Algebra n. 3 - NOTE ALLA LEZIONE 26

Esempio 26.4

Proviamo che, detto $B=\left\{a+b\frac{1+i\sqrt{19}}{2}\middle| a,b\in\mathbb{Z}\right\}$, si ha $B=\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$. Ricordiamo che quest'ultimo anello è l'insieme delle espressioni polinomiali, a coefficienti interi, di $\frac{1+i\sqrt{19}}{2}$. Poiché l'inclusione $\subset$ è immediata, basta provare l'inclusione $\supset$. A tal fine, è sufficiente dimostrare che ogni potenza intera positiva di $\frac{1+i\sqrt{19}}{2}$ appartiene a *B*. Procediamo per induzione sull'esponente $n>0$. La base dell'induzione è il caso (banale) in cui $n=1$. Sia ora $n\geq 1$, supponiamo la tesi vera per *n* e deduciamola per $n+1$. Basta considerare, per arbitrari interi *a*, *b*, il seguente prodotto:

$$\left(a+b\frac{1+i\sqrt{19}}{2}\right)\frac{1+i\sqrt{19}}{2}=a\left(\frac{1+i\sqrt{19}}{2}\right)+b\left(\frac{1}{4}+\frac{1}{2}i\sqrt{19}-\frac{19}{4}\right)=-5b+(a+b)\left(\frac{1+i\sqrt{19}}{2}\right)\in B.$$

Ciò conclude il passo induttivo.

Per le successive applicazioni, può essere utile un'ulteriore osservazione. In base a quanto abbiamo appena provato, l'anello $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ è l'insieme dei numeri della forma $\frac{(2a+b)+bi\sqrt{19}}{2}$, al variare di a e b in $\mathbb{Z}$. Quindi è l'insieme $\left\{\frac{r+si\sqrt{19}}{2}\middle| r,s\in\mathbb{Z},\text{ con } r\equiv s\,(\mathrm{mod}\,2)\right\}$.

Se fosse $c=1$, sarebbe $\alpha\beta^{-1}=a+bi\sqrt{19}\in\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$, in quanto tale numero è evidentemente un intero algebrico.

L'intero $w=ay-19bx$ è compreso fra due multipli consecutivi di *c*, siano questi *ck* e $c(k+1)$. Siano d_1 e d_2 le distanze che separano *w* da *ck* e $c(k+1)$, rispettivamente. Allora $|r|$ è il minimo tra d_1 e d_2 : precisamente, se questo è d_1, allora $r=d_1$ e $q=k$, altrimenti $r=-d_2$ e $q=k+1$.

Se $c=5$, allora $\frac{\left[\frac{c}{2}\right]^2+19}{c^2}=\frac{23}{25}<1$. Sia ora $c\geq 6$. Allora

$$\frac{\left[\frac{c}{2}\right]^2+19}{c^2}\leq\frac{\frac{c^2}{4}+19}{c^2}=\frac{1}{4}+\frac{19}{c^2}\leq\frac{1}{4}+\frac{19}{36}=\frac{28}{36}<1.$$

Sia $c = 3$. Si rammenti che i possibili resti di un quadrato modulo 3 sono 0 e 1. Quindi la somma di due quadrati può essere congrua a 0 modulo 3 solo se entrambi i quadrati sono divisibili per 3. Una volta appurato che il numero intero $a^2 + 19b^2$ non è divisibile per 3, detti *q* e *r* il quoziente ed il resto della sua divisione per 3, si avrà $a^2 + 19b^2 = 3q + r,$ ove $r \in \{1, 2\}$. Dunque, posto, come indicato, $s = a - bi\sqrt{19},$ e $t = q,$ si ottiene

$$s\alpha\beta^{-1} - t = \frac{a^2 + 19b^2}{3} - q = \frac{r}{3} \in \left\{\frac{1}{3}, \frac{2}{3}\right\}.$$

La norma di questo numero è minore di 1.

Sia ora $c = 4$. Se, tra *a* e *b*, uno è pari e l'altro è dispari, allora il calcolo è del tutto analogo al precedente. Se invece *a* e *b* sono entrambi dispari, il numero $a^2 + 19b^2$ è divisibile per 4, e quindi la divisione euclidea per 4 produrrebbe un resto $r = 0,$ inservibile ai nostri fini, dato che il numero $s\alpha\beta^{-1} - t$ dev'essere diverso da zero. Si può però ricorrere alla divisione per 8, in quanto il quadrato di un numero dispari è sempre congruo a 1 modulo 8, e dunque $a^2 + 19b^2 \equiv 4 \pmod 8$. Detto *q* il quoziente, si avrà allora

$$\frac{a^2 + 19b^2}{8} - q = \frac{1}{2},$$

un numero non nullo e (avente norma) minore di 1. Dunque, essendo $\alpha\beta^{-1} = \frac{a + bi\sqrt{19}}{4},$ si può prendere $s = \frac{a - bi\sqrt{19}}{2}, t = q.$

Esempio 26.7

Sia $\beta = \frac{r + si\sqrt{19}}{2},$ con *r*, *s* interi entrambi pari o entrambi dispari, un elemento di $\mathbb{Z}\left[\frac{1 + i\sqrt{19}}{2}\right]$.

Allora $N(\beta) = \frac{r^2}{4} + \frac{19s^2}{4} = 4s^2 + \frac{r^2 + 3s^2}{4}$ divide $N(2) = 4$ solo se $s = 0$. Quindi, se β è divisore di 2 in $\mathbb{Z}\left[\frac{1 + i\sqrt{19}}{2}\right]$, allora β è un numero intero. Anche i divisori di 3 in $\mathbb{Z}\left[\frac{1 + i\sqrt{19}}{2}\right]$ sono interi, in quanto, se $N(\beta)$ divide 9, allora $|s| \le 1,$ ma $|s| = 1$ implicherebbe $r^2 + 3 = 20,$ impossibile con *r* intero.

Si ha $N\left(\frac{\pm 1 + i\sqrt{19}}{2}\right) = \frac{1 + 19}{4} = 5, N\left(\frac{3 + i\sqrt{19}}{2}\right) = \frac{9 + 19}{4} = 7,$ entrambi dispari e non divisibili per 3.