KONEČNÁ TĚLESA

LIBOR BARTO, JÍŘÍ TŮMA

Obsah

1. Úvod

1.1. Definice tělesa a příklady.

Definice. *Těleso* $\mathbf{F}$ je množina se dvěma operacemi $+$, $\cdot$, splňující axiomy:

(A1) $a+(b+c)=(a+b)+c$ pro libovolné $a,b,c\in\mathbf{F}$
(A2) $a+b=b+a$ pro libovolné $a,b\in\mathbf{F}$
(A3) existuje $0\in\mathbf{F}$ tak, že pro všechna $a\in\mathbf{F}$ platí $a+0=0+a=a$
(A4) pro všechna $a\in\mathbf{F}$ existuje $-a\in\mathbf{F}$ tak, že platí $a+(-a)=(-a)+a=0$
(M1) $a\cdot(b\cdot c)=(a\cdot b)\cdot c$ pro všechna $a,b,c\in\mathbf{F}$
(M2) $a\cdot b=b\cdot a$ pro všechna $a,b\in\mathbf{F}$
(M3) existuje $1\in\mathbf{F}$ tak, že pro všechna $a\in\mathbf{F}$ platí $1\cdot a=a\cdot 1=a$
(M4) pro všechna $a\neq 0$ existuje $a^{-1}\in\mathbf{F}$ tak, že platí $a\cdot a^{-1}=a^{-1}\cdot a=1$
(D) $a\cdot(b+c)=a\cdot b+a\cdot c$ pro všechna $a,b,c\in\mathbf{F}$ (distributivita)
(N) $0\neq 1$ (netrivialita)

Je-li $\mathbf{F}$ konečná množina, pak $\mathbf{F}$ je konečné těleso. Těleso $\mathbf{K}$ nazýváme *podtělesem* tělesa $\mathbf{F}$, pokud $\mathbf{K}$ podmnožinou $\mathbf{F}$ a operace $+$ a $\cdot$ se v tělesech $\mathbf{K}$ a $\mathbf{F}$ shodují. Značíme $\mathbf{K}\leq\mathbf{F}$. Rovněž říkáme, že $\mathbf{F}$ je rozšíření tělesa $\mathbf{E}$.

Příklady.

- Množina racionálních čísel $\mathbb{Q}$, množina reálných čísel $\mathbb{R}$ a množina komplexních čísel $\mathbb{C}$ s běžnými operacemi sčítání a násobení jsou tělesa. Platí $\mathbb{Q}\leq\mathbb{R}\leq\mathbb{C}$.
- Množina celých čísel $\mathbb{Z}$ s běžnými operacemi těleso netvoří. Například k prvku 2 neexistuje inverzní prvek, tedy není splněn axiom (M4).
- Množina $\mathbb{Z}_p=\{0,1,\dots,p-1\}$, kde p je prvočíslo, s operacemi sčítání a násobení modulo p je tělesem. Ověřit všechny axiomy až na (M4) je snadné. Inverzní prvky lze hledat rozšířeným Euklidovým algoritmem, viz níže. Neplatí $\mathbb{Z}_p\leq\mathbb{Q}$ – operace sčítání ani násobení se neshodují.
- Pokud n je složené číslo, množina $\mathbb{Z}_n=\{0,1,\dots,n-1\}$ s operacemi sčítání a násobení modulo n není těleso. Selhává podmínka (M4), například 2 nemá inverzní prvek v $\mathbb{Z}_6$.
- Existuje řada těles mezi $\mathbb{Q}$ a $\mathbb{C}$. Příkladem takového tělesa je

$$\mathbb{Q}(\sqrt{2})=\{a+b\sqrt{2}\mid a,b\in\mathbb{Q}\}.$$

  Přesvěčte se, že tato množina splňuje všechny axiomy tělesa, zejména axiom (M4) (viz cvičení).

Poznámky.

- Součin $a\cdot b$ dvou prvků $a,b\in\mathbf{F}$ často zapisujeme stručně ab. Definujeme $a-b=a+(-b)$, $\frac{a}{b}=ab^{-1}$. Pro operace $+,-,\cdot,/$ platí řada pravidel známých pro racionální nebo reálná čísla. Například pro libovolné $a\in\mathbf{F}$ platí $0a=a$, $(-1)a=-a$, a podobně. Nad libovolným tělesem lze řešit soustavy lineárních rovnic Gaussovou eliminací.
- Součinem dvou nenulových prvků je nenulový prvek. Jinými slovy, množina nenulových prvků je uzavřená na násobení. Z axiomů (M1) – (M4) pak plyne, že množina $F-\{0\}$ s operací $\cdot$ tvoří komutativní grupu, mluvíme o *multiplikativní grupě* tělesa $\mathbf{F}$. Další komutativní grupou „ukrytou“ v tělese je množina F s operací $+$, tzv. *aditivní grupa* tělesa $\mathbf{F}$.

- Pokud jsou splněny všechny axiomy kromě (M2), mluvíme o *nekomutativním tělese*. Příkladem je těleso kvaternionů. Wedderburnova věta říká, že žádné nekomutativní konečné těleso neexistuje. Její důkaz v těchto skriptech nenajdete.

Jak bylo poznamenáno výše, $\mathbb{Z}_p$ spolu s operemi sčítání a násobení modulo p (kde p je prvočíslo) tvoří těleso. Jediné ne zcela zřejmé je dokázat existenci inverzního prvku. Ukážeme hledání inverzních prvků na příkladě. Nechť $p = 19997$ a hledejme inverzní prvek k číslu 16.

Pomocí rozšířeného Eukleidova algoritmu najdeme celá čísla a, b tak, že $a \cdot 16 + b \cdot p = \mathrm{NSD}(16, 19997) = 1$. Číslo $r = a \mod p$ bude hledaný inverzní prvek, protože

$$r \cdot 16 \equiv a \cdot 16 \equiv r \cdot 16 + b \cdot p = 1 \pmod{p},$$

tedy $r \cdot 16 = 1$ v tělese $\mathbb{Z}_p$.

Použitím Eukleidova algoritmu dostáváme:

$$19997 = 1249 \cdot 16 + 13$$
$$16 = 1 \cdot 13 + 3$$
$$13 = 4 \cdot 3 + 1$$

Teď spočteme čísla a a b. Z prvé rovnice dostáváme $13 = 19997 - 1249 \cdot 16$. Z druhé rovnice dostáváme $3 = 16 - 1 \cdot 13$ a po dosazení vyjádření z prvé rovnice dostáváme $3 = 16 - (19997 - 1249 \cdot 16) = 1250 \cdot 16 - 19997$. Z třetí rovnice dostáváme $1 = 13 - 4 \cdot 3$ a po dosazení vyjádření z prvé a druhé rovnice dostáváme $1 = (19997 - 1249 \cdot 16) - 4 \cdot (1250 \cdot 16 - 19997) = -6249 \cdot 16 + 5 \cdot 19997$.

Hledaným číslem je $-6249 \mod 13748 = -6249 + 19997 = 13748$. Inverz k číslu 16 v $\mathbb{Z}_{19997}$ je tedy číslo 13748.

1.2. **Polynomy.** Než na příkladě ukážeme konstrukci jiných konečných těles než je $\mathbb{Z}_p$, připomeňme několik základních faktů o polynomech.

- Polynom nad tělesem $\mathbf{F}$ stupně n je formální výraz tvaru $a_0 + a_1 x + \ldots a_n x^n$, kde $a_0, \ldots, a_n \in \mathbf{F}$, $a_n \neq 0$. Množinu všech polynomů nad tělesem $\mathbf{F}$ značíme $\mathbf{F}[x]$. Stupeň polynomu $f(x) \in \mathbf{F}[x]$ značíme $\deg f(x)$. Polynomy můžeme přirozeným způsobem sčítat, násobit a dělit se zbytkem. Konstantní polynomy nerozlišujeme od prvků $\mathbf{F}$.

  Poznamenejme, že polynomy nelze chápat jako zobrazení $\mathbf{F} \to \mathbf{F}$ výše uvedeného tvaru! Například nad tělesem $\mathbf{Z}_2$ určují polynomy x a x^2 tatáž zobrazení (po dosazení libovolného $a \in \mathbf{Z}_2$ je jejich hodnota stejná, totiž a), ale jedná se o různé polynomy.
- Polynom $f(x) \in \mathbf{F}[x]$ dělí polynom $g(x) \in \mathbf{F}[x]$, pokud existuje polynom $h(x) \in \mathbf{F}[x]$ takový, že $f(x) = g(x)h(x)$. Značíme $f(x) | g(x)$. Platí $f(x) | g(x)$ a zároveň $g(x) | f(x)$, právě tehdy, když existuje $0 \neq a \in \mathbf{F}$, pro něž $f(x) = ag(x)$. Pro libovolné dva polynomy $f(x), g(x) \in \mathbf{F}[x]$ existuje jejich největší společný dělitel (NSD), který je určen jednoznačně až na násobek nenulovým prvkem $\mathbf{F}$. Lze jej spočítat Euklidovým algoritmem. Rozšířený Euklidův algoritmus nám navíc poskytne polynomy $a(x), b(x) \in \mathbf{F}[x]$ takové, že
$$\mathrm{NSD}(f(x), g(x)) = a(x)f(x) + b(x)g(x).$$
- Prvek $a \in \mathbf{F}$ je kořenem polynomu $f(x) \in \mathbf{F}$ (neboli $f(a) = 0$) právě tehdy, když $(x - a) | f(x)$.

- Polynom $f(x) \in \mathbf{F}[x]$ se nazývá *ireducibilní*, nebo též *nerozložitelný*, pokud $\deg f(x) \geq 1$ a $f(x)$ není dělitelný žádným nekonstantním polynomem menšího stupně. Každý polynom lze rozložit na součin ireducibilních. Tento rozklad je jednoznačný až na pořadí činitelů a násobení činitelů prvkem $\mathbf{F}$.
- Ireducibilní polynom nad tělesem $\mathbf{F}$ nemá v $\mathbf{F}$ žádný kořen. Pokud polynom nemá v daném tělese žádný kořen a je stupně nejvýše 3, pak je ireducibilní.
- Kořen α polynomu $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbf{F}[x]$ je vícenásobný právě tehdy, když α je kořenem $f'(x) \in \mathbf{F}[x]$. Zde $f'(x)$ značí formální derivaci $f'(x) = n \cdot a_n x^{n-1} + \cdots + a_1$.

1.3. **Konstrukce konečných těles.** Uvažujme polynom $f(\alpha) = \alpha^3 + \alpha + 1 \in \mathbb{Z}_2[\alpha]$. Množina všech polynomů v proměnné α s koeficienty v $\mathbb{Z}_2$ stupně menšího nebo rovného 2 s operacemi sčítání a násobení modulo $f(\alpha) = \alpha^3 + \alpha + 1$ je těleso. Ověřit všechny axiomy tělesa až na (M4) je snadné.

Inverzní prvky existují v tomto tělese ze stejného důvodu jako v $\mathbb{Z}_p$. Vezměme polynom $\alpha + 1$ a hledejme jeho inverz. Pomocí Eukleidova algoritmu najdeme polynomy $a(\alpha), b(\alpha) \in \mathbb{Z}_2[\alpha]$ takové, aby platilo $a(\alpha) \cdot (x+1) + b(\alpha) \cdot f(\alpha) = NSD(f(\alpha), \alpha + 1) = 1$. Polynom $r(\alpha) = a(\alpha) \mod f(\alpha)$ bude hledaným inverzním prvkem. Vyjde

$$\alpha^3 + \alpha + 1 = (\alpha + 1) \cdot (\alpha^2 + \alpha) + 1$$

Tedy $(\alpha + 1)^{-1} = \alpha^2 + \alpha$.

V postupu jsme potřebovali, aby největší společný dělitel $f(\alpha)$ a $g(\alpha)$ byl 1 pro libovolný nenulový polynom $g(\alpha)$. To nastane právě tehdy, když $f(\alpha)$ je ireducibilní. Pokud bychom zvolili rozložitelný polynom $f(\alpha)$ např. $\alpha^3 + \alpha = \alpha \cdot (\alpha^2 + 1)$, nebyl by splněn axiom (M4) – například prvek α by neměl inverz.

Abychom se vyhnuli nedorozumění, budou polynomy v proměnné α značit prvky tělesa zkonstruovaného podobně jako výše, kdežto polynomy v proměnné x budou "opravdové" polynomy nad nějakým tělesem. Situace bude snad jasnější z následující příkladu. Těleso $\mathbf{E}$ uvažované v předchozích odstavcích má prvky

$$0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1.$$

Výraz $x^{20} + x^3$ lze chápat jako polynom nad $\mathbb{Z}_2$, nebo též jako polynom nad $\mathbf{E}$. Výraz $(1 + \alpha)x^3 + (\alpha^2 + 1)$ je příkladem polynomu nad $\mathbf{E}$. Polynom $x^3 + x + 1$ chápaný jako polynom nad $\mathbf{E}$ má kořen α, protože v tělese $\mathbf{E}$ platí $\alpha^3 + \alpha + 1 = 0$. Polynom $x^3 + x + 1$ má v tělese $\mathbf{E}$ ještě kořeny α^2 a $\alpha^2 + \alpha$ (viz cvičení).

Věta 1.1 (o existenci kořenového rozšíření tělesa $\mathbf{F}$ určeného ireducibilním polynomem)**.** *Nechť $f(x) \in \mathbf{F}[x]$ je polynom stupně n ireducibilní nad $\mathbf{F}$. Pak množina $\mathbf{E}$ všech polynomů z $\mathbf{F}[\alpha]$ stupně menšího než n se sčítáním a násobením modulo $f(\alpha)$ je těleso. Těleso $\mathbf{E}$ budeme značit $\mathbf{F}[\alpha]/(f(\alpha))$.*

Prvek $\alpha \in \mathbf{E}$ je kořenem polynomu $f(x) \in \mathbf{E}[x]$.

Důkaz. Všechny vlastnosti tělesa jsou zřejmé, až na vlastnost (M4). Pro každý polynom $0 \neq g(\alpha) \in \mathbf{F}[\alpha]$ stupně menšího než n platí $\mathrm{NSD}(f(\alpha), g(\alpha)) = 1$, tedy existují polynomy $a(\alpha), b(\alpha) \in \mathbf{F}[\alpha]$ takové, že $a(\alpha)g(\alpha) + b(\alpha)f(\alpha) = 1$. Položme $r(\alpha) = a(\alpha) \mod f(\alpha)$. Polynom $r(\alpha)$ je inverzní ke $g(\alpha)$, protože

$$r(\alpha)g(\alpha) \equiv a(\alpha)g(\alpha) \equiv a(\alpha)g(\alpha) + b(\alpha)f(\alpha) = 1 \pmod{f(\alpha)},$$

neboli $r(\alpha)g(\alpha) = 1$ v $\mathbf{E}$.

Prvek $\alpha \in \mathbf{E}$ je kořenem polynomu $f(x)$, protože $p(\alpha) \equiv 0 \pmod{p(\alpha)}$. □

Příklady.

- Uvažujme $\mathbf{F} = \mathbb{R}$ (těleso reálných čísel) a ireducibilní polynom $f(x) = x^2 + 1$. Prvky tělesa $\mathbf{E} = \mathbb{R}[\alpha]/(f(\alpha))$ jsou polynomy stupně méně než 2, neboli výrazy tvaru $a + b\alpha$, kde $a, b \in \mathbb{R}$. V $\mathbf{E}$ platí $\alpha^2 + 1 = 0$, neboli $\alpha^2 = -1$. V $\mathbf{E}$ tedy počítáme takto:

$$\begin{aligned}(a + b\alpha) + (c + d\alpha) &= (a + c) + (b + d)\alpha,\\ (a + b\alpha) \cdot (c + d\alpha) &= ac + ad\alpha + bc\alpha + bd\alpha^2 = (ac - bd) + (ad + bc)\alpha.\end{aligned}$$

  Vidíme, že jsme zkonstruovali těleso izomorfní tělesu komplexních čísel – $\mathbf{E}$ se od $\mathbb{C}$ liší pouze označením prvků.
- Podobně $\mathbb{Q}[\alpha]/(\alpha^2 - 2)$ je izomorfní tělesu $\mathbb{Q}(\sqrt{2})$.

1.4. **Homomorfismy těles.** V následující definici připomínáme pojem homomorfismu a izomorfismu těles a zavádíme pojmenování pro homomorfismy zachovávající společné podtěleso.

Definice. Nechť $\mathbf{E}, \mathbf{F}$ jsou dvě tělesa. Zobrazení $T : \mathbf{E} \to \mathbf{F}$ je *homomorfismus*, jestliže pro libovolné dva prvky $a, b \in \mathbf{E}$ platí

$$T(a + b) = T(a) + T(b),$$
$$T(a \cdot b) = T(a) \cdot T(b).$$

Bijektivní homomorfismus nazýváme *izomorfismus*. Izomorfismus $T : \mathbf{E} \to \mathbf{E}$ nazývýme *automorfismus*.

Nechť $\mathbf{K}$ je podtěleso těles $\mathbf{E}$ a $\mathbf{F}$. Homomorfismus (izo-, auto-) $T : \mathbf{E} \to \mathbf{F}$ se nazývá $\mathbf{K}$-*homomorfismus* ($\mathbf{K}$-izo-, $\mathbf{K}$-auto-), jestliže pro každé $a \in \mathbf{K}$ platí $\mathbf{T}(a) = a$.

Poznámky.

- Izomorfní tělesa se liší pouze přejmenováním prvků.
- Každý homomorfismus je buď triviální, tzn. $T(e) = 0$ pro každé $e \in \mathbf{E}$, nebo je prostý a zachovává operace $0, 1, -$ (unární i binární), $^{-1}, /$, tzn. $T(0) = 0$, $T(1) = 1$, $T(-a) = -T(a)$, $T(a - b) = T(a) - T(b)$, $T(a^{-1}) = [T(a)]^{-1}$, $T(a/b) = T(a)/T(b)$.

Příklad. Zobrazení $U : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ definované předpisem $U(a + b\sqrt{2}) = a - b\sqrt{2}$ je $\mathbb{Q}$-automorfismus (viz cvičení).

1.5. **Charakteristika tělesa, prvotěleso.**

Definice. Nechť $\mathbf{F}$ je těleso. Nejmenší přirozené číslo n, pro které platí

$$\underbrace{1 + 1 + \ldots + 1}_{n} = 0,$$

se nazývá *charakteristika* $\mathbf{F}$.

Pokud žádné takové n neexistuje, pak říkáme, že $\mathbf{F}$ má charakteristiku 0.

Charakteristiku tělesa $\mathbf{F}$ značíme char $\mathbf{F}$

Poznámka. Charakteristika libovolného tělesa je buď 0 nebo prvočíslo. Konečné těleso má vždy nenulovou charakteristiku.

Definice. Nejmenší podtěleso $\mathbf{K}$ tělesa $\mathbf{F}$ se nazývá *prvotěleso* tělesa $\mathbf{F}$.

Poznámka. Prvotěleso je izomorfní $\mathbb{Q}$ nebo $\mathbb{Z}_p$. To závisí na charakteristice $\mathbf{F}$:

(1) Nechť charakteristika $\mathbf{F}$ je rovna prvočíslu $p \geq 2$. V prvotělese leží prvky $0, 1, 1+1, 1+1+1, \ldots, \underbrace{1+1+\ldots+1}_{p-1}$. Snadno nahlédneme, že tyto prvky jsou navzájem různé. Označíme-li $\underbrace{1+1+\ldots+1}_{k} = k.1$, pak zřejmě $k.1 + l.1 = (k+l).1 = ((k+l) \mod p).1$ a $(k.1) \cdot (l.1) = (kl).1 = (kl \mod p).1$. Zobrazení $U : \mathbb{Z}_p \to \mathbf{K}$ definované $U(a) = a \cdot 1$ je tedy izomorfismus.
(2) Je-li charakteristika $\mathbf{F}$ rovna 0, pak prvotěleso v $\mathbf{F}$ je izomorfní s tělesem $\mathbb{Q}$ (viz cvičení).

1.6. **Cvičení.**

(1) Spočtěte 13^{-1} v $\mathbb{Z}_{101}$.
(2) Ověřte, že $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in Q\}$ s běžnými operacemi sčítání a násobení tvoří těleso.
(3) Najděte nejmenší podtěleso tělesa $\mathbb{R}$, které obsahuje $\sqrt[3]{2}$. Toto těleso značíme $\mathbb{Q}(\sqrt[3]{2})$.
(4) Najděte nejmenší podtěleso tělesa $\mathbb{R}$, které obsahuje $\sqrt{2}$ a zároveň $\sqrt{3}$. Toto těleso značíme $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.
(5) Najděte všechny ireducibilní polynomy stupně 1, 2, 3 a 4 nad $\mathbb{Z}_2$.
(6) Spočítejte součin všech ireducibilních polynomů stupně 1, 2 a 4 nad $\mathbb{Z}_2$.
(7) Spočtěte α^{40} v tělese $\mathbb{Z}_2[\alpha]/(\alpha^6 + \alpha^5 + 1)$.
(8) Ukažte, že polynom $f(x) = x^3 + x + 1$ má v tělese $\mathbb{Z}_2[\alpha]/(f(\alpha))$ kořeny α, α^2 a $\alpha^2 + \alpha$.
(9) Najděte všechny kořeny polynomu $f(x) = x^3 + 2x + 1$ v tělese $\mathbb{Z}_3[\alpha]/(f(\alpha))$.
(10) Ověřte, že zobrazení $U : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ definované předpisem $U(a + b\sqrt{2}) = a - b\sqrt{2}$ je $\mathbb{Q}$-automorfismus.
(11) Dokažte, že prvotěleso tělesa s nulovou charakteristikou je izomorfní $\mathbb{Q}$.

2. Charakterizace konečných těles

V této kapitole dokážeme, že každé konečné těleso má p^n prvků, kde p je prvočíslo a n přirozené číslo. Pro daná p a n existuje právě jedno těleso (až na izomorfismus), které má p^n prvků.

2.1. **Těleso jako vektorový prostor nad podtělesem.** Důkaz první části je jednoduchý užitím lineární algebry. Všimneme si, že těleso je vektorový prostor nad libovolným svým podtělesem.

Příklady.

- $\mathbb{Q}(\sqrt{2})$ je vektorový prostor nad tělesem $\mathbb{Q}$. Je to prostor dimenze 2, jeho báze je například $1, \sqrt{2}$ – každý prvek $\mathbb{Q}(\sqrt{2})$ můžeme jednoznačným způsobem vyjádřit jako lineární kombinaci prvků 1 a $\sqrt{2}$, tedy jako $a \cdot 1 + b \cdot \sqrt{2}$, kde $a, b \in \mathbb{Q}$. Tento prostor má samozřejmě mnoho jiných bází, například $3 + \sqrt{2}$, $\frac{5}{3} - 3\sqrt{2}$.
- Uvažujme těleso $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ ze cvičení předchozí kapitoly:

  $$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}.$$

  Toto těleso lze chápat jako vektorový prostor nad tělesem $\mathbb{Q}$ – báze je např. $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$, dimenze 4. Těleso $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ je též vektorový prostor nad tělesem $\mathbb{Q}(\sqrt{2})$ dimenze 2 s bází například $1, \sqrt{3}$. Nebo též vektorový prostor dimenze 2 nad $\mathbb{Q}(\sqrt{3})$.

Lemma 2.1. *Nechť $\mathbf{F}$ je konečné těleso a $\mathbf{K}$ je podtěleso $\mathbf{F}$. Pak $|\mathbf{F}| = |\mathbf{K}|^m$ pro nějaké přirozené číslo m.*

Důkaz. Jak bylo řečeno $\mathbf{F}$ je vektorový prostor nad $\mathbf{K}$ (je třeba ověřit axiomy vektorového prostoru). Ten má konečnou dimenzi $m \geq 1$, neboť má pouze konečně mnoho prvků. Každý vektorový prostor dimenze m je izomorfní aritmetickému vektorovému prostoru $\mathbf{K}^m$, tedy $|\mathbf{F}| = |\mathbf{K}|^m$. (Poněkud obšírněji: Zvolíme bázi $b_1, \ldots, b_m$ v $\mathbf{F}$. Každý prvek $c \in \mathbf{F}$ lze jednoznačně vyjádřit ve tvaru $c = a_1 b_1 + a_2 b_2 + \ldots + a_m b_m$, kde $a_1, a_2, \ldots, a_m \in \mathbf{K}$. Takových lineárních kombinací je právě $|\mathbf{K}|^m$.) □

Věta 2.2. *Každé konečné těleso $\mathbf{F}$ má p^k prvků, kde $p = \operatorname{char} \mathbf{F}$ (tedy p je prvočíslo) a k je přirozené číslo.*

Důkaz. Označme $\mathbf{K}$ prvotěleso $\mathbf{F}$. V předchozí kapitole jsme viděli, že $\mathbf{K}$ je izomorfní tělesu $\mathbf{Z}_p$, kde $p = \operatorname{char} \mathbf{F}$, takže z lemma 2.1 vidíme, že $|\mathbf{F}| = |\mathbf{K}|^k = p^k$. □

2.2. **Kořenová rozšíření.** Již dříve jsme využívali značení typu $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, atd. pro nejmenší podtělesa $\mathbb{R}$ obsahující $\mathbb{Q}$ a prvky v závorce. Obecněji:

Definice. Nechť $\mathbf{F}$ je těleso, $\mathbf{K} \leq \mathbf{F}$ a $\alpha_1, \ldots, \alpha_n \in \mathbf{F}$. Nejmenší podtěleso tělesa $\mathbf{F}$ (vzhledem k inkluzi), které obsahuje $\mathbf{K}$ a prvky $\alpha_1, \ldots, \alpha_n$, značíme $\mathbf{K}(\alpha_1, \ldots, \alpha_n)$.

Nechť $f(x)$ je polynom nad tělesem $\mathbf{E}$. Věta 1.1 říká, že existuje rozšíření $\mathbf{F}$ tělesa $\mathbf{E}$, v němž $f(x)$ má alespoň jeden kořen. Toto rozšíření není určeno jednoznačně ze dvou důvodů:

- Tělesa $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ a $\mathbb{R}$ zřejmě nejsou izomorfní, ale ve všech tělesech má polynom $f(x) = x^2 - 2 \in \mathbb{Q}[x]$ kořen. Důvod nejednoznačnosti je zde ten, že $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, $\mathbb{R}$ obsahují „přebytečné“ prvky.

- Polynom $f(x) = (x^2-2)(x^2-3) \in \mathbb{Q}[x]$ má kořen v $\mathbb{Q}(\sqrt{2})$ i $\mathbb{Q}(\sqrt{3})$ a tato tělesa nejsou izomorfní (viz cvičení). Důvod nejednoznačnosti zde spočívá v rozložitelnosti polynomu $f(x)$.

Definice. Nechť $\mathbf{K}$ je těleso a $f(x) \in \mathbf{K}[x]$ ireducibilní polynom. Těleso $\mathbf{E}$ se nazývá *kořenové rozšíření* $\mathbf{K}$ určené polynomem $f(x)$, jestliže

- $\mathbf{K} \leq \mathbf{E}$ (jde tedy opravdu o rozšíření),
- Polynom $f(x) \in \mathbf{E}[x]$ má v $\mathbf{E}$ nějaký kořen θ a
- $\mathbf{K}(\theta) = \mathbf{E}$ (žádné „přebytečné“ prvky).

Příklady.

- Má-li $f(x)$ kořen v $\mathbf{K}$, pak $\mathbf{K}$ je jediné kořenové rozšíření $\mathbf{K}$ určené polynomem $f(x)$.
- $\mathbb{C}$ je kořenové rozšíření $\mathbb{R}$ určené polynomem x^2+1.
- $\mathbb{Q}(\sqrt{2})$ je kořenové rozšíření $\mathbb{Q}$ určené polynomem x^2-2.
- Pro libovolný ireducibilní polynom $f(\alpha)$ nad $\mathbf{K}$ je $\mathbf{K}[\alpha]/(f(\alpha))$ kořenové rozšíření $\mathbf{K}$ určené $f(x)$.

Kořenová rozšíření existují a jsou určena jednoznačně:

Věta 2.3 (O existenci a jednoznačnosti kořenového rozšíření tělesa $\mathbf{K}$ určeného ireducibilním polynomem)**.** *Nechť $\mathbf{K}$ je těleso a $f(x) \in \mathbf{K}[x]$ je polynom ireducibilní nad $\mathbf{K}$. Potom existuje kořenové rozšíření $\mathbf{E}$ tělesa $\mathbf{K}$ určené polynomem $f(x)$. Kořenové rozšíření je určeno jednoznačně až na $\mathbf{K}$-izomorfismus.*

Důkaz. (1) Existence byla dokázána ve větě 1.1: těleso $\mathbf{E} = \mathbf{K}[\alpha]/(f(\alpha))$ je rozšířením tělesa $\mathbf{K}$, polynom $f(x)$ má v $\mathbf{E}$ kořen α a zřejmě $\mathbf{K}(\alpha) = \mathbf{E}$.

(2) Zbývá dokázat jednoznačnost. Nechť $\mathbf{F} \geq \mathbf{K}$ je nějaké kořenové rozšíření $\mathbf{K}$ obsahující kořen θ polynomu $f(x)$. Označme $m = \deg f(x)$. Definujme zobrazení $T : \mathbf{E} \to \mathbf{F}$ předpisem

$$T(b_{m-1}\alpha^{m-1} + \cdots + b_1\alpha + b_0) = b_{m-1}\theta^{m-1} + \ldots + b_1\theta + b_0.$$

Chceme dokázat, že T je $\mathbf{K}$-izomorfismus. Nejprveme si všimneme, že $T(a) = a$ pro libovolné $a \in \mathbf{K}$.

Nyní dokážeme, že T je homomorfismus. Nechť $g(\alpha), h(\alpha) \in \mathbf{E}$ jsou libovolné, $g(\alpha) = b_{m-1}\alpha^{m-1}+\ldots+b_1\alpha+b_0$ a $h(\alpha) = c_{m-1}\alpha^{m-1}+\ldots+c_1\alpha+c_0$. Potom platí

$$T(g(x)) = \sum_{i=0}^{m-1} b_i\theta^i, \qquad T(h(x)) = \sum_{i=0}^{m-1} c_i\theta^i,$$

$$T((g+h)(x)) = \sum_{i=0}^{m-1}(b_i+c_i)\theta^i = \sum_{i=0}^{m-1} b_i\theta^i + \sum_{i=0}^{m-1} c_i\theta^i = \\ = T(f(g)) + T(h(x)).$$

Podobně, využitím $f(\theta) = 0$, dostaneme

$$T(fg(x)) = T(f(x)) \cdot T(g(x)).$$

Protože T je netriviální homomorfismus, je T prostý.

Zbývá dokázat, že T je na $\mathbf{F}$. Im T je podtěleso $\mathbf{F}$ obsahující $\mathbf{K}$ a θ. Protože $\mathbf{K}(\theta) = \mathbf{F}$ ($\mathbf{F}$ je kořenové rozšíření), platí Im $T = \mathbf{F}$.

Mějme nyní $\mathbf{F}, \mathbf{G}$ dvě kořenová rozšíření $\mathbf{K}$ určená polynomem $f(x)$. Dokázali jsme, že existují $\mathbf{K}$-izomorfismy $T : \mathbf{E} \to \mathbf{F}$ a $U : \mathbf{E} \to \mathbf{G}$, takže $UT^{-1} : \mathbf{F} \to \mathbf{G}$ je $\mathbf{K}$-izomorfismus $\mathbf{F} \to \mathbf{G}$.

□

Poznámky.

- Jsou-li $\mathbf{F}$ a $\mathbf{G}$ dvě kořenová rozšíření tělesa $\mathbf{K}$ určená ireducibilním polynomem $f(x) \in \mathbf{K}[x]$ a označíme-li $\theta \in \mathbf{F}$ a $\sigma \in \mathbf{G}$ libovolné kořeny polynomu $f(x)$, pak $\mathbf{K}$-izomorfizmus $V = UT^{-1} : \mathbf{F} \to \mathbf{G}$ z posledního odstavce důkazu předchozí věty má vlastnost
$$V(\theta) = UT^{-1}(\theta) = U(x) = \sigma$$
- Kořenové rozšíření existuje i pro reducibilní polynomy $f(x)$. Stačí vzít kořenové rozšíření libovolného ireducibilního činitele polynomu $f(x)$. Nemusí však být určeno jednoznačně, viz výše.

2.3. **Rozkladová rozšíření.** V této části k danému polynomu $f(x) \in \mathbf{K}[x]$ zkonstruujeme rozšíření $\mathbf{E}$ tělesa $\mathbf{K}$, ve kterém se polynom $f(x) \in \mathbf{E}[x]$ rozkládá na lineární činitele.

Definice. Nechť $\mathbf{K}$ je těleso, $f(x) \in \mathbf{K}[x]$. Rozšíření $\mathbf{E}$ tělesa $\mathbf{K}$ nazýváme *rozkladové rozšíření* tělesa $\mathbf{K}$ určené polynomem $f(x)$, pokud

- $\mathbf{K} \leq \mathbf{E}$,
- Polynom $f(x) \in \mathbf{E}[x]$ se v $\mathbf{E}$ rozkládá na součin lineárních činitelů, neboli $f(x) = (x - \theta_1)(x - \theta_2)\dots(x - \theta_m)$, kde $\theta_1, \dots, \theta_m \in \mathbf{E}$ a
- $\mathbf{K}(\theta_1, \dots, \theta_m) = \mathbf{E}$ (minimalita).

Příklady.

- $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ je rozkladové rozšíření $\mathbb{Q}$ určené polynomem $(x^2 - 2)(x^2 - 3)$.
- $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ není rozkladové rozšíření $\mathbb{Q}$ určené polynomem $(x^2-2)(x^2-3)$, neboť nesplňuje třetí podmínku.
- $\mathbb{Z}_2[\alpha]/(\alpha^3+\alpha+1)$ je rozkladové rozšíření $\mathbb{Z}_2$ určené polynomem x^3+x+1. Rozklad na lineární činitele je
$$x^3 + x + 1 = (x + \alpha)(x + \alpha^2)(x + \alpha^2 + \alpha),$$
viz cvičení v přechozí kapitole.
- Pro libovolný ireducibilní polynom $f(\alpha)$ nad *konečným* tělesem platí, že kořenové rozšíření $\mathbf{K}[\alpha]/(f(\alpha))$ je zároveň rozkladovým rozšířením $\mathbf{K}$ určeným polynomem $f(x)$. To říká věta 3.7. Pro nekonečná tělesa toto tvrzení obecně neplatí. Například $\mathbb{Q}(\sqrt[3]{2})$ je kořenové rozšíření určené polynomem $x^3 - 2 \in \mathbb{Q}[x]$, ale toto rozšíření není rozkladové.

Nyní dokážeme, že rozkladová rozšíření existují a jsou určená jednoznačně.

Věta 2.4 (O existenci a jednoznačnosti rozkladového rozšíření)**.** *Pro každé těleso* $\mathbf{K}$ *a každý polynom* $f(x) \in \mathbf{K}[x]$ *stupně aspoň* 1 *existuje rozkladové rozšíření tělesa* $\mathbf{K}$ *určené polynomem* $f(x)$.

Každá dvě rozkladová rozšíření tělesa $\mathbf{K}$ *určená polynomem* $f(x)$ *jsou* $\mathbf{K}$*-izomorfní.*

Důkaz. (1) Nejprve dokážeme existenci. Nechť $\deg f = n$ a $f(x) = f_1 \cdot f_2 \cdots f_k$ je rozklad polynomu $f(x)$ na součin polynomů ireducibilních v $\mathbf{K}[x]$. Budeme postupovat indukcí podle $n-k$. Je-li $n-k = 0$, jsou všechny polynomy

$f_1, f_2, \dots, f_n$ lineární a těleso $\mathbf{K}$ je rozkladové rozšíření $\mathbf{K}$ určené polynomem $f(x)$.

Nechť $n - k > 0$. Pak aspoň jeden z činitelů $f_i(x)$ má stupeň aspoň 2. Nechť to je $f_1(x)$. Označme $\mathbf{G}$ kořenové rozšíření tělesa $\mathbf{K}$ určené polynomem $f_1(x)$. V $\mathbf{G}[x]$ se $f_1(x)$ rozkládá na součin aspoň dvou ireducibilních polynomů, tedy $f(x)$ se v $\mathbf{G}$ rozkládá na součin alespoň $k+1$ ireducibilních polynomů a stačí využít indukční předpoklad.

Poznámka: Všimněte si, že indukční předpoklad používáme pro jiné těleso, totiž $\mathbf{G}$. Zformulujme pro pořádek tvrzení, které dokazujeme indukcí podle l: Nechť $\mathbf{K}$ je těleso a $f(x) \in \mathbf{K}[x]$ polynom takový, že $\deg f(x) - k \leq l$, kde k je počet ireducibilních činitelů polynomu $f(x)$. Pak existuje rozkladové rozšíření tělesa $\mathbf{K}$ určené polynomem $f(x)$.

Nalezli jsme rozšíření $\mathbf{E}$ tělesa $\mathbf{K}$, ve kterém se polynom rozkládá na lineární činitele, tedy platí $f(x) = (x-\theta_1)\dots(x-\theta_n)$. Z postupu je patrné, že $\mathbf{K}(\theta_1, \dots, \theta_n) = \mathbf{E}$.

(2) Jednoznačnost dokážeme indukcí podle stupně polynomu $f(x)$ (zároveň pro všechna tělesa, jako při důkazu existence). Nechť $\mathbf{E}$ a $\mathbf{F}$ jsou rozkladová rozšíření $\mathbf{K}$ určená polynomem $f(x)$ stupně n. První krok je zřejmý: pokud $n = 1$, pak $\mathbf{K} = \mathbf{E} = \mathbf{F}$.

Nechť $f(x) = f_1(x)\dots f_k(x)$ je ireducibilní rozklad $f(x)$ nad $\mathbf{K}$. Označme α kořen polynomu $f_1(x)$ v tělese $\mathbf{E}$ a β kořen polynomu $f_1(x)$ v tělese $\mathbf{F}$. Tělesa $\mathbf{K}(\alpha) \leq \mathbf{E}$ a $\mathbf{K}(\beta) \leq \mathbf{F}$ jsou rozkladovými tělesy $\mathbf{K}$ určenými polynomem $f_1(x)$, takže podle věty 2.3 existuje $\mathbf{K}$-izomorfismus $T : \mathbf{K}(\alpha) \to \mathbf{K}(\beta)$. Podle poznámky za větou lze T volit tak, že $T(\alpha) = \beta$. Nyní přejmenujeme všechny prvky $a \in \mathbf{K}(\alpha)$ v tělese $\mathbf{E}$ na $T(a)$ a vzniklé těleso označíme $\mathbf{E}'$. Zřejmě existuje $\mathbf{K}$-izomorfismus $U : E \to E'$ (konkrétně $U(a) = T(a)$ pro $a \in \mathbf{K}(\alpha)$ a $U(a) = a$ jinak) a β je kořenem $f_1(x)$ v E', protože $U(\alpha) = T(\alpha) = \beta$. Nyní E' a F jsou rozkladová rozšíření $F(\beta)$ určená polynomem $f(x)/(x-\beta)$, který má stupeň menší než n. Z indukčního předpokladu máme $\mathbf{K}(\beta)$-izomorfismus $V : E' \to F$. Tedy VU je $\mathbf{K}$-izomorfismus $E \to F$.

□

2.4. **Charakterizace.** V této části dokážeme existenci a jednoznačnost konečných těles. Konkrétně ukážeme, že těleso s p^n prvky je izomorfní rozkladovému rozšíření tělesa $\mathbb{Z}_p$ určeného polynomem $x^{p^n} - x$.

Budeme potřebovat dva vzorce na mocnění prvků.

Lemma 2.5. *Nechť $\mathbf{F}$ je těleso charakteristiky $p > 0$. Pak pro libovolné $a, b \in \mathbf{F}$ a libovolné přirozené číslo $k > 0$ platí*

$$(a+b)^{p^k} = a^{p^k} + b^{p^k}$$

Důkaz. Důkaz provedeme indukcí dle k.

(1) Nechť $k = 1$. Podle binomické věty platí $(a+b)^p = a^p + \binom{p}{1}a^{p-1}b + \binom{p}{2}a^{p-2}b^2 + \dots + \binom{p}{p-1}ab^{p-1} + b^p$. Protože $p|\binom{p}{i}$ pro $i \in \{1, 2, \dots, p-1\}$, platí v tělese $\mathbf{F}$, že $\binom{p}{i}.1 = 0$. Tedy také $\binom{p}{i}a^{p-i}b^i = 0$ v $\mathbf{F}$ a proto $(a+b)^p = a^p + b^p$.

(2) Předpokládejme platnost tvrzení pro $k-1$, tedy $(a+b)^{p^{k-1}} = a^{p^{k-1}} + b^{p^{k-1}}$. Potom platí $(a+b)^{p^k} = ((a+b)^{p^{k-1}})^p = (a^{p^{k-1}} + b^{p^{k-1}})^p = a^{p^k} + b^{p^k}$.

□

Lemma 2.6. *Nechť* $\mathbf{F}$ *je konečné těleso s* q *prvky. Potom pro každé* $a \in \mathbf{F}$ *platí* $a^q = a$. *(Neboli* $a^{q-1} = 1$, *tedy* $a^k = a^{k \bmod (q-1)}$ *pro libovolné* $0 \neq a \in \mathbf{F}$ *a celé číslo* k.*)*

Důkaz. Pro $a = 0$ lemma platí, předpokládejme tedy $a \neq 0$. Multiplikativní grupa tělesa $\mathbf{F}$ má $q-1$ prvků. Protože řád libovolného prvku konečné grupy je dělitelem počtu prvků této grupy, platí $a^{q-1} = 1$. □

Příklad. V $\mathbb{Z}_{37}$ platí $10^{362} = 10^{362 \bmod 36} = 10^2 = 28$.

Věta 2.7. *Nechť* $\mathbf{F}$ *je konečné těleso s* q *prvky. Potom platí následující rovnost polynomů z* $\mathbf{F}[x]$*:*

$$x^q - x = \prod_{a \in \mathbf{F}} (x - a)$$

Důkaz. Podle lemma 2.6 platí pro každý prvek $a \in \mathbf{F}$, že $a^q = a$, tedy $a^q - a = 0$. Z toho plyne, že každý prvek $a \in \mathbf{F}$ je kořenem polynomu $x^q - x$, takže $(x-a)|(x^q - x)$. Protože polynomy $x - a$ jsou pro různá $a \in \mathbf{F}$ po dvou nesoudělné, platí také $\prod_{a \in \mathbf{F}}(x-a)|(x^q - x)$.

Oba polynomy mají stupeň q (protože $\mathbf{F}$ má q prvků) a vedoucí člen obou polynomů je x^q. Protože $\prod_{a \in \mathbf{F}}(x-a)|(x^q - x)$, oba polynomy se rovnají. □

Nyní již známe vše potřebné, abychom dokázali základní větu těchto skript.

Věta 2.8 (O existenci a jednoznačnosti konečných těles)**.** *Každé konečné těleso má* p^n *prvků, kde* p *je prvočíslo a* n *je přirozené číslo.*

Pro každé prvočíslo p *a přirozené číslo* n *existuje těleso s* $q = p^n$ *prvky.*

Libovolná dvě tělesa s p^n *prvky jsou izomorfní (a jsou izomorfní rozkladovému rozšíření tělesa* $\mathbb{Z}_p$ *určeného polynomem* $x^q - x \in \mathbb{Z}_p[x]$*).*

Důkaz. Omezení na počet prvků dává věta 2.2.

Nyní dokážeme existenci tělesa s $q = p^n$ prvky. Buď $\mathbf{F}$ rozkladové rozšíření $\mathbb{Z}_p$ určené polynomem $x^q - x \in \mathbb{Z}_p[x]$. Polynom $f(x) := x^q - x$ nemá v $\mathbf{F}$ vícenásobný kořen, protože derivace $(x^q - x)' = q.x^{q-1} - 1 = -1$ nemá žádný kořen. Tedy $x^q - x$ má v $\mathbf{F}$ přesně $q = p^n$ kořenů. Označme $\mathbf{G} = \{a \in \mathbf{F} : a^q = a\}$ množinu všech kořenů $x^q - x$. Ukážeme, že $\mathbf{G}$ je podtěleso $\mathbf{F}$. Pro všechna $a, b \in \mathbf{G}$ platí $(a.b)^q = a^q.b^q = a.b$ a $(a+b)^{p^k} = a^{p^k} + b^{p^k} = a + b$ (viz Lemma 2.5). Tedy $\mathbf{G}$ je podtěleso $\mathbf{F}$, které obsahuje $\mathbb{Z}_p$ a nad kterým se $x^q - x$ rozkládá na součin lineárních činitelů. Protože $\mathbf{F}$ je rozkladové rozšíření tělesa $\mathbb{Z}_p$ určené polynomem $x^q - x$, je $\mathbf{F} = \mathbf{G}$ a $\mathbf{F}$ má tedy q prvků.

Zbývá dokázat jednoznačnost. Nechť $\mathbf{E}$ je těleso s $q = p^n$ prvky. Pak podle věty 2.7 platí $x^q - x = \prod_{a \in \mathbf{F}}(x - a)$. Tedy $\mathbf{E}$ je rozkladové rozšíření $\mathbb{Z}_p$ určené polynomem $x^q - x \in \mathbb{Z}_p$. Podle věty 2.4 jsou libovolná dvě rozkladová rozšíření tělesa $\mathbb{Z}_p$ určená polynomem $x^q - x$ izomorfní. □

Definice. Těleso s q prvky značíme $\mathbf{F}_q$.

Poznámka. Nejsnadněji konečné těleso s p^n prvky zkonstruujeme jako rozkladové rozšíření $\mathbb{Z}_p$ určené ireducibilním polynomem stupně n. Existenci takového polynomu zaručuje věta 3.4.

2.5. **Aplikace.** Samotná existence konečného tělesa s p^n prvky umožňuje zkonstruovat zajímavé kombinatorické objekty, vhodné například k návrhu kódů. Ukážeme si konstrukci navzájem ortogonálních čtverců a projektivních rovin.

Definice. *Latinský čtverec A řádu n* je čtvercová matice typu $n \times n$ obsahující n různých symbolů (obvykle $0, 1, \dots, n-1$) taková, že každý řádek a každý sloupec obsahuje všechny symboly (právě jednou). Symbol v i-tém řádku a j-tém sloupci značíme A_{ij}. Řádky i sloupce budeme číslovat od nuly.

Příklad. Tabulka binární operace libovolné grupy řádu n je latinským čtvercem řádu n.

Definice. Nechť A, B jsou latinské čtverce řádu n. Čtverce A a B se nazývají *kolmé*, pokud pro každou dvojici symbolů a, b existuje řádek i a sloupec j tak, že $A_{ij} = a$ a $B_{ij} = b$.

Kolmost si lze představit takto: Vytvoříme matici C tak, že na pozici ij bude dvojice (A_{ij}, B_{ij}). A a B jsou kolmé právě tehdy, když matice C obsahuje všechny dvojice (právě jednou). Například následující latinské čtverce A a B jsou kolmé.

$$A = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{pmatrix}, \quad C = \begin{pmatrix} (0,0) & (1,1) & (2,2) \\ (1,2) & (2,0) & (0,1) \\ (2,1) & (0,2) & (1,0) \end{pmatrix}.$$

Označme $N(n)$ velikost největší možné množiny po dvou kolmých latinských čtverců řádu n. Předchozí příklad ukazuje, že $N(3) \geq 2$. Platí dokonce $N(3) = 2$:

Tvrzení 2.9. *Pro libovolné n platí $N(n) \leq n - 1$.*

Důkaz. Snadno nahlédneme, že přeznačíme-li libovolně symboly dvou kolmých latinských čtverců, výsledné latinské čtverce zůstanou kolmé. Můžeme tedy předpokládat, že v největší možné množině $\mathcal{K}$ po dvou kolmých latinských čtverců má každý latinský čtverec v nultém řádku symboly v pořadí $0, 1, \dots n-1$.

Prvek na místě 10 nemůže být 0, protože čtverec by nebyl latinský. Máme-li dvě kolmé matice $A, B \in \mathcal{K}$, musí být $A_{10} \neq B_{10}$, jinak by A a B nebyly kolmé – v příslušné matici C by se dvojice (A_{10}, B_{10}) vyskytovala na místě 10 a ještě v nultém řádku. Tedy $\mathcal{K}$ je nejvýše $n-1$ prvková. □

Využitím p^m-prvkového tělesa ukážeme, že $N(p^m) = p^m - 1$. Zda $N(n) = n - 1$ i pro jiná n je velmi těžký otevřený problém:

Hypotéza 2.10. *Nechť $n \geq 2$. Pak $N(n) = n - 1$ právě tehdy, když n je mocnina nějakého prvočísla.*

Pro ilustraci obtížnosti tohoto problému uveďme, že nerovnost $N(10) < 9$ byla dokázána teprve v roce 1989 a přesná hodnota $N(10)$ je dosud neznámá.

Věta 2.11. *Nechť $n = p^m$, kde p je prvočíslo. Pak $N(n) = n - 1$.*

Důkaz. Víme, že existuje n-prvkové těleso $\mathbf{F}_n$. Přeznačíme prvky tak, aby prvky $\mathbf{F}_n$ byly $\{0, 1, \dots, n-1\}$. Pro každý nenulový prvek $x \in \mathbf{F}_n$ uvažujme matici L^x typu $n \times n$, která má na místě ij prvek $xi + j$ (počítáno v $\mathbf{F}_n$). Je snadné ověřit, že pro libovolné $0 \neq x \in \mathbf{F}_n$ je L_x latinský čtverec.

Ukážeme, že L^x je kolmý na L^y pro libovolná nenulová různá $x, y \in \mathbf{F}_n$. Nechť tedy $a, b \in \{0, 1, \dots, n-1\}$. Chceme najít pozici ij tak, že $(L^x)_{ij} = a$ a $(L^y)_{ij} = b$.

Neboli chceme, aby $xi + j = a$ a $yi + j = b$. To je soustava dvou lineárních rovnic o dvou neznámých i, j. Ta má (právě jedno) řešení, například proto, že determinantem soustavy je $x - y \neq 0$. □

Nyní ukážeme konstrukci projektivních rovin pomocí konečných těles.

Definice. Systém L podmožin nějaké množiny P nazýváme *projektivní rovina*, pokud

- Pro libovolné $p_1 \neq p_2 \in P$ existuje právě jedno $l \in L$ takové, že $\{p_1, p_2\} \subseteq l$.
- Pro libovolné $l_1 \neq l_2 \in L$ je množina $l_1 \cap l_2$ jednoprvková.
- Existuje 4-prvková množina $C \subseteq P$, že pro libovolné $l \in L$ platí $|l \cap C| \leq 2$.

Prvky P nazýváme *body*. Prvky L (neboli množiny bodů) nazýváme *přímky*. Výše uvedené podmínky tedy říkají následující:

- Libovolnými dvěma různými body prochází právě jedna přímka.
- Libovolné dvě různé přímky se protínají v právě jednom bodě.
- Existují 4 body takové, že žádné tři z nich neleží na jedné přímce.

V mnoha knihách o kombinatorice lze nalézt následující tvrzení.

Věta 2.12. *Pro libovolnou konečnou projektivní rovinu existuje přirozené číslo $n \geq 2$ (nazývané* řád*) takové, že*

- *Na každé přímce leží právě $n + 1$ bodů. Každým bodem prochází $n + 1$ přímek.*
- *Máme přesně $n^2 + n + 1$ bodů a stejný počet přímek.*

Využitím konečného tělesa s $n = p^m$ prvky zkonstrujeme projektivní rovinu řádu n. Zda existují projektivní roviny jiných řádů je otevřeným problémem – lze ukázat, že existence projektivní roviny řádu n je ekvivalentní s $N(n) = n - 1$.

Věta 2.13. *Nechť $n = p^m$, kde p je prvočíslo. Pak existuje projektivní rovina řádu n.*

Důkaz. Nechť $\mathbf{F}$ je libovolné těleso. Připomeňme, že afinní přímkou v $\mathbf{F}^2$ rozumíme množinu prvků $\mathbf{F}^2$ tvaru

$$\vec{a} + \langle \vec{b} \rangle = \{\vec{a} + t\vec{b} \mid t \in \mathbf{F}\},$$

kde $\vec{a}, \vec{b} \in \mathbf{F}^2$, $\vec{b} \neq (0,0)$. Množinu $\langle \vec{b} \rangle = \{t\vec{b} \mid t \in \mathbf{F}\}$ nazýváme směrem této afinní přímky (směr je vlastně afinní přímka procházející bodem $(0,0)$ – počátkem). Poznamejme, že pro $\mathbf{F} = \mathbb{R}$ tyto pojmy odpovídají intuitivní představě.

Nyní zkonstruujeme projektivní rovinu s množinou bodů P a množinou přímek L. Množina P bude původní množina bodů $\mathbf{F}^2$, ke které přidáme nové body $x_{\langle \vec{b} \rangle}$ – pro každý směr jeden bod. Tyto nové body si lze představit jako „body v nekonečnu“, říká se jim *nevlastní body*.

$$P = \mathbf{F}^2 \cup \{x_{\langle \vec{b} \rangle} \mid (0,0) \neq \vec{b} \in \mathbf{F}^2\}.$$

Ke každé afinní přímce $\vec{a} + \langle \vec{b} \rangle$ přidáme nevlastní bod $x_{\langle \vec{b} \rangle}$ odpovídající jejímu směru. Do L ještě přidáme tzv. *nevlastní přímku*, která je tvořená všemi nevlastními body.

$$L = \{\{(a + \langle \vec{b} \rangle) \cup \{x_{\langle \vec{b} \rangle}\}\} \mid \vec{a}, \vec{b} \in \mathbf{F}^2, \vec{b} \neq (0,0)\} \cup \{\{x_{\langle \vec{b} \rangle} \mid (0,0) \neq b \in \mathbf{F}_2\}\}.$$

Není těžké ukázat, že zkonstruovaný systém L je skutečně projektivní rovinou (viz cvičení). Například dvě rovnoběžné přímky se protnou v nevlastním bodě, který odpovídá jejich společnému směru (pro $\mathbf{F} = \mathbb{R}$ se nabízí představa kolejí, které se přecejen potkají).

Položíme-li $\mathbf{F} = \mathbf{F}_n$ vznikne projektivní rovina řádu n, protože například na přímce $((0,0)+\langle(1,0)\rangle)\cup\{x_{\langle(1,0)\rangle}\}$ leží $n+1$ bodů – n vlastních a jeden nevlastní. □

2.6. **Cvičení.**

(1) Které podtěleso tělesa $\mathbb{C}$ je rozkladovým rozšířením $\mathbb{Q}$ určené polynomem $x^3 - 2$?
(2) Nakreslete 3 navzájem ortogonální latinské čtverce 4×4.
(3) Ověřte, že systém množin zkonstruovaný ve větě 2.13 je skutečně projektivní rovinou (pro libovolné těleso $\mathbf{F}$).
(4) Ověřte, že projektivní rovina zkonstruovaná ve větě 2.13 má skutečně $n^2 + n + 1$ bodů a $n^2 + n + 1$ přímek, na každé přímce leží $n + 1$ bodů a každým bodem prochází $n + 1$ přímek.

3. Struktura konečných těles

3.1. **Podtělesa.**

Věta 3.1 (O podtělesech konečných těles)**.** *Každé podtěleso tělesa* $\mathbf{F}_{p^n}$ *má* p^m *prvků pro nějaké* m*, které dělí* n*.*

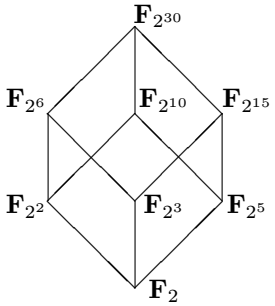
Pro každé $m|n$ *existuje právě jedno podtěleso tělesa* $\mathbf{F}_{p^n}$*, které má* p^m *prvků (a je tvořeno právě prvky* $a \in \mathbf{F}_{p^n}$ *pro něž* $a^{p^m} = a$*).*

Důkaz. Nejprve dokážeme první část věty. Je-li $\mathbf{G}$ podtěleso $\mathbf{F}_{p^n}$, má také charakteristiku p a tedy p^m prvků pro nějaké $m \leq n$. Navíc p^n musí být podle Lemma 2.1 mocninou p^m, čili $m|n$.

Zbývá dokázat druhou část věty. Ukážeme napřed, že z předpokladu $m|n$ plyne, že $(x^{p^m} - x)|(x^{p^n} - x)$, neboli $(x^{p^m-1} - 1)|(x^{p^n-1} - 1)$. Platí $(p^m - 1)|(p^n - 1)$, neboť z $n = k \cdot m$ plyne $(p^{km} - 1) = (p^m - 1)(p^{(k-1)m} + p^{(k-2)m} + \cdots + p^m + 1)$. Pokud $a = b \cdot c$, pak $(x^{bc} - 1) = (x^b - 1)(x^{(c-1)b} + x^{(c-2)b} + \ldots + x^b + 1)$. Tedy $(x^{p^m-1} - 1)|(x^{p^n-1} - 1)$ a tedy $(x^{p^m} - x)|(x^{p^n} - x)$. Protože $x^{p^m} - x$ dělí $x^{p^n} - x$ a polynom $x^{p^n} - x$ se v $\mathbf{F}_{p^n}$ rozkládá na lineární faktory (podle Věty 2.7), rozkládá se i polynom $x^{p^m} - x$ na lineární faktory. Takže $\mathbf{F}_{p^n}$ obsahuje rozkladové rozšíření $\mathbf{F}_p$ určené polynomem $x^{p^m} - x$, což je podle věty 2.8 těleso $\mathbf{F}_{p^m}$. Dvě různá podtělesa mohutnosti p^m by obsahovala dohromady více než p^m kořenů polynomu $x^{p^m} - x$, což nelze. □

Příklad. Podtělesa $\mathbf{F}_{2^{30}}$ jsou $\mathbf{F}_2, \mathbf{F}_{2^2}, \mathbf{F}_{2^3}, \mathbf{F}_{2^5}, \mathbf{F}_{2^6}, \mathbf{F}_{2^{10}}, \mathbf{F}_{2^{15}}, \mathbf{F}_{2^{30}}$.

Pomocí Haaseova diagramu můžeme znázornit, jak jsou obsažena jedno v druhém.



3.2. **Aditivní a multiplikativní grupa.**

Těleso $\mathbf{F}$ určuje dvě grupy – aditivní grupu $(\mathbf{F}, +)$ a multiplikativní grupu $\mathbf{F}^* = (\mathbf{F} - \{0\}, \cdot)$. Struktura aditivní grupy konečného tělesa je patrná z toho, že $\mathbf{F}_{p^n}$ je vektorový prostor nad $\mathbf{F}_p$.

Tvrzení 3.2. *Aditivní grupa tělesa* $\mathbf{F}_q$*, kde* $q = p^n$*, je izomorfní grupě* $(\mathbb{Z}_p, +_{\mathrm{mod}\ p})^n$.

Důkaz. Těleso $\mathbf{F}_{p^n}$ je vektorovým prostorem nad tělesem $\mathbf{F}_p$ dimenze n. Takže $\mathbf{F}_{p^n}$ je jakožto vektorový prostor izomorfní aritmetickému vektorovému prostoru $\mathbf{F}_p^n$. Speciálně, aditivní grupa $\mathbf{F}_{p^n}$ je izomorfní $(\mathbb{Z}_p, +_{\mathrm{mod}\ p})^n$. □

Poněkud obtížnější je odhalit strukturu multiplikativní grupy. Následující tvrzení je jedno z nejdůležitějších v teorii konečných těles.

Věta 3.3. *Multiplikativní grupa* $\mathbf{F}_q^*$ *konečného tělesa* $\mathbf{F}_q$ *je cyklická (tedy izomorfní grupě* $(\mathbb{Z}_{q-1}, +_{\mathrm{mod}\ q-1})$*).*

Důkaz. Položme $h = q-1 = p_1^{r_1} \cdot p_2^{r_2} \cdot \cdots \cdot p_k^{r_k}$. Polynom $x^{h/p_i} - 1$ má v $\mathbf{F}_q$ nejvýše $\frac{h}{p_i} < h$ nenulových kořenů, proto existuje $0 \neq a_i \in \mathbf{F}_q$ (neboli $a_i \in \mathbf{F}_q^*$) takové, že $a_i^{h/p_i} \neq 1$.

Položíme $b_i = a_i^{h/p_i^{r_i}} \neq 1$ a ukážeme, že b_i má řád $p_i^{r_i}$. Platí $b_i^{p_i^{r_i}} = a_i^h = 1$ (neboť řád a_i dělí počet prvků $\mathbf{F}_q^*$, viz též lemma 2.6). Protože $b_i^{p_i^{r_i-1}} = a_i^{h/p_i} \neq 1$, je řád b_i rovný $p_i^{r_i}$.

Položme $b = b_1 b_2 \cdots b_k$. Platí $b^h = 1$ (opět lemma 2.6). Dále pro $i = 1, 2, \ldots, k$ platí $b^{h/p_i} = \prod_{j=1}^k b_j^{h/p_i}$. Je-li $j \neq i$, tak $p_j^{r_j}$ dělí $\frac{h}{p_i}$ a tedy $b_j^{h/p_i} = 1$. Proto $b^{h/p_i} = b_i^{h/p_i} \neq 1$, neboť $p_i^{r_i} \nmid \frac{h}{p_i}$ a $p_i^{r_i}$ je řád b_i. Zjistili jsme, že řád b je rovný h, tedy grupa $\mathbf{F}_q^*$ je cyklická. □

Definice. Libovolný generátor $\mathbf{F}_q^*$ se nazývá *primitivní prvek* $\mathbf{F}_q$.

Poznámky.

- Prvek a je generátorem grupy $(\mathbb{Z}_n, +_{\mathrm{mod}\ n})$ právě tehdy, když čísla a a n jsou nesoudělná. Tedy počet primitivních prvků tělesa $\mathbf{F}_q$ je rovný počtu čísel menších než $q-1$ nesoudělných s $q-1$, t.j. $\varphi(q-1)$, kde φ je Eulerova funkce.
- Nechť $p(x) \in \mathbf{F}[x]$ je ireducibilní polynom. Prvek α nemusí být primitivním prvkem tělesa $\mathbf{F}[\alpha]/(p(\alpha))$. Příklad naleznete ve cvičeních.
- Je-li $\mathbf{F}_q \leq \mathbf{F}_r$ a α primitivní prvek $\mathbf{F}_r$, pak zřejmě $\mathbf{F}_r = \mathbf{F}_q(\alpha)$, protože $\mathbf{F}_q(\alpha)$ obsahuje 0 a všechny mocniny α, t.j. všechny prvky $\mathbf{F}_q$. [1]

3.3. **Minimální polynom.** V této části připomeneme některé základní poznatky o algebraických prvcích a jejich minimálních polynomech.

Definice. Nechť $\mathbf{F} \leq \mathbf{E}$ jsou tělesa. Prvek $\alpha \in \mathbf{E}$ nazýváme *algebraický* nad $\mathbf{F}$, pokud je kořenem nějakého nenulového polynomu nad $\mathbf{F}$ (tedy pokud existuje $p(x) \in \mathbf{F}[x]$ takový, že $p(\alpha) = 0$).

Příklady.

- $\sqrt{2}$ je algebraický prvek nad $\mathbb{Q}$, neboť je kořenem například polynomu x^2-2.
- Prvek π není algebraický nad $\mathbb{Q}$, ale není to snadné dokázat.

Definice. Nechť $\mathbf{F} \leq \mathbf{E}$ jsou tělesa a α je algebraický prvek nad $\mathbf{F}$. Nenulový monický polynom $m(x) \in \mathbf{F}[x]$ nejmenšího stupně takový, že $m(\alpha) = 0$, nazýváme *minimální polynom* prvku α nad $\mathbf{F}$.

Poznámky.

- Polynom $f(x) \in \mathbf{F}[x]$ má kořen α právě tehdy, když $m(x) | f(x)$. Jinak řečeno, polynomy z $\mathbf{F}[x]$, jejichž kořenem je α, jsou právě všechny násobky polynomu $m(x)$. K důkazu netriviální implikace se stačí podívat na NSD polynomů $m(x)$ a $f(x)$.
- Minimální polynom je ireducibilní. Jinak jeden z jeho netriviálních faktorů by měl kořen α a menší stupeň.
- Naopak, je-li $f(x) \in \mathbf{F}[x]$ ireducibilní, pak je $f(x)$ (po vydělení vedoucím koeficientem, aby byl monický) minimálním polynomem libovolného svého kořene. To plyne z předchozích dvou bodů.

[1] Nechť $\mathbf{E} \leq \mathbf{F}$ jsou tělesa. Těleso $\mathbf{F}$ se nazývá jednoduchým rozšířením $\mathbf{E}$, pokud $\mathbf{F} = \mathbf{E}(\alpha)$ pro nějaké $\alpha \in \mathbf{F}$. Poznámka tedy říká, že v případě konečných těles je každé rozšíření jednoduché.

- Dimenze $\mathbf{F}(\alpha)$, chápeme-li toto těleso jako vektorový prostor nad $\mathbf{F}$, je rovna stupni n minimálního polynomu $m(x)$, protože $\mathbf{F}(\alpha)$ je kořenové rozšíření $\mathbf{F}$ určené α a to je podle věty 2.3 izomorfní tělesu $\mathbf{F}[\alpha]/(m(\alpha))$, jež má nad $\mathbf{F}$ dimenzi n.
- Je-li dimenze $\mathbf{E}$ nad $\mathbf{F}$ konečná, řekněme k, pak stupeň n minimálního polynomu dělí k. (Důkaz: Máme posloupnost těles $\mathbf{F} \leq \mathbf{F}(\alpha) \leq \mathbf{E}$. $\mathbf{F}(\alpha)$ má nad $\mathbf{F}$ podle přechozího bodu dimenzi n, čili $\mathbf{F}(\alpha) \cong \mathbf{F}^n$ (izomorfismus vektorových prostorů). $\mathbf{E}$ má nad $\mathbf{F}$ dimenzi k, neboli $\mathbf{E} \cong \mathbf{F}^k$. $\mathbf{E}$ má nad $\mathbf{F}(\alpha)$ rovněž nějakou dimenzi, řekněme l, tedy $\mathbf{E} \cong (\mathbf{F}(\alpha))^l \cong (\mathbf{F}^n)^l \cong \mathbf{F}^{nl}$. Čili $\mathbf{F}^{nl} \cong \mathbf{F}^k$, z čehož plyne $nl = k$.)
- Je-li dimenze $\mathbf{E}$ nad $\mathbf{F}$ konečná, řekněme opět k, je každý prvek $\alpha \in \mathbf{E}$ algebraický. Stačí uvažovat prvky $1, \alpha, \alpha^2, \ldots, \alpha^k$. To je $k+1$ vektorů ve vektorovém prostoru $\mathbf{E}$ nad tělesem $\mathbf{F}$. Tyto prvky jsou lineárně závislé, protože $\mathbf{E}$ má dimenzi k nad $\mathbf{F}$, tedy existují skaláry $a_0, \ldots, a_k \in \mathbf{F}$, alespoň jeden nenulový, takové, že $a_0 + a_1\alpha + \cdots + a_k\alpha^k = 0$. Prvek α je tedy kořenem polynomu $a_0 + a_1x + \cdots + a_kx^k$.

Poslední poznámka rovněž dává návod, jak minimální polynom hledat:

Příklad. Najdeme minimální polynom $m(x)$ prvku $\alpha^2 \in \mathbb{Z}_3[\alpha]/(\alpha^3 + 2\alpha + 1)$ nad $\mathbb{Z}_3$. Polynom $m(x)$ zřejmě nemůže mít stupeň 1, takže má stupeň 3. Hledáme čísla $a_0, \ldots, a_3 \in \mathbb{Z}_3$ taková, že

$$a_0 + a_1\alpha^2 + a_2(\alpha^2)^2 + a_3(\alpha^2)^3 = 0.$$

Minimální polynom má nenulový konstatní člen, protože je ireducibilní. Bez újmy na obecnonsti tedy můžeme předpokládat, že $a_0 = 1$. Po úpravě dostaneme

$$1 + a_1\alpha^2 + a_2(\alpha^2 + 2\alpha) + a_3(\alpha^2 + \alpha + 1) = 0.$$

Srovnáním koeficientů u jednotlivých mocnin α vznikne soustava rovnic

$$\begin{aligned} 0 &= 1 + a_3 \\ 0 &= 2a_2 + a_3 \\ 0 &= a_1 + a_2 + a_3, \end{aligned}$$

která má řešení $a_1 = a_2 = a_3 = 2$. Prvek α^2 je tedy kořenem polynomu $2x^3 + 2x^2 + 2x + 1$. Znormováním (vydělením vedoucím koeficentem) dostáváme minimální polynom $m(x) = x^3 + x^2 + x + 2$.

3.4. **Ireducibilní polynomy.** Nad konečnými tělesy existuje ireducibilní polynom libovolného stupně:

Věta 3.4. *Nechť $\mathbf{F}_q$ je konečné těleso a n je přirozené číslo. Pak existuje ireducibilní polynom $f(x) \in \mathbf{F}_q[x]$ stupně n.*

Důkaz. Nechť α je primitivní prvek $\mathbf{F}_{q^n}$. Minimální polynom $m(x)$ prvku α nad $\mathbf{F}_q$ je ireducibilní a jeho stupeň je, podle jedné z poznámek za definicí minimálního polynomu, roven dimenzi vektorového prostoru $\mathbf{F}_q(\alpha)$ nad $\mathbf{F}_q$. Protože α je primitivní, platí $\mathbf{F}_q(\alpha) = \mathbf{F}_{q^n}$, neboli tato dimenze je n. □

Tvrzení 3.5. *Nechť $f(x) \in \mathbf{F}_q[x]$ je ireducibilní polynom stupně m. Potom platí $f(x) | (x^{q^n} - x)$ právě tehdy, když $m | n$.*

Důkaz. ($\Rightarrow$) Nechť $f(x)|(x^{q^n}-x)$. Polynom $x^{q^n}-x$ se v tělese $\mathbf{F}_{q^n}$ rozkládá na lineární činitele (viz větu 2.7) a tudíž se na lineární faktory v tomto tělese rozkládá i polynom $f(x)$. Speciálně $f(x)$ má v $\mathbf{F}_{q^n}$ má nějaký kořen, řekněme α. Nyní máme posloupnost těles $\mathbf{F}_q \leq \mathbf{F}_q(\alpha) \leq \mathbf{F}_{q^n}$. Těleso $\mathbf{F}_q(\alpha)$ je kořenovým rozšířením $\mathbf{F}_q$ určené polynomem $f(x)$ a tudíž je podle věty o jednoznačnosti kořenového rozšíření izomorfní s $\mathbf{F}_{q^m}$. Podle věty o podtělesech konečných těles platí $m|n$.

($\Leftarrow$) Nechť $m|n$. Pak $\mathbf{F}_{q^m} \leq \mathbf{F}_{q^n}$. Těleso $\mathbf{F}_{q^m}$ je kořenové rozšíření $\mathbf{F}_q$ určené polynomem $f(x)$, tedy obsahuje kořen α polynomu $f(x)$. Protože α je též kořenem polynomu $x^{q^n}-x$ (viz opět větu 2.7) a $f(x)$ je (po vydělení vedoucím koeficientem) minimálním polynomem α nad $\mathbf{F}_q$, platí $f(x)|(x^{q^n}-x)$. □

Důsledek 3.6. *Polynom $x^{q^n}-x$ je roven součinu všech monických ireducibilních polynomů nad $\mathbf{F}_q$, jejichž stupeň dělí n*

Důkaz. V rozkladu polynomu $x^{q^n}-x$ na součin monických ireducibilních polynomů nad $\mathbf{F}_q$ jsou podle předchozí věty všechny monické ireducibilní polynomy nad $\mathbf{F}_q$, jejichž stupeň dělí n. Žádný polynom se v rozkladu nevyskytuje vícekrát, protože polynom $x^{q^n}-x$ nemá ve svém rozkladovém nadtělese (to je $\mathbf{F}_{q^n}$) žádný vícenásobný kořen (věta 2.7). □

Příklad. Polynom $x^{16}-x$ je součinem všech monických ireducibilních polynomů nad $\mathbf{F}_2$ stupně 1, 2 a 4. Je též součinem všech monických ireducibilních polynomů nad $\mathbf{F}_4$ stupně 1 a 2, a také součinem všech monických ireducibilních polynomů nad $\mathbf{F}_{16}$ stupně 1. Poslední pozorování je vlastně věta 2.7 pro $q=16$.

Věta 3.7. *Nechť $f(x)$ je ireducibilní polynom nad $\mathbf{F}_q$ stupně m. Potom $f(x)$ má v $\mathbf{F}_{q^m}$ nějaký kořen α, prvky $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ jsou navzájem různé a tvoří množinu všech kořenů polynomu f.*

Důkaz. Kořenové rozšíření $\mathbf{F}_q$ určené polynomem $f(x)$ má q^m prvků a tedy se rovná $\mathbf{F}_{q^m}$. Je-li $\beta \in \mathbf{F}_{q^m}$ a $f(x) = a_m x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0$, pak

$$\begin{aligned}(f(\beta))^q &= (a_m\beta^m + \ldots + a_1\beta + a_0)^q = \\ &= a_m^q(\beta^m)^q + a_{m-1}^q(\beta^{m-1})^q + \ldots + a_1^q\beta^q + a_0^q = \\ &= a_m(\beta^q)^m + a_{m-1}(\beta^q)^{m-1} + \ldots + a_1\beta^q + a_0 = f(\beta^q),\end{aligned}$$

kde ve výpočtu využíváme Lemmata 2.5 a 2.6.

Je-li tedy $\alpha \in \mathbf{F}_{q^m}$ kořen polynomu $f(x)$, pak také $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ jsou kořeny polynomu $f(x)$.

Zbývá ještě dokázat, že tyto prvky jsou navzájem různé. Pro spor předpokládejme, že $\alpha^{q^i} = \alpha^{q^j}$ pro nějaké $0 \leq i < j \leq m-1$. Umocněním na q^{m-j} dostáváme $(\alpha^{q^i})^{q^{m-j}} = (\alpha^{q^j})^{q^{m-j}}$, tedy $\alpha^{q^{m-j+i}} = \alpha^{q^m} = \alpha$. Tedy α je kořenem polynomu $x^{q^{m-j+i}} - x$. Polynom $f(x)$ je (opět po znormování) minimálním polynomem prvku α, tedy $f(x)|(x^{q^{m-j+i}} - x)$. Podle tvrzení 3.5 platí $m|(m-j+i)$. Ovšem $0 < m-j+i < m$, spor. □

Příklad. Ireducibilní polynom $f(x) = x^3 + x^2 + 1$ má v tělese $\mathbf{F} = \mathbb{Z}_2[\alpha]/(f(\alpha))$ kořen α. Ostatní kořeny jsou α^2 a $\alpha^4 = \alpha^2 + \alpha + 1$. Polynom $f(x)$ se tedy v $\mathbf{F}$ rozkládá na lineární faktory takto:

$$f(x) = (x-\alpha)(x-\alpha^2)(x-(\alpha^2+\alpha)) = (x+\alpha)(x+\alpha^2)(x+\alpha^2+\alpha).$$

Okamžitým důsledkem je, že pro konečná tělesa je kořenové rozšíření libovolného polynomu již jeho rozkladovým rozšířením.

Důsledek 3.8. *Kořenové rozšíření konečného tělesa* $\mathbf{F}$ *určené ireducibilním polynomem* $f(x)$ *je rozkladovým rozšířením* $\mathbf{F}$ *určeným* $f(x)$*. Speciálně,* $\mathbf{F}_{q^m}$ *je rozkladové rozšíření* $\mathbf{F}_q$ *určené libovolným ireducibilním polynomem* $f \in \mathbf{F}_q[x]$ *stupně* m*.*

Definice. Jsou-li $\mathbf{F}_{q^n} \supseteq \mathbf{F}_q$ konečná tělesa a $\alpha \in \mathbf{F}_{q^n}$, pak prvky $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}$ se nazývají *konjugované* k α nad $\mathbf{F}_q$.

Je-li $\mathbf{F}_q$ prvotěleso tělesa $\mathbf{F}_{q^n}$ (neboli q je prvočíslo), pak prvky $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}$ se nazývají *absolutně konjugované* k α nad $\mathbf{F}_q$.

Poznámka. Nechť $m(x)$ je minimální polynom prvku $\alpha \in \mathbf{F}_{q^n}$ nad $\mathbf{F}_q$. Víme, že jeho stupeň d dělí n a jeho kořeny (α,α^q, …, $\alpha^{q^{d-1}}$) jsou navzájem různé a leží v podtělese $\mathbf{F}_{q^d}$ tělesa $\mathbf{F}_{q^n}$. Tedy

$$\underbrace{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{d-1}}}_{\text{navzájem různé}}, \alpha^{q^d} = \alpha, \alpha^{q^{d+1}} = \alpha^q, \ldots, \alpha^{q^{m-1}} = \alpha^{q^{d-1}},$$

a každý z navzájem různých prvků $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{d-1}}$ se opakuje přesně $\frac{n}{d}$-krát. Všimněte si, že platí

$$m(x) = (x - \alpha)(x - \alpha^q) \ldots (x - \alpha^{q^{d-1}}),$$

tedy konjugované prvky můžeme naopak využít pro hledání minimálního polynomu libovolného prvku.

Příklad. Uvažujme těleso $\mathbf{F}_{16} = \mathbb{Z}_2[\alpha]/(\alpha^4 + \alpha + 1)$ a prvek $\beta = \alpha^3 + \alpha \in \mathbf{F}_{16}$. Pak prvky konjugované k β nad $\mathbf{F}_2$ (tedy absolutně konjugované prvky) jsou

$$\beta = \alpha^3 + \alpha, \beta^2 = (\alpha^3 + \alpha)^2 = \alpha^3,$$
$$\beta^4 = (\beta^2)^2 = \alpha^6 = \alpha^3 + \alpha^2, \beta^8 = (\beta^4)^2 = (\alpha^3 + \alpha^2)^2 = \alpha^3 + \alpha^2 + \alpha + 1.$$

Prvky konjugované k β nad $\mathbf{F}_4$ jsou β, β^4.

Minimálním polynomem prvku β nad $\mathbf{F}_2$ je tedy

$$m(x) = (x - (\alpha^3 + \alpha))(x - \alpha^3)(x - (\alpha^3 + \alpha^2))(x - (\alpha^3 + \alpha^2 + \alpha + 1)),$$

což po roznásobení vyjde

$$m(x) = x^4 + x^3 + x^2 + x + 1.$$

Minimálním polynomem prvku β nad $\mathbf{F}_4$ je

$$m(x) = (x - (\alpha^3 + \alpha))(x - (\alpha^3 + \alpha^2)) = x^2 + (\alpha + \alpha^2)x + 1.$$

Prvek $\alpha + \alpha^2$ je skutečně prvkem $\mathbf{F}_4$, protože $(\alpha + \alpha^2)^4 = \alpha + \alpha^2$.

3.5. **Automorfismy.** Mezi automorfismy (symetriemi) konečného tělesa existuje jeden význačný, kterému se říká Frobeniův.

Věta 3.9. *Zobrazení* $\sigma_1 : \mathbf{F}_{p^n} \to \mathbf{F}_{p^n}$ *definované předpisem* $\sigma_1(\alpha) = \alpha^p$ *je automorfismem tělesa* $\mathbf{F}_{p^n}$

Důkaz. Zobrazení σ_1 pro libovolné $\alpha, \beta \in \mathbf{F}_{p^n}$ splňuje $\sigma_1(\alpha + \beta) = \sigma_1(\alpha) + \sigma_1(\beta)$ (podle Lemma 2.5) a $\sigma_1(\alpha \cdot \beta) = \sigma_1(\alpha)\sigma_1(\beta)$ (to je triviální). Zobrazení σ_1 je tedy homomorfismus. Protože σ_1 není nulové zobrazení (např. protože $\sigma_1(1) = 1$), je σ_1 monomorfismus. Prosté zobrazení mezi stejně velkými konečnými množinami je na, tedy σ_1 je automorfismus. □

Definice. Zobrazení σ_1 z předchozí věty se nazývá *Frobeniův automorfismus* tělesa $\mathbf{F}_{p^n}$.

Následující věta ukazuje, jak vypadají všechny automorfismy konečného tělesa.

Věta 3.10. *Zobrazení $\sigma_i : \mathbf{F}_{p^n} \to \mathbf{F}_{p^n}$ pro $i = 0, 1, 2, \ldots, n-1$ definovaná předpisem $\sigma_i = \sigma_1^i$ (neboli $\sigma_i(\alpha) = \alpha^{p^i}$) jsou navzájem různá a tvoří všechny automorfismy $\mathbf{F}_{p^n}$.*

Důkaz. Nechť σ je libovolný automorfismus $\mathbf{F}_{p^n}$. Cheme ukázat, že $\sigma = \sigma_i$ pro nějaké $0 \leq i < n-1$. Vezmeme libovolný primitivní prvek $\beta \in \mathbf{F}_{p^n}$ a $f(x)$ jeho minimální polynom $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ nad $\mathbf{F}_p$. Ukážeme, že i $\sigma(\beta)$ je kořenem f:

$$\begin{aligned} f(\sigma(\beta)) &= a_0 + a_1\sigma(\beta) + a_2(\sigma(\beta))^2 + \cdots + a_n(\sigma(\beta))^n \\ &= \sigma(a_0) + \sigma(a_1)\sigma(\beta) + \sigma(a_2)(\sigma(\beta))^2 + \cdots + \sigma(a_n)(\sigma(\beta))^n \\ &= \sigma(a_0 + a_1\beta + \cdots + a_n\beta^n) = \sigma(0) = 0, \end{aligned}$$

kde v první úpravě jsme využili, že σ je $\mathbf{F}_p$-automorfismus (každý automorfismus zachovává prvotěleso). Podle věty 3.7 je tedy $\sigma(\beta) = \beta^{p^i}$ pro nějaké $0 \leq i < m$. Pak ale $\sigma = \sigma_i$ protože automorfismus je jednoznačně určen obrazem primitivního prvku.

Zbývá ukázat, že automorfismy jsou navzájem různé. To jsme ale viděli v důkazu věty 3.7 – pokud $0 \leq i < j < n$, platí $\beta^{p^i} \neq \beta^{p^j}$, tedy $\sigma_i(\beta) \neq \sigma_j(\beta)$. Tím spíš $\sigma_i \neq \sigma_j$. □

Poznámky.

- Grupa automorfismů tělesa $\mathbf{F}_{p^n}$ je tedy cyklická grupa řádu n. Generátorem je například Frobeniův automorfismus σ_1.
- Připomeňme, že každý automorfismus $\mathbf{F}_{p^n}$ je $\mathbf{F}_p$-automorfismus. Snadno lze ukázat, že $\mathbf{F}_{p^m}$-automorfismy tělesa $\mathbf{F}_{p^n}$ jsou právě $\sigma_0, \sigma_m, \sigma_{2m}, \ldots \sigma_{n-m}$. Buď lze dokazovat stejně jako předchozí větu, nebo se podívat, které automorfismy zachovávají podtěleso $\mathbf{F}_{p^m}$. Grupa $\mathbf{F}_{p^m}$-automorfismů tělesa $\mathbf{F}_{p^n}$ je tedy cyklická grupa řádu $\frac{n}{m}$.
- Všimněte si, že všechny prvky absolutně konjugované k α jsou právě všechny prvky, které získáme aplikací všech automorfismů na α. Podobně, všechny prvky konjukované k $\alpha \in \mathbf{F}_{q^n}$ nad $\mathbf{F}_q$ získáme aplikací všech $\mathbf{F}_q$-automorfismů na α.
- Automorfismus tělesa určuje automorfismy jeho aditivní grupy a multiplikativní grupy. Vzhledem k tomu, že libovolný (grupový) izomorfismus zachovává řády prvků, platí, že prvky konjugované k α mají stejný řád v multiplikativní grupě tělesa. Speciálně, prvky konjugované k primitivnímu prvku jsou primitvní.

3.6. **Maticová reprezentace prvků konečných těles.** V této části ukážeme jak lze prvky konečných těles reprezentovat maticemi tak, že sčítání a násobení prvků tělesa odpovídají běžnému sčítání a násobení matic. Metoda je založená na doprovodné matici polynomu:

Definice. Nechť $f(x) = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} + x^n$ je ireducibilní polynom nad tělesem $\mathbf{F}$. *Doprovodnou maticí* polynomu f rozumíme následující matici A typu

$n \times n$ nad tělesem $\mathbf{F}$:

$$A = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & 0 & \dots & 0 & -a_2 \\ \vdots & \ddots & \ddots & \ddots & \vdots & \\ 0 & \dots & 0 & 1 & 0 & -a_{n-2} \\ 0 & \dots & 0 & 0 & 1 & -a_{n-1} \end{pmatrix}$$

Příklad. Doprovodnou maticí polynomu $f(x) = x^2 + 1 \in \mathbf{F}_3[x]$ je

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$$

Připomeneme pojem dosazení matice do polynomu a Cayley-Hamiltonovu větu z lineární algebry.

Definice. Mějme polynom $g(x) = b_0 + b_1 x + \cdots + b_m x^m$ nad tělesem $\mathbf{F}$ a čtvercovou matici A nad stejným tělesem. Pak definujeme

$$g(A) = b_0 I + b_1 A + \cdots + b_m A^m,$$

kde I je jednotková matice stejného řádu jako A.

Věta 3.11. *Nechť A je čtvercová matice řádu n nad tělesem $\mathbf{F}$ a $p(\lambda) = \det(A - \lambda I)$ její charakteristický polynom. Pak $p(A) = 0$ (kde 0 zde značí nulovou matici řádu n).*

Z předchozí věty vypočteme:

Věta 3.12. *Nechť A je doprovodná matice monického ireducibilního polynomu $f(x) \in \mathbf{F}[x]$. Pak $f(A) = 0$.*

Důkaz. Spočeteme charakteristický polynom matice A:

$$\det(A - \lambda I) = \det \begin{pmatrix} -\lambda & 0 & 0 & \dots & 0 & -a_0 \\ 1 & -\lambda & 0 & \dots & 0 & -a_1 \\ 0 & 1 & -\lambda & \dots & 0 & -a_2 \\ \vdots & \ddots & \ddots & \ddots & \vdots & \\ 0 & \dots & 0 & 1 & -\lambda & -a_{n-2} \\ 0 & \dots & 0 & 0 & 1 & -\lambda - a_{n-1} \end{pmatrix} =$$

$$= \det \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & -a_0 - a_1\lambda - \cdots - a_{n-1}\lambda^{n-1} - \lambda^n = -f(\lambda) \\ 1 & -\lambda & 0 & \dots & 0 & -a_1 \\ 0 & 1 & -\lambda & \dots & 0 & -a_2 \\ \vdots & \ddots & \ddots & \ddots & \vdots & \\ 0 & \dots & 0 & 1 & -\lambda & -a_{n-2} \\ 0 & \dots & 0 & 0 & 1 & -\lambda - a_{n-1} \end{pmatrix} =$$

$$= (-1)^{n+1}(-f(\lambda)) \det \begin{pmatrix} 1 & -\lambda & 0 & \dots & 0 \\ 0 & 1 & -\lambda & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & 1 & -\lambda \\ 0 & \dots & 0 & 0 & 1 \end{pmatrix} = (-1)^n f(\lambda).$$

V první úpravě jsme k prvnímu řádku přičetli λ-násobek 2. řádku, λ^2-násobek 3. řádku, ..., λ^{n-1}-násobek n-tého řádku. V druhé úpravě jsme determinant rozvinuli podle prvního řádku. V třetí úpravě jsme použili skutečnost, že determinant horní trojúhelníkové matice je roven součinu prvků na diagonále.

Věta je nyní důsledkem věty 3.11. □

Snadným důsledkem je následující tvrzení o maticové reprezentaci prvků kořenového rozšíření.

Tvrzení 3.13. *Nechť $f(x)$ je ireducibilní monický polynom nad $\mathbf{F}$ stupně n a A je jeho doprovodná matice. Označme*

$$M = \{g(A) \mid \deg g < n\}.$$

Pak zobrazení $\phi : \mathbf{F}[\alpha]/(f(\alpha)) \to M$ definované pro $g(\alpha) \in \mathbf{F}[\alpha]/(f(\alpha))$ vztahem $\phi(g(\alpha)) = g(A)$ je izomorfismem těles.

Důkaz. Zobrazení ϕ zřejmě zachovává sčítání. Důsledkem věty 3.12 je, že zachovává násobení. Protože ϕ je netriviální, je ϕ prostý homomorfismus. Ale ϕ je zřejmě na, tedy je to izomorfismus. □

Příklad. Pro $f(x) = x^2+1 \in \mathbf{F}_3[x]$ je doprovodná matice $A = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$. Skutečně platí $A^2+I = 0$. Za prvky $\mathbf{F}_9$ lze považovat matice $0, I, 2I, A, A+I, A+2I, 2A, 2A+I, 2A+2I$:

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix}.$$

Je to proto, že zobrazení $\phi : \mathbf{F}_3[\alpha]/(f(\alpha)) \to M$ z předchozího tvrzení (přiřazující prvku $a\alpha + b$ matici $aA + b$) je izomorfismem.

3.7. **Cvičení.**

(1) Nakreslete Hasseův diagram podtěles tělesa $\mathbf{F}_{37^{36}}$.
(2) Určete výčtem prvků podtěleso $\mathbf{F}_4$ tělesa $\mathbb{Z}_2[\alpha]/(\alpha^4 + \alpha^1 + 1)$.
(3) Ukažte, že α není primitivním prvkem tělesa $\mathbf{F} = \mathbb{Z}_3[\alpha]/(\alpha^2 + 1)$. Jaký je řád prvku α? Najděte v tělese $\mathbf{F}$ nějaký primitivní prvek.
(4) Najděte minimální polynom prvku $\sqrt{2} + \sqrt{3}$ nad tělesem $\mathbb{Q}$.
(5) Najděte minimální polynom prvku $\alpha^3 + \alpha^2$ nad tělesem $Z_2[\alpha]/(\alpha^4 + \alpha + 1)$.
(6) Zvolte si nějakou reprezentaci tělesa $\mathbf{F}_4$ a najděte nad tímto tělesem všechny ireducibilní polynomy stupně 1 a 2. Určete předem, kolik jich je.
(7) Najděte nějaký kořen polynomu $f(x) = x^4 + x + 1$ v tělese $\mathbb{Z}_2[\alpha]/(\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1)$. Dopočtěte zbylé kořeny užitím věty 3.7 a rozložte $f(x)$ na lineární činitele.
(8) Reprezentujte maticemi prvky $\mathbf{F}_9$ využitím polynomu $f(x) = x^2 + x + 2 \in \mathbf{F}_3[x]$. Ukažte, že α je primitivním prvkem $\mathbf{F}_3[\alpha]/(p(\alpha))$. Z toho plyne, že maticová reprezentace bude obsahovat matice $0, A, A^2, \ldots, A^8$, kde A je doprovodná matice $f(x)$. Vysvětlete proč.

4. Odmocniny z jedné a cyklotomické polynomy

V této sekci se budeme zabývat polynomy $x^n - 1$ a jeho kořeny – n-tými odmocninami z jedné. Tyto poznatky jsou potřebné např. v počítačové algebře (rychlá Fourierova transformace) a teorii kódů (dělitelé polynomu $x^n - 1$ odpovídají cyklickým kódům.)

Definice. Je-li $\mathbf{K}$ libovolné těleso, pak rozkladové rozšíření $\mathbf{K}$ určené polynomem $x^n - 1 \in \mathbf{K}[x]$ se nazývá *n-té cyklotomické těleso* nad $\mathbf{K}$ a označuje se $\mathbf{K}^{(n)}$. Množina všech kořenů polynomu $x^n - 1$ v $\mathbf{K}^{(n)}$ se značí $\mathbf{E}^{(n)}$, prvky $\mathbf{E}^{(n)}$ nazýváme *odmocniny z jedné*.

Příklad. V případě $\mathbf{K} = \mathbb{Q}$ máme $\mathbf{K}^{(n)} = \mathbb{Q}(e^{\frac{2\pi i}{n}})$ a $\mathbf{E}^{(n)} = \{e^{\frac{2\pi ij}{n}} \mid 0 \leq j < n\}$.

Poznámka. Těleso $\mathbf{F}_{p^n}$ je $(p^n - 1)$-ní cyklotomické rozšíření libovolného svého podtělesa (protože podle věty 2.8 se $x^{p^n-1} - 1$ v $\mathbf{F}_{p_n}$ rozkládá na součin lineárních činitelů a nerozkládá se na součin lineárních činitelů v žádném vlastním podtělese.)

Věta 4.1. *Nechť $n > 0$ a $\mathbf{K}$ je těleso charakteristiky p (připouštíme možnost $p = 0$). Pak platí*

1. *pokud $p \nmid n$, pak $x^n - 1$ má v $\mathbf{K}^{(n)}$ jednoduché kořeny a $\mathbf{E}^{(n)}$ je cyklická podgrupa řádu n multiplikativní grupy $(\mathbf{K}^{(n)})^*$ tělesa $\mathbf{K}^{(n)}$,*
2. *pokud $p|n$ a $n = p^l m$, kde $p \nmid m$, pak $x^n - 1 = (x^m - 1)^{p^l}$. Tedy $\mathbf{K}^{(n)} = \mathbf{K}^{(m)}$ a kořeny polynomu $x^n - 1$ jsou prvky $\mathbf{E}^{(m)}$, každý s násobností p^l.*

Důkaz. (1) Polynom $x^n - 1$ nemá společný kořen s jeho formální derivací $(x^n - 1)' = (n \bmod p)x^{n-1}$, protože $n \bmod p \neq 0$. Tedy $x^n - 1$ nemá žádný vícenásobný kořen a $\mathbf{E}^{(n)}$ obsahuje přesně n prvků.

Zřejmě $1 \in \mathbf{E}^n$. Jsou-li $\xi, \mu \in \mathbf{E}^{(n)}$, pak $(\xi\mu)^n = \xi^n\mu^n = 1$. Je-li $\xi \in \mathbf{E}^{(n)}$, pak $(\xi^{-1})^n = 1.(\xi^{-1})^n = \xi^n.(\xi^{-1})^n = 1^n = 1$. Tedy $\mathbf{E}^{(n)}$ je podgrupa $(\mathbf{K}^{(n)})^*$ (protože $\mathbf{E}^{(n)}$ je konečná, stačilo ověřovat uzavřenost na násobení).

Důkaz cykličnosti $\mathbf{E}^{(n)}$ je obdobný důkazu cykličnosti multiplikativní grupy konečného tělesa (Věta 3.3), proto vynecháme detaily. Nechť $n = p_1^{l_1} \cdot \ldots \cdot p_t^{l_t}$ je rozklad na prvočinitele. Pro každé $i = 1, \ldots, t$ existuje prvek $a_i \in \mathbf{E}^{(n)}$, pro který platí $a_i^{\frac{n}{p_i}} \neq 1$. Potom prvek $b_i = a_i^{\frac{n}{p_i^{l_i}}}$ má řád $p_i^{l_i}$ a $b_1, \ldots, b_t$ je generátor grupy $\mathbf{E}^{(n)}$.

(2) Podle Lemmatu 2.5 platí $(a+b)^{p^l} = a^{p^l} + b^{p^l}$ pro libovolné prvky $\mathbf{K}$. Zcela stejným způsobem se ověří, že vztah $(a(x) + b(x))^{p^l} = a(x)^{p^l} + b(x)^{p^l}$ platí i pro libovolné polynomy $a(x), b(x) \in \mathbf{K}[x]$. Takže $(x^m - 1)^{p^l} = (x^m)^{p^l} + (-1)^{p^l} = x^n + (-1)^{p^l}$. Pokud je p liché dostáváme $x^n - 1$. Pro $p = 2$ dostáváme $x^n + 1 = x^n - 1$.

□

Poznámka. Protože kořeny $x^n - 1$ v $\mathbf{K}^{(n)}$ jsou navzájem různé, platí

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

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

Poznámky.

- Jinými slovy ξ je primitivná n-tá odmocnina z 1, pokud $\xi^n = 1$ a $\xi^d \neq 1$ pro žádné $0 < d < n$.
- Každá n-tá odmocnina z 1 je primitivní d-tou odmocninou z 1 pro jisté $d|n$ (protože řád prvku grupy $\mathbf{E}^{(n)}$ dělí řád grupy $\mathbf{E}^{(n)}$, což je n).
- Je-li ξ generátor $\mathbf{E}^{(n)}$, pak $\mathbf{E}^{(n)} = \{1, \xi, \xi^2, \dots, \xi^{n-1}\}$. 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 $\mathbf{K}$.
- Obecněji, je-li ξ primitivní n-tou odmocninou z 1, je ξ^k primitivní $\frac{n}{\mathrm{NSD}(k,n)}$-tou odmocninou z 1.
- Pro libovolnou primitivní n-tou odmocninu z 1 ξ je zřejmě $\mathbf{K}^{(n)} = \mathbf{K}(\xi)$.

Příklad. Uvažujme $\mathbf{K} = \mathbb{Q}$ a $n = 6$. Primitivní n-té odmocniny z 1 jsou $e^{\frac{\pi i}{3}}$ a $e^{-\frac{\pi i}{3}}$.

Definice. Nechť $\mathbf{K}$ je těleso charakteristiky p, $p \nmid n$. Pak polynom

$$Q_n(x) = \prod_{\xi \text{ je primitivní } n\text{-tá odmocnina z } 1} (x - \xi)$$

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

Poznámka. Nechť ξ je libovolná primitivní n-tá odmocnina z 1. Pak podle předchozí poznámky platí

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

Stupeň polynomu Q_n je $\varphi(n)$.

Příklad. Uvažujme opět $\mathbf{K} = \mathbb{Q}$. Máme

$$\begin{aligned} Q_1(x) &= x - 1 \\ Q_2(x) &= x + 1 \\ Q_4(x) &= (x - i)(x + i) = x^2 + 1 \\ Q_6(x) &= (x - e^{\frac{\pi i}{3}})(x - e^{-\frac{\pi i}{3}}) = x^2 - x + 1 \end{aligned}$$

Věta 4.2. *Nechť $\mathbf{K}$ je těleso charakteristiky p, $p \nmid n > 0$. 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.*

Důkaz. (1) Tvrzení je důsledkem toho, že $x^n - 1 = \prod_{\xi \in \mathbf{E}^{(n)}} (x - \xi)$ a libovolný prvek $\xi \in \mathbf{E}^{(n)}$ je primitivní d-tá odmocnina z 1 pro nějaké $d|n$ (viz poznámky výše).

(2) Budeme postupovat indukcí dle n. Polynom $Q_1(x) = x - 1$ má koeficienty v prvotělese tělesa $\mathbf{K}$. Nechť tvrzení platí pro všechna $d < n$. 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 $\mathbf{K}$. Podílem dvou polynomů s koeficienty v $\mathbf{K}$ je opět polynom s koeficienty v $\mathbf{K}$ (během algoritmu pro dělení polynomů se zbytkem jsou všechny mezivýsledky polynomy nad $\mathbf{K}$).

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

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

a indukčního předpokladu vyplývá, že koeficienty $Q_n(x)$ jsou celočíselné, neboť dělíme-li monický celočíselný polynom monickým celočísleným polynomem, jsou všechny mezivýsledky celočíselnými polynomy.

□

Příklady. V následujících příkladech uvažujeme libovolné těleso $\mathbf{K}$ vhodné charakteristiky (aby byl splněn předpoklad o nesoudělnosti z předchozí věty).

- Spočteme $Q_r(x)$, kde r je prvočíslo. Víme, že $Q_r(x)$ má stupeň $\varphi(r) = r-1$. Z přechozí věty víme, že $x^r - 1 = Q_1(x) \cdot Q_r(x)$. Protože $Q_1(x) = x - 1$, máme
$$Q_r(x) = \frac{x^r - 1}{x - 1} = 1 + x + x^2 + \cdots + x^{r-1}.$$
- Spočteme $Q_{r^k}(x)$, kde r je prvočíslo a k je přirozené číslo. Stupeň musí vyjít $\varphi(r^k) = (r-1)r^{k-1}$. Z předchozí věty dostáváme
$$x^{r^k} - 1 = Q_1(x) \cdot Q_r(x) \cdot Q_{r^2}(x) \cdot \cdots \cdot Q_{r^k}(x),$$
ale také
$$x^{r^{k-1}} - 1 = Q_1(x) \cdot Q_r(x) \cdot \cdots \cdot Q_{r^{k-1}}(x),$$
čili
$$\begin{aligned} x^{r^k} - 1 &= (x^{r^{k-1}} - 1)Q_{r^k}(x) \\ Q_{r^k}(x) &= \frac{x^{r^k} - 1}{x^{r^{k-1}} - 1} \\ Q_{r^k}(x) &= 1 + x^{r^{k-1}} + x^{2r^{k-1}} + \cdots + x^{(r-1)r^{k-1}}. \end{aligned}$$
- Spočteme $Q_{12}(x)$. Při výpočtu využijeme $x^6 - 1 = Q_1(x)Q_2(x)Q_3(x)Q_6(x)$ a vztah pro Q_4 z přechozího cvičení.

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

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

Poznámky.

- Z přechozích příkladů by se mohlo zdát, že koeficienty polynomů jsou vždy 0,1 nebo -1. Není tomu tak, například

$$\begin{aligned} Q_{105}(x) = {} & x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - 2x^{41} - x^{40} - x^{39} + x^{36} + x^{35} + x^{34} \\ & + x^{33} + x^{32} + x^{31} - x^{28} - x^{26} - x^{24} - x^{22} - x^{20} + x^{17} + x^{16} + x^{15} \\ & + x^{14} + x^{13} + x^{12} - x^9 - x^8 - 2x^7 - x^6 - x^5 + x^2 + x + 1. \end{aligned}$$

- Polynom $Q_n(x)$ je stejný pro všechna tělesa $\mathbf{K}$ charakteristiky 0. Vezememe-li koeficienty modulo p vznikne n-tý cyklotomický polynom pro libovolné těleso $\mathbf{K}$ charakteristiky p (důkaz viz cvičení.)
- Pro tělesa charakteristiky 0 je polynom $Q_n(x)$ ireducibilní nad $\mathbb{Q}$. Důkaz lze najít například v ...

Věta 4.3. *Nechť $\mathbf{K} = \mathbf{F}_q$ a $\mathrm{NSD}(q, n) = 1$. Nechť d je nejmenší kladné přirozené číslo takové, že $q^d \equiv 1 \bmod n$. Pak*

- $\mathbf{K}^{(n)} = \mathbf{F}_{q^d}$
- *Polynom $Q_n(x)$ se rozkládá na součin $\frac{\varphi(n)}{d}$ různých monických ireducibilních polynomů téhož stupně d.*

Důkaz. 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 $q^k \equiv 1 \bmod n$. Takže $\xi \in \mathbf{F}_{q^d}$, ξ neleží v žádném vlastním podtělese $\mathbf{F}_{q^d}$ a $\mathbf{K}^{(n)} = \mathbf{K}(\xi) = \mathbf{F}_{q^d}$.

Nechť $f(x)$ je libovolný monický ireducibilní faktor $Q_n(x)$. Označme ξ libovolný kořen $Q_n(x)$ v $\mathbf{K}^{(n)}$. Zřejmě $f(x)$ je minimální polynom ξ nad $\mathbf{F}_q$ a ξ je primitivní n-tá odmocnina z jedné. Stupeň minimálního polynomu je roven dimenzi $\mathbf{K}(\xi)$ jakožto vektorového prostoru nad $\mathbf{K}$. Podle předchozího odstavce je tato dimenze rovna d. Stupeň $Q_n(x)$ je $\varphi(n)$ a $Q_n(x)$ nemá vícenásobné kořeny, takže $Q_n(x)$ se rozkládá na součin $\frac{\varphi(n)}{d}$ různých monických ireducibilních faktorů. □

Poznámka. Číslo d z předchozí věty dělí $\varphi(n)$.

Příklady.

- Uvažujme $\mathbf{K} = \mathbf{F}_5$ a polynom $x^{36} - 1$. Podle věty 4.2 platí

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

  kde polynomy na pravé straně mají stupně pořadě $1, 1, 2, 2, 2, 6, 4, 6, 12$. Z předchozí věty odstáváme, že polynom $Q_3(x)$ je ireducibilní, protože nejmenší d takové, že $5^d \equiv 1 \bmod 3$ je 2; polynom $Q_4(x)$ se rozkládá na lineární faktory, protože $5^1 \equiv 1 \bmod 4$ (skutečně, $Q_4(x) = x^2 + 1 = (x+2)(x-2)$); polynom $Q_6(x)$ je ireducibilní; polynom $Q_9(x)$ je ireducibilní, protože $5^2 \equiv -2 \not\equiv 1 \bmod 9$, $5^3 \equiv -1 \not\equiv 1 \bmod 9$ a hledané nejmenší d dělí $\varphi(9) = 6$; polynom $Q_{12}(x)$ se rozkládá na součin dvou kvadratických ireducibilních polynomů, protože $5^2 \equiv 1 \bmod 12$; polynom $Q_{18}(x)$ je ireducibilní, protože $5^2 \equiv 7 \bmod 18$ a $5^3 \equiv -1 \bmod 18$ a polynom $Q_{36}(x)$ se rozkládá na součin dvou ireducibilních polynomů stupně 6, protože $5^3 \equiv 17 \bmod 36$, $5^2 \equiv 25 \bmod 36$ a $5^6 \equiv 17^2 \equiv 1$. Rovněž jsme zjistili, že $\mathbf{F}_5^{(36)} = \mathbf{F}_{5^6}$.
- Uvažujme $\mathbf{K} = \mathbf{F}_5$ a polynom $x^{12} - 1$. Platí

  $$\begin{aligned} x^{12} - 1 &= Q_1(x)Q_2(x)Q_3(x)Q_4(x)Q_6(x)Q_{12}(x) = \\ &= (x-1)(x+1)(x^2+x+1)(x^2+1)(x^2-x+1)(x^4-x^2+1). \end{aligned}$$

  V předchozím příkladu jsme zjistili, že x^2+1 se dále rozkládá na $(x+2)(x-2)$ a že polynom $Q_{12}(x) = x^4 - x^2 + 1$ má dva ireducibilní faktory stupně 2 (takže $\mathbf{F}_5^{(12)} = \mathbf{F}_{5^2}$). Řešením $x^4 - x^2 + 1 = (x^2 + ax + b)(x^2 + cx + d)$ získáme rozklad $x^4 - x^2 + 1 = (x^2 + 2x - 1)(x^2 - 2x - 1)$. Tedy ireducibilní

rozklad $x^{12}-1$ nad $\mathbf{F}_5$ je

$$x^{12}-1=(x-1)(x+1)(x+2)(x-2)(x^2+x+1)(x^2-x+1)(x^2+2x-1)(x^2-2x-1).$$

Označme α jeden z kořenů x^2+2x-1. Z věty 3.7 víme, že druhým kořenem polynomu x^2+2x-1 je α^5. Polynom $x^2+2x-1=(x-\alpha)(x-\alpha^5)$ je minimálním polynomem α a α^5 nad $\mathbf{F}_5$. Další dvě primitivní 12-té odmociny z 1 jsou α^7 a α^{11} (viz poznámky za Větou 4.1). Jejich minimálním polynomem je nutně x^2-2x-1. Primitivní 6-té odmocniny z 1 jsou α^2 a α^{10}, jejich minimálním polynomem je $Q_6(x)=x^2-2x+1$; primitivní 4-té odmocniny z 1 jsou α^3, α^9 a platí $\{\alpha^3,\alpha^9\}=\{2,-2\}$ (protože $Q_4(x)=(x+2)(x-2)$); primitivní 3-tí odmocniny z 1 jsou α^4, α^8, jejich minimálním polynomem je x^2+2x+1; primitivní druhá odmocnina z 1 je $\alpha^6=-1$; primitivní první odmocina z 1 je $\alpha^0=1$.

- Uvažujme $\mathbf{K}=\mathbf{F}_5$ a polynom $x^{15}-1$. Z věty 4.1 dostáváme $x^{15}-1=(x^3-1)^5$. Z předchozích cvičení víme, že Q_3 je ireducibilní nad $\mathbf{F}_5$, tedy rozklad polynomu $x^{15}-1\in\mathbf{F}_5[x]$ na ireducibilní faktory je

$$x^{15}-1=(x^3-1)^5=(Q_1(x)Q_3(x))^5=(x-1)^5(x^2+x+1)^5.$$

4.1. **Cvičení.**

(1) Spočítejte $Q_{15}(x)$ nad $\mathbb{Q}$.
(2) Rozložte polynom $Q_{15}(x)\in\mathbf{F}_2[x]$ na ireducibilní činitele.
(3) Označme $Q_n(x)$ značí n-tý cyklotomický polynom nad $\mathbb{Q}$ a $R_n(x)$ značí n-tý cyklotomický polynom nad tělesem charakteristiky $p\nmid n$. Dokažte, že koeficienty $R_n(x)$ jsou stejné jako koeficienty $Q_n(x)$ modulo p.
(4) Najděte primitivní deváté odmocniny z 1 v tělese $\mathbf{F}_{19}$.
(5) Nechť $\mathbf{K}$ je libovolné těleso a $n>1$. Dokažte, že polynom $x^{n-1}+x^{n-2}+\cdots+1$ je rozložitelný kdykoliv n je složené.
(6) Najděte nejmenší prvočíslo takové, že $x^{22}+x^{21}+\cdots+1$ je ireducibilní nad $\mathbf{F}_p$.
(7) Najděte nejmenších deset prvočísel p pro něž je $x^{p-1}+x^{p-1}+\cdots+1$ ireducibilní nad $\mathbf{F}_2$.
(8) Dokažte následující vlastnosti cyklotomických polynomů (nad tělesem pro něž polynomy existují)
   - $Q_{mp}(x)=\frac{Q_m(x^p)}{Q_m(x)}$, kde p je prvočíslo a $p\nmid m$.
   - $Q_{mp}(x)=Q_m(x^p)$, kde p je prvočíslo a $p|m$.
   - $Q_{mp^k}(x)=Q_{mp}(x^{p^{k-1}})$, kde p je prvočíslo k,m jsou libovolná přirozená čísla.
   - $Q_{2n}(x)=Q_n(-x)$, kde $n\geq 3$ je liché.
   - $Q_n(0)=1$, kde $n\geq 2$.
   - $Q_n(x^{-1})x^{\phi(n)}=Q_n(x)$, kde $n\geq 2$
   -

$$Q_n(1)=\begin{cases}0 & \text{pokud } n=1,\\ p & \text{pokud } n \text{ je mocnina prvočísla } p,\\ 1 & \text{pokud } n \text{ má dva různé prvočíselné dělitele.}\end{cases}$$

- $$Q_n(-1) = \begin{cases} 0 & \text{pokud } n = 2, \\ -2 & \text{pokud } n = 1, \\ p & \text{pokud } n \text{ je dvojnásobek mocniny prvočísla } p, \\ 1 & \text{jinak.} \end{cases}$$

5. Möbiova inverzní formule

V této části si pomocí Möbiovy inverzní formule vypočteme počet monických ireducibilních polynomů daného stupně nad konečným tělesem $\mathbf{F}_q$, odvodíme vzorec pro součin monických ireducibilních polynomů a vzorec pro n-tý cyklotomický polynom.

Definice. *Möbiova funkce* je zobrazení $\mu : \mathbb{N} \to \{-1, 0, 1\}$ definované předpisem

$$\mu_n = \begin{cases} 1 & \text{pokud } n = 1 \\ (-1)^k & \text{pokud } n \text{ je součin } k \text{ různých prvočísel} \\ 0 & \text{pokud } p^2 | n \text{ pro nějaké prvočíslo p} \end{cases}$$

Jinými slovy, $\mu(n)$ je nenulová, pokud v rozkladu n na prvočísla je každé prvočíslo v první mocnině. V tomto případě je rovna 1, pokud je těchto prvočísel sudý počet a -1 jinak.

Lemma 5.1. *Pro libovolné přirozené číslo n platí*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \textit{pokud } n = 1 \\ 0 & \textit{pokud } n > 1 \end{cases}$$

Důkaz. Pro $n = 1$ je tvrzení zřejmé, předpokládejme tedy $n > 1$ a nechť $n = p_1^{k_1} p_2^{k^2} \dots p_l^{k_l}$ je rozklad n na prvočinitele.

$$\begin{aligned} \sum_{d|n} \mu(d) &= \mu(1) + \sum_{d=p_i} \mu(d) + \sum_{d=p_i p_j, i \neq j} \mu_d + \dots = \\ &= 1 - \binom{l}{1} + \binom{l}{2} - \binom{l}{3} + \dots + (-1)^l \binom{l}{l} = (1-1)^l = 0, \end{aligned}$$

kde předposlední rovnost plyne z binomického vzorce. □

Věta 5.2 (Möbiova inverzní formule)**.** *Nechť $\boldsymbol{G} = (G, +)$ je komutativní grupa a $H, h : \mathbb{N} \to G$ zobrazení. Pak*

$$H(n) = \sum_{d|n} h(d) \qquad \textit{pro všechna } n \in \mathbb{N}$$

právě tehdy, když

$$h(n) = \sum_{d|n} \mu(d) H\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) H(d) \qquad \textit{pro všechna } n \in \mathbb{N}$$

Důkaz. Dokážeme implikaci $\Rightarrow$. Druhou implikaci lze dokázat podobně (viz cvičení). Zřejmě platí $\sum_{d|n} \mu(d) H\left(\frac{n}{d}\right) = \sum_{d|n} \mu(\frac{n}{d}) H(d)$. Dále

$$\begin{aligned} \sum_{d|n} \mu(d) H\left(\frac{n}{d}\right) &= \sum_{d|n} \left(\mu(d) \sum_{c|\frac{n}{d}} h(c) \right) = \sum_{d|n} \sum_{c|\frac{n}{d}} \mu(d) h(c) = \sum_{c|n} \sum_{d|\frac{n}{c}} \mu(d) h(c) = \\ &= \sum_{c|n} \left(h(c) \sum_{d|\frac{n}{c}} \mu(d) \right) = h(n), \end{aligned}$$

kde v poslední úpravě jsme využili předchozí tvrzení. □

Poznámka. Máme-li grupu $\mathbf{G}$ psanou multiplikativně, pak předchozí věta říká, že

$$H(n) = \prod_{d|n} h(d) \quad \text{pro všechna } n \in \mathbb{N}$$

nastane právě tehdy, když

$$h(n) = \prod_{d|n} H\left(\frac{n}{d}\right)^{\mu(d)} = \prod_{d|n} H(d)^{\mu\left(\frac{n}{d}\right)} \quad \text{pro všechna } n \in \mathbb{N}$$

V této kapitole využijeme přechozí větu pro grupu celých čísel s operací sčítání a pro grupu racionálních funkcí (racionální funkce je podíl polynomů) s operací násobení.

5.1. **Součin monických ireducibilních polynomů stupně n nad $\mathbf{F}_q$.** Označme $\mathrm{MIP}_{q,n}(x)$ součin monických ireducibilních polynomů stupně n nad $\mathbf{F}_q$. Podle důsledku 3.6 je $x^{q^n} - x$ součinem všech monických ireducibilních polynomů nad $\mathbf{F}_q$ stupně, který dělí n. Seskupením polynomů podle stupňů dostaneme

$$x^{q^n} - x = \prod_{d|n} \mathrm{MIP}_{q,d}(x).$$

Použijeme Möbiovu invezní formuli pro grupu racionálních funkcí s operací násobení a funkce $H(n) = x^{q^n} - x$, $h(n) = \mathrm{MIP}_{q,d}(x)$. Dostáváme vztah

$$\mathrm{MIP}_{q,n}(x) = \prod_{d|n} \left(x^{q^{\frac{n}{d}}} - x\right)^{\mu(d)}.$$

Příklad. Součin všech monických ireducibilních polynomů stupně 6 nad $\mathbf{F}_2$ je

$$(x^{2^6} - x)^{\mu(1)}(x^{2^3} - x)^{\mu(2)}(x^{2^2} - x)^{\mu(3)}(x^2 - x)^{\mu(6)} = \frac{(x^{64} - x)(x^2 - x)}{(x^8 - x)(x^4 - x)} =$$

$$= \quad x^{54} + \dots$$

5.2. **Počet monických ireducibilních polynomů stupně n nad $\mathbf{F}_q$.** Označíme $\mathrm{PMIP}_{q,n}$ počet monických ireducibilních polynomů stupně n nad $\mathbf{F}_q$. Srovnáním stupňů ve vztahu $x^{q^n} - x = \prod_{d|n} \mathrm{MIP}_{q,d}(x)$ (viz výše) dostáváme

$$q^n = \sum_{d|n} d \cdot \mathrm{PMIP}_{q,d}.$$

Užitím Möbiovy inverzní formule pro grupu celých čísel s operací sčítání a funkce $H(n) = q^n$ a $h(n) = n \cdot \mathrm{PMIP}_{q,n}$ dostáváme

$$n \cdot \mathrm{PMIP}_{q,n} = \sum_{d|n} \mu(d) q^{\frac{n}{d}},$$

neboli

$$\mathrm{PMIP}_{q,n} = \frac{1}{n} \sum_{d|n} \mu(d) q^{\frac{n}{d}}.$$

Příklad. Počet monických ireducibilních polynomů stupně 20 nad $\mathbf{F}_2$ je

$$\frac{1}{20}(\mu(1)2^{20} + \mu(2)2^{10} + \mu(4)2^5 + \mu(5)2^4 + \mu(10)2^2 + \mu(20)2) =$$

$$= \frac{1}{20}(2^{20} - 2^{10} - 2^4 + 2^2) = \frac{1}{20}1047540 = 52377.$$

Poznámka. Odvozený vzorec lze též využít k důkazu, že existuje ireducibilní polynom stupně n: Užitím velmi hrubého odhadu dostáváme

$$\mathrm{PMIP}_{q,n} = \frac{1}{n}\sum_{d|n}\mu(d)q^{\frac{n}{d}} > \frac{1}{n}(q^n - q^{n-1} - q^{n-2} - \cdots - 1) = \frac{1}{n}\left(q^n - \frac{q^n-1}{q-1}\right) > 0.$$

5.3. **Výpočet $Q_n(x)$.** Mějme konečné těleso $\mathbf{F}_q$ a číslo n nesoudělné s q. Z věty 4.2 víme, že

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

Užitím Möbiovy inverzní formule pro grupu racionálních funkcí s operací násobení a funkce $H(n) = x^n - 1$ a $h(n) = Q_n(x)$ dostáváme

$$Q_n(x) = \prod_{d|n}(x^{\frac{n}{d}} - 1)^{\mu(d)}.$$

Příklad.

$$\begin{aligned} Q_{12}(x) &= (x^{12}-1)^{\mu(1)}(x^6-1)^{\mu(2)}(x^4-1)^{\mu(3)}(x^3-1)^{\mu(4)}(x^2-1)^{\mu(6)}(x-1)^{\mu(12)} = \\ &= \frac{(x^{12}-1)(x^2-1)}{(x^6-1)(x^4-1)} = x^4 - x^2 + 1. \end{aligned}$$

5.4. **Cvičení.**

(1) Dokažte, že Möbiova funkce splňuje $\mu(mn) = \mu(m)\mu(n)$, pokud $\mathrm{NSD}(m,n) = 1$.
(2) Dokažte pro libovolné přirozené číslo n rovnost
$$\sum_{d|n}\frac{\mu(d)}{d} = \frac{\phi(n)}{n}.$$
(3) Dokažte, že $\sum_{d|n}\mu(d)\phi(d)$ pro libovolné sudé n.
(4) Dokažte, že $\sum_{d|n}|\mu(d)| = 2^k$, kde k je počet různých prvočíselných dělitelů n.
(5) Dokažte druhou implikaci ve větě 5.2.
(6) Vypočtěte $\mathrm{MIP}_{2,6}(x)$ ze vzorce odvozeného v této kapitole.
(7) Dokažte, že
$$\mathrm{PMIP}_{q,n} \le \frac{1}{n}(q^n - q)$$
s rovností právě tehdy, když n je prvočíslo.
(8) Dokažte, že
$$\mathrm{PMIP}_{q,n} \ge \frac{1}{n}q^n - \frac{q}{n(q-1)}(q^{\frac{n}{2}} - 1).$$
(9) Vypočtěte $Q_{30}(x)$ ze vzorce odvozeného v této kapitole.
(10) Dokažte vlastnosti polynomů $Q_n(x)$ ze cvičení 8 z předchozí kapitoly.

6. Faktorizace polynomů nad konečným tělesem

V této části si ukážeme *Berlekampův algoritmus* na faktorizaci polynomu nad konečným tělesem.

6.1. **Bezčtvercová faktorizace.** Nejprve se naučíme daný polynom rozložit na součin tzv. bezčtvercových polynomů:

Definice. Nechť $\mathbf{F}$ je těleso. Polynom $f(x) \in \mathbf{F}[x]$ nazýváme *bezčtvercový*, pokud f není dělitelný druhou mocninou nějakého nekonstantního polynomu. (Neboli, pokud v rozkladu $f(x) = af_1^{k_1}(x) \dots f_n^{k^n}(x)$, kde $a \in \mathbf{F}$ a $f_i(x)$ jsou monické ireducibilní navzájem nesoudělné, je $k_1 = k_2 = \dots = k_n = 1$.)

Budeme potřebovat následující jednoduché tvrzení.

Tvrzení 6.1. *Nechť $g(x), f(x)$ jsou polynomy nad libovolným tělesem $\mathbf{F}$ a $k \geq 1$ je přirozené číslo. Pokud $g^k(x)|f(x)$, pak $g^{k-1}(x)|f'(x)$, kde $f'(x)$ značí formální derivaci $f(x)$.*

Důkaz. Důkaz je snadný užitím vzorce na derivaci součinu, viz cvičení. □

Spočítáme $f'(x)$ a $d(x) = \mathrm{NSD}(f(x), f'(x))$. Nastane jedna ze tří možností.

- $d(x) = 1$. Pak $f(x)$ je podle Tvrzení 6.1 bezčtvercový.
- $d(x) = f(x)$, neboli $f'(x) = 0$. Pak $f(x) = g^p(x)$ pro jistý polynom $g(x)$, kde p je charakteristika tělesa $\mathbf{F}$ (viz cvičení). Nyní stačí stejným postupem rozložit polynom $g(x)$.
- $0 < \deg d(x) < \deg f(x)$. V tomto případě je

$$f(x) = d(x) \cdot \frac{f(x)}{d(x)}$$

a tento rozklad je netriviální. Navíc $\frac{f(x)}{d(x)}$ je bezčtvercový (plyne z Tvrzení 6.1, viz cvičení), tedy stačí rozložit polynom $d(x)$.

Příklad. Rozložíme polynom $f(x) = x^8 + 2x^6 + x^5 + 2x^3 + x^2 + 2 \in \mathbb{Z}_3[x]$ na součin bezčtvercových polynomů. Spočítáme

$$\begin{aligned} f'(x) &= 2x^7 + 2x^4 + 2x \\ d(x) &= x^6 + x^3 + 1 \\ \frac{f(x)}{d(x)} &= x^2 + 2 \end{aligned}$$

Stačí tedy rozložit polynom $d(x) = x^6 + x^3 + 1$. Protože $d'(x) = 0$, musí platit $d(x) = g(x)^3$ pro jistý polynom $g(x)$. Skutečně, $d(x) = (x^2 + x + 1)^3$. Protože $\mathrm{NSD}(g(x), g'(x)) = 1$, polynom $g(x)$ je bezčtvercový. Tedy hledaný rozklad je

$$f(x) = (x^2 + 2)(x^2 + x + 1)^3.$$

Není to rozklad na ireducibilní činitele (viz cvičení).

6.2. **Rozklad bezčtvercového polynomu - Berlekampův algoritmus.** Nalézt netriviální rozklad bezčtvercového polynomu $f(x)$ nám umožňuje následující tvrzení.

Tvrzení 6.2. *Nechť $f(x) \in \mathbf{F}_q[x]$ je monický bezčtvercový polynom. Nechť $h(x) \in \mathbf{F}_q[x]$ je polynom takový, že $h^q(x) \equiv h(x) \pmod{f(x)}$. Pak*

$$f(x) = \prod_{a \in \mathbf{F}_q} \mathrm{NSD}(f(x), h(x) - a).$$

Důkaz. Zřejmě $\mathrm{NSD}(f(x), h(x) - a) | f$. Protože polynomy $h(x) - a$ a $h(x) - a'$ jsou pro $a \neq a'$ nesoudělné, jsou nesoudělné i polynomy $\mathrm{NSD}(f(x), h(x) - a)$ a $\mathrm{NSD}(f(x), h(x) - a')$. Tedy $\prod_{a \in \mathbf{F}_q} \mathrm{NSD}(f(x), h(x) - a) | f$.

Platí $f(x) | h^q(x) - h(x)$ (protože $h^q(x) \equiv h(x) \pmod{f(x)}$). Z věty 2.7 dostaneme dosazením polynomu $h(x)$ za proměnnou x vztah $h^q(x) - h(x) = \prod_{a \in \mathbf{F}_q} (h(x) - a)$. Takže

$$f | \prod_{a \in \mathbf{F}_q} (h(x) - a).$$

Nechť $f(x) = f_1(x) f_2(x) \dots f_n(x)$ je rozklad f na ireducibilní činitele. Pro libovolné $1 \leq i \leq n$ dostáváme z předchozího vztahu $f_i(x) | (h(x) - b)$ pro nějaké $b \in \mathbf{F}_q$, tedy $f_i(x) | \mathrm{NSD}(f(x), h(x) - b) | \prod_{a \in \mathbf{F}_q} \mathrm{NSD}(f(x), h(x) - a)$. Protože polynomy $f_i(x)$ jsou po dvou nesoudělné (využíváme bezčtvercovost $f(x)$), platí $f(x) = f_1(x) \dots f_n(x) | \prod_{a \in \mathbf{F}_q} \mathrm{NSD}(f(x), h(x) - a)$.

Zjistili jsme, že polynomy $f(x)$ a $\prod_{a \in \mathbf{F}_q} \mathrm{NSD}(f(x), h(x) - a)$ se navzájem dělí. Protože jsou oba monické, jsou stejné. □

Všimněte si, že rozklad polynomu $f(x)$ poskytnutý předchozím tvrzením je netriviální kdykoliv $0 < \deg h(x) < \deg f(x)$. Není samozřejmě ihned jasné, že takový vhodný polynom $h(x)$ vůbec existuje. Další tvrzení nejen dává kladnou odpověď, ale poskytuje mnohem více informací o struktuře těchto vhodných polynomů.

Tvrzení 6.3. *Nechť $f(x) \in \mathbf{F}_q[x]$ je polynom s ireducibilním rozkladem $f(x) = f_1(x) f_2(x) \dots f_n(x)$. Označme*

$$W = \{h(x) \in \mathbf{F}_q[x] \mid \deg h(x) < \deg f(x),\ h^q(x) \equiv h(x) \pmod{f(x)}\}.$$

Pak

- *pro libovolný polynom $h(x) \in W$ a $1 \leq i \leq n$ je $h(x) \bmod f_i(x) \in \mathbf{F}_q$ a*
- *zobrazení $\phi : W \to \mathbf{F}_q^n$*

  $$\phi(h(x)) = (h(x) \bmod f_1(x), h(x) \bmod f_2(x), \dots, h(x) \bmod f_n(x))$$

  je izomorfismem vektorových prostorů.

Množina W je tedy vektorový prostor nad $\mathbf{F}_q$ dimenze n.

Důkaz. V důkazu předchozího tvrzení jsme viděli, že pro libovolný polynom $h(x) \in W$ a $1 \leq i \leq j$ platí $f_i(x) | h(x) - a$ pro nějaké $a \in \mathbf{F}_q$, čili $h(x) \bmod f_i(x) = a \in \mathbf{F}_q$.

Zvolme libovolný vektor $(a_1, \dots, a_n) \in \mathbf{F}_q^n$ a uvažujme soustavu kongruencí $h(x) \equiv a_i \pmod{f_i(x)}$, $1 \leq i \leq n$. Čínská věta o zbytcích zaručuje právě jedno řešení $h(x)$ modulo $f_1(x) f_2(x) \dots f_n(x) = f(x)$. Tedy ϕ je prosté. Protože $h^q(x) \equiv a_i^q = a_i \pmod{f_i(x)}$ (viz Tvrzení 2.6), platí $h^q(x) \equiv h(x) \pmod{f(x)}$ (opět díky jednoznačnosti modulo $f(x)$). Zobrazení ϕ je tedy bijekce. Snadno nahlédneme, že ϕ zachovává sčítání a skalární násobení, tedy W je vektorovým prostorem nad $\mathbf{F}_1$ a ϕ je izomorfismus. □

Zbývá vyřešit otázku, jak prvky W nalézt.

Označme $k = \deg f(x)$. Uvažujme polynom $h(x) = b_0 + b_1x + \cdots + b_{k-1}x^{k-1} \in \mathbf{F}_q[x]$. Zajímá nás, kdy $h^q(x) \equiv h(x) \pmod{f(x)}$, neboli kdy $h^q(x) \bmod f(x) = h(x)$. Užitím Lemma 2.5 (podobně jako v důkazu 4.1 jej používáme pro polynomy) a Lemma 2.6 dostaneme

$$\begin{aligned} h^q &= (b_0 + b_1x + b_2x^2 + \cdots + b_{k-1}x^{k-1})^q = \\ &= b_0^q + (b_1x)^q + (b_2x^2)^q + \cdots + (b_{k-1}x^{k-1})^q = \\ &= b_0 + b_1x^q + b_2x^{2q} + \cdots + b_{k-1}x^{(k-1)q}. \end{aligned}$$

Označíme $s_{i,j}$ koeficient u x^i polynomu $x^{jq} \bmod f(x)$, $0 \le i, j < k$:

$$\begin{aligned} x^0 \bmod f(x) = 1 &= s_{0,0} + s_{1,0}x + \cdots + s_{k-1,0}x^{k-1} \\ x^q \bmod f(x) &= s_{0,1} + s_{1,1}x + \cdots + s_{k-1,1}x^{k-1} \\ \cdots &\quad \cdots \\ x^{(k-1)q} \bmod f(x) &= s_{0,k-1} + s_{1,k-1}x + \cdots + s_{k-1,k-1}x^{k-1} \end{aligned}$$

Nyní máme

$$\begin{aligned} h^q(x) \bmod f(x) &= \left(\sum_{j=0}^{k-1} b_j x^{jq}\right) \bmod f(x) = \sum_{j=0}^{k-1} b_j (x^{jq} \bmod f(x)) = \\ &= \sum_{j=0}^{k-1} \left(b_j \sum_{i=0}^{k-1} s_{i,j} x^i \right) = \\ &= \sum_{i=0}^{k-1} \left(x^i \sum_{j=0}^{k-1} s_{i,j} b_j \right) \end{aligned}$$

Označme $h^q(x) \bmod f(x) = c_0 + c_1x + \ldots c_{k-1}x^{k-1}$. Odvozený vztah lze maticově zapsat takto:

$$\begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{k-1} \end{pmatrix} = S \cdot \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{k-1} \end{pmatrix}, \quad \text{kde} \quad S = \begin{pmatrix} s_{0,0} & s_{0,1} & \cdots & s_{0,k-1} \\ s_{1,0} & s_{1,1} & \cdots & s_{1,k-1} \\ \vdots & \vdots & \ddots & \vdots \\ s_{k-1,0} & s_{k-1,1} & \cdots & s_{k-1,k-1} \end{pmatrix}$$

Rovnost $h^q(x) \bmod f(x) = h(x)$ tedy nastane právě tehdy, když $S(b_0, \ldots b_{k-1})^T = (b_0, \ldots, b_{k-1})^T$, tedy právě tehdy, když $(S - I)(b_0, \ldots, b_{k-1})^T = (0, 0, \ldots, 0)^T$ (I zde značí jednotkovou matici). Odvodili jsme následující tvrzení.

Tvrzení 6.4. *Nechť S je matice $k \times k$, jejíž sloupce jsou koeficenty polynomů $1, x^q \bmod f(x), x^{2q} \bmod f(x), \ldots, x^{(k-1)q} \bmod f(x)$. Pak polynom $h(x) = b_0 + b_1x + \cdots + b_{k-1}x^{k-1}$ leží ve W právě tehdy, když $(b_0, \ldots, b_{k-1})$ je řešením homogenní soustavy rovnic s maticí $S - I$.*

Bázi řešení homogenní soustavy rovnic s maticí $S - I$, tedy bázi prostoru W, získáme Gaussovou eliminací. Dimenze W (=počet prvků báze) je podle Tvrzení 6.3 rovná počtu ireducibilních faktorů polynomu $f(x)$. Všimněte si, že první sloupec matice $S - I$ je nulový, takže vektory $(a, 0, 0, \ldots, 0)$ jsou vždy řešením. Tyto vektory ale odpovídají konstantním polynomům ve W, které nás nezajímají, protože neposkytují netriviální rozklad.

Při rozkladu polynomu bychom tedy mohli postupovat takto:

- Řešením soustavy rovnic s maticí $S-I$ zjistíme počet ireducibilních faktorů n polynomu $f(x)$. Je-li $f(x)$ ireducibilní (neboli zjištěný počet faktorů je rovný jedné), jsme hotovi.
- Jinak určíme libovolné řešení dané soustavy různé od $(a,0,0,\ldots,0)$ a označíme příslušný polynom $h(x)$.
- Vzorec z Tvrzení 6.2 nám dá netriviální rozklad $f(x) = g_1(x)g_2(x)\ldots g_l(x)$.
- Pokud $l = n$ jsme hotovi, jinak rekurzivně určíme ireducibilní rozklad polynomů $g_1(x)$, $g_2(x)$, $\ldots g_l(x)$.

Uvedený postup lze poněkud optimalizovat. Místo nalezení libovolného "zajímavého" polynomu $h(x)$ určíme bázi $h_1(x) = 1, h_2(x), \ldots, h_n(x)$ prostoru W (polynom $h_1(x) = 1$ a jeho násobky odpovídají nezajímavým konstantním polynomům). Použijeme $h_2(x)$ na nalezení netriviálního rozkladu $f(x)$. Jednotlivé faktory se pokusíme dále rozložit polynomem $h_3(x)$, atd. Takto postupujeme dokud nenajdeme n netriviálních faktorů. Tento postup vede k cíli:

Tvrzení 6.5. *Nechť $f_1(x), f_2(x)$ jsou dva různé ireducibilní faktory $f(x)$. Pak existuje $2 \le i \le n$ takové, že $f_1(x)$ a $f_2(x)$ dělí různé členy rozkladu $f(x) = \prod_{a\in\mathbf{F}_q} \mathrm{NSD}(f(x), h_i(x) - a)$.*

Důkaz. Nechť $f(x) = f_1(x)f_2(x)\ldots f_n(x)$ je ireducibilní rozklad polynomu$f(x)$. Nejprve si všimneme, že polynom $f_j(x)$ $(j = 1,2)$ dělí $\mathrm{NSD}(f(x), h_i - a)$ právě tehdy, když $f_j(x)|h_i(x) - a$, což nastane právě tehdy, když $h_i(x) \bmod f_j(x) = a$.

Vektory $\phi(h_1(x)), \phi(h_2(x)), \ldots, \phi(h_n(x))$ (viz Tvrzení 6.3) tvoří bázi $\mathbf{F}_q^n$, takže alespoň jeden z těchto vektorů má různé první dvě složky. Jinými slovy, existuje i takové, že $a = h_i(x) \bmod f_1(x) \neq h_i(x) \bmod f_2(x)$. Pak ale $f_1(x)$ dělí $\mathrm{NSD}(f(x), h_i(x) - a)$, ale $f_2(x)$ tento polynom nedělí. □

Příklad. Rozložíme polynom $f(x) = x^4+1 \in \mathbf{F}_3[x]$ na ireducibilní činitele. Protože $\mathrm{NSD}(f(x), f'(x)) = 1$, f je bezčtvercový. Nejprve spočteme matici S. Platí

$$\begin{aligned}
x^0 \bmod f(x) &= 1\\
x^3 \bmod f(x) &= x^3\\
x^6 \bmod f(x) &= 2x^2\\
x^9 \bmod f(x) &= x^6x^3 \bmod f(x) = (2x^2)x^3 \bmod f(x) = 2x^5 \bmod f(x) = x.
\end{aligned}$$

Takže

$$S = \begin{pmatrix} 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 2 & 0\\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

Gaussovou eliminací převedeme $S - I$ do odstupňovaného tvaru

$$S - I = \begin{pmatrix} 0 & 0 & 0 & 0\\ 0 & 2 & 0 & 1\\ 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 2 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 & 0 & 2\\ 0 & 0 & 1 & 0\\ 0 & 2 & 0 & 1\\ 0 & 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 & 0 & 2\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Báze je například $(1,0,0,0),(0,1,0,1)$, což odpovídá polynomům $h_1(x)=1$, $h_2(x)=x+x^3$. Polynom $f(x)$ se tedy rozkládá na 2 ireducibilní činitele. Spočteme

$$\begin{aligned}\mathrm{NSD}(f(x),h_2(x)-0) &= \mathrm{NSD}(x^4+1,x^3+x)=1\\ \mathrm{NSD}(f(x),h_2(x)-1) &= \mathrm{NSD}(x^4+1,x^3+x+2)=x^2+2x+2\\ \mathrm{NSD}(f(x),h_2(x)-2) &= \mathrm{NSD}(x^4+1,x^3+x+1)=x^2+x+2.\end{aligned}$$

Hledaný rozklad je tedy

$$x^4+1=(x^2+2x+2)(x^2+x+2).$$

6.3. **Zassenhausův algoritmus.** Nechť opět $f(x)\in\mathbf{F}_q[x]$ a $h(x)\in W$ je nekonstantní polynom (tedy $h^q(x)\equiv h(x) \pmod{f(x)}$, $0<\deg h(x)<\deg f(x)$). Z předchozí části víme, že

$$f(x)=\prod_{a\in\mathbf{F}_q}\mathrm{NSD}(f(x),h(x)-a)$$

je netriviální rozklad polynomu $f(x)$. Pokud je q velké vzhledem k počtu ireducibilních faktorů polynomu $f(x)$, bude většina faktorů $\mathrm{NSD}(f(x),h(x)-a)$ rovna jedné, takže většinu největších společných dělitelů budeme počítat zbytečně. V této kapitole si ukážeme, jak určit "zajímavé" prvky $a\in\mathbf{F}_q$ – ty prvky pro něž $\mathrm{NSD}(f(x),h(x)-a)\neq 1$. Toto vylepšení Berlekampova algoritmu se nazývá *Zassenhaussův algoritmus*.

Označme A množinu "zajímavých" prvků:

$$A=\{a\in\mathbf{F}_q \mid \mathrm{NSD}(f(x),h(x)-a)\neq 1\},$$

Tedy

$$f(x)=\prod_{a\in A}\mathrm{NSD}(f(x),h(x)-a)$$

a žádný člen tohoto rozkladu již nelze vynechat. Uvažujme polynom

$$G(y)=\prod_{a\in A}(y-a).$$

Množina A je tedy množinou kořenů polynomu $G(y)$.

Protože $f(x)=\prod_{a\in A}\mathrm{NSD}(f(x),h(x)-a)$, platí $f(x)|\prod_{a\in A}(h(x)-a)=G(h(x))$, tedy $f(x)|G(h(x))$. Polynom $G(y)$ je monický polynom nejmenšího stupně s touto vlastností:

Věta 6.6. *Označme*

$$J=\{g(y)\in\mathbf{F}_q[y] \mid f(x)|g(h(x))\}.$$

Pak J je ideál $\mathbf{F}_q[y]$ generovaný $G(y)$ (neboli $J=G(y)\mathbf{F}_q[y]$).

Důkaz. Jsou-li $g_1(y),g_2(y)\in J$, pak $f(x)|g_1(h(x))$, $f(x)|g_2(f(x))$ a tedy i $f(x)|(g_1-g_2)(h(x))$. Je-li $k(y)\in\mathbf{F}_q[y]$, pak také $f(x)|k(h(x))\cdot g_1(h(x))=(k\cdot g_1)(h(x))$. Ukázali jsme, že J je ideál.

$\mathbf{F}_q[x]$ obor integrity hlavních ideálů, existuje monický $G_0(y)\in J$ takový, že všechny polynomy v J jsou násobkem $G_0(y)$, tedy $J=G_0[y]\mathbf{F}_q[y]$. Speciálně $G_0(y)|G(y)=\prod_{a\in A}(y-a)$, tedy $G_0(y)=\prod_{a\in A_0}(y-a)$ pro nějaké $A_0\subseteq A$. Protože $f(x)|G_0(h(x))=\prod_{a\in A_0}(h(x)-a)$, platí $f(x)=\prod_{a\in A_0}\mathrm{NSD}(f(x),h(x)-a)$. Odtud plyne $A_0=A$ (žádný prvek v rozkladu $f(x)=\prod_{a\in A}\mathrm{NSD}(f(x),h(x)-a)$ nelze vynechat, tak byla množina A zvolena) a tedy $G_0(y)=G(y)$. □

Označme $m = |A|$ (všimněte si, že m je nejvýše počet ireducibilních faktorů polynomu $f(x)$) a

$$G(y) = b_0 + b_1 y + \cdots + b_m y^m, \quad b_i \in \mathbf{F}_q,\ b_m = 1.$$

Vztah $f(x)|G(h(x))$ je ekvivalentní s $G(h(x)) \bmod f(x) = 0$.

$$\begin{aligned} G(h(x)) \bmod f(x) &= (b_0 + b_1 h(x) + \cdots + b_m h^m(x)) \bmod f(x) = \\ &= b_0 + b_1(h(x) \bmod f(x)) + \cdots + b_m(h^m(x) \bmod f(x)) \end{aligned}$$

Tedy $f(x)|G(h(x))$ právě tehdy, když

$$0 = b_0 + b_1(h(x) \bmod f(x)) + \cdots + b_m(h^m(x) \bmod f(x)),$$

tedy 0 je lineární kombinací polynomů 1, $h(x) \bmod f(x)$, ... a $b_0, \ldots, b_m = 1$ jsou koeficienty této lineární kombinace.

Při hledání $G(y)$ tedy můžeme postupovat takto: Počítáme postupně $h^j(x) \bmod f(x)$ a první index j, pro které jsou polynomy $1, h(x) \bmod f(x), \ldots, h^j(x) \bmod f(x)$ lineárně závislé. Spočteme $b_0, b_1, \ldots, b_{m-1}, b_m = 1$, aby $0 = b_0 + b_1(h(x) \bmod f(x)) + \cdots + b_m(h^m(x) \bmod f(x))$. Nyní najdeme kořeny $G(y)$ (např. postupem v následující části) a máme množinu A.

Příklad. Rozložíme polynom $f(x) = x^6 - 3x^5 + 5x^4 - 9x^3 - 5x^2 + 6x + 7 \in \mathbf{F}_{23}[x]$ pomocí Zassenhausenova algoritmu.

Spočteme, že platí $\mathrm{NSD}(f(x), f'(x)) = 1$, tedy $f(x)$ je bezčtvercový polynom.

Začneme počítat Berlekampovým algoritmem. Spočteme $x^{jq} \bmod f(x)$ pro $j = 0, \ldots, n-1$. Dostáváme matici

$$S = \begin{pmatrix} 1 & 5 & -10 & 0 & 11 & -3 \\ 0 & 0 & 10 & 7 & 0 & 0 \\ 0 & -1 & 10 & 9 & -4 & -10 \\ 0 & 8 & 0 & -8 & 7 & 9 \\ 0 & -3 & 1 & 10 & 7 & 2 \\ 0 & -10 & -9 & -11 & 2 & -9 \end{pmatrix}$$

Matice $S - I$ má hodnost 3, báze nulového prostoru je např.

$$(1,0,0,0,0,0), (0,4,2,1,0,0), (0,-2,9,0,1,1).$$

Polynom $f(x)$ má tedy 3 ireducibilní faktory.

Vezměme například polynom odpovídající druhému vektoru $h(x) = x^3 + 2x^2 + 4x \in W$. Platí

$$\begin{aligned} h^0(x) &= 1 \\ h^1(x) \bmod f(x) &= x^3 + 2x^2 + 4x \\ h^2(x) \bmod f(x) &= 7x^5 + 7x^4 + 2x^3 - 2x^2 - 6x - 7 \\ h^3(x) \bmod f(x) &= -11x^5 - 11x^4 - x^3 - 9x^2 - 5x - 2 \end{aligned}$$

Platí $(h^3(x) \bmod f(x)) - 5(h^2(x) \bmod f(x)) + 11(h(x) \bmod f(x)) - 10 = 0$, takže $G(y) = y^3 - 5y^2 + 11y - 10$. Kořeny $G(y)$ jsou $-3, 2 - 6$.

Zbývá spočítat

$$\begin{aligned} \mathrm{NSD}(f(x), x^3 + 2x^2 + 4x + 3) &= x - 4 \\ \mathrm{NSD}(f(x), x^3 + 2x^2 + 4x - 2) &= x^2 - x + 7 \\ \mathrm{NSD}(f(x), x^3 + 2x^2 + 4x - 6) &= x^3 + 2x^2 + 4x - 6 \end{aligned}$$

Takže

$$f(x) = (x-4)(x^2-x+7)(x^3+2x^2+4x-6)$$

a potože počet ireducibilních faktorů je 3 je toto již ireducibilní rozklad polynomu $f(x)$.

6.4. **Výpočet kořenů polynomů.** Buď $f(x) \in \mathbf{F}_q[x]$. Při hledání kořenů polynomu f, které leží v $\mathbf{F}_q$, napřed izolujeme tu část polynomu $f(x)$, která obsahuje lineární dělitele. To uděláme snadno, neboť víme, že každý prvek $a \in \mathbf{F}_q$ je (jednoduchým) kořenem polynomu $x^q - x \in \mathbf{F}_q[x]$. Každý lineární dělitel polynomu $f(x)$ tak dělí také polynom $x^q - x$ a tedy také $\mathrm{NSD}(f(x), x^q - x)$. Tento největší společný dělitel je tak součinem všech různých lineárních dělitelů polynomu $f(x)$.

Můžeme tedy od začátku předpokládat, že polynom $f(x) \in \mathbf{F}_q[x]$, jehož kořeny chceme najít, se nad $\mathbf{F}_q$ rozkládá na součin lineárních činitelů. Předpokládáme, že

$$f(x) = \prod_{i=1}^{n}(x - a_i),$$

kde $a_1, \ldots, a_n$ jsou navzájem různé prvky $\mathbf{F}_q$.

Je-li q malé číslo, pak lze najít kořeny $f(x)$ zkusmo dosazováním, neboli výpočtem hodnot $f(0), f(1), \ldots$.

Pokud q je liché, lze použít následující metodu. Pro $b \in \mathbf{F}_q$ platí

$$f(x-b) | x^q - x = x(x^{(q-1)/2} - 1)(x^{(q-1)/2} + 1).$$

Pokud je x dělitelem $f(x-b)$, platí $f(-b) = 0$ a našli jsme kořen $f(x)$.

Pokud x není dělitelem $f(x-b)$, platí $f(x) | (x^{(q-1)/2} - 1)(x^{(q-1)/2} + 1)$ a tedy

$$f(x-b) = \mathrm{NSD}(f(x-b), x^{(q-1)/2} - 1) \cdot \mathrm{NSD}(f(x-b), x^{(q-1)/2} + 1).$$

Dělí-li $f(x-b)$ jednoho z činitelů na pravé straně, pak platí buď $x^{(q-1)/2} \equiv 1 \bmod f(x-b)$ nebo $x^{(q-1)/2} \equiv -1 \bmod f(x-b)$. V tomto málo pravděpodobném případě zkusíme jiné b. Jinak dostáváme netriviální rozklad $f(x)$. Tím dostáváme pravděpodobnostní algoritmus pro nalezení kořenů $f(x) \in \mathbf{F}_q[x]$.

Příklad. Najdeme ty kořeny polynomu $f(x) = x^6 - 7x^5 + 3x^4 - 7x^3 + 4x^2 - x - 2 \in \mathbf{F}_{17}$, které leží v $\mathbf{F}_{17}$.

Hledané kořeny polynomu $f(x)$ jsou právě kořeny polynomu $g(x) = \mathrm{NSD}(f(x), x^{17} - x)$. Eukleidovým algoritmem zjistíme, že $g(x) = x^4 + 6x^3 - 5x^2 + 7x - 2$.

Napřed zvolíme $b = 0$. Přímým výpočtem zjistíme, že

$$x^{(q-1)/2} = x^8 \equiv 1 \bmod g(x)$$

takže tato volba b nedává netriviální rozklad $g(x)$.

Zvolíme $b = 1$. Pak $g(x-1) = x^4 + 2x^3 - 3x - 2$ a $x^{(p-1)/2} = x^8 \equiv -4x^3 - 7x^2 + 8x - 5 \bmod g(x-1)$, takže volba $b = 1$ nám dává netriviální faktorizaci $g(x-1)$. Platí

$$\mathrm{NSD}(g(x-1), x^8 + 1) = \mathrm{NSD}(x^4 + 2x^3 - 3x - 2, -4x^3 - 7x^2 + 8x - 4) = x^2 - 7x + 4$$

a

$$\mathrm{NSD}(g(x-1), x^8 - 1) = \mathrm{NSD}(x^4 + 2x^3 - 3x - 2, -4x^3 - 7x^2 + 8x - 6) = x^2 - 8x + 8$$

a tedy $g(x-1) = (x^2 - 7x + 4)(x^2 - 8x + 8)$, což vede k částečné faktorizaci

$$g(x) = (x^2 - 5x - 2)(x^2 - 6x + 1) = g_1(x)g_2(x)$$

Abychom rozložili $g_1(x)$ a $g_2(x)$, zkusíme $b = 2$. Platí $g_1(x-2) = x^2 + 8x - 5$ a $x^8 \equiv -8x + 2 \bmod g_1(x-2)$. Spočítáme

$$\mathrm{NSD}(g_1(x-2), x^8 + 1)) = \mathrm{NSD}(x^2 + 8x - 5, -8x + 3) = x + 6$$

a tedy $g_1(x-2) = (x+6)(x+2)$, neboli $g_1(x) = (x+8)(x+4)$.

Dále $g_2(x-2) = x^2+7x = x(x+7)$, čili -2 je kořen $g_2(x)$ a $g_2(x) = (x+2)(x+9) = (x+2)(x-8)$. Zjistili jsme tak, že

$$g(x) = g_1(x)g_2(x) = (x+8)(x+4)(x+2)(x-8)$$

a kořeny $g(x)$ a tedy i $f(x)$ v $\mathbf{F}_{17}$ jsou $-8, -4, -2, 8$.

Pro hledání kořenů polynomů s koeficienty v konečných tělesech neprvočíselné mohutnosti se používají jiné algoritmy.

6.5. **Cvičení.**

(1) Dokažte Tvrzení 6.1.
(2) Nechť $f(x) \in \mathbf{F}(x)$ je libovolný polynom a označme $d(x) = \mathrm{NSD}(f(x), f'(x))$, $d(x) \neq 0$. Dokažte, že $\frac{f(x)}{d(x)}$ je bezčtvercový.
(3) Nechť $f(x)$ je polynom nad tělsem $\mathbf{F}_{p^m}$ takový, že $f'(x) = 0$. Dokažte, že existuje polynom $g(x) \in \mathbf{F}_{p^m}[x]$ takový, že $f(x) = g^p(x)$.
(4) Rozložte polynom $f(x) = x^8+2x^6+x^5+2x^3+x^2+2 \in \mathbb{Z}_3[x]$ na ireducibilní činitele.
(5) Rozložte polynom $f(x) = x^8 + x^6 + x^4 + x^3 + 1 \in \mathbb{Z}_2[x]$ na ireducibilní činitele.
(6) Ukažte, že polynom $x^4 + 1$ je nerozložitelný nad racionálními čísly, ale je rozložitelný nad každým konečným tělesem.