(b) Bestimmen Sie für jedes der folgenden Polynome den Zerfällungskörper über $\mathbb{Q}$ als Teilkörper von $\mathbb{C}$, sowie den Grad des Zerfällungskörpers über $\mathbb{Q}$; begründen Sie kurz Ihre Antwort.

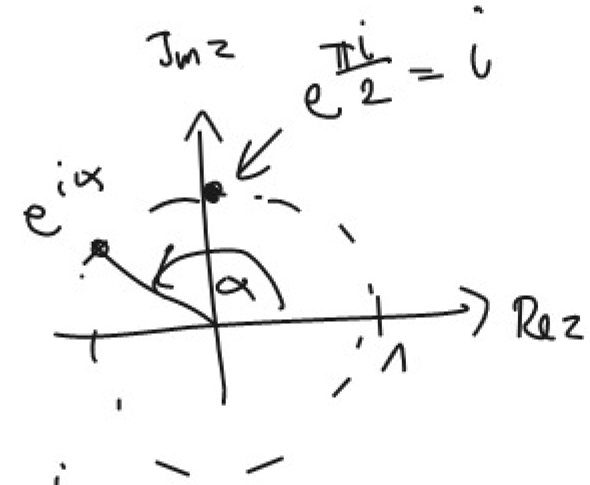
(i) $f = X^7 - 5$.

(ii) $g = 2X^2 + 3X - 2$.

ii) $g = 2\cdot\left(X^2 + \frac{3}{2}X - 1\right) =$

$= 2\cdot(X+2)\cdot\left(X - \frac{1}{2}\right)$

Zerfällungskörper von $g = \mathbb{Q}(-2, \frac{1}{2}) = \mathbb{Q}$ $\Rightarrow [\mathbb{Q}:\mathbb{Q}] = 1$



Aufgabe (Frühjahr 2007, T3A5)

Gegeben sei das Polynom $f = X^4 - 3 \in \mathbb{Q}[X]$.

a Beweisen Sie, dass $L = \mathbb{Q}(\sqrt[4]{3}, i)$ Zerfällungskörper von f ist.

b Bestimmen Sie den Grad der Körpererweiterung $L|\mathbb{Q}$.

c Beweisen Sie: $a = \sqrt[4]{3} + i$ ist ein primitives Element von L über $\mathbb{Q}$.

a) $x_k = \sqrt[4]{3}\cdot\left(e^{\frac{2\pi i}{4}}\right)^k \quad k = 0,1,2,3$

$x_0 = \sqrt[4]{3}$

$x_1 = \sqrt[4]{3}\cdot e^{\frac{2\pi i}{4}} = \sqrt[4]{3}\, e^{\frac{\pi i}{2}} = \sqrt[4]{3}\cdot i$

$x_2 = \sqrt[4]{3}\cdot\left(e^{\frac{2\pi i}{4}}\right)^2 = \sqrt[4]{3}\cdot i^2 = -\sqrt[4]{3}$

$x_3 = -\sqrt[4]{3}\cdot i$

Zerfällungskörper von $f = \mathbb{Q}(x_0, x_1, x_2, x_3)$

Zu zeigen: $\mathbb{Q}(x_0, x_1, x_2, x_3) \overset{!}{=} \mathbb{Q}(\sqrt[4]{3}, i)$

$\mathbb{Q}(x_0, x_1, x_2, x_3) = \mathbb{Q}(\sqrt[4]{3}, \sqrt[4]{3}i, -\sqrt[4]{3}, -\sqrt[4]{3}i)$

"$\subseteq$" klar

"$\supseteq$" $i = \frac{x_1}{x_0} = \frac{\sqrt[4]{3}i}{\sqrt[4]{3}} \in \mathbb{Q}(x_0, x_1, x_2, x_3)$ ✓

b) $[\mathbb{Q}(i, \sqrt[4]{3}) : \mathbb{Q}] = \underbrace{[\mathbb{Q}(\sqrt[4]{3})(i) : \mathbb{Q}(\sqrt[4]{3})]}_{=:d} \cdot \underbrace{[\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}]}_{= \operatorname{grad}(\mu_{\sqrt[4]{3},\mathbb{Q}}) = 4} = 2\cdot 4 = 8$

$d \neq 1$, da $\mathbb{Q}(\sqrt[4]{3}) \subseteq \mathbb{R}$ und $i \notin \mathbb{R}$

$\Rightarrow d = 2$ mit $\mu_{i,\mathbb{Q}(\sqrt[4]{3})} = X^2 + 1$

- $f = X^4 - 3 \in \mathbb{Q}[X]$ ✓
- $f(\sqrt[4]{3}) = 0$ ✓
- f normiert ✓
- f irreduzibel ✓ nach Eisenstein mit $p = 3$

$\Rightarrow f = \mu_{\sqrt[4]{3},\mathbb{Q}}$

miro

c)

Satz 3.14 (Satz vom primitiven Element). Sei $L|K$ eine endliche, separable Körpererweiterung. Dann existiert ein primitives Element der Erweiterung $L|K$, d. h. ein Element $\alpha \in L$ mit $L = K(\alpha)$.

Aufgabe (Frühjahr 2007, T3A5)

Gegeben sei das Polynom $f = X^4 - 3 \in \mathbb{Q}[X]$.

a Beweisen Sie, dass $L = \mathbb{Q}(\sqrt[4]{3}, i)$ Zerfällungskörper von f ist.

b Bestimmen Sie den Grad der Körpererweiterung $L|\mathbb{Q}$.

c Beweisen Sie: $a = \sqrt[4]{3} + i$ ist ein primitives Element von L über $\mathbb{Q}$.

c) Zu zeigen: $\mathbb{Q}(\underbrace{\sqrt[4]{3}+i}_{a}) = \overbrace{\mathbb{Q}(\sqrt[4]{3}, i)}^{L_2}$

Binomische Formel

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} \cdot a^k \cdot b^{n-k}$$

„$\subseteq$" klar, da $a = \underbrace{\sqrt[4]{3}}_{\in L_2} + \underbrace{i}_{\in L_2} \in L_2$

„$\supseteq$" $(a-i)^4 = 3$

$$a^4 + 4 \cdot a^3 \cdot (-i) + \underbrace{\binom{4}{2}}_{=6} \cdot a^2 \cdot (-1) + 4 \cdot a \cdot \underbrace{(\underbrace{-i}_{=i})^3}_{} + \underbrace{(-i)^4}_{=1} = 3$$

$(-1)^3 \cdot i^2 \cdot i$

$= (-1) \cdot (-1) \cdot i = i$

$$\binom{4}{2} = \frac{4!}{2! \cdot 2!} = 6$$

$$a^4 - 4a^3 i - 6a^2 + 4ai + 1 = 3$$

$$i \cdot (-4a^3 + 4a) = 3 - a^4 + 6a^2 - 1$$

$$i = \frac{2 - a^4 + 6a^2}{-4a^3 + 4a} = \frac{2 - a^4 + 6a^2}{\underbrace{4a}_{\neq 0} \cdot \underbrace{(-a^2 + 1)}_{\neq 0}} \in \mathbb{Q}(a)$$

$\Rightarrow i \in \mathbb{Q}(a)$

$\sqrt[4]{3} = \underbrace{a}_{\in \mathbb{Q}(a)} - \underbrace{i}_{\in \mathbb{Q}(a)} \in \mathbb{Q}(a)$ ✓

miro

Aufgabe (Frühjahr 2000, T2A3)

a Man bestimme ein primitives Element für die Körpererweiterung $\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{5})|\mathbb{Q}$.

Sei $\alpha = \sqrt[3]{2} \cdot \sqrt[4]{5}$

Zu zeigen: $\mathbb{Q}(\alpha) \overset{!}{=} \mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{5})$

"$\subseteq$" klar

"$\supseteq$"

$$\alpha^4 = 5 \cdot (\sqrt[3]{2})^{4 = 3+1} = 5 \cdot (\sqrt[3]{2})^3 \cdot \sqrt[3]{2} = 10 \cdot \sqrt[3]{2}$$

$$\Rightarrow \sqrt[3]{2} = \frac{\alpha^4}{10} \in \mathbb{Q}(\alpha) \checkmark$$

$$\Rightarrow \sqrt[4]{5} = \frac{\alpha \in \mathbb{Q}(\alpha)}{\sqrt[3]{2} \in \mathbb{Q}(\alpha)} \in \mathbb{Q}(\alpha) \checkmark$$

NK Hapuzak SS 18

Aufgabe 1 (2 Punkte):

Gibt es eine Untergruppe von $\mathbb{Z}/12\mathbb{Z}$, die isomorph zu $\mathbb{Z}/8\mathbb{Z}$ ist?

$|\mathbb{Z}/12\mathbb{Z}| = 12 \qquad |\mathbb{Z}/8\mathbb{Z}| = 8$

$\boxed{G \text{ Gruppe}, |G| < \infty \quad U \leq G \text{ Untergruppe} \Rightarrow |U| \mid |G|}$

Wenn $U \cong \mathbb{Z}/8\mathbb{Z} \Rightarrow |U| = 8$

$\Rightarrow 8 \nmid 12 \Rightarrow U$ keine UG von $\mathbb{Z}/12\mathbb{Z}$

Aufgabe 2 (1+2 Punkte):

Sei G eine endliche Gruppe und seien $H, H' \subsetneq G$ zwei echte Untergruppen. Zeigen Sie:

(a) Ist $H \subsetneq H'$, so ist $\#H \leq \frac{1}{4}\#G$.

(b) Ist $H \neq H'$, so ist $\#(H \cap H') \leq \frac{1}{4}\#G$.

a) $H \cap H'$ ist auch UG

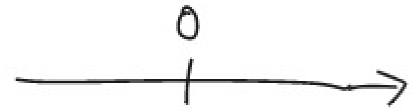
und $H \cap H' \subsetneq H'$ $\underset{a)}{\Rightarrow}$ Behauptung

miro

Aufgabe 2 (2+2 Punkte):

(a) Geben Sie ein Element $a \in \mathbb{Q}^\times$ der Ordnung 2 und ein Element $b \in \mathbb{Q}^\times$ der Ordnung ∞ an.

(b) Geben Sie einen injektiven Gruppenhomomorphismus von $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ nach $\mathbb{Q}^\times$ an.
Hinweis: Die Elemente a und b aus (a) sind nützlich.



a) G Gruppe, $g \in G$

$\mathrm{ord}(g) = \min\{n \in \mathbb{N} \mid g^n = 1\} = |\langle g \rangle|$

$\langle g \rangle = \{g^n \mid n \in \mathbb{N}\}$

$\mathrm{ord}(g) \mid |G|$

Sei $a := (-1)$ $\qquad a^1 \neq 1 \quad a^2 = 1$

$a^2 = (-1)^2 = 1 \Rightarrow \mathrm{ord}(a) = 2$

Wähle $b := 5 \qquad \mathrm{ord}(b) = \infty$

b) $f: \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{Q}^\times$

$(0, \bar{1}) \longmapsto -1$

$(0, \bar{0}) \longmapsto 1$

$(1, \bar{0}) \longmapsto 5$

$(-1, \bar{0}) \longmapsto \frac{1}{5}$

f ist dadurch eindeutig festgelegt

$f((3, \bar{1})) = f((1,\bar{0}) + (1,\bar{0}) + (1,\bar{0}) + (0,\bar{1}))$

$= f((1,\bar{0})) \cdot f((1,\bar{0})) \cdot f((1,\bar{0})) \cdot f((0,\bar{1}))$

$= 5 \cdot 5 \cdot 5 \cdot (-1) = -125$

$(G, +), (H, \cdot)$ Gruppen

$f: G \to H$ Gruppenhom. $:\Leftrightarrow$

$\forall g_1, g_2 \in G: f(g_1 + g_2) = f(g_1) \cdot f(g_2)$

$\Rightarrow \forall g \in G: \mathrm{ord}(g) = \mathrm{ord}(f(g))$

$f(0_G) = 1_H$

$\forall g \in G: f(g^{-1}) = (f(g))^{-1}$

miro

Aufgabe 4 (2 Punkte):

Sei G eine Gruppe der Ordnung 16, die auf einer Menge X mit 11 Elementen operiert. Zeigen Sie, dass eine solche Operation mindestens drei Bahnen hat.

Hinweis: Was können Sie über Bahnlängen sagen?

$\circ : G \times X \to X$

Gruppenop

Sei $x \in X$. $G(x) = \{g \cdot x \mid g \in G\} \subseteq X$

Bahn von x

$Stab(x) = \{g \in G \mid g \circ x = x\} \subseteq G$

Stabilisator

Es gilt $Stab(x)$ ist Untergruppe von G

und $|G(x)| = \frac{|G|}{|Stab(x)|} = (G : Stab(x))$

$\Rightarrow \boxed{|G(x)| \mid |G|}$

Angenommen es gäbe nur eine Bahn $G(x)$.

$\Rightarrow |G(x)| = 11$

Das geht nicht, da $11 \nmid 16$

Zwei Bahnen sind entweder gleich oder disjunkt!

Angenommen es gäbe zwei Bahnen $G(x_1)$ und $G(x_2)$

1. Fall $|G(x_1)| = 5$ $|G(x_2)| = 6$ geht nicht, da $5 \nmid 16$
2. Fall $|G(x_1)| = 4$ $|G(x_2)| = 7$ " $7 \nmid 16$
3. Fall " $= 3$ " $= 8$ " $3 \nmid 16$
4. Fall " $= 2$ " $= 9$ $9 \nmid 16$
5. Fall " $= 1$ " $= 10$ " $10 \nmid 16$

$\Rightarrow$ gibt mind. 3 Bahnen