Definice. Nechť $\mathbf{K}$ je těleso charakteristiky p a nechť $p \nmid n$. Pak libovolný generátor $\mathbf{E}^{(n)}$ nazýváme *primitivní n-tá odmocnina z* 1 nad $\mathbf{K}$.

Poznámka. Je-li ξ generátor $\mathbf{E}^{(n)}$, pak $\mathbf{E}^{(n)} = \{1, \xi, \xi^2, \ldots, \xi^{n-1}\}$. Platí, že ξ^s je také generátor $\mathbf{E}^{(n)}$ právě tehdy, když $\mathrm{NSD}(s, n) = 1$. Tedy pokud $p = \mathrm{char}\ \mathbf{T}$ nedělí n, pak existuje $\varphi(n)$ primitivních n-tých odmocnin z 1 nad $\mathbf{K}$.

Definice. Nechť $\mathbf{K}$ je těleso charakteristiky p, $p \nmid n$ a ξ je primitivní n-tá odmocnina z 1. Pak polynom

$$Q_n(x) = \prod_{\substack{0 \le s < n \\ \mathrm{NSD}(s,n)=1}} (x - \xi^s)$$

se nazývá *n-tý cyklotomický polynom* nad $\mathbf{K}$.

Poznámka. Polynom $Q_n(x)$ je nezávislý na výběru ξ, stupeň $Q_n(x)$ je $\varphi(n)$ a koeficienty leží v $\mathbf{K}^{(n)}$.

Věta 5.2. *Nechť $\mathbf{K}$ je těleso charakteristiky p, $n > 0$ je celé číslo nesoudělné s p. Pak platí*

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

(2) *koeficienty $Q_n(x)$ leží v prvotělese tělesa $\mathbf{K}$. Je-li $p = 0$, pak koeficienty $Q_n(x)$ jsou celá čísla.*

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

Důkaz. (1) Libovolný prvek $\xi \in \mathbf{E}^{(n)}$ je primitivní d-tá odmocnina z 1 pro nějaké $d|n$. Je tomu tak proto, že každý prvek $\xi \in \mathbf{E}^{(n)}$ má řád d pro nějaké $d|n$, platí tedy $\xi^d - 1 = 0$. Tedy ξ je d-tá odmocnina z 1 a je primitivní. Takže platí $x - \xi$ dělí $Q_d(x)$ a proto $x^n - 1 = \prod_{d|n} Q_d(x)$.

(2) Budeme postupovat indukcí dle n. Platí,že $Q_1(x) = x - 1$ má koeficienty v prvotělese tělesa $\mathbf{K}$. Nechť tvrzení platí pro všechna $d < n$. Pak z rovnosti $x^n - 1 = \prod_{d|n} Q_d(x)$ spočteme

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

Čitatel i jmenovatel zlomku mají koeficienty v prvotělese tělesa $\mathbf{K}$. Pomocí dělení polynomů se zbytkem dostaneme, že i $Q_n(x)$ má koeficienty v prvotělese tělesa $\mathbf{K}$.

V případě $p = 0$ jsou koeficienty $Q_1(x)$ celočíselné. Indukční předpoklad je, že koeficienty $Q_d(x)$ jsou celočíselné pro každé $d < n$. Z rovnosti

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

pak vyplývá pomocí indukčního předpokladu, že také koeficienty $Q_n(x)$ celočíselné, neboť každý polynom $Q_d(x)$ pro $d < n$ je monický a v procesu dělení se zbytkem jsou všechny koeficienty stále celočíselné.

□

Poznámka. Ve Větě 5.2 (1), je-li $\mathrm{char}\ \mathbf{K} = 0$, pak je to rozklad na ireducibilní činitele, tj. všechny plynomy $Q_d(x)$ jsou ireducibilní nad $\mathbf{K}$. V tělese nenulové charakteristiky to tak být nemusí.

Příklad. Spočtěte $Q_r(x)$ pro r prvočíslo.

Podle Věty 5.2 (1) dostáváme $x^r - 1 = Q_1(x) \cdot Q_r(x)$. Víme, že $Q_1(x) = x - 1$. Tedy

$$Q_r(x) = \frac{x^r - 1}{x - 1} = x^{r-1} + x^{r-2} + \ldots + x + 1$$

Příklad. Spočtěte $Q_{r^k}(x)$ pro r prvočíslo a k nezáporné celé číslo.

Protože r je prvočíslo, všechny dělitelé r^k jsou $r^0 = 1, r^1 = r, r^2, r^3, \ldots, r^{k-1}, r^k$. Podle Věty 5.2 (1) tedy platí

$$x^{r^k} - 1 = Q_1(x) \cdot Q_r(x) \cdot Q_{r^2}(x) \cdot \ldots \cdot Q_{r^{k-1}}(x) \cdot Q_{r^k}(x)$$

Všimněme si, že platí $x^{r^{k-1}} - 1 = Q_1(x) \cdot Q_r(x) \cdot Q_{r^2}(x) \cdot \ldots \cdot Q_{r^{k-1}}(x)$. Tedy

$$Q_{r^k}(x) = \frac{x^{r^k} - 1}{x^{r^{k-1}} - 1} = x^{(r-1).r^{k-1}} + x^{(r-2).r^{k-1}} + \ldots + x^{r^{k-1}} + 1$$

Věta 5.3. *n-té cyklotomické rozšíření tělesa $\mathbf{K}$ je jednoduchým algebraickým rozšířením tělesa $\mathbf{K}$ určeným vhodným ireducibilním polynomem z $\mathbf{K}[x]$.*

Nechť $\mathbf{K} = \mathbf{F}_q$ a $\mathrm{NSD}(q, n) = 1$. Potom se $Q_n(x)$ rozkládá na součin $\frac{\varphi(n)}{d}$ různých monických ireducibilních polynomů téhož stupně d, $\mathbf{K}^{(n)}$ je rozkladové rozšíření tělesa $\mathbf{K}$ určené libovolným ireducibilním faktorem Q_n v $\mathbf{K}[x]$ a $\dim_{\mathbf{K}} \mathbf{K}^{(n)} = d$, kde d je nejmenší kladné přirozené číslo takové, že $q^d \equiv 1 \bmod n$.

Důkaz. Pokud $\mathrm{char}\ \mathbf{K} \nmid n$, vezměme primitivní n-tou odmocninu z 1 a označme ji ξ. Nejmenší podtěleso $\mathbf{K}^{(n)}$ obsahující $\mathbf{K}$ a ξ musí obsahovat všechny prvky $\{1, \xi, \xi^2 \ldots, \xi^{n-1}\}$. Ty jsou navzájem různé a tvoří všechny kořeny polynomu $x^n - 1$. Tedy polynom $x^n - 1$ se rozkládá na součin lineárních činitelů nad nejmenším podtělesem tělesa $\mathbf{K}^{(n)}$ obsahujícím $\mathbf{K}$ a ξ. Protože $\mathbf{K}^{(n)}$ je rozkladové rozšíření $\mathbf{K}$ určené polynomem $x^n - 1$, platí, že $\mathbf{K}^{(n)}$ je nejmenší podtěleso $\mathbf{K}^{(n)}$ obsahující $\mathbf{K}$ a ξ. Vezměme minimální polynom prvku ξ nad $\mathbf{K}$ a označme jej f. Potom $\mathbf{K}^{(n)}$ je kořenovým rozšířením $\mathbf{K}$ určeným f.

Pokud $p = \mathrm{char}\ \mathbf{K} \mid n$, vezmeme rozklad $n = m \cdot p^l$, kde $p \nmid m$. Pak $\mathbf{K}^{(n)} = \mathbf{K}^{(m)}$, $\mathrm{char}\ \mathbf{K} \nmid m$ a $\mathbf{K}^{(m)}$ je jednoduché algebraické rozšíření $\mathbf{K}$ určené vhodným polynomem podle předchozího odstavce.

Zbývá dokázat druhou část věty. Nechť $\mathbf{K} = \mathbf{F}_q$ a $\mathrm{NSD}(q, n) = 1$. Buď ξ primitivní n-tá odmocnina z 1. Prvek ξ leží v tělese $\mathbf{F}_{q^k}$ právě tehdy, když platí $\xi^{q^k - 1} = 1$, což je ekvivalentní $n | q^k - 1$, tedy $q^k \equiv 1 \bmod n$. Nechť d je nejmenší $k > 0$, pro které to platí. Pak platí $\xi \in \mathbf{F}_{q^d}$ a neleží v žádném vlastním podtělese $\mathbf{F}_{q^d}$. Tedy minimální polynom ξ nad $\mathbf{F}_q$ má stupeň d. Minimální polynom ξ nad $\mathbf{F}_q$ je ireducibilní nad $\mathbf{F}_q$. Protože to platí pro libovolnou primitivní n-tou odmocninu z 1 nad $\mathbf{F}_q$, rozkládá se $Q_n(x)$ na součin ireducibilních polynomů stupně d a těch je $\frac{\varphi(n)}{d}$. □

Příklad. Buď $\mathbf{K} = \mathbf{F}_{11}$. Spočtěte $Q_{12}(x)$. Dále spočtěte nejmenší d, pro které platí $11^d \equiv 1 \bmod 12$.

Podle Věty 5.2 platí

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

Z Věty 5.2 taktéž víme, že $Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_6(x) = x^6 - 1$ a $Q_4 = x^2 + 1$. Tedy $x^{12} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_6(x) \cdot Q_4(x) \cdot Q_{12}(x) = (x^6 - 1)(x^2 + 1) \cdot Q_{12}(x) =$

$(x^8 + x^6 - x^2 - 1) \cdot Q_{12}(x)$ a proto

$$Q_{12}(x) = \frac{x^{12} - 1}{x^8 + x^6 - x^2 - 1} = x^4 - x^2 + 1$$

Hledané d spočteme podle Věty 5.3. Platí $\mathrm{NSD}(11, 12) = 1$ a podle Věty 5.3 se $Q_{12}(x)$ rozkládá na součin $\frac{\varphi(12)}{d}$ různých monických polynomů téhož stupně d. Platí $Q_{12}(x) = x^4 - x^2 + 1 = (x^2 + 5x + 1)(x^2 - 5x + 1)$. Jelikož $Q_{12}(x)$ se rozkládá na 2 polynomy stupně 2, je $d = 2$. Platí taky $d = \frac{\varphi(12)}{2} = \frac{4}{2} = 2$. Tedy $\mathbf{F}_{11}^{(12)} = \mathbf{F}_{11^2}$.