UNIVERSITÀ DEGLI STUDI ROMA TRE
FACOLTÀ DI S.M.F.N.

Sintesi della tesi di Laurea in Matematica
di

Daniela Ricci

Anelli di interi algebrici metà-fattoriali

Relatore
Prof.ssa Stefania Gabelli

ANNO ACCADEMICO 2001 - 2002
LUGLIO 2002

Classificazione AMS: 11R04, 11R11, 13F15
Parole chiave: interi algebrici, domini di Dedekind, domini atomici

Sintesi

La maggior parte dei problemi della teoria dei numeri algebrici sorge dalla mancanza di fattorizzazione unica degli interi algebrici. Un modo rivoluzionario di compensare questa deficienza fu trovato da Kummer e da Dedekind, i quali spostarono lo studio della fattorizzazione dagli elementi agli ideali. In questi ultimi anni, si è verificato un crescente interesse nella fattorizzazione dei numeri stessi e il metodo principale in questo studio è proprio la teoria degli ideali di Dedekind. Recentemente sono state studiate proprietà di fattorizzazione più deboli di quella unica; in particolare, nel 1960, Carlitz ha definito gli half-factorial-domains (HFD).

Definizione 0.1. *Un anello R è detto* ***dominio metà-fattoriale (HFD,*** *per* ***half-factorial-domain****), se sono verificate le seguenti due condizioni:*
($\exists$) Ogni $a \in R$, non nullo e non invertibile, è prodotto di elementi irriducibili di R.
(!) Date comunque due fattorizzazioni di a

$$a = \pi_1 \dots \pi_n = \xi_1 \dots \xi_m$$

con π_i e ξ_j irriducibili, allora $n = m$.

Scopo di questo lavoro è di studiare alcune proprietà di fattorizzazione degli anelli di interi algebrici, individuando la stretta connessione tra queste proprietà e la struttura algebrica del gruppo delle classi. La parte principale riguarda lo studio degli ordini di anelli di interi algebrici che sono HFD.

Definizione 0.2. *L'**anello degli interi algebrici** di un campo numerico K, denotato con $\mathcal{O}_K$, è l'insieme degli elementi di K che sono radici di qualche polinomio monico a coefficienti in $\mathbb{Z}$, ovvero:*

$$\mathcal{O}_K = \{\alpha \in K : \quad \exists h(x) \in \mathbb{Z}[x] \quad t.c. \quad h(\alpha) = 0\}$$

Nel primo capitolo abbiamo ricordato alcune proprietà degli anelli di interi algebrici (*traccia*, *norma*, *discriminante* e esistenza di *basi intere*).

Lo scopo del secondo capitolo è stato quello di caratterizzare i Domini di Dedekind, indicati con $\mathfrak{D}$, attraverso le proprietà moltiplicative dei loro ideali.

Definizione 0.3. *Un dominio D è detto **dominio di Dedekind** se soddisfa le seguenti proprietà equivalenti:*

- *D è noetheriano, integralmente chiuso e ogni ideale primo non nullo di D è massimale.*
- *Ogni ideale frazionario non nullo di D è invertibile.*
- *Ogni ideale non nullo di D può essere scritto in modo unico come prodotto di ideali primi.*

Invertendo la strada percorsa da Dedekind, abbiamo dimostrato che $\mathcal{O}_K$ è un dominio di Dedekind. Avendo osservato che in un dominio di Dedekind l'insieme degli ideali frazionari è un gruppo, è stato poi possibile definire il *gruppo delle classi*:

Definizione 0.4. *Siano $\mathscr{F}$ il gruppo degli ideali frazionari di $\mathfrak{D}$ e $\mathscr{P}$ il suo sottogruppo degli ideali principali frazionari. Allora il* ***gruppo delle classi*** *di $\mathfrak{D}$ è il gruppo quoziente*

$$\mathscr{C} = \mathscr{F}/\mathscr{P}.$$

Chiamiamo ***numero delle classi*** *$h = h(\mathfrak{D})$, l'ordine di $\mathscr{C}$.*

Grazie alla definizione di *norma di un ideale* di $\mathcal{O}_K$ ci è stato possibile dimostrare un importante teorema dovuto a Minkowski; che ci garantisce la finitezza del gruppo delle classi di $\mathcal{O}_K$.

Il terzo capitolo costituisce il fulcro di questa tesi; si divide in due parti: la prima tratta i domini a fattorizzazione unica (UFD), soprattutto da un punto di vista storico, mentre la seconda si concentra sullo studio dei domini metà-fattoriali (HFD).
Inzialmente, abbiamo cercato di individuare le cause della nascita dello studio degli UFD, sottolineando gli errori che storicamente costrinsero la comunità matematica a rendersi conto che non tutti i domini hanno le stesse proprietà fattoriali di $\mathbb{Z}$.
Quindi sezionando la definizine di UFD, abbiamo, dapprima, studiato l'eventuale esistenza in un dominio della fattorizzazione in elementi irriducibili; definendo *atomico* un dominio in cui ogni elemento non nullo e non invertibile è fattorizzabile in irriducibili. Non ci è stato difficile notare che $\mathbb{I}$, l'anello di tutti gli interi algebrici, non è atomico, mentre $\mathcal{O}_K$ lo è, dato che è noetheriano. In un secondo momento al fine di studiare l'unicità della fattorizzazione,

abbiamo mostrato degli esempi di domini atomici non UFD.

Teorema 0.5. *La fattorizzazione in irriducibili non è unica in* $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ *per (almeno) i seguenti valori di* d*:*

$$10, 15, 26, 30,$$
$$-5, -6, -10, -13, -14, -15, -17, -21, -22, -23, -26, -29, -30.$$

I valori di d fissati nel precedente teorema sembrano essere casuali, ma non è così. Infatti, guardiamo per quali valori di d, il dominio $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ è un UFD.

- Per $d < 0$, A. Backer e H. M. Stark hanno dimostrato che $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ è un UFD se e soltanto se

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

- Se invece $d > 0$, resta irrisolta la celebre congettura di Gauss, secondo cui $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ è un UFD per infiniti valori di d. È noto che gli interi d, con $1 < d < 100$, per cui è possibile la fattorizzazione unica sono tutti e soli i seguenti:

$$2, 3, 5, 6, 7, 11, 13, 14, 17, 19, 21, 22, 23, 29, 31, 33, 37, 38, 41, 43, 46, 47,$$

$$53, 57, 59, 61, 62, 67, 69, 71, 73, 77, 83, 86, 89, 93, 94, 97.$$

Siamo quindi passati ad uno studio più rigoroso degli UFD, caratterizzando i domini di Dedekind che sono UFD attraverso il gruppo delle classi.

Teorema 0.6. *Sia $\mathfrak{D}$ un dominio di Dedekind, $\mathfrak{D}$ è un UFD se e soltanto se $\mathfrak{D}$ è un dominio ad ideali principali, ovvero il numero delle classi h è uguale a 1.*

Abbiamo concluso la prima parte del terzo capitolo notando che il gruppo delle classi di un dominio è la misura della non unicità della fattorizzazione dello stesso: più è grande il numero delle classi, più il dominio sarà distante dall'essere un UFD.

Siamo così arrivati alla parte centrale della tesi, ovvero ai domini metà-fattoriali (HFD, da half-factorial-domains): un dominio atomico D è un HFD se due fattorizzazioni di un qualsiasi elemento in D, in fattori irriducibili, hanno la stessa lunghezza. A differenza degli UFD, gli HFD possono anche non essere integralmente chiusi. Quindi abbiamo suddiviso il nostro studio in due parti. Nel caso integralmente chiuso abbiamo mostrato un fondamentale teorema del 1960 dovuto a Carlitz [Cz]:

Teorema 0.7 (Carlitz, 1960). *$\mathcal{O}_K$ è un HFD se e soltanto se il suo numero delle classi è minore o uguale a due.*

Per fornire esempi di anelli di interi algebrici HFD, abbiamo dato una formula per il calcolo del numero delle classi degli anelli di interi algebrici di campi quadratici. Grazie a questa formula è stato possibile compilare una tabella nella quale al variare di $\mathbf{d}$, $\mathbf{h}$ indica il numero delle classi di $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, mentre $\mathbf{h}'$ indica il numero delle classi di $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$.

d	h	h′	d	h	h′	d	h	h′	d	h	h′	d	h	h′
1	-	1	21	1	4	41	1	8	65	2	8	85	2	4
2	1	1	22	1	2	42	2	4	66	2	8	86	1	10
3	1	1	23	1	3	43	1	1	67	1	1	87	2	6
5	1	2	26	2	6	46	1	4	69	1	8	89	1	12
6	1	2	29	1	6	47	1	5	70	2	4	91	2	2
7	1	1	30	2	4	51	2	2	71	1	7	93	1	4
10	2	2	31	1	3	53	1	6	73	1	4	94	1	8
11	1	1	33	1	4	55	2	4	74	2	10	95	2	8
13	1	2	34	2	4	57	1	4	77	1	8	97	1	4
14	1	4	35	2	2	58	2	2	78	2	4			
15	2	2	37	1	2	59	1	3	79	3	5			
17	1	4	38	1	6	61	1	6	82	4	4			
19	1	1	39	2	4	62	1	8	83	1	3			

Siamo quindi passati allo studio degli HFD non integralmente chiusi. E' stato necessario premettere le definizioni di *ordine* di un anello di interi algebrici e di *conduttore* di un ordine.

Definizione 0.8. *Sia K un campo quadratico e $\mathcal{O}_K$ il relativo anello degli interi algebrici.*
(1) Un ***ordine*** *A in K è un sottoanello di $\mathcal{O}_K$, che è uno $\mathbb{Z}$-modulo libero di rango 2.*
(2) Il ***conduttore*** *di A è il più piccolo intero f tale che $f\mathcal{O}_K \subseteq A$.*

L'analisi degli HFD non integralmente chiusi si basa su un teorema di Halter-Koch [H.K.].

Teorema 0.9 (Halter-Koch, 1983). *Sia A un ordine in un campo quadratico K e $f \neq 1$ il suo conduttore. Allora le seguenti condizioni sono equivalenti:*
(1) A è un HFD.

(2) $\mathcal{O}_K$ è un HFD, $\mathcal{O}_K = AU(\mathcal{O}_K)$ e f è un primo o due volte un primo dispari.

Il teorema di Halter-Koch ci ha permesso di dare alcuni esempi di ordini quadratici immaginari che sono HFD:

Corollario 0.10. *Supponiamo $d \in \mathbb{N}$, $d \leq 100$. Allora $\mathbb{Z}[\sqrt{-d}]$ è un HFD se e soltanto se d è uno dei seguenti interi:*

$$1, 2, 3, 5, 6, 10, 13, 22, 37, 58.$$

Un risultato più significativo ci è offerto, però, da Coykendall [Co].

Teorema 0.11 (Coykendall, 2001). *L'anello $\mathbb{Z}[\sqrt{-3}]$ è l'unico HFD quadratico immaginario non integralmente chiuso.*

Analogamente agli UFD, il caso reale è ben più complicato. Anche soltanto considerando il Teorema(0.9) ci rendiamo conto che il numero di ordini di interi quadratici che sono HFD è più alto. Halter-Koch stesso ci mostra questo:

Esempio: Supponiamo $2 \leq d \leq 100$, allora $\mathbb{Z}[\sqrt{d}]$ è un HFD ma non un UFD se e soltanto se d è uno dei seguenti numeri interi: 5, 10, 12, 13, 15, 18, 21, 26, 29, 30, 34, 35, 39, 42, 44, 45, 50, 51, 53, 55, 58, 61, 66,69, 70, 74, 76, 77, 78, 84, 85, 87, 91,93, 95.

Coykendall, recentemente, ha cercato di spingersi oltre, non ottenendo però i risultati sperati. Egli cerca in [Co] condizioni necessarie e sufficienti affinché un ordine di un campo quadratico possa essere un HFD. Il risultato più importante che ottiene in questo senso ci dice che un ordine di un campo quadratico è un HFD se e soltanto se la sua chiusura integrale è un HFD e ogni irriducibile nell'ordine è irriducibile anche nella chiusura integrale. Questo teorema e i suoi corollari ci mostrano che nel caso quadratico reale, gli HFD non integralmente chiusi devono essere scelti in un particolare sottoinsieme degli ordini quadratici in generale. Prima di tutto, devono essere sottoanelli di interi algebrici con la proprietà di essere HFD (cioè il loro numero delle classi non deve essere superiore a due). Inoltre, l'indice n, deve essere uguale a p oppure a $2p$, dove p è primo sia nell'ordine che nella sua chiusura integrale.

L'ovvia domanda a cui chiunque vorrebbe rispondere è: "Esiste un numero infinito di HFD reali quadratici?". Se ci restringiamo al caso integralmente chiuso, allora abbiamo un problema che è una generalizzazione della congettura di Gauss sull'esistenza di un numero infinito di UFD reali. Quindi il problema di provare l'esistenza di un numero infinito di HFD reali (nel caso integralmente chiuso) incontra le stesse difficoltà della congettura di Gauss. Più in generale, nel caso non integralmente chiuso il problema non è stato comunque risolto, ma Coykendall ci mostra alcuni esempi mirati a dare evidenza empirica al fatto che esistano effettivamente infiniti HFD reali.

Perciò conclude in questo modo: "*We conjecture that in the real quadratic case, there is an infinite number of HFDs*" [Co](pag.429).

Riferimenti bibliografici

[A.M.] Atiyah M.F., Macdonald I.G.: *Introduzione all'algebra commutativa* (con appendice di A. Maroscia), Feltrinelli (1981).

[B.S.] Borevic Z. I., Safarevic I.R.:*Number theory*, Academic Press, New York (1966).

[Cz] Carlitz L.: A characterization of algebraic number fields with class number two, *Proc. Amer. Math. Soc.* **11**(1960), 391-2.

[C.Co.] Chapman S. T., Coykendall J.: Half-factorial domains, a survey, *Non-noetherian commutative ring theory* (Chapman & Glaz eds.), Kluwer Academic Publisher, Dordrecht, NL (2001).

[Co] Coykendall J.: Half-factorial domain in quadratic fields, *Journal of Algebra* **235**, 417-430 (2001).

[F1] Fontana M.: *Una introduzione ad alcuni argomenti della teoria algebrica dei numeri*, Appunti del corso di Istituzioni di Algebra Superiore, A.A. 1980/1981, Università *La Sapienza* di Roma

[Gi] Gilmer R.: *Multiplicative ideal theory*, Marcel Dekker, inc. New York (1972).

[Gr] Grosswald E.: *Topics from the theory of numbers*, Birkhäuser, Boston (1984).

[H.K.] Halter-Koch F.: Factorization of algebraic integers, *Ber. Math. Stat. Sketion im Forschungszentrum* **191** (1983).

[J] Janusz G. J., *Algebraic number fields*, Academic Press, New York (1973).

[M] Marcus D.: *Number fields*, Springer, New York (1995).

[Mo] Mott J. L.: Groups of divisibility: a unifyng concept for integral domains and partially ordered groups, *Lattice-ordered groups, advances and techniques* (H. W. Glasses & W. Charles Holland eds.), Kluwer Academic Publisher, Dordrecht, NL (1989).

[N] Narkiewicz W.: *Elementary and analytic theory of algebraic numbers*, Warszawa (1974).

[P.D.] Pollard H., Diamond H.G.: *The theory of algebraic numbers*, The mathematical association of America (1975).

[R] Ribenboim P.: *Classical theory of algebraic number*, Springer (2001).

[S.T.] Stewart I.,Tall D.: *Algebraic number theory*, Chapman & Hall, London (1987).

[S] Stilwell J.: What are Algebraic integers and what are they for?, *Amer. Math. Montly* **101** (1994).

[Z1] Zaks A.: Half-factorial domains. *Bull. Amer. Math. Soc.* **82** (1976), 721-723.

[Z2] Zaks A.: Half-factorial domains. *Israel J. Math.* **37** (1980), 281-302.