

Odmocniny z jedné a cyklotomické polynomy

Konečná tělesa

22. května 2020

Obsah přednášky

Sekce 4: V této sekci budeme studovat rozkladová rozšíření polynomů $x^n - 1$, nazývaná ***n -tá cyklotomická nadtělesa***.

Obsah přednášky

Sekce 4: V této sekci budeme studovat rozkladová rozšíření polynomů $x^n - 1$, nazývaná *n -tá cyklotomická nadtělesa*.

- Ukážeme, že množina všech kořenů polynomu $x^n - 1$ tvoří cyklickou podgroupu multiplikativní grupy.

Obsah přednášky

Sekce 4: V této sekci budeme studovat rozkladová rozšíření polynomů $x^n - 1$, nazývaná ***n -tá cyklotomická nadtělesa***.

- Ukážeme, že množina všech kořenů polynomu $x^n - 1$ tvoří cyklickou podgrupu multiplikativní grupy.
- Generátory této podgrupy budeme nazývat ***primitivní n -té odmocniny z 1***.

Obsah přednášky

Sekce 4: V této sekci budeme studovat rozkladová rozšíření polynomů $x^n - 1$, nazývaná *n -tá cyklotomická nadtělesa*.

- Ukážeme, že množina všech kořenů polynomu $x^n - 1$ tvoří cyklickou podgrupu multiplikativní grupy.
- Generátory této podgrupy budeme nazývat *primitivní n -té odmocniny z 1*.
- Definujeme *n -tý cyklotomický polynom* jako součin lineárních polynomů $x - \xi$, kde ξ probíhá všechny primitivní n -té odmocniny z 1.

Obsah přednášky

Sekce 4: V této sekci budeme studovat rozkladová rozšíření polynomů $x^n - 1$, nazývaná ***n -tá cyklotomická nadtělesa***.

- Ukážeme, že množina všech kořenů polynomu $x^n - 1$ tvoří cyklickou podgrupu multiplikativní grupy.
- Generátory této podgrupy budeme nazývat ***primitivní n -té odmocniny z 1***.
- Definujeme ***n -tý cyklotomický polynom*** jako součin lineárních polynomů $x - \xi$, kde ξ probíhá všechny primitivní n -té odmocniny z 1.
- Ukážeme, že koeficienty cyklotomických polynomů nad tělesem F leží v prvotělese tělesa F .

Sekce 4: V této sekci budeme studovat rozkladová rozšíření polynomů $x^n - 1$, nazývaná *n -tá cyklotomická nadtělesa*.

- Ukážeme, že množina všech kořenů polynomu $x^n - 1$ tvoří cyklickou podgrupu multiplikativní grupy.
- Generátory této podgrupy budeme nazývat *primitivní n -té odmocniny z 1*.
- Definujeme *n -tý cyklotomický polynom* jako součin lineárních polynomů $x - \xi$, kde ξ probíhá všechny primitivní n -té odmocniny z 1.
- Ukážeme, že koeficienty cyklotomických polynomů nad tělesem F leží v prvotělese tělesa F .
- Naučíme se také cyklotomické polynomy počítat.

n -té cyklotomické nadtěleso

Definice

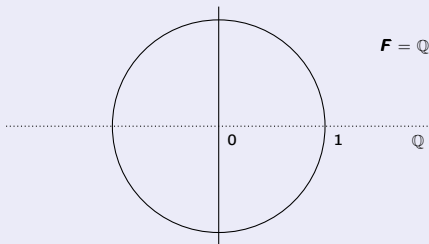
Bud' $\mathbf{F}$ libovolné těleso. Rozkladové rozšíření tělesa $\mathbf{F}$ určené polynomem $x^n - 1$ nazýváme *n -té cyklotomické těleso* nad $\mathbf{F}$ a značíme ho $\mathbf{F}^{(n)}$. Množinu všech kořenů polynomu $x^n - 1$ značíme $\mathbf{E}^{(n)}$. Kořeny polynomu $x^n - 1$ nazýváme *n -té odmocniny z jedné*.

n -té cyklotomické nadtěleso

Definice

Bud' F libovolné těleso. Rozkladové rozšíření tělesa F určené polynomem $x^n - 1$ nazýváme *n -té cyklotomické těleso* nad F a značíme ho $F^{(n)}$. Množinu všech kořenů polynomu $x^n - 1$ značíme $E^{(n)}$. Kořeny polynomu $x^n - 1$ nazýváme *n -té odmocniny z jedné*.

Příklad



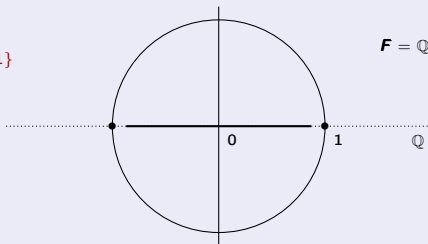
n -té cyklotomické nadtěleso

Definice

Bud' F libovolné těleso. Rozkladové rozšíření tělesa F určené polynomem $x^n - 1$ nazýváme *n -té cyklotomické těleso* nad F a značíme ho $F^{(n)}$. Množinu všech kořenů polynomu $x^n - 1$ značíme $E^{(n)}$. Kořeny polynomu $x^n - 1$ nazýváme *n -té odmocniny z jedné*.

Příklad

$$\begin{aligned} F^{(2)} &= \mathbb{Q} \\ E^{(2)} &= \{-1, 1\} \end{aligned}$$

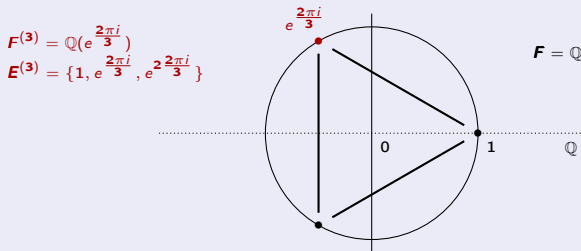


n -té cyklotomické nadtěleso

Definice

Bud' $\mathbf{F}$ libovolné těleso. Rozkladové rozšíření tělesa $\mathbf{F}$ určené polynomem $x^n - 1$ nazýváme **n -té cyklotomické těleso** nad $\mathbf{F}$ a značíme ho $\mathbf{F}^{(n)}$. Množinu všech kořenů polynomu $x^n - 1$ značíme $\mathbf{E}^{(n)}$. Kořeny polynomu $x^n - 1$ nazýváme **n -té odmocniny z jedné**.

Příklad



n -té cyklotomické nadtěleso

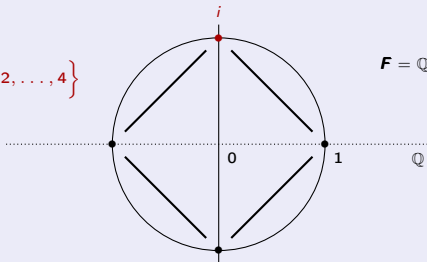
Definice

Bud' F libovolné těleso. Rozkladové rozšíření tělesa F určené polynomem $x^n - 1$ nazýváme **n -té cyklotomické těleso** nad F a značíme ho $F^{(n)}$. Množinu všech kořenů polynomu $x^n - 1$ značíme $E^{(n)}$. Kořeny polynomu $x^n - 1$ nazýváme **n -té odmocniny z jedné**.

Příklad

$$F^{(4)} = \mathbb{Q}(e^{\frac{\pi i}{2}}) = \mathbb{Q}(i)$$

$$E^{(4)} = \left\{ e^{j \frac{\pi i}{2}} \mid j = 1, 2, \dots, 4 \right\}$$



n -té cyklotomické nadtěleso

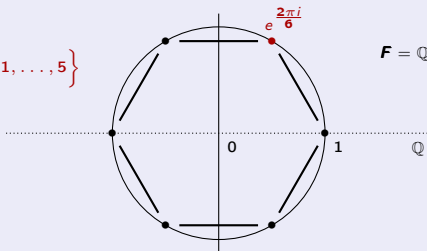
Definice

Bud' $\mathbf{F}$ libovolné těleso. Rozkladové rozšíření tělesa $\mathbf{F}$ určené polynomem $x^n - 1$ nazýváme *n -té cyklotomické těleso* nad $\mathbf{F}$ a značíme ho $\mathbf{F}^{(n)}$. Množinu všech kořenů polynomu $x^n - 1$ značíme $\mathbf{E}^{(n)}$. Kořeny polynomu $x^n - 1$ nazýváme *n -té odmocniny z jedné*.

Příklad

$$\mathbf{F}^{(6)} = \mathbb{Q}(e^{\frac{\pi i}{3}})$$

$$\mathbf{E}^{(6)} = \left\{ e^{j \frac{\pi i}{3}} \mid j = 0, 1, \dots, 5 \right\}$$



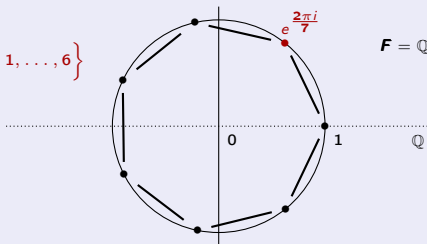
n -té cyklotomické nadtěleso

Definice

Bud' $\mathbf{F}$ libovolné těleso. Rozkladové rozšíření tělesa $\mathbf{F}$ určené polynomem $x^n - 1$ nazýváme *n -té cyklotomické těleso* nad $\mathbf{F}$ a značíme ho $\mathbf{F}^{(n)}$. Množinu všech kořenů polynomu $x^n - 1$ značíme $\mathbf{E}^{(n)}$. Kořeny polynomu $x^n - 1$ nazýváme *n -té odmocniny z jedné*.

Příklad

$$\begin{aligned}\mathbf{F}^{(7)} &= \mathbb{Q}(e^{\frac{2\pi i}{7}}) \\ \mathbf{E}^{(7)} &= \left\{ e^{j \frac{2\pi i}{7}} \mid j = 0, 1, \dots, 6 \right\}\end{aligned}$$



n -té cyklotomické nadtěleso

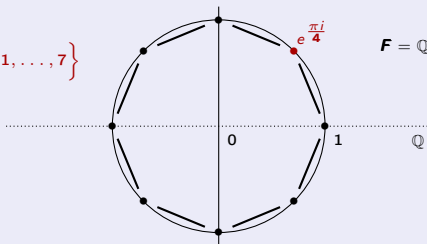
Definice

Bud' F libovolné těleso. Rozkladové rozšíření tělesa F určené polynomem $x^n - 1$ nazýváme *n -té cyklotomické těleso* nad F a značíme ho $F^{(n)}$. Množinu všech kořenů polynomu $x^n - 1$ značíme $E^{(n)}$. Kořeny polynomu $x^n - 1$ nazýváme *n -té odmocniny z jedné*.

Příklad

$$F^{(8)} = \mathbb{Q}(e^{\frac{\pi i}{4}})$$

$$E^{(8)} = \left\{ e^{j \frac{\pi i}{4}} \mid j = 0, 1, \dots, 7 \right\}$$



$$F = \mathbb{Q}$$

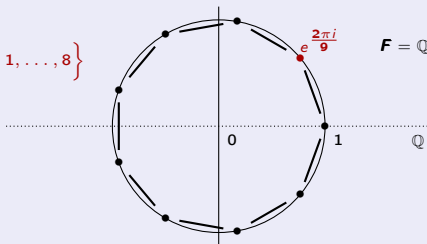
n -té cyklotomické nadtěleso

Definice

Bud' F libovolné těleso. Rozkladové rozšíření tělesa F určené polynomem $x^n - 1$ nazýváme *n -té cyklotomické těleso* nad F a značíme ho $F^{(n)}$. Množinu všech kořenů polynomu $x^n - 1$ značíme $E^{(n)}$. Kořeny polynomu $x^n - 1$ nazýváme *n -té odmocniny z jedné*.

Příklad

$$F^{(9)} = \mathbb{Q}(e^{\frac{2\pi i}{9}})$$
$$E^{(9)} = \left\{ e^{j \frac{2\pi i}{9}} \mid j = 0, 1, \dots, 8 \right\}$$



n -té cyklotomické nadtěleso

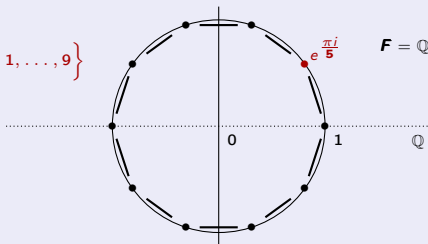
Definice

Bud' $\mathbf{F}$ libovolné těleso. Rozkladové rozšíření tělesa $\mathbf{F}$ určené polynomem $x^n - 1$ nazýváme *n -té cyklotomické těleso* nad $\mathbf{F}$ a značíme ho $\mathbf{F}^{(n)}$. Množinu všech kořenů polynomu $x^n - 1$ značíme $\mathbf{E}^{(n)}$. Kořeny polynomu $x^n - 1$ nazýváme *n -té odmocniny z jedné*.

Příklad

$$\mathbf{F}^{(10)} = \mathbb{Q}(e^{\frac{\pi i}{5}})$$

$$\mathbf{E}^{(10)} = \left\{ e^{j \frac{\pi i}{5}} \mid j = 0, 1, \dots, 9 \right\}$$



Věta (4.1)

Nechť $0 < n$ a F je těleso charakteristiky p (uvažujeme i $p = 0$).

Věta (4.1)

Nechť $0 < n$ a F je těleso charakteristiky p (uvažujeme i $p = 0$).

- Pokud $p \nmid n$, má polynom $x^n - 1$ v tělese $F^{(n)}$ jednoduché kořeny a $E^{(n)}$ je cyklická podgrupa řádu n multiplikativní grupy $(F^{(n)})^*$ tělesa $F^{(n)}$.

Věta (4.1)

Nechť $0 < n$ a F je těleso charakteristiky p (uvažujeme i $p = 0$).

- Pokud $p \nmid n$, má polynom $x^n - 1$ v tělese $F^{(n)}$ jednoduché kořeny a $E^{(n)}$ je cyklická podgrupa řádu n multiplikativní grupy $(F^{(n)})^*$ tělesa $F^{(n)}$.
- Pokud $p \mid n$ a je $n = p^k m$, kde $p \nmid m$, potom

$$x^n - 1 = (x^m - 1)^{p^k},$$

kořeny mají násobnost p^k , $E^{(n)} = E^{(m)}$ a $F^{(n)} = F^{(m)}$.

Věta (4.1)

Nechť $0 < n$ a F je těleso charakteristiky p (uvažujeme i $p = 0$).

- Pokud $p \nmid n$, má polynom $x^n - 1$ v tělese $F^{(n)}$ jednoduché kořeny a $E^{(n)}$ je cyklická podgrupa řádu n multiplikativní grupy $(F^{(n)})^*$ tělesa $F^{(n)}$.
- Pokud $p \mid n$ a je $n = p^k m$, kde $p \nmid m$, potom

$$x^n - 1 = (x^m - 1)^{p^k},$$

kořeny mají násobnost p^k , $E^{(n)} = E^{(m)}$ a $F^{(n)} = F^{(m)}$.

Poznámka

Pokud $p \nmid n$, nemá polynom $x^n - 1$ vícenásobné kořeny a platí

$$x^n - 1 = \prod_{\xi \in E^{(n)}} (x - \xi).$$

Věta (4.1)

Nechť $0 < n$ a F je těleso charakteristiky p (uvažujeme i $p = 0$).

- Pokud $p \nmid n$, má polynom $x^n - 1$ v tělese $F^{(n)}$ jednoduché kořeny a $E^{(n)}$ je cyklická podgrupa řádu n multiplikativní grupy $(F^{(n)})^*$ tělesa $F^{(n)}$.

Věta (4.1)

Nechť $0 < n$ a $\mathbf{F}$ je těleso charakteristiky p (uvažujeme i $p = 0$).

- Pokud $p \nmid n$, má polynom $x^n - 1$ v tělese $\mathbf{F}^{(n)}$ jednoduché kořeny a $\mathbf{E}^{(n)}$ je cyklická podgrupa řádu n multiplikativní grupy $(\mathbf{F}^{(n)})^*$ tělesa $\mathbf{F}^{(n)}$.

Důkaz.

Položme $f(x) := x^n - 1$. Protože $p \nmid n$, je $f'(x) = n \cdot x^{n-1} \neq 0$ a $\text{NSD}(f(x), f'(x)) = 1$.



Věta (4.1)

Nechť $0 < n$ a $\mathbf{F}$ je těleso charakteristiky p (uvažujeme i $p = 0$).

- Pokud $p \nmid n$, má polynom $x^n - 1$ v tělese $\mathbf{F}^{(n)}$ jednoduché kořeny a $\mathbf{E}^{(n)}$ je cyklická podgrupa řádu n multiplikativní grupy $(\mathbf{F}^{(n)})^*$ tělesa $\mathbf{F}^{(n)}$.

Důkaz.

Položme $f(x) := x^n - 1$. Protože $p \nmid n$, je $f'(x) = n \cdot x^{n-1} \neq 0$ a $\text{NSD}(f(x), f'(x)) = 1$.

Proto nemá polynom $f(x) = x^n - 1$ vícenásobné kořeny.



Věta (4.1)

Nechť $0 < n$ a F je těleso charakteristiky p (uvažujeme i $p = 0$).

- Pokud $p \nmid n$, má polynom $x^n - 1$ v tělese $F^{(n)}$ jednoduché kořeny a $E^{(n)}$ je cyklická podgrupa řádu n multiplikativní grupy $(F^{(n)})^*$ tělesa $F^{(n)}$.

Důkaz.

Položme $f(x) := x^n - 1$. Protože $p \nmid n$, je $f'(x) = n \cdot x^{n-1} \neq 0$ a $\text{NSD}(f(x), f'(x)) = 1$.

Proto nemá polynom $f(x) = x^n - 1$ vícenásobné kořeny.

Jsou-li $\alpha, \beta \in E^{(n)}$, pak $(\alpha\beta)^n = \alpha^n \beta^n = 1$ a tedy $\alpha\beta \in E^{(n)}$.



Věta (4.1)

Nechť $0 < n$ a $\mathbf{F}$ je těleso charakteristiky p (uvažujeme i $p = 0$).

- Pokud $p \nmid n$, má polynom $x^n - 1$ v tělese $\mathbf{F}^{(n)}$ jednoduché kořeny a $\mathbf{E}^{(n)}$ je cyklická podgrupa řádu n multiplikativní grupy $(\mathbf{F}^{(n)})^*$ tělesa $\mathbf{F}^{(n)}$.

Důkaz.

Položme $f(x) := x^n - 1$. Protože $p \nmid n$, je $f'(x) = n \cdot x^{n-1} \neq 0$ a $\text{NSD}(f(x), f'(x)) = 1$.

Proto nemá polynom $f(x) = x^n - 1$ vícenásobné kořeny.

Jsou-li $\alpha, \beta \in \mathbf{E}^{(n)}$, pak $(\alpha\beta)^n = \alpha^n \beta^n = 1$ a tedy $\alpha\beta \in \mathbf{E}^{(n)}$.

Protože je množina $\mathbf{E}^{(n)}$ konečná a uzavřená na násobení, tvoří podgrupu $((\mathbf{F}^{(n)})^*, \cdot)$.



Věta (4.1)

Nechť $0 < n$ a F je těleso charakteristiky p (uvažujeme i $p = 0$).

- Pokud $p \nmid n$, má polynom $x^n - 1$ v tělese $F^{(n)}$ jednoduché kořeny a $E^{(n)}$ je cyklická podgrupa řádu n multiplikativní grupy $(F^{(n)})^*$ tělesa $F^{(n)}$.

Důkaz.

Položme $f(x) := x^n - 1$. Protože $p \nmid n$, je $f'(x) = n \cdot x^{n-1} \neq 0$ a $\text{NSD}(f(x), f'(x)) = 1$.

Proto nemá polynom $f(x) = x^n - 1$ vícenásobné kořeny.

Jsou-li $\alpha, \beta \in E^{(n)}$, pak $(\alpha\beta)^n = \alpha^n \beta^n = 1$ a tedy $\alpha\beta \in E^{(n)}$.

Protože je množina $E^{(n)}$ konečná a uzavřená na násobení, tvoří podgrupu $((F^{(n)})^*, \cdot)$.

Konečná podgrupa multiplikativní grupy tělesa je cyklická.



Věta (4.1)

Nechť $0 < n$ a F je těleso charakteristiky p (uvažujeme i $p = 0$).

- Pokud $p \nmid n$, má polynom $x^n - 1$ v tělese $F^{(n)}$ jednoduché kořeny a $E^{(n)}$ je cyklická podgrupa řádu n multiplikativní grupy $(F^{(n)})^*$ tělesa $F^{(n)}$.
- Pokud $p \mid n$ a je $n = p^k m$, kde $p \nmid m$, potom

$$x^n - 1 = (x^m - 1)^{p^k},$$

kořeny mají násobnost p^k , $E^{(n)} = E^{(m)}$ a $F^{(n)} = F^{(m)}$.

Důkaz.



Věta (4.1)

Nechť $0 < n$ a F je těleso charakteristiky p (uvažujeme i $p = 0$).

- Pokud $p \nmid n$, má polynom $x^n - 1$ v tělese $F^{(n)}$ jednoduché kořeny a $E^{(n)}$ je cyklická podgrupa řádu n multiplikativní grupy $(F^{(n)})^*$ tělesa $F^{(n)}$.
- Pokud $p \mid n$ a je $n = p^k m$, kde $p \nmid m$, potom

$$x^n - 1 = (x^m - 1)^{p^k},$$

kořeny mají násobnost p^k , $E^{(n)} = E^{(m)}$ a $F^{(n)} = F^{(m)}$.

Důkaz.

Pro $p = 2$ dostaneme: $x^n - 1 = x^n + 1 = (x^m)^{p^k} + 1^{p^k} = (x^m + 1)^{p^k} = (x^m - 1)^{p^k}$.



Věta (4.1)

Nechť $0 < n$ a F je těleso charakteristiky p (uvvažujeme i $p = 0$).

- Pokud $p \nmid n$, má polynom $x^n - 1$ v tělese $F^{(n)}$ jednoduché kořeny a $E^{(n)}$ je cyklická podgrupa řádu n multiplikativní grupy $(F^{(n)})^*$ tělesa $F^{(n)}$.
- Pokud $p \mid n$ a je $n = p^k m$, kde $p \nmid m$, potom

$$x^n - 1 = (x^m - 1)^{p^k},$$

kořeny mají násobnost p^k , $E^{(n)} = E^{(m)}$ a $F^{(n)} = F^{(m)}$.

Důkaz.

Pro $p = 2$ dostaneme: $x^n - 1 = x^n + 1 = (x^m)^{p^k} + 1^{p^k} = (x^m + 1)^{p^k} = (x^m - 1)^{p^k}$.

Pro liché p platí: $x^n - 1 = (x^m)^{p^k} + (-1)^{p^k} = (x^m - 1)^{p^k}$.



Definice

Bud' F těleso charakteristiky p a n přirozené číslo takové, že $p \nmid n$. Libovolný generátor $E^{(n)}$ se nazývá *primitivní* n -tá odmocnina z 1 nad F . Množinu primitivních n -tých odmocnin z 1 budeme značit $P^{(n)}$.

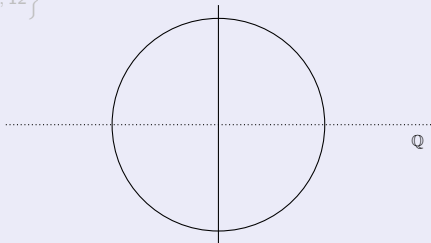
Definice

Buď F těleso charakteristiky p a n přirozené číslo takové, že $p \nmid n$. Libovolný generátor $E^{(n)}$ se nazývá *primitivní* n -tá odmocnina z 1 nad F . Množinu primitivních n -tých odmocnin z 1 budeme značit $P^{(n)}$.

Příklad

$$F = \mathbb{Q}$$

$$E^{(12)} = \left\{ e^{k \frac{2\pi i}{12}} \mid k = 0, 1, \dots, 12 \right\}$$



Definice

Buď F těleso charakteristiky p a n přirozené číslo takové, že $p \nmid n$. Libovolný generátor $E^{(n)}$ se nazývá **primitivní** n -tá odmocnina z 1 nad F . Množinu primitivních n -tých odmocnin z 1 budeme značit $P^{(n)}$.

Příklad

$$F = \mathbb{Q}$$

$$E^{(12)} = \left\{ e^{k \frac{2\pi i}{12}} \mid k = 0, 1, \dots, 11 \right\}$$

$$P^{(1)} = \{e^0\} = \{1\}$$

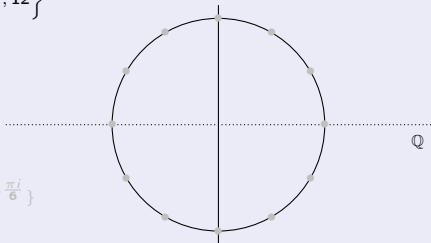
$$P^{(2)} = \{e^{\pi i}\} = \{-1\}$$

$$P^{(3)} = \{e^{2\frac{\pi i}{3}}, e^{4\frac{\pi i}{3}}\}$$

$$P^{(4)} = \{e^{\frac{\pi i}{2}}, e^{3\frac{\pi i}{2}}\} = \{i, -i\}$$

$$P^{(6)} = \{e^{\frac{\pi i}{3}}, e^{5\frac{\pi i}{3}}\}$$

$$P^{(12)} = \{e^{\frac{\pi i}{6}}, e^{5\frac{\pi i}{6}}, e^{7\frac{\pi i}{6}}, e^{11\frac{\pi i}{6}}\}$$



Definice

Buď F těleso charakteristiky p a n přirozené číslo takové, že $p \nmid n$. Libovolný generátor $E^{(n)}$ se nazývá **primitivní** n -tá odmocnina z 1 nad F . Množinu primitivních n -tých odmocnin z 1 budeme značit $P^{(n)}$.

Příklad

$$F = \mathbb{Q}$$

$$E^{(12)} = \left\{ e^{k \frac{2\pi i}{12}} \mid k = 0, 1, \dots, 12 \right\}$$

$$P^{(1)} = \{e^0\} = \{1\}$$

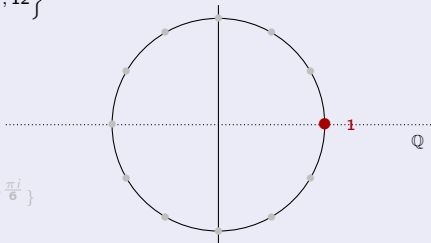
$$P^{(2)} = \{e^{\pi i}\} = \{-1\}$$

$$P^{(3)} = \{e^{\frac{2\pi i}{3}}, e^{\frac{4\pi i}{3}}\}$$

$$P^{(4)} = \{e^{\frac{\pi i}{2}}, e^{\frac{3\pi i}{2}}\} = \{i, -i\}$$

$$P^{(6)} = \{e^{\frac{\pi i}{3}}, e^{\frac{5\pi i}{3}}\}$$

$$P^{(12)} = \{e^{\frac{\pi i}{6}}, e^{\frac{5\pi i}{6}}, e^{\frac{7\pi i}{6}}, e^{\frac{11\pi i}{6}}\}$$



Definice

Buď F těleso charakteristiky p a n přirozené číslo takové, že $p \nmid n$. Libovolný generátor $E^{(n)}$ se nazývá **primitivní** n -tá odmocnina z 1 nad F . Množinu primitivních n -tých odmocnin z 1 budeme značit $P^{(n)}$.

Příklad

$$F = \mathbb{Q}$$

$$E^{(12)} = \left\{ e^{k \frac{2\pi i}{12}} \mid k = 0, 1, \dots, 11 \right\}$$

$$P^{(1)} = \{e^0\} = \{1\}$$

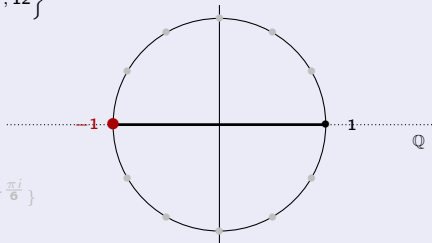
$$P^{(2)} = \{e^{\pi i}\} = \{-1\}$$

$$P^{(3)} = \{e^{2 \frac{\pi i}{3}}, e^{4 \frac{\pi i}{3}}\}$$

$$P^{(4)} = \{e^{\frac{\pi i}{2}}, e^{3 \frac{\pi i}{2}}\} = \{i, -i\}$$

$$P^{(6)} = \{e^{\frac{\pi i}{3}}, e^{5 \frac{\pi i}{3}}\}$$

$$P^{(12)} = \{e^{\frac{\pi i}{6}}, e^{5 \frac{\pi i}{6}}, e^{7 \frac{\pi i}{6}}, e^{11 \frac{\pi i}{6}}\}$$



Definice

Buď F těleso charakteristiky p a n přirozené číslo takové, že $p \nmid n$. Libovolný generátor $E^{(n)}$ se nazývá **primitivní** n -tá odmocnina z 1 nad F . Množinu primitivních n -tých odmocnin z 1 budeme značit $P^{(n)}$.

Příklad

$$F = \mathbb{Q}$$

$$E^{(12)} = \left\{ e^{k \frac{2\pi i}{12}} \mid k = 0, 1, \dots, 12 \right\}$$

$$P^{(1)} = \{e^0\} = \{1\}$$

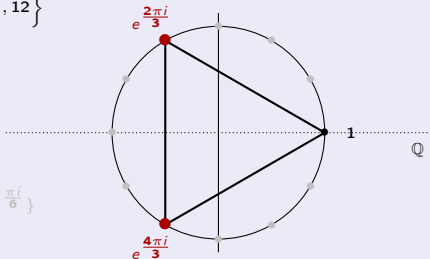
$$P^{(2)} = \{e^{\pi i}\} = \{-1\}$$

$$P^{(3)} = \left\{ e^{2 \frac{\pi i}{3}}, e^{4 \frac{\pi i}{3}} \right\}$$

$$P^{(4)} = \left\{ e^{\frac{\pi i}{2}}, e^{3 \frac{\pi i}{2}} \right\} = \{i, -i\}$$

$$P^{(6)} = \left\{ e^{\frac{\pi i}{3}}, e^{5 \frac{\pi i}{3}} \right\}$$

$$P^{(12)} = \left\{ e^{\frac{\pi i}{6}}, e^{5 \frac{\pi i}{6}}, e^{7 \frac{\pi i}{6}}, e^{11 \frac{\pi i}{6}} \right\}$$



Definice

Buď F těleso charakteristiky p a n přirozené číslo takové, že $p \nmid n$. Libovolný generátor $E^{(n)}$ se nazývá **primitivní** n -tá odmocnina z 1 nad F . Množinu primitivních n -tých odmocnin z 1 budeme značit $P^{(n)}$.

Příklad

$$F = \mathbb{Q}$$

$$E^{(12)} = \left\{ e^{k \frac{2\pi i}{12}} \mid k = 0, 1, \dots, 12 \right\}$$

$$P^{(1)} = \{e^0\} = \{1\}$$

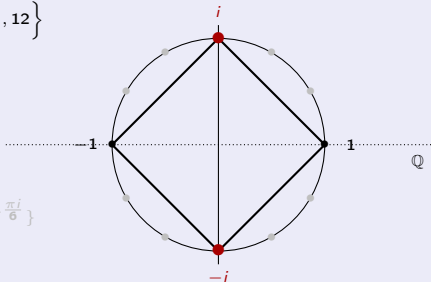
$$P^{(2)} = \{e^{\pi i}\} = \{-1\}$$

$$P^{(3)} = \{e^{\frac{2\pi i}{3}}, e^{\frac{4\pi i}{3}}\}$$

$$P^{(4)} = \{e^{\frac{\pi i}{2}}, e^{\frac{3\pi i}{2}}\} = \{i, -i\}$$

$$P^{(6)} = \{e^{\frac{\pi i}{3}}, e^{\frac{5\pi i}{3}}\}$$

$$P^{(12)} = \{e^{\frac{\pi i}{6}}, e^{\frac{5\pi i}{6}}, e^{\frac{7\pi i}{6}}, e^{\frac{11\pi i}{6}}\}$$



Definice

Buď F těleso charakteristiky p a n přirozené číslo takové, že $p \nmid n$. Libovolný generátor $E^{(n)}$ se nazývá **primitivní** n -tá odmocnina z 1 nad F . Množinu primitivních n -tých odmocnin z 1 budeme značit $P^{(n)}$.

Příklad

$$F = \mathbb{Q}$$

$$E^{(12)} = \left\{ e^{k \frac{2\pi i}{12}} \mid k = 0, 1, \dots, 11 \right\}$$

$$P^{(1)} = \{e^0\} = \{1\}$$

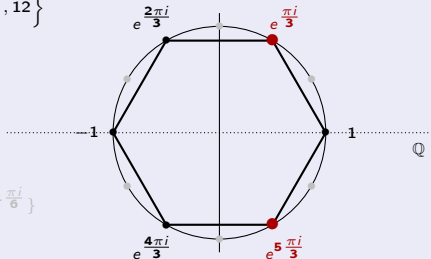
$$P^{(2)} = \{e^{\pi i}\} = \{-1\}$$

$$P^{(3)} = \{e^{\frac{2\pi i}{3}}, e^{\frac{4\pi i}{3}}\}$$

$$P^{(4)} = \{e^{\frac{\pi i}{2}}, e^{\frac{3\pi i}{2}}\} = \{i, -i\}$$

$$P^{(6)} = \{e^{\frac{\pi i}{3}}, e^{\frac{5\pi i}{3}}\}$$

$$P^{(12)} = \{e^{\frac{\pi i}{6}}, e^{\frac{5\pi i}{6}}, e^{\frac{7\pi i}{6}}, e^{\frac{11\pi i}{6}}\}$$



Definice

Buď F těleso charakteristiky p a n přirozené číslo takové, že $p \nmid n$. Libovolný generátor $E^{(n)}$ se nazývá **primitivní** n -tá odmocnina z 1 nad F . Množinu primitivních n -tých odmocnin z 1 budeme značit $P^{(n)}$.

Příklad

$$F = \mathbb{Q}$$

$$E^{(12)} = \left\{ e^{k \frac{2\pi i}{12}} \mid k = 0, 1, \dots, 11 \right\}$$

$$P^{(1)} = \{e^0\} = \{1\}$$

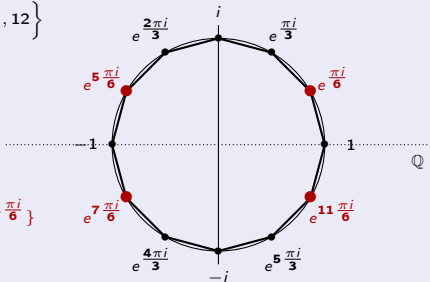
$$P^{(2)} = \{e^{\pi i}\} = \{-1\}$$

$$P^{(3)} = \{e^{\frac{2\pi i}{3}}, e^{\frac{4\pi i}{3}}\}$$

$$P^{(4)} = \{e^{\frac{\pi i}{2}}, e^{\frac{3\pi i}{2}}\} = \{i, -i\}$$

$$P^{(6)} = \{e^{\frac{\pi i}{3}}, e^{\frac{5\pi i}{3}}\}$$

$$P^{(12)} = \{e^{\frac{\pi i}{6}}, e^{\frac{5\pi i}{6}}, e^{\frac{7\pi i}{6}}, e^{\frac{11\pi i}{6}}\}$$



Definice

Bud' $\mathbf{F}$ těleso charakteristiky p , a n přirozené číslo takové, že $p \nmid n$. Polynom

$$Q_n(x) := \prod_{\xi \in P(n)} (x - \xi)$$

nazýváme *n -tý cyklotomický polynom* nad $\mathbf{F}$.

Definice

Bud' $\mathbf{F}$ těleso charakteristiky p , a n přirozené číslo takové, že $p \nmid n$. Polynom

$$Q_n(x) := \prod_{\xi \in P(n)} (x - \xi)$$

nazýváme *n -tý cyklotomický polynom* nad $\mathbf{F}$.

Věta (4.2)

Nechť $\mathbf{F}$ je těleso charakteristiky p a n kladné přirozené číslo takové, že $p \nmid n$. Potom

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

a všechny koeficienty polynomu $Q_n(x)$ leží v prvotělese tělesa $\mathbf{F}$. Je-li $p = 0$, jsou všechny koeficienty polynomu $Q_n(x)$ celočíselné.

Věta (4.2)

Necht' $\mathbf{F}$ je těleso charakteristiky p a n kladné přirozené číslo takové, že $p \nmid n$. Potom

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

Věta (4.2)

Nechť $\mathbf{F}$ je těleso charakteristiky p a n kladné přirozené číslo takové, že $p \nmid n$. Potom

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

Důkaz.

$$x^n - 1 = \prod_{\xi \in \mathbf{E}^{(n)}} (x - \xi)$$

Každé $\xi \in \mathbf{E}^{(n)}$ je primitivní d -tá odmocnina pro právě jedno $d \mid n$.



Věta (4.2)

Nechť $\mathbf{F}$ je těleso charakteristiky p a n kladné přirozené číslo takové, že $p \nmid n$. Potom

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

a všechny koeficienty polynomu $Q_n(x)$ leží v prvotělese tělesa $\mathbf{F}$.

Důkaz.

Indukcí podle n : $n = 1$, potom $Q_1(x) = x - 1$



Věta (4.2)

Nechť $\mathbf{F}$ je těleso charakteristiky p a n kladné přirozené číslo takové, že $p \nmid n$. Potom

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

a všechny koeficienty polynomu $Q_n(x)$ leží v prvotělese tělesa $\mathbf{F}$.

Důkaz.

Indukcí podle n : $n = 1$, potom $Q_1(x) = x - 1$

$$n - 1 \mapsto n: Q_n(x) = \frac{x^n - 1}{\prod_{d|n, d < n} Q_d(x)}.$$



Věta (4.2)

Nechť $\mathbf{F}$ je těleso charakteristiky p a n kladné přirozené číslo takové, že $p \nmid n$. Potom

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

a všechny koeficienty polynomu $Q_n(x)$ leží v prvotělese tělesa $\mathbf{F}$. Je-li $p = 0$, jsou všechny koeficienty polynomu $Q_n(x)$ celočíselné.

Důkaz.

Indukcí podle n : $n = 1$, potom $Q_1(x) = x - 1$

$$n - 1 \mapsto n: Q_n(x) = \frac{x^n - 1}{\prod_{d|n, d < n} Q_d(x)}.$$

Podílem dvou monických polynomů s celočíselnými koeficienty je polynom s celočíselnými koeficienty.



Důsledek

Nechť $\mathbf{F}$ je těleso charakteristiky p a r kladné přirozené číslo takové, že $p \nmid r$. Potom pro každé $0 \leq k$ platí rovnost

$$Q_{r^k}(x) = \frac{x^{r^k} - 1}{x^{r^{k-1}} - 1}.$$

Důsledek

Nechť $\mathbf{F}$ je těleso charakteristiky p a r kladné přirozené číslo takové, že $p \nmid r$. Potom pro každé $0 \leq k$ platí rovnost

$$Q_{r^k}(x) = \frac{x^{r^k} - 1}{x^{r^{k-1}} - 1}.$$

Příklad

Nad tělesem charakteristiky různé od 2 je

$$Q_4(x) = \frac{x^4 - 1}{x^2 - 1} = x^2 + 1.$$

Příklad

Bud' F těleso charakteristiky různé od 2 a 3. Spočteme Q_{12} .

Příklad

Bud' F těleso charakteristiky různé od 2 a 3. Spočteme Q_{12} .

- Dělitelé 12 jsou 1, 2, 3, 4, 6, 12, proto

$$x^{12} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_{12}(x).$$

Příklad

Bud' F těleso charakteristiky různé od 2 a 3. Spočteme Q_{12} .

- Dělitelé 12 jsou 1, 2, 3, 4, 6, 12, proto

$$x^{12} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_{12}(x).$$

- Dělitelé 6 jsou 1, 2, 3, 6, proto

$$x^6 - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_6(x).$$

Příklad

Bud' F těleso charakteristiky různé od 2 a 3. Spočteme Q_{12} .

- Dělitelé 12 jsou 1, 2, 3, 4, 6, 12, proto

$$x^{12} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_{12}(x).$$

- Dělitelé 6 jsou 1, 2, 3, 6, proto

$$x^6 - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_6(x).$$

- Z předchozího víme, že $Q_4(x) = x^2 + 1$.

Příklad

Bud' F těleso charakteristiky různé od 2 a 3. Spočteme Q_{12} .

- Dělitelé 12 jsou 1, 2, 3, 4, 6, 12, proto

$$x^{12} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_{12}(x).$$

- Dělitelé 6 jsou 1, 2, 3, 6, proto

$$x^6 - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_6(x).$$

- Z předchozího víme, že $Q_4(x) = x^2 + 1$.
- Odtud

$$Q_{12}(x) = \frac{x^{12} - 1}{(x^6 - 1)(x^2 + 1)} = x^4 - x^2 + 1.$$

Poznámka

Primitivní n -té odmocniny z 1 jsou právě $e^{k\frac{2\pi i}{n}}$, kde $\text{NSD}(k, n) = 1$. Těch je $\varphi(n)$. Proto

$$\deg Q_n(x) = \varphi(n).$$

Poznámka

Primitivní n -té odmocniny z 1 jsou právě $e^{k\frac{2\pi i}{n}}$, kde $\text{NSD}(k, n) = 1$. Těch je $\varphi(n)$. Proto

$$\deg Q_n(x) = \varphi(n).$$

Věta (4.3)

Bud' $F = \mathbb{F}_q$ a n nesoudělné s q . Necht' d je nejmenší kladné přirozené číslo takové, že $q^d \equiv 1 \pmod{n}$. Potom

Poznámka

Primitivní n -té odmocniny z 1 jsou právě $e^{k\frac{2\pi i}{n}}$, kde $\text{NSD}(k, n) = 1$. Těch je $\varphi(n)$. Proto

$$\deg Q_n(x) = \varphi(n).$$

Věta (4.3)

Bud' $F = \mathbb{F}_q$ a n nesoudělné s q . Necht' d je nejmenší kladné přirozené číslo takové, že $q^d \equiv 1 \pmod{n}$. Potom

- $F^{(n)} = \mathbb{F}_{q^d}.$

Poznámka

Primitivní n -té odmocniny z 1 jsou právě $e^{k\frac{2\pi i}{n}}$, kde $\text{NSD}(k, n) = 1$. Těch je $\varphi(n)$. Proto

$$\deg Q_n(x) = \varphi(n).$$

Věta (4.3)

Bud' $F = \mathbb{F}_q$ a n nesoudělné s q . Necht' d je nejmenší kladné přirozené číslo takové, že $q^d \equiv 1 \pmod{n}$. Potom

- $F^{(n)} = \mathbb{F}_{q^d}$.
- Polynom $Q_n(x)$ se rozkládá v součin $\varphi(n)/d$ různých monických polynomů stupně d .

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot Q_{18}(x) \cdot Q_{36}(x).$$

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot Q_{18}(x) \cdot Q_{36}(x).$$

$$Q_1(x) = x - 1 = x + 4$$

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot Q_{18}(x) \cdot Q_{36}(x).$$

$$Q_1(x) = x + 4,$$

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot Q_{18}(x) \cdot Q_{36}(x).$$

$$Q_1(x) = x + 4,$$

$$Q_2(x) = \frac{x^2 - 1}{x - 1} = x + 1$$

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot Q_{18}(x) \cdot Q_{36}(x).$$

$$Q_1(x) = x + 4, \quad Q_2(x) = x + 1,$$

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot Q_{18}(x) \cdot Q_{36}(x).$$

$$Q_1(x) = x + 4, \quad Q_2(x) = x + 1,$$

$$\deg Q_3(x) = \varphi(3) = 2$$

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot Q_{18}(x) \cdot Q_{36}(x).$$

$$Q_1(x) = x + 4, \quad Q_2(x) = x + 1,$$

$$\deg Q_3(x) = \varphi(3) = 2$$

$$5 \equiv 2 \pmod{3} \text{ a } 5^2 \equiv 1 \pmod{3}$$

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot Q_{18}(x) \cdot Q_{36}(x).$$

$$Q_1(x) = x + 4, \quad Q_2(x) = x + 1,$$

$$\deg Q_3(x) = \varphi(3) = 2$$

$$5 \equiv 2 \pmod{3} \text{ a } 5^2 \equiv 1 \pmod{3}$$

Nejmenší d takové, že $5^d \equiv 1 \pmod{3}$ je $2 = \deg Q_3(x)$

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot Q_{18}(x) \cdot Q_{36}(x).$$

$$Q_1(x) = x + 4, \quad Q_2(x) = x + 1,$$

$$\deg Q_3(x) = \varphi(3) = 2$$

$$5 \equiv 2 \pmod{3} \text{ a } 5^2 \equiv 1 \pmod{3}$$

Nejmenší d takové, že $5^d \equiv 1 \pmod{3}$ je $2 = \deg Q_3(x)$

Polynom $Q_3(x)$ je ireducibilní

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot Q_{18}(x) \cdot Q_{36}(x).$$

$$Q_1(x) = x + 4, \quad Q_2(x) = x + 1,$$

$$\deg Q_3(x) = \varphi(3) = 2$$

$$5 \equiv 2 \pmod{3} \text{ a } 5^2 \equiv 1 \pmod{3}$$

Nejmenší d takové, že $5^d \equiv 1 \pmod{3}$ je $2 = \deg Q_3(x)$

Polynom $Q_3(x)$ je ireducibilní

$$Q_3(x) = \frac{x^3 - 1}{x - 1} = x^2 + x + 1$$

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot Q_{18}(x) \cdot Q_{36}(x).$$

$$Q_1(x) = x + 4, \quad Q_2(x) = x + 1, \quad Q_3(x) = x^2 + x + 1,$$

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot Q_{18}(x) \cdot Q_{36}(x).$$

$$Q_1(x) = x + 4, \quad Q_2(x) = x + 1, \quad Q_3(x) = x^2 + x + 1,$$

$$\deg Q_4(x) = \varphi(4) = 2$$

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot Q_{18}(x) \cdot Q_{36}(x).$$

$$Q_1(x) = x + 4, \quad Q_2(x) = x + 1, \quad Q_3(x) = x^2 + x + 1,$$

$$\deg Q_4(x) = \varphi(4) = 2$$

$$5 \equiv 1 \pmod{4}$$

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot Q_{18}(x) \cdot Q_{36}(x).$$

$$Q_1(x) = x + 4, \quad Q_2(x) = x + 1, \quad Q_3(x) = x^2 + x + 1,$$

$$\deg Q_4(x) = \varphi(4) = 2$$

$$5 \equiv 1 \pmod{4}$$

Nejmenší d takové, že $5^d \equiv 1 \pmod{4}$ je 1

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot Q_{18}(x) \cdot Q_{36}(x).$$

$$Q_1(x) = x + 4, \quad Q_2(x) = x + 1, \quad Q_3(x) = x^2 + x + 1,$$

$$\deg Q_4(x) = \varphi(4) = 2$$

$$5 \equiv 1 \pmod{4}$$

Nejmenší d takové, že $5^d \equiv 1 \pmod{4}$ je 1

Polynom $Q_4(x)$ se rozkládá na lineární činitele

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot Q_{18}(x) \cdot Q_{36}(x).$$

$$Q_1(x) = x + 4, \quad Q_2(x) = x + 1, \quad Q_3(x) = x^2 + x + 1,$$

$$\deg Q_4(x) = \varphi(4) = 2$$

$$5 \equiv 1 \pmod{4}$$

Nejmenší d takové, že $5^d \equiv 1 \pmod{4}$ je 1

Polynom $Q_4(x)$ se rozkládá na lineární činitele

$$Q_4(x) = \frac{x^4 - 1}{x^2 - 1} = x^2 + 1 = (x + 2)(x - 2) = (x + 2)(x + 3)$$

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot Q_{18}(x) \cdot Q_{36}(x).$$

$$Q_1(x) = x + 4, \quad Q_2(x) = x + 1, \quad Q_3(x) = x^2 + x + 1, \quad Q_4(x) = (x + 2)(x + 3),$$

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot Q_{18}(x) \cdot Q_{36}(x).$$

$$Q_1(x) = x + 4, \quad Q_2(x) = x + 1, \quad Q_3(x) = x^2 + x + 1, \quad Q_4(x) = (x + 2)(x + 3),$$

$$\deg Q_6(x) = \varphi(6) = 2$$

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot Q_{18}(x) \cdot Q_{36}(x).$$

$$Q_1(x) = x + 4, \quad Q_2(x) = x + 1, \quad Q_3(x) = x^2 + x + 1, \quad Q_4(x) = (x + 2)(x + 3),$$

$$\deg Q_6(x) = \varphi(6) = 2$$

Nejmenší d takové, že $5^d \equiv 1 \pmod{6}$ je $2 = \deg Q_6(x)$

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot Q_{18}(x) \cdot Q_{36}(x).$$

$$Q_1(x) = x + 4, \quad Q_2(x) = x + 1, \quad Q_3(x) = x^2 + x + 1, \quad Q_4(x) = (x + 2)(x + 3),$$

$$\deg Q_6(x) = \varphi(6) = 2$$

Nejmenší d takové, že $5^d \equiv 1 \pmod{6}$ je $2 = \deg Q_6(x)$

Polynom $Q_6(x)$ je ireducibilní

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot Q_{18}(x) \cdot Q_{36}(x).$$

$$Q_1(x) = x + 4, \quad Q_2(x) = x + 1, \quad Q_3(x) = x^2 + x + 1, \quad Q_4(x) = (x + 2)(x + 3),$$

$$\deg Q_6(x) = \varphi(6) = 2$$

Nejmenší d takové, že $5^d \equiv 1 \pmod{6}$ je $2 = \deg Q_6(x)$

Polynom $Q_6(x)$ je ireducibilní

$$Q_6(x) = \frac{x^6 - 1}{Q_1(x) \cdot Q_2(x) \cdot Q_3(x)} = x^2 - x + 1 = x^2 + 4x + 1$$

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot Q_{18}(x) \cdot Q_{36}(x).$$

$$Q_1(x) = x + 4, \quad Q_2(x) = x + 1, \quad Q_3(x) = x^2 + x + 1, \quad Q_4(x) = (x + 2)(x + 3), \\ Q_6(x) = x^2 + 4x + 1,$$

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot Q_{18}(x) \cdot Q_{36}(x).$$

$$Q_1(x) = x + 4, \quad Q_2(x) = x + 1, \quad Q_3(x) = x^2 + x + 1, \quad Q_4(x) = (x + 2)(x + 3), \\ Q_6(x) = x^2 + 4x + 1,$$

$$\deg Q_9(x) = \varphi(9) = 6$$

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot Q_{18}(x) \cdot Q_{36}(x).$$

$$Q_1(x) = x + 4, \quad Q_2(x) = x + 1, \quad Q_3(x) = x^2 + x + 1, \quad Q_4(x) = (x + 2)(x + 3), \\ Q_6(x) = x^2 + 4x + 1,$$

$$\deg Q_9(x) = \varphi(9) = 6$$

Nejmenší d takové, že $5^d \equiv 1 \pmod{9}$ je 6

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot Q_{18}(x) \cdot Q_{36}(x).$$

$$Q_1(x) = x + 4, \quad Q_2(x) = x + 1, \quad Q_3(x) = x^2 + x + 1, \quad Q_4(x) = (x + 2)(x + 3), \\ Q_6(x) = x^2 + 4x + 1,$$

$$\deg Q_9(x) = \varphi(9) = 6$$

Nejmenší d takové, že $5^d \equiv 1 \pmod{9}$ je 6

Polynom $Q_9(x)$ je ireducibilní

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot Q_{18}(x) \cdot Q_{36}(x).$$

$$Q_1(x) = x + 4, \quad Q_2(x) = x + 1, \quad Q_3(x) = x^2 + x + 1, \quad Q_4(x) = (x + 2)(x + 3), \\ Q_6(x) = x^2 + 4x + 1,$$

$$\deg Q_9(x) = \varphi(9) = 6$$

Nejmenší d takové, že $5^d \equiv 1 \pmod{9}$ je 6

Polynom $Q_9(x)$ je ireducibilní

$$Q_9(x) = \frac{x^9 - 1}{x^3 - 1} = x^6 + x^3 + 1$$

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot Q_{18}(x) \cdot Q_{36}(x).$$

$$Q_1(x) = x + 4, \quad Q_2(x) = x + 1, \quad Q_3(x) = x^2 + x + 1, \quad Q_4(x) = (x + 2)(x + 3), \\ Q_6(x) = x^2 + 4x + 1, \quad Q_9(x) = x^6 + x^3 + 1,$$

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot Q_{18}(x) \cdot Q_{36}(x).$$

$$Q_1(x) = x + 4, \quad Q_2(x) = x + 1, \quad Q_3(x) = x^2 + x + 1, \quad Q_4(x) = (x + 2)(x + 3), \\ Q_6(x) = x^2 + 4x + 1, \quad Q_9(x) = x^6 + x^3 + 1,$$

$$\deg Q_{12}(x) = \varphi(12) = 4$$

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot Q_{18}(x) \cdot Q_{36}(x).$$

$$Q_1(x) = x + 4, \quad Q_2(x) = x + 1, \quad Q_3(x) = x^2 + x + 1, \quad Q_4(x) = (x + 2)(x + 3), \\ Q_6(x) = x^2 + 4x + 1, \quad Q_9(x) = x^6 + x^3 + 1,$$

$$\deg Q_{12}(x) = \varphi(12) = 4$$

Nejmenší d takové, že $5^d \equiv 1 \pmod{12}$ je 2

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot Q_{18}(x) \cdot Q_{36}(x).$$

$$Q_1(x) = x + 4, \quad Q_2(x) = x + 1, \quad Q_3(x) = x^2 + x + 1, \quad Q_4(x) = (x + 2)(x + 3), \\ Q_6(x) = x^2 + 4x + 1, \quad Q_9(x) = x^6 + x^3 + 1,$$

$$\deg Q_{12}(x) = \varphi(12) = 4$$

Nejmenší d takové, že $5^d \equiv 1 \pmod{12}$ je 2

Polynom $Q_{12}(x)$ se rozkládá v součin dvou polynomů stupně 2

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot Q_{18}(x) \cdot Q_{36}(x).$$

$$Q_1(x) = x + 4, \quad Q_2(x) = x + 1, \quad Q_3(x) = x^2 + x + 1, \quad Q_4(x) = (x + 2)(x + 3), \\ Q_6(x) = x^2 + 4x + 1, \quad Q_9(x) = x^6 + x^3 + 1,$$

$$\deg Q_{12}(x) = \varphi(12) = 4$$

Nejmenší d takové, že $5^d \equiv 1 \pmod{12}$ je 2

Polynom $Q_{12}(x)$ se rozkládá v součin dvou polynomů stupně 2

$$Q_{12}(x) = \frac{x^{12}-1}{Q_6(x) \cdot Q_4(x) \cdot Q_3(x) \cdot Q_2(x) \cdot Q_1(x)} = \frac{x^{12}-1}{(x^6-1) \cdot (x^2+1)} = (x^2 + 2x + 4)(x^2 + 3x + 4)$$

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot Q_{18}(x) \cdot Q_{36}(x).$$

$$Q_1(x) = x + 4, \quad Q_2(x) = x + 1, \quad Q_3(x) = x^2 + x + 1, \quad Q_4(x) = (x + 2)(x + 3), \\ Q_6(x) = x^2 + 4x + 1, \quad Q_9(x) = x^6 + x^3 + 1, \quad Q_{12}(x) = (x^2 + 2x + 4)(x^2 + 3x + 4),$$

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot Q_{18}(x) \cdot Q_{36}(x).$$

$$Q_1(x) = x + 4, \quad Q_2(x) = x + 1, \quad Q_3(x) = x^2 + x + 1, \quad Q_4(x) = (x + 2)(x + 3), \\ Q_6(x) = x^2 + 4x + 1, \quad Q_9(x) = x^6 + x^3 + 1, \quad Q_{12}(x) = (x^2 + 2x + 4)(x^2 + 3x + 4),$$

$$\deg Q_{18}(x) = \varphi(18) = \varphi(2)\varphi(9) = 6$$

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot Q_{18}(x) \cdot Q_{36}(x).$$

$$Q_1(x) = x + 4, \quad Q_2(x) = x + 1, \quad Q_3(x) = x^2 + x + 1, \quad Q_4(x) = (x + 2)(x + 3), \\ Q_6(x) = x^2 + 4x + 1, \quad Q_9(x) = x^6 + x^3 + 1, \quad Q_{12}(x) = (x^2 + 2x + 4)(x^2 + 3x + 4),$$

$$\deg Q_{18}(x) = \varphi(18) = \varphi(2)\varphi(9) = 6$$

Nejmenší d takové, že $5^d \equiv 1 \pmod{18}$ je 6

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot \mathbf{Q_{18}(x)} \cdot Q_{36}(x).$$

$$Q_1(x) = x + 4, \quad Q_2(x) = x + 1, \quad Q_3(x) = x^2 + x + 1, \quad Q_4(x) = (x + 2)(x + 3), \\ Q_6(x) = x^2 + 4x + 1, \quad Q_9(x) = x^6 + x^3 + 1, \quad Q_{12}(x) = (x^2 + 2x + 4)(x^2 + 3x + 4),$$

$$\deg Q_{18}(x) = \varphi(18) = \varphi(2)\varphi(9) = 6$$

Nejmenší d takové, že $5^d \equiv 1 \pmod{18}$ je 6

Polynom $Q_{18}(x)$ je ireducibilní

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot Q_{18}(x) \cdot Q_{36}(x).$$

$$Q_1(x) = x + 4, \quad Q_2(x) = x + 1, \quad Q_3(x) = x^2 + x + 1, \quad Q_4(x) = (x + 2)(x + 3), \\ Q_6(x) = x^2 + 4x + 1, \quad Q_9(x) = x^6 + x^3 + 1, \quad Q_{12}(x) = (x^2 + 2x + 4)(x^2 + 3x + 4),$$

$$\deg Q_{18}(x) = \varphi(18) = \varphi(2)\varphi(9) = 6$$

Nejmenší d takové, že $5^d \equiv 1 \pmod{18}$ je 6

Polynom $Q_{18}(x)$ je ireducibilní

$$Q_{18}(x) = \frac{x^{18}-1}{Q_9(x) \cdot Q_6(x) \cdot Q_3(x) \cdot Q_2(x) \cdot Q_1(x)} = \frac{x^{18}-1}{(x^6-1) \cdot Q_9(x)} = \frac{(x^{18}-1)(x^3-1)}{(x^6-1)(x^9-1)} = \frac{x^9+1}{x^3+1} =$$

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot \mathbf{Q_{18}(x)} \cdot Q_{36}(x).$$

$$Q_1(x) = x + 4, \quad Q_2(x) = x + 1, \quad Q_3(x) = x^2 + x + 1, \quad Q_4(x) = (x + 2)(x + 3), \\ Q_6(x) = x^2 + 4x + 1, \quad Q_9(x) = x^6 + x^3 + 1, \quad Q_{12}(x) = (x^2 + 2x + 4)(x^2 + 3x + 4),$$

$$\deg Q_{18}(x) = \varphi(18) = \varphi(2)\varphi(9) = 6$$

Nejmenší d takové, že $5^d \equiv 1 \pmod{18}$ je 6

Polynom $Q_{18}(x)$ je ireducibilní

$$Q_{18}(x) = \frac{x^{18}-1}{Q_9(x) \cdot Q_6(x) \cdot Q_3(x) \cdot Q_2(x) \cdot Q_1(x)} = \frac{x^{18}-1}{(x^6-1) \cdot Q_9(x)} = \frac{(x^{18}-1)(x^3-1)}{(x^6-1)(x^9-1)} = \frac{x^9+1}{x^3+1} = \\ = x^6 - x^3 + 1 = x^6 + 4x^3 + 1$$

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot Q_{18}(x) \cdot Q_{36}(x).$$

$$\begin{aligned} Q_1(x) &= x + 4, & Q_2(x) &= x + 1, & Q_3(x) &= x^2 + x + 1, & Q_4(x) &= (x + 2)(x + 3), \\ Q_6(x) &= x^2 + 4x + 1, & Q_9(x) &= x^6 + x^3 + 1, & Q_{12}(x) &= (x^2 + 2x + 4)(x^2 + 3x + 4), \\ Q_{18}(x) &= x^6 + 4x^3 + 1, \end{aligned}$$

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot Q_{18}(x) \cdot Q_{36}(x).$$

$$\begin{aligned} Q_1(x) &= x + 4, & Q_2(x) &= x + 1, & Q_3(x) &= x^2 + x + 1, & Q_4(x) &= (x + 2)(x + 3), \\ Q_6(x) &= x^2 + 4x + 1, & Q_9(x) &= x^6 + x^3 + 1, & Q_{12}(x) &= (x^2 + 2x + 4)(x^2 + 3x + 4), \\ Q_{18}(x) &= x^6 + 4x^3 + 1, \end{aligned}$$

$$\deg Q_{36}(x) = \varphi(36) = \varphi(4)\varphi(9) = 12$$

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot Q_{18}(x) \cdot Q_{36}(x).$$

$$\begin{aligned} Q_1(x) &= x + 4, & Q_2(x) &= x + 1, & Q_3(x) &= x^2 + x + 1, & Q_4(x) &= (x + 2)(x + 3), \\ Q_6(x) &= x^2 + 4x + 1, & Q_9(x) &= x^6 + x^3 + 1, & Q_{12}(x) &= (x^2 + 2x + 4)(x^2 + 3x + 4), \\ Q_{18}(x) &= x^6 + 4x^3 + 1, \end{aligned}$$

$$\deg Q_{36}(x) = \varphi(36) = \varphi(4)\varphi(9) = 12$$

Nejmenší d takové, že $5^d \equiv 1 \pmod{36}$ je 6

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot Q_{18}(x) \cdot Q_{36}(x).$$

$$\begin{aligned} Q_1(x) &= x + 4, & Q_2(x) &= x + 1, & Q_3(x) &= x^2 + x + 1, & Q_4(x) &= (x + 2)(x + 3), \\ Q_6(x) &= x^2 + 4x + 1, & Q_9(x) &= x^6 + x^3 + 1, & Q_{12}(x) &= (x^2 + 2x + 4)(x^2 + 3x + 4), \\ Q_{18}(x) &= x^6 + 4x^3 + 1, \end{aligned}$$

$$\deg Q_{36}(x) = \varphi(36) = \varphi(4)\varphi(9) = 12$$

Nejmenší d takové, že $5^d \equiv 1 \pmod{36}$ je 6

Polynom $Q_{36}(x)$ se rozkládá v součin dvou ireducibilních polynomů stupně 6

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot Q_{18}(x) \cdot Q_{36}(x).$$

$$\begin{aligned} Q_1(x) &= x + 4, & Q_2(x) &= x + 1, & Q_3(x) &= x^2 + x + 1, & Q_4(x) &= (x + 2)(x + 3), \\ Q_6(x) &= x^2 + 4x + 1, & Q_9(x) &= x^6 + x^3 + 1, & Q_{12}(x) &= (x^2 + 2x + 4)(x^2 + 3x + 4), \\ Q_{18}(x) &= x^6 + 4x^3 + 1, \end{aligned}$$

$$\deg Q_{36}(x) = \varphi(36) = \varphi(4)\varphi(9) = 12$$

Nejmenší d takové, že $5^d \equiv 1 \pmod{36}$ je 6

Polynom $Q_{36}(x)$ se rozkládá v součin dvou ireducibilních polynomů stupně 6

$$Q_{36}(x) = \frac{x^{36} - 1}{Q_{18} \cdot Q_{12}(x) \cdot Q_9(x) \cdot Q_6(x) \cdot Q_4(x) \cdot Q_3(x) \cdot Q_2(x) \cdot Q_1(x)} = \frac{x^{36} - 1}{(x^{18} - 1) \cdot Q_{12}(x) \cdot Q_4(x)} =$$

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot Q_{18}(x) \cdot Q_{36}(x).$$

$$\begin{aligned} Q_1(x) &= x + 4, & Q_2(x) &= x + 1, & Q_3(x) &= x^2 + x + 1, & Q_4(x) &= (x + 2)(x + 3), \\ Q_6(x) &= x^2 + 4x + 1, & Q_9(x) &= x^6 + x^3 + 1, & Q_{12}(x) &= (x^2 + 2x + 4)(x^2 + 3x + 4), \\ Q_{18}(x) &= x^6 + 4x^3 + 1, \end{aligned}$$

$$\deg Q_{36}(x) = \varphi(36) = \varphi(4)\varphi(9) = 12$$

Nejmenší d takové, že $5^d \equiv 1 \pmod{36}$ je 6

Polynom $Q_{36}(x)$ se rozkládá v součin dvou ireducibilních polynomů stupně 6

$$\begin{aligned} Q_{36}(x) &= \frac{x^{36}-1}{Q_{18} \cdot Q_{12}(x) \cdot Q_9(x) \cdot Q_6(x) \cdot Q_4(x) \cdot Q_3(x) \cdot Q_2(x) \cdot Q_1(x)} = \frac{x^{36}-1}{(x^{18}-1) \cdot Q_{12}(x) \cdot Q_4(x)} = \\ &= \frac{(x^{36}-1)(x^6-1)}{(x^{18}-1)(x^{12}-1)} = \frac{x^{18}+1}{x^6+1} = x^{12} - x^6 + 1 = (x^6 + 2x^3 + 4)(x^6 + 3x^3 + 4) \end{aligned}$$

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot Q_{18}(x) \cdot Q_{36}(x).$$

$$\begin{aligned} Q_1(x) &= x + 4, & Q_2(x) &= x + 1, & Q_3(x) &= x^2 + x + 1, & Q_4(x) &= (x + 2)(x + 3), \\ Q_6(x) &= x^2 + 4x + 1, & Q_9(x) &= x^6 + x^3 + 1, & Q_{12}(x) &= (x^2 + 2x + 4)(x^2 + 3x + 4), \\ Q_{18}(x) &= x^6 + 4x^3 + 1, & Q_{36}(x) &= (x^6 + 2x^3 + 4)(x^6 + 3x^3 + 4). \end{aligned}$$

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot Q_{18}(x) \cdot Q_{36}(x).$$

$$\begin{aligned} Q_1(x) &= x + 4, & Q_2(x) &= x + 1, & Q_3(x) &= x^2 + x + 1, & Q_4(x) &= (x + 2)(x + 3), \\ Q_6(x) &= x^2 + 4x + 1, & Q_9(x) &= x^6 + x^3 + 1, & Q_{12}(x) &= (x^2 + 2x + 4)(x^2 + 3x + 4), \\ Q_{18}(x) &= x^6 + 4x^3 + 1, & Q_{36}(x) &= (x^6 + 2x^3 + 4)(x^6 + 3x^3 + 4). \end{aligned}$$

Nejmenší d takové, že $5^d \equiv 1 \pmod{36}$ je 6. Proto platí, že

Příklad

Uvažme polynom $x^{36} - 1$ nad tělesem $\mathbb{F}_5$. Hledáme rozklad tohoto polynomu v součin ireducibilních polynomů.

$$x^{36} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_9(x) \cdot Q_{12}(x) \cdot Q_{18}(x) \cdot Q_{36}(x).$$

$$\begin{aligned} Q_1(x) &= x + 4, & Q_2(x) &= x + 1, & Q_3(x) &= x^2 + x + 1, & Q_4(x) &= (x + 2)(x + 3), \\ Q_6(x) &= x^2 + 4x + 1, & Q_9(x) &= x^6 + x^3 + 1, & Q_{12}(x) &= (x^2 + 2x + 4)(x^2 + 3x + 4), \\ Q_{18}(x) &= x^6 + 4x^3 + 1, & Q_{36}(x) &= (x^6 + 2x^3 + 4)(x^6 + 3x^3 + 4). \end{aligned}$$

Nejmenší d takové, že $5^d \equiv 1 \pmod{36}$ je 6. Proto platí, že

$$\mathbb{F}_5^{(36)} = \mathbb{F}_{5^6}.$$

Příklad

Nad tělesem $\mathbb{F}_5$ máme rozklad polynomu $x^{12} - 1$ v součin ireducibilních polynomů:

Příklad

Nad tělesem $\mathbb{F}_5$ máme rozklad polynomu $x^{12} - 1$ v součin ireducibilních polynomů:

$$x^{12} - 1 = \underbrace{(x - 1)}_{Q_1(x)} \underbrace{(x + 1)}_{Q_2(x)} \underbrace{(x^2 + x + 1)}_{Q_3(x)} \underbrace{(x + 2)(x + 3)}_{Q_4(x)} \underbrace{(x^2 + 4x + 1)}_{Q_6(x)} \underbrace{(x^2 + 2x + 4)(x^2 + 3x + 4)}_{Q_{12}(x)}.$$

Příklad

Nad tělesem $\mathbb{F}_5$ máme rozklad polynomu $x^{12} - 1$ v součin ireducibilních polynomů:

$$x^{12} - 1 = \underbrace{(x - 1)}_{Q_1(x)} \underbrace{(x + 1)}_{Q_2(x)} \underbrace{(x^2 + x + 1)}_{Q_3(x)} \underbrace{(x + 2)(x + 3)}_{Q_4(x)} \underbrace{(x^2 + 4x + 1)}_{Q_6(x)} \underbrace{(x^2 + 2x + 4)(x^2 + 3x + 4)}_{Q_{12}(x)}.$$

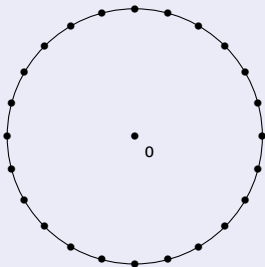
Protože $5 \not\equiv 1$ a $5^2 \equiv 1 \pmod{12}$ platí, že $\mathbb{F}_5^{(12)} = \mathbb{F}_{5^2}$

Příklad

Nad tělesem $\mathbb{F}_5$ máme rozklad polynomu $x^{12} - 1$ v součin ireducibilních polynomů:

$$x^{12} - 1 = \underbrace{(x-1)}_{Q_1(x)} \underbrace{(x+1)}_{Q_2(x)} \underbrace{(x^2+x+1)}_{Q_3(x)} \underbrace{(x+2)(x+3)}_{Q_4(x)} \underbrace{(x^2+4x+1)}_{Q_6(x)} \underbrace{(x^2+2x+4)(x^2+3x+4)}_{Q_{12}(x)}.$$

Protože $5 \not\equiv 1$ a $5^2 \equiv 1 \pmod{12}$ platí, že $\mathbb{F}_5^{(12)} = \mathbb{F}_{5^2}$



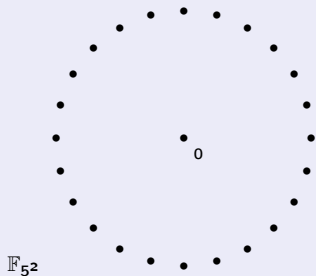
Prvky $\mathbb{F}_{5^2}^*$ si můžeme představit jako body na kružnici.

Příklad

Nad tělesem $\mathbb{F}_5$ máme rozklad polynomu $x^{12} - 1$ v součin ireducibilních polynomů:

$$x^{12} - 1 = \underbrace{(x-1)}_{Q_1(x)} \underbrace{(x+1)}_{Q_2(x)} \underbrace{(x^2+x+1)}_{Q_3(x)} \underbrace{(x+2)(x+3)}_{Q_4(x)} \underbrace{(x^2+4x+1)}_{Q_6(x)} \underbrace{(x^2+2x+4)(x^2+3x+4)}_{Q_{12}(x)}.$$

Protože $5 \not\equiv 1$ a $5^2 \equiv 1 \pmod{12}$ platí, že $\mathbb{F}_5^{(12)} = \mathbb{F}_{5^2}$



Prvky $\mathbb{F}_{5^2}^*$ si můžeme představit jako body na kružnici.

Příklad

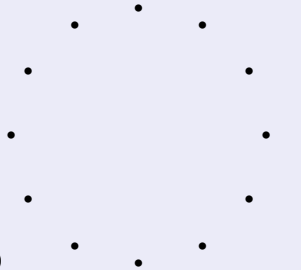
Nad tělesem $\mathbb{F}_5$ máme rozklad polynomu $x^{12} - 1$ v součin ireducibilních polynomů:

$$x^{12} - 1 = \underbrace{(x-1)}_{Q_1(x)} \underbrace{(x+1)}_{Q_2(x)} \underbrace{(x^2+x+1)}_{Q_3(x)} \underbrace{(x+2)(x+3)}_{Q_4(x)} \underbrace{(x^2+4x+1)}_{Q_6(x)} \underbrace{(x^2+2x+4)(x^2+3x+4)}_{Q_{12}(x)}.$$

Protože $5 \not\equiv 1$ a $5^2 \equiv 1 \pmod{12}$ platí, že $\mathbb{F}_5^{(12)} = \mathbb{F}_{5^2}$

Prozkoumáme 12-té odmocniny z jedné nad tělesem $\mathbb{F}_{5^2}$.

$E^{(12)}$

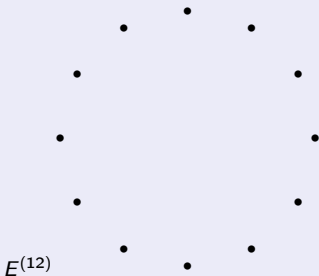


Příklad

Nad tělesem $\mathbb{F}_5$ máme rozklad polynomu $x^{12} - 1$ v součin ireducibilních polynomů:

$$x^{12} - 1 = \underbrace{(x-1)}_{Q_1(x)} \underbrace{(x+1)}_{Q_2(x)} \underbrace{(x^2+x+1)}_{Q_3(x)} \underbrace{(x+2)(x+3)}_{Q_4(x)} \underbrace{(x^2+4x+1)}_{Q_6(x)} \underbrace{(x^2+2x+4)(x^2+3x+4)}_{Q_{12}(x)}.$$

Protože $5 \not\equiv 1$ a $5^2 \equiv 1 \pmod{12}$ platí, že $\mathbb{F}_5^{(12)} = \mathbb{F}_{5^2}$



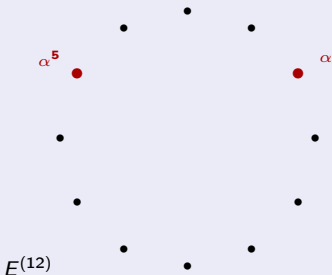
Nejprve najdeme primitivní 12-té odmocniny z jedné.

Příklad

Nad tělesem $\mathbb{F}_5$ máme rozklad polynomu $x^{12} - 1$ v součin ireducibilních polynomů:

$$x^{12} - 1 = \underbrace{(x-1)}_{Q_1(x)} \underbrace{(x+1)}_{Q_2(x)} \underbrace{(x^2+x+1)}_{Q_3(x)} \underbrace{(x+2)(x+3)}_{Q_4(x)} \underbrace{(x^2+4x+1)}_{Q_6(x)} \underbrace{(x^2+2x+4)(x^2+3x+4)}_{Q_{12}(x)}.$$

Protože $5 \not\equiv 1$ a $5^2 \equiv 1 \pmod{12}$ platí, že $\mathbb{F}_5^{(12)} = \mathbb{F}_{5^2}$



Nejprve najdeme primitivní 12-té odmocninu z jedné.

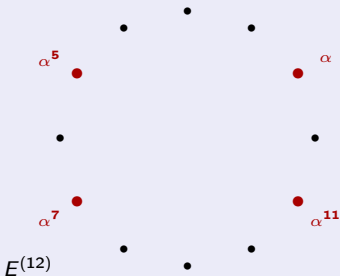
Zvolíme jeden z ireducibilních dělitelů polynomu $Q_{12}(x)$, například $x^2 + 3x + 4$ a jeden z jeho kořenů označíme α . Druhý z kořenů je nutně α^5 .

Příklad

Nad tělesem $\mathbb{F}_5$ máme rozklad polynomu $x^{12} - 1$ v součin ireducibilních polynomů:

$$x^{12} - 1 = \underbrace{(x-1)}_{Q_1(x)} \underbrace{(x+1)}_{Q_2(x)} \underbrace{(x^2+x+1)}_{Q_3(x)} \underbrace{(x+2)(x+3)}_{Q_4(x)} \underbrace{(x^2+4x+1)}_{Q_6(x)} \underbrace{(x^2+2x+4)(x^2+3x+4)}_{Q_{12}(x)}.$$

Protože $5 \not\equiv 1$ a $5^2 \equiv 1 \pmod{12}$ platí, že $\mathbb{F}_5^{(12)} = \mathbb{F}_{5^2}$



Nejprve najdeme primitivní 12-té odmocniny z jedné.

Zvolíme jeden z ireducibilních dělitelů polynomu $Q_{12}(x)$, například $x^2 + 3x + 4$ a jeden z jeho kořenů označíme α . Druhý z kořenů je nutně α^5 .

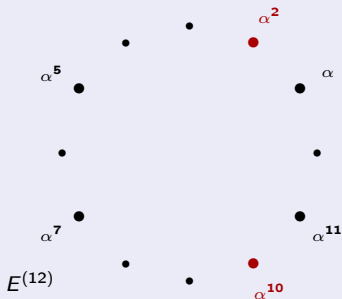
Kořeny druhého z ireducibilních dělitelů $Q_{12}(x)$, tedy polynomu $x^2 + 2x + 4$, jsou α^7 a α^{11} .

Příklad

Nad tělesem $\mathbb{F}_5$ máme rozklad polynomu $x^{12} - 1$ v součin ireducibilních polynomů:

$$x^{12} - 1 = \underbrace{(x-1)}_{Q_1(x)} \underbrace{(x+1)}_{Q_2(x)} \underbrace{(x^2+x+1)}_{Q_3(x)} \underbrace{(x+2)(x+3)}_{Q_4(x)} \underbrace{(x^2+4x+1)}_{Q_6(x)} \underbrace{(x^2+2x+4)(x^2+3x+4)}_{Q_{12}(x)}.$$

Protože $5 \not\equiv 1$ a $5^2 \equiv 1 \pmod{12}$ platí, že $\mathbb{F}_5^{(12)} = \mathbb{F}_{5^2}$



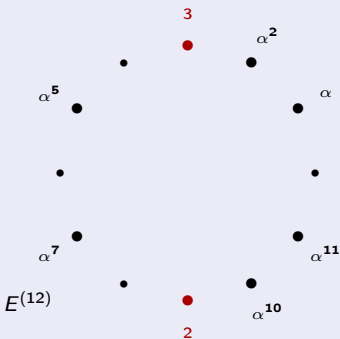
Primitivní 6-té odmocniny z jedné, kořeny polynomu $Q_6(x) = x^2 + 4x + 1$, jsou α^2 a α^{10} .

Příklad

Nad tělesem $\mathbb{F}_5$ máme rozklad polynomu $x^{12} - 1$ v součin ireducibilních polynomů:

$$x^{12} - 1 = \underbrace{(x-1)}_{Q_1(x)} \underbrace{(x+1)}_{Q_2(x)} \underbrace{(x^2+x+1)}_{Q_3(x)} \underbrace{(x+2)(x+3)}_{Q_4(x)} \underbrace{(x^2+4x+1)}_{Q_6(x)} \underbrace{(x^2+2x+4)(x^2+3x+4)}_{Q_{12}(x)}.$$

Protože $5 \nmid 1$ a $5^2 \equiv 1 \pmod{12}$ platí, že $\mathbb{F}_5^{(12)} = \mathbb{F}_{5^2}$



Primitivní 6-té odmocniny z jedné, kořeny polynomu $Q_6(x) = x^2 + 4x + 1$, jsou α^2 a α^{10} .

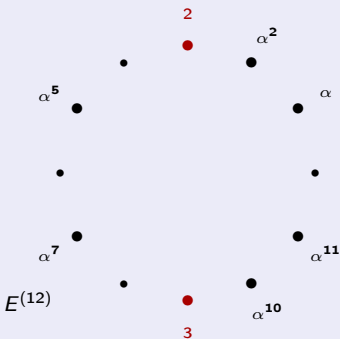
Primitivní 4-té odmocniny z jedné jsou 2 a 3. V závislosti na úvodní volbě ireducibilního dělitele polynomu Q_{12} je $3 = \alpha^3$ a $2 = \alpha^9, \dots$

Příklad

Nad tělesem $\mathbb{F}_5$ máme rozklad polynomu $x^{12} - 1$ v součin ireducibilních polynomů:

$$x^{12} - 1 = \underbrace{(x-1)}_{Q_1(x)} \underbrace{(x+1)}_{Q_2(x)} \underbrace{(x^2+x+1)}_{Q_3(x)} \underbrace{(x+2)(x+3)}_{Q_4(x)} \underbrace{(x^2+4x+1)}_{Q_6(x)} \underbrace{(x^2+2x+4)(x^2+3x+4)}_{Q_{12}(x)}.$$

Protože $5 \nmid 1$ a $5^2 \equiv 1 \pmod{12}$ platí, že $\mathbb{F}_5^{(12)} = \mathbb{F}_{5^2}$



Primitivní 6-té odmocniny z jedné, kořeny polynomu $Q_6(x) = x^2 + 4x + 1$, jsou α^2 a α^{10} .

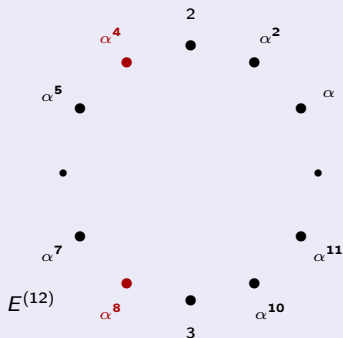
Primitivní 4-té odmocniny z jedné jsou 2 a 3. V závislosti na úvodní volbě ireducibilního dělitele polynomu Q_{12} je $3 = \alpha^3$ a $2 = \alpha^9$, nebo naopak $2 = \alpha^3$ a $3 = \alpha^9$.

Příklad

Nad tělesem $\mathbb{F}_5$ máme rozklad polynomu $x^{12} - 1$ v součin ireducibilních polynomů:

$$x^{12} - 1 = \underbrace{(x-1)}_{Q_1(x)} \underbrace{(x+1)}_{Q_2(x)} \underbrace{(x^2+x+1)}_{Q_3(x)} \underbrace{(x+2)(x+3)}_{Q_4(x)} \underbrace{(x^2+4x+1)}_{Q_6(x)} \underbrace{(x^2+2x+4)(x^2+3x+4)}_{Q_{12}(x)}.$$

Protože $5 \nmid 1$ a $5^2 \equiv 1 \pmod{12}$ platí, že $\mathbb{F}_5^{(12)} = \mathbb{F}_{5^2}$



Primitivní 6-té odmocniny z jedné, kořeny polynomu $Q_6(x) = x^2 + 4x + 1$, jsou α^2 a α^{10} .

Primitivní 4-té odmocniny z jedné jsou 2 a 3. V závislosti na úvodní volbě ireducibilního dělitele polynomu Q_{12} je $3 = \alpha^3$ a $2 = \alpha^9$, nebo naopak $2 = \alpha^3$ a $3 = \alpha^9$.

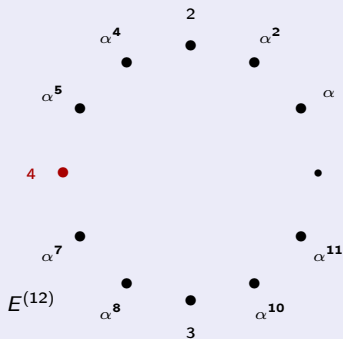
Primitivní třetí odmocniny z jedné jsou α^4 a α^8 .

Příklad

Nad tělesem $\mathbb{F}_5$ máme rozklad polynomu $x^{12} - 1$ v součin ireducibilních polynomů:

$$x^{12} - 1 = \underbrace{(x-1)}_{Q_1(x)} \underbrace{(x+1)}_{Q_2(x)} \underbrace{(x^2+x+1)}_{Q_3(x)} \underbrace{(x+2)(x+3)}_{Q_4(x)} \underbrace{(x^2+4x+1)}_{Q_6(x)} \underbrace{(x^2+2x+4)(x^2+3x+4)}_{Q_{12}(x)}.$$

Protože $5 \not\equiv 1$ a $5^2 \equiv 1 \pmod{12}$ platí, že $\mathbb{F}_5^{(12)} = \mathbb{F}_{5^2}$



Primitivní 6-té odmocniny z jedné, kořeny polynomu $Q_6(x) = x^2 + 4x + 1$, jsou α^2 a α^{10} .

Primitivní 4-té odmocniny z jedné jsou 2 a 3. V závislosti na úvodní volbě ireducibilního dělitele polynomu Q_{12} je $3 = \alpha^3$ a $2 = \alpha^9$, nebo naopak $2 = \alpha^3$ a $3 = \alpha^9$.

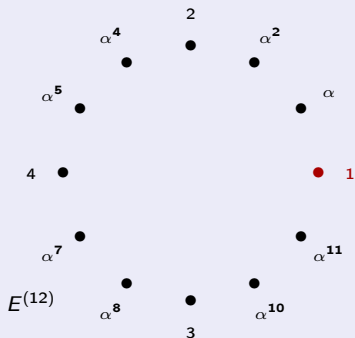
Primitivní třetí odmocniny z jedné jsou α^4 a α^8 . Primitivní druhá odmocnina z jedné je $4 = -1 = \alpha^6$.

Příklad

Nad tělesem $\mathbb{F}_5$ máme rozklad polynomu $x^{12} - 1$ v součin ireducibilních polynomů:

$$x^{12} - 1 = \underbrace{(x-1)}_{Q_1(x)} \underbrace{(x+1)}_{Q_2(x)} \underbrace{(x^2+x+1)}_{Q_3(x)} \underbrace{(x+2)(x+3)}_{Q_4(x)} \underbrace{(x^2+4x+1)}_{Q_6(x)} \underbrace{(x^2+2x+4)(x^2+3x+4)}_{Q_{12}(x)}.$$

Protože $5 \not\equiv 1$ a $5^2 \equiv 1 \pmod{12}$ platí, že $\mathbb{F}_5^{(12)} = \mathbb{F}_{5^2}$



Primitivní 6-té odmocniny z jedné, kořeny polynomu $Q_6(x) = x^2 + 4x + 1$, jsou α^2 a α^{10} .

Primitivní 4-té odmocniny z jedné jsou 2 a 3 . V závislosti na úvodní volbě ireducibilního dělitele polynomu Q_{12} je $3 = \alpha^3$ a $2 = \alpha^9$, nebo naopak $2 = \alpha^3$ a $3 = \alpha^9$.

Primitivní třetí odmocniny z jedné jsou α^4 a α^8 . Primitivní druhá odmocnina z jedné je $4 = -1 = \alpha^6$. Jediný kořen polynomu $Q_1(x)$ je 1 .