UN'INTRODUZIONE STORICA ALLA TEORIA DELLA DIVISIBILITÀ NEI DOMINI INTEGRI

Stefania Gabelli
Dipartimento di Matematica

Il gruppo di ricerca in Algebra dell'Università di Roma Tre è formato da:

M. Fontana (Prof. Ordinario), S. Gabelli (Prof. Associato), F. Pappalardi (Prof. Associato), F. Girolami (Ricercatore), F. Tartarone (Ricercatore), G. Picozza (Dottorando), A. Susa (Dottorando).

Il lavoro di questo gruppo si svolge nell'ambito dell'*Algebra Commutativa* e della *Teoria Algebrica dei Numeri*: due settori importanti della ricerca di base contemporanea in Algebra.

Per motivi di spazio e competenza, tralascerò qui di parlare della Teoria dei Numeri, settore in cui lavorano F. Pappalardi e A. Susa, scegliendo di illustrare alcuni temi di ricerca in Algebra Commutativa.

L'Algebra è nata inizialmente come lo studio delle equazioni polinomiali; infatti il termine Algebra deriva dal termine arabo *Al-jabr*, che indica l'operazione di spostare i termini di una equazione da una parte all'altra del segno di uguaglianza. Successivamente l'Algebra si è evoluta nello studio delle cosiddette *strutture algebriche*, cioè degli insiemi in cui sono definite alcune operazioni che soddisfano determinati assiomi.

In Italia è presente una lunga tradizione di studi algebrici, che risale al *Liber Abaci* di Leonardo Pisano, detto il Fibonacci, del 1202.

Nel Rinascimento il contributo della scuola italiana bolognese allo studio delle equazioni polinomiali è stato fondamentale. Basti ricordare la scoperta delle formule risolutive delle equazioni di terzo grado (attorno al 1515 da parte di Scipione del Ferro e indipendentemente Nicolò Tartaglia) ed in seguito delle formule per le equazioni di quarto grado (da parte di Ludovico Ferrari). All'illustrazione di queste formule è dedicata buona parte del libro *Algebra* di Raffaele Bombelli, del 1572.

Successivamente molti grandi matematici tentarono di determinare formule risolutive per le equazioni di grado superiore. Il primo a dimostrare l'impossibilità di risolvere per radicali l'equazione generale di quinto grado è stato l'italiano Paolo Ruffini, all'inizio dell'800. Ma il contributo più importante alla teoria delle equazioni polinomiali è stato dato da Evariste Galois, che nel 1831 stabilì dei criteri precisi per determinare se una data equazione polinomiale sia o meno risolubile per radicali.

Galois è forse uno dei pochi matematici noti ai non specialisti. La sua vita avventurosa e le circostanze della sua morte, avvenuta in duello all'età di venti anni, hanno contribuito non poco alla nascita di quella figura dell'immaginario collettivo che è il matematico "genio ribelle".

Agli studi di Galois risale l'origine di una delle più importanti strutture algebriche, quella di *Gruppo*. Oggetto di studio dell'Algebra Commutativa sono invece delle strutture algebriche più complesse che si chiamano *Anelli Commutativi*.

Un anello commutativo è un insieme in cui sono definite due operazioni, che possiamo chiamare *addizione* e *moltiplicazione*, che soddisfano tutte le buone proprietà delle ope-

razioni tra numeri o tra polinomi a coefficienti numerici, come ad esempio le proprietà associativa, commutativa e distributiva, l'esistenza di uno zero e di una unità. A queste proprietà di base se ne possono aggiungere poi varie altre, che caratterizzano le particolari strutture alle quali ci si vuole interessare. Ad esempio un *dominio integro* è un anello commutativo in cui vale la legge dell'*annullamento del prodotto*, ovvero in cui il prodotto di due elementi diversi da zero non può essere uguale a zero.

La ricerca in questo settore è molto specializzata e si avvale di metodi diversi; gli algebristi commutativi di Roma Tre lavorano principalmente nell'ambito della *Teoria degli Ideali*.

Illustrare in modo comprensibile questi metodi senza fare uso del linguaggio specifico della materia è praticamente impossibile. Infatti molte parole che hanno un senso compiuto nel linguaggio corrente assumono in matematica un significato completamente diverso. Alcune delle parole chiave che ricorrono nella Teoria degli Ideali sono ad esempio: *Ideale massimale, primo, divisoriale, forte, invertibile; Trasformato di un ideale; Contenuto di un ideale; Dominio locale, essenziale, localmente diviso, Isomorfismo; (Completa) chiusura integrale; Normalità; Seminormalità; Gruppo delle Classi di ideali; Divisibilità; Fattorialità; Sistemi localizzanti; Traccia, radicale;* e addirittura *Sollevamento di alberi (di ideali primi).*

Chi ascoltasse una conversazione di matematica su questi argomenti e cercasse di capire di che cosa si stia parlando attribuendo alle parole il loro significato usuale avrebbe serie difficoltà. Mi sono resa bene conto di ciò qualche tempo fa: mentre viaggiavamo in treno, stavo illustrando ad una collega un problema che mi interessava quando un compagno di viaggio, perplesso e incuriosito, ci ha chiesto di che cosa mai stessimo discutendo – forse di sociologia? La risposta che si trattava di matematica lo ha lasciato meravigliato ed incredulo.

Nell'impossibilità di dare qui le definizioni tecniche necessarie a comprendere anche soltanto gli enunciati dei teoremi scientificamente più rilevanti dimostrati di recente dal nostro gruppo, cercherò di illustrare il tipo di ricerca che si svolge in algebra commutativa attraverso le origini storiche di un problema di cui si sono occupati alcuni di noi: lo studio delle *proprietà aritmetiche dei domini integri*.

1. Le origini: La Congettura di Fermat

I sei libri dell'*Arithmetica* di Diofanto (circa 250 A.C.), miracolosamente scampati al barbarico incendio della biblioteca di Alessandria, sono stati tra gli ultimi libri dei matematici greci ad essere tradotti in latino. In esso venivano affrontati più di cento problemi aritmetici che avevano per soluzione numeri interi. Questo tipo di problemi vengono oggi chiamati *Problemi Diofantei*.

Pierre de Fermat (1601-1665), il precursore della moderna Teoria dei Numeri, usava annotare le sue osservazioni in margine alla sua copia dell'Arithmetica (una traduzione di Bachet, del 1621). Molte di queste acute annotazioni consistevano nell'enunciazione di vari teoremi, che Fermat asseriva di aver provato, ma di cui purtroppo non dava alcuna dimostrazione. Agli inizi dell'800 tutti i problemi posti da Fermat erano stati risolti, in positivo o in negativo, tranne quello che viene oggi conosciuto come *l'Ultimo Teorema di Fermat*.

In relazione ad alcuni quesiti riguardanti il Teorema di Pitagora, Fermat scrisse di aver trovato una "sorprendente dimostrazione" del seguente fatto:

Ultimo Teorema di Fermat (1637):
Per $n \geq 3$, non esistono dei numeri interi *a, b, c* diversi da zero tali che

$a^n + b^n = c^n$;

ovvero l'equazione

$X^n + Y^n = Z^n$

non ha soluzioni intere non banali.

Nonostante la semplicità dell'enunciato, questo problema si è rivelato essere uno tra i più difficili di tutti i tempi. Nel tentativo di dimostrarlo, sono stati introdotti molti nuovi concetti e metodi che hanno apportato grande ricchezza alla matematica moderna, favorendone lo sviluppo e la diversificazione. Nel corso dei secoli la congettura di Fermat è stata dimostrata per valori sempre più grandi di *n*, ma è stata definitivamente risolta soltanto nel 1994, circa 350 anni dopo la sua formulazione, da A. Wiles, con il contributo di R. Taylor.

La dimostrazione dell'Ultimo Teorema di Fermat è una delle più grandi conquiste matematiche del secolo scorso; in essa si fa uso di tutte le tecniche più recenti e sofisticate, accessibili soltanto a pochi specialisti. È perciò molto probabile che la congettura di Fermat sia stata una geniale intuizione basata su un errore di ragionamento.

2. La nascita del concetto di anello

Il Teorema di Fermat è evidentemente falso per $n = 2$, perchè, come era già noto ad Euclide, esistono (infiniti) triangoli rettangoli con lati di lunghezza intera ed inoltre il Teorema di Pitagora ci assicura che, se i cateti hanno lunghezza uguale ad *a* e *b* e l'ipotenusa ha lunghezza uguale a *c*, allora $a^2 + b^2 = c^2$; dunque la terna di numeri interi (*a, b, c*) è soluzione dell'equazione $X^2 + Y^2 = Z^2$. Le terne di questo tipo, come ad esempio (*2, 3, 5*) oppure (*5, 12, 13*), si dicono *terne pitagoriche.*

Per dimostrare il Teorema di Fermat per $n > 2$, ci si può ridurre facilmente a considerare il caso in cui $n = 4$ oppure $n = p$, con *p* un numero primo dispari.

Per convincersene, basta ricordare che ogni numero naturale si può scrivere in modo unico come prodotto di numeri primi (*Teorema Fondamentale dell'Aritmetica*); dunque ogni numero intero maggiore di *2* è un multiplo di *4* oppure di un numero primo $p > 2$. Inoltre, se il Teorema è vero per un numero naturale *m*, è vero anche per tutti i suoi multipli *mk* .

Infatti, per $k, m \geq 1$, posto $U = X^m$, $V = Y^m$, $W = Z^m$, se l'equazione

$U^k + V^k = W^k$

non ha soluzioni, non le può avere neanche l'equazione

$(X^m)^k + (Y^m)^k = (Z^m)^k$.

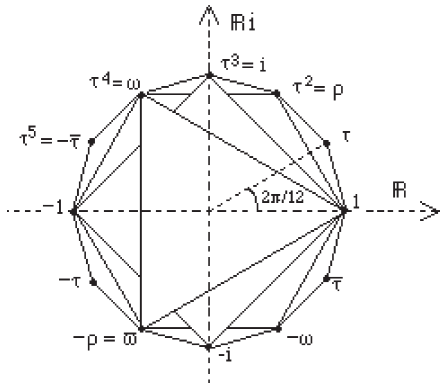
Un metodo per dimostrare la congettura nel caso $n = 4$ si trova già negli scritti di Fermat e probabilmente Fermat pensava erroneamente che questo stesso metodo potesse essere impiegato per risolvere il caso generale. Effettivamente questa tecnica è stata poi usata da L. Euler per dimostrare nel 1770, seppure in modo incompleto, il caso $n = 3$; ma si è rivelata inefficace per valori superiori.

Euler ebbe la fondamentale idea di ampliare il concetto di numero intero, lavorando con

dei particolari numeri complessi che vengono oggi chiamati *interi algebrici*. Per illustrarne l'utilità in relazione alla congettura di Fermat, è necessario introdurre *le radici complesse n-sime dell'unità*.

Un numero complesso ζ è una radice *n*-sima dell'unità se $\zeta^n = 1$. Le radici *n*-sime dell'unità sono dunque le soluzioni complesse dell'equazione $X^n - 1 = 0$. Esse sono tutte distinte e, nel piano complesso, si dispongono ai vertici di un poligono regolare di *n* lati, centrato nell'origine e con un vertice in *1*.

Nella figura sono rappresentate le radici *12*-sime, che contengono quelle terze, quarte, seste.



Se *p* è un numero primo, una proprietà molto utile è il fatto che le radici *p*-esime sono tutte esprimibili come potenze di una qualsiasi di esse diversa da *1*. Cioè, se $\xi \neq 1$ è una radice p-esima, allora tutte e sole le radici p-esime sono:

$$1 , \xi , \xi^2 \dots , \xi^{p-1} .$$

Con l'aiuto delle radici *p*-esime dell'unità, l'equazione di Fermat si può fattorizzare linearmente:

$$X^p + Y^p = (X + Y)(X + \xi Y)(X + \xi^2 Y)\dots(X + \xi^{p-1} Y) = Z^p .$$

Sostituendo alle indeterminate *X, Y, Z* dei numeri interi *a, b, c,* otteniamo una fattorizzazione in *numeri complessi*:

$$a^p + b^p = (a + b)(a + \xi b)(a + \xi^2 b)\dots(a + \xi^{p-1} b) = c^p$$

dove i fattori $a + \xi^i b$ sono del tipo:

$$a_0 + a_1\xi + a_2\xi^2 + \dots + a_{p-1}\xi^{p-1} ,$$

con $a_0 , a_1 , \dots , a_{p-1}$ numeri interi.

L'insieme di tutti i numeri interi si indica con $\mathbb{Z}$ e l'insieme dei numeri complessi sopra definiti si indica con $\mathbb{Z}[\xi]$. Per ogni primo *p* ,

$$\mathbb{Z}[\xi] = \{a_0 + a_1\xi + \dots + a_{p-1}\xi^{p-1} \; ; \; a_i \in \mathbb{Z}\}$$

è un anello commutativo integro ed è il prototipo di questa classe di anelli; esso si chiama l'*anello* degli *interi ciclotomici* ed è un particolare anello di *interi algebrici*.

Il termine *anello* è dovuto al fatto che le radici *n*-sime dell'unità si dispongono su una circonferenza, mentre il termine *ciclotomico* (che deriva dal greco e significa *che taglia il cerchio*) è dovuto al fatto che esse tagliano tale circonferenza in *n* archi uguali.

3. La nascita del concetto di ideale

Nel 1847 G. Lamé presentò all'Accademia di Parigi una sua dimostrazione dell'Ultimo Teorema di Fermat. Essa si basava sul fatto che nell'anello degli interi ciclotomici valesse un teorema analogo al Teorema Fondamentale dell'Aritmetica, ovvero sul fatto che ogni intero ciclotomico si potesse fattorizzare in modo unico nel prodotto di interi ciclotomici irriducibili.

Come fu osservato da J. Liouville, tale supposizione non aveva nessun fondamento. Ed infatti E. Kummer, venuto a conoscenza del problema sollevato da Liouville, gli scrisse che essa era in realtà del tutto falsa. Il più piccolo numero primo per il quale il teorema di fattorizzazione fallisce è *23* .

Kummer dimostrò tuttavia che in certi casi il teorema di fattorizzazione unica poteva essere ripristinato per gli interi ciclotomici introducendo dei *numeri ideali*. Questo permetteva di provare il Teorema di Fermat per quasi tutti i numeri primi minori di *100* .

In una sua fondamentale memoria del 1871, R. Dedekind osservò poi che la funzione dei numeri ideali di Kummer poteva essere svolta più generalmente in tutti gli anelli di interi algebrici da particolari sottoinsiemi, che egli chiamò ancora *ideali*.

Gli ideali, come i numeri, si possono addizionare e moltiplicare. Dedekind dimostrò che in ogni anello di interi algebrici un ideale si può sempre fattorizzare in modo unico nel prodotto di ideali primi, anche nei casi in cui il teorema di fattorizzazione unica fallisce per gli elementi.

Senza entrare nei dettagli, facciamo un esempio per illustrare questo fatto.

Esempio:

Consideriamo l'anello degli interi algebrici del tipo $a+bi\sqrt{5}$, dove a e b sono numeri interi e i è l'unità immaginaria:

$$\mathbb{Z}[i\sqrt{5}] = \{a+bi\sqrt{5};\ a, b \in \mathbb{Z},\ i^2 = -1\}.$$

Alcuni elementi di questo anello si possono fattorizzare in modi differenti nel prodotto di elementi irriducibili, ad esempio:

$$21 = 3\cdot 7 = (1+2i\sqrt{5})(1-2i\sqrt{5}).$$

Passando agli ideali, abbiamo:

$$<21> = <3><7>\ ;$$

ma gli ideali $<3>$ e $<7>$ non sono primi. Infatti la loro fattorizzazione in ideali primi è:

$$<3> = <3,1+2i\sqrt{5}><3,1-2i\sqrt{5}>\ ;$$

$$<7> = <7,1+2i\sqrt{5}><7,1-2i\sqrt{5}>\ .$$

Dunque l'unica fattorizzazione di $<21>$ in ideali primi è:

$$<21> = <3,1+2i\sqrt{5}><3,1-2i\sqrt{5}><7,1+2i\sqrt{5}><7,1-2i\sqrt{5}>.$$

4. Il concetto astratto di anello

La formalizzazione delle proprietà degli anelli di interi algebrici e dei polinomi a coefficienti numerici ha portato all'inizio del 1900 al concetto astratto di *anello*.

Negli anni '20, ci sono stati enormi progressi nello studio degli anelli commutativi, soprattutto ad opera di maestri quali Emmy Noether ed Emil Artin.

E. Noether ha caratterizzato tra l'altro i domini integri in cui, come negli anelli di interi algebrici, ogni ideale non nullo è prodotto di ideali primi. Questi anelli vengono oggi chiamati *Domini di Dedekind*.

La classe dei Domini di Dedekind è l'intersezione di due classi fondamentali di anelli, gli *Anelli Noetheriani* e i *Domini di Prüfer*.

Gli Anelli Noetheriani (che prendono il nome da E. Noether) sono gli anelli che intervengono in Geometria Algebrica ed hanno il loro prototipo negli anelli di funzioni algebriche.

I Domini di Prüfer, (che prendono il nome da H. Prüfer) sono gli anelli che intervengono nella Teoria Algebrica dei Numeri ed hanno il loro prototipo nei domini di *valutazione*.

5. La Teoria degli Ideali come strumento per studiare i problemi di divisibilità

La validità della legge di annullamento del prodotto permette di introdurre per i domini integri i concetti di *massimo comune divisore*, *minimo comune multiplo*, elemento *irriducibile* e *primo*, *fattorizzazione* e in definitiva di costruire una *Teoria della Divisibilità* del tutto simile a quella valida per i numeri interi e i polinomi a coefficienti razionali.

La Teoria degli Ideali è uno strumento molto potente per studiare i problemi di divisibilità. Ad esempio la validità del teorema di fattorizzazione unica si riflette nell'annullarsi del cosiddetto *Gruppo delle Classi degli ideali divisoriali*. Un teorema del 1960, dovuto a P. Samuel, asserisce infatti che in un dominio vale il teorema di fattorizzazione unica per gli elementi se e soltanto se il dominio è di Krull e il suo gruppo delle classi è nullo (i *domini di Krull* prendono il nome dal matematico W. Krull e sono generalizzazioni dei domini di Dedekind).

In seguito la nozione di Gruppo delle Classi è stata estesa ad un qualsiasi dominio, con interessanti applicazioni. Tra queste citiamo una generalizzazione del teorema di Samuel, ottenuta da A. Bouvier e M. Zafrullah nel 1982. Essi hanno dimostrato che in un dominio esiste sempre il massimo comune divisore di due elementi se e soltanto se il dominio è pseudo-Prüferiano e il suo gruppo delle classi è nullo (i domini *pseudo-Prüferiani* includono i domini di Prüfer).

Dal punto di vista della divisibilità:

- I domini $\mathbb{Z}$ (dei numeri interi) e $\mathbb{Q}[X]$ (dei polinomi nell'indeterminata X a coefficienti razionali) sono molto buoni. Essi sono *Domini Euclidei*;

- I domini $\mathbb{Z}[X]$ (dei polinomi nell'indeterminata X a coefficienti interi) e $\mathbb{Q}[X,Y]$ (dei polinomi nelle indeterminate X e Y a coefficienti razionali) sono ancora buoni. Essi sono *Domini a Fattorizzazione Unica*;

- Il dominio $\mathbb{Z}+X\mathbb{Q}[X]$ (dei polinomi in X a coefficienti razionali il cui termine noto è intero) è meno buono, ma in esso esiste ancora il massimo comune divisore di due elementi.

- I domini $\mathbb{Z}[i\sqrt{5}]$ e $\mathbb{R}+X\mathbb{C}[X]$ (dei polinomi in X a coefficienti complessi il cui termine noto è reale) sono quasi buoni. Essi sono *Domini metà-Fattoriali*, ovvero la fattorizzazione in elementi irriducibili esiste ma non è unica, tuttavia due fattorizzazioni hanno lo stesso numero di elementi;

- Il dominio *Int(ℤ)* dei polinomi a valori interi su ℤ (i polinomi a coefficienti razionali che calcolati in un intero assumono valore intero, come ad esempio $X(X-1)/2$) è un dominio di Prüfer che non ha alcuna buona proprietà di fattorizzazione.

6. Alcuni contributi degli algebristi di Roma Tre

Un problema generale della Teoria degli Anelli consiste nel confrontare le proprietà di due anelli *A* e *B* nel caso in cui *A* sia contenuto in *B*. Casi rilevanti si ottengono quando *B* è una *localizzazione* di *A*, oppure B è un *anello di polinomi* su *A*, oppure *A* è un *pull-back* di *B*.

Per fare qualche esempio:

- L'anello delle frazioni del tipo a/p^n , dove *a* è un intero qualsiasi e *p* un numero primo fissato, è una localizzazione dell'anello ℤ degli interi;
- Gli anelli $\mathbb{Q}[X]$, $\mathbb{Z}[X]$, $\mathbb{Q}[X,Y]$ sopra considerati sono anelli di polinomi;
- Gli anelli $\mathbb{Z}+X\mathbb{Q}[X]$ e $\mathbb{R}+X\mathbb{C}[X]$ sopra definiti sono anelli ottenuti per pull-back.

Come abbiamo visto, per confrontare le proprietà di divisibilità di due domini, è utile confrontare i loro gruppi delle classi di ideali. Alcuni contributi degli algebristi commutativi di Roma Tre a questo problema sono stati i seguenti:

Caratterizzazione dei domini A che hanno gruppo delle classi isomorfo a quello dell'anello dei polinomi su A:

- **S. Gabelli**, *On divisorial ideals in polynomial rings over Mori domains*, Comm. Algebra, 1987.

Condizioni di sufficienza perchè il gruppo delle classi di una localizzazione di A sia omomorfo a quello di A :

- **S. Gabelli – M. Roitman**, *On Nagata's Theorem for the class group*, J. Pure Appl. Algebra, 1990;
- **S. Gabelli**, *On Nagata's Theorem for the class group II*, Lecture Notes in Pure and Appl. Math., n. 206, 1999.

Descrizione del gruppo delle classi di anelli ottenuti per pull-back:

- **M. Fontana - S. Gabelli**, *On the class group and the local class group of a pull-back*, J. Algebra, 1996.

Dal momento poi che il gruppo delle classi misura in qualche modo le proprietà di fattorizzazione, è importante poter calcolare questo gruppo, o almeno dare dei criteri per stabilire quando esso è nullo. Anche nei casi classici questo non è sempre possibile. Ad esempio esistono formule ben note per calcolare il numero delle classi di ideali di particolari anelli di interi algebrici; tuttavia il problema di determinare tutti gli anelli di interi algebrici che hanno gruppo delle classi nullo, ovvero che sono a fattorizzazione unica, è ancora aperto.

Il problema si può semplificare se, come nel caso dei domini di Krull, si possono trovare dei *generatori* per il gruppo delle classi, ovvero dei particolari ideali la cui struttura determina completamente quella del gruppo delle classi.

Alcuni risultati ottenuti dagli algebristi di Roma Tre sono i seguenti:

Descrizione del gruppo delle classi di particolari classi di domini:

- **V. Barucci - S. Gabelli**, *On the class group of a Mori domain*, J. Algebra, 1987;
- **M. Fontana - N. Popescu**, *Sur une classe d'anneaux de Prüfer avec groupe de classes de torsion*, Comm. Algebra, 1995;
- **S. Gabelli**, *A class of Prüfer domains with nice divisorial ideals*, Lecture Notes in Pure and Appl. Math., n. 185, 1997;
- **S. Gabelli - N. Popescu**, *Invertible and divisorial ideals of generalized Dedekind domains,* J. Pure Appl. Algebra, 1999.

Costruzione di domini con gruppo delle classi assegnato:

- **V. Barucci - S. Gabelli – M. Roitman**, *The class group of a strongly Mori domain*, Comm. Algebra, 1994.

Studio dei generatori del gruppo delle classi:

- **M. Fontana - S. Gabelli**, *Prüfer domains with class group generated by the classes of invertible maximal ideals*, Comm. Algebra, 1997;
- **S. Gabelli - F. Tartarone**, *On the class group of integer-valued polynomial rings over Krull domains,* J. Pure Appl. Algebra, 2000.