Van der Waerden - Algebra - pag. 69 - (Anhang 1)

UNIVERSITA' DEGLI STUDI DI MODENA

La dimostrazione del fatto che è possibile dividere l'uno per l'altro due numeri dell'anello di Gauss e ottenere per resto un numero dalla norma minore del divisore si può ottenere anche come segue (col vantaggio di poterla estendere anche ad altri anelli):

Sia $\alpha = a + bi$ e $\beta = c + di$ e sia da dividere α/β

secondo il procedimento abituale si fa

$(a+bi)/(c+di) = (a+bi)(c-di)/(c^2 + d^2) =$

$= ((ac+bd) + i(bc-ad)) / (c^2 + d^2)$

Si dividano ora la parte reale ed il coefficiente dell'immaginario per $(c^2 + d^2)$: si ottiene

$ac+bd = (c^2 + d^2)\, p + u$

$bc - ad = (c^2 + d^2)\, q + v$

essendo u e v in valore assoluto minori ciascuno di $1/2$ (perchè non ci importa di avere resti negativi purchè siano piccoli in valore assoluto) . Quindi

$(a+bi)/(c+di) = p+iq + (u+iv)/(c^2 + d^2)$

Si osservi ora che il numero $(u+iv)/(c^2+d^2)$ moltiplicato per $c+id$ dà un intero (complesso) ρ che è il resto . Quindi

$N(\rho) = N(c+id)\, N((u+iv)/(c^2 + d^2))$

Ma abbiamo osservato che ciascuno dei due numeri $u/(c^2 + d^2)$ e $v/(c^2 + d^2)$ è minore in valore assoluto di $1/2$ ~~quindi~~ la norma del numero per cui

$(u+iv)/(c^2+d^2)$ è minore di $1/4 + 1/4 = 1/2$

quindi la norma di ρ è minore di quella del divisore.

Esempio

$$\frac{10+11i}{2+3i} = \frac{(10+11i)(2-3i)}{13} = \frac{53}{13} + i\,\frac{-8}{13} =$$

$$= 4 - i + \frac{1+5i}{13}$$

ma è $N\left(\frac{1+5i}{13}\right) = \frac{26}{169} < 1$

e moltiplicando per $(2+3i)$ si ha

$$10+11i = (4-i)(2+3i) + \frac{(1+5i)(2+3i)}{13} =$$

$$= (4-i)(2+3i) + (-1+i)$$

Il resto è $(-1+i)$ col modulo

$N(\text{resto}) = N\left(\frac{1+5i}{13}\right) N(2+3i)$ segue

$N(\text{resto}) < N(\text{divisore})$

Cfr. Bianchi: Numeri algebrici - Cap. II § 15. p. 62 et sqq.

UNIVERSITÀ DEGLI STUDI DI MODENA

Anello dei numeri $a + b\rho$ con a e b interi e ρ che obbedisce alla regola di calcolo

(1) $$\rho^2 = -\rho - 1$$

Si noti anzitutto che dalla (1) segue

(2) $$\rho^3 = 1$$

infatti moltiplicando la (1) per ρ si ha

$$\rho^3 = -\rho^2 - \rho^1 = (\rho + 1) - \rho = 1$$

Diciamo "coniugato" del numero $a + b\rho$ il numero

$$a + b\rho^2$$

Si ha immediatamente che l'operazione di coniugio è involutoria, per la (2); definiamo poi la "norma" di un numero come prodotto del numero per il suo coniugato.

Si ha

$$N(a+b\rho) = (a+b\rho)(a+b\rho^2) = a^2 + b^2\rho^3 + ab(\rho + \rho^2) =$$
$$= a^2 + b^2 - ab$$

Si verifica facilmente che la norma di un numero è sempre positiva; infatti si ha

$$a^2 + b^2 - ab = (a - b/2)^2 + 3b^2/4$$

Si verifica pure facilmente che

" La norma di un prodotto è il prodotto delle norme dei fattori "

Sia infatti il prodotto

$$(a+b\rho)(c+d\rho) = ac + bd(-\rho - 1) + (ad+bc)\rho =$$
$$= ac - bd + (ad+bc-bd)\rho$$

allora la sua norma è data da

$$(ac-bd)^2 + (ad+bc-bd)^2 - (ac-bd)(ad+bc-bd)$$

Sviluppando i calcoli si verifica che questa espressione

./.

N.B. I numeri $\pm 1, \pm\rho, \pm\rho^2$ formano le unità-perché $N(1) = N(\rho) = N(\rho^2)$

è uguale al prodotto delle norme
$(a^2 + b^2 - ab)(c^2 + d^2 - cd)$

~~Pertanto si possono rifare gli stessi ragionamenti che sono svolti nel testo a proposito del corpo degli interi a+bi di Gauss.~~ dell'anello

Si osservi che è possibile dall'anello dei numeri ora definiti $a+b\rho$ passare ad un corpo-quoziente perchè è semplicissimo definire il reciproco di un numero : si ha infatti

$$1/(a+b\rho) = (a+b\rho^2)/N(a+b\rho)$$

* Si immagini ora di eseguire la divisione di un numero su un altro $\frac{a+b\rho}{c+d\rho}$; ripetendo le considerazioni fatte nell'Anhang 1 si conclude che si arriverà ad un resto $\frac{u+v\rho}{N(c+d\rho)}$ nel quale $\frac{|u|}{N} \leq 1/2$; $\frac{|v|}{N} \leq 1/2$

Ora la norma del resto ~~divisa~~ per $N(c+d\rho)$

$\frac{u^2+v^2-uv}{N^2}$ e si ha

$$\frac{|u^2+v^2-uv|}{N^2} \leq \frac{u^2+v^2+uv}{N^2} \leq \frac{1}{4}+\frac{1}{4}+\frac{1}{4} = 3/4$$

Quindi, moltiplicando per $c+d\rho$ e con ragionamenti analoghi a quelli fatti ivi si vede che la norma del resto è minore della norma del divisore. Si conclude che è possibile istituire un algoritmo euclideo.

Bianchi: Numeri algebrici Cap. III° §26 p. 101

et 199

Van der Waerden - Algebra - pg. 69 - Aufg. 5 (II°)

UNIVERSITA' DEGLI STUDI DI MODENA

Le stesse considerazioni si possono fare per l'anello dei numeri $a+b\sqrt{2}$; si definisce anzitutto il coniugato del numero $a + b\sqrt{2}$ come il numero $a-b\sqrt{2}$ e poi si definisce la norma di un numero come il valore assoluto del prodotto dei due coniugati

$$N(a+b\sqrt{2}) = |(a+b\sqrt{2})(a-b\sqrt{2})| = |a^2-2b^2|$$

risulta chiaro che la norma di un numero non può essere zero se il numero non è zero, perchè la equazione

$$a^2 - 2\,b^2 = 0$$

non ammette soluzioni intere. Inoltre la norma di un prodotto è data dal prodotto delle norme: infatti $(a+b\sqrt{2})(c+d\sqrt{2}) = ac+2bd+(ad+bc)\sqrt{2}$ e quindi la sua norma è data da

$$(ac+2bd)^2 - 2\,(ad+bc)^2$$

si verifica che questo numero è uguale al prodotto dei valori assoluti di

$$(a^2-2b^2)(c^2-2d^2)$$

* La funzione dell'algoritmo euclideo viene scritta come sia in (1), in (2). Ha la seguente

$$\frac{a+b\sqrt{2}}{c+d\sqrt{2}} = \frac{(a+b\sqrt{2})(c-d\sqrt{2})}{c^2-2d^2} = \frac{ac-2bd+\sqrt{2}(bc-ad)}{c^2-2d^2} =$$

$$= p+q\sqrt{2} + \frac{u+\sqrt{2}v}{r(c+d\sqrt{2})}$$

Si ha anzitutto che $N(\text{resto}) = N(c+d\sqrt{2})\, N\left[\frac{u+v\sqrt{2}}{N(c+d\sqrt{2})}\right]$

Ora si ha che $\frac{|u|}{N} \leq \frac{1}{2}$; $\frac{|v|}{N} \leq \frac{1}{2}$

Quindi l'ultimo num.

$$N\left[\frac{u+v\sqrt{2}}{c^2+2d^2}\right] = \left|\frac{u^2}{(\ )^2} - 2\frac{v^2}{(\ )^2}\right| \leq \frac{u^2}{(\ )^2} + \frac{2v^2}{(\ )^2} \leq$$

$$\leq \frac{1}{4} + \frac{2}{4} = 3/4$$

$< \frac{2}{4} = \frac{1}{2}$

pertanto il num del resto è minimo di quello del divisore e si può costruire un algoritmo euclideo.

Birkhoff - Mac Lane algebra Cap. II § 24 p. 106

UNIVERSITÀ DEGLI STUDI DI MODENA

* Il ragionamento svolto in 1, 2, 3 non dà più eccezione nel caso del corpo dei numeri $a+i\sqrt{3}b$.

Infatti qui si ha che $N(a+i\sqrt{3}b) = a^2+3b^2$.

I ragionamenti svolti portano a concludere:

$$\frac{a+i\sqrt{3}b}{c+i\sqrt{3}d} = \frac{(a+i\sqrt{3}b)(c+i\sqrt{3}d)}{c^2+3d^2} = \frac{ac-3bd+i\sqrt{3}(ad+bc)}{c^2+3d^2}$$

Posto allora

$$\begin{cases} ac-3bd = p\,(c^2+3d^2)+u \\ ad+bc = q\,(c^2+3d^2)+v \end{cases}$$

si ha allora

$$\frac{a+i\sqrt{3}b}{c+i\sqrt{3}d} = p+i\sqrt{3}\,q+\frac{u+i\sqrt{3}v}{c^2+3d^2}$$

con

$$\frac{|u|}{c^2+3d^2} \leq \frac{1}{2} \quad ; \quad \frac{|v|}{c^2+3d^2} \leq \frac{1}{2}$$

Ma se la norma del numero $\frac{u+i\sqrt{3}v}{c^2+3d^2}$ è limitata da $N\left(\frac{u+i\sqrt{3}v}{c^2+3d^2}\right) \leq \frac{1}{4}+3\cdot\frac{1}{4} \leq 1$

e non si può escludere che sia uno.

Quindi, moltiplicando per $c+i\sqrt{3}d$

non si può estendere che la norma del resto sia uguale a quella del divisore.

Esempi:

$$\frac{3+13i\sqrt{3}}{1+i\sqrt{3}} = 10+3i\sqrt{3} + \frac{2}{1+i\sqrt{3}} \quad \text{ecc.}$$

la norma del resto, 2, è uguale alla norma del divisore.

Pertanto non è possibile istituire un algoritmo di divisioni successive e quindi non sussiste il Teor. fondamentale: se un numero divide un prodotto col è primo con uno dei fattori; deve dividere l'altro.

Infatti il 4 ammette due ~~scomposizioni~~ scomposizioni in fattori essenzialmente distinte

$$(1+i\sqrt{3})(1-i\sqrt{3}) = 2\cdot 2$$

UNIVERSITÀ DEGLI STUDI DI MODENA

L'ideale $(2, 1+\sqrt{-3})$ (per le notazioni cfr. a pag. 60 N° 4) nell'anello dei numeri $a + b\rho$ con la regola di calcolo

$$\rho^2 = -\rho - 1$$

è certo un ideale principale; ciò segue dalla proposizione alla fine di pag. 66 e dal fatto che l'anello suddetto è certo euclideo (V. Allegato N° 2) .

La proprietà è d'altronde facilmente verificabile in via diretta. Infatti posto per un momento

$$\alpha = 1 + \sqrt{-3}$$

si ha facilmente che è

$$\alpha = -2\rho^2$$

Infatti α soddisfa alla legge di calcolo

$$\alpha^2 = 2(\alpha - 2)$$

ed a questa soddisfa pure il numero $-2\rho^2$.

Quindi l'ideale suddetto è semplicemente l'ideale principale generato dal numero 2 .