UNIVERSITÀ DEGLI STUDI ROMA TRE
Facoltà di Scienze Matematiche Fisiche e Naturali

Sintesi della Tesi di Laurea in Matematica

presentata da Cristina Cuomo

Domini euclidei e domini ad ideali principali

Relatore Prof. F. Girolami

ANNO ACCADEMICO 2001-2002
Luglio 2002

Uno dei primi e fondamentali strumenti utilizzati nello studio delle proprietà di divisibilità nell'anello degli interi è l'algoritmo di divisione:
Dati comunque due interi a, b con $b \neq 0$, allora esistono e sono univocamente determinati gli interi q, r detti rispettivamente quoziente e resto della divisione di a per b, tali che

$$a = bq + r \quad 0 \leq r < |b|.$$

Prendendo spunto dalle proprietà di $\mathbb{Z}$ viene naturale considerare la seguente classe di domini:
Sia A un dominio e $A^* := A \setminus \{0\}$, allora A è detto ***dominio euclideo*** *(in breve ED) se può essere dotato di un'applicazione $\varphi : A \longrightarrow \mathbb{N}$ tale che le seguenti condizioni siano soddisfatte:*
1)per tutti gli $a \in A$ e $b \in A^*$, $\varphi(ab) \geq \varphi(a)$;
2)presi comunque $a \in A$ e $b \in A^*$, allora esistono q ed r in A, detti rispettivamente un quoziente e un resto tali che

$$a = bq + r \qquad \varphi(r) < \varphi(b).$$

L'applicazione φ viene detta un **algoritmo euclideo** in A.

L'anello degli interi è un dominio euclideo rispetto al valore assoluto, l'anello dei polinomi in un'indeterminata a coefficienti in un campo è euclideo rispetto all'applicazione così definita:

$$\varphi(f) := \begin{cases} 1 + deg(f), & f \neq 0 \\ 0 & \text{altrimenti.} \end{cases}$$

Un altro importante esempio di dominio euclideo è l'anello degli interi di Gauss $\mathbb{Z}[i]$, rispetto all'usuale norma complessa.

Dopo aver esaminato in dettaglio le proprietà di cui gode un algoritmo euclideo su un dominio, abbiamo dimostrato il seguente importante risultato:
Ogni dominio euclideo è un dominio ad ideali principali.

$$ED \Rightarrow PID$$

Definiamo un'altra importante classe di domini:

Un dominio A è un ***dominio a fattorizzazione unica*** *(in breve UFD) se:*

1) per ogni $a \in A$ non zero e non invertibile esiste $u \in U(A)$ e un numero finito di elementi irriducibili $q_1, \ldots, q_n \in A$ $(n \geq 1)$ in modo tale che:

$$a = uq_1 \ldots q_n$$

2) tale fattorizzazione è unica a meno dell' ordine dei fattori e di elementi associati.

Le relazioni tra le classi di domini fin qui esaminate possono essere rappresentate nel modo seguente:

$$ED \Rightarrow PID \Rightarrow UFD$$

Le implicazione precedenti non possono essere invertite: un UFD in generale non è un PID (basti pensare all'anello dei polinomi in un'indeterminata a coefficienti interi), ed esistono domini ad ideali principali non euclidei.

La ricerca di esempi di PID non euclidei ha portato ad un interessante studio dell'anello degli interi di campi quadratici:

sia $\mathbb{Q}(\sqrt{d})$ un campo quadratico[1] e $\alpha \in \mathbb{Q}(\sqrt{d})$, α è detto intero in $\mathbb{Q}(\sqrt{d})$ se norma e traccia,[2] che indicheremo rispettivamente con $N(\alpha)$ e $Tr(\alpha)$, sono numeri interi.

L'insieme degli elementi interi di $\mathbb{Q}(\sqrt{d})$ si denota con I_d; I_d è un anello ed inoltre

$$\mathbb{Z}[\sqrt{d}] \subseteq I_d \subset \mathbb{Q}(\sqrt{d})$$

[1] Ricordiamo che $\mathbb{Q}(\sqrt{d})$ è il campo ottenuto per ampliamento di $\mathbb{Q}$ con $\sqrt{d}, d \in \mathbb{Z}\setminus\{0,1\}$ e d privo di fattori quadratici, i suoi elementi sono della forma $a + b\sqrt{d}$ con $a, b \in \mathbb{Q}$; se $d < 0$ il campo $\mathbb{Q}(\sqrt{d})$ viene detto campo quadratico immaginario, campo quadratico reale altrimenti.

[2] Sia $\alpha = a + b\sqrt{d}$ un elemento di $\mathbb{Q}(\sqrt{d}$, definiamo $Tr(\alpha)$ e $N(\alpha)$ i numeri razionali

$$Tr(\alpha) = \alpha + \bar{\alpha} = a^2 - b^2 d \qquad N(\alpha) = \alpha\bar{\alpha} = 2a$$

dove $\bar{\alpha} = a - b\sqrt{d}$ è detto coniugato di α (in $\mathbb{Q}(\sqrt{d})$).

dunque I_d è un dominio. Possiamo dare la seguente definizione:
Sia $\mathbb{Q}(\sqrt{d})$ *un campo quadratico allora l'anello* $I_d \subset \mathbb{Q}(\sqrt{d})$ *viene detto* ***anello degli interi*** *di* $\mathbb{Q}(\sqrt{d})$.

La possibilità di estendere ad I_d una teoria della divisibilità analoga a quella degli interi ha condotto allo studio dei valori di d per i quali I_d è un dominio euclideo, un dominio ad ideali principali e un dominio a fattorizzazione unica.

Il problema della determinazione dei valori di d per i quali l'anello degli interi di un campo quadratico è euclideo rispetto al modulo della norma è stato oggetto di studio per molti decenni suscitando l'interesse di numerosi matematici. Nel caso $d < 0$ il problema fu di facile soluzione, infatti già negli anni venti L.E. Dickson[3] osservò che I_d è euclideo rispetto al modulo della norma se e solo se $d = -1, -2, -3, -7, -11$. Il problema di stabilire per quali valori di d positivi I_d è euclideo, sempre rispetto al modulo della norma, fu inizialmente studiato da L.E. Dickson che mostrò che I_d è euclideo per $d = 2, 3, 5, 13$. Intorno agli anni '30-40 a tali valori di d positivi vennero aggiunti $d = 6, 7, 11, 17, 19, 21, 29, 33, 37, 41, 57, 73$. Intorno al 1950 i matematici Chatland e Davenport[4] esclusero alcuni valori di $d > 0$ sui quali permaneva il dubbio (d=193,241,313,337,457,601) e mostrarono che I_d non poteva essere euclideo rispetto al modulo della norma per $d > 2^{14}$, limitando così lo studio ad un numero finito di valori, seppur ancora molto grande. Grazie anche ai risultati ottenuti dai matematici S. H. Min e L. K. Hua e Chatland nel 1944 e nel 1949,[5] il problema è stato completamente risolto giungendo al seguente risultato conclusivo:
L'anello degli interi I_d *di un campo quadratico è euclideo rispetto al modulo*

[3]Algebren und ihre Zahlentheorie, Zurich Leipzig (1927), pagg.150-151.

[4]Euclids algorithm in real quadratic fields, Canad. J. Math 2 (1950),289-196

[5]L. K. Hua, S.H. Min,On the distribution of quadratic non-residues and the Euclidean algorithm in real quadratic fields II, Trans. Amer. Math. Soc. 56 (1944), 547-569; H. Chatland, On the Euclidean algorithm in quadratic number fields, Bull. Amer. Math. Soc. 55 (1949), 948-953.

della norma, se e solo se d è uno dei seguenti interi:

$$-11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$$

Per valori di d positivi la classificazione degli I_d quadratici che sono euclidei rispetto ad algoritmi diversi dal modulo della norma è un problema ancora oggi senza soluzione, mentre Per valori di d negativi, già nel 1958, i matematici D.W, Dubois e A. Steger[6] provarono che per valori di d diversi da quelli citati, I_d non è euclideo neppure rispetto ad algoritmi distinti dal modulo della norma.

Un problema analogo è stato posto riguardo la classificazione degli anelli di interi quadratici tra i domini ad ideali principali, ma ancora non si è giunti alla completa soluzione. Tra il 1966 e il 1967 si giunse al risultato che I_d, per di $d < 0$, è un dominio ad ideali principali se e solo se

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

Da queste considerazione si ricavano esempi di PID non euclidei:

$$I_{-163}, I_{-67}, I_{-43}, I_{-19}.$$

Ricordiamo che se A è un dominio a fattorizzazione unica, $Q(A)$ il campo dei quozienti e $\mathcal{P}$ l'insieme degli elementi primi di A, allora per ogni $p \in \mathcal{P}$ può essere definita la seguente applicazione:

$$v_p : Q(A) \to \mathbb{Z} \cup \{\infty\} =: \mathbb{Z}_\infty \tag{1}$$

tale che per ogni $x \in Q(A)$

$$v_p(x) = \begin{cases} \infty & se\ x = 0 \\ s - r & se\ x = p^s x'/p^r y' \end{cases}$$

con p che non divide né x' né y'.
v_p viene detta **valutazione discreta p-adica**.

[6] Can.J. math. 10 (1958), 285-286.

L'introduzione della definizione di valutazione discreta p-adica ha permesso di giungere al seguente risultato:
Sia A un PID con un numero finito di ideali massimali $p_1A \dots p_nA$. Allora A è euclideo per l' algoritmo:

$$\varphi(a) = \begin{cases} 1 + \sum_{i=1}^{n} v_{p_i}(a) & a \neq 0 \\ 0 & a = 0 \end{cases}$$

Nella definizione di algoritmo euclideo non è richiesta l'unicità del quoziente e del resto; la seguente proposizione caratterizza i domini euclidei in cui tale unicità vale:
Sia A un ED e φ un algoritmo euclideo in A, allora quoziente e resto sono univocamente determinati se e solo se presi comunque $a, b \in A^*$ risulti

$$\varphi(a+b) \leq max(\varphi(a), \varphi(b)).$$

Il teorema seguente mostra come l'unicità del *quoziente* e *resto*, caratterizzi, tra i domini euclidei, gli anelli dei polinomi in una indeterminata a coefficienti in un campo:
Sia A un ED, se quoziente e resto in A sono unici allora l'insieme $(U(A) \cup \{0\})$ costituito dagli elementi invertibili e dallo zero, forma un campo F; se $A \neq F$ allora $A \cong F[x]$.

Analogamente la seguente proprietà caratterizza l'anello degli interi $\mathbb{Z}$ tra i domini euclidei:
Sia A un dominio euclideo e φ un suo algoritmo euclideo, diremo che A gode della ***proprietà del doppio resto*** *(in breve* ***d.r.p.****) se per ogni coppia (a, b) tale che $a \in A$, $b \in A^*$ e $b \nmid a$, esistono esattamente due coppie (q_1, r_1), (q_2, r_2) di elementi di A tali che $a = q_i b + r_i$ e $\varphi(r_i) < \varphi(b)$ per $i = 1, 2$.*

Se un dominio euclideo A gode della *d.r.p.*, allora $A \cong \mathbb{Z}$.

La nozione di dominio euclideo può essere estesa ad anelli non necessariamente integri:
Dato un anello A, un algoritmo euclideo in A è un' applicazione $\varphi : A \longrightarrow W$ dove W è un insieme ben ordinato, tale che:
dati $a, b \in A,\ b \neq 0$ esistono $q, r \in A$ tali che

$$a = bq + r \qquad con\ \varphi(r) < \varphi(b).$$

Un anello dotato di un algoritmo euclideo si dice ***anello euclideo****.*

Naturalmente ogni anello euclideo è un anello ad ideali principali ed inoltre si verificano delle importanti proprietà di stabilità per anelli euclidei e per domini euclidei:

- Un prodotto finito di anelli euclidei è euclideo.
- Se A è un dominio euclideo e S una parte moltiplicativa di A tale che $0 \notin S$, allora $S^{-1}A$ è ancora euclideo.
- Se (A, φ) è un anello euclideo allora $A' = A[[X]][X^{-1}]$ è euclideo.

Infine diamo la definizione di algoritmo euclideo minimo per un anello euclideo:
Sia A un anello euclideo, W un insieme ben ordinato e $(\varphi_\alpha : A \longrightarrow W)_{\alpha \in \Lambda}$ una famiglia non vuota di algoritmi euclidei su A. Allora

$$\begin{aligned} \vartheta := inf(\varphi_\alpha)_{\alpha \in \Lambda} : & A \to W \\ & a \to inf(\varphi_\alpha(a) : \alpha \in \Lambda) \end{aligned}$$

è un algoritmo euclideo per A.
L'algoritmo ϑ viene detto **algoritmo euclideo minimo** per l'anello A. La ricerca dell'algoritmo minimo in un anello euclideo è basata sulla costruzione di una successione di sottoinsiemi di A con il metodo di costruzione transfinita. In $\mathbb{Z}$, ad esempio, l'algoritmo minimo è la funzione che associa ad ogni

intero non nullo il numero delle cifre della rappresentazione in base 2 del suo valore assoluto.

Nel quarto capitolo introduciamo la nozione di *dominio quasi-euclideo* (in breve AED):
Un dominio A è detto ***quasi-euclideo*** *se esiste un' applicazione*

$$\psi : A \longrightarrow \mathbb{Z}^+ \cup \{0\}$$

tale che:

i) $\psi(0) = 0$ *e* $\psi(a) > 0$ *per ogni* $a \in A^*$*;*

ii) se $b \in A^*$*, allora* $\psi(ab) \geq \psi(a)$ *per ogni* $a \in A$*;*

iii) per ogni $a \in A$ *e* $b \in A^*$ *allora solo una delle seguenti condizioni è soddisfatta:*

1) $a = bq$ *per un certo* $q \in A$

2) $0 < \psi(ax - by) < \psi(b)$ *per certi* $x, y \in A$*.*

Un dominio quasi-euclideo è un dominio ad ideali principali:

$$AED \Rightarrow PID$$

Il sottoanello dei numeri complessi $\mathbb{Z}[(1+\sqrt{-19})/2] = I_{-19}$ è un AED ma non è euclideo, esso dunque rappresenta un esempio di dominio ad ideali principali non euclideo. Tuttavia l'introduzione della classe dei domini quasi-euclidei non determina l'individuazione di una classe intermedia di domini tra i PID e gli ED, infatti solo nel 1997 J.Green [9] mostra il seguente risultato:
Un dominio A è un dominio ad ideali principali se e solo se è un dominio quasi-euclideo.

$$AED \Leftrightarrow PID$$

Nell'ultimo capitolo ci proponiamo di enunciare e dimostrare un teorema di esistenza di domini ad ideali principali non euclidei nell'ambito della teoria

degli anelli commutativi, fornendo un metodo per la costruzione di PID non euclidei. A tale proposito ricordiamo la definizione di dimensione di Krull di un anello, di anello Noetheriano e di anello locale regolare:

Una catena di ideali primi di un anello A è una successione finita strettamente crescente

$$P_0 \subset P_1 \ldots \subset P_n$$

dove n denota la ***lunghezza*** *della catena;*
l'estremo superiore delle lunghezze di tutte le catene di ideali primi è detta ***dimensione*** *(di Krull) di A, che indicheremo con $dim(A)$; $dim(A) \geq 0$ oppure $dim(A) = +\infty$.*

Un anello A si dice ***Noetheriano*** *se soddisfa una delle seguenti condizioni equivalenti:*
1) ogni catena ascendente di ideali in A è stazionaria;
2) ogni ideale di A è finitamente generato.

Sia $(A, \mathcal{M})$ un anello locale Noetheriano, A si dice ***anello locale regolare*** *se*

$$dim(A) = dim_K(\mathcal{M}/\mathcal{M}^2)$$

ossia se $dim(A)$ coincide con il minimo numero di generatori dell'ideale massimale $\mathcal{M}$.

Il matematico D.D.Anderson, nel 1988 [1], fornisce un metodo per la costruzione di esempi di domini ad ideali principali non euclidei:

Sia R un dominio e f un elemento primo non nullo tale che $f \in J(R)$[7] *e tale che risulti $\cap_{n=1}^{\infty}(f^n) = (0)$. Allora $A = R_f$ è euclideo se e solo se*

[7]Il radicale di Jacobson di un anello A (in simboli $J(A)$) è definito come l'intersezione di tutti gli ideali massimali di A; i suoi elementi sono caratterizzati nel modo seguente: $x \in J(A)$ se e solo se $1 - xy \in U(A)$ per ogni $y \in A$.

$\bar{R} = R/fR$ è euclideo. In questo caso R è un DVR oppure R è un UFD regolare di dimensione 2 in cui ogni ideale primo P di A è generato da un numero di elementi pari all'altezza di P e $f \notin \mathcal{M}^2$ per ogni ideale massimale $\mathcal{M}$ di R.

Conseguenza importante del teorema precedente è il seguente risultato:

Sia $(R, \mathcal{M})$ un UFD locale 2-dimensionale e $f \in \mathcal{M}$ un elemento primo non nullo. Allora $R_f = A$ è un PID; inoltre se A è un dominio euclideo allora $f \notin \mathcal{M}^2$ e R è un dominio locale Noetheriano 2-dimensionale regolare. Viceversa se $(R, \mathcal{M})$ è un dominio locale Noetheriano 2-dimensionale regolare e se $f \in \mathcal{M} \setminus \mathcal{M}^2$ allora A è un dominio euclideo.

Ora sarà sufficiente considerare un anello locale regolare di dimensione 2 e f un elemento primo non nullo dell'anello, tale che $f \in \mathcal{M}^2$. Allora, in base alle considerazioni fatte, la localizzazione dell'anello rispetto all'elemento f è un PID non euclideo.

Un altro esempio può essere fatto considerando un dominio a fattorizzazione unica, 2-dimensionale, locale, non-Noetheriano, allora la localizzazione rispetto ad un elemento primo non nullo appartenente all'ideale massimale, è un dominio ad ideali principali non euclideo. L'esistenza di almeno un esempio di un dominio a fattorizzazione unica, 2-dimensionale, locale, che non sia Noetheriano è stata provata da R. Gilmer in [8]; egli mostra che comunque scelto un numero primo p, e un campo F di caratteristica p, l'anello gruppo $D = F[X; L]$[8] di L su F, con L gruppo abeliano soddisfacente certe ipotesi, è

[8]Sia $(G, +)$ un gruppo abeliano, R un anello e $R[X; G]$ l'insieme delle funzioni $f : G \longrightarrow R$ quasi ovunque nulle. Per $f, g \in R[X; G]$ poniamo:

$$f = g \Leftrightarrow f(a) = g(a) \ \ \forall a \in G$$
$$(f + g)(a) = f(a) + g(a) \ \ \forall a \in G$$
$$(fg)(a) = \sum_{b+c=a} f(b)g(c) \ \ \forall a, b, c \in G$$

Con le operazioni introdotte $R[X; G]$ è detto **anello gruppo di G su R**.

un dominio a fattorizzazione unica 2-dimensionale, non-Noetheriano; inoltre se $\mathcal{M}$ è l'ideale massimale di D, generato dall'elemento $\{1 - X^g \mid g \in L\}$, allora $D_{\mathcal{M}}$ è un dominio a fattorizzazione unica, non-Noetheriano, locale, 2-dimensionale di caratteristica p.

R. Gilmer in [8] perviene inoltre ad un risultato più generale: egli mostra che comunque scelto un intero $k \geq 2$ esiste un UFD non-noetheriano, k-dimensionale di caratteristica arbitraria.

Bibliografia

[1] D. D. Anderson, *An existence theorem for non-Euclidean Pid's*, Communications in Algebra **16(6)** (1988),1221-1229.

[2] M. F. Atyah,I. G. Macdonald, *Introduzione all'algebra commutativa*, Feltrinelli, Milano 1980..

[3] O. Campoli, *A principal ideal domain that in not an euclidean domain*, Am.Math.Monthly **95** (1988),868-871.

[4] J. Dugundji, *Topology*, Boston, Allyn and Bacon, 1966.

[5] M. Fontana, *Anelli*, (1989).

[6] S. Galovich, *A characterization of the integers among euclidean domains*, Am.Math.Monthly (1978),572-575.

[7] R. Gilmer, *Multiplicative ideal theory*, M.Dekker, Inc. N.Y., 1972.

[8] ————, *A two-dimensional non-Noetherian factorial ring*, Proc.Am.Math.Soc. **44** numero 1 (1974),25-30.

[9] J. Greene, *Principal ideal domains are almost euclidean*, Am.Math.Monthly **104** (1997),154-156.

[10] G.H. Hardy and E.M. Wright, *An introduction to the theory of numbers*, Oxford Univ. Press, Oxford, 1954.

[11] M. A. Jodeit, Jr., *Uniqueness in the division algorithm*, Am.Math. Monthly **74** (1967).

[12] I. Kaplasky, *Commutative rings*, The University of Chicago Press, 1974.

[13] H. Matsumura, *Commutative ring theory*, Cambridge University Press, 1986.

[14] A. Oppenheim, *Quadratic fields with and without Euclid's Algorithm*, Math.Ann.,**109** (1933),349-352.

[15] K. Rogers, *The axioms for euclidean domains*, Amer.Math.Month., **78** (1971),1127-1128.

[16] P. Samuel, *About euclidean rings*, J.Algebra **19** (1971), 282-301.

[17] R. Y. Sharp, *Steps in commutative algebra*, Second Edition, London Mathematical Society Student Texts 51, Cambridge University Press,2000

[18] I. Stewart and D. Tall, *Algebraic number theory*, Second Edition, Chapman & Hall, London,1986.

[19] B. L. Van Der Waerden, *Modern Algebra*, Ungar, New York, Vol.1, 1953.

[20] O. Zariski and P. Samuel, *Commutative Algebra*, Vol.1, Van Nostrand, Princeton, N.J.,1958.