Sei K ein Zahlkörper vom Grad n.

9.1. Norm von Idealen. Sei p eine Primzahl. Zeige:

(a) Ist P ein Primideal in $\mathcal{O}_K$ mit $p|N(P)$, so ist $|N(P)| = p^s$ mit $1 \leq s \leq n$.

(b) Es gibt höchstens n Primideale P mit $p|N(P)$.

(c) Gibt es nur ein Primideal P mit $p|N(P)$ und ist $N(P) = p^s$, so ist s ein Teiler von n, und $P^{n/s} = \langle p \rangle$.

(d) Seien $P_1, \ldots, P_t$ die Primideale mit $p|N(P_i)$ (paarweise verschieden). Es ist $\prod N(P_i) \leq p^n$ und aus $\prod N(P_i) = p^n$ folgt $\langle p \rangle = P_1 \cdots P_t$.

9.2. Klassengruppe. Sei h die Klassenzahl von K. Zeige:

(a) Seien I, J Ideale von $\mathcal{O}_K$. Ist $I^m \sim J^m$ für eine natürliche Zahl m und ist $(m, h) = 1$, so ist $I \sim J$.

(b) Es gibt Ideale $I_1, \ldots, I_t$ und Primzahlpotenzen $q_1, \ldots, q_t$ mit folgenden Eigenschaften:

(1) Für jedes i ist $I_i^{q_i}$ ein Hauptideal.

(2) Für jedes Ideal $J \neq 0$ in $\mathcal{O}_K$ gibt es natürliche Zahlen $0 \leq n_i < q_i$ mit $J \sim I_1^{n_1} \cdots I_t^{n_t}$, und

(3) $h = q_1 \cdots q_t$.

9.3. Diskriminante, Grad 3. Sei $f(X) = a + bX + cX^2 + X^3$ ein irreduzibles Polynom in $\mathbb{Q}[X]$. Sei $\alpha \in \mathbb{C}$ eine Nullstelle von f. Dann ist natürlich $K = \mathbb{Q}[\alpha]$ ein Zahlkörper vom Grad 3. Zeige:

$$\Delta(1, \alpha, \alpha^2) = -27a^2 + 18abc - 4ac^3 - 4b^3 + b^2c^2.$$

(Was ist zu tun? Man muss $(X_1 - X_2)^2(X_1 - X_3)^2(X_2 - X_3)^2$ als Produkt der elementar-symmetrischen Funktionen schreiben — eine etwas langwierige, aber problemlose Rechnung, muss auch mal sein! Zusatz: Die Formel wird besser verständlich, wenn wir den Koeffizienten $d = 1$ von X^3 mitschleppen:

$$-27a^2d^2 + 18abcd - 4ac^3 - 4b^3d + b^2c^2,$$

es handelt sich also um ein homogenes Polynom vom Grad 4 in den Variablen a, b, c, d.)

9.4. Sei $\alpha \in \mathbb{C}$ eine Wurzel des Polynoms $f = X^3 - X - 1$ und $K = \mathbb{Q}[\alpha]$.

(a) Zeige: f ist irreduzibel (Hilfe: verwende das Gauß-Lemma).

(b) $\Delta(1, \alpha, \alpha^2) = -23$ und daher ist $1, \alpha, \alpha^2$ eine Ganzheitsbasis von $\mathbb{Q}[\alpha]$.

(c) Betrachte das Polynom f modulo $2, 3, 5, 7, 23$ um das Zerlegungsverhalten dieser Primzahlen in $\mathbb{Q}[\alpha]$ anzugeben.