F12-T2-A4

Es sei $L \subseteq \mathbb{C}$ der Zerfällungskörper von $f = X^4 + 4X^2 + 2 \in \mathbb{Q}[X]$.

a) Begründen Sie, dass f irreduzibel ist.

b) Warum ist die Körpererweiterung $L/\mathbb{Q}$ Galoissch?

c) Es sei $\alpha \in L$ eine Nullstelle von f. Begründen Sie, dass $\beta := \alpha^3 + 3\alpha$ eine Nullstelle von f ist.

d) Begründen Sie, dass $\mathbb{Q}(\alpha) = L$ gilt.

e) Wie viele Elemente enthält die Galoisgruppe $\mathrm{Gal}(L|\mathbb{Q})$?

f) Ist die Galoisgruppe zyklisch? Begründen Sie Ihre Antwort. (Hinweis: Betrachten Sie den $\mathbb{Q}$-Automorphismus σ, der durch $\sigma(\alpha) = \beta$ gegben ist, und bestimmen Sie $\sigma^2(\alpha)$.

Lösungsvorschlag. Zu a). f ist irreduibel nach dem Lemma von Gauß und dem Eisensteinkriterium für die Primzahl 2.
Zu b). L ist Zerfällungskörper eines separablen Polynomes über $\mathbb{Q}$ und damit sowohl normal als auch separabel (letzteres war ohnehin klar, da die Erweiterung endlich und $\mathbb{Q}$ ein perfekter Körper ist), also Galoissch.
Zu c).

Explizite Variante Wir setzen β in f ein und rechen $f(\beta) = 0$ (unter Verwendeung von $f(\alpha) = 0$) nach.

Variante mit etwas weniger Rechenaufwand Da f von der Form $f(X) = g(X^2)$ für ein $f \in \mathbb{Q}[X]$ ist, wissen wir bereits, dass die Nullstellen von f von der Form $\pm\alpha, \pm\beta'$ für ein $\beta' \in L$ sein müssen. Nun kann offensichtlich nicht $\beta = -\alpha$ gelten, da sonst $h(X) = X^3 - 2X$ ein Polynom wäre, dass α als Nullstelle hätte, aber $\deg(h) < \deg(f)$ im Widerspruch zur Irreduzibilität von f. Weiter wissen wir (nach Koeffizientenvergleich zwischen f und $(X - \alpha) \cdots (X + \beta')$), dass $2 = \alpha^2(\beta')^2$ gilt. Dies bestimmt β' bis auf Vorzeichen, denn ist $\alpha^2(\beta')^2 = 2 = \alpha^2(\beta'')^2$, so folgt $(\beta')^2 = 2/\alpha^2 = (\beta'')^2$, also $\beta' = \pm\beta''$. Mit dieser Vorüberlegung genügt es nun, Nachzurechnen, dass $\alpha^2\beta^2 = 2$ gilt:

$$\alpha^2\beta^2 = \alpha^2(\alpha^6 + 6\alpha^4 + 9\alpha^2) = \alpha^2(\underbrace{\alpha^6 + 4\alpha^4 + 2\alpha^2}_{=\alpha^2 f(\alpha)=0} + 2\alpha^4 + 7\alpha^2) =$$
$$= \alpha^2(2\alpha^4 + 8\alpha^2 + 4 - \alpha^2 - 4) = \alpha^2(-\alpha^2 - 4) = -\alpha^4 - 4\alpha^2 = 2$$

Zu d). Nach obigen Überlegunen ist bereits bekannt, dass $L = \mathbb{Q}(\pm\alpha, \pm\beta) = \mathbb{Q}(\alpha, \beta)$, und damit wegen $\beta \in \mathbb{Q}(\alpha)$:

$$L = \mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha).$$

Zu e). Es ist $|\mathrm{Gal}(L|\mathbb{Q})| = [L : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f) = 4.$

Zu f). Wie bereits gezeigt ist $L = \mathbb{Q}(\alpha)$. Wir setzen $G := \mathrm{Gal}(L|\mathbb{Q})$. Wie in Teil e) beobachtet gilt $|G| = 4$, womit nur die Möglichkeiten $G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ und $G \simeq \mathbb{Z}_4$ bleiben. Die vier Elemente von $G = \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha)$ sind gerade durch die Bilder von α eindeutig bestimmt, also

$$G = \{\mathrm{Id} = \sigma_1 \colon \alpha \mapsto \alpha, \sigma_2 \colon \alpha \mapsto -\alpha, \sigma := \sigma_3 \colon \alpha \mapsto \beta, \sigma_4 \colon \alpha \mapsto -\beta\}.$$

Nach Definition ist $\mathrm{ord}(\sigma_2) = 2$. Ist nun $\mathrm{ord}(\sigma) = 2$, so existieren bereits zwei Elemente der Ordnung 2, womit $G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ nicht zyklisch wäre. Ist aber $\mathrm{ord}(\sigma) = 4$, so ist $G \simeq \mathbb{Z}_4$ zyklisch. Wir untersuchen also dem Hinweis folgend die Ordnung von σ und berechnen

$$\begin{gathered}\sigma^2(\alpha) = \sigma(\beta) = \sigma(\alpha)^3 + 3\sigma(\alpha) = \beta^3 + 3\beta = (\alpha^3 + 3\alpha)^3 + 3\alpha^3 + 9\alpha = \\ = \alpha^9 + 9\alpha^7 + 27\alpha^5 + 27\alpha^3 + 3\alpha^3 + 9\alpha = \alpha(\alpha^8 + 4\alpha^6 + 2\alpha^4 + 5\alpha^6 + 25\alpha^4 + 30\alpha^2 + 9) = \\ = \alpha(5\alpha^6 + 20\alpha^4 + 10\alpha^2 + 5\alpha^4 + 20\alpha^2 + 9) = \alpha(5\alpha^4 + 20\alpha^2 + 10 - 1) = -\alpha.\end{gathered}$$

Somit ist $\sigma^2 \neq \mathrm{Id}$, also $\mathrm{ord}(\sigma) = 4$, womit G zyklisch ist.