Anelli di interi biquadratici

In questa nota daremo un esempio di un campo di numeri $\mathbb{F}$ tale che $\mathcal{O}_{\mathbb{F}}$ non è della forma $\mathbb{Z}[\alpha]$, provando che l'anello degli interi di $\mathbb{F} = \mathbb{Q}[\sqrt{7}, \sqrt{10}]$ non è un'estensione semplice di $\mathbb{Z}$. Questo esempio è un esercizio tratto dal libro *Number Fields* di D. Marcus.

Sia $g \in \mathbb{Z}[x]$. Indichiamo con $\overline{g}$ l'immagine di g tramite la proiezione $\pi : \mathbb{Z}[x] \longrightarrow \mathbb{F}_3[x]$. Per assurdo supponiamo che $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}[\alpha]$ per qualche intero algebrico α. Sia f il polinomio minimo di α su $\mathbb{Q}$.

(1) *Sia $g \in \mathbb{Z}[x]$. Allora 3 divide $g(\alpha)$ in $\mathbb{Z}[\alpha]$ se e solo se $\overline{f}$ divide $\overline{g}$ in $\mathbb{F}_3[x]$.*

Sappiamo che $\mathbb{Z}[\alpha]$ è isomorfo a $\mathbb{Z}[x]/(f)$ ed un isomorfismo è dato da $h(x)+(f) \longmapsto h(\alpha)$. Da questo è facile dedurre che $\mathbb{Z}[\alpha]/(3)$ è isomorfo a $\mathbb{Z}[x]/(f,3)$, ed un isomorfismo naturale è $h(x) + (f,3) \longmapsto h(\alpha) + (3)$. D'altra parte $\mathbb{Z}[x]/(f,3) \simeq \mathbb{F}_3[x]/(\overline{f})$ e, componendo i vari isomorfismi, si ottiene facilmente che la mappa $h(\alpha) + (3) \longmapsto \overline{h} + (\overline{f})$ è un isomorfismo tra $\mathbb{Z}[\alpha]/(3)$ ed $\mathbb{F}_3[x]/(\overline{f})$. Dato $g(\alpha) \in \mathbb{Z}[\alpha]$, $3 \mid g(\alpha)$ se e solo se $g(\alpha) + (3)$ è 0 in $\mathbb{Z}[\alpha]/(3)$ e quindi se e solo se $\overline{g} + (\overline{f}) = 0$, ovvero se e solo se $\overline{f} \mid \overline{g}$.

Consideriamo i seguenti interi algebrici di $\mathbb{F}$:

$$\begin{aligned}
\alpha_1 &= (1+\sqrt{7})(1+\sqrt{10}) \\
\alpha_2 &= (1+\sqrt{7})(1-\sqrt{10}) \\
\alpha_3 &= (1-\sqrt{7})(1+\sqrt{10}) \\
\alpha_4 &= (1-\sqrt{7})(1-\sqrt{10}).
\end{aligned}$$

(2) *Dimostrare che tutti i prodotti $\alpha_i\alpha_j$ con $i \neq j$ sono divisibili per 3 in $\mathbb{Z}[\alpha]$. Provare che 3 non divide ${\alpha_i}^n$ per ogni $n \in \mathbb{N}$, considerando la traccia di ${\alpha_i}^n/3$.*

Che 3 divida ciascuno dei prodotti $\alpha_i\alpha_j$ con $i \neq j$ si controlla facilmente. Osserviamo ora che, fissato α_i, gli altri α_j si ottengono come immagini di α_i tramite le immersioni di $\mathbb{F}$. Allora

$$\mathrm{Tr}({\alpha_i}^n) = {\alpha_1}^n + {\alpha_2}^n + {\alpha_3}^n + {\alpha_4}^n.$$

Dato che $3 \mid \alpha_i\alpha_j$ quando $i \neq j$, abbiamo che

$$(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)^n \equiv {\alpha_1}^n + {\alpha_2}^n + {\alpha_3}^n + {\alpha_4}^n \pmod 3$$

per cui, visto che $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 4$, ne segue che

$$\mathrm{Tr}({\alpha_i}^n) \equiv 1 \pmod 3$$

per ogni $n \in \mathbb{N}$. Allora $\mathrm{Tr}({\alpha_i}^n/3)$ non è un intero e, pertanto, 3 non divide ${\alpha_i}^n$ in $\mathbb{Z}[\alpha]$.

(3) *Per ogni* $i = 1, 2, 3, 4$ *sia* $f_i \in \mathbb{Z}[x]$ *tale che* $\alpha_i = f_i(\alpha)$. *Mostrare che* $\overline{f} \mid \overline{f_i}\,\overline{f_j}$ *quando* $i \neq j$, *ma* $\overline{f} \nmid \overline{f_i}^n$ *per ogni* $n \in \mathbb{N}$.

Questa è una conseguenza immediata dei punti (1) e (2).

(4) *Dimostrare che, per ogni* $i = 1, 2, 3, 4$, $\overline{f}$ *ha un fattore irriducibile che divide* $\overline{f_j}$ *se e solo se* $j \neq i$.

Dato che, per ogni $n \in \mathbb{N}$, $\overline{f} \nmid \overline{f_i}^n$ abbiamo che, per ogni i, esiste almeno un fattore irriducibile di $\overline{f}$ che non divide $\overline{f_i}$. Sia p_i uno di questi.Posto $d_i = \mathrm{MCD}(\overline{f}, \overline{f_i})$ il polinomio p_i non divide $\overline{f}/d_i$ quindi, preso $j \neq i$, da $\overline{f} \mid \overline{f_i}, \overline{f_j}$, si ottiene $\overline{f}/d_i \mid \overline{f_j}$, e di conseguenza $p_i \mid \overline{f_j}$ se e solo se $i \neq j$.

In particolare i polinomi p_i sono non associati. Ma $\overline{f}$ ha grado minore o uguale a 4 e quindi ogni p_i ha grado 1. Questa è una contraddizione perchè non esistono in $\mathbb{F}_3[x]$ quattro polinomi di grado 1 a due a due non associati. Questa contraddizione mostra che $\mathcal{O}_{\mathbb{F}} \neq \mathbb{Z}[\alpha]$.