Aufgabe 1

(a) Es gilt

$$\mathrm{Gal}(\mathbb{Q}(\zeta_8)|\mathbb{Q}) \cong (\mathbb{Z}/8\mathbb{Z})^\times \xrightarrow{\phi} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

mit

$$\begin{aligned}\phi\colon (\mathbb{Z}/8\mathbb{Z})^\times = \{1,3,5,7\} &\to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\\ 1 &\mapsto (0,0)\\ 3 &\mapsto (1,0)\\ 5 &\mapsto (0,1)\\ 7 &\mapsto (1,1)\end{aligned}$$

Nachrechnen ergibt, dass es sich tatsächlich um einen Homomorphismus handelt, dieser ist offensichtlich surjektiv und auf endlichen Gruppen definiert, also ein Isomorphismus. Weiter gilt

$$\zeta_8 = e^{i\frac{\pi}{4}} = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2} = \frac{\sqrt{2}}{2}(1+i)$$

. Insbesondere erhalten wir $i = (\zeta_8)^2 = \frac{1}{2}(1+2i-1)$, $\sqrt{2} = \zeta_8 + \zeta_8^{-1} = \frac{\sqrt{2}}{2}(1+i) + \frac{\sqrt{2}}{2}(1-i) = \frac{\sqrt{2}}{2}\cdot 2$ und $\sqrt{-2} = \zeta_8 - \zeta_8^{-1} = \frac{\sqrt{2}}{2}(1+i) - \frac{\sqrt{2}}{2}(1-i) = \frac{\sqrt{2}}{2}\cdot 2i$. Es gilt $[K:\mathbb{Q}] = \phi(8) = \phi(2^3) = 4$. Wegen $[\mathbb{Q}(i):\mathbb{Q}] = [\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{-2}):\mathbb{Q}] = 2$ sind alle drei quadratische Unterkörper von K.

(b) Nach Korollar 6.11 (i) ist p unverzweigt, da $8 \not\equiv 0 \mod p$ ist. Da die Erweiterung $K|\mathbb{Q}$ endlich galoissch ist, folgt mit Korollar 5.36, dass die Zerlegungsgruppe Z_p zyklisch sein muss und durch den Frobeniusautomorphismus $\mathrm{Frob}_p\colon a \mapsto a^{\#k(\mathfrak{p}\cap\mathcal{O}_\mathbb{Q})} = a^{\#k(p\mathbb{Z})} = a^p$ erzeugt wird (gilt für ein beliebiges Primideal $\mathfrak{p}$ über p).

$p \equiv 1 \mod 8$ Dann gilt $\mathrm{Frob}_p = (\zeta_8 \mapsto \zeta_8^p = \zeta_8) = \mathrm{id}$. Als Untergruppe von $(\mathbb{Z}/8\mathbb{Z})^\times$ erhalten wir $Z_p = \{1\}$.

$p \equiv 3 \mod 8$ Dann gilt $\mathrm{Frob}_p = (\zeta_8 \mapsto \zeta_8^p = \zeta_8^3)$. Als Untergruppe von $(\mathbb{Z}/8\mathbb{Z})^\times$ wird Z_p also von 3 erzeugt, wegen $3^2 \equiv 1 \mod 8$ folgt $Z_p = \{1,3\}$. Der Zerfällungskörper K^{Z_p} ist wegen $\#Z_p = 2$ ein quadratischer Unterkörper von K. Wegen $\mathrm{Frob}_p(\zeta_8 + \zeta_8^3) = \zeta_8^3 + \zeta_8^9 = \zeta_8 + \zeta_8^3$ muss

$$\zeta_8 + \zeta_8^3 = \frac{\sqrt{2}}{2}(1+i) + \frac{\sqrt{2}}{2}(-1+i) = \frac{\sqrt{2}}{2}\cdot 2i = \sqrt{-2}$$

in K^{Z_p} enthalten sein. Nun ist aber $\mathbb{Q}(\sqrt{-2})$ bereits ein quadratischer Unterkörper von K, es folgt $K^{Z_p} = \mathbb{Q}(\sqrt{-2})$.

$p \equiv 5 \mod 8$ Dann gilt $\mathrm{Frob}_p = (\zeta_8 \mapsto \zeta_8^p = \zeta_8^5)$. Als Untergruppe von $(\mathbb{Z}/8\mathbb{Z})^\times$ wird Z_p also von 5 erzeugt, wegen $5^2 \equiv 1 \mod 8$ folgt $Z_p = \{1,5\}$. Der Zerfällungskörper K^{Z_p} ist wegen $\#Z_p = 2$ ein quadratischer Unterkörper von K. Wegen $\mathrm{Frob}_p(\zeta_5^2) = \zeta_5^{10} = \zeta_8^2 = i$ muss i in K^{Z_p} enthalten sein. Nun ist aber $\mathbb{Q}(i)$ bereits ein quadratischer Unterkörper von K, es folgt $K^{Z_p} = \mathbb{Q}(i)$.

$p \equiv 7 \mod 8$ Dann gilt $\mathrm{Frob}_p = (\zeta_7 \mapsto \zeta_8^p = \zeta_8^7)$. Als Untergruppe von $(\mathbb{Z}/8\mathbb{Z})^\times$ wird Z_p also von 7 erzeugt, wegen $7^2 \equiv 1 \mod 8$ folgt $Z_p = \{1,7\}$. Der Zerfällungskörper K^{Z_p} ist wegen $\#Z_p = 2$ ein quadratischer Unterkörper von K. Wegen $\mathrm{Frob}_p(\zeta_8 + \zeta_8^7) = \zeta_8^7 + \zeta_8^{49} = \zeta_8 + \zeta_8^7$ muss

$$\zeta_8 + \zeta_8^7 = \frac{\sqrt{2}}{2}(1+i) + \frac{\sqrt{2}}{2}(1-i) = \frac{\sqrt{2}}{2}\cdot 2 = \sqrt{2}$$

in K^{Z_p} enthalten sein. Nun ist aber $\mathbb{Q}(\sqrt{2})$ bereits ein quadratischer Unterkörper von K, es folgt $K^{Z_p} = \mathbb{Q}(\sqrt{2})$.

Aufgabe 2

Es gilt nach VL

$$\mathcal{O}_{\mathbb{Q}(\zeta_n+\zeta_n^{-1})} = \mathcal{O}_{\mathbb{Q}(\zeta_n)} \cap \mathbb{Q}(\zeta_n + \zeta_n^{-1}) = \mathbb{Z}[\zeta_n] \cap \mathbb{Q}(\zeta_n + \zeta_n^{-1}).$$

Daraus folgt sofort

$$\mathbb{Z}[\zeta_n + \zeta_n^{-1}] \subset \mathcal{O}_{\mathbb{Q}(\zeta_n+\zeta_n^{-1})} \subset \mathbb{Z}[\zeta_n].$$

Der schwierige Teil des Beweises fehlt

Aufgabe 3

Z.Z.:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{2}}$$

Beweis. Den größten Teil der Äquivalenzen aus dem Beweis von Korollar 6.12 können wir sofort für $q = 2$ übernehmen. Es gilt $\left(\frac{2}{p}\right) = 1 \Leftrightarrow 2$ zerfällt in $K \coloneqq \mathbb{Q}(\sqrt{(-1)^{\frac{p-1}{2}}p})$. Dass 2 in diesem quadratischen Zahlkörper zerfällt, ist nach Satz 5.23(ii) äquivalent dazu, dass $(-1)^{\frac{p-1}{2}} \cdot p = d_K \equiv 1 \mod 8$ ist. Das ist der Fall, wenn $p \equiv \pm 1 \mod 8$ ist, $(-1)^{2k} \cdot p = p \equiv 1$ oder $(-1)^{2k-1} \cdot p = -1 \cdot p \equiv -1 \cdot -1 \equiv 1 \mod 8$. Ist $p \equiv \pm 3 \mod 8$, so erhalten wir $(-1)^{\frac{p-1}{2}}p = p \equiv -3 \mod 8$ oder $(-1)^{\frac{p-1}{2}}p = -p \equiv -3 \mod 8$. Es gilt also $\left(\frac{2}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \mod 8$. Laut der Umformulierung aus Theorem 2.11 ist das bereits die zu zeigende Aussage. □

Aufgabe 4

Z.Z.: Satz 6.14

Beweis. Angenommen, es gibt nur endlich viele Primzahlen $p \equiv 1 \mod n$. Sei P ihr Produkt. Betrachte nun $\Phi_n(xnP) \in \mathbb{N}$ für beliebiges $x \in \mathbb{N}$. Angenommen, $\Phi_n(xnP) > 1$. Dann existiert eine Primzahl p mit $p|\Phi_n(xnP)$. Nach Lemma 6.13 gilt dann $p \equiv 1 \mod n$, also $p|P$. Folglich gilt $xnP \equiv 0 \mod p$ und $\Phi_n(xnP) \equiv 0 \mod p$. Wir erhalten $\Phi_n(0) = 0 \mod p$, d.h. 0 ist eine Nullstelle von $\Phi_n(X)$ in $\mathbb{Z}/p\mathbb{Z}[X]$. Das kann wegen $\Phi_n(X)|X^n - 1$ nicht sein. Aus Lemma 6.13 geht hervor, dass es sich bei $\Phi_n(xnP)$ um eine natürliche Zahl handelt. Wäre $\Phi_n(xnP) = 0$ für ein x, so hätte Φ_n eine Nullstelle in $\mathbb{Z}$, im Widerspruch zur Irreduzibilität. Also folgt $\Phi_n(xnP) = 1 \forall x \in \mathbb{N}$. Damit hätte $\Phi_n(xnP) - 1$ unendlich viele Nullstellen in $\mathbb{Z}[X]$. Das ist ein Widerspruch und damit folgt die Behauptung. □