

**Università degli Studi Roma Tre**  
**Corso di Laurea in Matematica - a.a.2010/2011**  
**AL420 - Teoria Algebrica dei Numeri (Prof. S. Gabelli)**  
**Esercizi 8**

1. *Teorema di Dedekind* (1878):

Sia  $K = \mathbb{Q}(\theta)$ ,  $\theta \in \mathcal{O}_K$  con polinomio minimo  $m(X) \in \mathbb{Z}[X]$ , e sia  $d = [\mathcal{O}_K : \mathbb{Z}[\theta]]$ . Sia  $p \in \mathbb{Z}$  un numero primo che non divide  $d$  e

$$\overline{m}(X) = \overline{q_1}(X)^{e_1} \overline{q_2}(X)^{e_2} \dots \overline{q_s}(X)^{e_s}$$

la fattorizzazione di  $\overline{m}(X)$  in polinomi irriducibili su  $\mathbb{F}_p$ . Allora, per  $i = 1, \dots, s$ ,

- (1)  $P_i = (p, q_i(\theta)) \subseteq \mathcal{O}_K$  è un ideale primo;
- (2)  $P_i \neq P_j$  per  $i \neq j$ ;
- (2)  $N(P_i) = p^{\deg(\overline{q_i}(X))}$ ;
- (3)  $p\mathcal{O}_K = P_1^{e_1} P_2^{e_2} \dots P_s^{e_s}$ .

*Suggerimento:* Procedere come per il caso  $\mathcal{O}_K = \mathbb{Z}[\theta]$  visto a lezione, osservando che  $\mathcal{O}_K/P_i$  è isomorfo a  $\mathbb{Z}[\theta]/(\mathbb{Z}[\theta] + q_i(\theta)\mathbb{Z}[\theta])$  via la moltiplicazione per  $dp$ .

2. Sia  $K = \mathbb{Q}(\theta)$ ,  $\theta \in \mathcal{O}_K$  con polinomio minimo  $m(X) \in \mathbb{Z}[X]$  e supponiamo che il discriminante  $D$  di  $m(X)$  non abbia fattori quadratici. Dimostrare che  $\mathcal{O}_K = \mathbb{Z}[\theta]$  e che  $D$  è il discriminante del campo  $K$ .
3. Sia  $m(X) = X^3 - 4X + 2 \in \mathbb{Z}[X]$  e sia  $\theta$  una sua radice.
  - (1) Verificare che  $m(X)$  è irriducibile su  $\mathbb{Q}$ .
  - (2) Posto  $K = \mathbb{Q}(\theta)$ , dimostrare che  $\mathcal{O}_K = \mathbb{Z}[\theta]$ .
  - (3) Fattorizzare gli ideali  $p\mathcal{O}_K$  per  $p = 2, 3, 5$ .
4. Sia  $\theta \in \mathbb{C}$  tale che  $\theta^3 + \theta - 1 = 0$ . Determinare l'anello degli interi algebrici di  $K = \mathbb{Q}(\theta)$  ed il discriminante di  $K$ .
5. Si  $\xi$  una radice primitiva quinta dell'unità. Fattorizzare l'ideale  $p\mathbb{Z}[\xi]$  in ideali primi di  $\mathbb{Z}[\xi]$  per  $p \leq 13$  primo.