della condizione delle catene ascendenti, in breve a.c.c., come strumento di studio della scomposizione degli ideali di anelli generici. Da quel momento in poi l'a.c.c. (e la condizione di finitezza associata) è diventata un'ipotesi estremamente comune negli ambiti di ricerca e la classe di anelli di Noether ha acquistato una notevole importanza all'interno dell'algebra commutativa. La loro regolarità porta con sè un numero non indifferente di proprietà e teoremi che rendono più semplice il loro studio. Tra questi si ricorda il teorema di Lasker-Noether, che riguarda la scomposizione in ideali, e il teorema delle basi di Hilbert, che riguarda gli anelli di polinomi in un numero finito di variabili a coefficienti in un anello di Noether.

Figura 1. Emmy Noether

Nello stesso periodo un altro matematico, decisamente meno noto, ha lavorato sulla condizione apparentemente simmetrica rispetto a quella di Noether, ovvero la condizione delle catene discendenti (o d.c.c.). Si trattava di Emil Artin, il ricercatore boemo che per primo ha individuato e studiato questa proprietà e la corrispondente classe di anelli. Come ci si potrebbe aspettare, le similitudini tra le due teorie delle catene sono molte, ma altrettante sono le differenze. In particolare, la forte regolarità fornita dall'a.c.c. manca nella d.c.c. e questo ha condannato gli anelli di Artin ad essere messi in secondo piano rispetto a quelli di Noether. Non solo, nel decennio successivo tre ricercatori (Akizuki,

Hopkins e Levitzki) hanno dimostrato come gli anelli artiniani altro non siano che un particolare tipo di anelli noetheriani. In generale, sono la forma di anello più regolare dopo i campi e proprio per questa loro semplicità il loro studio si rivela di un certo interesse, anche se il loro utilizzo è stato estremamente più limitato.

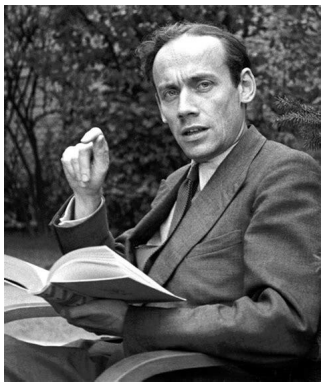

Figura 2. Amil Artin

Sempre negli stessi anni e sempre in Germania, un altro matematico ha messo le basi per una nuova disciplina che sarebbe stata al centro delle ricerche per tutto il ventesimo secolo e oltre. In particolare, il Nullstellensatz, enunciato e dimostrato da David Hilbert, rappresenta il punto di partenza della geometria algebrica, ma non solo. È infatti un ponte tra algebra e un geometria, in quanto lega gli ideali in anelli di polinomi a coefficienti in un campo algebricamente chiuso con le varietà algebriche. In questa esposizione, si presenteranno tutti i concetti di cui si è parlato in questa introduzione e si cercherà di farlo nel modo più chiaro possibile, procedendo a piccoli passi in modo che ogni passaggio appaia coerente col discorso generale.

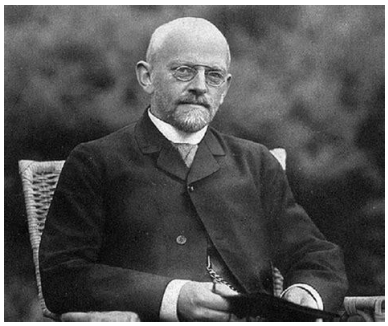

Figura 3. David Hilbert

Capitolo 1

Nozioni fondamentali

Prima di addentrarsi nella teoria delle catene, è necessario fare un breve ripasso dei concetti fondamentali dell'algebra. Alcune dimostrazioni sono omesse in quanto fanno parte del programma del corso di Istituzioni di algebra e geometria.

1.1 Le Strutture di Base

Definizione 1.1. *Un insieme G non vuoto dotato di un'operazione '+' è detto gruppo se rispetta le seguenti condizioni:*

1. *Vale la proprietà associativa, ovvero:* $x + (y + z) = (x + y) + z,\ \forall x, y, z \in G$
2. *Esiste un elemento x in G tale che* $x + y = y + x = y,\ \forall y \in G$
   Questo prende il nome di elemento neutro e si indica con 0_G.
3. *Ogni elemento possiede un elemento inverso, ovvero :*
   $\forall x \in G,\ \exists\, (-x) \in G \mid x + (-x) = 0$

In ogni gruppo, l'elemento neutro e gli elementi inversi sono unici. È possibile dare la stessa definizione di gruppo con la notazione moltiplicativa; in quel caso l'operazione di indica con *, l'elemento neutro si indica con 1_G e gli elementi inversi con x^{-1}

Definizione 1.2. *Un gruppo G è detto abeliano se vale la proprietà commutativa, ovvero:*
$$x + y = y + x \quad \forall\ x,\ y \in G$$

All'interno di un gruppo è possibile definire un altro tipo di struttura, *il sottogruppo.*

Definizione 1.3. *Dato un gruppo $(G, +)$, un sottoinsieme $H \subseteq G$ è detto sottogruppo se è un gruppo per la restrizione ad H dell'operazione del gruppo G. Questo è equivalente alla seguente condizione:* $x - y \in H \quad \forall x, y \in H$

Osservazione. $\{0_G\}$ *e G sono sempre sottogruppi di G stesso e sono detti impropri.*

Definizione 1.4. *Un insieme A dotato di due operazioni, dette somma e prodotto e indicate con + e *, è detto anello se rispetta le seguenti condizioni:*

1. *(A,+) è un gruppo abeliano*
2. ** è un'operazione associativa, ovvero:* $x * (y * z) = (x * y) * z, \ \forall x, y, z \in A$
3. *Vale la proprietà distributiva a destra e a sinistra di * rispetto a +, ovvero:*
$$x * (y + z) = x * y + x * z, \ (y + z) * x = y * x + z * x \quad \forall \ x, y, z \in A$$

Dalla definizione è chiaro che (A,) non è necessariamente un gruppo, tuttavia è possibile aggiungere alcune ipotesi sull'operazione moltiplicativa per ottenere diversi tipi di anello:*

- *Se l'anello contiene un elemento neutro rispetto a *,* 1_G*, allora è detto unitario*
- *Se vale la proprietà commutativa rispetto a *, l'anello è detto commutativo*
  In questa esposizione, se non chiaramente indicato, si farà sempre riferimento ad anelli unitari e commutativi.
- *Se l'anello contiene tutti gli elementi inversi rispetto a *, allora è detto corpo*
- *Un corpo commutativo è detto campo*

Diversamente da quanto accade nei gruppi, all'interno degli anelli è possibile definire **due** tipi di sottostrutture, *il sottoanello e l'ideale*

Definizione 1.5. . *La seconda sarà particolarmente importante in quanto la teoria che sarà presentata ne fa un uso estensivo. Dato un anello (A,+,*), un sottoinsieme* $S \in A$ *è detto sottoanello se è un anello per la restrizione delle operazioni di A. Questo equivalenti alla condizione:*
$$x - y \in S \quad \wedge \quad x * y \in S \quad \forall x, y \in S$$

Definizione 1.6. *Dato un anello (A,+,*), un sottoinsieme* $S \subset A$ *è detto ideale bilatero se vale la seguente proprietá:*
$$x - y \in S \quad \wedge \quad a * x = x * a \in S \quad \forall x, y \in S, \ \forall a \in S$$
Un ideale I è detto primo se, presi $a, b \in A$ *tali che* $a * b \in I$*, allora o* $a \in I$ *oppure* $b \in I$*. Un ideale è detto massimale se non è contenuto propriamente in nessun altro ideale. Ogni ideale massimale è anche primo, ma il viceversa non vale. Un ideale è generato da una famiglia di elementi* (x_i) *se è possibile scrivere ogni suo elemento nella forma* $\sum_{i \geq 1} a_i * x_i$*. Un elemento di A è detto unità se è un divisore di* 1_A*, ovvero se l'ideale da esso generato è uguale all'anello stesso.*

Se A non è commutativo, modificando la seconda ipotesi si ottiene una distinzione tra ideali destri e sinistri, in base al lato da cui si moltiplica per a. Chiaramente questa distinzione viene meno in ambienti commutativi.

Definizione 1.7. *Dato un anello A e un suo ideale I, si consideri l'insieme* $\{x \in A \mid x^n \in I \text{ per qualche } n\}$*. Questo è un ideale, è detto radicale di I e si indica con* $r(I)$

Dato un ideale, è possibile definire una nuova tipologia di anelli, detti *anelli quozienti*:

Definizione 1.8. *Dato un anello A e un suo ideale I, si definisce classe laterale di $a \in A$ in questo modo: $[a] = (I + a) = \{i + a,\ i \in I\}$. L'insieme formato da tutte le classi laterali degli elementi di A assume la struttura di anello quando viene associato alle seguenti operazioni:*

- $(I + a)\ +\ (I + b)\ = (I + a + b)$;
- $(I + a)\ *\ (I + b)\ = (I + a * b)$.

Questo tipo di anello prende il nome di anello quoziente e viene indicato con A/I. Dalla definizione è chiaro che $0_{A/I} = I$ e $1_{A/I} = (I + 1_A)$

La seguenti proposizioni riguardanti gli ideali torneranno utili più avanti.

Proposizione 1.9. *Dato un anello A e un suo ideale non banale I:*
I è primo $\iff$ A/I è un dominio d'integrità.
I è massimale $\iff$ A/I è un campo.

Proposizione 1.10. *Dato un anello A, una famiglia di ideali primi $(P_i)_{i=1}^n$ e un ideale I, se $I \subseteq \bigcup_{i=1}^n P_i$ allora $I \subseteq P_i$ per qualche i.*

Dimostrazione. Per prima cosa si riscrive la proposizione in questa forma: se $I \nsubseteq P_i\ \forall i$, allora $I \nsubseteq \bigcup_{i=1}^n P_i$. A questo punto si applica il principio d'induzione: chiaramente per n=1 la tesi vale. Se si ipotizza che valga anche per $n-1$, allora esiste una famiglia $\{x_i\}$ tale che $x_i \in P_j$ se e solo se $i = j$. Questo perchè considerando solo n-1 ideali primi per volta, la tesi è verificata e almeno un elemento di I non appartiene alla loro unione. A questo punto se almeno un x_i non è incluso in P_i, la tesi è verificata. Se invece $x_i \in \bigcup_{i=1}^n P_i\ \forall i$, allora si definisce l'elemento $y := \sum_{i=1}^n x_1 * x_2 * ... * x_{i-1} * x_{i+1} * ... * x_n$, che appartiene chiaramente ad I ma non appartiene a nessun P_i. Allora $I \nsubseteq \bigcup_{i=1}^n P_i$. □

Inoltre, data una famiglia di ideali $\{I_i\}_{i=1}^n$ e un ideale primo P che contiene $\bigcap_{i=1}^n I_i$, allora $I_i \subseteq P$ per qualche i.

Dimostrazione. Se per assurdo $I_i \nsubseteq P\ \forall i$, allora esiste una famiglia $\{x_i\}$ tale che $x_i \in I_i$ e $x_i \notin P\ \forall i$. Il prodotto $y := \prod_{i=1}^n x_i$ è contenuto nell'ideale $\prod_{i=1}^n I_i$[1], che a sua volta è contenuto nell'ideale $\cap_{i=1}^n I_i$. Tuttavia $y \notin P$, in quanto P è primo, di conseguenza P non contiene $\cap_{i=1}^n I_i$. ↯ □

1.2 Omomorfismi

Un omomorfismo, in termini molto generali, è un'applicazione tra due strutture dello stesso tipo che preserva le operazioni di tali strutture. Seguono le definizioni per omomorfismo tra gruppi e tra anelli.

[1] l'ideale generato da tutti i prodotti $\prod_{i=1}^n a_i$, con $a_i \in I_i$, $\forall i$

Definizione 1.11. *Dati due gruppi (G, ×) e (H, *), un'applicazione* $f: G \to H$ *è detta omomorfismo tra gruppi se* $f(x \times y) = f(x) * f(y),\ \forall x, y \in G$

Definizione 1.12. *Dati due anelli (A,* $\oplus$*,×) e (B,+,*), un'applicazione* $f: A \to B$ *è detta omomorfismo tra anelli se* $f(x \oplus y) = f(x) + f(y),\ f(x \times y) = f(x) * f(y), \forall x, y \in A$

Sono considerati noti i concetti di iniettività, suriettività, insieme immagine e kernel di un omomorfismo.
Per evitare confusione, però, si ricorda la nomenclatura dei vari tipi di omomorfismi:

Definizione 1.13.

- *Un omomorfismo iniettivo è detto monomorfismo;*
- *Un omomorfismo suriettivo è detto epimorfismo;*
- *Un omomorfismo biettivo è detto isomorfismo;*
- *Un omomorfismo da una struttura in se stessa è detto endomorfismo;*
- *Un endomorfismo biettivo è detto automorfismo.*

Ad esempio, dato un anello A, un ideale I e l'anello quoziente A/I, l'applicazione che associa ad ogni elemento di A la sua classe laterale in A/I è un epimorfismo con kernel I.
Si enuncia ora un teorema di estrema importanza che verrà richiamato all'interno di questa trattazione:

Teorema 1.14 (Teorema fondamentale degli omomorfismi di anelli)**.** *Sia* φ *un omomorfismo di anelli,* $\varphi: A \to A'$*, e sia* $K = Ker(\varphi)$*. Esiste un omomorfismo di anelli* $\psi: A/K \to A'$ *tale che* $\varphi = \psi(\pi)$*, dove* π *è la proiezione naturale da A su* A/K*. In particolare, si ha che* $A/K \cong Im(\varphi)$*.*

1.3 I Moduli e le loro Proprietà

Nel corso del 20° secolo l'attenzione degli studiosi si è spostata verso una struttura che racchiude e generalizza i concetti di anello e di ideale: *il modulo.*

Definizione 1.15. *Dato un anello commutativo (A,+,*), si definisce A-modulo un gruppo (M,+) dotato di un'applicazione* φ *da* $A \times M$ *in M che soddisfa le seguenti proprietà. Questa applicazione può essere banalmente vista come un prodotto tra uno scalare (ovvero un elemento di A) e un elemento di M, per questo motivo verrà utilizzata la notazione ax al posto della più classica* $\varphi(a, x)$

1. $a(x + y) = ax + ay$
2. $(a+b)x = ax + bx$
3. $(a*b)x = a(bx)$
4. $1_A x = x$ $\qquad \forall\ a,\ b \in A, \quad \forall x,\ y \in M$

Notare come il prodotto tra a e b è quello dell'anello A, non quello associato al modulo. Come per gli ideali, rimuovendo l'ipotesi della commutatività di A si possono definire due tipi di A-moduli distinti: quelli destri e quelli sinistri, in base al lato da cui si moltiplica per lo scalare. Il concetto di generatore di e di modulo finitamente generato sono analoghi a quelli relativi agli anelli.

Si dimostra ora l'affermazione precedenza, ovvero che il modulo è una generalizzazione dell'ideale:

Proposizione 1.16. *Dato un anello (A,+,*) e un suo ideale I, allora I è un A-modulo. In particolare, A stesso è un A-modulo.*

Dimostrazione. Per definizione di ideale è possibile considerare (I,+) come gruppo additivo e * come prodotto per uno scalare. In questo modo la verifica delle ipotesi è triviale, in quanto il prodotto di A le rispetta per definizione, e (I,*) è un A-modulo. Inoltre A è sempre un ideale improprio di sé stesso, quindi è anche un A-modulo. □

Quello che è stato detto finora non trasmette appieno l'importanza di questa struttura. Un modulo infatti è la generalizza il concetto di spazio vettoriale rimuovendo l'ipotesi del campo degli scalari, che ora possono essere contenuti in un anello qualsiasi. Tutto ciò è racchiuso nella seguente proposizione:

Proposizione 1.17. *Se l'anello A è un campo, allora un A-modulo è un spazio vettoriale su A.*

Dimostrazione. Imponendo che A sia un campo, tutte le proprietà di spazio vettoriale sono rispettate. La verifica è triviale. □

Ora che è chiaro il concetto di A-modulo, è possibile definire gli omomorfismi tra queste strutture.

Definizione 1.18. *Dato un anello A e due A-moduli M e N, un'applicazione* $f: M \to N$ *è detta omomorfismo tra A-moduli se*

- $f(x+y) = f(x) + f(y) \ \ \forall x, y \in G;$
- $f(ax) = af(x) \ \ \forall a \in A, x \in M.$

Di fatto, un omomorfismo tra A-moduli altro non è che un omomorfismo tra i gruppi additivi che agisce linearmente sugli elementi di A.

Come già visto per gruppi e anelli, si definisce una sotto-struttura del modulo:

Definizione 1.19. *Dato un A-modulo M, un sottoinsieme* $M \subset M$ *è detto sottomodulo di M se è un suo sottogruppo additivo ed è chiuso rispetto al prodotto per uno scalare. Il concetto di modulo quoziente e le sue proprietà sono analoghi a quanto detto per gli anelli, in particolare il 1.14 vale anche i moduli.*

Proposizione 1.20. *Dato un omomorfismo* $\varphi: M \to N$*, con M e N A-moduli, l'immagine di un sottomodulo di M è un sottomodulo di N. Similarmente, la controimmagine di un sottomodulo è ancora un sottomodulo.*

Dimostrazione. Detti M' il sottomodulo di M e N' la sua immagine, è noto che N' è ancora un sottogruppo. Inoltre, presi $a \in A$ e $x' \in N'$, $\exists x \in M | \varphi(x) = x'$ e vale la seguente:
$ax' = a\varphi(x) = \varphi(ax) \in N'$, in quanto $ax \in M'$. N' è quindi un sottogruppo additivo chiuso rispetto al prodotto per uno scalare. La seconda parte si prova come la precedente. □

Un particolare tipo di A-moduli che verrà utilizzato nel secondo capitolo è il *modulo libero*:

Definizione 1.21. *Un A-modulo M è detto modulo libero se è isomorfo a un A-modulo della forma $\bigoplus_{i \in I} M_i$, dove $M_i \cong A$, $\forall i \in I$. A è inteso come A-modulo. Se I è un insieme finito allora M è detto libero e finitamente generato ed è isomorfo a $\bigoplus_{i=1}^{n} A$[2].*

Proposizione 1.22. *Un A-modulo M è finitamente generato $\iff$ M è isomorfo ad un quoziente di A^n, per qualche valore di n.*

Dimostrazione. $\implies$ Si considera un A-modulo M generato dalla famiglia $(x_i)_{i=1}^{n}$ e si definisce l'applicazione $\varphi : A^n \to M$, con $\varphi(a_1, ..., a_n) = a_1x_1 + ... + a_nx_n$. Si verifica facilmente che φ è un omomorfismo tra moduli con immagine M, quindi per il 1.14 $M \cong A^n / Ker(\varphi)$.
$\impliedby$ Sempre per il 1.14 esiste un epimorfismo $\varphi : A^n \to M$. Si definisce $e_i = (0, ..., 0, 1_A, 0, ..., 0)$, dove l'unità si trova nella i-esima posizione. E' evidente che $(e_i)_{i=1}^{n}$ genera A^n, quindi $(\varphi(e_i))_{i=1}^{n}$ genera M. □

[2] *Questa somma diretta sarà indicata con A^n*

Capitolo 2

Anelli noetheriani e artiniani

In questo capitolo verrà definita e analizzata la teoria delle catene ascendenti e della relativa condizione di finitezza. Dopodiché si approfondiranno alcune proprietà importanti riguardanti la trasmissibilità della proprietà di noetherianità fino ad arrivare al teorema delle basi di Hilbert per gli anelli di polinomi ad un numero finito di variabili. Infine, il discorso verrà allargato agli anelli artiniani, alle loro proprietà e alla loro relazione con gli anelli di Noether tramite il teorema di Akizuki-Hopkins-Levitzki. Nonostante il titolo, si farà largo uso dei moduli nelle proposizioni preliminari, necessarie a dimostrare i teoremi e le proprietà degli anelli.

2.1 Condizione della catena ascendente

Le condizioni della catena sono una coppia di ipotesi riguardanti i sottomoduli di un modulo. Verranno discusse entrambe, ma inizialmente si porrà l'attenzione sulla cosiddetta *a.c.c.*, ovvero la condizione della catena ascendente. Nella trattazione di E. Noether [1921] questa proprietà viene discussa come conseguenza dell'ipotesi di finitezza, tuttavia in questa esposizione si svilupperà il ragionamento in senso contrario, seguendo l'ordine usato da I.G. MacDonald [1994] e da H. Matsumura [1989].

Proposizione 2.1. *Sia dato un insieme A dotato di una relazione d'ordine $\leq$, allora le seguenti condizioni sono equivalenti:*

1. *ogni successione crescente $x_1 \leq x_2 \leq ...$ contenuta in A è stazionaria, ovvero $\exists j \geq 1 \mid x_n = x_m \ \forall n, m \geq j$*
2. *Tutti i sottoinsiemi non vuoti di A hanno un elemento massimale, ovvero un elemento X per se $\exists Y$ tale che $X \leq Y$, allora $X = Y$*

Dimostrazione. $1 \Rightarrow 2$ Preso un sottoinsieme $S \subset A$, si suppone per assurdo che non abbia un elemento massimale. Si considera un elemento $x_1 \in S$ e l'insieme S_{x_1} composto da tutti gli elementi $y \in S$ tali che $y \geq x$. Per l'assioma della scelta esiste una funzione ϕ che associa a S_{x_1} un suo elemento. Si definisce $x_2 := \phi(S_{x_1})$ e si ripete il procedimento. Avendo ipotizzato l'assenza di un massimale, la successione $(x_k)_{k\geq 1} \in S$ non può essere

stazionaria. ↯
$2 \Rightarrow 1$ Ogni successione crescente forma un sottoinsieme parzialmente ordinato, che per ipotesi ha massimale. Allora la successione è necessariamente stazionaria. □

La proposizione precedente ha un valore molto generale, ma in questa trattazione si considererà solo i cas in cui A sia l'insieme di tutti i sottomoduli di un modulo, ordinati secondo la relazione d'inclusione $\subseteq$, oppure l'insieme di tutti gli ideali di un anello, ordinati allo stesso modo. Con queste ipotesi la condizione **1** viene chiamata **condizione della catena ascendente** o, più brevemente, *a.c.c.*, mentre la condizione **2** viene chiamata **condizione massimale**. Più avanti in questo capitolo si andrà a discutere anche il caso in cui la relazione associata ad A sia $\supseteq$, e si mostrerà il motivo per cui questa scelta, di solito, non viene fatta.
Ora è tutto pronto per la definizione cardine di questa trattazione:

Definizione 2.2. *Un modulo (anello) A che rispetta la condizione della catena ascendente (oppure l'equivalente condizione massimale) sui suoi sottomoduli (ideali) è detto* ***noetheriano****.*
Per la condizione massimale, l'insieme di tutti gli ideali propri di un anello di questo tipo ha un elemento massimale, ovvero ogni anello di Noether possiede almeno un ideale proprio massimale.

La prossima proprietà è di fondamentale importanza per la teoria dei moduli noetheriani ed è il motivo per il loro largo utilizzo. Citando I.G. MacDonald [1994], *"the Noetherian condition is just the right finiteness condition to make a lot of theorems work"*.

Proposizione 2.3. *Un modulo M è noetheriano $\iff$ Ogni sottomodulo di M è finitamente generato*[1]*.*

Dimostrazione. $\implies$ Si consideri un sottomodulo $N \in M$ e l'insieme Γ di tutti i sottomoduli finitamente generati di N. Per ipotesi, Γ contiene un elemento massimale, detto N_0. Se $N \neq N_0$ è possibile considerare un elemento $x \in N - N_0$ e costruire il sottomodulo $N_0 + Ax$ che appartiene ad N ed è finitamente generato, quindi appartiene a Γ. ↯
Allora $N = N_0$, quindi N è finitamente generato.
$\impliedby$ Sia $M_1 \subseteq M_2 \subseteq M_3 \subseteq ...$ una catena ascendente arbitraria di sottomoduli di M. Si definisce $N = \bigcup_{k \geq 1} M_k$. N è ancora un sottomodulo di M ed è quindi finitamente generato; arbitrariamente si scelgono come generatori $(x_1, x_2, ..., x_r)$. Per definizione di N, vale che $\forall j \geq 1, \exists\ k_j = min\,(k \mid x_j \in M_k)$. Definendo $n = \max(n_j)$, è chiaro che $\forall j \in (1, \ldots, r)$, $x_j \in M_n$, quindi $N = M_k$, $\forall k \geq n$ e dunque la successione è stazionaria. □

Alcuni autori, ad esempio Eisenbud [1995], preferiscono definire i moduli noetheriani usando questa condizione e solo in seguito mostrare l'equivalenza con la a.c.c e con la condizione massimale. Noether stessa descrisse l'a.c.c come proprietà degli anelli che rispettano la condizione di finitezza dei propri sottoanelli.

[1] *Ovvero esiste un numero finito di elementi del sottomodulo, detti generatori, tale che ogni altro elemento del sottomodulo è esprimibile come combinazione lineare di quei generatori*

Esiste infine una quarta formulazione, equivalente alle precedenti, attribuita al matematico tedesco Hilbert (Eisenbud [1995]).

Proposizione 2.4. *Un A-modulo M è noetheriano* $\iff$ *Data un successione arbitraria di elementi di M, detta* m_1, m_2, ..., *esiste un numero t tale che* $m_n = \sum_{i=1}^{t} a_i m_i \quad \forall n \geq t$, *con* $a_i \in A$.

Dimostrazione. $\Longleftarrow$ Lo si mostra per assurdo negando la condizione di finitezza. Se non esiste un insieme finito di generatori allora è possibile considerare un elemento generico m_1 e creare iterativamente una successione dove m_n è sempre scelto fuori dal sottomodulo generato dagli elementi precedenti. È chiaro che $m_1, m_2, ...$ non rispetta la condizione di Hilbert $\lightning$
$\Longrightarrow$ Lo si dimostra come conseguenza della *a.c.c.* Se esiste una successione per cui non vale la condizione di Hilbert, allora non può essere stazionaria. $\lightning$ □

Si illustrano ora alcuni esempi molto semplici di anelli di Noether

Esempi.

1. *Ogni campo è noetheriano, in quanto un campo ha solo 2 ideali (0 e il campo stesso).*
2. *Per la condizione di finitezza, ogni PID è noetheriano. Per questo l'anello Z è noetheriano, così come l'anello* $K[x]$ *con K campo*
3. *Ogni anello abeliano finito inteso come Z-Modulo è noetheriano, in quanto deve necessariamente rispettare l'a.c.c.*
4. *L'anello* $k[x_1, x_2, ...]$, *ovvero l'anello dei polinomi a coefficienti nel campo K ad infinite variabili non è noetheriano in quanto non soddisfa l'a.c.c.. Basta considerare la successione di ideali* $(x_1) \subseteq (x_1, x_2) \subseteq (x_1, x_2, x_3) \subseteq ...$.

2.2 Proprietà degli Anelli di Noether

Ora che gli anelli di Noether sono stati definiti, è possibile approfondire alcune delle loro proprietà. In primo luogo si vedrà come la condizione che li caratterizza si trasmette tra diverse strutture e si dimostrerà il teorema delle basi di Hilbert. Secondariamente ci si concentrerà sulla decomposizione in ideali primari e si mostrerà come gli anelli noetheriani rappresentino la principale famiglia di anelli in cui tale decomposizione è unica.

2.2.1 Trasmissibilità della condizione di noetherianetà

Le proprietà che si andranno ad analizzare sono 3 e riguardano rispettivamente l'effetto di un omomorfismo su un anello noetheriano, la relazione tra anelli e sottoanelli noetheriani e infine gli anelli di polinomi a coefficienti in un anello noetheriano, descritti dal celebre teorema delle basi di Hilbert. Tuttavia, prima di poter enunciare e dimostrare tali proposizioni, è necessario approfondire ulteriormente la teoria dei moduli noetheriani, partendo da due definizioni.

Definizione 2.5. *Dati due A-moduli M e N, la somma diretta $M \oplus N$ è l'insieme di tutte le coppie (x, y), con $x \in M, y \in N$. Questo insieme diventa a sua volta un A-modulo se fornito delle seguenti operazioni:*

- $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$
- $a\,(x, y) = (ax, ay)$

Allo stesso modo si può definire la somma diretta di una famiglia $\{M_i\}_{i\in I}$ di A-moduli. Gli elementi di tale insieme sono famiglie $\{x_i\}_{i\in I}$ dove $x_i \in M_i\ \forall i \in I$ e solo un numero finito di elementi è non nullo. Equivalentemente, si dice che gli elementi sono quasi tutti nulli. Rimuovendo quest'ultima ipotesi si definisce il prodotto diretto $\prod_{i\in I} M_i$.

Definizione 2.6. *Una sequenza di A-moduli e di omomorfismi da A in A nella forma*

$$\ldots \xrightarrow{f_{i-1}} M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \xrightarrow{f_{i+2}} \ldots$$

è detta esatta se $Im(f_i) = Ker(f_{i+1}),\ \forall i$

Osservazione. *Dalla definizione derivano queste tre proprietà:*

1. $0 \to M' \xrightarrow{f} M$ *è esatta* $\iff f$ *è iniettiva;*
2. $M \xrightarrow{g} M'' \to 0$ *è esatta* $\iff g$ *è suriettiva;*
3. $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ *è esatta* $\iff f$ *è iniettiva, g è suriettiva e induce un isomorfismo da $M/Im(f)$[2] a M'' .*

Le dimostrazioni sono immediate e poco interessanti, tuttavia la sequenza esatta del punto 3 è di particolare importanza e viene detta ***corta****. Ogni sequenza del tipo*

$$\ldots \xrightarrow{f_{i-1}} M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \xrightarrow{f_{i+2}} \ldots$$

può essere suddivisa in sequenze esatte corte, tutte nella forma

$$0 \to N_1 \to M_i \to N_{i+1} \to 0$$

dove $N_i = Im(f_i) = Ker(f_{i+1})$.

Proposizione 2.7. *Data la sequenza esatta corta $0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$ di A-moduli, si ha che: M è notheriano $\iff$ M' e M" sono noetheriani.*

Dimostrazione. Si tenga a mente la proposizione 1.20.
$\Longrightarrow$ Data una catena ascendente $(M'_i) \subset M'$, $(\alpha\,(M'_i))$ è una catena ascendente in M, quindi è stazionaria per ipotesi. Di conseguenza anche (M'_i) lo è, in quanto α è iniettiva, dunque M' è noetheriano per l'*a.c.c.*. Il ragionamento per M'' è analogo.
$\Longleftarrow$ Data una catena ascendente di sottomoduli (M_i) in M, considero le catene ascendenti $(\alpha^{-1}\,(M_i))$ e $(\beta(M_i))$. Queste sono entrambe stazionarie, quindi anche (M_i) lo è, dunque M è noetheriano. □

[2] *questo quoziente è detto cokernel di f*

Proposizione 2.8. *Data una famiglia finita di moduli noetheriani* $(M_i)_{i=1}^n$*, la somma diretta* $\bigoplus_{i=1}^n M_i$ *è ancora un modulo noetheriano.*

Dimostrazione. Si applica il principio di induzione alla sequenza esatta corta $0 \to M_n \xrightarrow{f} \bigoplus_{i=1}^n M_i \xrightarrow{g} \bigoplus_{i=1}^{n-1} M_i \to 0$. La definizione è verificata se f associa ad ogni elemento $m \in M$ la n-upla $(0, ..., 0, m)$, come una sorta di identità, e se g associa ad ogni n-upla $m' \in \bigoplus_{i=1}^n M_i$ una (n-1)-upla composta dai primi n-1 elementi di m'. Il passo base, per $n = 1$, è ovvio per 2.7. Assumendo vera la proposizione per un certo $n \geq 1$, si considera il caso $n + 1$. Per ipotesi M_{n+1} e $\bigoplus_{i=1}^n M_i$ sono entrambi noetheriani, quindi la tesi è nuovamente verificata per 2.7. □

Da queste due proposizioni ne seguono altre due: la prima riguarda i moduli finitamente generati, mentre la seconda gli ideali.

Proposizione 2.9. *Dato un anello noetheriano* A *e un* A*-modulo finitamente generato* M*, si ha che* M *è noetheriano.*

Dimostrazione. Dalla 1.22 è noto che $M \cong A^n/Q$, per un certo $Q \subseteq A^n$. Dalla 2.8 si sa che $A^n = \bigoplus_{i=1}^n A$ è noetheriano. A questo punto è possibile costruire la sequenza esatta corta $0 \to Q \xrightarrow{f} A^n \xrightarrow{g} A^n/Q \to 0$, dove f è l'identità e g è la proiezione naturale. La 2.7 implica che A^n/Q sia noetheriano, quindi anche M. □

Proposizione 2.10. *Dato un anello noetheriano* A *e un suo ideale* I*, allora* A/I *è un anello noetheriano.*

Dimostrazione. Usando la 2.7 alla sequenza esatta corta $0 \to a \xrightarrow{f} A \xrightarrow{g} A/I \to 0$[3] è chiaro che A/I è noetheriano. In questo caso A/I è visto come un A-modulo in quanto, per ipotesi, la sequenza esatta corta dev'essere composta da A-moduli, tuttavia la noetherianetà si mantiene anche se A/I è visto come A/I-modulo e quindi come anello. □

Tutte queste proposizioni rendono possibile enunciare e dimostrare con relativa semplicità le seguenti tre proprietà degli anelli noetheriani.

Proposizione 2.11. *Dati due anelli* A *e* B *e un epimorfismo* $\varphi : A \to B$*, se* A *è noetheriano allora anche* B *lo è.*

Dimostrazione. Per il 1.14, $B \cong A/Ker(\varphi)$ che è noetheriano per la 2.10. Quindi anche B è noetheriano. □

Proposizione 2.12. *Dato un anello* B *e un suo sottoanello* A*. Se* A *è noetheriano e se* B *è un* A*-modulo finitamente generato, allora* B *è noetheriano.*

Dimostrazione. Per la 2.9, B è un A-modulo noetheriano. Dunque lo è anche come B-modulo, quindi come anello. □

Teorema 2.13 (delle basi di Hilbert)**.** *Dato un anello* A *noetheriano,* $A[x]$ *è noetheriano.*

[3] funzioni definite come nella dimostrazione precedente

Dimostrazione. Sia I un ideale di $A[x]$ e C l'insieme dei coefficienti direttivi dei polinomi di I. Prima di tutto, è necessario provare che C è un ideale. Presi $c, c' \in C$ e $a \in A$, devono esistere due polinomi, $p(x)$ e $q(x)$ che hanno rispettivamente c e c' come coefficienti direttivi. Per la proprietà di ideale di I, e visto che $a \in A[x]$ inteso come polinomio di grado zero, si ha che $a * p(x) \in I$ e ha $a * c$ come coefficiente direttivo, quindi $a * c \in C$. Per dimostrare che $c - c' \in C$ si definiscono g e g' come i gradi dei polinomi $p(x)$ e $q(x)$, con ad esempio $g \geq g'$, e si definisce il polinomio $h(x) = p(x) + x^{g-g'} * q(x)$. È chiaro che $h(x) \in I$ e ha $c - c'$ come coefficiente direttivo, quindi $c - c' \in C$ e C è un ideale.
Ora invece si mostrerà che ogni elemento di I è esprimibile come una somma tra due polinomi appartenenti a due ideali finitamente generati. Siccome A è noetheriano, C è finitamente generato e si definisce $(c_i)_{i=1}^n$ una sua famiglia di generatori. Ogni generatore c_i appartiene chiaramente ad C, quindi esiste una famiglia di polinomi $(f_i)_{i=1}^n \subseteq I$ tale che f_i è di grado d_i e ha c_i come coefficiente direttivo. Si definisce $d := max_i(d_i)$ e si definisce $I' \subseteq I$ l'ideale generato dalla famiglia delle f_i. Ora si considera un polinomio generico $f \in I$ di grado r e con c come coefficiente direttivo. Nel caso in cui $r > d$ si scrive $c = \sum_{n=1}^n u_i c_i$ e si considera il polinomio $g := f - \sum_{i=1}^n u_i f_i x^{r-d_i}$, che è necessariamente di grado minore di r. Se non è ancora minore di d si ripete l'operazione, altrimenti si ha che $f = h + g$ con $h \in I'$. Si definisce M l'A-modulo generato da $1, x, x^2, ..., x^{d-1}$, che è noetheriano per 2.9, e si ha quindi $I = (I \cap M) + I'$. Per la 2.3 il sottomodulo $I \cap M$ di M è finitamente generato, quindi si può definire $(g_i)_{i=1}^m$ una famiglia di generatori di $I \cap M$. È finalmente possibile affermare che I è generato dalla famiglia finita $(f_i)_{i=1}^n \cup (g_i)_{i=1}^m$, quindi è finitamente generato. Per arbitrarietà di I, $A[x]$ è noetheriano. □

Il teorema appena dimostrato si può generalizzare per anelli di polinomi con un numero finito di variabili.

Teorema 2.14 (delle basi di Hilbert generalizzato)**.** *Dato un anello A noetheriano, $A[x_1, ..., x_n]$ è noetheriano.*

Dimostrazione. Lo si mostra applicando il principio d'induzione e il teorema in forma semplice. Il passo base è infatti mostrato nel 2.13. Si suppone ora che la tesi valga per $A[x_1, ..., x_{n-1}]$ e si mostrerà che vale anche per $A[x_1, ..., x_n]$.
Per far ciò basta replicare fedelmente i passaggi svolti nella dimostrazione precedente: per definire l'ideale C si considerano i coefficienti direttivi delle sola variabile x_n, mentre in tutti i passaggi successivi si ignorano i termini polinomiali che non la contengono. In questo modo si arriva a mostrare che $A[x_1, ..., x_n]$ è noetheriano, e che quindi lo è per ogni n. □

2.3 Anelli di Artin

Per concludere il capitolo si andrà ad analizzare la già accennata condizione delle catene discendenti e si andranno a definire gli anelli (e i moduli) artiniani. In particolare verranno presentate alcune similitudini e alcune differenze con gli anelli noetheriani e si dimostrerà il teorema di Akizuki-Hopkins-Levitzki, che evidenzia come un anello artiniano sia un caso molto particolare di anello noetheriano. Come per gli anelli noetheriani, sarà necessario enunciare alcune definizioni e alcune proprietà preliminari, iniziando dalla definizione stessa di anello artiniano.

Proposizione 2.15. *Sia dato un insieme A dotato di una relazione d'ordine $\geq$, allora le seguenti condizioni sono equivalenti:*

1. *ogni successione decrescente $x_1 \geq x_2 \geq \ldots$ contenuta in A è stazionaria, ovvero $\exists j \geq 1 \mid x_n = x_m \ \forall n, m \geq j$*
2. *Tutti i sottoinsiemi non vuoti di A hanno un elemento minimale, ovvero un elemento X per cui se $\exists Y$ tale che $Y \geq X$ allora $X = Y$*

La prima condizione è detta condizione della catena discendente, mentre la seconda condizione minimale.

Dimostrazione. La dimostrazione è analoga a quella della proposizione 2.1. □

Da questa deriva la definizione:

Definizione 2.16. *Un modulo (anello) che rispetta la d.c.c. (o l'equivalente condizione minimale) sui suoi sottomoduli (ideali) è detto* ***artiniano****.*

Apparentemente esiste una sorta di simmetria tra i moduli noetheriani e i moduli artiniani. Questo è testimoniato dal fatto che le proprietà 2.7, 2.8, 2.9, 2.10 sono verificate anche per moduli noetheriani. Inoltre anche negli anelli di Artin esiste sempre almeno un ideale massimale. Infatti se si considera l'insieme di tutti gli ideali e l'insieme di tutti i loro complementari, il secondo ha per ipotesi un elemento minimale e quindi il corrispettivo ideale è necessariamente massimale. Tuttavia una fondamentale proprietà dei moduli di Noether, la 2.3, non vale per i moduli di Artin:

Proposizione 2.17.

1. *Dato un modulo artiniano $M \not\Rightarrow$ tutti i suoi sottomoduli sono finitamente generati.*
2. *Dato un modulo M tale che tutti i suoi sottomoduli sono finitamente generati $\not\Rightarrow$ M è artiniano.*

Dimostrazione.

1. Si considerano il gruppo additivo $G := \mathbb{Q}/\mathbb{Z}$ e il suo Z-modulo associato. Si considera il sottogruppo $G' \subseteq G$ composto da tutti gli elementi con ordine p^n, dove p è un numero primo fissato e $n \geq 0$. Allora, per ogni n, esiste esattamente un sottogruppo G'_n contenente tutti gli elementi con ordine p^n. La catena ascendente $G'_0 \subset G'_1 \subset$

G'_2... non è stazionaria, quindi G non è noetheriano e per la 2.3 i suoi sottomoduli non sono finitamente generati. Inoltre i sottogruppi G'_n sono gli unici sottogruppi di G', quindi qualsiasi catena discendente è necessariamente stazionaria, ovvero G è artiniano.

2. Come già accennato, $\mathbb{Z}$ è un anello (e uno Z-modulo) noetheriano: i suoi sottomoduli sono tutti finitamente generati. Tuttavia $\mathbb{Z}$ non è artiniano in quanto la catena discendente $(a) \supset (a^2) \supset (a^3)$ ... non è stazionaria.

□

Prima di affrontare il teorema di Akizuki e quindi il cuore dell'esposizione, si presentano due proprietà interessanti degli anelli di Artin. Per far ciò è prima necessario introdurre due tipologie molto particolari di ideali:

Definizione 2.18. *Dato un anello A, un suo elemento x non nullo è detto nilpotente se esiste $n \geq 1$ tale che $x^n = 0_A$.*
L'insieme di tutti gli elementi nilpotenti è un ideale ed è chiamato nilradicale di A. Si indica con $nil\,(A)$. Si dimostra che è l'intersezione di tutti gli ideali primi di A.
L'intersezione di tutti gli ideali massimali di A è chiamato radicale di Jacobson e si indica con $rad\,(A)$.

Il radicale di Jacobson possiede la seguente caratterizzazione:

Proposizione 2.19. *$x \in rad\,(A) \iff 1 - xy$ è un'unità di A $\forall y \in A$.*

Dimostrazione. $\Rightarrow$ Si assume per assurdo che $1-xy$ non è un'unità. Necessariamente deve appartenere ad un ideale massimale m, in quanto esso genera un ideale diverso dall'anello stesso, che quindi può essere massimale o contenuto in un ideale massimale. Tuttavia $x \in m$ per ipotesi, quindi anche $xy \in m$ e $1 = (1 - xy) + (xy) \in m$, che è un assurdo. ↯
$\Leftarrow$ Si assume per assurdo che esiste un ideale massimale m di A che non contiene $1 - xy$. Allora necessariamente m e x generano l'anello stesso (per la massimalità di m) e quindi esistono $y \in m$, $a \in A$ tale che $y + ax = 1$ e quindi $1 - xy \in m$, che è un assurdo. ↯ □

Dopo questa lunga premessa, si può passare alle proposizioni vere e proprie.

Proposizione 2.20. *In un anello di Artin ogni ideale primo è massimale.*

Dimostrazione. Dato un anello A e un suo ideale primo P, la 1.9 implica che $B := A/P$ è un dominio d'integrità. Preso $x \in B$ non nullo, per la d.c.c. la catena $(x) \supset (x^2) \supset (x^2)$ ... è stazionaria, ovvero $\exists n \geq 1$ tale che $(x^n) = (x^{n+1})$. Di conseguenza $\exists y \in B$ tale che $x^n = y * x^{n+1}$ e quindi, per quanto detto finora, $1 = y * x$. Di conseguenza x ha elemento inverso in B, che è dunque un campo. Sempre per la 1.9, P è massimale. □

Una banale conseguenza è che il nilradicale e il radicale di Jacobson di A coincidono.

Proposizione 2.21. *Un anello di Artin possiede solo un numero finito di ideali massimali.*

Dimostrazione. Si consideri l'insieme formato da tutte le intersezioni finite di ideali massimali. Per ipotesi questo insieme ha un elemento minimale, indicato con $m_1 \cap ... \cap m_n$, e vale che $m \cap m_1 \cap ... \cap m_n = m_1 \cap ... \cap m_n$ per ogni m ideale massimale. Questo implica che $m \supset m_1 \cap ... \cap m_n$ e che, per la 1.10, $\exists i$ tale che $m \supset m_i$. Tuttavia sia m che m_i sono massimali, quindi $m = m_i$ e la tesi è verificata. □

Si andrà ora a dimostrare un'affermazione fatta in precedenza, ovvero che un anello artiniano è un caso particolare di anello noetheriano. Prima di poterlo fare, sono necessarie una serie di definizioni e proposizioni riguardanti sia i moduli di Artin che quelli di Noether. Si inizia con il concetto di lunghezza di un modulo, che deriva strettamente dalle condizioni della catena:

Definizione 2.22. *Data una catena ascendente o discendente priva di elementi ripetuti, il numero di simboli di inclusione è chiamato lunghezza della catena. Una catena di questo tipo è detta serie di composizione se è massimale, ovvero se è impossibile aggiungere altri sottomoduli tra due già presenti. Si afferma senza dimostrazione che se un modulo M ha una serie di composizione di lunghezza n, allora tutte le serie di composizione in M hanno la stessa lunghezza e ogni catena può essere estesa ad una serie di composizione.*[4] *Un modulo che possiede una serie di composizione è detto di lunghezza finita e la sua lunghezza è indicata con (M).*

Proposizione 2.23. *Un modulo M possiede una serie di composizione $\iff$ M Soddisfa entrambe le condizioni della catena.*

Dimostrazione. $\implies$ Tutte le catene in M hanno lunghezza finita, quindi valgono sia l'a.c.c. che la d.c.c.
$\impliedby$ La serie di composizione si costruisce come segue: M soddisfa la condizione massimale, quindi $\exists!$ M_0 sottomodulo massimale di M che a sua volta è noetheriano e contiene M_1 sottomodulo massimale. Continuando in questo modo si ottiene la catena discendente $M \subset M_0 \subset M_1 \subset M_2$.... Per la d.c.c. questa catena ha lunghezza finita e per costruzione è necessariamente una serie di composizione. □

Proposizione 2.24. *La lunghezza di un A-modulo è una funzione additiva nella classe degli A-moduli di lunghezza finita*

Dimostrazione. Considerando la sequenza esatta corta $0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$, l'obiettivo è mostrare che $l(M) = l(M') + l(M'')$. Chiamate X' e X'' le serie di composizione di M' e M'', la serie di composizione di M, detta X, è $\alpha(X') \cup \beta(X'')$. Infatti tutti i sottomoduli che compongono X' hanno come immagine un sottomodulo di Mcontenuto in $Ker(\beta)$. Al contrario, tutti i sottomoduli che compongono X'', e che quindi contengono $0_{M''}$, hanno come controimmagine un sottomodulo che contiene $Ker(\beta)$. Inoltre X' ha come elemento massimale M' stesso, mentre X'' ha come elemento minimale $0_{M''}$. Per ipotesi $\alpha(M') = Ker(\beta) = \beta^{-1}(0_{M''})$, quindi si può visualizzare X come una catena crescente composta prima da tutti gli elementi di X' e poi da tutti gli elementi di X'',

[4] *La dimostrazione si trova sul I.G. MacDonald [1994], proposizione 6.7*

con $Ker(\beta)$ che fa da separatore. Se per assurdo si potesse aggiungere un sottomodulo $M*$ a X allora la sua immagine o la sua controimmagine si potrebbe inserire in X' o X'' rispettivamente, ma ciò va contro le ipotesi. □

Proposizione 2.25. *Dato uno spazio vettoriale V, le seguenti condizioni sono equivalenti:*

- *Dimensione di V finita;*
- *Lunghezza di V finita;*
- *A.c.c.;*
- *D.c.c.;*

Inoltre, se una di queste è verificata, $dim(V) = l(V)$.
Tenendo a mente la 2.23, la dimostrazione è triviale in quasi tutti i suoi passaggi. Le implicazione $3 \Rightarrow 1$ e $4 \Rightarrow 1$ si dimostrano per assurdo. Se esistessero infiniti generatori, allora la catena crescente degli spazi generati da un numero crescente di generatori non sarebbe stazionaria, così come la catena discendente dei loro complementari.

Ora invece si approfondiranno due concetti importanti riguardanti i moduli. Il primo è un metodo per costruire dei particolari tipi di ideali e sottomoduli, mentre il secondo è noto come il lemma di Nakayama.

Definizione 2.26. *Dato un anello A, un A-modulo M e due suoi sottomoduli N e N', si definisce l'insieme $\{a \in A | an' \in N,\ \forall n' \in N'\}$. Questo insieme è un ideale di A e si indica con $(N : N')_A$. In particolare si definisce l'ideale $(0 : M)_A$ come l'annihilator di A e lo si indica con $ann(A)$. Allo stesso modo, dato un ideale I di A si può definire il sottomodulo $\{x \in M | xy \in N,\ \forall y \in I\}$ diM, che viene indicato con $(N : I)_M$.*

Proposizione 2.27 (Lemma di Nakayama)**.** *Dato un anello A, un A-modulo M finitamente generato e un ideale I di A contenuto in $rad(A)$, allora se $IM = \{y*m | y \in I, m \in M\} = M$ si ha che $M = 0$.*

Dimostrazione. Supponendo $M \neq 0$ e generato dalla famiglia minimale $(x_i)_{i=1}^n$, grazie all'ipotesi fatta si può scrivere che $x_n = \sum_{i=1}^n a_i x_i$, con $a_i \in I\ \forall i$. Sistemando i termini si arriva a $(1 - a_n) x_n = \sum_{i=1}^{n-1} a_i x_i$: dalla 2.19 si ottiene che $1 - a_n$ è un'unità di A e che quindi x_n è una combinazione lineare degli $(x_i)_{i=1}^{n-1}$. Ciò è un assurdo. ↯ □

Una conseguenza importante di questo lemma è la seguente: dato un A-modulo M finitamente generato, un suo sottomodulo N e un ideale I di A tale che $I \subseteq rad(A)$, allora $M = IM + N$ implica che $M = N$.

Dimostrazione. La dimostrazione si basa sul mostrare che $I(M/N) = M/N$ per poter applicare il lemma precedente e concludere che $M = N$. Preso un elemento generico di M/N, questo è nella forma $m + N$, con $m \in M$ quindi l'elemento generico di $I(M/N)$ è $Im + N$. Inoltre $IM/N = (IM + N)/N$, in quanto il sottomodulo somma ha come elementi le somme finite di elementi di IM e N e queste, quando sono proiettate sullo spazio quoziente, diventano gli elementi di M/N. Quindi $I(M/N) = M/N$ e di conseguenza $M/N = 0$, ovvero $M = N$ □

Ora tutto è pronto per enunciare e dimostrare il seguente:

Teorema 2.28 (Akizuki-Hopkins-Levitzki)**.** *Un anello artiniano è noetheriano*

Dimostrazione. Dato un anello artiniano A, per la 2.21 possiede solo un numero finito di ideali massimali $\{m_i\}_{i=1}^r$. Si definisce $I := rad(A) = \cap_{i=1}^r m_i$; per la d.c.c. la catena discendente $I \supset I^2 \supset ...$ è stazionaria, ovvero $\exists s \geq 1$ tale che $I^s = I^{s+1}$. Inoltre si definisce $J := Ann(I^s) = Ann(I^{s+1})$. L'obiettivo è dimostrare che $J = A$ e lo si fa per assurdo. Se infatti si assume che $J \neq A$, allora l'insieme di tutti gli ideali che contengono J ha per ipotesi un elemento minimale, detto J', che per la sua minimalità è nella forma $J' = Ax+J$, dove $x \in J' - J$ arbitrario. Ovviamente $J' \neq J$, quindi per il corollario del 2.27 si ha che $J' \neq Ix + J$. Ma sfruttando nuovamente la minimalità di J' si ottiene che $J = Ix + J$ e di conseguenza $Ix \in J$, ovvero che $x \in (J : I)_A = ((0 : I^s)_A : I)_A = (0 : I^{s+1})_A = J$. Ma ciò va contro le ipotesi fatte su x, quindi si è arrivati ad un assurdo e dunque $J = A$, che a sua volta implica che $I^s = 0$. Ora è possibile costruire la catena discendente $A \supset m_1 \supset m_1m_2 \supset ... \supset I \supset Im_1 \supset ... \supset I^2 \supset ...I^s = 0$. La prima cosa da notare è che prendendo due elementi consecutivi M e Mm_i, il quoziente M/Mm_1 è uno spazio vettoriale su A/m_i. La verifica è immediata in quanto A/m_i è un campo per la 1.9 e l'applicazione $\varphi(a + m_i, x + Mm_i) = ax + Mm_i \ \forall a \in A, x \in M$ rispetta tutte le proprietà necessarie per rendere M/Mm_i un A/m_i-modulo, ergo uno spazio vettoriale. Dalla 2.25 è noto che in uno spazio vettoriale vale la relazione *a.c.c.* $\iff$ *d.c.c.* e ora si dimostrerà che M/Mm_i è artiniano (noetheriano)$\iff$ lo è anche A. Costruendo la sequenza esatta corta $0 \to m_1 \xrightarrow{\alpha} A \xrightarrow{\beta} A/m_1 \to 0$, con α funzione identità e β proiezione naturale, si deduce dalla 2.7 che sia m_1 che A/m_1 sono artiniani. Ripetendo questo passaggio per ogni M e Mm_i si ottiene che ogni elemento della catena è artiniano e, per quanto detto, anche noetheriano. A questo punto si definisce la sequenza esatta corta $0 \to I^s \xrightarrow{\alpha} I^{s-1}\prod_{i=1}^{r-1} m_i \xrightarrow{\beta} I^{s-1}\prod_{i=1}^{r-1} m_i/I^s \to 0$ e sempre dalla 2.7 si deduce che $I^{s-1}\prod_{i=1}^{r-1} m_i$ è noetheriano[5]. Ripetendo questo passaggio "risalendo" la catena si arriva ad affermare che A è noetheriano. □

Questa dimostrazione per anelli commutativi è da attribuire ad Akizuki, mentre la forma più generali per anelli non commutativi è stata trovata da Hopkins e Levitzki

[5] $I^s = 0$, quindi è noetheriano

Capitolo 3

Il Nullstellensatz di Hilbert

Come accennato nell'introduzione, questa esposizione termina con l'introduzione dei concetti che stanno alla base della geometria algebrica. In questo capitolo verranno introdotte le varietà algebriche e enunciato il Nullstellensatz, ovvero il teorema degli zeri di Hilbert. Tra le molte versioni equivalenti, è stato scelto di enunciare e dimostrare quella presente sul I.G. MacDonald [1994], in quanto la sua dimostrazione sfrutta alcune proposizioni che discendono quasi direttamente da quanto fatto nel capitolo precedente, in particolare dal 2.14. In preparazione alla dimostrazione verranno inoltre enunciati il teorema di Artin-Tate e il lemma di Zariski.

3.1 Introduzione ed enunciato

Prima di introdurre gli oggetti di studio di questo ramo della matematica, è necessario definire una nuova struttura algebrica, leggermente più complessa dei moduli e degli anelli.

Definizione 3.1. *Dati due anelli A e B e un omomorfismo di anelli $\varphi : A \to B$, è possibile definire un prodotto $A \times B \to B$ che lega due elementi $a \in A$ e $b \in B$ all'elemento $\varphi(a)\, b$. Tramite φ e la sua operazione di addizione, B è un A-modulo. Notare che per ipotesi $a(xy) = (ax)\, y = x(ay)$.*
Date queste condizioni, B è detto A-algebra.
Se gli elementi di B sono riscrivibili in forma di un polinomio in $x_1, ..., x_n$ a coefficienti in $f(A)$, si dice che B è finitamente generato.

Come per gruppi, anelli e moduli, si definisce l'omomorfismo tra algebre:

Definizione 3.2. *Dato un anello A e due A-algebre B e C, un'applicazione $f : B \to C$ è detta omomorfismo tra A-algebre se è un omomorfismo tra B e C sia intesi come anelli che come moduli.*

Siccome un'algebra è costruita su un modulo, molte delle definizioni e proprietà viste nei capitoli precedenti valgono anche per queste nuove strutture. In particolare, la noetherianità di un algebra rispetta la seguente proposizione:

Proposizione 3.3. *Dato un anello noetheriano A e un A-algebra B finitamente generata, B è noetheriana.*

Dimostrazione. La definizione data di algebra finitamente generata è equivalente alla seguente: una A-algebra è finitamente generata da n generatori se e solo se esiste un epimorfismo da $A[t_1, ..., t_n]$ in B entrambe intese come A-algebre .
La dimostrazione deriva direttamente da questa definizione alternativa. □

Conclusa questa premessa, si può proseguire ed entrare nel mondo della geometria algebrica. Questa disciplina ha tra i suoi fondamenti lo studio di una struttura algebrica molto precisa: la *varietà algebrica*. Prima di arrivare alla sua definizione, però, è necessario richiamarne un'altra altrettanto importante.

Definizione 3.4. *Un campo K è detto algebricamente chiuso se ogni polinomio non costante incluso in $K[x]$ ha soluzioni in K.*

Il campo dei numeri reali è notoriamente non chiuso, in quanto ad esempio il polinomio $x^2 + 1$ non ha soluzioni in $\mathbb{R}$. Al contrario il campo dei complessi è algebricamente chiuso.

Definizione 3.5. *Dato un campo algebricamente chiuso K, un anello di polinomi in n variabili $K[x_1, ..., x_n]$ e un suo ideale S, l'insieme delle soluzioni comuni a tutti i polinomi in S è detta varietà algebrica definita su S , in simboli:*

$$V \;=\; \{y = (y_1, ..., y_n) \in K^n \mid f(y) = 0 \;\forall y \in S\}$$

.

Contrariamente a quanto fatto per i teoremi precedente, verrà inizialmente dato solo l'enunciato del Nullstellensatz di Hilbert. Dopodichè saranno presentate una serie di proposizioni che forniranno tutti gli strumenti necessari per una completa dimostrazione. Verrà inoltre presentato un corollario di grande importanza, a cui spesso si fa riferimento con il nome di Nullstellensatz debole.

Teorema 3.6 (Nullstellensatz forte)**.** *Siano dati un campo algebricamente chiuso K, l'anello di polinomi $A := K[x_1, ..., x_n]$, un suo ideale S e la varietà algebrica V definita su S. Si definisce $I(V)$ l'ideale di tutti i polinomi in A che si annullano per ogni elemento di V. Allora $V(I) = r(S)$* [1]

Dimostrazione. È chiaro che $r(S) \subseteq V(I)$ in quanto, preso un polinomio $p \in r(S)$, si ha che $p^n \in S$ (ovvero che $p(x)^n = 0$) per qualche n e per ogni elemento $x \in V$. Ciò significa che $p(x) = 0 \;\forall x \in V$ e quindi $p \in I(V)$.
Come già accennato, per dimostrare l'inclusione opposta è necessario approfondire ulteriormente la teoria delle algebre. □

[1] *vedi 1.7*

3.2 Dimostrazione del Teorema

In questa sezione verranno presentate due proposizioni in preparazione alla dimostrazione del Nullstellensatz forte. In particolare, la seconda ha come corollario il cosiddetto Nullstellensatz debole che, oltre ad avere una propria importanza, sarà la chiave della dimostrazione della versione forte.

Proposizione 3.7. *Dati tre anelli A, B e C tali che $A \subseteq B \subseteq C$, se valgono le ipotesi:*

- *A è noetheriano;*
- *C finitamente generato come A-algebra e come B-modulo;*

allora B è finitamente generato come A-algebra.

Dimostrazione. Si ipotizza che la famiglia $\{x_i\}_{i=1}^n$ generi C come A-algebra e che la famiglia $\{y_i\}_{i=1}^m$ generi C come B-modulo. Dalla 1.22 è noto che vale la seguente: $x = \sum_{j=1}^m b_j y_j$, con $b_j \in B \ \forall x \in B$. In particolare questa relazione vale anche per gli elementi della famiglia $\{x_i\}_{i=1}^n$ e gli elementi nella forma $y_i y_j \in C \forall i, j$. Riassumendo:

1. $x_i = \sum_{j=1}^m b_{i,j} y_j$;
2. $y_i y_j = \sum_{k=1}^m b_{i,j,k} y_k$

Si può ora definire la A-algebra generata da tutti i $b_{i,j}$ e tutti i $b_{i,j,k}$, verrà indicata con B_0. Dalla 3.3 si deduce che B_0 è noetheriano e dalle ipotesi vale che $A \subseteq B_0 \subseteq B$, inoltre C è finitamente generato come B-modulo quindi per definizione ogni suo elemento può essere scritto come polinomio in $y_1, ..., y_m$. In simboli $c = \sum_{j \geq 1} \sum_{i=1}^m a_{i,j} y_i^j, \ \forall x \in C$. Sostituendo prima la relazione 1 e poi la 2 per un il numero necessario di volte, si ottiene che ogni elemento di C è esprimibile come combinazione lineare degli elementi della famiglia $\{y_i\}_{i=1}^m$ a coefficienti in B_0, ovvero che C è finitamente generato come B_0-modulo. Siccome B_0 è noetheriano, la 2.9 implica che anche C lo è, quindi ogni suo sottomodulo, tra cui B stesso, è finitamente generato come B_0-modulo. Da questo consegue che B è anche finitamente generato come A-algebra[2]. □

Su alcuni di testi quest'ultima proposizione prende il nome di *teorema di Artin-Tate*, in onore dei due matematici che lo hanno dimostrato.
Prima di procedere con l'enunciato successivo è necessario ricordare alcune definizioni importanti riguardanti le estensioni di campi.

Definizione 3.8. *Dati due campi A e B, si dice che B è un'estensione di A se esiste un monomorfismo di campi, detto immersione, da A in B. In tale caso, si indica con $B|A$.*
La dimensione di B come spazio vettoriale su A è detta grado dell'estensione. Un elemento di B è detto algebrico su A se è radice di un polinomio non banale a coefficienti in A, altrimenti è detto trascendente.
Se ogni elemento di B è algebrico su A allora l'estensione è detta algebrica.

[2]Per dimostrare quest'ultimo passaggio si scrive ogni elemento di B come combinazione dei suoi generatori con coefficienti in B_0, e si sfrutta il fatto che B_0 è finitamente generato come A-algebra

Si può ora passare all'ultima proposizione preliminare.

Proposizione 3.9 (Lemma di Zariski)**.** *Dato un campo K e una K-algebra E finitamente generata, se E è un campo allora è un estensione algebrica finita di K.*

Cenni di dimostrazione. Questo lemma può essere dimostrato sia per assurdo che per induzione. Nel primo caso si assume che E non sia algebrico su K. Da questo segue che è possibile costruire un campo diverso da K su cui E è algebrico e sfruttando la 3.7 si arriva ad una contraddizione. Alternativamente si può procedere per induzione sugli n generatori di E. Il caso $n = 1$ è semplice, mentre per il passo induttivo si fa nuovamente uso del ragionamento per assurdo. Entrambe le strade avrebbero richiesto la definizione di altri concetti preliminari e per questo non saranno approfondite oltre. □

Da questo lemma segue direttamente:

Teorema 3.10 (Nullstellensatz debole)**.** *Dato un campo K, una K-algebra A finitamente generata e un ideale massimale m di A, il campo A/m è un'estensione algebrica finita di K. In particolare, se K è algebricamente chiuso allora A/m è isomorfo a K.*

Dimostrazione. Come accennato, questo teorema è un'immediata conseguenza della proposizione precedente, in quanto ne rappresenta un caso particolare. Infatti prendendo $E = A/m$ gli enunciati diventano uguali. □

Ora che tutti i preparativi sono stati fatti si può riprendere la dimostrazione lasciata a metà nella sezione precedente.

Dimostrazione. Si ricorda che si deve mostrare l'inclusione $I(V) \subseteq r(S)$.
Si considera per assurdo un polinomio $f \in I(V)$ che non appartiene a $rad(S)$. Per definizione del radicale di S esiste un ideale primo P contenente S ma non f. Si indica con f' l'immagine di f rispetto alla proiezione naturale di A su $B := A/P$ e con C l'insieme $B[1/f']$. C è una K-algebra finitamente generata in quanto ogni suo elemento è un polinomio con $1/f'$ come incognita e a coefficienti in B. Se φ è l'omomorfismo che rende A una K-algebra e π è la proiezione naturale su B, la loro composizione è un omomorfismo che rende C una K-algebra finitamente generata. Considerando un ideale massimale di C, detto m, dal 3.10 si ha che C/m è isomorfo a K. Le immagini dei generatori di A in C/m formano un punto $t := (t_1, ..., t_m) \in K^n$ e per costruzione vale che $t \in V$ e $f(t) \neq 0$, che è un assurdo. ↯

□

Bibliografia

D. Berlyne E. Noether. Idealtheorie in ringbereichen (ideal theory in rings), 1921. URL https://arxiv.org/pdf/1401.2577.pdf.

D. Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*. Springer-Verlag, 1995.

M. Reid H. Matsumura. *Commutative ring theory*. Cambridge University Press, 1989.

M.F. Atiyah I.G. MacDonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Company, 1994.