NI-MPI handouts

Obsah

Cílem tohoto cvičení je připomenout

- pojem funkce, derivace a polynom – budete tyto pojmy potřebovat později, zejména při studiu funkcí více proměnných,
- rozšířený Euklidův algoritmus (EEA).
- Eulerovu funkci.

Pokud byste potřebovali k procvičení více příkladů, projděte si materiály k bakalářským předmětům BI-MA1, BI-MA2 a BI-DML.
Následující příklady byly vybrány tak, abyste si mohli vytvořit představu o tom, jaké se předpokládají znalosti u studentů tohoto předmětu.

1 Funkce a derivace funkce

Cvičení 1.1 Buď $f(x) = \sin x$ a $g(x) = (x-3)^3$. Čemu se rovnají následující funkce? Čemu se rovnají jejich derivace?

(a) $(f \circ g)(x)$,

(b) $(g \circ f)(x)$,

(c) $(f \circ g^{-1})(x)$,

(d) $(g^{-1} \circ f)(x)$.

Značení 1.1. *Značení $f \circ g$ používáme tak, že g je vnitřní funkce:*

$$(f \circ g)(x) = f(g(x))$$

pro všechna x z definičního oboru funkce $f \circ g$.

Cvičení 1.2 Zderivujte následující funkce (a je reálný parametr):

(a) $(x^4 + 3x^3)x^8$,

(b) e^{2ax},

(c) $\dfrac{x+3a}{x^2}$,

(d) $\ln\left((x+4)^{15a}\right)$,

(e) $\sin^2 x + \cos^2 x$,

(f) xe^{2x},

(g) $e^{x^{2a}}$,

(h) x^x.

Cvičení 1.3 Buď $p(x) = \sum_{k=0}^{n} a_k x^k$ polynom n-tého stupně (tj. $a_n \neq 0$), kde $n \in \mathbb{N}$. Čemu se rovná jeho n-tá derivace $p^{(n)}$?

Značení 1.2. *Značení $\mathbb{N}$ je označení pro nezáporná celá čísla, tedy přirozená čísla s nulou.*

Cvičení 1.4 S využitím faktu, že derivace funkce v bodě x se rovná směrnici tečny grafu této funkce v bodě x, najděte body a, kde

(a) tečna grafu $f(x) = x^3$ svírá s osou x úhel $\pi/3$,

(b) tečna grafu $f(x) = (x^2 - x)^{\frac{1}{3}}$ svírá s osou x úhel $\pi/2$.

Cvičení 1.5 Najděte rovnici tečny

(a) funkce $x^3 + x$ v bodě $x = 1$,

(b) funkce $\sin x$ v bodě $x = \pi/4$,

(c) funkce $(x-1)^3 - 1$ v bodě průsečíku grafu této funkce s přímkou $y = 2x + 1$.

Cvičení 1.6 Najděte směrnici tečen kružnice se středem v bodě $[2, 1]$ a s poloměrem 2 v bodech průniku této kružnice s přímkou

(a) $y = x$,

(b) $y = x + 1$.

Cvičení 1.7 Představte si, že jedete přes kopec, který má profil zadaný funkcí $f(x) = 5e^{-(x-2)^2}$. Kde to bude nejvíce z kopce a nejvíce do kopce?

Cvičení 1.8 Představte si, že jedete po krajině, která má profil zadaný funkcí $f(x) = \arctan x + \frac{x}{10}$. Jste sice zdatný cyklista resp. zdatná cyklistka, ale více jak 100% stoupání už nezvládnete. Kam nejdále můžete dojet, za předpokladu, že máte nekonečnou výdrž, pokud vyrazíte z Vašeho domu umístěného v místě $x = 10$? Změní se nějak Váš dojezd, pokud si dáte podmínku, že chcete být schopni se vrátit domů?

Cvičení 1.9 Najděte funkci $f(x)$ tak, aby platila následující rovnice:

(a) $f'(x) = 2f(x)$,

(b) $f''(x) = -3f(x)$.

2 Polynomy

Cvičení 2.1 Vydělte polynom $p(x)$ polynomem $q(x)$, pokud

(a) $p(x) = x^3 + 3x^2 - x - 3$ a $q(x) = x + 1$,

(b) $p(x) = x^3 + 3x^2 - x - 3$ a $q(x) = x + 2$,

(c) $p(x) = x^4 + 3x + 2$ a $q(x) = x^2 + x + 1$,

(d) $p(x) = x^5 + 1$ a $q(x) = x + 1$.

(e) $p(x) = x^5 + 1$ a $q(x) = x - 1$.

Cvičení 2.2 Najděte všechny kořeny polynomu $p(x) = x^3 + 3x^2 - x - 3$, jestliže víte, že jedním z kořenů je -1.

Cvičení 2.3 Najděte všechny kořeny polynomu $p(x) = x^3 - 9x^2 - 16x + 60$, jestliže víte, že jedním z kořenů je 2.

3 Rozšířený Euklidův algoritmus

V této části cvičení se také procvičíme ve vlastnostech největšího společného dělitele (gcd).

Cvičení 3.1 Nechť $a \in \mathbb{Z}$, kolik je $\gcd(a, 0)$?

Cvičení 3.2 Dokažte následující tvrzení.

(a) Pro $m \neq 0$ takové, že $m|a$ a $m|b$, platí $\gcd(a/m, b/m) = \gcd(a, b)/m$.

(b) Pro a nesoudělné s b platí $\gcd(ab, c) = \gcd(a, c) \cdot \gcd(b, c)$.

Cvičení 3.3 Najděte pomocí rozšířeného Euklidova algoritmu největší společný dělitel a Bézoutovy koeficienty čísel

(a) 124 a 523;

(b) 321 a 225.

Cvičení 3.4 — *Stamp problem.* Princezna chce poslat drakovi pohled ze země za devatero horami. Tam mají k dispozici jenom známky v hodnotě 47 zlatých a 22 zlatých. Za každou další horu, kterou listonoš musí s pohledem překonat, se platí 3-krát tolik, co za předchozí horu (odpovídá rychlosti ošoupávání si podrážek s daným zatížením), a první hora stojí 2 zlaté. Na pohledu ovšem musí být cena přesně, jinak pošta pohled odmítne doručit. Poraďte princezně, kolik kterých známek má použít.

Nápověda: začněte od Bézoutovy rovnosti.

4 Eulerova funkce

Cvičení 4.1 Pro Eulerovu funkci φ a dvě nesoudělná kladná přirozená čísla m a n platí $\varphi(mn) = \varphi(m)\varphi(n)$. S využitím tohoto faktu najděte vzorec pro výpočet $\varphi(n)$ čísla n s prvočíselným rozkladem $n = \prod_{i=1}^{m} p_i^{k_i}$.

Cvičení 4.2 Spočtěte

(a) $\varphi(114)$,

(b) $\varphi(432)$.

Co byste si měli z tohoto cvičení odnést:

- Jak se parciálně derivuje.
- Co je to gradient funkce a jaký je jeho geometrický význam.
- Jak nám gradient pomáhá spočítat derivaci ve směru (a co to je).
- Jak najít rovnici tečné roviny.

5 Spojitost a limita

Cvičení 5.1 Zjistěte, zda je funkce $f : \mathbb{R}^2 \to \mathbb{R}$ definovaná předpisem

$$f(x,y) = \begin{cases} \frac{xy}{x^2+y^2} & \text{pro } (x,y) \in \mathbb{R}^2 \setminus \{(0,0)\} \\ 0 & \text{pro } (x,y) = (0,0) \end{cases}$$

Spojitá a po částech spojitá[a] v bodě $(0,0)$.

[a] Funkce $f(x,y)$ je po částech spojitá v bodě (x_0,y_0), pokud jsou funkce jedné proměnné $f(x_0,y)$ a $f(x,y_0)$ spojité po řadě v bodech y_0 a x_0.

6 Parciální derivace

Cvičení 6.1

(a) najděte $\frac{\partial f}{\partial x}$ a $\frac{\partial f}{\partial y}$ pro $f(x,y) = xy + e^x \cos y$,

(b) pro předchozí funkci vyčíslete hodnotu parciální derivace podle x v bodě $(1, \pi/2)$

(c) najděte $\frac{\partial z}{\partial x}$ a $\frac{\partial z}{\partial y}$ pro $z(x,y) = x^2y^3 + x^3y^4 - e^{xy^2}$,

(d) najděte hodnotu $\frac{\partial f}{\partial z}$ v bodě $(1,2,3)$ pro $f(x,y,z) = \sin(xy/z)$,

(e) najděte $\frac{\partial f}{\partial x}$ pro $f(x,y) = e^{-x^2-y^2}$,

(f) najděte $\frac{\partial f}{\partial x}$ pro $f(x,y) = \ln(x^2+y^2+1)$,

(g) najděte $\frac{\partial f}{\partial x}$ pro $f(x,y) = \frac{1}{x^3+y^3}$.

Cvičení 6.2 V jakém bodě nemá funkce $\sqrt{x^2+y^2}$ parciální derivaci a proč?

Cvičení 6.3 Spočítejte druhou parciální derivaci podle x a y, tj. $\frac{\partial^2 f}{\partial x^2}$ a $\frac{\partial^2 f}{\partial y^2}$, pro funkce

(a) $f(x,y) = x^2y^2$,

(b) $f(x,y) = \sin(xy)$,

(c) $f(x,y) = xy^2 - ye^{-x} - \cos(x-y)$.

Funkci můžeme derivovat dvakrát také podle dvou různých proměnných, takové derivaci se říká *smíšená* a značí se

$$\frac{\partial}{\partial x}\left(\frac{\partial f}{\partial y}\right) = \frac{\partial^2 f}{\partial x \partial y}.$$

Cvičení 6.4 Spočítejte smíšené derivace $\frac{\partial^2 f}{\partial x \partial y}$ a $\frac{\partial^2 f}{\partial y \partial x}$ pro funkce

(a) $f(x, y, z) = e^{xz} + y \cos x$,

(b) $f(x, y, z) = z \cos(xy) + x \sin(yz)$.

To, že obě smíšené derivace v předchozím příkladě vyšly stejné, není náhoda. Platí totiž následující věta:

Věta 6.1 Nechť $f : D_f \to \mathbb{R}, D_f \subset \mathbb{R}^2$ a $\mathbf{b} \in D_f$.
Pokud existuje $\frac{\partial^2 f}{\partial x \partial y}(\mathbf{b})$ a funkce $\frac{\partial^2 f}{\partial x \partial y}$ je v $\mathbf{b}$ spojitá, potom $\frac{\partial^2 f}{\partial y \partial x}(\mathbf{b})$ existuje a platí

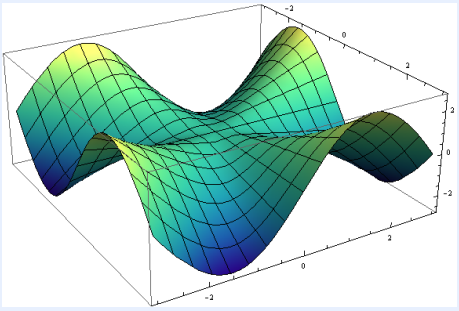
$$\frac{\partial^2 f}{\partial x \partial y}(\mathbf{b}) = \frac{\partial^2 f}{\partial y \partial x}(\mathbf{b}).$$

Tedy nezáleží na pořadí parciálního derivování.

Cvičení 6.5 Příkladem, kdy se smíšené derivace nerovnají, je funkce

$$f(x, y) = \begin{cases} 0 & \text{v bodě } (0, 0) \\ \frac{xy(x^2 - y^2)}{x^2 + y^2} & \text{jinak.} \end{cases}$$

Zkuste vysvětlit s pomocí grafu této funkce, proč tomu tak je:



Cvičení 6.6 Dokažte, že funkce $f(x, y) = x^3 - 3xy^2$ splňuje tzv. *Laplaceovu rovnici*

$$\frac{\partial^2 f}{\partial x^2} + \frac{\partial^2 f}{\partial y^2} = 0.$$

Cvičení 6.7 Dokažte, že funkce $g(x, t) = 2 + e^{-t} \sin x$ splňuje tzv. *rovnici vedení tepla*

$$\frac{\partial g}{\partial t} = \frac{\partial^2 g}{\partial x^2}.$$

(Zde je $g(x, t)$ teplota železné tyče v místě x a čase t. Co se stane pro t jdoucí do nekonečna?).

7 Gradient, derivace ve směru a tečná rovina

Gradient funkce $f(x_1, x_2, \ldots, x_n)$ v daném bodě $b \in \mathbb{R}^n$ je vektor

$$\nabla f(b) = \left(\frac{\partial f}{\partial x_1}(b), \frac{\partial f}{\partial x_2}(b), \ldots, \frac{\partial f}{\partial x_n}(b) \right).$$

Tento vektor ukazuje směr nejvyššího růstu dané funkce.

Cvičení 7.1 Najděte gradient následujících funkcí

(a) $f(x,y,z) = \sqrt{x^2+y^2+z^2}$,

(b) $f(x,y,z) = xy + xz + zy$,

(c) $f(x,y,z) = x + y^2 + z^3$,

(d) $f(x,y,z) = zx^2 + xy^2 + yz^2$,

(e) $f(x,y) = xe^{xy^3+3}$,

(f) $f(x,y) = xe^{x^2+y^2}$.

Cvičení 7.2 Najděte gradient funkce $f(x,y) = x^2/10 + y^2/10$. Jakým směrem by se začala kutálet kulička a kde by se nakonec zastavila, pokud byste ji položili na graf této funkce v bodě $(1,3)$?

Cvičení 7.3 Představte si, že vyrážíte z Prahy, tedy zhruba z 50 stupňů zeměpisné šířky a 14 stupňů zeměpisné délky, po tuhé zimě na dovolenou. Kolega meteorolog Vám předal vzorec, který hrubě odhaduje teplotu v místě se zeměpisnou šířkou x a délkou y:

$$T(x,y) = (-0,0003)x^2y + (0,9307)y\,.$$

Jakým směrem se vydat, aby se teplota zvyšovala co nejrychleji?

Cvičení 7.4 Kapitán Astroš se prohání vesmírem poblíž strany Merkuru přivrácené ke slunci. Najednou mu začne být nesnesitelné horko a zámky dveří na jeho lodi začnou roztávat. Kudy se má vydat, aby teplota klesla co nejrychleji, jestliže je teplota v těchto místech dána funkcí

$$T(x,y,z) = e^{-x} + e^{-2y} + e^{3z}$$

a kapitán se nachází v bodě $(1,1,1)$?

Následující cvičení je demonstrací toho, že chceme-li spočítat derivaci funkce $f(x_1,x_2,\ldots,x_n)$ v bodě $(b_1,b_2,\ldots,b_n)$ a ve směru jednotkového (sloupcového) vektoru $\vec{v}$, stačí spočítat gradient a pak se derivace rovná

$$\nabla f(b_1,b_2,\ldots,b_n)\cdot\vec{v}.$$

Cvičení 7.5 Uvažujme graf funkce $z(x,y) = x^2+3y^2$. Pronikneme jej s rovinou rovnoběžnou s osou z a procházející přímkou $y = 2x$: vzniklou množinu lze chápat jako graf jednorozměrné funkci nad touto přímkou (pro pořádek: na přímce se pohybujeme směrem z třetího kvadrantu, kde je x a y záporné, do prvního, kde jsou kladná). Najděte analytický předpis nějaké takové jednorozměrné funkce a dokažte, že její derivace v bodě přímky ve vzdálenosti 2 od počátku souřadnic v prvním kvadrantu je rovna

$$\nabla z\left(\frac{2}{\sqrt{5}},\frac{4}{\sqrt{5}}\right)\cdot\left(\frac{1}{\sqrt{5}},\frac{2}{\sqrt{5}}\right),$$

kde $\cdot$ značí skalární součin vektorů.

Cvičení 7.6 Spočítejte derivaci funkce f v bodě (x_0,y_0) ve směru vektoru $\vec{d}$, kde

(a) $f(x,y) = x + 2x^2 - 3xy, (x_0,y_0) = (1,1)$ a $\vec{d} = (3/5, 4/5)$,

(b) $f(x,y) = \ln\left(\sqrt{x^2+y^2}\right), (x_0,y_0) = (1,0)$ a $\vec{d} = (2/\sqrt{5}, 1/\sqrt{5})$,

(c) $f(x,y,z) = xyz, (x_0,y_0,z_0) = (1,1,1)$ a $\vec{d} = (1/\sqrt{2}, 1/\sqrt{2}, 0)$.

■

Cvičení 7.7 Představte si, že programujete primitivní simulátor autíčka jedoucího po 3D krajině, jež je dána grafem funkce $z(x, y) = x/2 + y/3 - 2$. Jediný vstup od uživatele je jednotkový vektor $\vec{s} = (s_1, s_2)$, který udává horizontální směr pohybu autíčka a který uživatel nastavuje pomocí šipek. ?

Rychlost auta je nepřímo úměrná sklonu povrchu vyjádřenému úhlem α (v radiánech) a je zadána funkcí $f(\alpha) = 20 - 40\alpha$. Najděte funkci $r(x, y, \vec{s})$, která udává rychlost autíčka v bodě (x, y) pohybujícího se ve směru vektoru jednotkového $\vec{s}$.

Cvičení 7.8 Jak by vypadala funkce $r(x, y, \vec{s})$ (z předchozího cvičení), pokud by se autíčko pohybovalo po krajině dané rovnicí $z = x^2/2 + y^2/2 + xy$? ?

Cvičení 7.9 Odvoďte rovnici tečné roviny v bodě (x_0, y_0) pro funkci $f(x, y)$. ?

Co byste si měli z tohoto cvičení odnést:

- Co to je kritický bod a jaký je jeho význam pro hledání extrémů.
- Jak pro danou vícerozměrnou funkci najít Hessovu matici (Hessián).
- Jak zjistit, jestli je daný Hessián pozitivně/negativně (semi)definitní nebo indefinitní (Sylvestrovo kritérium),
- a jak nám toto zjištění pomůže k určení povahy kritického bodu: je to maximum/minimum/ani jedno (sedlový bod)?
- Ti zdatnější by měli znát geometrický význam Hessiánu a s jeho pomocí umět vysvětlit, proč z něj můžeme poznat povahu extrému.

A co byste se měli doučit pokud to ještě/už neumíte:

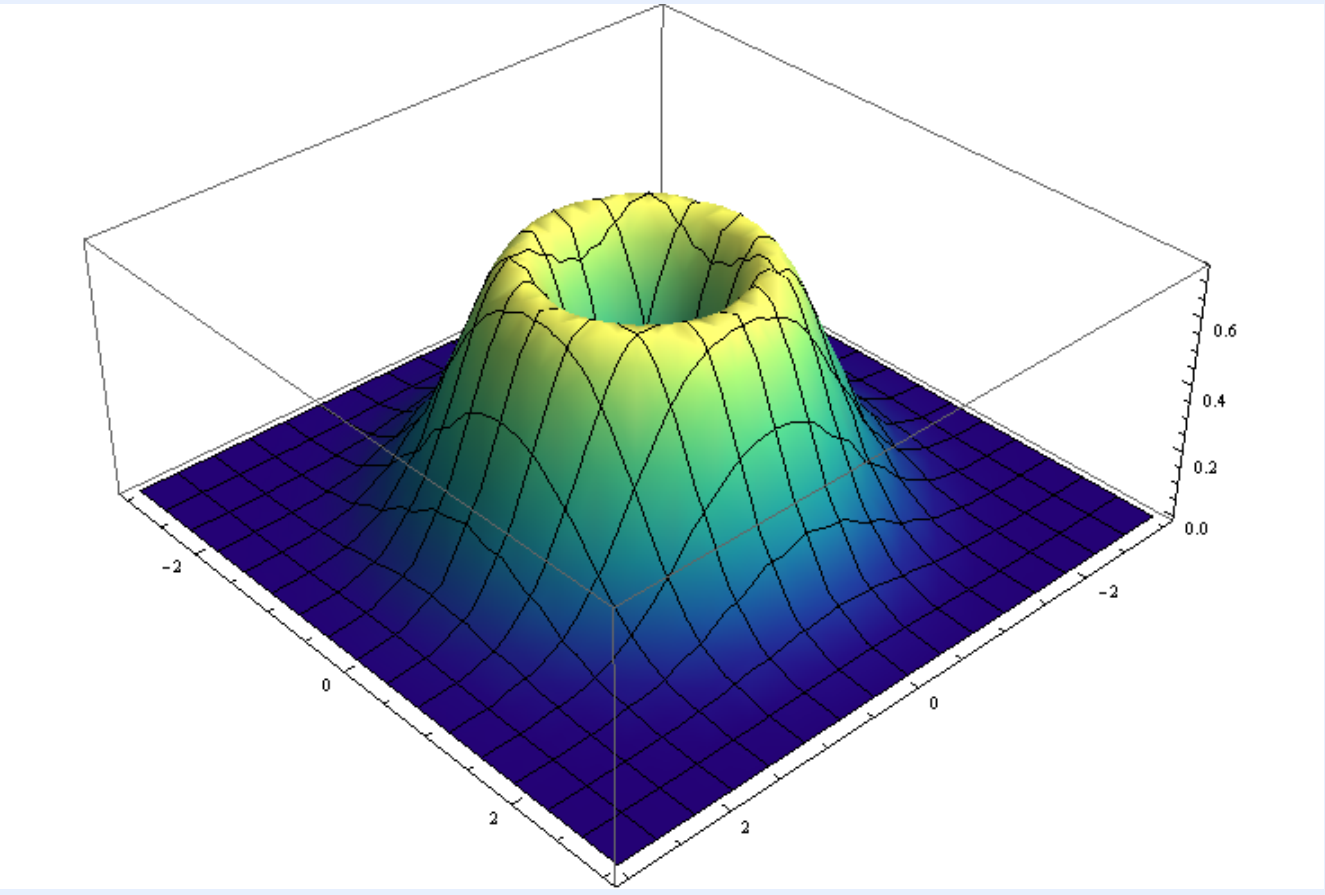
- Řešit soustavu lineárních rovnic a příp. jednodušší nelineární soustavy.
- Spočítat determinant matic o rozměrech 2×2 a 3×3.
- Násobit matice a vektory.
- Derivovat!

8 Kritické body

Cvičení 8.1 Uvažujme funkci $f(x, y) = 2(x^2 + y^2)e^{-x^2-y^2}$. ?

(a) S pomocí grafu na následujícím obrázku odhadněte, kde jsou lokální/globální maxima/minima, a určete, která z nich jsou ostrá.

(b) Pomocí geometrického významu gradientu najděte přesné souřadnice těchto bodů.

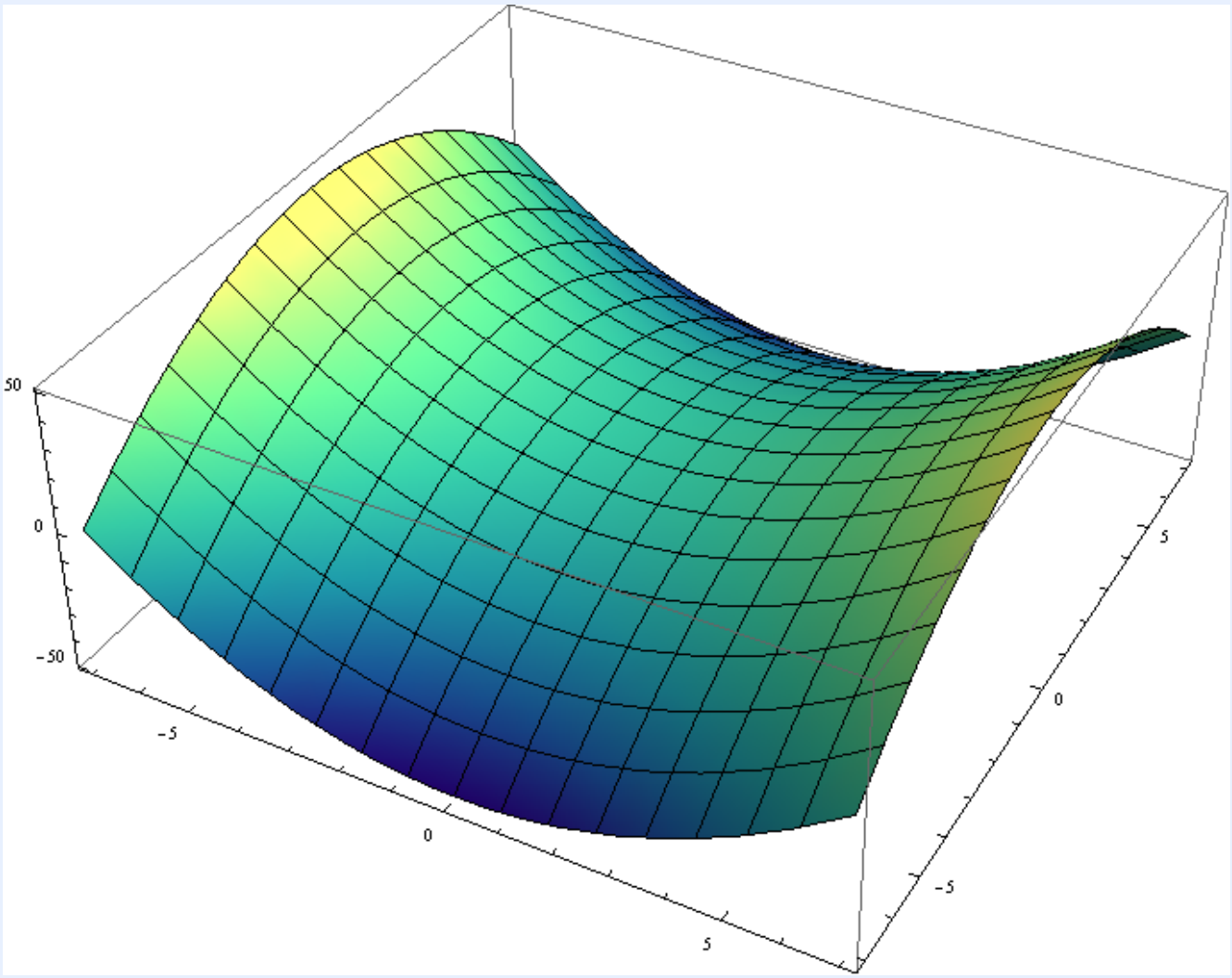


■

Cvičení 8.2 Uvažujme funkci $f(x, y) = x^2 - y^2$. ?

(a) S pomocí grafu na následujícím obrázku odhadněte, v jakých bodech je tečná rovina rovnoběžná s osami x a y?

(b) Pomocí rovnice tečné roviny najděte přesné souřadnice těchto bodů.



Definice 8.1 Body definičního oboru funkce, kde je gradient dané funkce nulový vektor nebo není definován, se nazývají *kritické body*.

Význam kritických bodů je stejný, jako význam bodů, ve kterých je derivace nulová (či neexistuje) pro jednorozměrné funkce: jsou to body *podezřelé z extrému*. Platí totiž podobně jako v jednorozměrném případě následující věta:

Věta 8.2 Je-li bod $b \in \mathbb{R}^n$ lokální extrém funkce $f : \mathbb{R}^n \to \mathbb{R}$ a má-li tato funkce v bodě b parciální derivace, potom jsou tyto parciální derivace nulové (tzn. b je kritický bod).

Cvičení 8.3 Najděte všechny kritické body následujících funkcí:

(a) $f(x, y) = x^2 + 2y^2$,

(b) $f(x, y, z) = 3x^2 + xy + 3zy$,

(c) $f(x, y) = e^{-x^2-7y^2+3}$,

(d) $f(x, y) = x^2 + y^2 + 3xy + 10$,

(e) $f(x, y) = \sin(x^2 + y^2)$.

Cvičení 8.4 Funkce

$$f(x,y) = \frac{\sin(\pi\sqrt{x^2+y^2})}{\pi\sqrt{x^2+y^2}}.$$

není definována v bodě $(0,0)$.

(a) Jak musíme dodefinovat funkční hodnotu $f(0,0)$, aby výsledkem mohla být všude spojitá funkce?

(b) Jaké jsou kritické body této spojité funkce?

9 Hessián, definitnost matic, extrémy

V případě jednorozměrných funkcí jsme mohli rozhodnout, jestli je daný kritický bod minimum, maximum či inflexní bod pomocí druhé derivace a jejího znaménka. V případě vícerozměrné funkce $f(x_1, x_2, \ldots, x_n)$ hraje roli druhé derivace *Hessova matice (Hessián)*

$$\nabla^2 f = \begin{pmatrix} \frac{\partial^2 f}{\partial x_1^2} & \cdots & \frac{\partial^2 f}{\partial x_1 \partial x_n} \\ \vdots & & \vdots \\ \frac{\partial^2 f}{\partial x_n \partial x_1} & \cdots & \frac{\partial^2 f}{\partial x_n^2} \end{pmatrix}.$$

avšak u matice pojem znaménka ztrácí smysl. Přesto (většinou) umíme z této matice určit, jestli se jedná o maximum či minimum: k tomu slouží pojmy pozitivně/negativně (semi)definitní matice.

Definice 9.1 Matice $A \in \mathbb{R}^{n,n}$ je

(i) *pozitivně definitní*, jestliže pro všechny **nenulové** vektory $\vec{a} \in \mathbb{R}^n$ platí

$$\vec{a}^T A \vec{a} > 0,$$

(ii) *pozitivně semidefinitní*, jestliže pro všechny vektory $\vec{a} \in \mathbb{R}^n$ platí

$$\vec{a}^T A \vec{a} \geq 0,$$

(iii) *negativně definitní*, jestliže pro všechny **nenulové** vektory $\vec{a} \in \mathbb{R}^n$ platí

$$\vec{a}^T A \vec{a} < 0,$$

(iv) *negativně semidefinitní*, jestliže pro všechny vektory $\vec{a} \in \mathbb{R}^n$ platí

$$\vec{a}^T A \vec{a} \leq 0,$$

(v) *indefinitní* pokud nenastává ani jeden z výše uvedených případů.

U jednorozměrných funkcí platila pravidla typu: „Je-li druhá derivace v kritickém bodě x_0 kladná, jedná se o minimum a funkce je zde konvexní.“ Ve více rozměrech kladnost a zápornost nahrazuje pozitivní resp. negativní definitnost, jinak pravidla zůstávají analogická.

Věta 9.2 — Postačující podmínka existence extrému a sedlového bodu. Nechť $\mathbf{b} \in D_f$ je stacionární bod funkce $f : D_f \to \mathbb{R}, D_f \subset \mathbb{R}^n$. Nechť existuje okolí $H(\mathbf{b}) \subset D_f$ takové, že f má na $H(\mathbf{b})$ spojité všechny druhé parciální derivace, potom

- je-li $\nabla^2 f(\mathbf{b})$ pozitivně definitní, pak $\mathbf{b}$ je bodem ostrého lokálního minima;
- je-li $\nabla^2 f(\mathbf{b})$ negativně definitní, pak $\mathbf{b}$ je bodem ostrého lokálního maxima;
- je-li $\nabla^2 f(\mathbf{b})$ indefinitní, pak $\mathbf{b}$ je sedlový bod.

Geometrický význam Hessiánu: V předchozím cvičení jsme ukázali, jak lze gradient použít k výpočtu *první derivace v bodě b ve směru* daného jednotkového vektoru $\vec{s}$: ta se rovnala skalárnímu součinu gradientu v tomto bodě

a tohoto vektoru:

$$\nabla f(b) \cdot \vec{s}.$$

Podobně bychom se mohli ptát, jak spočítat druhou derivaci v bodě b ve směru jednotkového (sloupcového) vektoru $\vec{s}$. A odpověď je, že tato derivace se rovná

$$\vec{s}^T \cdot \nabla^2 f(b) \cdot \vec{s},$$

tedy Hessiánu maticově vynásobeným zleva i zprava směrovým vektorem. Pomocí tohoto poznatku můžeme interpretovat pravidlo „Je-li $\nabla^2 f(b)$ pozitivně definitní, je b bodem ostrého lokálního minima.“ takto: uděláme-li v daném kritickém bodě řez libovolným směrem a vzniklá jednorozměrná funkce bude mít v tomto bodě druhou derivaci vždy kladnou, jedná se o lokální minimum původní vícerozměrné funkce.

Základní cvičení 9.1 Uvažme funkce

$$\begin{aligned} f(x,y) &= x^2 + y^2 \\ g(x,y) &= x^2 - y^2 \\ h(x,y) &= x^2 + y^3 \\ u(x,y) &= xy \\ w(x,y) &= (x+y)^2 \\ z(x,y) &= x^4 + y^4 \end{aligned}$$

Pro všechny funkce nalezněte všechny kritické body a zjistěte, zda se jedná o lokální minimum, lokální maximum nebo sedlový bod. Prof funkce f a g spočtěte první a druhou derivaci ve směru přímky $y = x$ v bodě $(1, 1)$. ■

Základní cvičení 9.2 Mějme

$$f(x,y,z) = x^3 + y^2 + z^2 + 12xy + 2z.$$

Nalezněte všechny kritické body a zjistěte, zda se jedná o lokální minimum, lokální maximum nebo sedlový bod. ■

Cvičení 9.3 Najděte Hessián následujících funkcí:

(a) $f(x,y) = x^2y^2$,

(b) $f(x,y) = e^{-(x+y)}$,

(c) $f(x,y,z) = x^2 + y^3 + z^4$.

Cvičení 9.4 V bodě b najděte druhou derivaci funkce f ve směru vektoru $\vec{s}$, kde

(a) $f(x,y) = x + 2x^2 - 3xy, b = (1,1)$ a $\vec{s}^T = (3/5, 4/5)$,

(b) $f(x,y) = \ln\left(\sqrt{x^2+y^2}\right), b = (1,0)$ a $\vec{s}^T = (2/\sqrt{5}, 1/\sqrt{5})$,

(c) $f(x,y,z) = xyz, b = (1,1,1)$ a $\vec{s}^T = (1/\sqrt{2}, 1/\sqrt{2}, 0)$.

■

Poznat, jestli je matice pozitivně či negativně (semi)definitní, není jednoduchý úkol. Pomoci nám můžou následující kritéria:

Věta 9.3 Buď M *symetrická* matice. Potom platí následující:

- Matice M je pozitivně definitní právě tehdy, když všechna její vlastní čísla jsou kladná.
- [Sylvestrovo kritérium] Pro matici $M \in \mathbb{R}^{n,n}$ definujeme matice $M_1, M_2, \ldots, M_n$ takto: $M_k \in \mathbb{R}^{k,k}$ je čtvercová matice v levém horním rohu matice M. Platí:
  - Matice M pozitivně definitní právě tehdy, když je determinant všech matic $M_1, M_2, \ldots, M_n$ kladný.
  - Matice M negativně definitní právě tehdy, když je determinant matic M_k záporný pro k liché a kladný pro k sudé.

Všimněte si, že předchozí větu lze použít pouze pro určení definitnosti, nikoli semidefinitnosti!

Cvičení 9.5 Rozhodněte, pro jaké hodnoty konstant $A, B, C \in \mathbb{R} \setminus \{0\}$ je bod $(0,0)$ pro funkci $g(x,y) = Ax^2 + 2Bxy + Cy^2$ bodem lokálního minima resp. lokálního maxima.

Cvičení 9.6 Najděte všechny maxima a minima funkce

(a) $f(x,y) = x^2 + 3xy + y^2 + 16$,

(b) $f(x,y) = 3x^2 - 5xy + 3y^2$.

Cvičení 9.7 Najděte lokální maxima, minima a sedlové body funkce

$$f(x,y) = (x^2 - y^2)e^{(-x^2-y^2)/2}.$$

Cvičení 9.8 Najděte bod na rovině $x + 3y - z = 6$, který je nejblíže počátku $(0,0,0)$.

Cvičení 9.9 Najděte bod na „dvoj-kuželu“ $z^2 = x^2 + y^2$, který je nejblíže bodu $(1,2,0)$.

Cvičení 9.10 Máme navrhnout tvar krabice (ve tvaru kvádru) bez víka na kočičí žrádlo tak, aby se do ní vešlo 256 cm^3 zmíněné hmoty a abychom co nejvíce ušetřili na materiálu. Jaké budou rozměry této krabice? Jaký by byl výsledek, pokud by byla krabice zavřená i shora?

Cvičení 9.11 Najděte lokální maxima a minima funkcí

(a) $f(x,y) = e^{1+x^2-y^2}$,

(b) $f(x_1,x_2,x_3) = x_1^2 + 3x_2^2 - 3x_1x_2 + 4x_2x_3 + 6x_3^2$,

(c) $f(x_1,x_2,x_3) = x_1x_3 + x_1^2 - x_2 + x_2x_3 + x_2^2 + 3x_3^2$.

Na následujícím příkladě si ukážeme *metodu nejmenších čtverců* (the least squares method). Ta se používá hlavně ve statistice při regresní analýze, což je jedna z nejpoužívanějších (ne-li nejpoužívanější) metoda analyzování dat.

Cvičení 9.12 Představme si, že máme program, který nějakým způsobem zpracovává text. Z teoretické analýzy víme, že délka běhu tohoto programu závisí na mnoha faktorech, ale v zásadě je úměrná délce vstupu: tzn. „skoro

přesně platí“

$$t(n) = a + bn,$$

kde $t(n)$ je délka běhu pro text délky n a a, b jsou neznámé parametry.

Po získání vstupu od uživatele byste chtěli vypsat hlášku: „Zpracování Vašeho textu bude trvat asi x vteřin.“, jak co nejlépe odhadnout hodnotu x?

Cvičení 9.13 Uvažujme funkci $f(x, y) = x^3 + xy + y^2$.

Prověřte, zda je v následujících bodech lokální extrém funkce f:

a) $(0, 0)$;

b) $(-2, 6)$;

c) $(0, 5)$;

d) $\left(\frac{1}{6}, -\frac{1}{12}\right)$.

Co byste si měli z tohoto cvičení odnést:

- Jak sestavit Lagrangeovu funkci pro optimalizaci s vazbami ve tvaru rovností.
- Jak najít kritické body a rozhodnout o jejich povaze (ostrá lok. maxima/minima)

A co byste se měli doučit, pokud to ještě/už neumíte:

- Hledat lokální extrémy funkcí více proměnných bez vazeb.

10 Vázané extrémy s rovnostními podmínkami: Lagrangeova metoda

V tomto cvičení budeme řešit následující úlohu: hledáme opět lokální extrémy funkce více (reálných) proměnných

$$f(x_1, x_2, \ldots, x_n),$$

ovšem pouze pro množinu takových $x_1, x_2, \ldots, x_n$, které splňují následující podmínky:

$$\begin{aligned} g_1(x_1, x_2, \ldots, x_n) &= 0 \\ g_2(x_1, x_2, \ldots, x_n) &= 0 \\ &\vdots \\ g_m(x_1, x_2, \ldots, x_n) &= 0. \end{aligned}$$

Označme si množinu všech $x_1, x_2, \ldots, x_n$ splňujících těchto p rovnic jako $\mathcal{M}$, tedy

$$\mathcal{M} = \{(x_1, x_2, \ldots, x_n) \in \mathbb{R}^n \colon g_i(x_1, x_2, \ldots, x_n) = 0, i = 1, 2, \ldots, m\}.$$

Aby všechno, co píšeme níže, platilo (tj. bylo možné dokázat), je třeba o funkcích f a g_i něco málo předpokládat (a tedy ověřit): funkce f a g_i mají spojité všechny druhé parciální derivace (jsou z $C_2(\mathbb{R}^n)$).

Začneme příkladem, který lze spočítat bez využití Lagrangeovy metody.

Cvičení 10.1 Najděte všechna lokální maxima a minima funkce $f(x, y) = 3x - 4y + 3$ na množině bodů kružnice $x^2 + y^2 = 4$. ?

a) Využijte faktu, že graf funkce f je (nakloněná) rovina, a extrémy najděte s využitím znalosti gradientu (a jeho geometrické interpretace).

b) Převeďte úlohu na problém hledání extrémů funkce jedné proměnné pomocí parametrizace kružnice.

■

Funkci $L : \mathcal{M} \times \mathbb{R}^m \to \mathbb{R}$ definovanou

$$L(x; \lambda) = f(x) + \sum_{j=1}^{m} \lambda_j g_j(x)$$

nazýváme **Lagrangeovou funkcí** pro danou úlohu.

Věta 10.1 — Postačující podmínka existence ostrého lokálního minima pro rovnostní vazby. Nechť $f, g_j, j \in \{1, \ldots, m\}$ mají spojité všechny druhé parciální derivace na nějaké otevřené nadmnožině $\tilde{\mathcal{M}} \supset \mathcal{M}$. Pokud dvojice $(x^*; \lambda^*) \in \mathbb{R}^n \times \mathbb{R}^m$ splňuje podmínky: !

(0) (0. derivace) $x^* \in \mathcal{M}$;

(1) (1. derivace) $\forall i, \frac{\partial L}{\partial x_i}(x^*; \lambda^*) = 0$;

(2) (2. derivace) pro každý (sloupcový) vektor $0 \neq v \in \mathbb{R}^n$ splňující

$$\nabla g_j(x^*) \cdot v = 0, \quad \text{pro } \forall j \in \{1, \ldots, m\},$$

platí

$$v^T \cdot \nabla_x^2 L(x^*; \lambda^*) \cdot v > 0;$$

kde $\nabla_x^2 L$ je Hessova matice funkce L vzhledem k proměnným $x = (x_1, x_2, \ldots, x_n)$, potom je x^* bodem ostrého lokálního minima.

Všimněme si, že body (0) a (1) jsou ekvivalentní rovnosti $\nabla L(x^*;\lambda^*)=0$.

Cvičení 10.2 Najděte všechny extrémy a určete jejich povahu pro funkci a vazbu z cvičení 10.1. ■

Základní cvičení 10.3 Najděte lokální extrémy funkce $f(x,y)=\frac{x^3}{3}-x+y^2$ za podmínky

a) $g(x,y)=y-1=0$;

b) $g(x,y)=y=0$;

c) $g(x,y)=x^2+2x+y^2=0$.

■

Cvičení 10.4 Najděte lokální extrémy funkce $f(x,y)=xy$ na množině zadané podmínkou

$$x+y=1.$$

Cvičení 10.5 Najděte lokální extrémy funkce $f(x,y)=x^2+y^2$ na množině zadané podmínkou

$$\frac{x}{a}+\frac{y}{b}=1,$$

kde a a b jsou nenulová reálná čísla.

Cvičení 10.6 Najděte lokální extrémy funkce $f(x,y)=2x^2-2y^2$ na množině zadané podmínkou

$$y+e^{-x^2}=1.$$

Cvičení 10.7 Najděte lokální extrémy funkce $f(x,y)=\cos^2 x+\cos^2 y$ na množině zadané podmínkou

$$x-y=\frac{\pi}{4}.$$

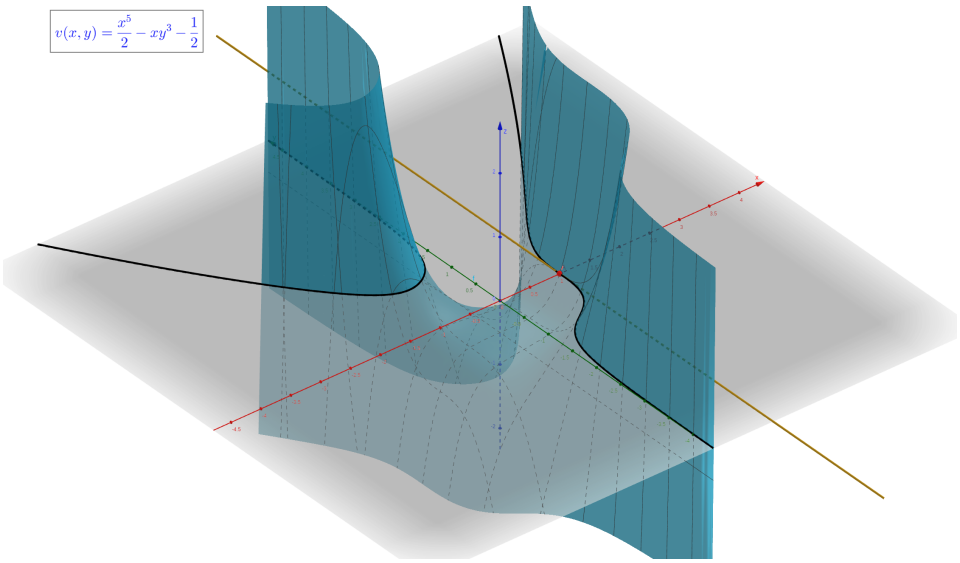
Cvičení 10.8 Najděte lokální extrémy funkce $f(x,y,z)=xyz$ na množině zadané podmínkami

$$x+y+z=5 \quad \text{a} \quad xy+yz+zx=8.$$

Geometrická představa Lagrangeovy metody se mimo jiné opírá o fakt, že gradient je kolmý na tečnu na vrstevnici, pokud tato tečna existuje. Toto vyjádření i naše představivost vyžaduje, aby funkce měla pouze dvě proměnné. Vrstevnicí je myšlena množina bodů, jejichž funkční hodnota je rovna zafixované konstantě. K dokázání tohoto faktu je třeba věta o implicitní funkci a její derivaci.

Kolmost je zachována i pro funkce více než 2 proměnných s tím, že

- pojem vrstevnice je někdy rezervován pro $\mathbb{R}^2$, obecně lze hovořit o „množině bodů s konstantní funkční hodnotou“ (*level set*):
$$D_f(c)=\{(x_1,\dots,x_n)\in D_f\colon f(x_1,\dots,x_n)=c\};$$
- místo tečny je nutno hovořit o tečném prostoru.



Obrázek 1: Vyobrazení vrstevnice z cvičení 10.9.

Cvičení 10.9 — Kolmost gradientu a tečny vrstevnice v $\mathbb{R}^2$. Pro funkci $f(x,y) = \frac{x^5}{2} - xy^3$ uvažujte její vrstevnici

$$D_f\left(\frac{1}{2}\right) = \left\{(x,y)\colon f(x,y) = \frac{1}{2}\right\}.$$

(Ilustrace na obrázku 10 níže.)

1. Ukažte, že pro každý bod $A \in D_f\left(\frac{1}{2}\right)$ existuje okolí $H(A)$ takové, že množinu $H(A) \cap D_f\left(\frac{1}{2}\right)$ je lze jednoznačně vyjádřiti jako graf funkce φ proměnné x nebo jako graf funkce ψ proměnné y.
2. Ukažte, že v každém bodě $A \in D_f\left(\frac{1}{2}\right)$ je gradient funkce f kolmý na tečnu ke grafu funkce φ nebo ψ z bodu (1).
3. Pro body $(1,0)$ a $(2,2)$ napište rovnici tečny ke grafu funkce z bodu (1).
4. Uvažme vrstevnici $D_f(0)$. Ve kterých bodech ji nelze lokálně popsat implicitní funkcí? Porovnejte s obrázkem 10.

11 Vázané extrémy s rovnostními podmínkami a nerovnostními podmínkami

Základní cvičení 11.1 Najděte lokální extrémy funkce $f(x,y) = x^2 + y$ za podmínky

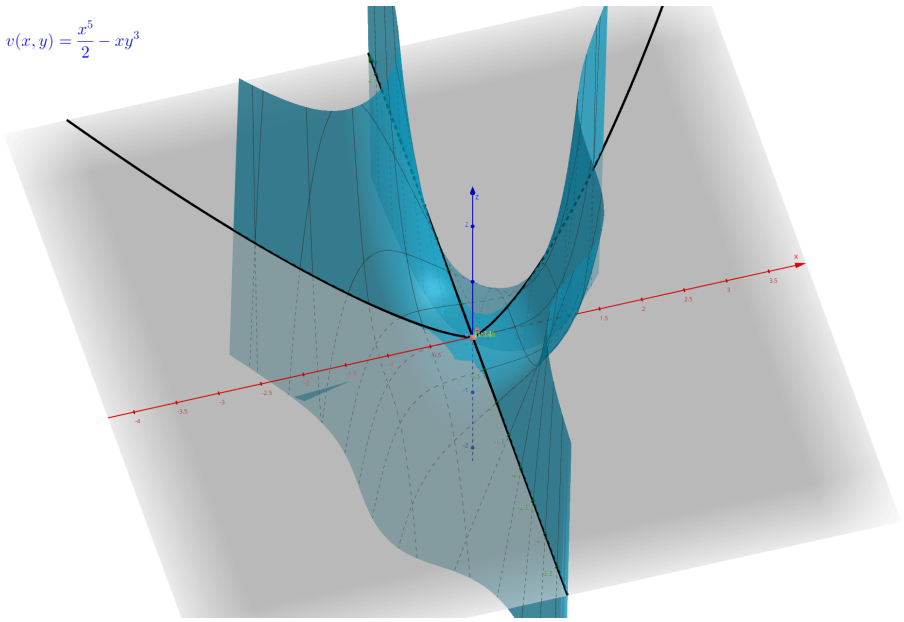
$$h(x,y) = x^2 + y^2 \leq 1.$$

Základní cvičení 11.2 Najděte lokální extrémy funkce $f(x,y) = \frac{x^3}{3} - x + y^2$ za podmínky

$$h(x,y) = x^2 + 2x + y^2 \leq 0.$$

Cvičení 11.3 Najděte lokální extrémy funkce $f(x,y) = x^2 - y^2$ na množině zadané podmínkou

$$x^2 + y^2 \leq 4$$



Obrázek 2: Vyobrazení vrstevnice z cvičení 10.9(4).

Cvičení 11.4 Uvažujme funkce $f(x,y) = x^3 + xy + y^2$ a $h(x,y) = x + 2y - 10$.

Prověřte, zda jsou body z následujícího seznamu, body lokálního extrému funkce f vzhledem k podmínce $h(x,y) \leq 0$:

a) $(0,0)$;

b) $(-2,6)$;

c) $(0,5)$;

d) $\left(\frac{1}{6}, -\frac{1}{12}\right)$;

Co byste si měli z tohoto cvičení odnést:

- Jak spočítat vícerozměrný integrál přes obdélníkovou a obecnou oblast.
- Jak provést substituci ve vícerozměrném intergrálu.

A co byste se měli doučit pokud to ještě/už neumíte:

- Integrovat funkce jedné proměnné.

12 Integrály přes obdélníkovou oblast

Při výpočtech využíváme násl. větu, která nám dovoluje problém integrace přes více proměnných převést (v „rozumných“ případech) na integraci přes jednu proměnnou.

Věta 12.1 Buď $f(x,y)$ integrabilní funkce na $D=[a,b]\times[c,d]$. Pokud existuje jeden z integrálů

$$\int_a^b\left(\int_c^d f(x,y)\mathrm{d}y\right)\mathrm{d}x \quad \text{nebo} \int_c^d\left(\int_a^b f(x,y)\mathrm{d}x\right)\mathrm{d}y$$

potom je roven dvojnému integrálu

$$\iint_D f(x,y)\mathrm{d}x\mathrm{d}y\,.$$

Základní cvičení 12.1 Buď $f(x,y)=\frac{x^2}{1+y^2}$ a $D=[2,3]\times[0,3]$. Spočítejte

$$\int_D f(x,y)\mathrm{d}x\mathrm{d}y.$$

Cvičení 12.2 Buď $f(x,y)=e^{2x+y}$ a $D=[0,1]\times[0,3]$. Spočítejte

$$\iint_D f(x,y)\mathrm{d}x\mathrm{d}y$$

Cvičení 12.3 Buď $f(x,y)=\sin(x+y)$ a $D=[0,\pi]\times[0,2\pi]$. Spočítejte

$$\iint_D f(x,y)\mathrm{d}x\mathrm{d}y$$

Cvičení 12.4 Spočítejte objem tělesa ohraničeného rovinami $x=0, x=3, y=-1, y=1, z=0$ a plochou $z=f(x,y)=x^2+y^2$.

Cvičení 12.5 Buď $f(x,y,z)=(x+2y+3z)^2$ a $D=[0,1]\times[-\frac{1}{2},0]\times[0,\frac{1}{3}]$. Spočítejte

$$\iiint_D f(x,y,z)\mathrm{d}x\mathrm{d}y\mathrm{d}z$$

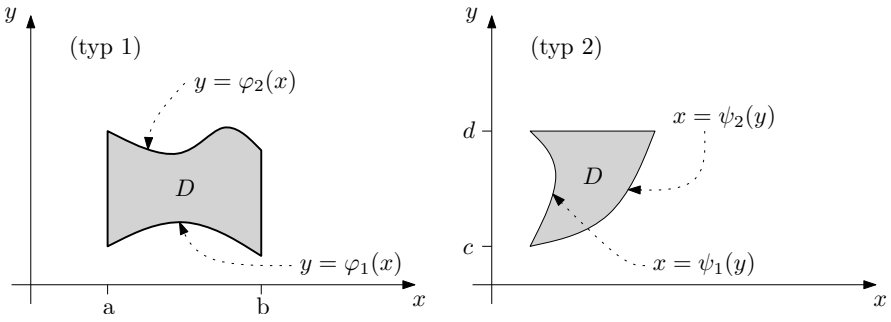
Cvičení 12.6 Buď $f(x,y,z) = e^{x+y+z}$ a $D = [0,1] \times [0,1] \times [0,1]$. Spočítejte

$$\iiint_D f(x,y,z)\mathrm{d}x\mathrm{d}y\mathrm{d}z$$

13 Integrály přes obecnou oblast

Budeme uvažovat dva typy oblastí:

- (typ 1) x je z intervalu $[a,b]$ a y je omezené spoj. funkcemi $\varphi_1(x)$ a $\varphi_2(x)$ splňujícími $\varphi_1(x) \leq \varphi_2(x)$ pro všechna $x \in [a,b]$,
- (typ 2) y je z intervalu $[c,d]$ a x je omezené spoj. funkcemi $\psi_1(y)$ a $\psi_2(y)$ splňujícími $\psi_1(y) \leq \psi_2(y)$ pro všechna $y \in [c,d]$.



A integrály přes takovéto oblasti budeme počítat dle následující věty.

Věta 13.1 Pokud integrály napravo existují, platí pro oblast D, že

- je-li D typu 1, máme

$$\iint_D f(x,y)\mathrm{d}x\mathrm{d}y = \int_a^b \left(\int_{\varphi_1(x)}^{\varphi_2(x)} f(x,y)\mathrm{d}y \right) \mathrm{d}x.$$

- je-li D typu 2, máme

$$\iint_D f(x,y)\mathrm{d}x\mathrm{d}y = \int_c^d \left(\int_{\psi_1(y)}^{\psi_2(y)} f(x,y)\mathrm{d}x \right) \mathrm{d}y.$$

Základní cvičení 13.1 Buď $f(x,y) = xy$. Spočítejte

$$\int_D f(x,y)\mathrm{d}x\mathrm{d}y,$$

kde D je omezená množina ohraničená křivkami $y^2 = x$ a $y = x - 2$.

Cvičení 13.2 Vypočítejte

$$\iint_D (x+y)\mathrm{d}x\mathrm{d}y\,,$$

kde D je oblast pod grafem funkce $y = x^2$ pro $x \in [0, \frac{1}{2}]$.

Cvičení 13.3 Vypočítejte

$$\iint_D (x+y)^2\mathrm{d}x\mathrm{d}y\,,$$

kde D je „vyplněný“ trojúhelník s vrcholy $(0,0)$, $(0,1)$ a $(2,2)$.

Cvičení 13.4 Vypočítejte

$$\int_0^1 \int_x^1 xy \mathrm{d}y \mathrm{d}x\,.$$

Cvičení 13.5 Vypočítejte

$$\int_0^1 \int_{1-y}^1 (x+y^2) \mathrm{d}x \mathrm{d}y\,.$$

Cvičení 13.6 Vypočítejte

$$\iint_D (x-y) \mathrm{d}x \mathrm{d}y\,,$$

kde D je „vyplněný“ trojúhelník s vrcholy $(0,0)$, $(1,0)$ a $(2,1)$.

14 Substituce v integrálu

Mějme $\Psi : \mathbb{R}^n \to \mathbb{R}^n$, $\Psi(\mathbf{v}) = (\Psi_1(\mathbf{v}), \ldots, \Psi_n(\mathbf{v}))$. **Jacobiho matice** funkce Ψ je následující zobrazení $\mathbb{R}^n \to \mathbb{R}^{n,n}$ (pro $\mathbf{v} = (v_1, v_2, \ldots, v_n)$)

$$J_\Psi = \begin{pmatrix} \frac{\partial \Psi_1}{\partial v_1} & \cdots & \frac{\partial \Psi_1}{\partial v_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial \Psi_n}{\partial v_1} & \cdots & \frac{\partial \Psi_n}{\partial v_n} \end{pmatrix},$$

pokud všechny parciální derivace existují.

Věta 14.1 Nechť D je omezená uzavřená množina na $\mathbb{R}^n$. Nechť $\Psi : \mathbb{R}^n \to \mathbb{R}^n$ má spojité všechny parciální derivace (všech složek) na nějaké otevřené nadmnožině množiny D a *skoro všude* na D platí, že Ψ je bijekce a $\det J_\Psi$ je nenulový. Potom pro každou spojitou funkci $f : D \to \mathbb{R}$ platí

$$\int_{\psi(D)} f(\mathbf{x}) \mathrm{d}\mathbf{x} = \int_D f(\Psi(\mathbf{v})) \left|\det J_\Psi(\mathbf{v})\right| \mathrm{d}\mathbf{v}$$

kde $\mathbf{x} = (x_1, x_2, \ldots, x_n)$.

Základní cvičení 14.1 Buď $f(x,y) = 3x + 2y - 1$. Spočítejte

$$\int_D f(x,y) \mathrm{d}x \mathrm{d}y,$$

kde $D = \{(x,y) \colon 1 \le x^2 + y^2 \le 4 \text{ a } x \le y\}$.

Cvičení 14.2 Spočtěte

$$\iint_D xy \mathrm{d}x \mathrm{d}y,$$

kde $D = \{(x,y) \in \mathbb{R}^2 \colon x \le y \le x+1, 1-x \le y \le 2-x\}$.
Použijte substituci $u = x + y, v = x - y$.

Cvičení 14.3 Spočtěte

$$\iint_D \sqrt{x^2+y^2} \mathrm{d}x \mathrm{d}y,$$

kde $D = \{(x, y) \in \mathbb{R}^2 : 1 \leq x^2 + y^2 \leq 4, x \leq y \leq \sqrt{3}x\}$.

Cvičení 14.4 Mějme desku ve tvaru čtvrtkruhu o poloměru r. Plošná hustota desky v daném bodě je rovna druhé mocnině vzdálenosti tohoto bodu od středu kruhu. Spočtěte souřadnice těžiště této desky. ?

Cvičení 14.5 Vypočtěte objem (3D) koule o poloměru r. ■ ?

15 Strojová čísla

Cvičení 15.1 Jak přesně bude vypadat 32 bitů reprezentujících následující čísla (uvažujeme jednoduchou přesnost, pouze normalizovaná čísla a zaokrouhlování směrem k nule – první bit je znaménko, pak exponent a pak signifikant): ?

a) $-1/13$,

b) $1/17$,

c) součet těchto (reprezentovaných) čísel.

Nápověda: nejprve si vyjádřete čísla ve dvojkové soustavě.

Základní cvičení 15.2 Jak přesně bude vypadat 32 bitů reprezentujících následující čísla (uvažujeme jednoduchou přesnost, pouze normalizovaná čísla a zaokrouhlování k nejbližšímu, nerozhodné směrem od nuly – první bit je znaménko, pak exponent a pak signifikant): !

a) $-1/5$,

b) $2/3$,

c) součet těchto (reprezentovaných) čísel.

■

Cvičení 15.3 Formát bfloat16 je alternativa k binary16, a má následující parametry: na signifikand je 7 bitů a na exponent je 8 bitů. Parametr b, posun exponentu, je 127. Porovnejte rozsah a relativní přesnosti tohoto formátu s formátem binary16. ? ■

16 Odhady v numerických algoritmech

Lemma 16.1. *Pokud* $|\delta_i| \leq \mathbf{u}$ *a* $|\rho_i| = 1$ *pro všechna* $i \in \{1, \ldots, n\}$, $n\mathbf{u} < 1$, *tak platí*

$$\prod_{i=1}^{n}(1+\delta_i)^{\rho_i} = 1 + \Theta_n,$$

kde $|\Theta_n| \leq \dfrac{n\mathbf{u}}{1-n\mathbf{u}}$.

Následující značení se hodí pro počítání nakumulovaných chyb (zanedbává přesnou hodnotu nakumulované chyby):

Značení 16.2. $\langle n \rangle = \prod_{i=1}^{n}(1+\delta_i)^{\rho_i}$

Cvičení 16.1 Dokažte lemma 16.1. ?

Základní cvičení 16.2 Mějme pevně danou množinu strojových čísel F (např. v jednoduché přesnosti) a uvažujme standardní model aritmetických operací.

Uvažujme algoritmus $V : F^n \to F$, který počítá skalární součin, tedy

$$V(x_1, x_2, \ldots, x_n) = \alpha_1 x_1 + \alpha_2 x_2 + \ldots \alpha_n x_n,$$

kde $\alpha \in F$ jsou pevně zvolené parametry. !

1. Odhadněte dopřednou chybu.
2. Odhadněte zpětnou chybu.

Předpokládáme, že nedojde k podtečení, přetečení apod. ■

Základní cvičení 16.3 Mějme pevně danou množinu strojových čísel F (např. v jednoduché přesnosti) a uvažujme standardní model aritmetických operací.

Uvažujme zobrazení $p : x \mapsto (x-2)^9$ a 3 způsoby jeho výpočtu: !

a) $p_a(x) = (x-2)^9$;

b) $p_b(x) = x^9 - 18x^8 + 144x^7 - 672x^6 + 2016x^5 - 4032x^4 + 5376x^3 - 4608x^2 + 2304x - 512$;

c) $p_c(x) = -512 + x\,(2304 + x\,(-4608 + x\,(\ldots)))$ (Hornerova metoda/pravidlo).

Uvažujme algoritmus $V_z : F \to F : x \mapsto p_z(x)$ pro $z \in \{a, b, c\}$ (tedy počítá fukční hodnotu $p(x)$ 3 výše uvedenými způsoby).

Pro všechny 3 varianty

1. odhadněte dopřednou chybu, a
2. odhadněte zpětnou chybu.

Předpokládáme, že nedojde k podtečení, přetečení apod. ■

Co byste si měli z tohoto cvičení odnést:

- jak poznat, že je něco grupoid / pologrupa / monoid / grupa,
- najít a poznat podgrupy různých grup.

A co byste se měli doučit, pokud to ještě/už neumíte:

- stačí znát z přednášky definice a základní vlastnosti výše zmíněných pojmů.

17 Grupoid, monoid, pologrupa, grupa – definice

Definice 17.1 Grupoid je uspořádaná dvojice $(M, \circ)$, kde M je libovolná neprázdná množina a $\circ$ je binární operace na M.

- Pologrupa je grupoid $(M, \circ)$, pro který je $\circ$ asociativní operace.
- Monoid je pologrupa $(M, \circ)$, ve které existuje neutrální prvek e takový, že

$$\text{pro všechna } a \in M \quad \text{platí} \quad e \circ a = a \circ e = a.$$

- Grupa je monoid $(M, \circ)$, ve kterém ke každému $a \in M$ existuje inverzní prvek a^{-1} takový, že

$$a^{-1} \circ a = a \circ a^{-1} = e.$$

- Komutativní (abelovská) grupa je grupa $(M, \circ)$, kde $\circ$ je komutativní operace.

Základní cvičení 17.1 Určete, které z následujících číselných množin s uvedenou operací tvoří grupoid / pologrupu / monoid / grupu / abelovskou grupu. Pokud existuje, najděte neutrální prvek a zjistěte, jak vypadají inverzní prvky.

(a) $(\mathbb{R}_0^+, +)$,

(b) $(\mathbb{R}_0^+, \cdot)$,

(c) $(\mathbb{R} \setminus \{0\}, \div)$,

(d) $(\mathbb{Q}, -)$,

(e) $(\mathbb{Q}, \cdot)$,

(f) $(\mathbb{Q}, +)$.

Cvičení 17.2 Buď M množina všech prostých reálných funkcí jejichž definiční obor je roven $\mathbb{R}$.

(a) Je M uzavřená vůči operaci skládání funkcí? Tzn. platí $f \circ g \in M$ pro všechny funkce $f, g \in M$?

(b) Je M uzavřená vůči operaci inverze funkce? Tzn. platí $f^{-1} \in M$ pro všechny funkce $f \in M$?

Je M s operací skládání funkcí grupoid / pologrupa / monoid / grupa / abelovská grupa?

Základní cvičení 17.3 Mějme množinu $M = \{0, 1, \ldots, n-1\}$. Rozhodněte, zda tvoří dvojice $(M, \circ)$ grupoid / pologrupu / monoid / grupu / abelovskou grupu pokud je operace „$\circ$“

(a) sčítání modulo n.

(b) násobení modulo n.

Cvičení 17.4 Mějme množinu $M = \{0, 1, 2, 3, 4, 5\}$. Odeberte z M co nejméně prvků tak, aby výsledná množina spolu s násobením modulo 6 tvořila grupu.

Cvičení 17.5 Mějme množinu $M = \{0, 1, \ldots, n-1\}$. Jaké prvky musíme z M odebrat, aby výsledná množina tvořila spolu s operací násobení modulo n grupu?

Cvičení 17.6 Buď P množina všech reálných polynomů. Je P uzavřená vůči derivaci? Tzn. platí $p \in P \Rightarrow p' \in P$? ■

Cvičení 17.7 Najděte co nejmenší množinu $M \subset \mathbb{R}$ obsahující alespoň dva prvky takovou, aby s operací dělení tvořila grupu. Je výsledná grupa abelovská?

Cvičení 17.8 Najděte co nejmenší množinu $M \subset \mathbb{R}$ obsahující číslo 1 takovou, aby s operací sčítání tvořila grupu.

Cvičení 17.9 Určete, které z následujících číselných množin s uvedenou operací tvoří grupoid / pologrupu / monoid / grupu / abelovskou grupu. Pokud existuje, najděte neutrální prvek a zjistěte jak vypadají inverzní prvky.

(a) $(\mathbb{Q}, \circ)$, kde $a \circ b = a^b$,

(b) $(\mathbb{N} \setminus \{0\}, \circ)$, kde $a \circ b = a^b$,

(c) $(\{-1, 1\}, \circ)$, kde $a \circ b = a^b$,

(d) $(\mathbb{R}, \circ)$, kde $a \circ b = a + b + 1$,

(e) $(\mathbb{R}, \circ)$, kde $a \circ b = a + b + ab$,

(f) $(\mathbb{R}^2, \circ)$, kde $A \circ B$ je střed úsečky mezi body A a B,

(g) $(\mathbb{N} \setminus \{0\}, \circ)$, kde $n \circ m = \gcd(n, m)$.

Cvičení 17.10 Tvoří potenční množina neprázdné množiny spolu s operací sjednocení množin grupu? ■

Cvičení 17.11 Tvoří potenční množina neprázdné množiny spolu s operací průniku množin grupu? ■

Cvičení 17.12 Buď $M = \{(a, b) \mid a, b \in \mathbb{R}, a < 0 < b\}$ (tj. množina otevřených omezených intervalů obsahujících nulu). Rozhodněte, jestli M s operací sjednocení $\cup$ tvoří grupoid / pologrupu. Přidejte do M jeden prvek tak, aby vznikl monoid.

Cvičení 17.13 Buď $M = \{(a, b) \mid a, b \in \mathbb{R}, a < 0 < b\}$ (tj. množina otevřených omezených intervalů obsahujících nulu). Rozhodněte, jestli M s operací průniku $\cap$ tvoří grupoid / pologrupu. Přidejte do M jeden prvek tak, aby vznikl monoid.

Cvičení 17.14 Uvažujme množinu $M = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

(i) Tvoří M s operací sčítání čísel grupu? Pokud ne, přidejte/uberte co nejméně prvků tak, aby $(M, +)$ byla grupa.

(ii) Tvoří M s operací násobení čísel grupu? Pokud ne, přidejte/uberte co nejméně prvků tak, aby $(M, \cdot)$ byla

grupa.

Cvičení 17.15 Je následující tabulka Cayleyovou tabulkou abelovské grupy?

	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

Cvičení 17.16 Dokažte, že každá grupa řádu menšího než 4 je abelovská.

18 Podgrupy

Definice 18.1 Buď $G = (M, \circ)$ grupa. Podgrupou grupy G nazveme libovolnou dvojici $H = (N, \circ)$ takovou, že

- $N \subset M$,
- $H = (N, \circ)$ je grupa.

Základní cvičení 18.1 Mějme grupu $\mathbb{Z}_8^\times$. Kolik má prvků? Najděte všechny vlastní podgrupy této grupy.

Cvičení 18.2 Které z následujících množin jsou podgrupou grupy $(\mathbb{Q} \setminus \{0\}, \cdot)$?

(a) množina sudých celý čísel bez nuly,

(b) množina lichých celých čísel,

(c) $\{2^n : n \in \mathbb{Z}\}$,

(d) $\{2^n \cdot 3^m : n, m \in \mathbb{Z}\}$,

(e) $\left\{\frac{1+2n}{1+2m} : n, m \in \mathbb{Z}\right\}$

Cvičení 18.3 Najděte všechny podgrupy grupy zadané násl. tabulkou.

	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

Cvičení 18.4 Je množina $G = \{a + b\sqrt{2} : a, b \in \mathbb{Q}, a \neq 0 \vee b \neq 0\}$ podgrupou grupy $(\mathbb{R} \setminus \{0\}, \cdot)$?

Cvičení 18.5 Mějme monoid $(M, \circ)$ a označme $G := \{a \in M : a \text{ je invertibilní}\}$. Zjistěte a odůvodněte, zda musí být $(G, \circ)$ grupa.

Co byste si měli z tohoto cvičení odnést:

- jak najít podgrupy generované množinami,
- jak najít efektivně generátory multiplikativních grup modulo prvočíslo p.

A co byste se měli doučit, pokud to ještě/už neumíte:

- stačí znát z přednášky definice a základní vlastnosti výše zmíněných pojmů.

19 Cyklické grupy a generátory

Cvičení 19.1 Najděte všechny generátory a všechny podgrupy grupy $\mathbb{Z}_{15}^{+}$. Najděte také inverzní prvky ke všem prvkům. ■

Cvičení 19.2 Najděte konečnou grupu, která má podgrupy řádu $3, 5$ a 7. ■

Cvičení 19.3 Najděte podgrupu grupy $(\mathbb{Z}, +)$ generovanou množinou

(a) $\{2\}$,

(b) $\{2, 3\}$,

(c) $\{2, 5\}$,

(d) $\{6, 15\}$,

(e) $\{n, m\}$, kde $n \neq m$ jsou kladná přirozená čísla.

Cvičení 19.4 Popište jak vypadají podgrupy cyklické grupy $(\mathbb{Z}, +)$.

Známe z přednášky: Je-li $(G, \circ)$ cyklická grupa řádu n a a nějaký její generátor, potom a^k je také generátor tehdy a jen tehdy, když k a n jsou nesoudělná (tj. $\gcd(k, n) = 1$).

Cvičení 19.5 Najděte všechny generátory a všechny podgrupy grupy $\mathbb{Z}_{11}^{\times}$. Najděte také inverzní prvky ke všem prvkům. ■

Cvičení 19.6 Najděte všechny generátory a všechny podgrupy grupy $\mathbb{Z}_{17}^{\times}$. Najděte také inverzní prvky ke všem prvkům. ■

Cvičení 19.7 Najděte nejmenší podgrupu grupy regulárních matic z $\mathbb{R}^{3,3}$ s klasickým maticovým násobením, která obsahuje matici

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

(a) Je tato podgrupa cyklická?

(b) Je cyklická výše zmíněná grupa všech regulárních matic z $\mathbb{R}^{3,3}$?

■

Cvičení 19.8 Najděte všechny generátory a podgrupy aditivní grupy modulo 22, tj. grupy $\mathbb{Z}_{22}^{+}$.

Cvičení 19.9 Najděte všechna kladná $n \in \mathbb{Z}$ taková, že grupa $\mathbb{Z}_n^\times$ má řád 12.

Cvičení 19.10 Najděte nejmenší podgrupu grupy $(\mathbb{R}^+, \cdot)$ kladných reálných čísel s klasickým násobením, která obsahuje

(a) čísla 5 a 10;

(b) všechna prvočísla.

Cvičení 19.11 Buďte f a g dvě permutace z S_9, kde

$$f = (2,4,5,6,3,1,8,9,7) \quad \text{a} \quad g = (8,1,5,2,6,3,7,9,4)\,.$$

(a) Čemu se rovná $f \circ g$?

(b) Čemu se rovná $\langle f \rangle$, tzn. nejmenší podgrupa S_n obsahující f?

(c) Čemu se rovná $f^{100} \circ g^{100}$?

Cvičení 19.12 Nalezněte grupu G a dva její prvky a, b řádu 3 takové, že prvek $c = a \circ b$ nemá řád 3 a není neutrální. Může být grupa G abelovská? ■

20 Generátory grup $\mathbb{Z}_p^\times$

Cvičení 20.1 Jaká je pravděpodobnost, že náhodně zvolený prvek grupy $\mathbb{Z}_{23}^\times$ je generátor?

Základní cvičení 20.2

(a) Je 5 generátor grupy $\mathbb{Z}_{23}^\times$? (Pokuste se toto ověřit či vyvrátit bez nutnosti výčtu množiny generované prvkem 5.)

(b) Je 2 generátor grupy $\mathbb{Z}_{23}^\times$?

(c) Nalezněte všechny generátory grupy $\mathbb{Z}_{23}^\times$.

Základní cvičení 20.3 Ukažte že množina $H = \{a^{11} : a \in \mathbb{Z}_{23}^\times\}$ je podgrupa grupy $\mathbb{Z}_{23}^\times$ a zjistěte její řád. ■

Cvičení 20.4 Mějme libovolná přirozená čísla k a n. Ukažte že množina $H = \{a^k : a \in \mathbb{Z}_n^\times\}$ je podgrupa grupy $\mathbb{Z}_n^\times$ a zjistěte (popiště a zdůvodněte), pro která k se jedná o vlastní podgrupu. ■

Cvičení 20.5 Nalezněte nosnou množinu grupy $\mathbb{Z}_{18}^\times$ a všechny její generátory.

Cvičení 20.6 Nalezněte nosnou množinu grupy $\mathbb{Z}_{30}^\times$ a všechny její generátory.

Co byste si měli z tohoto cvičení odnést:

- Jak poznat homomorfismus a najít izomorfismus grup.

A co byste se měli doučit, pokud to ještě/už neumíte:

- stačí znát z přednášky definice a základní vlastnosti výše zmíněných pojmů.

21 Homomorfismus a izomorfismus

Cvičení 21.1 Zjistěte, která z následujících zobrazení jsou homomorfismem a která z nich jsou izomorfismy (pro dané grupoidy). ?

(a) Zobrazení $f(n) = 3n + 2$ z grupy $(\mathbb{Z}, +)$ do $(\mathbb{R}, +)$.

(b) Zobrazení $f(x) = 2^x$ z grupy $(\mathbb{R}, +)$ do $(\mathbb{R}^+, \cdot)$.

(c) Zobrazení $f(A) = A_{1,1}$ z grupy reálných matic dimenze $n \times n$ se sčítáním po prvcích $(\mathbb{R}^{n\times n}, +)$ do $(\mathbb{R}, +)$.

(d) Zobrazení $f(A) = A_{1,1}$ z grupy regulárních reálných matic dimenze $n \times n$ s maticovým násobením $(\mathbb{R}^{n\times n}_{\text{reg}}, \cdot)$ do $(\mathbb{R}, \cdot)$.

Cvičení 21.2 Najděte nějaký homomorfismus grupy regulárních reálných matic s maticovým násobením $(\mathbb{R}^{n\times n}_{\text{reg}}, \cdot)$ do $(\mathbb{R}, \cdot)$. ?

Cvičení 21.3 Je $\mathbb{Z}_{10}^\times$ izomorfní s $\mathbb{Z}_5^\times$? Pokud ano, najděte nějaký izomorfismus. ?

Základní cvičení 21.4 Pro prvočíslo p popište, jak byste našli izomorfismus grupy $\mathbb{Z}_p^\times$ s grupou $\mathbb{Z}_{p-1}^+$. Kolik různých izomorfismů existuje? !

Cvičení 21.5 Mějme grupy G a H, kde $G := \mathbb{Z}_5^+$ a $H := \mathbb{Z}_{13}^\times$. Nalezněte všechny homomorfismy z G do H a zdůvodněte, že jsou všechny. ?

Cvičení 21.6 Buď $\varphi : G \to H$ nějaký homomorfismus grup $G = \mathbb{Z}_{12}^+$ a $H = \mathbb{Z}_6^+$. Ukažte, že $\varphi(4) \neq 5$. ?

22 Diskrétní logaritmus

Cvičení 22.1 Vyřešte rovnici ?

$$5^x \equiv 12 \pmod{23}.$$

Cvičení 22.2 Anastázie chce předat Bořivojovi tajnou zprávu během hodiny dějepisu a tak Bořivojovi naprosto veřejně pošle papírek říkající: „Bořivoji, něco Ti pošlu a použiji Diffie-Hellmana. Můj veřejný klíč je prvočíslo 29, generátor 8 a vypočítané číslo 24“. Bořivoj na to: „Jasně, Anastázie, moje je 15“. Anastázie: „Super, je-li n naše sdílené tajemství, tak se sejdeme $(n - 2 \mod 7)$-tý den příštího týdne v $n - 7$ hodin na hřbitově u hrobu číslo $5n + 6$. Tož zatím!“ Kdy a kde se Anastázie a Bořivoj setkají? ?

Co byste si měli z tohoto cvičení odnést:

- Jak poznat, jestli daná trojice „množina a dvě binární operace“ tvoří okruh nebo těleso.
- Jak počítat v tělesech, kde se násobí modulo ireducibilní polynom.

A co byste se měli doučit, pokud to ještě/už neumíte:

- Jak funguje rozšířený Euklidův algoritmus.
- Co je to ireducibilní polynom.

23 Okruhy a tělesa

Definice 23.1 — okruh (*ring*). Buďte M neprázdná množina a $+$ a $\cdot$ binární operace na této množině. Řekneme, že trojice $R = (M, +, \cdot)$ je okruh, pokud platí:

- $(M, +)$ je **abelovská grupa**,
- $(M, \cdot)$ je **monoid**,
- platí (levý a pravý) **distributivní zákon**:

$$(\forall a, b, c \in M)\big(a(b + c) = ab + ac \wedge (b + c)a = ba + ca\big).$$

Definice 23.2 — těleso (*field*). Okruh $T = (M, +, \cdot)$ se nazývá těleso, jestliže $(M \setminus \{0\}, \cdot)$ je abelovská grupa. Tuto grupu nazýváme multiplikativní grupou tělesa T.

Cvičení 23.1 Zjistěte, zda následující množina s operacemi obvyklého sčítání a násobení čísel tvoří okruh:

(a) Množina celých sudých čísel.

(b) Množina celých lichých čísel.

(c) Množina celých čísel.

(d) Množina nezáporných celých čísel.

(e) Množina racionálních čísel.

Cvičení 23.2

(a) Je množina matic $(\mathbb{R}^{n,n}, +, \cdot)$ se sčítáním po prvcích a maticovým násobením okruhem?

(b) Je tělesem? Pokud není, jakou podmnožinu jejího nosiče lze vzít, aby tělesem byla (při použití stejných binárních operací)?

Cvičení 23.3 Uvažujme nějakou abelovskou grupu $G = (M, +)$ a množinu všech homomorfismů z G do G. Označme ji $\mathrm{End}(G)$ (takovému homomorfismu se říká endomorfismus). Zaveďme sčítání homomorfismů $f, g \in \mathrm{End}(G)$ takto:

$$\forall x \in G, (f + g)(x) = f(x) + g(x).$$

Je $(\mathrm{End}(G), +, \circ)$ okruhem? Je tělesem? Symbolem $\circ$ značíme skládání zobrazení jako v předchozích cvičeních. ■

24 Konečná tělesa řádu p^n

Jako další zajímavý studijní materiál je k dispozici ukázkový SageMath Jupyter notebook.

Pro hledání inverzních prvků v $\mathbb{Z}_n^\times$ se používá rozšířený Euklidův algoritmus. Již byste jej měli znát, ale pro jistotu si jej nyní připomeneme.

Základní cvičení 24.1 V tělese $\mathbb{Z}_{263}$ najděte multiplikativní inverzi k prvku 112. !

Základní cvičení 24.2 Rozhodněte, zda je polynom $P(x)$ ireducibilní nad tělesem $\mathbb{Z}_5$, kde !

(a) $P(x) = x^3 + 2x + 1$;

(b) $P(x) = x^2 + 2x + 2$;

Základní cvičení 24.3 Rozhodněte, zda je polynom $P(x)$ ireducibilní nad tělesem $\mathbb{Z}_3$, kde !

(a) $P(x) = 2x^4 + x^3 + 2x + 1$;

(b) $P(x) = x^4 + x^3 + x + 2$;

(c) $P(x) = x^4 + x + 2$.

Cvičení 24.4 Sestavte Cayleyho tabulky pro obě operace pro těleso $GF(2^2)$, kde se násobí modulo x^2+x-1. Najděte neutrální prvky, generátory a inverzní prvek k $x+1$ a x. ?

Cvičení 24.5 Sestavte Cayleyho tabulku pro násobení pro těleso $GF(3^2)$, kde se násobí modulo $x^2 - x - 1$. ?

Cvičení 24.6 Najděte všechny ireducibilní polynomy z okruhu $\mathbb{Z}_2[x]$ stupně menšího než 5. ?

Základní cvičení 24.7 V tělese $GF(3^2)$, kde se násobí modulo ireducibilní polynom $x^2 + 2x + 2$, najděte !

(a) všechna y taková, aby $21(y + 11) = 01 + y$,

(b) najděte všechny generátory multiplikativní grupy tohoto tělesa.

Cvičení 24.8 Uvažujme těleso $GF(2^3)$, kde se násobí modulo $x^3 + x + 1$. ?

(a) Definujte pojem ireducibilní polynom nad tělesem $\mathbb{Z}_2$.

(b) Najděte inverzní prvek k prvku 010.

(c) Vypočítejte

$$100 \cdot (010)^{-1} + 010 \cdot 010$$

Cvičení 24.9 V tělese $GF(3^3)$ kde se násobí modulo $x^3 + 2x + 2$ najděte ?

(a) inverzní prvek k prvku 011,

(b) vypočtěte $101 \cdot 222$.

Cvičení 24.10 V tělese $GF(2^3)$, kde se násobí modulo x^3+x^2+1, najděte

(a) inverzní prvek k prvku 101,

(b) všechna y z tohoto tělesa splňující rovnici

$$101 \cdot (100+y) = 100\,.$$

Cvičení 24.11 Uvažujte těleso $GF(2^4)$, kde se počítá modulo polynom x^4+x^3+1.

(a) Najděte inverzi k prvku 1100.

(b) Vyřešte rovnici $(y+1010)(0101+1100) = 0110$.

(c) Najděte všechna y z tohoto tělesa splňující rovnici

$$y^2+y+1010 = 0000\,.$$

Cvičení 24.12 Buď α tzv. zlatý řez, tedy kořen polynomu x^2-x-1. Označme $\mathbb{Z}_3(\alpha) = \{a\alpha+b \mid a,b \in \mathbb{Z}_3\}$ množinu, kde se sčítá po složkách modulo 3 (např. $(\alpha+2)+(2\alpha+2) = 3\alpha+4 = 0\alpha+1 = 1$, v jiném zápisu $12+22=01$) a násobí klasicky (např. $(2\alpha+1)\cdot\alpha = 2\alpha^2+\alpha = 2(\alpha+1)+\alpha = 3\alpha+2 = 2$). Je $\mathbb{Z}_3(\alpha)$ těleso? Jestli ano, najděte Cayleyho tabulku pro násobení. (Srovnejte s Příkladem 24.5)

Cvičení 24.13 Nechť $v(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$ je polynom z okruhu $\mathbb{Z}_p[x]$, kde p je prvočíslo a m je kladné celé číslo. Dokažte že platí

$$(v(x))^p = v(x^p),$$

tj. že umocnit polynom $v(x)$ na p je to samé, jako do něho dosadit jako argument x^p.
[Nápověda: lze dokázat pomocí Fermatovy věty a vhodně použité binomické věty]

Cvičení 24.14 V tělese $GF(3^3)$, kde se násobí modulo ireducibilní polynom x^3+2x+1, najděte všechna y taková, aby $y^{107} = 111$.

Cvičení 24.15 Rozhodněte, jestli je polynom $4x^3+2x^2+4x+2$ ireducibilní nad $\mathbb{Z}_5$.

Základní cvičení 24.16 Mějme těleso $GF(5^3)$, kde se násobí modulo ireducibilní polynom x^3+3x+3.

(a) Nalezněte inverzní prvek vzhledem k násobení k prvku x^2+2x.

(b) Nalezněte všechna $y \in GF(5^3)$, která splňují $120 \cdot y^2 = 111$.

Cvičení 24.17 Mějme těleso $GF(5^3)$, kde se násobí modulo ireducibilní polynom x^3+3x+3.

(a) Nalezněte inverzní prvek vzhledem k násobení k prvku x^2+2x+1.

(b) Nalezněte všechna $y \in GF(5^3)$, která splňují $121 \cdot (y^2+y+1) = 101$.

Cvičení 24.18 Mějme dvě tělesa, , F a F', prvočíselného řádu p. Dokažte, že jsou tato tělesa izomorfní. ■ ?

Cvičení 24.19 Mějme dvě tělesa, F a F', řádu 8. V F se násobí modulo $x^3 + x + 1$ a v F' modulo $x^3 + x^2 + 1$. Nalezněte izomorfismus těchto dvou těles. ■ ?

Řešení

Řešení Cvičení 1.1: (a) $\sin(x-3)^3$, derivace $3(x-3)^2\cos(x-3)^3$ (b) $(\sin x-3)^3$, derivace $3(\sin x-3)^2\cos x$ (c) $\sin(\sqrt[3]{x}+3)$, derivace $\cos(\sqrt[3]{x}+3)\frac{1}{3}x^{-2/3}$ (d) $\sqrt[3]{\sin x}+3$, derivace $\frac{1}{3}(\sin x)^{-2/3}\cos x$

Řešení Cvičení 1.2: (a) $12x^{11}+33x^{10}$, (b) $2ae^{2ax}$, (c) $-\frac{1}{x^2}-\frac{6a}{x^3}$, (d) $\frac{15a}{x+4}$, (e) 0, (f) $(1+2x)e^{2x}$, (g) $2ax^{2a-1}e^{x^{2a}}$, (h) $(1+\ln x)x^x$

Řešení Cvičení 1.3: $a_n n!$

Řešení Cvičení 1.4: (a) $a=\pm 3^{-1/4}$, (b) $a\in\{0,1\}$

Řešení Cvičení 1.7: $x=2\pm\frac{1}{\sqrt{2}}$ km.

Řešení Cvičení 1.9: (a) např. e^{2x}, (b) např. $\cos(\sqrt{3}\cdot x)+\dfrac{1}{\sqrt{3}}\sin(\sqrt{3}\cdot x)$

Řešení Cvičení 2.2: kořeny jsou -3,-1,1

Řešení Cvičení 2.3: kořeny jsou -3,2,10

Řešení Cvičení 3.1: $\gcd(a,0)=|a|$ až na $\gcd(0,0)$, což není definováno. (V některých zdrojích naleznete, že $\gcd(0,0)=0$. Tento rozdíl je způsoben lehce odlišnou definicí největšího společného dělitele.)

Řešení Cvičení 3.3: $1=23\cdot 523-97\cdot 124$; $\quad -7\cdot 321+10\cdot 225=3$

Řešení Cvičení 3.4: Obecně lze nakombinovat jakoukouliv cenu větší než nebo rovnou $(a-1)(b-1)$, kde a a b jsou nesoudělné ceny známek. (Důkaz tohoto faktu není rovnou vidět, je třeba trošku zapracovat...)

Spočítáme cenu v našem případě $2\frac{1-3^9}{1-3}=2\frac{19683-1}{2}=19682$.

Spočítáme Bézoutovy koeficienty: $-7\cdot 47+15\cdot 22=1$.

Tedy $19682\cdot(-7)\cdot 47+19682\cdot 15\cdot 22=19682$ a rovností $22\cdot 47-47\cdot 22=0$ vyrobíme kladné koeficienty, aby princezna nemusela lepit na pohled dlužní úpisy na známky.

Hledáme k takové, aby $19682\cdot(-7)+k\cdot 22>0$.

Najdeme $k=6263$ a máme $19682\cdot(-7)+22\cdot 6263=12$ a $19682\cdot 15-47\cdot 6263=869$, tedy $12\cdot 47+869\cdot 22=19682$ a drak se může těšit na psaníčko!

Řešení Cvičení 4.1: Jelikož čísla $p_i^{k_i}$ v produktu jsou navzájem nesoudělná, platí

$$\varphi(n)=\prod_{i=1}^{m}\varphi(p_i^{k_i}).$$

Je snadné ověřit, že pro lib. prvočíslo p a přirozené kladné k platí $\varphi(p^k)=p^k-p^{k-1}$, neboť soudělná čísla s p^k jsou pouze násobky p a těch je mezi čísly od 1 do p^k právě $p^k/p=p^{k-1}$. Z tohoto již pak snadno plyne, že

$$\varphi(n)=\prod_{i=1}^{m}p_i^{k_i}\left(1-\frac{1}{p_i}\right)=n\prod_{p\mid n}\left(1-\frac{1}{p}\right).$$

Řešení Cvičení 4.2: (a) 36, (b) 144

Řešení Cvičení 6.1: (a) $y+e^x\cos y$ resp. $x-e^x\sin y$, (b) $\pi/2$, (c) $2xy^3+3x^2y^4-y^2e^{xy^2}$ resp. $3x^2y^2+4x^3y^3-2xye^{xy^2}$, (d) $-\dfrac{2}{9}\cos\left(\dfrac{2}{3}\right)$.

Řešení Cvičení 6.2: v bodě $(0,0)$ protože je tam špičatá: derivace ani podle x a podle y není definovaná.

Řešení Cvičení 6.3: (a) $2y^2$ resp. $2x^2$, (b) $-y^2\sin(xy)$ resp. $-x^2\sin(xy)$, (c) $-ye^{-x}+\cos(x-y)$ resp. $2x+\cos(x-y)$

Řešení Cvičení 6.4: (a) obě jsou $-\sin x$, (b) obě jsou $-z\sin(xy)-xyz\cos(xy)+z\cos(yz)$

Řešení Cvičení 7.1: (a) $\left(x/\sqrt{x^2+y^2+z^2},y/\sqrt{x^2+y^2+z^2},z/\sqrt{x^2+y^2+z^2}\right)$, (b) $(y+z,x+z,x+y)$, (c) $(1,2y,3z^2)$, (f) $((1+2x^2)e^{x^2+y^2},2xye^{x^2+y^2})$

Řešení Cvičení 7.4: Měl by vyrazit ve směru $-\nabla T(1,1,1)$, tedy $(e^{-1},2e^{-2},-3e^3)$.

Řešení Cvičení 7.5: (Náznak) Nejdříve sestavme funkci hledaného řezu jako funkci jedné proměnné: jedná se o přímku, kterou lze parametrizovat pomocí bodu a směrového vektoru např. takto

$$(0,0)+t(1,2).$$

Aby vzdálenosti 2 odpovídala hodnota $t=2$, je třeba aby ten vektor měl normu (délku) 1, máme tedy

$$(0,0)+t(1,2)\frac{1}{\sqrt{5}}.$$

Nyní už dostáváme příslušnou jednorozměrnou funkci

$$f(t)=z\left(0+\frac{1}{\sqrt{5}}t,0+\frac{2}{\sqrt{5}}t\right)=\left(\frac{t}{\sqrt{5}}\right)^2+3\left(\frac{2t}{\sqrt{5}}\right)^2$$

Derivace v bodě $t=2$ je tedy

$$4/5+48/5=52/5.$$

Nyní spočítejme čemu se rovná výraz

$$\nabla z\left(\frac{2}{\sqrt{5}},\frac{4}{\sqrt{5}}\right)\cdot\left(\frac{1}{\sqrt{5}},\frac{2}{\sqrt{5}}\right)=\left(2\frac{2}{\sqrt{5}},6\frac{4}{\sqrt{5}}\right)\cdot\left(\frac{1}{\sqrt{5}},\frac{2}{\sqrt{5}}\right)=4/5+48/5=52/5.$$

Připomeňme, že bod na přímce $y=2x$ se vzdáleností 2 od počátku je $(2/\sqrt{5},4/\sqrt{5})$.

Řešení Cvičení 7.7: Jelikož je krajina nakloněná rovina, závisí rychlost pouze na směru, neboť gradient je konstantní:

$$r(x,y,\vec{s})=20-40\arctan\left(\frac{s_1}{2}+\frac{s_2}{3}\right)$$

Řešení Cvičení 7.8:

$$r(x,y,\vec{s})=20-40\arctan\left((x+y)(s_1+s_2)\right)$$

Řešení Cvičení 7.9:

$$z=\frac{\partial f}{\partial x}(x_0,y_0)\cdot(x-x_0)+\frac{\partial f}{\partial y}(x_0,y_0)\cdot(y-y_0)+f(x_0,y_0)$$

Srovnejte s rovnicí tečny jednorozměrné funkce!

Řešení Cvičení 8.3: (a) $(0,0)$, (b) $(0,0,0)$, (c) $(0,0)$, (d) $(0,0)$, (e) $(0,0)$ a body na kružnicích $x^2+y^2=k\pi+\pi/2, k\in\mathbb{N}$

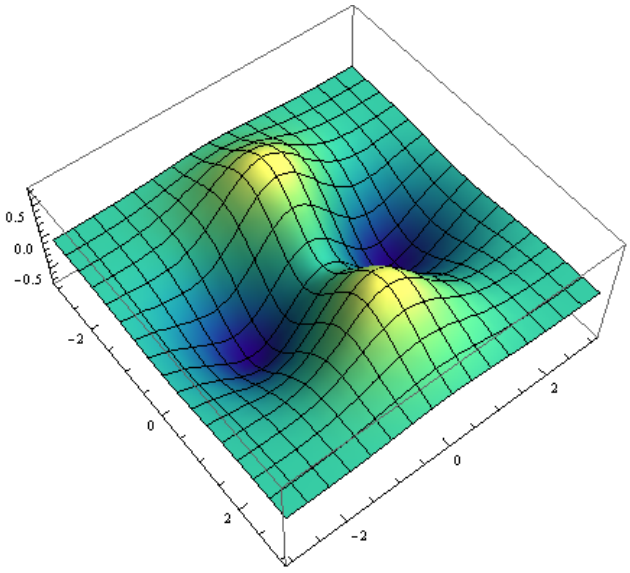
Řešení Cvičení 8.4: (a) $f(0,0)=1$ díky známe limitě $\lim_{r\to 0}\sin r/r=1$, (b) na kružnicích, jejichž poloměr splňuje $\pi r=\tan(\pi r)$

Řešení Cvičení 9.3: (a) matice $[2y^2,4xy\mid 4xy,2x^2]$, (b) matice $[e^{-(x+y)},e^{-(x+y)}\mid e^{-(x+y)},e^{-(x+y)}]$, (c) diagonální matice $\operatorname{diag}(2,6y,12z^2)$.

Řešení Cvičení 9.5: pro $A>0$ a $AC-B^2>0$ se jedná o ostré minimum, pro $A<0$ a $AC-B^2>0$ o maximum a pro $AC-B^2<0$ ani o jedno

Řešení Cvičení 9.6: (a) bod $(0,0)$ je jediný krit. bod, ale není ani maximem ani minimem, je to sedlový bod, (b) bod $(0,0)$ je jediný krit. bod a jedná se o minimum

Řešení Cvičení 9.7: $(0,0)$ je sedlo, $(\sqrt{2},0),(-\sqrt{2},0)$ jsou lok. maxima a $(0,\sqrt{2}),(0,-\sqrt{2})$ lok. minima



Řešení Cvičení 9.8: $(6/11, 18/11, -6/11)$

Řešení Cvičení 9.9: $(1/2, 1, \sqrt{5}/2)$, $(1/2, 1, -\sqrt{5}/2)$

Řešení Cvičení 9.10: musí mít co nejmenší povrch, tedy $8 \times 8 \times 4$ cm

Řešení Cvičení 9.11: (a) jediný krit. bod je $(0, 0)$ ale není ani max. ani min, (b) jediný krit. bod je $(0, 0, 0)$, je to lok. minimum, (c) jediný krit. bod je $(1/20, 11/20, -2/20)$, je to lok. minimum

Řešení Cvičení 10.1: v bodě (6/5,-8/5) je ostré lok. maximum a v bodě (-6/5,8/5) je ostré lok. minimum

Řešení Cvičení 10.4: maximum v bodě (1/2, 1/2)

Řešení Cvičení 10.5: minimum v bodě $\left(\frac{ab^2}{a^2+b^2}, \frac{a^2b}{a^2+b^2}\right)$

Řešení Cvičení 10.6: v bodě $(0, 0)$ je ostré lokální minimum.

Řešení Cvičení 10.7: extrémy jsou body (x, y), kde $x = \frac{\pi}{8} + k\frac{\pi}{2}$ a $y = -\frac{\pi}{8} + k\frac{\pi}{2}$ pro všechna $k \in \mathbb{Z}$. Pro lichá k se jedná o minima, pro sudá o maxima.

Řešení Cvičení 10.8: minima v bodech (2,2,1), (2,1,2) a (1,2,2) a maxima v $\frac{1}{3}(4, 4, 7)$, $\frac{1}{3}(4, 7, 4)$ a $\frac{1}{3}(7, 4, 4)$

Řešení Cvičení 10.9:

1. Ukažte že gradient f je ve všech bodech f nenulový a užijte větu o implicitní funkci.
2. Užitím věty o implicitní funkci nalzněte směrový vektor tečny v obecném bodě $A \in V$ a ukažte, že jeho skalární součin s gradientem je 0.
3. V bodě $(1, 0)$: $x = 1$, v bodě $(2, 2)$: $y = \frac{4}{3}x - \frac{2}{3}$.

Řešení Cvičení 11.3: $(0, \pm 2)$ je minimum a $(\pm 2, 0)$ maximum

Řešení Cvičení 12.2:

$$\iint_D e^{2x+y}\mathrm{d}x\mathrm{d}y = \int_0^3 \left(\int_0^1 e^{2x+y}\mathrm{d}x\right)\mathrm{d}y = \int_0^3 \left[\frac{1}{2}e^{2x+y}\right]_{x=0}^1 \mathrm{d}y = \frac{1}{2}\int_0^3 (e^{2+y} - e^y)\mathrm{d}y =$$
$$= \frac{1}{2}(e^2 - 1)\int_0^3 e^y \mathrm{d}y = \frac{(e^2-1)(e^3-1)}{2}$$

Řešení Cvičení 12.3: 0 (plocha pod rovinou danou osami x a y se počítá jako záporná, stejně jako v případě funkcí jedné proměnné)

Řešení Cvičení 12.4: 20

Řešení Cvičení 12.5: $\frac{1}{12}$

Řešení Cvičení 12.6: $(e-1)^3$

Řešení Cvičení 13.2:

$$\iint_D (x+y)\mathrm{d}x\mathrm{d}y = \int_0^{1/2} \left(\int_0^{x^2} (x+y)\mathrm{d}y\right)\mathrm{d}x = \int_0^{1/2} \left[xy + \frac{y^2}{2}\right]_{y=0}^{x^2} \mathrm{d}x = \int_0^{1/2} (x^3 + \frac{x^4}{2}\mathrm{d}x = \left[\frac{x^4}{4} + \frac{x^5}{10}\right]_0^{1/2} = \frac{3}{160}$$

Řešení Cvičení 13.3:

$$\iint_D (x+y)^2\mathrm{d}x\mathrm{d}y = \int_0^2 \left(\int_x^{x/2+1} (x+y)^2\mathrm{d}y\right)\mathrm{d}x = \cdots = \frac{21}{6}$$

Řešení Cvičení 13.4: $\frac{1}{8}$

Řešení Cvičení 13.5: $\frac{7}{12}$

Řešení Cvičení 13.6: $\frac{1}{3}$

Řešení Cvičení 14.2: $\frac{1}{4}$

Řešení Cvičení 14.3: $\frac{7\pi}{36}$

Řešení Cvičení 14.4: Těžiště je ve vzdálenoti $\frac{9r\sqrt{2}}{5\pi}$ od středu kruhu na jeho ose zrcadlové symetrie (souřadnice záleží na volbě souřadného systému).

Řešení Cvičení 15.1: Nejprve musíme najít binární reprezentaci zadaných čísel. Použijeme k tomu hladový algoritmus. Jelikož 1/13 nelze zapsat ve tvaru $n/2^\ell$, kde n a ℓ jsou celá čísla, bude binární reprezentace nekonečná a periodická. Najdeme k tak, že $2^{k+1} > 1/13 \geq 2^k$, zřejmě $k = -4$. Čtvrtý bit za tečkou a_{-4} tedy bude první nenulový a $r_{-4} = \frac{1/13}{1/2^4} - 1 = 3/13$.

Pokračujeme následovně:

$$\begin{aligned}
a_{-5} &= \left\lfloor 2\frac{3}{13} \right\rfloor = 0 \qquad & r_{-5} &= \frac{6}{13} - 0 = \frac{6}{13} \\
a_{-6} &= \left\lfloor 2\frac{6}{13} \right\rfloor = 0 \qquad & r_{-6} &= \frac{12}{13} - 0 = \frac{12}{13} \\
a_{-7} &= \left\lfloor 2\frac{12}{13} \right\rfloor = 1 \qquad & r_{-7} &= \frac{24}{13} - 1 = \frac{11}{13} \\
a_{-8} &= \left\lfloor 2\frac{11}{13} \right\rfloor = 1 \qquad & r_{-8} &= \frac{22}{13} - 1 = \frac{9}{13} \\
a_{-9} &= \left\lfloor 2\frac{9}{13} \right\rfloor = 1 \qquad & r_{-9} &= \frac{18}{13} - 1 = \frac{5}{13} \\
a_{-10} &= \left\lfloor 2\frac{5}{13} \right\rfloor = 0 \qquad & r_{-10} &= \frac{10}{13} - 0 = \frac{10}{13} \\
a_{-11} &= \left\lfloor 2\frac{10}{13} \right\rfloor = 1 \qquad & r_{-11} &= \frac{20}{13} - 1 = \frac{7}{13} \\
a_{-12} &= \left\lfloor 2\frac{7}{13} \right\rfloor = 1 \qquad & r_{-12} &= \frac{14}{13} - 1 = \frac{1}{13} \\
a_{-13} &= \left\lfloor 2\frac{1}{13} \right\rfloor = 0 \qquad & r_{-13} &= \frac{2}{13} - 0 = \frac{2}{13} \\
a_{-14} &= \left\lfloor 2\frac{2}{13} \right\rfloor = 0 \qquad & r_{-14} &= \frac{4}{13} - 0 = \frac{4}{13} \\
a_{-15} &= \left\lfloor 2\frac{4}{13} \right\rfloor = 0 \qquad & r_{-15} &= \frac{8}{13} - 0 = \frac{8}{13} \\
a_{-16} &= \left\lfloor 2\frac{8}{13} \right\rfloor = 1 \qquad & r_{-16} &= \frac{16}{13} - 1 = \frac{3}{13}
\end{aligned}$$

a jelikož $r_{-4} = r_{-16}$ budou se další bity periodicky opakovat ($a_{-17} = a_{-5}$, $a_{-18} = a_{-6}$, atd.), získáváme tedy binární reprezentaci

$$-1/13 = -(0.000\overline{1100111011000})_2,$$

kde čarou označujeme opakující se část reprezentace. Tu můžeme přepsat do tvaru

$$-1/13 = (-1)^1(1.\overline{001110110001})_2 2^{123-127},$$

z čehož je již jasné, že reprezentace ve tvaru $s|e|m$ je

$$1|01111011|00111011000100111011000.$$

Pro 1/17 postupujeme stejně, najdeme k tak, že $2^{k+1} > 1/17 \geq 2^k$, zřejmě $k = -5$. Pátý bit za tečkou a_{-5} tedy bude první nenulový a $r_{-5} = \frac{1/17}{1/2^5} - 1 = 15/17$. Pokračujeme následovně:

$$\begin{aligned}
a_{-6} &= \left\lfloor 2\frac{15}{17} \right\rfloor = 1 \qquad & r_{-6} &= \frac{30}{17} - 1 = \frac{13}{17} \\
a_{-7} &= \left\lfloor 2\frac{13}{17} \right\rfloor = 1 \qquad & r_{-7} &= \frac{26}{17} - 1 = \frac{9}{17} \\
a_{-8} &= \left\lfloor 2\frac{9}{17} \right\rfloor = 1 \qquad & r_{-8} &= \frac{18}{17} - 1 = \frac{1}{17}
\end{aligned}$$

$$
\begin{aligned}
a_{-9} &= \left\lfloor 2\frac{1}{17} \right\rfloor = 0 \qquad & r_{-9} &= \frac{2}{17} - 0 = \frac{2}{17} \\
a_{-10} &= \left\lfloor 2\frac{2}{17} \right\rfloor = 0 \qquad & r_{-10} &= \frac{4}{17} - 0 = \frac{4}{17} \\
a_{-11} &= \left\lfloor 2\frac{4}{17} \right\rfloor = 0 \qquad & r_{-11} &= \frac{8}{17} - 0 = \frac{8}{17} \\
a_{-12} &= \left\lfloor 2\frac{8}{17} \right\rfloor = 0 \qquad & r_{-12} &= \frac{16}{17} - 0 = \frac{16}{17} \\
a_{-13} &= \left\lfloor 2\frac{16}{17} \right\rfloor = 1 \qquad & r_{-13} &= \frac{32}{17} - 1 = \frac{15}{17} \\
a_{-14} &= \left\lfloor 2\frac{15}{17} \right\rfloor = 1 \qquad & r_{-14} &= \frac{30}{17} - 1 = \frac{13}{17}
\end{aligned}
$$

a jelikož $r_{-6} = r_{-14}$ budou se další bity periodicky opakovat ($a_{-15} = a_{-7}$, $a_{-16} = a_{-8}$, atd.), získáváme tedy binární reprezentaci

$$1/17 = (0.\overline{00001111})_2.$$

Tu můžeme přepsat do tvaru

$$1/17 = (-1)^0(1.\overline{11100001})_2 2^{122-127},$$

z čehož je již jasné, že reprezentace ve tvaru $s|e|m$ je

$$0|01111010|11100001111000011110000.$$

Pro jednoduší a čitelnější postup reprezentujeme číslo 1/13 - 1/17 a pak otočíme znaménko. Čísla si napíšeme ve tvaru součtu mocnin čísla 2:

$$1/13 = 2^{-4}\left(1 + 2^{-3} + 2^{-4} + 2^{-5} + 2^{-7} + 2^{-8} + 2^{-12} + 2^{-15} + 2^{-16} + 2^{-17} + 2^{-19} + 2^{-20}\right)$$

a podobně pro 1/17 (aby se čísla lépe odečítala, uděláme to tak, aby před závorkou bylo 2^{-4})

$$1/17 = 2^{-4}\left(2^{-1} + 2^{-2} + 2^{-3} + 2^{-4} + 2^{-9} + 2^{-10} + 2^{-11} + 2^{-12} + 2^{-17} + 2^{-18} + 2^{-19} + 2^{-20}\right).$$

Při odečítání využijeme toho, že $1 - 2^{-1} - 2^{-2} = 2^{-2}$, $2^{-8} - 2^{-9} - 2^{-10} - 2^{-11} = 2^{-11}$ a $2^{-16} - 2^{-18} = 2^{-17} + 2^{-18}$, a dostaneme výsledek

$$2^{-6}\left(1 + 2^{-3} + 2^{-5} + 2^{-9} + 2^{-13} + 2^{-15} + 2^{-16}\right)$$

což dává (otáčíme znaménko a $e = 121$)

$$1|01111001|00101000100010110000000.$$

Řešení Cvičení 16.1: Důkaz. Dokážeme indukcí.

$n = 1$ a $\rho_1 = 1$, pak $|\Theta_1| = |\delta_1| \leq \mathbf{u} < \dfrac{\mathbf{u}}{1-\mathbf{u}}$.

$n = 1$ a $\rho_1 = -1$, pak $\frac{1}{1+\delta_1} = 1 - \frac{\delta_1}{1+\delta_1}$ a tedy $|\Theta_1| = \frac{|\delta_1|}{|1+\delta_1|} \leq \dfrac{\mathbf{u}}{1-\mathbf{u}}$. Předpokládejme, že tvrzení platí pro $n = j-1$.

Nechť $\rho_j = 1$, pak $\prod_{i=1}^{j}(1+\delta_i)^{\rho_i} = (1+\Theta_{j-1})(1+\delta_j) = 1 + \underbrace{\delta_j + \Theta_{j-1} + \delta_j\Theta_{j-1}}_{\Theta_j}$.

$|\Theta_j| \leq |\delta_j| + |\Theta_{j-1}| + |\delta_j\Theta_{j-1}| \leq \mathbf{u} + \dfrac{(j-1)\mathbf{u}}{1-(j-1)\mathbf{u}} + \dfrac{(j-1)\mathbf{u}^2}{1-(j-1)\mathbf{u}}$,

výraz sečteme a dostaneme $\dfrac{j\mathbf{u}}{1-(j-1)\mathbf{u}} \leq \dfrac{j\mathbf{u}}{1-j\mathbf{u}}$.

Nechť $\rho_j = -1$, pak $\prod_{i=1}^{j}(1+\delta_i)^{\rho_i} = \dfrac{1+\Theta_{j-1}}{1+\delta_j} = 1 + \underbrace{\dfrac{-\delta_j + \Theta_{j-1}}{1+\delta_j}}_{\Theta_j}$.

$|\Theta_j| \leq \dfrac{|\delta_j|}{|1+\delta_j|} + \dfrac{|\Theta_{j-1}|}{|1+\delta_j|} \leq \dfrac{\mathbf{u}}{1-\mathbf{u}} + \dfrac{1}{1-\mathbf{u}}\dfrac{(j-1)\mathbf{u}}{1-(j-1)\mathbf{u}}$,

výraz sečteme a dostaneme $\dfrac{j\mathbf{u} - (j-1)\mathbf{u}^2}{1-j\mathbf{u}+j\mathbf{u}^2} \leq \dfrac{j\mathbf{u}}{1-j\mathbf{u}}$. ■

Řešení Cvičení 17.1: (a) monoid – chybí inverze, (b) monoid – chybí inverze k 0, (c) grupoid – není asociativní, (d) grupoid – není asociativní, (e) monoid – chybí inverze nuly, (f) abelovská grupa

Řešení Cvičení 17.2: (a) ano, (b) ne. Jde o monoid, operace skládání funkcí je asociativní a identické zobrazení je neutrální prvek.

Řešení Cvičení 17.3: (a) Jedná se o abelovskou grupu, kterou značíme $\mathbb{Z}_n^+$. (b) Jedná se o monoid s neutrálním prvkem 1, který je navíc komutativní. O grupu se nejedná, protože například k prvku 0 neexistuje prvek inverzní.

Řešení Cvičení 17.4: Z Cvičení 17.3 (b) víme, že M s uvedenou operací tvoří monoid s neutrálním prvkem 1. Aby vznikla grupa je třeba z M odebrat prvky $0, 2, 3$ a 4. K nim neexistuje prvek inverzní.

Řešení Cvičení 17.5: Musíme odebrat všechny prvky, které nemají multiplikativní inverzi modulo n (viz předmět BI-ZDM). To jsou všechna k z M taková, že $gcd(k, n) > 1$. S užitím Bézoutovy rovnosti a trochy přemýšlení lze nahlédnout, že to již stačí. Výslednou grupu značíme $\mathbb{Z}_n^\times$. **Pozor na to, že grupa $\mathbb{Z}_n^\times$ má VŽDY jinou nosnou množinu než grupa $\mathbb{Z}_n^+$.**

Řešení Cvičení 17.7: $M = \{1, -1\}$

Řešení Cvičení 17.8: $M = \mathbb{Z}$

Řešení Cvičení 17.9: (a) nic – není uzavřené na operaci, (b) grupoid – není asociativní, (c) pologrupa – chybí neutrální prvek (je tam jenom pravý), (d) abelovská grupa – neutr. prvek je -1, inverze $a^{-1} = -a - 2$, (e) monoid – neutrální prvek 0, ale -1 nemá inverzi, (f) grupoid – není asociativní, (g) pologrupa – je to asociativní, ale chybí neutrální prvek (důkaz toho, že takový prvek neexistuje, je vhodné provést sporem)

Řešení Cvičení 17.12: jedná se o grupid a i o pologrupu, jako neutrální prvek je možné vzít $\{0\}$ (tj. množinu obsahující pouze nulu) nebo $\emptyset$.

Řešení Cvičení 17.13: jedná se o grupid a i o pologrupu, jako neutrální prvek je možné vzít $\mathbb{R}$ (tj. množinu všech reálných čísel)

Řešení Cvičení 17.14: V prvním případě se o grupu zjevně jedná. Ve druhém je potřeba odebrat nulu, tj. prvek, kdy $a = b = 0$.

Řešení Cvičení 18.2: (a) ne, (b) ne, (c) ano, (d) ano, (e) ano

Řešení Cvičení 18.4: ano, je

Řešení Cvičení 18.5: Ano, $(G, \circ)$ je grupa.

Řešení Cvičení 19.3: (a) sudá čísla, (b) $(\mathbb{Z}, +)$, (c) $(\mathbb{Z}, +)$, (d) násobky tří, (e) násobky $\gcd(n, m)$

Řešení Cvičení 19.4: Z předchozího cvičení lze odvodit, že se bude jednat vždy o podgrupy tvaru $\langle k \rangle$, $k \in \mathbb{Z}$.

Řešení Cvičení 19.8: Obecný postup je následující. Najdeme nějaký generátor g: v grupě $\mathbb{Z}_{22}^+$ je to snadné, neboť očividným generátorem je 1. Potom využijeme větu, která říká, že g^k je generátor právě když k je nesoudělné s řádem grupy: v grupě $\mathbb{Z}_{22}^+$ se používá aditivní značení, takže místo g^k píšeme $k \times g$ a generátory jsou tedy čísla $k \times 1 = k$ nesoudělná s řádem grupy 22. Takových čísel je $\varphi(22) = \varphi(2)\varphi(11) = 1 \cdot 10 = 10$ (Eulerova funkce): $\{1, 3, 5, 7, 9, 13, 15, 17, 19, 21\}$.

Řešení Cvičení 19.9: Odpovědí je samozřejmě číslo 42, ale není samo. Všechna možná hledaná n můžeme najít díky tomu, že řád grupy $\mathbb{Z}_n^\times$ je roven $\varphi(n)$, kde φ je Eulerova funkce. Hledání n takových, že $\mathbb{Z}_n^\times$ má řád 12 tedy odpovídá řešení rovnice

$$\varphi(n) = 12.$$

Postupovat můžeme buď tak, že využijeme faktu, že pro hodnotu $\varphi(n)$ existují spodní odhady (vizte např. zde), a pak projdeme všechna n, pro která je tento odhad menší než 12. Tento postup je ale zoufale nematematický, a proto jej tady nebudeme rozpitvávat.

Zajímavější je postup analytický. Vyjdeme z toho, že $\varphi(n)$ se dá napsat jako součin výrazů tvaru $(p^k - p^{k-1})$, kde p^k je nejvyšší mocnina prvočísla p, která dělí n. Číslo 12 se dá napsat jako součin celých kladných čísel pouze osmi způsoby:

$$12 = 1 \cdot 12 = 2 \cdot 6 = 1 \cdot 2 \cdot 6 = 2 \cdot 2 \cdot 3 = 1 \cdot 2 \cdot 2 \cdot 3 = 4 \cdot 3 = 1 \cdot 4 \cdot 3.$$

Hledáme tedy prvočísla p a kladná celá čísla k taková, že výraz $(p^k - p^{k-1})$ se rovná 1, 2, 3, 4, 6 nebo 12. Snadno ověříme, že pro všechna uvažovaná p a k platí $(p^k - p^{k-1}) \geq p - 1$ a že $(p^k - p^{k-1})$ je rostoucí posloupností (vzhledem ke k). Proto platí $(p^k - p^{k-1}) = 1$ pouze pro $p = 2$ a $k = 1$, $(p^k - p^{k-1}) = 2$ pouze pro $p = 3$ a $k = 1$ resp. $p = 2$ a

$k = 2$ (pro větší hodnoty p a k už je výraz nutně větší než 2). Podobně dostaneme, že $(p^k - p^{k-1}) = 3$ nemá řešení. Z toho je zřejmé, že není třeba uvažovat poslední čtyři součiny ve výčtu výše:

$$2 \cdot 2 \cdot 3 = 1 \cdot 2 \cdot 2 \cdot 3 = 4 \cdot 3 = 1 \cdot 4 \cdot 3.$$

A zbývá tedy vyřešit rovnici $(p^k - p^{k-1}) = 6$ opět stačí uvažovat pouze prvočísla ostře menší než 8 a prvních pár hodnot k. Dostaneme pouhá dvě řešení: $p = 7$ a $k = 1$ resp. $p = 3$ a $k = 2$.

Celkově tedy dostáváme pro hledaná n násl. možnosti prvočíselných rozkladů:

$$n = 13, n = 2 \cdot 13, n = 3 \cdot 7, n = 2 \cdot 3 \cdot 7, n = 2^2 \cdot 7, n = 2^2 \cdot 3^2,$$

tedy čísla $13, 26, 21, 42, 28, 36$.

Řešení Cvičení 19.10: (a) Budeme doplňovat čísla do množiny $\{5, 10\}$ tak, aby byly splněny všechny požadavky na grupu.

1. Abychom zajistili uzavřenost vůči operaci násobení, musíme přidat $5 \cdot 5, 5 \cdot 5 \cdot 5, \ldots$ neboli všechny mocniny pětky $5^k, k = 1, 2, 3, \ldots$. Podobně pro 10 musíme přidat $10^\ell, \ell = 1, 2, 3, \ldots$. Množina ale stále není uzavřená, neb tam chybí např. součin $5^2 10^3$, proto musíme přidat všechna čísla tvaru $5^k 10^\ell$, kde alespoň jedno z nezáporných čísel k a ℓ je nenulové. Taková množina již je uzavřená.

2. Asociativita je vlastnost operace a operace násobení čísel je samozřejmě asociativní.

3. Neutrální prvek je číslo jedna a to nám tam stále chybí, proto umožníme i případ, kdy v $5^k 10^\ell$ jsou nulové k i ℓ, a tím získáme monoid: i po přidání čísla 1 množina zůstává uzavřená.

4. Inverze k prvku $5^k 10^\ell$ je číslo $5^{-k} 10^{-\ell}$, přidáme tam tedy i tato čísla a výsledek je množina

   $$\{5^k 10^\ell \mid k, \ell \in \mathbb{Z}\},$$

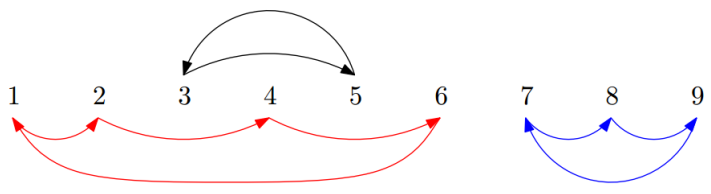
   která je uzavřená vůči násobení (to je třeba zkontrolovat pokaždé, když tam něco přidáme, neb by se uzavřenost mohla narušit), a tedy se již jedná o grupu. Z konstrukce je jasné, že se jedná o nejmenší možnou grupu.

(b) U množiny prvočísel postupujeme podobně: musíme přidat všechny kladné mocniny všech prvočísel, a pak také všechny jejich vzájemné součiny. Tím ale dostaneme všechna celá čísla ostře větší než 1 (každé takové číslo se dá napsat jako součin mocnin prvočísel!). Tak dostaneme grupoid. Asociativita opět platí a po přidání jedničky dostáváme monoid. Abychom dostali grupu, přidáme ke všem kladným celým číslům inverze: v množině tak máme čísla $1, 2, 3, \ldots$ a $1/2, 1/3, 1/4, \ldots$. Tato množina ale není uzavřená (např. chybí $3 \cdot 1/5$), proto musíme přidat i všechny vzájemné součiny a tím dostaneme $\mathbb{Q}^+$, množinu všech kladných racionálních čísel, která již tvoří grupu.

Řešení Cvičení 19.11: část (i): Zápis $f = (2, 4, 5, 6, 3, 1, 8, 9, 7)$ vlastně znamená, že $f(1) = 2, f(2) = 4, f(3) = 5$, a tak dále. Složení $f \circ g$ se pak konstruuje jako standardní složení zobrazení. Například $(f \circ g)(1) = f(g(1))$ a jelikož $g(1) = 8$ a $f(8) = 9$, je $(f \circ g)(1) = 9$. Opakováním této úvahy dostaneme, že

$$f \circ g = (9, 2, 3, 4, 1, 5, 8, 7, 6).$$

část (ii): Abychom lépe pochopili strukturu permutace f, nakreslíme si následující orientovaný graf: vrcholy budou čísla 1 až 9, tedy definiční obor f, a z vrcholu k povede vždy právě jedna šipka do vrcholu $f(k)$. Např. z 1 vedeme šipku do 2, z 2 do 4 atd. Výsledek vypadá takto:



Snadno si rozmyslíme, že pro každý vrchol platí, že z něho vede právě jedna šipka (neb f je zobrazení), a také že do něho vede právě jedna šipka (neb f je bijekce!). To nutně znamená, že se graf skládá z uzavřených nezávislých cyklů. Pro permutaci f jsou to cykly na vrcholech $1, 2, 4, 6$ (červené šipky), $3, 5$ (černé šipky) a $7, 8, 9$ (modré šipky). S pomocí tohoto grafu snadno zjistíme, jak vypadají mocniny f. Např. f^2 získáme tak, že vždy uděláme po šipkách dva kroky: 1 se zobrazí na 4, 2 na 6, 3 na 3 atd. Celkově

$$f^2 = (4, 6, 3, 1, 5, 2, 9, 7, 8).$$

Víme, že obecně platí

$$\langle f \rangle = \{f^k \ : \ k \in \mathbb{Z}\}.$$

Díky obrázku výše ovšem víme o permutaci f důležitou věc: mocnění f znamená pohyb po cyklech délky 4, 2 a 3. Nejmenší společný násobek těchto čísel je 12 a tak platí, že $f^{12} = f^0 = \mathrm{id}$. Z toho již plyne, že

$$\langle f \rangle = \{f^k \ : \ k \in \mathbb{Z}\} = \{f^0, f^1, f^2, \ldots, f^{11}\}.$$

Jak přesně tyto permutace vypadají získáme snadno z obrázku výše.
část (*iii*): Z předchozího bodu víme, že f^{100} se rovná f^4, protože $100 \equiv 4 \pmod{12}$. Abychom si zjednodušili podobně g^{100}, nakreslíme si opět příslušný orientovaný graf a z něho zjistíme, že g obsahuje cykly délek 5, 3 a 1. Nejmenší společný násobek těchto čísel je 15, a tedy platí $g^{100} = g^{10}$. Nyní už jednoduše zjistíme, že

$$f^{100} \circ g^{100} = f^4 \circ g^{10} = (1,2,3,4,5,6,8,9,7) \circ (1,2,5,4,6,3,7,8,9) = (1,2,5,4,6,3,8,9,7)\,.$$

Řešení Cvičení 20.1: Jelikož počet generátorů je $\varphi(22) = 10$, je pravděpodobnost rovna $10/22 = 0,45454545\cdots$.

Řešení Cvičení 20.2: (a) ano, je, (b) ne, není, (c) $\{5^k \mod 23 : gcd(k, 22) = 1\}$.

Řešení Cvičení 20.5: Nosná množina je $\{1, 5, 7, 11, 13, 17\}$ a generátory jsou prvky 5 a 11.

Řešení Cvičení 20.6: Nosná množina grupy $\mathbb{Z}_{30}^{\times}$ je množina $\{1, 7, 11, 13, 17, 19, 23, 29\}$. Dle věty z přednášky (30 není tvaru 2, 4, p^k, nebo $2p^k$, kde p je liché prvočíslo a k je kladné přirozené číslo) se nejedná o cyklickou grupu a proto její množina generátorů je prázdná.

Řešení Cvičení 21.1: (a) ne, (b) ano, je to i izomorfismus, (c) ano, izomorfismus ovšem pouze pro $n = 1$ (d) ne, pouze triviálně pro $n = 1$ jde o homomorfismus; izomorfismus to není nikdy

Řešení Cvičení 21.2: Například $f(A) = \det(A)$, $f(A) = \frac{1}{\det(A)}$ nebo $f(A) = |det(A)|$. Lze vzít obecněji také $f(A) = (\det(A))^k$ pro $k \in \mathbb{Z}$ a $f(A) = |\det(A)|^\ell$ pro $\ell \in \mathbb{R}$. Triviálně i $f(A) = 0$.

Řešení Cvičení 21.3: ano je, např. $1 \to 1, 2 \to 3, 3 \to 7, 4 \to 9$

Řešení Cvičení 21.4: Najdeme generátor g, izomorfismus je pak zobrazení které prvku g^k přiřadí k. Izomorfismů je stejně jako generátorů, tedy $\varphi(p-1)$.

Řešení Cvičení 22.2: $n = 25$, soukromý klíč Anastázie je 12 a Bořivoje 9.

Řešení Cvičení 23.1: (a) ani okruh (chybí neutrální prvek vůči násobení), (b) ani okruh, ani těleso, (c) okruh, ale ne těleso, (d) ani okruh (e) těleso.

Řešení Cvičení 23.2: Okruh ano, těleso ne. Ani podmínka regularity nestačí, neboť součet regulárních matic nemusí být regulární. Dokonce ani regulární diagonální nefungují.

Řešení Cvičení 24.1: jelikož $23 \cdot 263 + (-54) \cdot 112 = 1$, je $112 \cdot (-54) \equiv 1 \pmod{263}$ a tedy $112^{-1} = -54 \equiv 209 \pmod{263}$

Řešení Cvičení 24.3: (a) Protože $P(1) = 0$, má polynom kořen a není ireducibilní. (b)Snadno spočteme, že $P(0) = 2$, $P(1) = 2$, $P(2) = 1$. Proto $P(x)$ nemá kořen. Přesto není polynom $P(x)$ ireducibilní, neboť lze vyjádřit jako $P(x) = (x^2 + x + 2) \cdot (x^2 + 1)$. (c) $P(x)$ je ireducibilní.

Řešení Cvičení 24.4: Celkově tabulka pro operaci násobení vypadá takto:

$\cdot$	01	10	11
01	01	10	11
10	10	11	01
11	11	01	10

Generátory jsou jak 10 tak 11.

Řešení Cvičení 24.5: Náznak řešení:

$\cdot$	01	02	10	11	12	20	21	22
21	21	12	02	20	11	01	22	10

Využijte distributivního zákona! Např. víme-li, že $21 \cdot 01 = 21$ a $21 \cdot 10 = 02$, spočítáme $21 \cdot 12 = 21 \cdot (10 + 01 + 01) = 02 + 21 + 21 = 44 = 11$.

Řešení Cvičení 24.6: Polynomy stupně 1 jsou všechny ireducibilní, $x^2 + x + 1$ je jediný ireducibilní stupně 2, další ireducibilní jsou: $x^3 + x^2 + 1$, $x^3 + x + 1$, $x^4 + x + 1$, $x^4 + x^3 + 1$, $x^4 + x^3 + x^2 + x + 1$

Řešení Cvičení 24.7: (a) Jelikož x^2 se v této grupě rovná $x+1$ a $(2x+1)(x+1) = 2x^2+1 = 2x+2+1 = 2x$, můžeme rovnici pomocí distributivního zákona

$$21(y + 11) = 01 + y$$

přepsat do tvaru

$$21(y + 11) = 21y + 21 \cdot 11 = 21y + 20 = 01 + y.$$

K obou stranám rovnice přičteme $02y + 10$ a dostaneme

$$21y + 02y = 20y = 11.$$

Je třeba najít multiplikativní inverzi prvku 20. Pak po úpravě platí, že

$$y = 20^{-1} \cdot 11.$$

Inverzi k $20 = 2x$ najdeme buď pomocí rozšířeného Euklidova algoritmu, nebo si prostě všimneme, že

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

Dostáváme tak

$$y = 21 \cdot 11 = 20\,,$$

jak jsme již spočítali výše.

(b) Z přednášky víme, že multiplikativní grupy těles $GF(p^k)$ jsou vždy cyklické. Jelikož v případě $GF(3^2)$ má multiplikativní grupa řád 8 (prvek 00 musíme vyhodit), má celkem $\varphi(8) = 4$ generátorů. Zkusme jeden z nich najít a vygenerovat pomocí něho všechny ostatní prvky. Začněme např. s prvkem $10 = x$ (prvky 01 a 02 jistě generátory nejsou). Při násobení využíváme toho, že v zadaném tělese je $x^2 = x + 1$:

$$x^2 = x + 1, x^3 = x^2 + x = 2x + 1, x^4 = 2x^2 + x = 2, x^5 = 2x, x^6 = 2x + 2, x^7 = x + 2, x^8 = 1,$$

a tedy 10 je generátor.

Dále použijeme větu, která říká, že umocníme-li generátor na všechny exponenty nesoudělné s řádem (pro řád 8 tedy čísla 1,3,5,7), dostaneme všechny generátory. Dle tohoto návodu dostáváme výsledek: všechny generátory jsou prvky 10, 21, 20 a 12.

Řešení Cvičení 24.8: (b) 101, (c) 110

Řešení Cvičení 24.9: (a) 120, (b) 1.

Řešení Cvičení 24.10: (a) 111, (b) 010

Řešení Cvičení 24.11: Označme polynom ze zadání $p(x) = x^4 + x^3 + 1$.

(a) Použitím jednoho kroku rozšířeného Euklidova algritmu dostáváme Bézoutovu rovnost ve tvaru

$$1 = p(x) - x \cdot (x^3 + x^2).$$

Inverzí k $x^3 + x^2$ je tedy x, v řeči koeficientů $(1100)^{-1} = 0010$.

(b) Přímočarými úpravami vyjádříme y jako

$$y = (1001)^{-1} \cdot 0110 - 1010. \tag{1}$$

Je třeba nalézt inverzi 1001, označme si $q(x) = x^3 + 1$ a použijme rozšířený Euklidův algoritmus

		podíl	zbytek
$p(x)$	$q(x)$	$x + 1$	$x = p(x) - (x + 1)q(x)$
$q(x)$	x	x^2	$1 = q(x) - x^2 \cdot x = (x^3 + x^2 + 1)q(x) - x^2 p(x)$

Tudíž hledanou inverzí je $(1001)^{-1} = 1101$. Dosazením do (1) dostáváme výsledek

$$y = 1101 \cdot 0110 - 1010 = 0101 - 1010 = 1111.$$

Součin 1101 a 0110 lze vypočítat vynásobením příslušných polynomů (nezapomeňte, že koeficienty se počítají modulo 2)

$$(x^3 + x^2 + 1) \cdot (x^2 + x) = x^5 + x^3 + x^2 + x$$

a vypočtením zbytku po dělení polynomem $p(x)$:

$$(x^5 + x^3 + x^2 + x) \pmod{p(x)} = x^2 + 1.$$

(c) Libovolné y z $GF(2^4)$ lze vyjádřit ve tvaru $y = abcd$, resp. $y(x) = ax^3 + bx^2 + cx + d$, kde $a, b, c, d \in \{0, 1\}$. Nejprve je potřeba vypočítat kvadrát y, čili nejprve vynásobit polynomy

$$\begin{aligned} y(x)^2 &= a^2x^6 + 2abx^5 + (b^2 + 2ac)x^4 + 2(ad + bc)x^3 + (c^2 + 2bd)x^2 + 2cdx + d^2 = \\ &= ax^6 + bx^4 + cx^2 + d. \end{aligned}$$

Zde jsme opět použili toho, že složky jsou dány modulo 2 a navíc $\alpha^2 = \alpha$ pro $\alpha \in \{0, 1\}$. Dále je nutné nalézt zbytek po dělení polynomem $x^4 + x^3 + 1$. Použitím standardního algoritmu dostáváme

$$ax^6 + bx^4 + cx^2 + d \pmod{x^4 + x^3 + 1} = -(a + b)x^3 + (c - a)x^2 + ax + d - a - b.$$

Tj. $y(x) \cdot y(x) = -(a + b)x^3 + (c - a)x^2 + ax + d - a - b$. Hledáme $a, b, c, d \in \{0, 1\}$ tak, aby

$$y(x)^2 + y(x) + x^3 + x = (1 - b)x^3 + (c - a + b)x^2 + (a + c + 1)x - a - b \stackrel{!}{=} 0.$$

Koeficienty jsme opět upravili modulo 2. Z prvního koeficientu jasně plyne, že $b = 1$. Takže potom $a = 1$ (absolutní člen) a $c = 0$ (lineární člen). Kvadratický člen je pak nulový $c - a + b = 0 - 1 + 1 = 0$. Na d jsme žádnou podmínku nezískali a může proto být libovolné. Shrnujeme, že řešením zadané rovnice jsou dvě

$$y_1 = 1100 \quad \text{a} \quad y_2 = 1101.$$

Řešení Cvičení 24.13: Budeme chtít využít binomické věty, která říká, že pro libovolná reálná čísla a a b (a klasické násobení a sčítání čísel) a nezáporné celé číslo n platí:

$$(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k.$$

Abychom binomickou větu dokázali (a dávala smysl), potřebujeme vědět, že sčítání a násobení jsou asociativní a komutativní, to ale platí i pro okruh polynomů $\mathbb{Z}^p[x]$ a příslušné operace sčítání a násobení polynomů.

Pro dva polynomy $u(x)$ a $w(x)$ ze $\mathbb{Z}^p[x]$ tedy dostáváme

$$(u(x) + w(x))^p = \sum_{k=0}^{p} \binom{p}{k} (u(x))^{p-k} (w(x))^k.$$

Jelikož jsou koeficienty ze $\mathbb{Z}_p$, je $\binom{p}{k} = 0$ pro všechna k mimo $k = 0$ a $k = p$. Z toho dostáváme

$$(u(x) + w(x))^p = (u(x))^p + (w(x))^p.$$

Nyní využijeme tento fakt při výpočtu $(v(x))^p$, kde

$$v(x) = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0.$$

Nejprve aplikujeme binomickou větu pro polynomy $u(x) = a_m x^m$ a $w(x) = a_{m-1} x^{m-1} + \cdots + a_1 x + a_0$:

$$(v(x))^p = (u(x) + w(x))^p = (a_m)^p x^{pm} + \left(a_{m-1} x^{m-1} + \cdots + a_1 x + a_0\right)^p.$$

S využitím Malé Fermatovy věty máme $a_m^p = a_m$ (podobně i pro všechny ostatní koeficienty $a_i, i = m-1, m-2, \ldots, 0$ níže). S opětovným použitím binomické věty, tentokráte pro volbu $u(x) = a_{m-1} x^{m-1}$ a $w(x) = a_{m-2} x^{m-2} + \cdots + a_1 x + a_0$, dostáváme

$$(v(x))^p = (u(x) + w(x))^p = a_m x^{pm} + a_{m-1} x^{p(m-1)} + \left(a_{m-2} x^{m-2} + \cdots + a_1 x + a_0\right)^p.$$

Takto pokračujeme ještě $m - 3$ krát a dostaneme

$$(v(x))^p = a_m x^{pm} + a_{m-1} x^{p(m-1)} + + \cdots + a_1 x^p + a_0 = v(x^p),$$

což bylo dokázati.

Řešení Cvičení 24.14: Multiplikativní grupa tělesa $GF(3^3)$ má řád 26, a tedy pro každý její prvek y platí, že y^{26} je neutrální prvek 001. Proto platí, že $y^{107} = (y^{26})^4 y^3 = y^3$, a příklad se tak zjednodušuje na řešení rovnice

$$y^3 = 111.$$

Označme $y = ax^2 + bx + c$, koeficienty a, b, c určíme z rovnice

$$(ax^2 + bx + c)^3 = x^2 + x + 1.$$

S využitím příkladu 24.13 (pro $v(x) = ax^2 + bx + c$ a $p = 3$) máme

$$(ax^2 + bx + c)^3 = ax^6 + bx^3 + c.$$

Spočítáme-li, že $x^3 = x + 2$ a $x^6 = (x^3)^2 = (x + 2)^2 = x^2 + x + 1$ dostáváme rovnici

$$(ax^2 + bx + c)^3 = ax^2 + (a + b)x + (a + 2b + c) = x^2 + x + 1.$$

Z toho již plyne, že $a = 1$, $b = 0$ a $c = 0$ a jediným řešením je tedy $y = 100$.

Řešení Cvičení 24.15: Ověření ireducibility polynomu je v tomto případě jednoduché, neboť se jedná o polynom stupně tři. Pokud by polynom $p(x) = 4x^3 + 2x^2 + 4x + 2$ nebyl ireducibilní, musí být dělitelný polynomem stupně jedna, a tedy mít kořen buď 0, 1, 2, 3 nebo 4. Jelikož platí, že $p(2) = 0$, je polynom dělitelný např. $x + 3$, a není tedy ireducibilní. Skutečně:

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

Řešení Cvičení 24.16: (a): 111, (b): 111 a -111.