Rozkladové nadtěleso $x^3 - 2$ nad $\mathbb{Q}$

Označme $\omega = e^{\frac{2\pi i}{3}}$, pak jsou kořeny polynomu $f = x^3 - 2$ v komplexních číslech $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$ a $\omega^2\sqrt[3]{2}$. Rozkladovým tělesem nad $\mathbb{Q}$ je tedy

$$T := \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}).$$

Zjednodušme to, jak T vyrábíme z $\mathbb{Q}$. Nemusíme explicitně přidávat $\omega^2\sqrt[3]{2}$, protože už jej vyrobíme z druhých dvou kořenů jako

$$\left(\omega\sqrt[3]{2}\right)^2 \cdot \left(\sqrt[3]{2}\right)^2 \cdot \frac{1}{2},$$

takže stačí uvažovat $T = \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2})$. Oba tyto kořeny už uvažovat musíme, protože např. $T \neq \mathbb{Q}(\sqrt[3]{2})$ (to je podtěleso $\mathbb{R}$, kdežto $\omega\sqrt[3]{2}$ není reálné!).

Jaký je stupeň rozšíření $[T : \mathbb{Q}]$? Oba prvky, které přidáváme, mají stupeň 3 nad $\mathbb{Q}$, nicméně stupeň rozšíření T není 9: můžeme rozepsat

$$[T : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}) : \mathbb{Q}] = \underbrace{[\mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{2})]}_{=?} \cdot \underbrace{[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]}_{=3}.$$

Pod otazníkem se neschovává trojka, protože nad tělesem $\mathbb{Q}(\sqrt[3]{2})$ už $x^3 - 2$ není minimálním polynomem $\omega\sqrt[3]{2}$, protože se rozkládá

$$x^3 - 2 = (x - \sqrt[3]{2})\left(x^2 - \sqrt[3]{2}x + \sqrt[3]{4}\right),$$

takže minimálním polynomem $\omega\sqrt[3]{2}$ je $x^2 - \sqrt[3]{2}x + \sqrt[3]{4}$ (to už skutečně je ireducibilní, jelikož je kvadratický a nemá v $\mathbb{Q}(\sqrt[3]{2})$ kořen). Dostaneme tedy $[T : \mathbb{Q}] = 2 \cdot 3$.

K témuž jsme mohli dojít také zapsáním $T = \mathbb{Q}(\sqrt[3]{2}, \omega)$, jelikož $\omega = \frac{\omega\sqrt[3]{2}}{\sqrt[3]{2}} \in \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2})$ a naopak $\omega\sqrt[3]{2} = \sqrt[3]{2} \cdot \omega \in \mathbb{Q}(\sqrt[3]{2}, \omega)$. Samo ω je kvadratické už nad $\mathbb{Q}$ (minimální polynom je $x^2 + x + 1$)

Co je $\mathrm{Gal}(T/\mathbb{Q})$? Budeme využívat tvrzení 2.12 ze skript. Každý $\mathbb{Q}$-automorfismus $\varphi : T \to T$ už je jednoznačně určený tím, kam se pošlou kořeny $x^3 - 2$ (generují T jako tělesové rozšíření $\mathbb{Q}$). Podle 2.12a) ale musí φ musí tyto kořeny permutovat, takže se $\mathrm{Gal}(T/\mathbb{Q})$ vnořuje do S_3. To znamená, že je izomorfní nějaké podgrupě S_3. Ukážeme, že je to celá S_3.

Ze zápisu $T = \mathbb{Q}(\sqrt[3]{2}, \omega)$ víme, že automorfismy v $\mathrm{Gal}(T/\mathbb{Q})$ jsou také jednoznačně určeny tím, kam se pošlou $\sqrt[3]{2}$ (prvek s kubickým minimálním polynomem) a ω (prvek s kvadratickým minimálním polynomem) – to je $3 \cdot 2$ možností. Místo manuálního ověření, že to všechno jsou automorfismy (vždy zvolíme, kam se pošlou kořeny, rozšíříme linearitou a následně potřebujeme ověřit, že výsledné zobrazení respektuje násobení a je bijekcí), využijeme grupovou strukturu:

Nejdřív uvážíme T jako rozšíření $\mathbb{Q}(\omega)$. Jakýkoliv $\mathbb{Q}(\omega)$-automorfismus $\varphi : T \to T$ musí tím spíš být i $\mathbb{Q}$-automorfismus, takže $\mathrm{Gal}(T/\mathbb{Q}(\omega)) \subset \mathrm{Gal}(T/\mathbb{Q})$. Můžeme přitom interpretovat T jako *rozkladové* nadtěleso $x^3 - 2$ nad $\mathbb{Q}(\omega)$, takže podle 2.12b) pro každou volbu kořene, na který se může poslat $\sqrt[3]{2}$, existuje automorfismus φ, který jej tam skutečně pošle. Máme tedy nějaké

$$\varphi \in \mathrm{Gal}(T/\mathbb{Q}(\omega)) \subset \mathrm{Gal}(T/\mathbb{Q})$$

splňující $\varphi(\omega) = \omega$ a zároveň $\varphi(\sqrt[3]{2}) = \omega\sqrt[3]{2}$. Nahlédněme, že φ má v Galoisově grupě řád 3:

$$\begin{aligned}
\varphi(\omega) &= \omega, & \varphi(\sqrt[3]{2}) &= \omega\sqrt[3]{2},\\
\varphi^2(\omega) &= \omega, & \varphi^2(\sqrt[3]{2}) &= \varphi(\omega) \cdot \varphi(\sqrt[3]{2}) = \omega^2\sqrt[3]{2},\\
\varphi^3(\omega) &= \omega, & \varphi^3(\sqrt[3]{2}) &= \varphi(\omega)^2 \cdot \varphi(\sqrt[3]{2}) = \omega^3\sqrt[3]{2} = \sqrt[3]{2}.
\end{aligned}$$

Tedy φ^3 se shoduje na obou generujících prvcích s id, takže $\varphi^3 = \mathrm{id}$, ale žádná menší mocnina tuto vlastnost nemá. Takže φ je prvek v $\mathrm{Gal}(T/\mathbb{Q})$ řádu 3.

Úplně obdobně se můžeme na T dívat jako na kvadratické rozšíření $T = \left(\mathbb{Q}(\sqrt[3]{2})\right)(\omega)$ o kořen ireducibilního kvadratického polynomu $x^2 + x + 1$. Analogicky bychom pak získali automorfismus $\psi \in \mathrm{Gal}(T/\mathbb{Q}(\sqrt[3]{2})) \subset \mathrm{Gal}(T/\mathbb{Q})$, který zobrazuje $\sqrt[3]{2} \mapsto \sqrt[3]{2}$ a $\omega \mapsto \overline{\omega} = \omega^2 = -\omega - 1$. Ten má v Galoisově grupě řád 2.

Dohromady tak víme, že $\mathrm{Gal}(T/\mathbb{Q})$ je izomorfní podgrupě S_3, která v sobě má prvek řádu 3 i prvek řádu 2. Z Lagrangeovy věty to už musí být celá šestiprvková S_3. Tím jsme také nepřímo dokázali, že kdykoliv zvolíme, kam se pošle $\sqrt[3]{2}$ a kam se pošle ω, vyrobíme z toho validní $\mathbb{Q}$-automorfismus.