Algebra II

Lösungsskizze zur Nachklausur

Aufgabe 1:
Entscheide, welche der folgenden Ringe Dedekindringe sind (mit Begründung).
i) $\mathbb{Z}[\sqrt{-1}]$
ii) $\mathbb{F}_p[\![X]\!]$
iii) $\mathbb{Z}[\sqrt{5}]$
iv) $\mathbb{Z}[X]$
v) Der ganze Abschluss $\bar{\mathbb{Z}}$ von $\mathbb{Z}$ in $\bar{\mathbb{Q}}$, wobei $\bar{\mathbb{Q}} \subset \mathbb{C}$ der Körper der algebraischen Zahlen ist.

Zu i): Der Ring $\mathbb{Z}[\sqrt{-1}]$ ist ein Hauptidealring, insbesondere noethersch, ganzabgeschlossen und jedes nicht-triviale Primideal ist maximal.
Zu ii): Der Ring $\mathbb{F}_p[\![X]\!]$ ist ein diskreter Bewertungsring und damit ein Dedekindring, siehe i).
Zu iii): Der Ring $\mathbb{Z}[\sqrt{5}]$ ist nicht ganzabgeschlossen, z.B. das Element des Quotientenkörpers $\frac{1+\sqrt{5}}{2} \in \mathbb{Q}(\sqrt{5})$ ist ganz, aber nicht in $\mathbb{Z}[\sqrt{5}]$ enthalten. Also ist $\mathbb{Z}[\sqrt{5}]$ kein Dedekindring.
Zu iv): Das Ideal (X) ist nicht-trivial und prim, aber nicht maximal. Daher ist $\mathbb{Z}[X]$ kein Dedekindring.
Zu v): Der Ring $\bar{\mathbb{Z}}$ ist nicht noethersch und daher kein Dedekindring.

Aufgabe 2:
Sei $d \in \mathbb{Z}\backslash\{0,1\}$ 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 $p\mathcal{O}$ zerfällt in zwei verschiedene Primideale in $\mathcal{O}$.
ii) Die Gleichung $x^2 \equiv d \pmod{p}$ ist lösbar.

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 zerfällt $p\mathcal{O}$ genau dann in zwei verschiedene Primideale, wenn $X^2 - d$ in $\mathbb{F}_p[X]$ in verschiedene Linearfaktoren zerfällt. Wegen $p \neq 2$ und $(p,d) = 1$ ist dies äquivalent zur Lösbarkeit von $x^2 \equiv d \pmod{p}$.

Aufgabe 3:
Sei $K = \mathbb{Q}(\sqrt{-5})$ mit Ganzheitsring $\mathcal{O}_K$.
i) Man bestimme die absolute Diskriminante d_K von K.
ii) Man bestimme den Ganzheitsring $\mathcal{O}_K$.
iii) Man bestimme die Minkowski-Konstante $M = (\frac{4}{\pi})^{r_2} \cdot \frac{n!}{n^n} \cdot \sqrt{|d_K|}$.
iv) Man bestimme die Klassengruppe $\mathfrak{cl}_K$.

Zu i) und ii): Es gilt $-5 \equiv 3 \pmod{4}$. Damit ist nach Vorlesung $d_K = 4 \cdot (-5) = -20$ und $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$.

Zu iii): Es gilt $r_2 = 1$. Damit ist

$$M \;=\; \frac{4}{\pi} \cdot \frac{2}{2^2} \cdot \sqrt{20} < 3.$$

Zu iv): Die Klassengruppe wird von den Idealklassen der Primideale erzeugt. Nach der Vorlesung enthält jede Idealklasse ein ganzes Ideal $\mathfrak{a}$ von Norm $\leq M < 3$. Daher wird $\mathfrak{cl}_K$ von den Primidealen mit Norm ≤ 2 erzeugt. Über der Primzahl 2 ist die Erweiterung $K/\mathbb{Q}$ nach i) verzweigt mit

$$2\mathcal{O}_K \;=\; \mathfrak{p}^2,$$

wobei $\mathfrak{p} = (1+\sqrt{-5}, 2)$. Dies zeigt, dass $\mathfrak{cl}_K = \langle [\mathfrak{p}] \rangle$, wobei $[\mathfrak{p}]^2 = 1$. Angenommen $\mathfrak{p} = (\alpha)$ ist ein Hauptideal. Sei $\alpha = a + \sqrt{-5}b$ mit $a, b \in \mathbb{Z}$. Dann gilt für die Norm

$$\pm 2 = N(\alpha) = a^2 - 5b^2,$$

was modulo 5 zu einem Widerspruch führt. Damit gilt $\mathfrak{cl}_K \simeq \mathbb{Z}/2$.

Aufgabe 4:

Sei $p \geq 3$ eine Primzahl.

i) Zeige, dass $\mathbb{Q}_p^\times$ die Gruppe der $(p-1)$-ten Einheitswurzeln enthält.

ii) Zeige, dass $\mathbb{Q}_p^\times$ nicht die Gruppe der p-ten Einheitswurzeln enthält.

Zu i): Aus der Vorlesung ist bekannt, dass $\mathbb{Z}_p$ kanonisch zu dem Ring der Wittvektoren $W(\mathbb{F}_p)$ isomorph ist. Der Teichmüller-Lift ist ein injektiver Homomorphismus von Gruppen

$$\mu \colon \mathbb{F}_p^\times \longrightarrow \mathbb{Z}_p^\times.$$

Das Bild $\mu(\mathbb{F}_p^\times)$ ist die Gruppe der $(p-1)$-ten Einheitswurzeln.

Zu ii): Sei ζ_p eine primitive p-te Einheitswurzel und sei $K = \mathbb{Q}_p(\zeta_p)$. Aus der Vorlesung ist bekannt, dass die Erweiterung $K/\mathbb{Q}_p$ voll verzweigt vom Grad $p-1$ ist. Daher kann $\mathbb{Q}_p^\times$ nicht die Gruppe der p-ten Einheitswurzeln enthalten.

Aufgabe 5:

Sei $K = \mathbb{Q}_p(\zeta_n)$ für $n \geq 3$, wobei ζ_n eine primitive n-te Einheitswurzel ist. Sei $\mathcal{O}_K$ der Ganzheitsring von K mit Maximalideal $\mathfrak{p}$ und sei k der Restklassenkörper mit $|k| = p^r$, $r \geq 1$. Nehme an, dass $(p, n) = 1$.

i) Zeige, dass die Erweiterung $K/\mathbb{Q}_p$ eine unverzweigte Galoiserweiterung ist und dass der kanonische Homomorphismus von Galoisgruppen

$$\mathrm{Gal}(K/\mathbb{Q}_p) \longrightarrow \mathrm{Gal}(k/\mathbb{F}_p)$$

ein Isomorphismus ist.

ii) Sei $W(k)$ der Wittring von k. Zeige, dass $\mathcal{O}_K \simeq W(k)$. Wie kann man einen solchen Isomorphismus eindeutig charakterisieren?

Zu i): Als Zerfällungskörper von $X^n - 1$ ist $K/\mathbb{Q}_p$ eine Galoiserweiterung. Sei ϕ das Minimalpolynom von ζ_n über $\mathbb{Q}_p$. Dann hat ϕ ganzzahlige Koeffizienten und die Reduktion $\bar{\phi}$ ist das Minimalpolynom von $\bar{\zeta_n} = \zeta_n \mod \mathfrak{p}$ über $\mathbb{F}_p$. In der Tat, wegen $(p, n) = 1$ zerfällt $\bar{\phi}$ als Teiler von $X^n - 1$ über einem algebraischen Abschluss von $\mathbb{F}_p$ in verschiedene Linearfaktoren und muss daher nach Hensels Lemma irreduzibel über $\mathbb{F}_p$ sein. Daraus folgt

$$[K : \mathbb{Q}_p] \;=\; \deg(\phi) \;=\; \deg(\bar{\phi}) \;=\; [k : \mathbb{F}_p].$$

Dies zeigt, dass $K/\mathbb{Q}_p$ eine unverzweigte Galoiserweiterung vom Grad $[k : \mathbb{F}_p]$ ist. Der Homomorphismus

$$\pi \colon \mathrm{Gal}(K/\mathbb{Q}_p) \longrightarrow \mathrm{Gal}(k/\mathbb{F}_p)$$

ist nach Vorlesung surjektiv. Weil beide Gruppen diesselbe Kardinalität haben, ist π ein Isomorphismus.

Zu ii): Nach Vorlesung existiert ein eindeutiger Homomorphismus von Ringen $\varphi \colon W(k) \to \mathcal{O}_K$, der die Identität auf den Restklassenkörpern induziert. Durch φ ist $\mathcal{O}_K$ ein freier $W(k)$-Modul vom Rang $e \geq 1$, wobei e den Verzweigungsgrad von $K/\mathbb{Q}_p$ bezeichnet. Nach i) gilt $e = 1$. Dies zeigt, dass φ ein Isomorphismus ist.