Algebra II

Lösungsskizze zur Klausur

Aufgabe 1:

Sei k ein beliebiger Körper und sei $k[X]$ der Polynomring mit Quotientenkörper $k(X)$.

i) Zeige, dass $k[X]$ ein Dedekindring ist.

ii) Zeige, dass für jedes normierte irreduzible Polynom $P \in k[X]$ eine diskrete Bewertung

$$v_P : k(X) \to \mathbb{Z} \cup \{\infty\}$$

existiert, sodass $v_P(P) = 1$ und $v_P|_{k\setminus\{0\}} \equiv 0$.

iii) Bestimme den Bewertungsring $\mathcal{O}_P$ von $(k(X), v_P)$.

iv) Bestimme die Vervollständigung von $\mathcal{O}_P$ entlang seines maximalen Ideals für k algebraisch abgeschlossen. Was passiert, wenn k nicht algebraisch abgeschlossen ist?

Zu i): Der Ring $k[X]$ ist ein Hauptidealring, insbesondere noethersch, ganzabgeschlossen und jedes nicht-triviale Primideal ist maximal.

Zu ii): Sei $f \in k(X)\setminus\{0\}$. Dann sind die ganzen Zahlen $\{v_P(f)\}_P$ eindeutig bestimmt durch die Gleichung

$$f \;=\; u \cdot \prod_P P^{v_P(f)},$$

wobei $u \in k^\times$ und das Produkt über alle normierten, irreduziblen Polynome $P \in k[X]$ gebildet wird. Beachte, dass $v_P(f) = 0$ für fast alle P.

Zu iii): $\mathcal{O}_P = \{f/g \in k(X) \mid f, g \in k[X], g \neq 0 \text{ und } (P, g) = 1\}$

Zu iv): Ist k algebraisch abgeschlossen, so ist jedes irreduzible Polynom P von der Form $P = X - \lambda$ für ein $\lambda \in k$. Damit gilt für die Vervollständigung

$$\hat{\mathcal{O}}_P \;\simeq\; k[\![X - \lambda]\!] \;\simeq\; k[\![X]\!].$$

Ist k nicht algebraisch abgeschlossen, so gilt nach der Vorlesung immer noch $\hat{\mathcal{O}}_P \simeq K[\![T]\!]$, wobei $K = k[X]/(P)$ der Restklassenkörper ist (Satz von Cohen). Der Isomorphismus ist im Allgemeinen nicht eindeutig. In dem Falle, dass k perfekt ist und positive Charakteristik hat, existiert jedoch ein kanonischer Isomorphismus, der auf K die Identität induziert.

Aufgabe 2:

Sei $d \in \mathbb{Z}\setminus\{0, 1\}$ quadratfrei und sei $p \geq 3$ eine Primzahl mit $(p, d) = 1$. Sei $\mathcal{O}$ der Ring der ganzen Zahlen von $\mathbb{Q}(\sqrt{d})$. Zeige, dass folgende Aussagen äquivalent sind:

i) Das Ideal $p\mathcal{O}$ ist ein Primideal in $\mathcal{O}$.

ii) Die Gleichung $x^2 \equiv d \pmod p$ ist unlösbar.

Aus der Vorlesung ist bekannt, dass der Ganzheitsring $\mathcal{O}$ entweder $\mathbb{Z}[\sqrt{d}]$ oder $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ ist. Insbesondere gilt $\mathcal{O}[\frac{1}{2}] = \mathbb{Z}[\frac{1}{2}][\sqrt{d}]$. Wegen $p \neq 2$ erhält man $\mathcal{O}/p\mathcal{O} = \mathbb{F}_p[X]/(X^2 - d)$. Daher ist $p\mathcal{O}$ genau dann prim, wenn $X^2 - d$ in $\mathbb{F}_p[X]$ irreduzibel ist, was äquivalent zur Unlösbarkeit von $x^2 \equiv d \pmod p$ ist.

Aufgabe 3:

Sei $K = \mathbb{Q}(\sqrt{-7})$ mit Ganzheitsring $\mathcal{O}_K$.

i) Man bestimme die absolute Diskriminante d_K von K.

ii) Zeige, dass $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$.

iii) Man bestimme die Minkowski-Konstante $M = (\frac{4}{\pi})^{r_2} \cdot \frac{n!}{n^n} \cdot \sqrt{|d_K|}$.

iv) Zeige, dass $\mathcal{O}_K$ ein Hauptidealring ist.

Zu i) und ii): Es gilt $-7 \equiv 1 \pmod 4$. Damit ist nach Vorlesung $d_K = -7$ und $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$.
Zu iii): Es gilt $r_2 = 1$. Damit ist

$$M \;=\; \frac{4}{\pi} \cdot \frac{2}{2^2} \cdot \sqrt{7} \;=\; 2 \cdot \frac{\sqrt{7}}{\pi} < 2.$$

Zu iv): Nach der Vorlesung enthält jede Idealklasse ein ganzes Ideal $\mathfrak{a}$ von Norm $\leq M < 2$, also von Norm 1. Damit ist die Klassenzahl 1 und $\mathcal{O}_K$ ist ein Hauptidealring.

Aufgabe 4:

Sei p eine Primzahl und sei R ein Ring mit $p \cdot R = 0$. Sei $W(R)$ der Ring der Wittvektoren zur Primzahl p. Bezeichne mit $F : W(R) \to W(R)$ den Frobenius und mit $V : W(R) \to W(R)$ die Verschiebung. Aus der Vorlesung ist bekannt, dass $FV = VF = p$ und $V(\underline{a}) \cdot \underline{b} = V(\underline{a} \cdot F(\underline{b}))$, $\underline{a}, \underline{b} \in W(R)$.

i) Zeige, dass für alle $m, n \geq 0$ gilt

$$V^m(\underline{a}) \cdot V^n(\underline{b}) \;=\; V^{m+n}(F^n(\underline{a}) \cdot F^m(\underline{b})).$$

ii) Zeige, dass $W(R)$ genau dann nullteilerfrei ist, wenn R nullteilerfrei ist.

Zu i): Aus der Gleichung $V(\underline{a}) \cdot \underline{b} = V(\underline{a} \cdot F(\underline{b}))$ folgt durch Induktion $V^m(\underline{a}) \cdot \underline{b} = V^m(\underline{a} \cdot F^m(\underline{b}))$. Aus Symmetriegründen folgt i).
Zu ii): Seien $a, b \in R \backslash \{0\}$. Ist $W(R)$ nullteilerfrei, so gilt

$$(a, 0, \ldots) \cdot (b, 0, \ldots) = (ab, 0, \ldots) \neq 0.$$

Damit ist R nullteilerfrei. Umgekehrt sei R nullteilerfrei und seien $\underline{a}, \underline{b} \in W(R) \backslash \{0\}$. Schreibe $\underline{a} = V^m(\underline{a}')$ und $\underline{b} = V^n(\underline{b}')$ mit $a'_0, b'_0 \neq 0$. Nach i) gilt

$$\underline{a} \cdot \underline{b} = V^{m+n}(F^n(\underline{a}') \cdot F^m(\underline{b}')).$$

Nun ist $F^n(\underline{a}') \cdot F^m(\underline{b}') = ((a'_0)^{p^n} (b'_0)^{p^m}, \ldots) \neq 0$, weil R nullteilerfrei ist. Daraus folgt $\underline{a} \cdot \underline{b} \neq 0$.

Aufgabe 5:

Sei $K = \mathbb{Q}(\zeta_n)$ für $n \geq 3$, wobei ζ_n eine primitive n-te Einheitswurzel ist. Zeige, dass folgende Aussagen äquivalent sind:

i) Die Primzahl p ist unverzweigt in $K/\mathbb{Q}$.

ii) Es gilt $(p, n) = 1$ für $p \geq 3$ und $4 \nmid n$ für $p = 2$.

i)⇒ii): Angenommen $p|n$. Dann ist $\zeta_p \in K$, wobei ζ_p eine primitive p-te Einheitswurzel ist. Man betrachte den Turm von Körpererweiterungen $K/\mathbb{Q}(\zeta_p)/\mathbb{Q}$. Sei $\mathfrak{p}$ ein Primideal in $\mathcal{O}_{\mathbb{Q}(\zeta_p)}$ über (p). Nach der Vorlesung gilt für den Verzweigungsindex $e_{\mathfrak{p}/(p)} = p-1$. Sei $\mathfrak{P}$ ein Primideal in $\mathcal{O}_K$ über $\mathfrak{p}$. Dann ist

$$e_{\mathfrak{P}/(p)} \;=\; e_{\mathfrak{P}/\mathfrak{p}} \cdot e_{\mathfrak{p}/(p)} \geq p-1.$$

Für $p \geq 3$ ist p damit verzweigt in $K/\mathbb{Q}$. Für $p = 2$ nehmen wir an, dass $4|n$ und somit $\mathbb{Q}(i) \subset K$. Daher ist 2 verzweigt in K.

i)⇒ii): Zunächst sei $(p, n) = 1$. Sei $R = \mathbb{Z}[\zeta_n]$ die von ζ_n erzeugte $\mathbb{Z}$-Unteralgebra von $\mathcal{O}_K$. Man betrachte den induzierten Morphismus

$$f\colon R/pR \longrightarrow \mathcal{O}_K/p\mathcal{O}_K.$$

Es genügt zu zeigen, dass f ein Isomorphismus ist und R/pR in ein Produkt von Körpern zerfällt. Dies impliziert, dass $\mathcal{O}_K/p\mathcal{O}_K$ reduziert ist, folglich p unverzweigt in $K/\mathbb{Q}$ ist. Aber R/pR ist genau dann ein Produkt von Körpern, wenn jeder irreduzible Faktor P von $X^n - 1$ in $\mathbb{F}_p[X]$ mit Multiplizität 1 auftaucht. Angenommen $P^2|(X^n - 1)$. Dann teilt P die Ableitung nX^{n-1} und wegen $n \not\equiv 0 \pmod p$, folgt $P|X^{n-1}$. Dies ist ein Widerspruch. Als nächstes zeigen wir, dass f ein Isomorphismus. Beide Algebren haben Dimension $\varphi(n)$ über $\mathbb{F}_p$. Fassen wir $\mathcal{O}_K/p\mathcal{O}_K$ via f als R/pR-Algebra auf, zerfällt diese entsprechend der obigen Zerlegung in ein Produkt. Die Dimensionsgleichheit gilt jetzt faktorweise, also muss f ein Isomorphismus sein. Ist nun $p = 2$ und $n = 2m$ gerade mit $2 \nmid m$, dann gilt $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_m)$. Das reduziert uns auf den bereits behandelten Fall.