H23-T1-A5

a) Zeigen Sie, dass der Kreisteilungskörper $\mathbb{Q}(\zeta_8)$ genau drei quadratische Teilkörper besitzt, d.h. Zwischenkörper $\mathbb{Q} \subseteq K \subseteq \mathbb{Q}(\zeta_8)$ mit $[K : \mathbb{Q}] = 2$.

b) Bestimmen Sie in Teil a) drei Elemente $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{Q}$ so, dass die Zwischenkörper $K_i := \mathbb{Q}(\sqrt{\alpha_i})(1 \leq i \leq 3)$ genau die quadratischen Teilkörper sind.

c) Zeigen Sie, dass das Polynom $X^4 + X + 1 \in \mathbb{F}_2[X]$ irreduzibel ist.

d) Nach Teil c) gilt $\mathbb{F}_{16} = \mathbb{F}_2(\alpha)$ für ein $\alpha \in \overline{\mathbb{F}}_2$ mit $\alpha^4 + \alpha + 1 = 0$. Bestimmen sie die Grade $[\mathbb{F}_2(\beta) : \mathbb{F}_2]$ in den beiden Fällen $\beta = \alpha + 1$ und $\beta = \alpha^3 + 1$.

Lösung

a) Bekanntlich gilt $\mathrm{Gal}(\mathbb{Q}(\zeta_8)|\mathbb{Q}) \cong (\mathbb{Z}/8\mathbb{Z}, \cdot)^*$. Wir zeigen, dass $(\mathbb{Z}/8\mathbb{Z}, \cdot)^*$ nicht zyklisch ist. Die Einheiten können leicht berechnet werden, man erhält

$$(\mathbb{Z}/8\mathbb{Z}, \cdot)^* = \{1, 3, 5, 7\}.$$

Man rechnet leicht nach, dass die Ordnung aller Elemente der Einheitengruppen, abgesehen des neutralen Elements, 2 ist, daher gilt $(\mathbb{Z}/8\mathbb{Z}, \cdot)^* \cong (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$. Diese Gruppe hat bekanntlich genau 3 Untegruppen der Ordnung 2 und daraus folgt mit dem Hauptsatz der Galois-Theorie (dieser ist hier anwendbar, da $\mathbb{Q}(\zeta_8)|\mathbb{Q}$ endlich, normal da Zerfällungskörper von $X^8 - 1$ über $\mathbb{Q}$ und seperabel da der Grundkörper Charakteristik 0 hat), dass es genau 3 solche Zwischenerweiterungen K gibt.

b) Mit der Euler-Formel erhält man $\zeta_8 = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$. Wir behaupten nun $\mathbb{Q}(\zeta_8) = \mathbb{Q}(i, \sqrt{2})$. Die Inklusion „$\subseteq$“ ist trivial. Für die andere Inklusion betrachtet man $\zeta_8^2 = i$ woraus $i \in \mathbb{Q}(\zeta_8)$ folgt. Hieraus folgert man mit einigen Umformungen $\frac{2 \cdot \zeta_8}{1+i} = \sqrt{2} \in \mathbb{Q}(\sqrt{2})$ was den Beweis der Behauptung abschließt. Man betrachte daher die Teilkörper von $\mathbb{Q}(i, \sqrt{2})$ $K_1 = \mathbb{Q}(\sqrt{2}), K_2 = \mathbb{Q}(\sqrt{-1})$ sowie $K_3 = \mathbb{Q}(\sqrt{-2})$ (nach der obigen Behauptung sieht man nun leicht, dass dies Teilkörper von $\mathbb{Q}(\zeta_8)$ sind). Dass diese quadratische Teilkörper sind, zeigt man indem man nachweist, dass $X^2 - 2, X^2 + 1$ und $X^2 + 2$ die Minimalpolynome von $\sqrt{2}$, $\sqrt{-1}$ und $\sqrt{-2}$ sind (Bitte nachweisen!). $\alpha_1 = 2, \alpha_2 = -1$ und $\alpha_3 = -2$ lösen also Teil b).

c) $f = X^4 + X + 1$ hat in $\mathbb{F}_2$ offenbar keine Nullstellen. Wäre f also reduzibel, so müsste es folglich in zwei Polynome von Grad 2 zerfallen. Diese sind oBdA normiert und haben als freien Term 1. Man betrachtet daher

$$(X^2 + aX + 1) \cdot (X^2 + bX + 1) = X^4 + (a+b)X^3 + abX^2 + (a+b)X + 1 \overset{!}{=} f$$

Nach Koeffizientenvergleich folgt also $a + b = 0$ und $ab = 0$. Dies liefert einen Widerspruch im Körper mit 2 Elementen. Folglich ist f irreduzibel.

d) Wir betrachten zunächst den folgenden Körperturm:

$$\begin{array}{c} \mathbb{F}_2(\alpha) \\ | \\ \mathbb{F}_2(\beta) \\ | \\ \mathbb{F}_2. \end{array}$$

In beiden Fällen gilt offenbar $\mathbb{F}_2(\beta) \subseteq \mathbb{F}_2(\alpha)$ und da $[\mathbb{F}_2(\alpha) : \mathbb{F}_2] = 4$ folgt nach Gradformel $[\mathbb{F}_2(\beta) : \mathbb{F}_2] \in \{1, 2, 4\}$. Angenommen $\beta \in \mathbb{F}_2$, dann wäre in beiden Fälle $f = X^4 + X + 1$ nicht das Minimalpolynom von α (im Fall $\beta = \alpha + 1$ wäre also $X + 1$ ein Polynom mit kleinerem Grad als das Minimalpolynom welches α als Nullstelle hat, im Fall $\beta = \alpha^3 + 1$ wäre $X^3 + 1$ so ein Polynom vom kleineren Grad) - ein Widerspruch zur Irreduzibilität von f. Man bemerkt noch, dass es in $\mathbb{F}_2[X]$ ausschließlich das irreduzible Polynom $g := X^2 + X + 1$ vom Grad 2 gibt.

i) Sei $\beta = \alpha + 1$. Man zeigt zunächst:

$$f(\beta) = (\alpha + 1)^4 + (\alpha + 1) + 1 = \alpha^4 + \alpha + 1 = 0.$$

Hieraus folgt, dass β Nullstelle von f ist und da f nach c) irreduzibel und normiert ist, folgt $[\mathbb{F}_2(\beta) : \mathbb{F}_2] = 4$.

ii) Sei nun $\beta = \alpha_3 + 1$.

$$g(\beta) = \alpha^6 + 1 + \alpha^3 + 1 + 1 = \alpha^6 + \alpha^3 + 1 = \alpha^6 + \alpha^3 + (\alpha^4 + \alpha) = \alpha^2 + 1 = \alpha^5 + \alpha + 1 \neq 0,$$

da $f \nmid X^5 + X + 1$ und f das Minimalpolynom von α über $\mathbb{Q}$ ist. Nach dem Ausschlusskriterium folgt schließlich erneut $[\mathbb{F}_2(\beta) : \mathbb{F}_2] = 4$.