Kruhové těleso

Definice. Libovolné komplexní číslo α, které je kořenem polynomu $x^n - 1$, kde $n \in \mathbb{N}$, se nazývá n-tá odmocnina z jedné.

Kruhové těleso

Definice. Libovolné komplexní číslo α, které je kořenem polynomu $x^n - 1$, kde $n \in \mathbb{N}$, se nazývá n-tá odmocnina z jedné.
Jestliže má α v multiplikativní grupě $\mathbb{C}^\times$ řád n, tj. není kořenem žádného polynomu $x^m - 1$, kde $1 \leq m < n$, nazývá se primitivní n-tá odmocnina z jedné.

Kruhové těleso

Definice. Libovolné komplexní číslo α, které je kořenem polynomu $x^n - 1$, kde $n \in \mathbb{N}$, se nazývá n-tá odmocnina z jedné.
Jestliže má α v multiplikativní grupě $\mathbb{C}^\times$ řád n, tj. není kořenem žádného polynomu $x^m - 1$, kde $1 \leq m < n$, nazývá se primitivní n-tá odmocnina z jedné.

Označení. Pro libovolné $n \in \mathbb{N}$ označme $\zeta_n = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$.

Kruhové těleso

Definice. Libovolné komplexní číslo α, které je kořenem polynomu $x^n - 1$, kde $n \in \mathbb{N}$, se nazývá n-tá odmocnina z jedné.
Jestliže má α v multiplikativní grupě $\mathbb{C}^\times$ řád n, tj. není kořenem žádného polynomu $x^m - 1$, kde $1 \leq m < n$, nazývá se primitivní n-tá odmocnina z jedné.

Označení. Pro libovolné $n \in \mathbb{N}$ označme $\zeta_n = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}$.

Věta 15. *Prvky grupy* $\langle \zeta_n \rangle = \{1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}\}$ *jsou právě všechny n-té odmocniny z jedné, a tedy*

$$x^n - 1 = \prod_{j=1}^{n} (x - \zeta_n^j).$$

Kruhové těleso

Definice. Libovolné komplexní číslo α, které je kořenem polynomu $x^n - 1$, kde $n \in \mathbb{N}$, se nazývá n-tá odmocnina z jedné.
Jestliže má α v multiplikativní grupě $\mathbb{C}^\times$ řád n, tj. není kořenem žádného polynomu $x^m - 1$, kde $1 \leq m < n$, nazývá se primitivní n-tá odmocnina z jedné.

Označení. Pro libovolné $n \in \mathbb{N}$ označme $\zeta_n = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}$.

Věta 15. *Prvky grupy* $\langle \zeta_n \rangle = \{1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}\}$ *jsou právě všechny n-té odmocniny z jedné, a tedy*

$$x^n - 1 = \prod_{j=1}^{n} (x - \zeta_n^j).$$

Primitivní n-té odmocniny z jedné jsou právě ty kořeny ζ_n^j, *pro které* $(j, n) = 1$.

Kruhové těleso

Definice. Libovolné komplexní číslo α, které je kořenem polynomu $x^n - 1$, kde $n \in \mathbb{N}$, se nazývá n-tá odmocnina z jedné.
Jestliže má α v multiplikativní grupě $\mathbb{C}^\times$ řád n, tj. není kořenem žádného polynomu $x^m - 1$, kde $1 \leq m < n$, nazývá se primitivní n-tá odmocnina z jedné.

Označení. Pro libovolné $n \in \mathbb{N}$ označme $\zeta_n = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}$.

Věta 15. *Prvky grupy* $\langle\zeta_n\rangle = \{1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}\}$ *jsou právě všechny n-té odmocniny z jedné, a tedy*

$$x^n - 1 = \prod_{j=1}^{n}(x - \zeta_n^j).$$

Primitivní n-té odmocniny z jedné jsou právě ty kořeny ζ_n^j, *pro které* $(j, n) = 1$.

Definice. Těleso $\mathbb{Q}(\zeta_n)$ se nazývá n-té kruhové těleso.

Kruhové těleso

Definice. Libovolné komplexní číslo α, které je kořenem polynomu $x^n - 1$, kde $n \in \mathbb{N}$, se nazývá n-tá odmocnina z jedné.
Jestliže má α v multiplikativní grupě $\mathbb{C}^\times$ řád n, tj. není kořenem žádného polynomu $x^m - 1$, kde $1 \leq m < n$, nazývá se primitivní n-tá odmocnina z jedné.

Označení. Pro libovolné $n \in \mathbb{N}$ označme $\zeta_n = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$.

Věta 15. *Prvky grupy* $\langle \zeta_n \rangle = \{1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}\}$ *jsou právě všechny n-té odmocniny z jedné, a tedy*

$$x^n - 1 = \prod_{j=1}^{n} (x - \zeta_n^j).$$

Primitivní n-té odmocniny z jedné jsou právě ty kořeny ζ_n^j, *pro které* $(j, n) = 1$.

Definice. Těleso $\mathbb{Q}(\zeta_n)$ se nazývá n-té kruhové těleso.

Poznámka. Protože $\mathbb{Q}(\zeta_n)$ je rozkladové těleso polynomu $x^n - 1$ nad $\mathbb{Q}$, je rozšíření $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_n)$ Galoisovo.

Kruhový polynom

Definice. Polynom

$$\Phi_n(x) = \prod_{\substack{j=1,\dots,n \\ (j,n)=1}} (x - \zeta_n^j)$$

se nazývá n-tý kruhový polynom.

Kruhový polynom

Definice. Polynom

$$\Phi_n(x) = \prod_{\substack{j=1,\dots,n \\ (j,n)=1}} (x - \zeta_n^j)$$

se nazývá n-tý kruhový polynom.

Věta 16. Pro každé přirozené číslo n platí

$$x^n - 1 = \prod_{d|n} \Phi_d(x),$$

kde v součinu probíhá d množinu všech kladných dělitelů čísla n.

Kruhový polynom

Definice. Polynom

$$\Phi_n(x) = \prod_{\substack{j=1,\dots,n \\ (j,n)=1}} (x - \zeta_n^j)$$

se nazývá n-tý kruhový polynom.

Věta 16. Pro každé přirozené číslo n platí

$$x^n - 1 = \prod_{d|n} \Phi_d(x),$$

kde v součinu probíhá d množinu všech kladných dělitelů čísla n.

Příklad. $\Phi_1(x) = x - 1$, $\Phi_2(x) = x + 1$, $\Phi_3(x) = x^2 + x + 1$, $\Phi_4(x) = x^2 + 1$, $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$, $\Phi_6(x) = x^2 - x + 1$.

Kruhový polynom

Definice. Polynom

$$\Phi_n(x) = \prod_{\substack{j=1,\dots,n \\ (j,n)=1}} (x - \zeta_n^j)$$

se nazývá n-tý kruhový polynom.

Věta 16. *Pro každé přirozené číslo n platí*

$$x^n - 1 = \prod_{d|n} \Phi_d(x),$$

kde v součinu probíhá d množinu všech kladných dělitelů čísla n.

Příklad. $\Phi_1(x) = x - 1$, $\Phi_2(x) = x + 1$, $\Phi_3(x) = x^2 + x + 1$, $\Phi_4(x) = x^2 + 1$, $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$, $\Phi_6(x) = x^2 - x + 1$.

Věta 17. *Pro každé $n \in \mathbb{N}$ je $\Phi_n(x)$ normovaný polynom stupně $\varphi(n)$ a platí $\Phi_n(x) \in \mathbb{Z}[x]$.*

Kruhový polynom

Definice. Polynom

$$\Phi_n(x) = \prod_{\substack{j=1,\dots,n \\ (j,n)=1}} (x - \zeta_n^j)$$

se nazývá n-tý kruhový polynom.

Věta 16. Pro každé přirozené číslo n platí

$$x^n - 1 = \prod_{d|n} \Phi_d(x),$$

kde v součinu probíhá d množinu všech kladných dělitelů čísla n.

Příklad. $\Phi_1(x) = x - 1$, $\Phi_2(x) = x + 1$, $\Phi_3(x) = x^2 + x + 1$, $\Phi_4(x) = x^2 + 1$, $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$, $\Phi_6(x) = x^2 - x + 1$.

Věta 17. Pro každé $n \in \mathbb{N}$ je $\Phi_n(x)$ normovaný polynom stupně $\varphi(n)$ a platí $\Phi_n(x) \in \mathbb{Z}[x]$.

Věta 18. Pro každé $n \in \mathbb{N}$ je $\Phi_n(x)$ ireducibilní polynom nad $\mathbb{Q}$, je to tedy minimální polynom čísla ζ_n nad $\mathbb{Q}$ a $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.

Galoisova grupa kruhového tělesa

Věta 19. *Pro každé $n \in \mathbb{N}$ je $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathbb{Z}_n^\times$. V tomto izomorfismu odpovídá zbytkové třídě $[a]_n$, kde $a \in \mathbb{Z}$, $(a, n) = 1$, automorfismus σ_a určený podmínkou $\sigma_a(\zeta_n) = \zeta_n^a$.*

Galoisova grupa kruhového tělesa

Věta 19. *Pro každé $n \in \mathbb{N}$ je* $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathbb{Z}_n^\times$. *V tomto izomorfismu odpovídá zbytkové třídě* $[a]_n$, *kde* $a \in \mathbb{Z}$, $(a, n) = 1$, *automorfismus* σ_a *určený podmínkou* $\sigma_a(\zeta_n) = \zeta_n^a$.

Příklad. Nechť $n \in \mathbb{N}$, $n > 2$. Automorfismus σ_1 je identita.

Galoisova grupa kruhového tělesa

Věta 19. *Pro každé $n \in \mathbb{N}$ je* $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathbb{Z}_n^\times$. *V tomto izomorfismu odpovídá zbytkové třídě* $[a]_n$, *kde* $a \in \mathbb{Z}$, $(a, n) = 1$, *automorfismus* σ_a *určený podmínkou* $\sigma_a(\zeta_n) = \zeta_n^a$.

Příklad. Nechť $n \in \mathbb{N}$, $n > 2$. Automorfismus σ_1 je identita. Platí $\sigma_{-1}(\zeta_n) = \zeta_n^{-1}$, což je číslo komplexně konjugované s ζ_n.

Galoisova grupa kruhového tělesa

Věta 19. *Pro každé $n \in \mathbb{N}$ je* $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathbb{Z}_n^\times$. *V tomto izomorfismu odpovídá zbytkové třídě* $[a]_n$, *kde* $a \in \mathbb{Z}$, $(a, n) = 1$, *automorfismus* σ_a *určený podmínkou* $\sigma_a(\zeta_n) = \zeta_n^a$.

Příklad. Nechť $n \in \mathbb{N}$, $n > 2$. Automorfismus σ_1 je identita. Platí $\sigma_{-1}(\zeta_n) = \zeta_n^{-1}$, což je číslo komplexně konjugované s ζ_n. Protože zúžení komplexní konjugovanosti na $\mathbb{Q}(\zeta_n)$ je automorfismus tohoto tělesa, platí $\sigma_{-1}(\alpha) = \overline{\alpha}$ pro každé $\alpha \in \mathbb{Q}(\zeta_n)$.

Galoisova grupa kruhového tělesa

Věta 19. *Pro každé $n \in \mathbb{N}$ je* $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathbb{Z}_n^\times$. *V tomto izomorfismu odpovídá zbytkové třídě* $[a]_n$, *kde* $a \in \mathbb{Z}$, $(a, n) = 1$, *automorfismus* σ_a *určený podmínkou* $\sigma_a(\zeta_n) = \zeta_n^a$.

Příklad. Nechť $n \in \mathbb{N}$, $n > 2$. Automorfismus σ_1 je identita. Platí $\sigma_{-1}(\zeta_n) = \zeta_n^{-1}$, což je číslo komplexně konjugované s ζ_n. Protože zúžení komplexní konjugovanosti na $\mathbb{Q}(\zeta_n)$ je automorfismus tohoto tělesa, platí $\sigma_{-1}(\alpha) = \overline{\alpha}$ pro každé $\alpha \in \mathbb{Q}(\zeta_n)$.
Podle hlavní věty Galoisovy teorie odpovídá dvouprvkové podgrupě $\langle \sigma_{-1} \rangle = \{\sigma_{-1}, \sigma_1\}$ podtěleso K tělesa $\mathbb{Q}(\zeta_n)$ právě těch prvků, které jsou ponechány na místě komplexní konjugovaností, tj. těch, které jsou reálné.

Galoisova grupa kruhového tělesa

Věta 19. Pro každé $n \in \mathbb{N}$ je $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathbb{Z}_n^\times$. V tomto izomorfismu odpovídá zbytkové třídě $[a]_n$, kde $a \in \mathbb{Z}$, $(a, n) = 1$, automorfismus σ_a určený podmínkou $\sigma_a(\zeta_n) = \zeta_n^a$.

Příklad. Nechť $n \in \mathbb{N}$, $n > 2$. Automorfismus σ_1 je identita. Platí $\sigma_{-1}(\zeta_n) = \zeta_n^{-1}$, což je číslo komplexně konjugované s ζ_n. Protože zúžení komplexní konjugovanosti na $\mathbb{Q}(\zeta_n)$ je automorfismus tohoto tělesa, platí $\sigma_{-1}(\alpha) = \overline{\alpha}$ pro každé $\alpha \in \mathbb{Q}(\zeta_n)$.
Podle hlavní věty Galoisovy teorie odpovídá dvouprvkové podgrupě $\langle \sigma_{-1} \rangle = \{\sigma_{-1}, \sigma_1\}$ podtěleso K tělesa $\mathbb{Q}(\zeta_n)$ právě těch prvků, které jsou ponechány na místě komplexní konjugovaností, tj. těch, které jsou reálné. Označme $K = \mathrm{Fix}(\langle \sigma_{-1} \rangle)$, tedy $K = \mathbb{Q}(\zeta_n) \cap \mathbb{R}$.

Galoisova grupa kruhového tělesa

Věta 19. Pro každé $n \in \mathbb{N}$ je $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathbb{Z}_n^\times$. V tomto izomorfismu odpovídá zbytkové třídě $[a]_n$, kde $a \in \mathbb{Z}$, $(a, n) = 1$, automorfismus σ_a určený podmínkou $\sigma_a(\zeta_n) = \zeta_n^a$.

Příklad. Nechť $n \in \mathbb{N}$, $n > 2$. Automorfismus σ_1 je identita. Platí $\sigma_{-1}(\zeta_n) = \zeta_n^{-1}$, což je číslo komplexně konjugované s ζ_n. Protože zúžení komplexní konjugovanosti na $\mathbb{Q}(\zeta_n)$ je automorfismus tohoto tělesa, platí $\sigma_{-1}(\alpha) = \overline{\alpha}$ pro každé $\alpha \in \mathbb{Q}(\zeta_n)$.
Podle hlavní věty Galoisovy teorie odpovídá dvouprvkové podgrupě $\langle \sigma_{-1} \rangle = \{\sigma_{-1}, \sigma_1\}$ podtěleso K tělesa $\mathbb{Q}(\zeta_n)$ právě těch prvků, které jsou ponechány na místě komplexní konjugovaností, tj. těch, které jsou reálné. Označme $K = \mathrm{Fix}(\langle \sigma_{-1} \rangle)$, tedy $K = \mathbb{Q}(\zeta_n) \cap \mathbb{R}$. Protože $\zeta_n + \zeta_n^{-1} = 2 \cos \frac{2\pi}{n} \in \mathbb{R}$, je $\mathbb{Q}(\zeta_n + \zeta_n^{-1}) \subseteq K$.

Galoisova grupa kruhového tělesa

Věta 19. Pro každé $n \in \mathbb{N}$ je $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathbb{Z}_n^\times$. V tomto izomorfismu odpovídá zbytkové třídě $[a]_n$, kde $a \in \mathbb{Z}$, $(a, n) = 1$, automorfismus σ_a určený podmínkou $\sigma_a(\zeta_n) = \zeta_n^a$.

Příklad. Nechť $n \in \mathbb{N}$, $n > 2$. Automorfismus σ_1 je identita. Platí $\sigma_{-1}(\zeta_n) = \zeta_n^{-1}$, což je číslo komplexně konjugované s ζ_n. Protože zúžení komplexní konjugovanosti na $\mathbb{Q}(\zeta_n)$ je automorfismus tohoto tělesa, platí $\sigma_{-1}(\alpha) = \overline{\alpha}$ pro každé $\alpha \in \mathbb{Q}(\zeta_n)$.
Podle hlavní věty Galoisovy teorie odpovídá dvouprvkové podgrupě $\langle \sigma_{-1} \rangle = \{\sigma_{-1}, \sigma_1\}$ podtěleso K tělesa $\mathbb{Q}(\zeta_n)$ právě těch prvků, které jsou ponechány na místě komplexní konjugovaností, tj. těch, které jsou reálné. Označme $K = \mathrm{Fix}(\langle \sigma_{-1} \rangle)$, tedy $K = \mathbb{Q}(\zeta_n) \cap \mathbb{R}$. Protože $\zeta_n + \zeta_n^{-1} = 2\cos\frac{2\pi}{n} \in \mathbb{R}$, je $\mathbb{Q}(\zeta_n + \zeta_n^{-1}) \subseteq K$. Polynom $(x - \zeta_n)(x - \zeta_n^{-1}) = x^2 - (\zeta_n + \zeta_n^{-1})x + 1 \in \mathbb{Q}(\zeta_n + \zeta_n^{-1})[x]$ má kořen ζ_n, přičemž $\zeta_n \notin K$, a tedy $\zeta_n \notin \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, proto je to minimální polynom čísla ζ_n nad $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$, a tedy $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n + \zeta_n^{-1})] = 2$.

Galoisova grupa kruhového tělesa

Věta 19. Pro každé $n \in \mathbb{N}$ je $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathbb{Z}_n^\times$. V tomto izomorfismu odpovídá zbytkové třídě $[a]_n$, kde $a \in \mathbb{Z}$, $(a, n) = 1$, automorfismus σ_a určený podmínkou $\sigma_a(\zeta_n) = \zeta_n^a$.

Příklad. Nechť $n \in \mathbb{N}$, $n > 2$. Automorfismus σ_1 je identita. Platí $\sigma_{-1}(\zeta_n) = \zeta_n^{-1}$, což je číslo komplexně konjugované s ζ_n. Protože zúžení komplexní konjugovanosti na $\mathbb{Q}(\zeta_n)$ je automorfismus tohoto tělesa, platí $\sigma_{-1}(\alpha) = \overline{\alpha}$ pro každé $\alpha \in \mathbb{Q}(\zeta_n)$.
Podle hlavní věty Galoisovy teorie odpovídá dvouprvkové podgrupě $\langle \sigma_{-1} \rangle = \{\sigma_{-1}, \sigma_1\}$ podtěleso K tělesa $\mathbb{Q}(\zeta_n)$ právě těch prvků, které jsou ponechány na místě komplexní konjugovaností, tj. těch, které jsou reálné. Označme $K = \mathrm{Fix}(\langle \sigma_{-1} \rangle)$, tedy $K = \mathbb{Q}(\zeta_n) \cap \mathbb{R}$. Protože $\zeta_n + \zeta_n^{-1} = 2\cos\frac{2\pi}{n} \in \mathbb{R}$, je $\mathbb{Q}(\zeta_n + \zeta_n^{-1}) \subseteq K$. Polynom $(x - \zeta_n)(x - \zeta_n^{-1}) = x^2 - (\zeta_n + \zeta_n^{-1})x + 1 \in \mathbb{Q}(\zeta_n + \zeta_n^{-1})[x]$ má kořen ζ_n, přičemž $\zeta_n \notin K$, a tedy $\zeta_n \notin \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, proto je to minimální polynom čísla ζ_n nad $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$, a tedy $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n + \zeta_n^{-1})] = 2$. Porovnáním stupňů $K = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$.

Příklad: nalezněme všechna podtělesa tělesa $\mathbb{Q}(\zeta_7)$

Protože $\mathbb{Z}_7^\times = \langle [3]_7 \rangle$, platí $\mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q}) = \langle \sigma_3 \rangle$.

Příklad: nalezněme všechna podtělesa tělesa $\mathbb{Q}(\zeta_7)$

Protože $\mathbb{Z}_7^\times = \langle [3]_7 \rangle$, platí $\mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q}) = \langle \sigma_3 \rangle$.
Tato grupa má jedinou podgrupu řádu d pro každé $d \mid 6$.

Příklad: nalezněme všechna podtělesa tělesa $\mathbb{Q}(\zeta_7)$

Protože $\mathbb{Z}_7^\times = \langle [3]_7 \rangle$, platí $\mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q}) = \langle \sigma_3 \rangle$.
Tato grupa má jedinou podgrupu řádu d pro každé $d \mid 6$.
Fixní těleso dvouprvkové podgrupy $\langle \sigma_{-1} \rangle = \{\sigma_{-1}, \sigma_1\}$ je $\mathbb{Q}(\zeta_n + \zeta_n^{-1}) = \mathbb{Q}(2\cos\frac{2\pi}{7})$.

Příklad: nalezněme všechna podtělesa tělesa $\mathbb{Q}(\zeta_7)$

Protože $\mathbb{Z}_7^\times = \langle [3]_7 \rangle$, platí $\mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q}) = \langle \sigma_3 \rangle$.
Tato grupa má jedinou podgrupu řádu d pro každé $d \mid 6$.
Fixní těleso dvouprvkové podgrupy $\langle \sigma_{-1} \rangle = \{\sigma_{-1}, \sigma_1\}$ je $\mathbb{Q}(\zeta_n + \zeta_n^{-1}) = \mathbb{Q}(2\cos\frac{2\pi}{7})$.
Fixní těleso tříprvkové podgrupy $\langle \sigma_2 \rangle = \{\sigma_2, \sigma_4, \sigma_1\}$ obsahuje $\alpha = \zeta_7 + \zeta_7^2 + \zeta_7^4$, neboť $\sigma_2(\alpha) = \zeta_7^2 + \zeta_7^4 + \zeta_7^8 = \alpha$.

Příklad: nalezněme všechna podtělesa tělesa $\mathbb{Q}(\zeta_7)$

Protože $\mathbb{Z}_7^\times = \langle [3]_7 \rangle$, platí $\mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q}) = \langle \sigma_3 \rangle$.
Tato grupa má jedinou podgrupu řádu d pro každé $d \mid 6$.
Fixní těleso dvouprvkové podgrupy $\langle \sigma_{-1} \rangle = \{\sigma_{-1}, \sigma_1\}$ je $\mathbb{Q}(\zeta_n + \zeta_n^{-1}) = \mathbb{Q}(2\cos\frac{2\pi}{7})$.
Fixní těleso tříprvkové podgrupy $\langle \sigma_2 \rangle = \{\sigma_2, \sigma_4, \sigma_1\}$ obsahuje $\alpha = \zeta_7 + \zeta_7^2 + \zeta_7^4$, neboť $\sigma_2(\alpha) = \zeta_7^2 + \zeta_7^4 + \zeta_7^8 = \alpha$. Přitom $\alpha^2 = \zeta_7^2 + \zeta_7^4 + \zeta_7^8 + 2(\zeta_7^3 + \zeta_7^5 + \zeta_7^6) = -2 - \alpha$, a tedy α je kořen polynomu $x^2 + x + 2$.

Příklad: nalezněme všechna podtělesa tělesa $\mathbb{Q}(\zeta_7)$

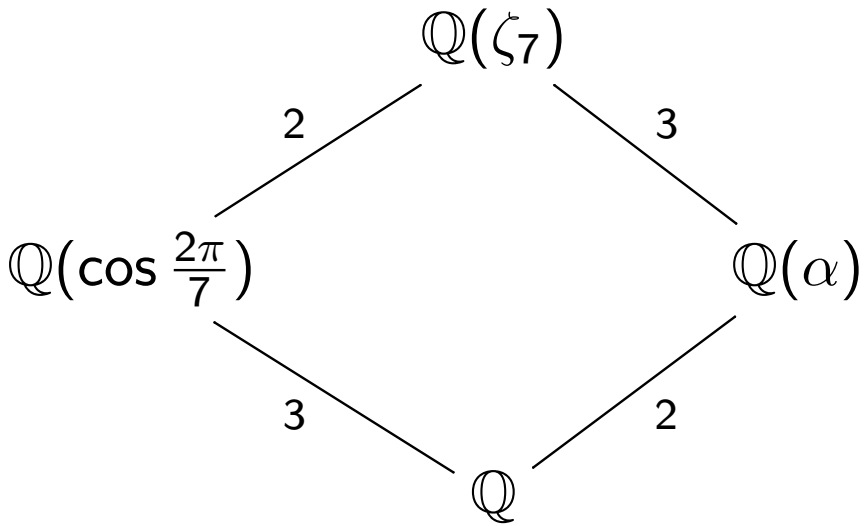
Protože $\mathbb{Z}_7^\times = \langle [3]_7 \rangle$, platí $\mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q}) = \langle \sigma_3 \rangle$.
Tato grupa má jedinou podgrupu řádu d pro každé $d \mid 6$.
Fixní těleso dvouprvkové podgrupy $\langle \sigma_{-1} \rangle = \{\sigma_{-1}, \sigma_1\}$ je $\mathbb{Q}(\zeta_n + \zeta_n^{-1}) = \mathbb{Q}(2\cos\frac{2\pi}{7})$.
Fixní těleso tříprvkové podgrupy $\langle \sigma_2 \rangle = \{\sigma_2, \sigma_4, \sigma_1\}$ obsahuje $\alpha = \zeta_7 + \zeta_7^2 + \zeta_7^4$, neboť $\sigma_2(\alpha) = \zeta_7^2 + \zeta_7^4 + \zeta_7^8 = \alpha$. Přitom $\alpha^2 = \zeta_7^2 + \zeta_7^4 + \zeta_7^8 + 2(\zeta_7^3 + \zeta_7^5 + \zeta_7^6) = -2 - \alpha$, a tedy α je kořen polynomu $x^2 + x + 2$. Tento polynom je ireducibilní nad $\mathbb{Q}$, a je to tedy minimální polynom čísla α nad $\mathbb{Q}$.

Příklad: nalezněme všechna podtělesa tělesa $\mathbb{Q}(\zeta_7)$

Protože $\mathbb{Z}_7^\times = \langle [3]_7 \rangle$, platí $\mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q}) = \langle \sigma_3 \rangle$.
Tato grupa má jedinou podgrupu řádu d pro každé $d \mid 6$.
Fixní těleso dvouprvkové podgrupy $\langle \sigma_{-1} \rangle = \{\sigma_{-1}, \sigma_1\}$ je $\mathbb{Q}(\zeta_n + \zeta_n^{-1}) = \mathbb{Q}(2\cos\frac{2\pi}{7})$.
Fixní těleso tříprvkové podgrupy $\langle \sigma_2 \rangle = \{\sigma_2, \sigma_4, \sigma_1\}$ obsahuje $\alpha = \zeta_7 + \zeta_7^2 + \zeta_7^4$, neboť $\sigma_2(\alpha) = \zeta_7^2 + \zeta_7^4 + \zeta_7^8 = \alpha$. Přitom $\alpha^2 = \zeta_7^2 + \zeta_7^4 + \zeta_7^8 + 2(\zeta_7^3 + \zeta_7^5 + \zeta_7^6) = -2 - \alpha$, a tedy α je kořen polynomu $x^2 + x + 2$. Tento polynom je ireducibilní nad $\mathbb{Q}$, a je to tedy minimální polynom čísla α nad $\mathbb{Q}$. Proto $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$.
Porovnáním stupňů $\mathrm{Fix}(\langle \sigma_2 \rangle) = \mathbb{Q}(\alpha)$.

Příklad: nalezněme všechna podtělesa tělesa $\mathbb{Q}(\zeta_7)$

Protože $\mathbb{Z}_7^\times = \langle [3]_7 \rangle$, platí $\mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q}) = \langle \sigma_3 \rangle$.
Tato grupa má jedinou podgrupu řádu d pro každé $d \mid 6$.
Fixní těleso dvouprvkové podgrupy $\langle \sigma_{-1} \rangle = \{\sigma_{-1}, \sigma_1\}$ je $\mathbb{Q}(\zeta_n + \zeta_n^{-1}) = \mathbb{Q}(2\cos\frac{2\pi}{7})$.
Fixní těleso tříprvkové podgrupy $\langle \sigma_2 \rangle = \{\sigma_2, \sigma_4, \sigma_1\}$ obsahuje $\alpha = \zeta_7 + \zeta_7^2 + \zeta_7^4$, neboť $\sigma_2(\alpha) = \zeta_7^2 + \zeta_7^4 + \zeta_7^8 = \alpha$. Přitom $\alpha^2 = \zeta_7^2 + \zeta_7^4 + \zeta_7^8 + 2(\zeta_7^3 + \zeta_7^5 + \zeta_7^6) = -2 - \alpha$, a tedy α je kořen polynomu $x^2 + x + 2$. Tento polynom je ireducibilní nad $\mathbb{Q}$, a je to tedy minimální polynom čísla α nad $\mathbb{Q}$. Proto $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$.
Porovnáním stupňů $\mathrm{Fix}(\langle \sigma_2 \rangle) = \mathbb{Q}(\alpha)$. Svaz všech podtěles tělesa $\mathbb{Q}(\zeta_7)$ tedy je



Abelovská tělesa

Definice. Podtěleso K tělesa $\mathbb{C}$ se nazývá abelovské, jestliže $K/\mathbb{Q}$ je Galoisovo rozšíření s komutativní Galoisovou grupou.

Abelovská tělesa

Definice. Podtěleso K tělesa $\mathbb{C}$ se nazývá abelovské, jestliže $K/\mathbb{Q}$ je Galoisovo rozšíření s komutativní Galoisovou grupou.

Důsledek. *Každé podtěleso K libovolného kruhového tělesa je abelovské.*

Abelovská tělesa

Definice. Podtěleso K tělesa $\mathbb{C}$ se nazývá abelovské, jestliže $K/\mathbb{Q}$ je Galoisovo rozšíření s komutativní Galoisovou grupou.

Důsledek. *Každé podtěleso K libovolného kruhového tělesa je abelovské.*

Poznámka. Následující hluboká a slavná věta Kroneckera a Webera ukazuje, že je tomu i naopak:

Věta (Kronecker–Weber). *Každé abelovské těleso K je podtělesem vhodného kruhového tělesa, tj. existuje $n \in \mathbb{N}$ tak, že $K \subseteq \mathbb{Q}(\zeta_n)$.*

Jednoduché grupy

Definice. Grupa $(G, \cdot)$ se nazývá jednoduchá, jestliže není triviální a jediné její normální podgrupy jsou sama G a triviální podgrupa $\{1\}$.

Jednoduché grupy

Definice. Grupa $(G, \cdot)$ se nazývá jednoduchá, jestliže není triviální a jediné její normální podgrupy jsou sama G a triviální podgrupa $\{1\}$.

Příklad. Komutativní grupa je jednoduchá, právě když je konečná cyklická prvočíselného řádu.

Jednoduché grupy

Definice. Grupa $(G, \cdot)$ se nazývá jednoduchá, jestliže není triviální a jediné její normální podgrupy jsou sama G a triviální podgrupa $\{1\}$.

Příklad. Komutativní grupa je jednoduchá, právě když je konečná cyklická prvočíselného řádu.

Příklad. Grupa $\mathbb{A}_4$ není jednoduchá, protože má normální podgrupu $V_4 = \{\mathrm{id}, (1,2)\circ(3,4), (1,3)\circ(2,4), (1,4)\circ(2,3)\}$. Všechny prvky grupy $\mathbb{A}_4$, které nepatří do V_4, totiž mají řád 3, a proto $\mathbb{A}_4$ má jedinou 2-Sylowskou podgrupu, která je proto normální.

Jednoduché grupy

Definice. Grupa $(G, \cdot)$ se nazývá jednoduchá, jestliže není triviální a jediné její normální podgrupy jsou sama G a triviální podgrupa $\{1\}$.

Příklad. Komutativní grupa je jednoduchá, právě když je konečná cyklická prvočíselného řádu.

Příklad. Grupa $\mathbb{A}_4$ není jednoduchá, protože má normální podgrupu $V_4 = \{\mathrm{id}, (1,2)\circ(3,4), (1,3)\circ(2,4), (1,4)\circ(2,3)\}$. Všechny prvky grupy $\mathbb{A}_4$, které nepatří do V_4, totiž mají řád 3, a proto $\mathbb{A}_4$ má jedinou 2-Sylowskou podgrupu, která je proto normální.

Příklad. Pro každé $n \geq 5$ platí, že $\mathbb{A}_n$ je jednoduchá grupa a že jedinými normálními podgrupami grupy $\mathbb{S}_n$ jsou $\mathbb{S}_n$, $\mathbb{A}_n$ a $\{\mathrm{id}\}$ (důkaz není obtížný, jen poněkud pracný).

Normální, subnormální a kompoziční řada podgrup

Definice. Nechť $(G, \cdot)$ je konečná grupa. Řada podgrup $G = H_0 \geq H_1 \geq H_2 \geq \cdots \geq H_k = \{1\}$ grupy G se nazývá normální (resp. subnormální), jestliže pro každé $i = 1, \ldots, k$ platí $H_i \trianglelefteq G$ (resp. $H_i \trianglelefteq H_{i-1}$).

Normální, subnormální a kompoziční řada podgrup

Definice. Nechť $(G, \cdot)$ je konečná grupa. Řada podgrup $G = H_0 \geq H_1 \geq H_2 \geq \cdots \geq H_k = \{1\}$ grupy G se nazývá normální (resp. subnormální), jestliže pro každé $i = 1, \ldots, k$ platí $H_i \trianglelefteq G$ (resp. $H_i \trianglelefteq H_{i-1}$). Faktorgrupy H_{i-1}/H_i se nazývají faktory této řady, číslo k délka této řady.

Normální, subnormální a kompoziční řada podgrup

Definice. Nechť $(G, \cdot)$ je konečná grupa. Řada podgrup $G = H_0 \geq H_1 \geq H_2 \geq \cdots \geq H_k = \{1\}$ grupy G se nazývá normální (resp. subnormální), jestliže pro každé $i = 1, \ldots, k$ platí $H_i \trianglelefteq G$ (resp. $H_i \trianglelefteq H_{i-1}$). Faktorgrupy H_{i-1}/H_i se nazývají faktory této řady, číslo k délka této řady. Tato řada se nazývá kompoziční, jestliže je subnormální a všechny její faktory jsou jednoduché grupy.

Normální, subnormální a kompoziční řada podgrup

Definice. Nechť $(G, \cdot)$ je konečná grupa. Řada podgrup $G = H_0 \geq H_1 \geq H_2 \geq \cdots \geq H_k = \{1\}$ grupy G se nazývá normální (resp. subnormální), jestliže pro každé $i = 1, \ldots, k$ platí $H_i \trianglelefteq G$ (resp. $H_i \trianglelefteq H_{i-1}$). Faktorgrupy H_{i-1}/H_i se nazývají faktory této řady, číslo k délka této řady. Tato řada se nazývá kompoziční, jestliže je subnormální a všechny její faktory jsou jednoduché grupy.

Příklad. Grupa $\mathbb{S}_3$ má kompoziční řadu $\mathbb{S}_3 \geq \mathbb{A}_3 \geq \{\mathrm{id}\}$.

Normální, subnormální a kompoziční řada podgrup

Definice. Nechť $(G, \cdot)$ je konečná grupa. Řada podgrup $G = H_0 \geq H_1 \geq H_2 \geq \cdots \geq H_k = \{1\}$ grupy G se nazývá normální (resp. subnormální), jestliže pro každé $i = 1, \ldots, k$ platí $H_i \trianglelefteq G$ (resp. $H_i \trianglelefteq H_{i-1}$). Faktorgrupy H_{i-1}/H_i se nazývají faktory této řady, číslo k délka této řady. Tato řada se nazývá kompoziční, jestliže je subnormální a všechny její faktory jsou jednoduché grupy.

Příklad. Grupa $\mathbb{S}_3$ má kompoziční řadu $\mathbb{S}_3 \geq \mathbb{A}_3 \geq \{\mathrm{id}\}$. Grupa $\mathbb{Z}_6$ má kompoziční řady $\mathbb{Z}_6 \geq \langle [2]_6 \rangle \geq \{[0]_6\}$ a $\mathbb{Z}_6 \geq \langle [3]_6 \rangle \geq \{[0]_6\}$.

Normální, subnormální a kompoziční řada podgrup

Definice. Nechť $(G, \cdot)$ je konečná grupa. Řada podgrup $G = H_0 \geq H_1 \geq H_2 \geq \cdots \geq H_k = \{1\}$ grupy G se nazývá normální (resp. subnormální), jestliže pro každé $i = 1, \ldots, k$ platí $H_i \trianglelefteq G$ (resp. $H_i \trianglelefteq H_{i-1}$). Faktorgrupy H_{i-1}/H_i se nazývají faktory této řady, číslo k délka této řady. Tato řada se nazývá kompoziční, jestliže je subnormální a všechny její faktory jsou jednoduché grupy.

Příklad. Grupa $\mathbb{S}_3$ má kompoziční řadu $\mathbb{S}_3 \geq \mathbb{A}_3 \geq \{\mathrm{id}\}$. Grupa $\mathbb{Z}_6$ má kompoziční řady $\mathbb{Z}_6 \geq \langle [2]_6 \rangle \geq \{[0]_6\}$ a $\mathbb{Z}_6 \geq \langle [3]_6 \rangle \geq \{[0]_6\}$.

Poznámka. Je zřejmé, že každá konečná grupa má alespoň jednu kompoziční řadu.

Normální, subnormální a kompoziční řada podgrup

Definice. Nechť $(G, \cdot)$ je konečná grupa. Řada podgrup $G = H_0 \geq H_1 \geq H_2 \geq \cdots \geq H_k = \{1\}$ grupy G se nazývá normální (resp. subnormální), jestliže pro každé $i = 1, \ldots, k$ platí $H_i \trianglelefteq G$ (resp. $H_i \trianglelefteq H_{i-1}$). Faktorgrupy H_{i-1}/H_i se nazývají faktory této řady, číslo k délka této řady. Tato řada se nazývá kompoziční, jestliže je subnormální a všechny její faktory jsou jednoduché grupy.

Příklad. Grupa $\mathbb{S}_3$ má kompoziční řadu $\mathbb{S}_3 \geq \mathbb{A}_3 \geq \{\mathrm{id}\}$. Grupa $\mathbb{Z}_6$ má kompoziční řady $\mathbb{Z}_6 \geq \langle [2]_6 \rangle \geq \{[0]_6\}$ a $\mathbb{Z}_6 \geq \langle [3]_6 \rangle \geq \{[0]_6\}$.

Poznámka. Je zřejmé, že každá konečná grupa má alespoň jednu kompoziční řadu. Dvě kompoziční řady téže grupy se nazývají ekvivalentní, mají-li stejnou délku a existuje-li permutace indexů, při níž odpovídající faktory jsou izomorfní grupy.

Normální, subnormální a kompoziční řada podgrup

Definice. Nechť $(G, \cdot)$ je konečná grupa. Řada podgrup $G = H_0 \geq H_1 \geq H_2 \geq \cdots \geq H_k = \{1\}$ grupy G se nazývá normální (resp. subnormální), jestliže pro každé $i = 1, \ldots, k$ platí $H_i \trianglelefteq G$ (resp. $H_i \trianglelefteq H_{i-1}$). Faktorgrupy H_{i-1}/H_i se nazývají faktory této řady, číslo k délka této řady. Tato řada se nazývá kompoziční, jestliže je subnormální a všechny její faktory jsou jednoduché grupy.

Příklad. Grupa $\mathbb{S}_3$ má kompoziční řadu $\mathbb{S}_3 \geq \mathbb{A}_3 \geq \{\mathrm{id}\}$. Grupa $\mathbb{Z}_6$ má kompoziční řady $\mathbb{Z}_6 \geq \langle [2]_6 \rangle \geq \{[0]_6\}$ a $\mathbb{Z}_6 \geq \langle [3]_6 \rangle \geq \{[0]_6\}$.

Poznámka. Je zřejmé, že každá konečná grupa má alespoň jednu kompoziční řadu. Dvě kompoziční řady téže grupy se nazývají ekvivalentní, mají-li stejnou délku a existuje-li permutace indexů, při níž odpovídající faktory jsou izomorfní grupy. Uveďme alespoň bez důkazu větu Jordan–Hölder: Každé dvě kompoziční řady libovolné konečné grupy G jsou ekvivalentní.

Normální, subnormální a kompoziční řada podgrup

Definice. Nechť $(G, \cdot)$ je konečná grupa. Řada podgrup $G = H_0 \geq H_1 \geq H_2 \geq \cdots \geq H_k = \{1\}$ grupy G se nazývá normální (resp. subnormální), jestliže pro každé $i = 1, \ldots, k$ platí $H_i \trianglelefteq G$ (resp. $H_i \trianglelefteq H_{i-1}$). Faktorgrupy H_{i-1}/H_i se nazývají faktory této řady, číslo k délka této řady. Tato řada se nazývá kompoziční, jestliže je subnormální a všechny její faktory jsou jednoduché grupy.

Příklad. Grupa $\mathbb{S}_3$ má kompoziční řadu $\mathbb{S}_3 \geq \mathbb{A}_3 \geq \{\mathrm{id}\}$. Grupa $\mathbb{Z}_6$ má kompoziční řady $\mathbb{Z}_6 \geq \langle [2]_6 \rangle \geq \{[0]_6\}$ a $\mathbb{Z}_6 \geq \langle [3]_6 \rangle \geq \{[0]_6\}$.

Poznámka. Je zřejmé, že každá konečná grupa má alespoň jednu kompoziční řadu. Dvě kompoziční řady téže grupy se nazývají ekvivalentní, mají-li stejnou délku a existuje-li permutace indexů, při níž odpovídající faktory jsou izomorfní grupy. Uveďme alespoň bez důkazu větu Jordan–Hölder: Každé dvě kompoziční řady libovolné konečné grupy G jsou ekvivalentní. Lze tedy hovořit o kompozičních faktorech dané konečné grupy (jsou určeny jednoznačně až na izomorfismus).

Řešitelné grupy

Definice. Konečná grupa $(G, \cdot)$ se nazývá řešitelná, jestliže existuje její subnormální řada s komutativními faktory.

Řešitelné grupy

Definice. Konečná grupa $(G, \cdot)$ se nazývá řešitelná, jestliže existuje její subnormální řada s komutativními faktory.

Příklad. Grupa $\mathbb{S}_4$ je řešitelná, protože má subnormální řadu $\mathbb{S}_4 \geq \mathbb{A}_4 \geq V_4 \geq \{\mathrm{id}\}$ s faktory $\mathbb{S}_4/\mathbb{A}_4 \cong \mathbb{Z}_2$, $\mathbb{A}_4/V_4 \cong \mathbb{Z}_3$, $V_4/\{\mathrm{id}\} \cong V_4$.

Řešitelné grupy

Definice. Konečná grupa $(G, \cdot)$ se nazývá řešitelná, jestliže existuje její subnormální řada s komutativními faktory.

Příklad. Grupa $\mathbb{S}_4$ je řešitelná, protože má subnormální řadu $\mathbb{S}_4 \geq \mathbb{A}_4 \geq V_4 \geq \{\mathrm{id}\}$ s faktory $\mathbb{S}_4/\mathbb{A}_4 \cong \mathbb{Z}_2$, $\mathbb{A}_4/V_4 \cong \mathbb{Z}_3$, $V_4/\{\mathrm{id}\} \cong V_4$.

Příklad. Pro každé $n \geq 5$ platí, že ani $\mathbb{S}_n$ ani $\mathbb{A}_n$ nejsou řešitelné grupy.

Řešitelné grupy

Definice. Konečná grupa $(G, \cdot)$ se nazývá řešitelná, jestliže existuje její subnormální řada s komutativními faktory.

Příklad. Grupa $\mathbb{S}_4$ je řešitelná, protože má subnormální řadu $\mathbb{S}_4 \geq \mathbb{A}_4 \geq V_4 \geq \{\mathrm{id}\}$ s faktory $\mathbb{S}_4/\mathbb{A}_4 \cong \mathbb{Z}_2$, $\mathbb{A}_4/V_4 \cong \mathbb{Z}_3$, $V_4/\{\mathrm{id}\} \cong V_4$.

Příklad. Pro každé $n \geq 5$ platí, že ani $\mathbb{S}_n$ ani $\mathbb{A}_n$ nejsou řešitelné grupy. Jediná subnormální řada grupy $\mathbb{A}_n$ je $\mathbb{A}_n \geq \{\mathrm{id}\}$, protože grupa $\mathbb{A}_n$ je jednoduchá.

Řešitelné grupy

Definice. Konečná grupa $(G, \cdot)$ se nazývá řešitelná, jestliže existuje její subnormální řada s komutativními faktory.

Příklad. Grupa $\mathbb{S}_4$ je řešitelná, protože má subnormální řadu $\mathbb{S}_4 \geq \mathbb{A}_4 \geq V_4 \geq \{\mathrm{id}\}$ s faktory $\mathbb{S}_4/\mathbb{A}_4 \cong \mathbb{Z}_2$, $\mathbb{A}_4/V_4 \cong \mathbb{Z}_3$, $V_4/\{\mathrm{id}\} \cong V_4$.

Příklad. Pro každé $n \geq 5$ platí, že ani $\mathbb{S}_n$ ani $\mathbb{A}_n$ nejsou řešitelné grupy. Jediná subnormální řada grupy $\mathbb{A}_n$ je $\mathbb{A}_n \geq \{\mathrm{id}\}$, protože grupa $\mathbb{A}_n$ je jednoduchá. Podobně subnormální řady grupy $\mathbb{S}_n$ jsou pouze dvě, totiž $\mathbb{S}_n \geq \{\mathrm{id}\}$ a $\mathbb{S}_n \geq \mathbb{A}_n \geq \{\mathrm{id}\}$.

Řešitelné grupy

Definice. Konečná grupa $(G, \cdot)$ se nazývá řešitelná, jestliže existuje její subnormální řada s komutativními faktory.

Příklad. Grupa $\mathbb{S}_4$ je řešitelná, protože má subnormální řadu $\mathbb{S}_4 \geq \mathbb{A}_4 \geq V_4 \geq \{\mathrm{id}\}$ s faktory $\mathbb{S}_4/\mathbb{A}_4 \cong \mathbb{Z}_2$, $\mathbb{A}_4/V_4 \cong \mathbb{Z}_3$, $V_4/\{\mathrm{id}\} \cong V_4$.

Příklad. Pro každé $n \geq 5$ platí, že ani $\mathbb{S}_n$ ani $\mathbb{A}_n$ nejsou řešitelné grupy. Jediná subnormální řada grupy $\mathbb{A}_n$ je $\mathbb{A}_n \geq \{\mathrm{id}\}$, protože grupa $\mathbb{A}_n$ je jednoduchá. Podobně subnormální řady grupy $\mathbb{S}_n$ jsou pouze dvě, totiž $\mathbb{S}_n \geq \{\mathrm{id}\}$ a $\mathbb{S}_n \geq \mathbb{A}_n \geq \{\mathrm{id}\}$.

Poznámka. Lze dokázat, že konečná grupa je řešitelná, právě když všechny její kompoziční faktory jsou prvočíselného řádu.

Jak zjistit, zda je daná grupa řešitelná?

Věta 20. *Libovolná podgrupa řešitelné grupy je řešitelná.*

Jak zjistit, zda je daná grupa řešitelná?

Věta 20. *Libovolná podgrupa řešitelné grupy je řešitelná.*

Věta 21. *Nechť G je konečná grupa, H její normální podgrupa. Pak platí: grupa G je řešitelná, právě když jsou H i G/H řešitelné grupy.*

Jak zjistit, zda je daná grupa řešitelná?

Věta 20. *Libovolná podgrupa řešitelné grupy je řešitelná.*

Věta 21. *Nechť G je konečná grupa, H její normální podgrupa. Pak platí: grupa G je řešitelná, právě když jsou H i G/H řešitelné grupy.*

Poznámka. Otázka, které konečné grupy jsou řešitelné, vedla k velkému rozvoji teorie grup, zmiňme následující hluboké výsledky:

- *Věta (Burnside).* *Je-li řád $|G|$ grupy G dělitelný nejvýše dvěma prvočísly, je G řešitelná.*

Jak zjistit, zda je daná grupa řešitelná?

Věta 20. *Libovolná podgrupa řešitelné grupy je řešitelná.*

Věta 21. *Nechť G je konečná grupa, H její normální podgrupa. Pak platí: grupa G je řešitelná, právě když jsou H i G/H řešitelné grupy.*

Poznámka. Otázka, které konečné grupy jsou řešitelné, vedla k velkému rozvoji teorie grup, zmiňme následující hluboké výsledky:

- *Věta (Burnside).* *Je-li řád $|G|$ grupy G dělitelný nejvýše dvěma prvočísly, je G řešitelná.*
- *Věta (Feit–Thompson).* *Je-li řád $|G|$ grupy G liché číslo, je G řešitelná.*

Jak zjistit, zda je daná grupa řešitelná?

Věta 20. *Libovolná podgrupa řešitelné grupy je řešitelná.*

Věta 21. *Nechť G je konečná grupa, H její normální podgrupa. Pak platí: grupa G je řešitelná, právě když jsou H i G/H řešitelné grupy.*

Poznámka. Otázka, které konečné grupy jsou řešitelné, vedla k velkému rozvoji teorie grup, zmiňme následující hluboké výsledky:

- *Věta (Burnside).* *Je-li řád $|G|$ grupy G dělitelný nejvýše dvěma prvočísly, je G řešitelná.*
- *Věta (Feit–Thompson).* *Je-li řád $|G|$ grupy G liché číslo, je G řešitelná.*
- *Věta (Thompson).* *Grupa G není řešitelná, právě když existují prvky $x, y \in G$, $x \neq 1 \neq y$, takové, že řády prvků x, y a xy jsou po dvou nesoudělné.*

Jak zjistit, zda je daná grupa řešitelná?

Věta 20. *Libovolná podgrupa řešitelné grupy je řešitelná.*

Věta 21. *Nechť G je konečná grupa, H její normální podgrupa. Pak platí: grupa G je řešitelná, právě když jsou H i G/H řešitelné grupy.*

Poznámka. Otázka, které konečné grupy jsou řešitelné, vedla k velkému rozvoji teorie grup, zmiňme následující hluboké výsledky:

- *Věta (Burnside).* *Je-li řád $|G|$ grupy G dělitelný nejvýše dvěma prvočísly, je G řešitelná.*
- *Věta (Feit–Thompson).* *Je-li řád $|G|$ grupy G liché číslo, je G řešitelná.*
- *Věta (Thompson).* *Grupa G není řešitelná, právě když existují prvky $x, y \in G$, $x \neq 1 \neq y$, takové, že řády prvků x, y a xy jsou po dvou nesoudělné.*

Příklad. V grupě $\mathbb{A}_n$ (případně $\mathbb{S}_n$), kde $n \geq 5$, zvolme $x = (12345)$, $y = (12)(34)$, pak $xy = (135)$, a tedy prvky x, y a xy mají řády 5, 2, 3.

Jak zjistit, zda je daná grupa řešitelná?

Věta 20. *Libovolná podgrupa řešitelné grupy je řešitelná.*

Věta 21. *Nechť G je konečná grupa, H její normální podgrupa. Pak platí: grupa G je řešitelná, právě když jsou H i G/H řešitelné grupy.*

Poznámka. Otázka, které konečné grupy jsou řešitelné, vedla k velkému rozvoji teorie grup, zmiňme následující hluboké výsledky:

- *Věta (Burnside).* *Je-li řád $|G|$ grupy G dělitelný nejvýše dvěma prvočísly, je G řešitelná.*
- *Věta (Feit–Thompson).* *Je-li řád $|G|$ grupy G liché číslo, je G řešitelná.*
- *Věta (Thompson).* *Grupa G není řešitelná, právě když existují prvky $x, y \in G$, $x \neq 1 \neq y$, takové, že řády prvků x, y a xy jsou po dvou nesoudělné.*

Příklad. V grupě $\mathbb{A}_n$ (případně $\mathbb{S}_n$), kde $n \geq 5$, zvolme $x = (12345)$, $y = (12)(34)$, pak $xy = (135)$, a tedy prvky x, y a xy mají řády 5, 2, 3. Proto z Thompsonovy věty plyne, že grupy $\mathbb{A}_n$ ani $\mathbb{S}_n$ nejsou řešitelné.

Radikálová rozšíření, čísla vyjádřitelná v radikálech

Definice. Rozšíření těles $F \subseteq K$ se nazývá jednoduché radikálové rozšíření, jestliže existují $\alpha \in K$, $n \in \mathbb{N}$ tak, že $K = F(\alpha)$ a $\alpha^n \in F$.

Radikálová rozšíření, čísla vyjádřitelná v radikálech

Definice. Rozšíření těles $F \subseteq K$ se nazývá jednoduché radikálové rozšíření, jestliže existují $\alpha \in K$, $n \in \mathbb{N}$ tak, že $K = F(\alpha)$ a $\alpha^n \in F$.

Příklad. Pro libovolná $k, m \in \mathbb{N}$ je rozšíření těles $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[k]{m})$ jednoduché radikálové rozšíření.

Radikálová rozšíření, čísla vyjádřitelná v radikálech

Definice. Rozšíření těles $F \subseteq K$ se nazývá jednoduché radikálové rozšíření, jestliže existují $\alpha \in K$, $n \in \mathbb{N}$ tak, že $K = F(\alpha)$ a $\alpha^n \in F$.

Příklad. Pro libovolná $k, m \in \mathbb{N}$ je rozšíření těles $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[k]{m})$ jednoduché radikálové rozšíření. Podobně $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_m)$ je jednoduché radikálové rozšíření.

Radikálová rozšíření, čísla vyjádřitelná v radikálech

Definice. Rozšíření těles $F \subseteq K$ se nazývá jednoduché radikálové rozšíření, jestliže existují $\alpha \in K$, $n \in \mathbb{N}$ tak, že $K = F(\alpha)$ a $\alpha^n \in F$.

Příklad. Pro libovolná $k, m \in \mathbb{N}$ je rozšíření těles $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[k]{m})$ jednoduché radikálové rozšíření. Podobně $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_m)$ je jednoduché radikálové rozšíření.

Definice. Rozšíření těles $F \subseteq K$ se nazývá radikálové rozšíření, jestliže existují tělesa $F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_m = K$ tak, že $F_{i-1} \subseteq F_i$ je jednoduché radikálové rozšíření pro každé $i = 1, 2, \ldots, m$.

Radikálová rozšíření, čísla vyjádřitelná v radikálech

Definice. Rozšíření těles $F \subseteq K$ se nazývá jednoduché radikálové rozšíření, jestliže existují $\alpha \in K$, $n \in \mathbb{N}$ tak, že $K = F(\alpha)$ a $\alpha^n \in F$.

Příklad. Pro libovolná $k, m \in \mathbb{N}$ je rozšíření těles $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[k]{m})$ jednoduché radikálové rozšíření. Podobně $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_m)$ je jednoduché radikálové rozšíření.

Definice. Rozšíření těles $F \subseteq K$ se nazývá radikálové rozšíření, jestliže existují tělesa $F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_m = K$ tak, že $F_{i-1} \subseteq F_i$ je jednoduché radikálové rozšíření pro každé $i = 1, 2, \ldots, m$.

Definice. Číslo $\alpha \in \mathbb{C}$ se nazývá vyjádřitelné v radikálech, jestliže existuje radikálové rozšíření tělesa $\mathbb{Q}$ obsahující α.

Radikálová rozšíření, čísla vyjádřitelná v radikálech

Definice. Rozšíření těles $F \subseteq K$ se nazývá jednoduché radikálové rozšíření, jestliže existují $\alpha \in K$, $n \in \mathbb{N}$ tak, že $K = F(\alpha)$ a $\alpha^n \in F$.

Příklad. Pro libovolná $k, m \in \mathbb{N}$ je rozšíření těles $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[k]{m})$ jednoduché radikálové rozšíření. Podobně $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_m)$ je jednoduché radikálové rozšíření.

Definice. Rozšíření těles $F \subseteq K$ se nazývá radikálové rozšíření, jestliže existují tělesa $F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_m = K$ tak, že $F_{i-1} \subseteq F_i$ je jednoduché radikálové rozšíření pro každé $i = 1, 2, \ldots, m$.

Definice. Číslo $\alpha \in \mathbb{C}$ se nazývá vyjádřitelné v radikálech, jestliže existuje radikálové rozšíření tělesa $\mathbb{Q}$ obsahující α.

Poznámka. Každé komplexní číslo, které lze napsat jako algebraický výraz obsahující racionální čísla, operace sčítání, odčítání, násobení, dělení a n-té odmocniny, kde $n \in \mathbb{N}$, je vyjádřitelné v radikálech.

Řešitelné polynomy

Definice. Nekonstantní polynom $f \in \mathbb{Q}[x]$ se nazývá řešitelný, jestliže je každý kořen polynomu f vyjádřitelný v radikálech.

Řešitelné polynomy

Definice. Nekonstantní polynom $f \in \mathbb{Q}[x]$ se nazývá řešitelný, jestliže je každý kořen polynomu f vyjádřitelný v radikálech.

Poznámka. Řešitelný je každý polynom $f \in \mathbb{Q}[x]$, který je kvadratický (vzpomeňme na středoškolský vzorec), kubický (Cardanovy vzorce) anebo stupně 4 (jeho kořeny lze vyjádřit pomocí kořenů jeho kubické resolventy).

Řešitelné polynomy

Definice. Nekonstantní polynom $f \in \mathbb{Q}[x]$ se nazývá řešitelný, jestliže je každý kořen polynomu f vyjádřitelný v radikálech.

Poznámka. Řešitelný je každý polynom $f \in \mathbb{Q}[x]$, který je kvadratický (vzpomeňme na středoškolský vzorec), kubický (Cardanovy vzorce) anebo stupně 4 (jeho kořeny lze vyjádřit pomocí kořenů jeho kubické resolventy). Proč pro polynomy stupně 5 neexistuje univerzální vzorec na výpočet jejich kořenů, vysvětlil až Galois následující větou (kterou uvedeme bez důkazu).

Řešitelné polynomy

Definice. Nekonstantní polynom $f \in \mathbb{Q}[x]$ se nazývá řešitelný, jestliže je každý kořen polynomu f vyjádřitelný v radikálech.

Poznámka. Řešitelný je každý polynom $f \in \mathbb{Q}[x]$, který je kvadratický (vzpomeňme na středoškolský vzorec), kubický (Cardanovy vzorce) anebo stupně 4 (jeho kořeny lze vyjádřit pomocí kořenů jeho kubické resolventy). Proč pro polynomy stupně 5 neexistuje univerzální vzorec na výpočet jejich kořenů, vysvětlil až Galois následující větou (kterou uvedeme bez důkazu). Připomeňme, že Galoisova grupa polynomu $f \in \mathbb{Q}[x]$ nad $\mathbb{Q}$ je $\mathrm{Gal}(K/\mathbb{Q})$, kde K je rozkladové těleso polynomu f nad $\mathbb{Q}$.

Řešitelné polynomy

Definice. Nekonstantní polynom $f \in \mathbb{Q}[x]$ se nazývá řešitelný, jestliže je každý kořen polynomu f vyjádřitelný v radikálech.

Poznámka. Řešitelný je každý polynom $f \in \mathbb{Q}[x]$, který je kvadratický (vzpomeňme na středoškolský vzorec), kubický (Cardanovy vzorce) anebo stupně 4 (jeho kořeny lze vyjádřit pomocí kořenů jeho kubické resolventy). Proč pro polynomy stupně 5 neexistuje univerzální vzorec na výpočet jejich kořenů, vysvětlil až Galois následující větou (kterou uvedeme bez důkazu). Připomeňme, že Galoisova grupa polynomu $f \in \mathbb{Q}[x]$ nad $\mathbb{Q}$ je $\mathrm{Gal}(K/\mathbb{Q})$, kde K je rozkladové těleso polynomu f nad $\mathbb{Q}$.

Věta (Galois). Nechť $f \in \mathbb{Q}[x]$ je libovolný nekonstantní polynom. Pak platí: polynom f je řešitelný, právě když Galoisova grupa polynomu f nad $\mathbb{Q}$ je řešitelná.

Řešitelné polynomy

Definice. Nekonstantní polynom $f \in \mathbb{Q}[x]$ se nazývá řešitelný, jestliže je každý kořen polynomu f vyjádřitelný v radikálech.

Poznámka. Řešitelný je každý polynom $f \in \mathbb{Q}[x]$, který je kvadratický (vzpomeňme na středoškolský vzorec), kubický (Cardanovy vzorce) anebo stupně 4 (jeho kořeny lze vyjádřit pomocí kořenů jeho kubické resolventy). Proč pro polynomy stupně 5 neexistuje univerzální vzorec na výpočet jejich kořenů, vysvětlil až Galois následující větou (kterou uvedeme bez důkazu). Připomeňme, že Galoisova grupa polynomu $f \in \mathbb{Q}[x]$ nad $\mathbb{Q}$ je $\mathrm{Gal}(K/\mathbb{Q})$, kde K je rozkladové těleso polynomu f nad $\mathbb{Q}$.

Věta (Galois). Nechť $f \in \mathbb{Q}[x]$ je libovolný nekonstantní polynom. Pak platí: polynom f je řešitelný, právě když Galoisova grupa polynomu f nad $\mathbb{Q}$ je řešitelná.

Poznámka. Galoisova věta ukazuje, že grupy symetrií hrají v matematice významnou úlohu: to, zda je daný polynom řešitelný, nepoznáme přímo na něm, ale poznáme to na grupě symetrií jeho rozkladového tělesa.

Polynom, který není řešitelný

Příklad. Nechť $f = x^5 - 6x + 3 \in \mathbb{Q}[x]$ a K je rozkladové těleso polynomu f nad $\mathbb{Q}$.

Polynom, který není řešitelný

Příklad. Nechť $f = x^5 - 6x + 3 \in \mathbb{Q}[x]$ a K je rozkladové těleso polynomu f nad $\mathbb{Q}$. Podle Eisensteinova kriteria je f ireducibilní nad $\mathbb{Q}$, a proto pro libovolný kořen α polynomu f platí $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$, a tedy $5 \mid [K : \mathbb{Q}]$.

Polynom, který není řešitelný

Příklad. Nechť $f = x^5 - 6x + 3 \in \mathbb{Q}[x]$ a K je rozkladové těleso polynomu f nad $\mathbb{Q}$. Podle Eisensteinova kriteria je f ireducibilní nad $\mathbb{Q}$, a proto pro libovolný kořen α polynomu f platí $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$, a tedy $5 \mid [K : \mathbb{Q}]$. Protože $f(-2) = -17$, $f(0) = 3$, $f(1) = -2$ a $f(2) = 23$, má f alespoň tři reálné kořeny.

Polynom, který není řešitelný

Příklad. Nechť $f = x^5 - 6x + 3 \in \mathbb{Q}[x]$ a K je rozkladové těleso polynomu f nad $\mathbb{Q}$. Podle Eisensteinova kriteria je f ireducibilní nad $\mathbb{Q}$, a proto pro libovolný kořen α polynomu f platí $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$, a tedy $5 \mid [K : \mathbb{Q}]$. Protože $f(-2) = -17$, $f(0) = 3$, $f(1) = -2$ a $f(2) = 23$, má f alespoň tři reálné kořeny. Protože $f' = 5x^4 - 6$, je f rostoucí na intervalech $(-\infty, -\sqrt[4]{\frac{6}{5}})$ a $(\sqrt[4]{\frac{6}{5}}, \infty)$ a je klesající na intervalu $(-\sqrt[4]{\frac{6}{5}}, \sqrt[4]{\frac{6}{5}})$, a tedy f má právě tři reálné kořeny a jednu dvojici komplexně sdružených kořenů.

Polynom, který není řešitelný

Příklad. Nechť $f = x^5 - 6x + 3 \in \mathbb{Q}[x]$ a K je rozkladové těleso polynomu f nad $\mathbb{Q}$. Podle Eisensteinova kriteria je f ireducibilní nad $\mathbb{Q}$, a proto pro libovolný kořen α polynomu f platí $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$, a tedy $5 \mid [K : \mathbb{Q}]$. Protože $f(-2) = -17$, $f(0) = 3$, $f(1) = -2$ a $f(2) = 23$, má f alespoň tři reálné kořeny. Protože $f' = 5x^4 - 6$, je f rostoucí na intervalech $(-\infty, -\sqrt[4]{\frac{6}{5}})$ a $(\sqrt[4]{\frac{6}{5}}, \infty)$ a je klesající na intervalu $(-\sqrt[4]{\frac{6}{5}}, \sqrt[4]{\frac{6}{5}})$, a tedy f má právě tři reálné kořeny a jednu dvojici komplexně sdružených kořenů. Z příkladu za větou 10 víme, že $\mathrm{Gal}(K/\mathbb{Q})$ je izomorfní s podgrupou grupy permutací kořenů polynomu f, tedy grupy $\mathbb{S}_5$.

Polynom, který není řešitelný

Příklad. Nechť $f = x^5 - 6x + 3 \in \mathbb{Q}[x]$ a K je rozkladové těleso polynomu f nad $\mathbb{Q}$. Podle Eisensteinova kriteria je f ireducibilní nad $\mathbb{Q}$, a proto pro libovolný kořen α polynomu f platí $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$, a tedy $5 \mid [K : \mathbb{Q}]$. Protože $f(-2) = -17$, $f(0) = 3$, $f(1) = -2$ a $f(2) = 23$, má f alespoň tři reálné kořeny. Protože $f' = 5x^4 - 6$, je f rostoucí na intervalech $(-\infty, -\sqrt[4]{\frac{6}{5}})$ a $(\sqrt[4]{\frac{6}{5}}, \infty)$ a je klesající na intervalu $(-\sqrt[4]{\frac{6}{5}}, \sqrt[4]{\frac{6}{5}})$, a tedy f má právě tři reálné kořeny a jednu dvojici komplexně sdružených kořenů. Z příkladu za větou 10 víme, že $\mathrm{Gal}(K/\mathbb{Q})$ je izomorfní s podgrupou grupy permutací kořenů polynomu f, tedy grupy $\mathbb{S}_5$. Protože zúžení komplexní konjugovanosti na K ponechá na místě právě ty kořeny, které jsou reálné, obsahuje tato podgrupa transpozici.

Polynom, který není řešitelný

Příklad. Nechť $f = x^5 - 6x + 3 \in \mathbb{Q}[x]$ a K je rozkladové těleso polynomu f nad $\mathbb{Q}$. Podle Eisensteinova kriteria je f ireducibilní nad $\mathbb{Q}$, a proto pro libovolný kořen α polynomu f platí $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$, a tedy $5 \mid [K : \mathbb{Q}]$. Protože $f(-2) = -17$, $f(0) = 3$, $f(1) = -2$ a $f(2) = 23$, má f alespoň tři reálné kořeny. Protože $f' = 5x^4 - 6$, je f rostoucí na intervalech $(-\infty, -\sqrt[4]{\frac{6}{5}})$ a $(\sqrt[4]{\frac{6}{5}}, \infty)$ a je klesající na intervalu $(-\sqrt[4]{\frac{6}{5}}, \sqrt[4]{\frac{6}{5}})$, a tedy f má právě tři reálné kořeny a jednu dvojici komplexně sdružených kořenů. Z příkladu za větou 10 víme, že $\mathrm{Gal}(K/\mathbb{Q})$ je izomorfní s podgrupou grupy permutací kořenů polynomu f, tedy grupy $\mathbb{S}_5$. Protože zúžení komplexní konjugovanosti na K ponechá na místě právě ty kořeny, které jsou reálné, obsahuje tato podgrupa transpozici. Protože $5 \mid [K : \mathbb{Q}]$, podle Cauchyovy věty obsahuje tato podgrupa prvek prvek řádu 5.

Polynom, který není řešitelný

Příklad. Nechť $f = x^5 - 6x + 3 \in \mathbb{Q}[x]$ a K je rozkladové těleso polynomu f nad $\mathbb{Q}$. Podle Eisensteinova kriteria je f ireducibilní nad $\mathbb{Q}$, a proto pro libovolný kořen α polynomu f platí $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$, a tedy $5 \mid [K : \mathbb{Q}]$. Protože $f(-2) = -17$, $f(0) = 3$, $f(1) = -2$ a $f(2) = 23$, má f alespoň tři reálné kořeny. Protože $f' = 5x^4 - 6$, je f rostoucí na intervalech $(-\infty, -\sqrt[4]{\frac{6}{5}})$ a $(\sqrt[4]{\frac{6}{5}}, \infty)$ a je klesající na intervalu $(-\sqrt[4]{\frac{6}{5}}, \sqrt[4]{\frac{6}{5}})$, a tedy f má právě tři reálné kořeny a jednu dvojici komplexně sdružených kořenů. Z příkladu za větou 10 víme, že $\mathrm{Gal}(K/\mathbb{Q})$ je izomorfní s podgrupou grupy permutací kořenů polynomu f, tedy grupy $\mathbb{S}_5$. Protože zúžení komplexní konjugovanosti na K ponechá na místě právě ty kořeny, které jsou reálné, obsahuje tato podgrupa transpozici. Protože $5 \mid [K : \mathbb{Q}]$, podle Cauchyovy věty obsahuje tato podgrupa prvek prvek řádu 5. Je možné ukázat, že pro grupu $\mathbb{S}_5$ platí, že libovolná transpozice a libovolný prvek řádu 5 spolu generují celou grupu.

Polynom, který není řešitelný

Příklad. Nechť $f = x^5 - 6x + 3 \in \mathbb{Q}[x]$ a K je rozkladové těleso polynomu f nad $\mathbb{Q}$. Podle Eisensteinova kriteria je f ireducibilní nad $\mathbb{Q}$, a proto pro libovolný kořen α polynomu f platí $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$, a tedy $5 \mid [K : \mathbb{Q}]$. Protože $f(-2) = -17$, $f(0) = 3$, $f(1) = -2$ a $f(2) = 23$, má f alespoň tři reálné kořeny. Protože $f' = 5x^4 - 6$, je f rostoucí na intervalech $(-\infty, -\sqrt[4]{\frac{6}{5}})$ a $(\sqrt[4]{\frac{6}{5}}, \infty)$ a je klesající na intervalu $(-\sqrt[4]{\frac{6}{5}}, \sqrt[4]{\frac{6}{5}})$, a tedy f má právě tři reálné kořeny a jednu dvojici komplexně sdružených kořenů. Z příkladu za větou 10 víme, že $\mathrm{Gal}(K/\mathbb{Q})$ je izomorfní s podgrupou grupy permutací kořenů polynomu f, tedy grupy $\mathbb{S}_5$. Protože zúžení komplexní konjugovanosti na K ponechá na místě právě ty kořeny, které jsou reálné, obsahuje tato podgrupa transpozici. Protože $5 \mid [K : \mathbb{Q}]$, podle Cauchyovy věty obsahuje tato podgrupa prvek prvek řádu 5. Je možné ukázat, že pro grupu $\mathbb{S}_5$ platí, že libovolná transpozice a libovolný prvek řádu 5 spolu generují celou grupu. Proto $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{S}_5$ není řešitelná grupa, a tedy polynom f není řešitelný.

Vzorec na výpočet kořenů polynomu stupně 5 neexistuje

Poznámka. Ukázali jsme si příklad polynomu $f \in \mathbb{Q}[x]$ stupně 5, který je ireducibilní a není řešitelný.

Vzorec na výpočet kořenů polynomu stupně 5 neexistuje

Poznámka. Ukázali jsme si příklad polynomu $f \in \mathbb{Q}[x]$ stupně 5, který je ireducibilní a není řešitelný. Pro takový polynom platí, že existuje jeho kořen, který není vyjádřitelný v radikálech, a tedy jej nelze napsat jako algebraický výraz obsahující racionální čísla, operace sčítání, odčítání, násobení, dělení a odmocniny.

Vzorec na výpočet kořenů polynomu stupně 5 neexistuje

Poznámka. Ukázali jsme si příklad polynomu $f \in \mathbb{Q}[x]$ stupně 5, který je ireducibilní a není řešitelný. Pro takový polynom platí, že existuje jeho kořen, který není vyjádřitelný v radikálech, a tedy jej nelze napsat jako algebraický výraz obsahující racionální čísla, operace sčítání, odčítání, násobení, dělení a odmocniny.

Pro libovolné dva kořeny α, β polynomu f existuje podle věty 7 izomorfismus $\tau : \mathbb{Q}(\alpha) \to \mathbb{Q}(\beta)$ splňující $\tau(\alpha) = \beta$.

Vzorec na výpočet kořenů polynomu stupně 5 neexistuje

Poznámka. Ukázali jsme si příklad polynomu $f \in \mathbb{Q}[x]$ stupně 5, který je ireducibilní a není řešitelný. Pro takový polynom platí, že existuje jeho kořen, který není vyjádřitelný v radikálech, a tedy jej nelze napsat jako algebraický výraz obsahující racionální čísla, operace sčítání, odčítání, násobení, dělení a odmocniny.

Pro libovolné dva kořeny α, β polynomu f existuje podle věty 7 izomorfismus $\tau : \mathbb{Q}(\alpha) \to \mathbb{Q}(\beta)$ splňující $\tau(\alpha) = \beta$. K tomuto izomorfismu τ existuje podle věty 8 automorfismus $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ splňující $\sigma(\alpha) = \beta$. Proto žádný kořen polynomu f není vyjádřitelný v radikálech.

Vzorec na výpočet kořenů polynomu stupně 5 neexistuje

Poznámka. Ukázali jsme si příklad polynomu $f \in \mathbb{Q}[x]$ stupně 5, který je ireducibilní a není řešitelný. Pro takový polynom platí, že existuje jeho kořen, který není vyjádřitelný v radikálech, a tedy jej nelze napsat jako algebraický výraz obsahující racionální čísla, operace sčítání, odčítání, násobení, dělení a odmocniny.

Pro libovolné dva kořeny α, β polynomu f existuje podle věty 7 izomorfismus $\tau : \mathbb{Q}(\alpha) \to \mathbb{Q}(\beta)$ splňující $\tau(\alpha) = \beta$. K tomuto izomorfismu τ existuje podle věty 8 automorfismus $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ splňující $\sigma(\alpha) = \beta$. Proto žádný kořen polynomu f není vyjádřitelný v radikálech.

Neexistuje tedy žádný vzorec, kterým bychom mohli vypočítat byť jen jediný kořen tohoto polynomu f.

Vzorec na výpočet kořenů polynomu stupně 5 neexistuje

Poznámka. Ukázali jsme si příklad polynomu $f \in \mathbb{Q}[x]$ stupně 5, který je ireducibilní a není řešitelný. Pro takový polynom platí, že existuje jeho kořen, který není vyjádřitelný v radikálech, a tedy jej nelze napsat jako algebraický výraz obsahující racionální čísla, operace sčítání, odčítání, násobení, dělení a odmocniny.

Pro libovolné dva kořeny α, β polynomu f existuje podle věty 7 izomorfismus $\tau : \mathbb{Q}(\alpha) \to \mathbb{Q}(\beta)$ splňující $\tau(\alpha) = \beta$. K tomuto izomorfismu τ existuje podle věty 8 automorfismus $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ splňující $\sigma(\alpha) = \beta$. Proto žádný kořen polynomu f není vyjádřitelný v radikálech.

Neexistuje tedy žádný vzorec, kterým bychom mohli vypočítat byť jen jediný kořen tohoto polynomu f. Uvědomte si, že to je silnější tvrzení než pouze to, že neexistuje univerzální vzorec na výpočet kořenů pro polynomy pátého stupně!