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

Sintesi della
Tesi di Laurea in Matematica
presentata da

Alessandro Russo

Proprietà di fattorizzazione per anelli di interi algebrici e gruppo delle classi

Relatore

Prof.ssa Francesca Tartarone

ANNO ACCADEMICO 2005 - 2006
Luglio 2006

Classificazione AMS : 11R04, 11R11, 13F15,
Parole Chiave : FATTORIZZAZIONI, ANELLO DEGLI INTERI, DOMINI DI DEDEKIND, GRUPPO DELLE CLASSI IDEALI.

Sintesi

Un discreto numero di scoperte nell'ambito della Matematica sono avvenute in maniera del tutto casuale, durante lo studio di problemi che avevano scarsa attinenza coi risultati conseguiti. La teoria dei numeri algebrici (e più implicitamente la *teoria della fattorizzazione*), nacque a seguito dei molteplici e invani tentativi, da parte dei matematici del tempo, di dimostrare l'Ultimo Teorema di Fermat. E' il caso di Ernst Eduard Kummer (1810-93), un allievo di Gauss e di Dirichlet che era passato dalla teologia alla matematica e che diventò in seguito professore a Berlino. Nel 1843, Kummer aveva dato definizioni appropriate di numero intero, di numero primo, di relazioni di divisibilità, ma commise l'errore di assumere che nella classe dei numeri algebrici (che ebbe il merito di introdurre) valesse la fattorizzazione unica. Tale assunzione era necessaria per dimostrare il teorema di Fermat. Quando si accorse che ciò non era sempre vero, per ristabilire la fattorizzazione unica, Kummer creò allora una teoria relativa ai *numeri ideali*; essi, pur non essendo definiti in maniera generale, gli servirono a verificare l'enunciato di Fermat per un centinaio di numeri primi.
Contemporaneamente, Richard Dedekind (1831-1916) si accostò al problema della fattorizzazione unica in maniera completamente nuova ed originale. Dopo aver generalizzato la nozione di numero algebrico, egli si accinse a restaurare la fattorizzazione unica nei campi di numeri algebrici e, successivamente, in una classe di domini che li generalizzano (detti, appunto, domini di Dedekind) mediante un procedimento del tutto diverso da quello di Kummer. In luogo dei numeri ideali egli introdusse delle classi di numeri algebrici che chiamò *ideali* in onore dell'opera svolta dal suo collega. Tali oggetti rappresentano gli strumenti che hanno permesso di stabilire, nell'arco del XX secolo, una vera e propria teoria sulla fattorizzazione unica.

In questo lavoro abbiamo esaminato alcune proprietà di fattorizzazione degli anelli di interi algebrici (sulla base dei risultati che Kummer e Dedekind ci hanno lasciato in eredità), individuando la stretta connessione tra queste proprietà e la struttura algebrica del gruppo delle classi.

Nel primo capitolo, abbiamo cominciato col richiamare la definizione di *anello degli interi algebrici*, e più in generale di *dominio di Dedekind*.

- *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:*

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

- *Un dominio R è detto dominio di Dedekind se è noetheriano, integralmente chiuso ed ogni ideale primo non nullo di R è massimale.*

Abbiamo verificato che per questi particolari domini esiste un'*unica decomposizione* come prodotto di ideali primi:

> *In un dominio di Dedekind R esistono unici ideali primi non nulli $\mathfrak{p}_1, ..., \mathfrak{p}_r$ a due a due distinti ed unici numeri interi non nulli $n_1, ..., n_r$ tali che*
>
> $$\mathfrak{a} = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_r^{n_r},$$
>
> *dove $\mathfrak{a}$ è un ideale frazionario proprio non nullo di R.*

Fatto questo, è stato introdotto un concetto di fondamentale importanza, il *gruppo delle classi* di ideali di un dominio di Dedekind:

> *Sia $\mathcal{F}$ il gruppo degli ideali frazionari di un dominio di Dedekind R e $\mathcal{P}$ il suo sottogruppo degli ideali principali frazionari. Allora il gruppo delle classi di R è il gruppo quoziente*
>
> $$\mathcal{C}l(R) := \mathcal{F}/\mathcal{P}.$$

L'ordine di $\mathcal{C}l(R)$ è chiamato numero delle classi.

Dopo aver fatto vedere che tale gruppo è finito, abbiamo dimostrato un risultato che costituisce il vero e proprio punto di partenza di questa tesi.

Proposizione. *Sia R un dominio di Dedekind. Allora $|\mathcal{C}l(R)| = 1$ se e soltanto se R è un dominio a fattorizzazione unica.*

Attraverso questa affermazione è possibile rendersi conto del fatto che il gruppo delle classi rappresenta lo strumento che misura quanto un dominio di Dedekind si discosta dall'essere a fattorizzazione unica, in breve UFD (*Unique factorization domain*).

Nel secondo capitolo, inizialmente abbiamo rivisitato da un punto di vista storico il concetto di UFD, fornendo definizioni precise e utili ai nostri scopi.

- *Un dominio d'integrità R si dice* atomico *se ogni elemento non zero, fatta eccezione dell'unità, si può scrivere come prodotto di elementi irriducibili (o* atomi*) di R. L'insieme degli elementi irriducibili di R si rappresenta con $\mathcal{I}rr(R)$.*

- *Un dominio d'integrità atomico R si dice a fattorizzazione unica se, per ogni $\alpha_i, \beta_j \in \mathcal{I}rr(R)$ tali che $\alpha_1 \cdots \alpha_n = \beta_1 \cdots \beta_m$, sono verificate le seguenti proprietà:*

  UF1. $n = m$;

  UF2. *Esiste una permutazione σ di $\{1, ..., n\}$ tale che α_i e $\beta_{\sigma(i)}$ sono associati.*

Dopo aver trattato piuttosto brevemente le principali proprietà che caratterizzano un UFD, abbiamo generalizzato tale concetto, ottenendo due nuove classi[1]:

- *Gli HFD (*Half-factorial domains*), ossia domini in cui ogni fattorizzazione di un elemento in irriducibili ha la stessa lunghezza; in altre parole, essi verificano soltanto la proprietà UF1.*

- *Gli OHFD (*Other half-factorial domains*), ossia domini i cui elementi possono avere fattorizzazioni di differenti lunghezze e al più una di lunghezza n, per ogni intero n; detto altrimenti, essi verificano la proprietà UF2.*

Abbiamo analizzato in maniera dettagliata la prima classe, rendendo conto in particolare di un risultato, enunciato e dimostrato nel 1960 da Leonard Carlitz (1907-99)[2]:

Teorema. *Sia R un anello di interi algebrici. Allora $|\mathcal{C}l(R)| \leq 2$ se e soltanto se R è un HFD.*

Tale teorema si può giustamente collocare al centro della teoria della fattorizzazione. Esso ci ha permesso di fornire molti esempi di domini HFD che non sono UFD, come $\mathbb{Z}[\sqrt{-3}]$ oppure $\mathbb{Z}[\sqrt{-5}]$.
In seguito, sono stati messi a confronto gli HFD con gli UFD, con l'intenzione di capire se le proprietà verificate per i secondi, sono valide anche per i primi; abbiamo visto, attraverso dei controesempi, che la maggior parte di queste

[1]Tali definizioni sono state date rispettivamente da Abraham Zaks (Technion - Israel Institute of Technology) nel 1976 e da James Coykendall (North Dakota State University) nel 2004.

[2]Leonard Carlitz è stato professore presso la Duke University, negli Stati Uniti, dal 1932 al 1977. Egli è certamente uno dei ricercatori matematici più prolifici della seconda metà del novecento; al suo attivo, infatti, si possono annoverare addirittura 771 articoli.

non si mantengono.
La seguente tabella esplicita quanto detto:

R è UFD $\Rightarrow$ R è integr. chiuso	R è HFD $\not\Rightarrow$ R è integr. chiuso
R è UFD $\Rightarrow$ R_S è UFD	R è HFD $\not\Rightarrow$ R_S è HFD
R è UFD $\Rightarrow$ $R[X]$ è UFD	R è HFD $\not\Rightarrow$ $R[X]$ è HFD
R è UFD $\Rightarrow$ R verifica la ACCP	R è HFD $\Rightarrow$ R verifica la ACCP

Fatto questo, siamo passati ad analizzare gli OHFD, introducendo alcuni concetti preliminari, come quello di fattorizzazione *non degenerata* e *master*, di elementi irriducibili *lunghi* e *corti*.

- *Una fattorizzazione in irriducibili* $\pi_1 \cdots \pi_n = \xi_1 \cdots \xi_m$ *si dice* non degenerata *se gli elementi irriducibili* π_i *e* ξ_j *sono a due a due non associati.*

- *Sia* R *un dominio atomico e* π_1 *un elemento irriducibile. Diremo che* π_1 *è un atomo* lungo *(risp.* corto*) se esiste una fattorizzazione in irriducibili* $\pi_1 \cdots \pi_n = \xi_1 \cdots \xi_m$ *tale che* $n > m$ *(risp.* $n < m$*).*

- *Siano* $\{\pi_1, ..., \pi_k\}$ *e* $\{\xi_1, ..., \xi_m\}$ *gli insiemi rispettivamente degli elementi irriducibili lunghi e corti in* R*. Consideriamo scomposizioni del*

tipo

$$\pi_1^{a_1} \cdots \pi_k^{a_k} = \xi_1^{b_1} \cdots \xi_m^{b_m}$$

tali che $\sum_{i=1}^{k} a_i > \sum_{i=1}^{m} b_i$ *e tutti gli irriducibili sono a due a due non associati. Tra queste, scegliamo quella per cui* a_1 *sia minimo; una tale fattorizzazione è definita* fattorizzazione master *(in breve MF).*

Per mezzo di queste definizioni abbiamo potuto fare le seguenti affermazioni:

(1) *Sia R un OHFD, che non è un HFD, e sia $\pi \in \mathcal{I}rr(R)$ non primo. Allora π non può essere contemporaneamente lungo e corto.*

(2) *Se $x \in R$ è un elemento irriducibile che non è né lungo né corto, allora è primo.*

(3) *Sia $\pi_1^{a_1} \cdots \pi_k^{a_k} = \xi_1^{b_1} \cdots \xi_m^{b_m}$ la MF. Allora ogni altra fattorizzazione non degenerata è potenza di questa MF.*

Tali risultati ci hanno permesso, a loro volta, di mostrare un Teorema molto interessante:

> *Sia R un dominio d'integrità. Se R è un OHFD, allora è anche un HFD. Questo, in particolare, significa che R è un OHFD se, e soltanto se, è un UFD.*

Pertanto, tale classe coincide con quella dei domini a fattorizzazione unica; è possibile, dunque, affermare che la definizione di UFD è *ridondante* e può essere indebolita considerevolmente.

Nell'ultimo capitolo, ci siamo interessati a risolvere la seguente naturale questione (posta nel 1974 da Wladyslaw Narkiewicz[3]):

[3]Professore titolare di Teoria dei Numeri ed Algebra presso la Wroclaw University (Polonia) dal 1974.

Trovare, attraverso proprietà aritmetiche, una o più caratterizzazioni di anelli di numeri algebrici che abbiano numero delle classi diverso da 1 *e* 2.

Ci siamo concentrati su due casi particolari, quando, cioè, il gruppo delle classi ha *ordine tre* e *quattro*.
Abbiamo introdotto le seguenti specifiche *proprietà aritmetiche*:

- *Un dominio di Dedekind R verifica la* proprietà $\mathcal{V}_n$, $n \geq 2$, *se per ogni* $a_1, a_2, b_1, ..., b_k \in \mathcal{I}rr(R)$, *l'uguaglianza* $a_1 a_2 = b_1 \cdots b_k$ *implica che* $k \leq n$.

- *Un dominio di Dedekind R verifica la* proprietà $\mathcal{W}_n$, $n \geq 2$, *se soddisfa la proprietà* $\mathcal{V}_n$ *e, in più, se per ogni elemento irriducibile* $a, b_1, ..., b_k$ *del dominio, l'uguaglianza* $a^2 = b_1 \cdots b_k$ *implica che* $k = 2$.

Successivamente, abbiamo dato una reinterpretazione del Teorema di Carlitz, in funzione delle proprietà aritmetiche appena enunciate:

Sia R un anello di interi algebrici. $|\mathcal{C}l(R)| \leq 2$ *se e solo se R verifica la proprietà* $\mathcal{V}_2$.

Quindi, è stata fornita una prima risposta al problema che c'eravamo posti:

Teorema. *Sia R un anello di interi algebrici. Allora*

i) $|\mathcal{C}l(R)| \leq 3$ *se e soltanto se R soddisfa la proprietà* $\mathcal{W}_3$.

ii) $|\mathcal{C}l(R)| \leq 4$ *se e soltanto se R soddisfa la proprietà* $\mathcal{W}_4$.

Fatto questo, abbiamo ricordato che se R è un dominio di Dedekind, per ogni $r \in R$ ($r \neq 0$ e non invertibile), l'ideale proprio generato da r si può scrivere, in modo unico, come prodotto di ideali primi $(r) = \mathfrak{p}_1 \cdots \mathfrak{p}_n$. Conseguentemente, denotata con X la generica classe di $\mathcal{C}l(R)$ e con E l'elemento

neutro (ossia la classe contenente tutti gli ideali principali), abbiamo dato le seguenti definizioni:

- $m(X, r) := |\{\mathfrak{p}_i : \mathfrak{p}_i \in X\}|$;
- $m(r) := \min\{m(X, r) : X \in \mathcal{C}l(R),\ X \neq E\}$;
- $m_0(r) := \min\{m(X, r) : X \in \mathcal{C}l(R),\ X$ non è un quadrato$\}$ (nel caso in cui ogni elemento in $\mathcal{C}l(R)$ è un quadrato, porremo $m_0(r) = 0$).

Grazie a queste, è stato possibile fornire altre due caratterizzazioni, questa volta facendo uso di proprietà riguardanti il numero di fattori di due diverse decomposizioni di un elemento, che danno luogo ad un particolare limite superiore relativo alla differenza tra le lunghezze delle scomposizioni considerate.

Teorema. *Sia R un dominio di Dedekind e sia r un elemento non nullo e non invertibile di R tale che*

$$r = a_1 \cdots a_k = b_1 \cdots b_h,$$

con $a_1, ..., a_k, b_1, ..., b_h \in \mathcal{I}rr(R)$. Allora

i) $|\mathcal{C}l(R)| = 3$ *se e soltanto se esiste r tale che $k \neq h$ e $|k - h| \leq m(r)/3$.*

ii) $|\mathcal{C}l(R)| = 4$ *se e soltanto se $|k - h| \leq m_0(r)/2$, per ogni $r \in R$.*

La tesi è stata conclusa con una generalizzazione riguardante gli HFD; abbiamo definito, cioè, una nuova classe, i CHFD (*Congruence half-factorial domains*)[4]:

[4]Tale generalizzazione è stata proposta da Scott T. Chapman (Trinity University) e William W. Smith (University of North Carolina at Chapel Hill) per la prima volta nel 1988.

Sia R un dominio d'integrità. R si dice dominio metà-fattoriale congruente *(CHFD) di ordine r se, per ogni α_i, β_j elementi irriducibili tali che $\alpha_1 \cdots \alpha_n = \beta_1 \cdots \beta_m$, esiste un intero $r > 1$ per cui $m \equiv n \pmod{r}$.*

Quindi, sono stati dati esempi di CHFD che non sono HFD:

Sia R un dominio di Dedekind con $\mathcal{C}l(R) \cong \mathbb{Z}_n$, $n \geq 3$. Supponiamo che tutti gli ideali primi (non principali) di R siano distribuiti nelle classi $X_1 := [1]$ e $X_{n-1} := [n-1]$. Allora R è un CHFD di ordine $n-2$, ma non un HFD.

Abbiamo inoltre riadattato (e indebolito) il Teorema di Carlitz al caso dei CHFD:

Sia R un anello degli interi algebrici. Allora $|\mathcal{C}l(R)| \leq 2$ se e soltanto se R è un CHFD per qualche $r > 1$.

Ciò ci ha permesso, infine, di fornire ancora un'altra caratterizzazione riguardante gli anelli degli interi con gruppo delle classi di ordine uguale a tre.

Teorema. *Sia R un dominio di Dedekind tale che $|\mathcal{C}l(R)| \leq 3$. Allora R è un HFD se e soltanto se R è un CHFD, per qualche $r > 1$.*

Bibliografia

[1] D.D. Anderson, D.F. Anderson, M. Zafrullah, *Factorization in integral domains*, J. Pure Appl. Algebra **69** (1990), 1-19.

[2] D.D. Anderson, D.F. Anderson, M. Zafrullah, *Rings between D[X] and K[X]*, Houston J. Math. **17**(1991), 109-129.

[3] D.F. Anderson, S.T. Chapman, W.W. Smith, *Overrings of half-factorial domains*, Canad. Math. Bul. **37** (1994), 437-442.

[4] M. Artin, *Algebra*, Bollati Boringhieri, 1998.

[5] M.F. Atiyah, I.G. Macdonald, *Introduction to Commutative Algebra*, Addison Wesley, 1969.

[6] Z.I. Borevich, I.R. Shafarevich, *Number Theory*, Academic Press, New York, 1966.

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

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

[9] L. Claborn, *Every abelian group is a class group*, Pacific. J. Math. **18** (1966), 219-222.

[10] L. Claborn, *Specified relations in the ideal group*, Michigan Math. J. **15** (1968), 249-255.

[11] H. Cohn, *A classical invitation to algebraic numbers and class fields*, Universitext Springer-Verlag.

[12] P.M. Cohn, *Unique factorization domains*, Am. Math. Monthly **80** (1973), 1-18.

[13] J. Coykendall, W.W. Smith, *On unique factorization domains*, preprint.

[14] J. Coykendall, *Extensions of half-factorial domains: a survey*, to appear.

[15] J. Coykendall, *Half-factorial domains in quadratic fields*, J. Algebra **235** (2001), 417-430.

[16] A. Czogala, *Arithmetic characterization of algebraic number fields with small class number*, Math. Z. **176**(1981), 247-253.

[17] F. Di Franco, F. Pace, *Arithmetical characterization of rings of algebraic integers with class number three and four*, Boll. Un. Mat. Ital. D(6) **4** (1985), 63-69.

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

[19] R. Gilmer, W. Heinzer, W.W. Smith, *On the distribution of prime ideals within the ideal class group*, Houston J. Math. **22** (1996), 51-59.

[20] A. Grams, *The distribution of prime ideals of a Dedekind domain*, Bull. Austral. Math. Soc. **11** (1974), 429-441.

[21] I. Kaplansky, *Commutative Rings*, The University of Chicago Press, Chicago, Ill.-London, 1974.

[22] M. Kline, *Storia del pensiero matematico II*, Biblioteca Einaudi (1972).

[23] D.A. Marcus, *Numberfields*, Universitext Springer-Verlag.

[24] W. Narkiewicz, *Some unsolved problems*, Bull. Soc. Math. France **25** (1971), 159-164.

[25] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, Springer-Verlag, 1990.

[26] H. Pollard, H.G. Diamond, *The Theory of Algebraic Numbers*, Mathematical Association of America, Buffalo, 1950.

[27] P. Samuel, *On unique factorization domains*, Illinois J. Math. **5** (1961), 945-952.

[28] R.Y. Sharp, *Steps in commutative algebra*, London Mathematical Society Society Student Texts 51, Cambridge University Press.

[29] I.N. Stewart, D.O. Tall, *Algebraic number theory*, Chapman-Hall, 1987.

[30] I. Stewart, *Galois Theory*, Second Edition, Chapman and Hall, 1989.

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

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