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

Caratterizzazioni di alcuni domini euclidei in base al numero dei resti

Sintesi della tesi di Laurea in Matematica
di Alessia Santini
Relatore: Prof. Marco Fontana

Un'importante classe di domini è data dai *Domini Euclidei* che "assiomatizzano" i domini nei quali è possibile effettuare l'algoritmo delle divisioni successive. Euclide fu il primo a "provare" che $\mathbb{Z}$, l'anello degli interi relativi, è euclideo. Un secondo esempio di dominio euclideo è dato da $\mathbb{R}[X]$, l'anello dei polinomi in una indeterminata a coefficienti in $\mathbb{R}$, la dimostrazione fu data da Simon Stevin nel XVI secolo. È subito visto che un ragionamento analogo a quello che permette di dimostrare che $\mathbb{R}[X]$ è euclideo mostra che $K[X]$ è un dominio euclideo, per ogni campo K. Ulteriori esempi di anelli euclidei si trovano tra gli anelli ciclotomici. Gauss fu il primo a mostrare che due di tali anelli, $\mathbb{Z}[\zeta_3]$ e $\mathbb{Z}[i] = \mathbb{Z}[\zeta_4]$, sono euclidei. Nel 1832 pubblicò un lavoro sulla legge di reciprocità biquadratica, nel quale incluse le dimostrazioni di tale fatto (per approfondimenti cfr. [**?**]). Nel 1844 Kummer, in due lettere a Kronecker, mostrò che $\mathbb{Z}[\zeta_5]$ è euclideo e osservò che il metodo poteva essere applicato anche a $\mathbb{Z}[\zeta_7]$. Sessantacinque anni dopo, e prima della

pubblicazione di queste lettere, anche Ouspensky dimostrò che $\mathbb{Z}[\zeta_5]$ è un dominio euclideo (cfr. [**?**]). Una dimostrazione che $\mathbb{Z}[\zeta_8]$ è euclideo fu data nel 1850 da Eisenstein. Bisogna aspettare fino al 1975 per avere ulteriori nuovi risultati rilevanti in questo ambito. Infatti Masley ha provato che $\mathbb{Z}[\zeta_{12}]$ è euclideo (cfr. [**?**]) e Lenstra ha provato che $\mathbb{Z}[\zeta_n]$ è euclideo, per $n \in \{7, 9, 11, 15, 20\}$ (cfr. [**?**]). Successivamente è stato dimostrato che $\mathbb{Z}[\zeta_{16}]$ e $\mathbb{Z}[\zeta_{24}]$ sono anch'essi euclidei, rispettivamente da Ojala nel 1977 e Lenstra 1978 (cfr. [**?**]).

Oltre agli anelli ciclotomici, particolarmente importanti sono i domini euclidei che si possono incontrare tra gli anelli degli interi dei campi quadratici. Ogni campo di numeri quadratici è della forma $K = \mathbb{Q}(\sqrt{d})$, dove d è un intero privo di fattori quadratici, e l'anello degli interi relativo al campo è della forma $\mathbb{Z}[\omega_d]$ dove

$$\omega_d = \begin{cases} \sqrt{d}, & \text{se } d \equiv 2, 3 \pmod 4; \\ \dfrac{1+\sqrt{d}}{2}, & \text{se } d \equiv 1 \pmod 4. \end{cases}$$

Determinare quali anelli sono euclidei nei campi quadratici immaginari ($d < 0$) è "abbastanza" facile. In particolare gli anelli con $d = -3, -1$ sono uguali agli anelli ciclotomici $\mathbb{Z}[\zeta_3] = \mathbb{Z}[\rho]$ dove $\rho = \zeta_3 = \dfrac{-1+\sqrt{-3}}{2}$ è la radice primitiva terza dell'unità e $\mathbb{Z}[\zeta_4] = \mathbb{Z}[i]$ dove $i = \zeta_4$ è una radice quarta primitiva dell'unità, cioè $i^2 = -1$ ed $i \neq \pm 1$. In un supplemento ad un celebre lavoro di Dirichlet (cfr. [**?**]), Dedekind dimostrò che $\mathbb{Z}[\omega_d]$ è euclideo per $d \in \{-1, -2, -3, -7, -11, 5, 13\}$.

Nel 1927, Dickson provò che i soli domini euclidei $\mathbb{Z}[\omega_d]$ con $d < 0$ sono quelli della lista di Dedekind, cioè $d \in \{-1, -2, -3, -7, -11\}$ (cfr. [**?**]). Il problema di stabilire quali anelli $\mathbb{Z}[\omega_d]$ con $d > 0$ siano euclidei, rispetto al valore assoluto della norma, è risultato essere molto più impegnativo. La dimostrazione definitiva sui valori $d > 0$ per i quali tali anelli sono euclidei è stata data nel 1948 da Chatland e Davenport.

In questa tesi ci si propone di caratterizzare alcune classi di domini euclidei (A, φ), basandosi sulla cardinalità dell'insieme dei resti nella divisione di a per b, con $a, b \in A$ e $b \neq 0$. In certi casi, il dominio A è completamente determinato dalle proprietà della funzione φ relativamente al numero dei resti.

Il nostro obiettivo è quello di vedere sotto quali ipotesi, sul comportamento di φ rispetto ai resti, si riesce a descrivere opportunamente un dominio A.
Cominceremo la trattazione con un capitolo zero che conterrà i principali prerequisiti che aiuteranno a rendere più comprensibili e chiari i successivi approfondimenti del lavoro. Precisamente, un primo paragrafo introduce le proprietà generali degli anelli e la definizione di caratteristica di un anello, un secondo paragrafo è dedicato alla divisibilità in un dominio ed, infine, un paragrafo finale dedicato agli anelli di interi di campi quadratici, dove enunceremo il Teorema delle "unità" di Dirichlet (cfr. [**?**]).
Nel primo capitolo introdurremo il concetto di dominio euclideo e dimostreremo alcune proprietà, facendo riferimento al caso più generale di anelli commutativi unitari non necessariamente integri.
A questo punto, verranno discussi vari esempi di domini euclidei. Nel secondo capitolo, seguiremo il percorso storico della determinazione di tali domini e ci soffermeremo su alcuni esempi come quello di Euclide dove dimostra che $\mathbb{Z}$ è un dominio euclideo con l'algoritmo $\varphi := |\ |$. Gli altri esempi riguarderanno $K[X]$, l'anello dei polinomi in una variabile con coefficienti nel campo K, con l'applicazione dall'insieme dei polinomi non nulli ad $\mathbb{N}$ definita come $\varphi(f) := deg(f)$, cioè il grado di f ($\varphi(0) := -1$); $\mathbb{Z}[i]$, gli interi di Gauss, con $\varphi := N$ la funzione norma cioè $N(\alpha) := \alpha\bar{\alpha}$ dove $\alpha \in \mathbb{Z}[i]$ e $\bar{\alpha}$ è il coniugato di α. Studieremo poi, l'anello $\mathbb{Z}[\zeta_3]$, che abbiamo visto essere uguale a $\mathbb{Z}[\rho]$, con $\rho = \zeta_3$, e quindi soddisfacente $\rho^2 + \rho + 1 = 0$, per il quale prenderemo come algoritmo $\varphi := |\ |^2$. Riporteremo un ultimo risultato relativo agli anelli degli interi dei campi quadratici (con $d = -11, -7, -3, -2, -1, 2, 3, 5, 13$), avente come algoritmo il valore assoluto della norma cioè $\varphi(a) = |\ N(a)\ |$ per ogni $a \in \mathbb{Z}[\omega_d]$.
Nel terzo capitolo, caratterizzeremo i domini euclidei per i quali, presi comunque a, $b \in A$ con $b \neq 0$, nella divisione di a per b il resto ed il quoziente sono unici, cioè la cardinalità dell'insieme dei resti è 1. Un dominio euclideo (A, φ), dove A non è un campo, in cui la divisione con resto è unica si identifica con un anello di polinomi $K[X]$ su un campo K ([**?**]). Questo è dovuto, principalmente, al fatto che l'algoritmo euclideo φ soddisfa la seguente proprietà: presi comunque $a, b \in A$, con $a \neq b$, si ha $\varphi(a - b) \leqslant \sup(\varphi(a), \varphi(b))$. Infatti, mostreremo che tale proprietà garantisce, o meglio caratterizza, l'uni-

cità della divisione.
Nel quarto capitolo daremo una caratterizzazione di $\mathbb{Z}$ come dominio euclideo nel quale la divisione euclidea ha al più due resti e due quozienti. Cominceremo con lo studiare il problema, esaminando i domini euclidei per i quali l'algoritmo φ soddisfa le proprietà formali del valore assoluto su $\mathbb{Z}$. Scopriremo che un dominio euclideo (A, φ) dove φ verifica "tali proprietà" è isomorfo a $\mathbb{Z}$ ([**?**]). Come nel capitolo precedente, anche qui sarà essenziale l'ipotesi che A non sia un campo. Potremo, inoltre, caratterizzare $\mathbb{Z}$ introducendo la *proprietà del doppio resto* (**d.r.p.**) cioè per ogni coppia $a \in A$, $b \in A \setminus \{0\}$ tale che b non divide a allora esistono esattamente due coppie distinte (q_i, r_i), con $i = 1, 2$ di elementi di A tali che: $a = bq_i + r_i$ con $\varphi(r_i) < \varphi(b)$. Non è difficile assicurarsi che il dominio $\mathbb{Z}$ gode di tale proprietà rispetto a $|\ |$.
Quindi arriveremo ad enunciare il seguente risultato: se (A, φ) è un dominio euclideo con **d.r.p.** allora A è isomorfo a $(\mathbb{Z}, |\ |)$ ([**?**]). Osserveremo poi che questi due risultati sono tra loro equivalenti e permettono di caratterizzare in due maniere diverse l'anello $\mathbb{Z}$, in relazione alle proprietà dell'algoritmo euclideo.
Nel quinto ed ultimo capitolo caratterizzeremo alcuni tipi di domini euclidei (A, φ), assieme al loro gruppo delle unità, sotto alcune condizioni sull'insieme dei resti. Infatti, se un dominio euclideo (A, φ), che non è un campo, ha la proprietà che l'insieme dei resti della divisione di 1 per b, con $b \in A \setminus \{0\}$, è finito, allora $U(A) \cup \{0\}$ è un campo oppure $U(A)$ è isomorfo ad uno dei seguenti gruppi ciclici finiti $\mathbb{Z}_2$, $\mathbb{Z}_4$ o $\mathbb{Z}_6$ ([**?**]). Un corollario interessante mostrerà che se l'insieme dei resti della divisione di a per b è finito, presi comunque a, b nel dominio A, allora esiste una coppia di elementi tale che la cardinalità dell'insieme dei resti non supera 6.
Un ultimo risultato caratterizzerà un dominio euclideo che, oltre ad avere l'insieme dei resti della divisione di 1 per b finito, per tutti gli elementi b appartenenti ad A, ha anche un sottogruppo del gruppo delle unità $U(A)$ tale che A è un modulo finitamente generato sull'anello generato dal sottogruppo. Sotto queste ipotesi A è isomorfo ad uno degli anelli degli interi dei campi quadratici $\mathbb{Q}(\sqrt{-d})$, dove $d \in \{1, 2, 3, 7, 11\}$.

Bibliografia

[B] BOURBAKI, N., *Commutative Algebra*, Addison-Wesley, Reading MA, 1972.

[Br] BRUDNYI, A., *On the Euclidean Domains*, Comm. Algebra, 21 (1993), 3327-3336.

[D] DICKSON, L.E., *Algebren und ihre Zahlentheorie* , Orell Fussli Verlag, 1927.

[Di] DIRICHLET, P.G., *Vorlesungen über Zahlentheorie*, Chelsea Publishing Co., New York, 1968.

[F] FONTANA, M., *Anelli, campi e risolubilità per radicali*, Appunti del secondo ciclo di lezioni del Corso di Algebra.

[F1] FONTANA, M., *Una introduzione ad alcuni argomenti della teoria algebrica dei numeri*, Appunti del corso di Istituzioni di Algebra Supuriore A.A. 1980/81, Università la Sapienza di Roma.

[G] GALOVICH, S., *A characterization of the integers among Euclidean domains*, Amer. Math. Month., 85 (1978), 572-575.

[Ga] GAUSS, C.F., *Theorie der biquadratische Rest, Untersuchungen über höhere Arithmetik*, New York: Chelsea, (1965), 511-588.

[J] JACOBSON, *A note on non-commutative polynomials*, Ann. Math., 35 (1934), 209-210.

[Jo] JODEIT, M.A., *Uniqueness in the division algorithm*, Amer. Math. Month., 74 (1967), 835-836.

[L] LENSTRA jr, H.W., *Euclid's algorithm in cyclotomic fields*, J. Lond. Math. Soc., 10 (1975), 457-465.

[Ma] MASLEY, J.M., *On Euclidean rings of integers in cyclotomic fields*, J. reine angew. Math., 272 (1975), 45-48.

[M] MOTZKIN, T.S., *The Euclidean Algorithm*, Bull. Amer. Math. Soc., 55 (1949), 1142-1146.

[O] OUSPENSKY, J., *Note sur le nombres entiers dépendent d'une racine cinquiéme de l'unité*, Math. Ann., 66 (1909), 109-112.

[P] PICAVET, G.,*Caractérisation de certains types d'anneaux euclidiens*, Einsegn. Math., 18 (1972), 245-254.

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

[S] SAMUEL, P., *About Euclidean Rings*, J. Algebra, 19 (1971), 282-301.

[S1] SAMUEL, P., *Théorie Algébrique des nombres*, Hermann, Paris, 1967.

[VdL] VAN DER LINDER, F.J., *Euclidean rings with two infinite primes*, CWI Tracs, Amsterdam, 1985.

[ZS] ZARISKI, O. e SAMUEL, P., *Commutative Algebra*, Springer, New York, 1958.

La bibliografia si riferisce all'intera Tesi di Laurea.