

## ESERCIZI DI TEORIA DEI NUMERI

A. BERNARDI

### 1. FOGLIO 4

**Esercizio 1.** Sia  $K$  un campo di numeri e  $\alpha \in K$ .

- (1) Mostrare che esiste  $0 \neq m \in \mathbb{Z}$  tale che  $m\alpha \in \mathcal{O}_K$ . Concludere che una base intera di  $\mathcal{O}_K$  è una base del  $\mathbb{Q}$ -spazio vettoriale  $K$ .
- (2) Il viceversa non è vero: dare un esempio di una  $\mathbb{Q}$ -base di  $K$  fatta da interi algebrici che non sia una base intera.

**Esercizio 2.** Ri-dimostriamo l'esistenza di una base intera di un ideale non nullo  $I \subset \mathcal{O}_K$ , con  $K$  campo di numeri.

- (1) Sia  $E$  un  $K$ -spazio vettoriale e  $f : E \times E \rightarrow K$  una forma bilineare simmetrica non degenere. Sia  $B = (e_1, \dots, e_n)$  una base di  $E$ . Mostrare che esiste una base  $(v_1, \dots, v_n)$  di  $E$  tale che  $f(e_i, v_j) = \delta_{i,j}$ .
- (2) Sia  $K$  un campo di numeri di grado  $n$  e sia  $I \subset \mathcal{O}_K$  un ideale. Sia  $(\omega_1, \dots, \omega_n)$  una base di  $K/\mathbb{Q}$ . Esiste  $0 \neq c \in \mathbb{Z}$  tale che  $\alpha_i = c\omega_i \in I$ . Per (1) esiste una  $\mathbb{Q}$ -base  $(\gamma_1, \dots, \gamma_n)$  tale che la traccia  $Tr(\alpha_j \gamma_j) = \delta_{i,j}$ . Se  $\alpha \in I$ ,  $\alpha = \sum_{i=1}^n a_i \gamma_i$ ,  $a_i \in \mathbb{Q}$ , mostrare che  $a_i \in \mathbb{Z}$  per ogni  $i$ .
- (3) Per (2),  $I \subset \gamma_1 \mathbb{Z} + \dots + \gamma_n \mathbb{Z}$ . Dedurre che  $I$  è uno  $\mathbb{Z}$ -modulo libero di rango  $m \leq n$ .
- (4) Per (3) esiste  $B = (\beta_1, \dots, \beta_m)$  una  $\mathbb{Z}$ -base di  $I$ . Mostrare che  $B$  è una base di  $K/\mathbb{Q}$ . Quindi  $m = n$  e  $B$  è una base intera di  $I$ .

**Esercizio 3.** Si  $z$  un elemento primitivo di  $K/\mathbb{Q}$ ,  $M(x)$  il suo polinomio minimo e  $z_1, \dots, z_n$  i suoi coniugati.

- (1) Indichiamo con  $M'(x)$  la derivata di  $M(x)$ . Mostrare che  $M'(z_j) = \prod_{i \neq j} (z_j - z_i)$ .
- (2) Mostrare che  $N(M'(z)) = \prod_{j=1}^n M'(z_j)$ .
- (3) Concludere che  $N(M'(z)) = \prod_{i,j=1, i \neq j}^n (z_j - z_i) = (-1)^{n(n-1)/2} \prod_{1 \leq i < j \leq n} (z_i - z_j)^2$ .

**Esercizio 4.** Sia  $\zeta$  una radice  $p$ -esima dell'unità con  $p$  primo.

- (1) Mostrare che  $\Phi_p(x) := x^{p-1} + \dots + x + 1 \in \mathbb{Z}[x]$  è irriducibile<sup>2</sup>. Concludere che  $K = \mathbb{Q}(\zeta)$  ha grado  $\varphi(p) = p - 1$  e che  $B = (1, \zeta, \zeta^2, \dots, \zeta^{p-2})$  è una  $\mathbb{Q}$  base di  $K$ . Osservare che  $\zeta^i \in \mathcal{O}_K$ .
- (2) I coniugati di  $\zeta$  sono  $\sigma_i(\zeta) = \zeta^i$ . In particolare  $\mathbb{Q}(\zeta)/\mathbb{Q}$  è di Galois.
- (3) Mostrare che  $Tr(\zeta^i) = -1$ ,  $Tr(1 - \zeta^i) = p$  ( $1 \leq p \leq p - 1$ ),  $N(1 - \zeta) = p$ .
- (4) Mostrare che  $(1 - \zeta)\mathcal{O}_K \cap \mathbb{Z} = (p)$ .
- (5) Sia  $\alpha \in \mathcal{O}_K$  e sia  $\sigma_i \in \text{Aut}_{\mathbb{Q}}(K)$  tale che  $\sigma_i(\zeta) = \zeta^i$ . Mostrare che  $\sigma_i(\alpha(1 - \zeta)) \in (1 - \zeta)\mathcal{O}_K$ . Concludere che  $Tr(\alpha(1 - \zeta)) = a_0 p$  e concludere che  $a_0 \in \mathbb{Z}$ .
- (6) Osservare che  $\zeta^{-1} \in \mathcal{O}_K$ , quindi  $\alpha_1 = (\alpha - a_0)\zeta^{-1} = a_1 + a_2\zeta + \dots + a_{p-2}\zeta^{p-3} \in \mathcal{O}_K$ . Ripetendo il ragionamento precedente mostrare che  $a_1 \in \mathbb{Z}$  e quindi  $a_i \in \mathbb{Z}$  per ogni  $i$ .

<sup>1</sup>Usare il teorema di struttura dei moduli su un PID.

<sup>2</sup>Considerare  $\Phi_p(x+1)$ .

(7) Mostrare che

$$D_K := \prod_{1 \leq i < j \leq p-1} (\zeta_i - z_j)^2 = (-1)^{(p-1)/2} p^{p-2}.$$

**Esercizio 5** (Relazione di Stickelberger).<sup>3</sup> Sia  $K/\mathbb{Q}$  un campo di numeri di grado  $n$ . Se  $(\omega_1, \dots, \omega_n)$  è una base intera, allora per definizione  $D_K = \text{disc}(\omega_1, \dots, \omega_n) = \det((\sigma_i(\omega_j)))^2$ , dove  $\sigma_1, \dots, \sigma_n$  sono le  $n$   $\mathbb{Q}$ -immersioni di  $K$  in  $\overline{\mathbb{Q}}$ .

Se  $M = (a_{i,j})_{i,j=1,\dots,n}$  è una matrice  $n \times n$

$$\det(M) = \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{\sigma(1),1} \cdots a_{\sigma(n),n} = P - N$$

dove  $P = \sum_{\sigma|\varepsilon(\sigma)=1} a_{\sigma(1),1} \cdots a_{\sigma(n),n}$  e  $N = \sum_{\sigma|\varepsilon(\sigma)=-1} a_{\sigma(1),1} \cdots a_{\sigma(n),n}$ .

D'ora in poi  $P$  ed  $N$  li prendiamo definiti su una base intera:  $\det(\sigma_i(\omega_j)) = P - N$  con  $(\omega_i)$  base intera.

- (1) Mostrare che  $\sigma_i(P + N) = P + N$  e che  $\sigma_i(PN) = PN$ , per ogni  $i = 1, \dots, n$ .
- (2) Sia  $\alpha \in K$  tale che  $\sigma_i(\alpha) = \alpha$ , per ogni  $i = 1, \dots, n$ . Mostrare che  $\alpha \in \mathbb{Q}$ . Concludere che  $P + N, PN \in \mathbb{Q}$ .
- (3) Mostrare che  $P + N$  e  $PN$  sono interi algebrici. Dedurre che  $P + N, PN \in \mathbb{Z}$ .
- (4) [Relazione di Stickelberger] Concludere che  $D_K \equiv 0, 1 \pmod{4}$ .

---

<sup>3</sup>Chi avesse difficoltà a dimostrarla nella sua generalità può aggiungere l'ipotesi  $K/\mathbb{Q}$  di Galois e dimostrarne in questo modo una versione semplificata.