Bollettino
Unione Matematica Italiana

*Sezione A – La Matematica nella Società e nella Cultura*

Paola Piazza

# I fondamenti di Zolotarev della teoria dei numeri algebrici

*Bollettino dell'Unione Matematica Italiana, Serie 8*, Vol. **3-A**—*La Matematica nella Società e nella Cultura* (2000), n.1S, p. 169–172.

Unione Matematica Italiana

<http://www.bdim.eu/item?id=BUMI_2000_8_3A_1S_169_0>

Bollettino dell'Unione Matematica Italiana, Unione Matematica Italiana, 2000.

Bollettino U. M. I.
La Matematica nella Società e nella Cultura
Serie VIII, Vol. III-A, Supplemento ad Aprile 2000, 169-172

# I fondamenti di Zolotarev della teoria dei numeri algebrici.

Paola Piazza

Il mio lavoro di tesi riguarda la teoria dei numeri ideali del matematico russo Egor Ivanovich Zolotarev (1847-1878) che generalizzò nel 1876 la teoria dei numeri ideali di Ernst Eduard Kummer (1810-1893), valida per gli anelli di interi ciclotomici, ad ogni anello $\mathbb{O}$ di interi algebrici di un'estensione finita del campo razionale.

È noto che già nel 1871, Richard Dedekind (1831-1916) generalizzò la teoria di Kummer ad ogni anello di interi algebrici. La sua idea fu quella di identificare il numero ideale di Kummer con l'insieme degli interi che tale numero divide. Questo insieme fu chiamato ideale, per evidente analogia con i numeri ideali. La teoria degli ideali fu completata da Dedekind in ogni sua parte nel 1877. Il matematico russo Zolotarev proponeva proprio negli stessi anni una soluzione alternativa a quella di Dedekind, che però non fu in generale studiata sopratutto nell'Europa occidentale, nonostante fosse pubblicata sul famoso *giornale di Liouville*. I motivi di questo possono essere in parte legati al fatto che la teoria di Zolotarev fu pubblicata solo nel 1880, quindi due anni dopo la morte del giovane matematico (anche se la teoria fu sottoposta per la pubblicazione sul giornale di Liouville già nel 1876). Al tempo, la nuova teoria degli ideali di Dedekind sembrava essere largamente accettata, e pare piuttosto questo il motivo del disinteresse diffuso per la teoria di Zolotarev, che rimane invece per molti aspetti strettamente legata ai «vecchi» metodi di Kummer. La teoria di Zolotarev rimane quasi nell'oblio fino ai giorni nostri e per gli storici della matematica, che pur hanno ampiamente studiato la teoria dei numeri della fine dell'Ottocento, restava questa lacuna in quella parte fondamentale di storia della matematica che riguarda l'origine del concetto di ideale. Per colmare questa lacuna era necessario prima di tutto capire la teoria di Zolotarev e fornirne una descrizione valida dal punto di vista matematico moderno.

La teoria di Zolotarev può essere interpretata come una teoria della divisibilità nell'anello $\mathbb{O}_{(p)}$ dei cosiddetti *p-interi algebrici* (dove $p$ è un numero primo). Sia dapprima $\mathbb{Z}_{(p)}$ l'anello dei cosiddetti *p-interi razionali*, ossia:

$$\mathbb{Z}_{(p)} = \{s \in \mathbb{Q} : s = m/n,\ m \in \mathbb{Z},\ n \in \mathbb{Z} \setminus p\mathbb{Z}\}.$$

Consideriamo poi un'estensione algebrica finita $\mathbb{K}$ del campo razionale $\mathbb{Q}$. La chiusura intera di $\mathbb{Z}_{(p)}$ in $\mathbb{K}$ è l'anello $\mathbb{O}_{(p)}$ dei *p–interi algebrici*. Si ha inoltre che

$$\mathbb{O}_{(p)} = \{\alpha \in \mathbb{K} : s = \beta/M,\ \beta \in \mathbb{O},\ M \in \mathbb{Z} \setminus p\mathbb{Z}\},$$

ossia $\mathbb{O}_{(p)}$ è il localizzato di $\mathbb{O}$ rispetto alla parte moltiplicativa $\mathbb{Z}\backslash p\mathbb{Z}$. Dall'algebra commutativa moderna sappiamo che $\mathbb{O}_{(p)}$ è un anello semilocale ed è un anello a ideali principali *(PID)*. Denotando con $\pi_1, \ldots, \pi_g$ i primi in $\mathbb{O}_{(p)}$, abbiamo che $\pi_1\mathbb{O}_{(p)}, \ldots, \pi_g\mathbb{O}_{(p)}$ sono gli ideali primi distinti in $\mathbb{O}_{(p)}$. Modernamente, si può facilmente dimostrare che dal fatto che $\mathbb{O}_{(p)}$ è un *PID* con un numero finito di ideali primi si ottiene che $\mathbb{O}$ è un *dominio di Dedekind*.

La potenza più alta di $p$ nella norma $N_{\mathbb{K}/\mathbb{Q}}(\alpha)$ di un $p$-intero algebrico $\alpha$, denotata con $n(\alpha)$, è poi detta *p-norma* (è una funzione moltiplicativa e inoltre $n(\alpha) \geq 1$ per ogni $\alpha$ in $\mathbb{O}_{(p)}$).

Nella sua teoria, Zolotarev definisce dapprima $\alpha$ in $\mathbb{O}$ una unità in $\mathbb{O}_{(p)}$ se $n(\alpha) = 1$ (ossia se $\alpha$ divide 1 in $\mathbb{O}_{(p)}$). Si consideri inoltre l'anello quoziente $\mathbb{O}_{(p)}/p\mathbb{O}_{(p)}$. Notiamo che qualsiasi elemento di questo anello può essere scelto in $\mathbb{O}$, dal momento che vale il seguente isomorfismo:

$$\mathbb{O}/p\mathbb{O} \cong \mathbb{O}_{(p)}/p\mathbb{O}_{(p)}.$$

Zolotarev definisce $p$ primo in $\mathbb{O}$ se ogni rappresentante in $(\mathbb{O}/p\mathbb{O})^*$ è una unità in $\mathbb{O}_{(p)}$. Per gli altri numeri primi $p$, l'idea di Zolotarev è dunque quella di scegliere un insieme di rappresentanti per $(\mathbb{O}/p\mathbb{O})^*$ in modo tale che ognuno di essi abbia $p$-norma minima nella sua classe resto. Chiamiamo questo insieme

$$\mathbb{A} = \{\alpha_1, \ldots, \alpha_r\},$$

dove $r = p^n - 1$. A questo punto, Zolotarev prova il risultato più importante della sua teoria, ossia quello che chiamerò il *Lemma Fondamentale di Zolotarev*, che asserisce il fatto seguente:

1) Sia $\alpha$ in $\mathbb{A}$. Allora $\alpha | p$ in $\mathbb{O}_{(p)}$.

Come immediata conseguenza di questo fatto abbiamo che

2) Sia $\beta$ in $\mathbb{O}_{(p)}/p\mathbb{O}_{(p)}$ e $n(\beta) > 1$. Allora esiste $\alpha$ in $\mathbb{A}$ tale che $n(\alpha) > 1$ e $\alpha | \beta$ in $\mathbb{O}_{(p)}$.

Dal punto 2) segue facilmente che gli elementi $\pi$ irriducibili in $\mathbb{O}_{(p)}$, se esistono, si trovano proprio fra gli elementi dell'insieme $\mathbb{A}$ e quindi in $\mathbb{O}$ per l'isomorfismo precedente (intendendo come elemento irriducibile in $\mathbb{O}_{(p)}$, così come Zolotarev lo ha essenzialmente definito, un elemento $\pi \in \mathbb{O}_{(p)}$ tale che $n(\pi) > 1$ e tale che $\pi$ divide $\gamma$ in $\mathbb{O}_{(p)}$ per ogni $\gamma$ in $\mathbb{O}_{(p)}$ non coprimo con $\pi$ in $\mathbb{O}_{(p)}$. Utilizzando il suo *Lemma Fondamentale*, Zolotarev dimostra quindi che un elemento siffatto esiste. Prendiamo dunque in $\mathbb{A}$ (che è un insieme finito) tutti gli elementi distinti $\pi$ irriducibili in $\mathbb{O}_{(p)}$. A questo punto è facile dimostrare che $\mathbb{O}_{(p)}$ è un dominio a fattorizzazione unica *(UFD)* con un numero finito di elementi primi, cioè che $\mathbb{O}_{(p)}$ è un *PID* e quindi, come già osservato, che $\mathbb{O}$ è un *dominio di Dedekind*. Zolotarev però procede nel modo illustrato di seguito. Ad ogni elemento irriducibile $\pi$, egli associa un *«fattore primo ideale»* $\mathcal{P}$ di $p$, nel modo seguente. Per ogni $\alpha$ in $\mathbb{O}^*$ e

per ogni $k \geq 0$, si dice che

$$\mathcal{P}^k \| \alpha \quad \text{se e solo se} \quad \pi^k \| \alpha \text{in } \mathbb{O}_{(p)}.$$

Più precisamente, viene definita una funzione $v_{\mathcal{P}}$: $\mathbb{O}^* \to \mathbb{N}$, tale che

$$v_{\mathcal{P}}(\alpha) = k \quad \text{se e solo se} \quad \pi^k \| \alpha \text{in} \mathbb{O}_{(p)}$$

per ogni $\alpha$ in $\mathbb{O}^*$ e per ogni $k \geq 0$. Zolotarev prova che la funzione $v_{\mathcal{P}}$ è una valutazione. In conclusione, possiamo dire che *un numero primo ideale $\mathcal{P}$ è introdotto come una valutazione, che è la valutazione definita da un elemento $\pi$ in $\mathbb{O}_{(p)}$ irriducibile in $\mathbb{O}_{(p)}$* o, come modernamente si direbbe, *uniformizzante locale in $\mathbb{O}_{(p)}$*. Sia $\Gamma$ l'insieme delle valutazioni corrispondenti agli elementi irriducibili di $\mathbb{O}_{(p)}$ per ogni numero primo $p$. Per questo insieme, Zolotarev dimostra essenzialmente il fatto seguente, che è lo scopo, diciamo, della sua teoria. Siano $\alpha$ e $\beta$ elementi di $\mathbb{O}^*$. Allora $\alpha$ è divisibile per $\beta$ in $\mathbb{O}$ se e solo se $v(\beta) \leq v(\alpha)$ per ogni $v \in \Gamma$ tale che $v(\beta) > 0$. Si noti del resto che vale il teorema seguente:

TEOREMA. – *Un insieme di valutazioni $\Gamma$ di $\mathbb{K}$ induce una teoria dei divisori su $\mathbb{O}$ se e solo se valgono le due condizioni seguenti:*

(i) *Siano $\alpha$ e $\beta$ in $\mathbb{O}^*$; allora $\alpha$ è divisibile per $\beta$ in $\mathbb{O}$ se e solo se $v(\beta) \leq v(\alpha)$ per ogni $v \in \Gamma$ tale che $v(\beta) > 0$.*

(ii) *Per ogni insieme di valutazioni distinte $v_1, v_2, \ldots, v_m$ di $\Gamma$ e per ogni insieme di interi non negativi $k_1, k_2, \ldots, k_m$ esiste un elemento $\alpha$ in $\mathbb{O}$ tale che*:

$$v_1(\alpha) = k_1,\ v_2(\alpha) = k_2,\ \ldots,\ v_m(\alpha) = k_m.$$

La seconda condizione si deriva molto facilmente dalle definizioni di Zolotarev come io ho dimostrato nella mia tesi. Pertanto, riferendoci a questo teorema possiamo dire effettivamente che la teoria dei numeri ideali di Zolotarev non è altro che una *teoria dei divisori* per l'anello $\mathbb{O}$. Più precisamente, per il *Teorema*, partendo dall'anello $\mathbb{O}_{(p)}$ e dall'insieme dei suoi elementi irriducibili, è possibile definire un insieme di valutazioni che induce una *teoria dei divisori* in $\mathbb{O}$.

Dunque, poiché $\mathbb{O}$ è un *dominio di Dedekind*, Zolotarev ottiene una teoria equivalente alla teoria degli ideali in $\mathbb{O}$ e quindi risolve anch'egli come Dedekind e contemporaneamente a Dedekind il problema di generalizzare la teoria di Kummer ad ogni anello $\mathbb{O}$ di interi algebrici.

È d'uopo osservare che Zolotarev non introduce direttamente l'anello $\mathbb{O}_{(p)}$ dei $p$-interi algebrici che fu definito ben più tardi, agli inizi del Novecento da Kurt Hensel (1861-1941), come chiusura intera nell'estensione semplice considerata dell'anello $\mathbb{Z}_{(p)}$ dei $p$-interi razionali e (in maniera equivalente) come il localizzato di $\mathbb{O}$ rispetto all'insieme moltiplicativo $\mathbb{Z}\backslash p\mathbb{Z}$. Zolotarev utilizza solo quello che io ho definito «*divisibilità modulo p*» nell'anello $\mathbb{O}$ degli interi algebrici. Ossia, dati

$\alpha$ e $\beta$ in $\mathbb{O}$, si dice che «$\alpha|\beta$ *modulo* $p$» se esiste $H$ in $\mathbb{Z}\backslash p\mathbb{Z}$ e $\gamma$ in $\mathbb{O}$ tali che

$$\alpha\gamma = \beta H \, .$$

È chiaro che questa definizione di divisibilità estesa in maniera naturale all'anello $\mathbb{O}_{(p)}$ non è altro che la definizione di divisibilità stessa in $\mathbb{O}_{(p)}$. Partendo da questo fatto, risulta abbastanza semplice e naturale interpretare la teoria di Zolotarev utilizzando il linguaggio della divisibilità in $\mathbb{O}_{(p)}$.

I metodi che Zolotarev utilizza si riferiscono alla pratica della teoria dei numeri nota alla fine dell'Ottocento. Non si tratta di un approccio completamente nuovo e radicalmente diverso nei fondamenti come quello presentato da Dedekind con l'introduzione del concetto di ideale. In particolare, sono evidenti le analogie con la teoria di Kummer. Sia Kummer che Zolotarev introducono i numeri primi ideali essenzialmente come valutazioni, dopodiché le loro due teorie procedono esattamente nello stesso modo, seguono gli stessi passi, giungendo entrambe al passo fondamentale: $\alpha \in \mathbb{O}^*$ *è divisibile per* $\beta \in \mathbb{O}^*$ *nell'anello* $\mathbb{O}$ *se e solo se* $v(\beta) \leqslant v(\alpha)$ *per ogni* $v$ (dove $v$ è una qualunque valutazione definita da un elemento irriducibile in $\mathbb{O}_{(p)}$, come decritto precedentemente).

Questo passo determina la teoria di Kummer e quella di Zolotarev come teoria dei divisori per anelli di interi algebrici. In questo senso e in questo contesto, Zolotarev può essere considerato un immediato *successore* di Kummer.

## BIBLIOGRAFIA

[1] KUMMER E. E. *Zur Theorie der Complexen Zahlen*, Monatsber. Akad. Wiss. Berlin (1846), 87-96. Anche in *J. Reine Angew. Math.*, **35** (1847), 319-326.

[2] DEDEKIND R., *X supplemento a* Vorlesungen über Zahlentheorie von P. G. Lejeune Dirichlet, seconda edizione, Vieweg, Braunschweig (1871).

[3] DEDEKIND R., *Sur la théorie des nombres entiers algébriques*, Bull. des Sci. Math. Astron. (1), **XI** (1876), 278-288; 2$^{e}$ Série, **I** (1877), 1$^{re}$ partie, 17-41, 69-92, 144-164, 207-248.

[4] ZOLOTAREV E. I., *Polnoe Sobranie Sochineny Egora Ivanovicha Zolotareva (Opere complete di Egor Ivanovich Zolotarev)*, **I-II**, V. A Steklov Institute of Physics and Mathematics, Leningrad (1931-1932).

[5] ZOLOTAREV E. I., *Sur la théorie des nombres complexes*, Journal de Mathématiques, **6** 3$^{e}$ Série (1880), 51-84, 129-166. Anche nelle, *Opere complete*, **I** 72-179.

Via delle Fornaci, 19/A - 57128 Livorno; e-mail: p.piazza@tin.it
Dottorato in Matematica (sede amministrativa: Messina) - Ciclo X
Direttore di ricerca: Prof. Aldo Brigaglia, Università di Palermo