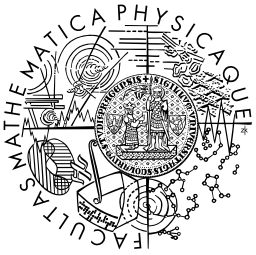


MATEMATICKO-FYZIKÁLNÍ
FAKULTA
Univerzita Karlova

BAKALÁŘSKÁ PRÁCE

Adam Beran

Eliptické křivky nad konečnými tělesy

Katedra algebry

Vedoucí bakalářské práce: doc. RNDr. Jan Šťovíček, Ph.D.

Studijní program: Matematika

Studijní obor: Matematické metody informační bezpečnosti

Praha 2018

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V ..... dne ..... Podpis autora

Rád bych poděkoval doc. RNDr. Janu Šťovíčkovi, Ph.D., za cenné připomínky a odborné vedení při vypracování bakalářské práce.

Název práce: Eliptické křivky nad konečnými tělesy

Autor: Adam Beran

Katedra: Katedra algebry

Vedoucí bakalářské práce: doc. RNDr. Jan Šťovíček, Ph.D., Katedra algebry

Abstrakt: V této práci se zabýváme teorií eliptických křivek, zvláštní pozornost věnujeme eliptickým křivkám nad konečnými tělesy. Představíme základní teorii, zohledníme přitom několik technických aspektů (singularita křivky, vliv charakteristiky tělesa na rovnici křivky). Algebraicky odvodíme a zformulujeme grupový zákon neboli definici operace sčítání na množině bodů na eliptické křivce. Dále zpracujeme důkaz známého faktu, že množina bodů na eliptické křivce spolu s operací sčítání tvoří komutativní grupu. K důkazu přistoupíme elementárně, některé výpočty z důvodu jejich náročnosti provedeme v počítačovém programu Mathematica. Nakonec studujeme endomorfismy eliptických křivek nad konečnými tělesy (homomorfismy na množině bodů eliptické křivky, jež jsou zadané racionálními funkcemi). Pomocí získaných výsledků dokážeme Hasseho větu, která poskytuje odhad na řád grupy bodů na eliptické křivce nad konečným tělesem.

Klíčová slova: eliptické křivky, grupový zákon, Hasseho věta

Title: Elliptic curves over finite fields

Author: Adam Beran

Department: Department of Algebra

Supervisor: doc. RNDr. Jan Šťovíček, Ph.D., Department of Algebra

Abstract: In this thesis, we study the theory of elliptic curves, with the main focus on elliptic curves over finite fields. We present basic theory, taking several technical aspects into consideration (singularity of the curve, effect of field characteristic on the form of the equation of elliptic curve). We algebraically deduce and formulate the group law, that is the definition of addition on a set of points on elliptic curve). We prove a known result saying that the set of points on elliptic curve under addition forms a group. We present an elementary proof, some of the calculations will be carried out in computer program Mathematica due to their complexity. Finally, we study endomorphisms of elliptic curves over finite fields (homomorphisms on the set of points on elliptic curve that are defined by rational functions). Using obtained results, we prove the Hasse's theorem, which provides an estimate of the order of the group of points on elliptic curve over finite field.

Keywords: elliptic curves, group law, Hasse's theorem

Obsah

Úvod

Pod pojmem *eliptická křivka* si budeme představovat množinu řešení rovnice tvaru $y^2 = x^3 + Ax + B$ nad nějakým tělesem K. Jednotlivá řešení této rovnice budeme nazývat *body na křivce*. Později tuto definici upřesníme (budeme uvažovat pouze tělesa charakteristiky různé od 2, 3; k množině bodů přidáme bod v nekonečnu; budeme vyžadovat, aby křivka neměla násobný bod).

Motivace

Nabízí se otázka, proč nás speciálně tyto křivky zajímají. Odpovědí je jejich poměrně překvapivá vlastnost – množina všech bodů na eliptické křivce tvoří (komutativní) grupu. Díky tomuto výsledku si eliptické křivky našly uplatnění v rozličných matematických oblastech, zejména v teorii čísel a kryptografii.

Jako příklad aplikace eliptických křivek v teorii čísel uveďme *congruent number problem* – ptáme se, zda dané kladné celé číslo n je obsahem nějakého pravoúhlého trojúhelníku s racionálními délkami stran. Poměrně snadným výpočtem se tato úloha převede na úlohu řešení rovnice $y^2 = x^3 - n^2x$ (místo s trojúhelníky tedy pracujeme s body na eliptické křivce). Tento problém – přestože více než 1 000 let starý – dosud není kompletně vyřešený; detaily viz [1, str. 3–7]. Mezi problémy vedoucí na eliptické křivky patří i slavná Velká Fermatova věta (dokázaná koncem 20. století A. Wilesem).

Mnoho kryptografických algoritmů stojí na náročnosti řešení *problému diskrétního logaritmu* (pro prvky h a g nějaké grupy G najít celé číslo k takové, že $h = g^k$). Tyto algoritmy běžně využívají grupu $\mathbb{Z}_p^*$ pro nějaké prvočíslo p, pro grupu bodů na eliptické křivce nad konečným tělesem je ovšem problém diskrétního logaritmu podle všeho ještě o něco náročnější, a tedy je použití této grupy z bezpečnostního hlediska výhodnější. Kromě toho se eliptické křivky využívají například v algoritmech pro řešení *problému faktorizace* (hledání prvočíselných rozkladů celých čísel). Pro více informací viz [2].

Čemu se věnuje tato práce

V první kapitole se zaměříme na základní teorii eliptických křivek. Definujeme množinu bodů na eliptické křivce, popíšeme operaci sčítání na této množině (tzv. grupový zákon) a nakonec dokážeme, že tato množina společně s operací sčítání tvoří komutativní grupu; důkaz asociativity z důvodu náročnosti a rozsahu přesuneme do druhé kapitoly.

Druhou kapitolu věnujeme výhradně důkazu asociativity sčítání. Tento důkaz se typicky provádí geometricky, v této práci ovšem představíme méně obvyklý elementární důkaz. Některé výpočty kvůli jejich náročnosti provedeme na počítači (konkrétně využijeme program *Mathematica*).

Ve třetí kapitole se podíváme na vlastnosti eliptických křivek nad konečnými tělesy. Budeme zkoumat Frobeniův endomorfismus a jeho využití při určování počtu bodů na eliptické křivce, hlavním cílem pak bude zpracování důkazu Hasseho věty (ta dává odhad na počet bodů na eliptické křivce).

1. Základní teorie

1.1 Definice

Obecná definice eliptické křivky vyžaduje několik geometrických pojmů, které jsou nad rámec této práce; takovou definici včetně potřebné teorie lze nalézt v [3]. My se budeme držet elementárnějšího přístupu představeného v [1], budeme se tedy muset spokojit s méně obecnou definicí.

Ať K je těleso. *Eliptickou křivkou E (definovanou) nad tělesem K* rozumíme množinu řešení rovnice tvaru

$$y^2 = x^3 + Ax + B, \tag{1.1}$$

kde proměnné x, y mohou nabývat hodnot z tělesa K a A, B jsou konstanty z K. Rovnice (1.1) se nazývá *Weierstrassova rovnice*.

Nyní uvedeme klíčovou definici množiny bodů na eliptické křivce. Z technických důvodů budeme předpokládat, že tato množina obsahuje jistý speciální bod – *bod v nekonečnu*[1], značíme $\mathcal{O}$.

Definice 1. Ať E je eliptická křivka definovaná nad tělesem K a L je těleso splňující $K \subseteq L$. *Množina bodů na eliptické křivce E nad tělesem L* je množina

$$E(L) = \left\{(x, y) \in L^2 \mid y^2 = x^3 + Ax + B\right\} \cup \{\mathcal{O}\}.$$

Poznámka. V dalším textu budeme často používat označení E, resp. K bez dalšího komentáře; v takovém případě automaticky předpokládáme, že K je nějaké těleso a E je eliptická křivka definovaná nad K.

Definice představená výše ještě není úplně přesná – opomenuli jsme několik technických, nicméně důležitých aspektů; na ty se zaměříme v sekcích 1.2 a 1.3.

1.2 Diskriminant a singularita

Uvažujme Weierstrassovu rovnici, tj. rovnici tvaru $y^2 = x^3 + Ax + B$, kde A, B jsou prvky nějakého tělesa K. Abychom křivku určenou touto rovnicí skutečně označili za eliptickou, požadujeme, aby polynom $x^3 + Ax + B$ neměl vícenásobný kořen. Tuto podmínku lze snadno ověřit použitím následující definice a lemmatu.

Definice 2. *Diskriminant* polynomu $x^3 + Ax + B$ je

$$\Delta = -(4A^3 + 27B^2).$$

Lemma 1. *Polynom $x^3 + Ax + B$ má vícenásobný kořen, právě když $\Delta = 0$.*

[1] Bod v nekonečnu bychom mohli definovat formálněji, k tomu bychom se ale neobešli bez konceptu projektivního prostoru a související teorie. V této práci si vystačíme s neformálním pohledem – bod v nekonečnu budeme chápat jednoduše jako symbol, se kterým počítáme podle nějakých pravidel (detaily uvidíme v sekci 1.4).

Důkaz. Označme kořeny polynomu $f(x) \coloneqq x^3 + Ax + B$ jako x_1, x_2 a x_3 (tyto kořeny nemusí nutně ležet v K, nicméně určitě existují v algebraickém uzávěru $\overline{K}$ tělesa K). Dokážeme, že $\Delta = (x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2$. Závěr pak plyne z faktu, že výpočty provádíme nad tělesem (speciálně tedy nad oborem integrity).

Vedoucí koeficient polynomu $f(x)$ je 1, a tedy v $\overline{K}$ můžeme psát

$$x^3 + Ax + B = (x - x_1)(x - x_2)(x - x_3) = x^3 - (x_1 + x_2 + x_3)x^2 + \cdots . \quad (1.2)$$

Porovnáním koeficientů u x^2 dostaneme $0 = -(x_1+x_2+x_3)$, neboli $x_3 = -x_1-x_2$. Dosadíme do (1.2), dostaneme

$$\begin{aligned} x^3 + Ax + B = (x - x_1)(x - x_2)(x + x_1 + x_2) = \\ = x^3 - (x_1^2 + x_1x_2 + x_2^2)x + (x_1^2x_2 + x_1x_2^2). \end{aligned}$$

Opět porovnáme koeficienty, tím získáme hodnoty A a B:

$$\begin{aligned} A &= -(x_1^2 + x_1x_2 + x_2^2), \\ B &= x_1^2x_2 + x_1x_2^2. \end{aligned}$$

Nakonec provedeme přímý výpočet: dosadíme A a B do předpisu pro Δ a výsledek porovnáme s výrazem $(x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2$. Zjistíme, že oba výrazy jsou totožné; tím je důkaz dokončen. □

Nadále tedy budeme předpokládat, že rovnice eliptické křivky splňuje

$$-(4A^3 + 27B^2) \neq 0.$$

Dva příklady eliptických křivek nad $\mathbb{R}$ jsou znázorněny v obrázku 1.1. Pokud $\Delta = 0$, pak se výsledná křivka nazývá *singulární*. Označme vícenásobný kořen polynomu x^3+Ax+B jako x_0, pak bod $(x_0, 0)$ na křivce nazýváme *singulární bod*. Dva příklady singulárních křivek nad $\mathbb{R}$ jsou znázorněny v obrázku 1.2. V této práci se singulárními křivkami dále zabývat nebudeme; více informací lze nalézt v [1, str. 59–61], [3, sekce III.1].

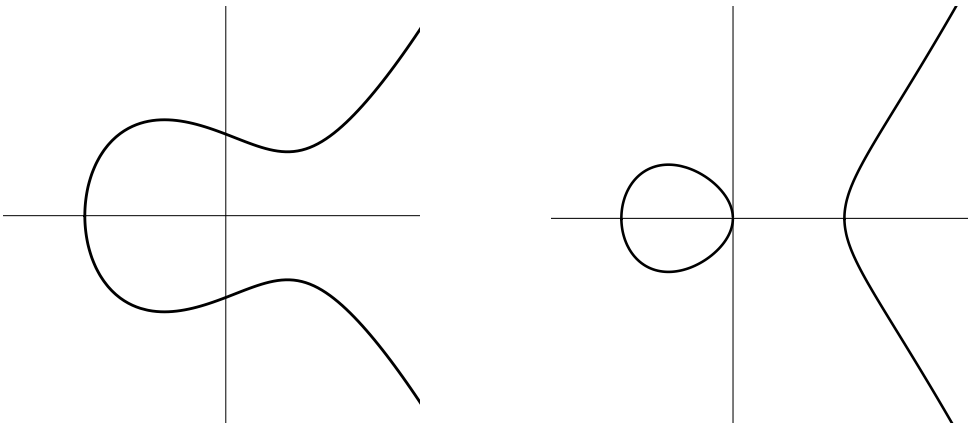
1.3 Zobecněná Weierstrassova rovnice

Místo rovnice (1.1) se někdy v definici eliptické křivky uvádí rovnice obecnější:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad (1.3)$$

kde a_i jsou konstanty. Rovnici (1.3) budeme nazývat *zobecněná Weierstrassova rovnice*. Níže ukážeme, jakým způsobem lze tuto rovnici „převést“ na rovnici (1.1). Postup jsme převzali z [1, str. 10] a [4][2].

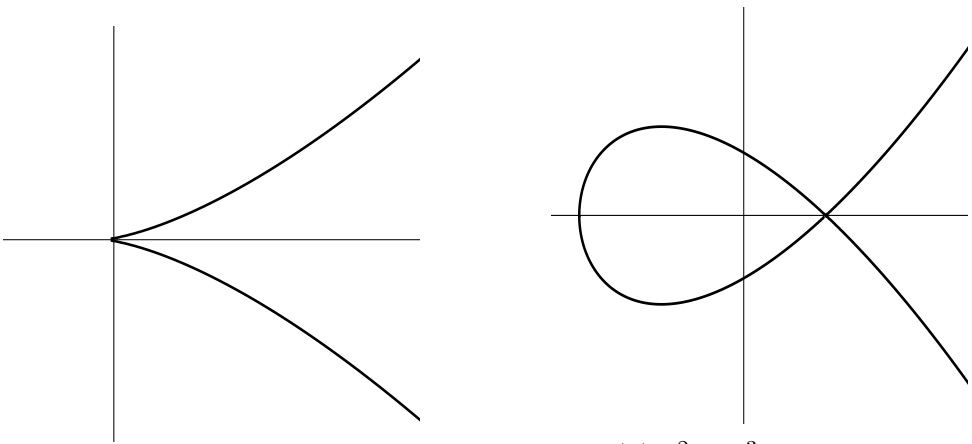
[2] V tomto textu i v některých dalších zdrojích je diskriminant Δ definovaný pro rovnici (1.3), pro rovnici (1.1) potom vyjde $\Delta = -16(4A^3 + 27B^2)$. Všimněme si, že tato hodnota se oproti naší definici liší o konstantu; tato konstanta závisí na tom, jakým konkrétním způsobem provádíme substituce v postupu uvedeném v této sekci. Pro nás toto ovšem není důležité, neboť vztah diskriminantu a singularity se tím nijak nemění.



(a) $y^2 = x^3 - x + 1$, $\Delta < 0$.

(b) $y^2 = x^3 - 2x$, $\Delta > 0$.

Obrázek 1.1: Příklad eliptických křivek nad $\mathbb{R}$.



(a) $y^2 = x^3$.

(b) $y^2 = x^3 - 3x + 2 = (x-1)^2(x+2)$.

Obrázek 1.2: Příklad singulárních křivek nad $\mathbb{R}$.

Upravíme rovnici (1.3) pomocí doplnění na čtverec:

$$y^2 + 2y\left(\frac{a_1}{2}x + \frac{a_3}{2}\right) = x^3 + a_2x^2 + a_4x + a_6,$$
$$y^2 + 2y\left(\frac{a_1}{2}x + \frac{a_3}{2}\right) + \left(\frac{a_1}{2}x + \frac{a_3}{2}\right)^2 = x^3 + a_2x^2 + a_4x + a_6 + \left(\frac{a_1}{2}x + \frac{a_3}{2}\right)^2,$$
$$\left(y + \frac{a_1}{2}x + \frac{a_3}{2}\right)^2 = x^3 + b_2x^2 + b_4x + b_6$$

pro nějaké konstanty b_2, b_4, b_6. Nyní provedeme substituce

$$\widetilde{y} \coloneqq y + \frac{a_1}{2}x + \frac{a_3}{2},$$
$$\widetilde{x} \coloneqq x + \frac{b_2}{3},$$

dostáváme

$$\widetilde{y}^2 = \left(\widetilde{x} - \frac{b_2}{3}\right)^3 + b_2\left(\widetilde{x} - \frac{b_2}{3}\right)^2 + b_4\left(\widetilde{x} - \frac{b_2}{3}\right) + b_6,$$
$$\widetilde{y}^2 = \widetilde{x}^3 + A\widetilde{x} + B$$

pro nějaké konstanty A, B.

Poznámka. Úpravy výše nelze provést nad tělesem charakteristiky 2 nebo 3, v takovém případě je nutné uvažovat rovnici (1.3). V této práci budeme pro jednoduchost předpokládat, že charakteristika tělesa je vždy různá od 2 i 3, a tedy si vystačíme pouze s rovnicí (1.1). Tento předpoklad bude klíčový zejména v následující sekci, kde na základě rovnice (1.1) odvodíme grupový zákon.

1.4 Grupový zákon

Uvažujme eliptickou křivku E danou rovnicí $y^2 = x^3 + Ax + B$. Všimněme si, že z tvaru této rovnice plyne následující fakt: je-li $P = (x_0, y_0)$ bod na E, pak na E leží i bod $P' = (x_0, -y_0)$; navíc potom jiný bod než P, P' s první složkou rovnou x_0 na E ležet nemůže. Značení P' budeme dále používat. Následující text čerpá z [1, sekce 2.2].

1.4.1 Geometrický pohled

Uvažujme body P_1, P_2 na E splňující $P_1, P_2 \neq \mathcal{O}$. Nejprve ať $P_1 \neq P_2$. Sečtení bodů provedeme následovně.

1. Vezměme přímku procházející body P_1 a P_2.
2. Třetí bod, v němž tato přímka protíná křivku E, označme jako P_3.
3. Definujme $P_1 + P_2 = P_3'$.

Pokud platí $P_1' = P_2$, pak se postup liší: přímka procházející oběma body je svislá, a tedy v žádném třetím bodě křivku E neprotíná; v tomto případě definujeme $P_1 + P_2 = \mathcal{O}$.

Nyní ať $P_1 = P_2$. Sečtení bodů provedeme stejně jako v situaci $P_1 \neq P_2$, pouze místo přímky procházející body P_1, P_2 vezmeme tečnu ke křivce E v bodě P_1. Pokud platí $P_1' = P_2$, pak je tečna svislá; podobně jako v předchozím případě pak definujeme $P_1 + P_2 = \mathcal{O}$.

Nakonec definujeme $P + \mathcal{O} = \mathcal{O} + P = P$ pro libovolný bod P na E. Sčítání bodů v jednotlivých situacích je geometricky znázorněné v obrázcích 1.3 a 1.4.

1.4.2 Algebraický pohled

Zajímá nás, jak lze vyjádřit součet bodů $P_1 = (x_1, y_1)$ a $P_2 = (x_2, y_2)$ v případě, kdy přímka procházející body P_1, P_2, resp. tečna v bodě P_1 není svislá (ostatní případy jsou na základě předchozího rozboru triviální).

Nejprve ať $P_1 \neq P_2$, $P_1' \neq P_2$ (tj. $x_1 \neq x_2$). Směrnice přímky procházející body P_1 a P_2 je

$$m = \frac{y_2 - y_1}{x_2 - x_1},$$

rovnice přímky pak je

$$y - y_1 = m(x - x_1).$$

Nyní spočítáme průsečík přímky s křivkou E dosazením $y = m(x - x_1) + y_1$ do rovnice křivky:

$$\begin{aligned}(m(x - x_1) + y_1)^2 &= x^3 + Ax + B,\\ 0 &= x^3 - m^2x^2 + \cdots .\end{aligned}$$

Známe řešení x_1 a x_2, neboť body P_1 a P_2 jsou průsečíky, zbývající řešení pak je $x_3 = m^2 - x_1 - x_2$ (používáme stejný trik jako v důkazu lemmatu 1); z rovnice přímky snadno dopočítáme, že $y_3 = m(x_3 - x_1) + y_1$. Součet $P_1 + P_2$ je potom roven $P_3' = (x_3', y_3')$, kde

$$\begin{aligned}x_3' &= x_3 = m^2 - x_1 - x_2,\\ y_3' &= -y_3 = m(x_1 - x_3) - y_1.\end{aligned}$$

Nyní ať $P_1 = P_2$, $P_1' \neq P_2$ (tj. $y_1 \neq 0$). Vycházíme z rovnice křivky E, směrnici tečny v bodě P_1 získáme pomocí implicitní[3] derivace:

$$\begin{aligned}y^2 &= x^3 + Ax + B,\\ 2yy' &= 3x^2 + A,\\ y' &= (3x^2 + A)/(2y);\end{aligned}$$

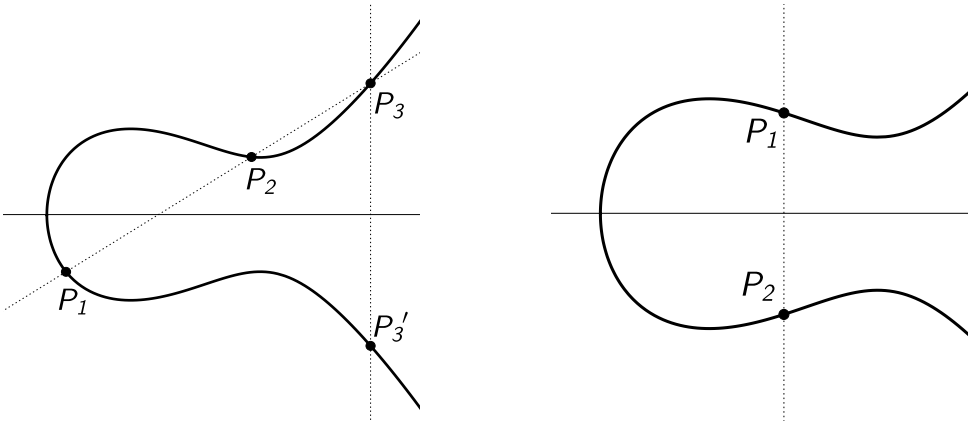
směrnice tečny v bodě P_1 proto je

$$m = \frac{3x_1^2 + A}{2y_1}.$$

Zbytek postupu je prakticky totožný s předchozí situací. Součet bodů P_1 a P_2 tedy je $P_3' = (x_3', y_3')$, kde

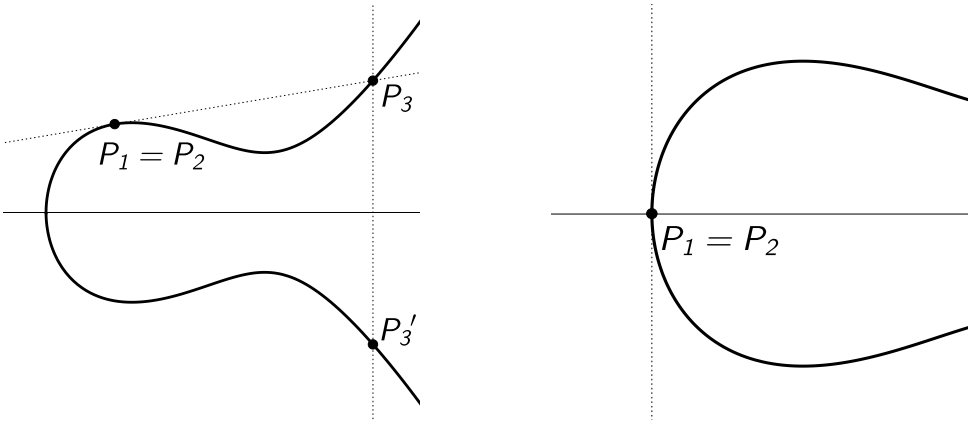
$$\begin{aligned}x_3' &= x_3 = m^2 - x_1 - x_2 = m^2 - 2x_1,\\ y_3' &= m(x_1 - x_3) - y_1.\end{aligned}$$

[3] Neformálně řečeno derivujeme podle proměnné x, přičemž y chápeme jako funkci x; formální výpočet derivace provedeme v sekci 3.2.



(a) $P_1' \neq P_2$. (b) $P_1' = P_2$.

Obrázek 1.3: Sčítání bodů v situaci $P_1 \neq P_2$.



(a) $P_1' \neq P_2$. (b) $P_1' = P_2$.

Obrázek 1.4: Sčítání bodů v situaci $P_1 = P_2$.

1.4.3 Formulace grupového zákona

Definice 3 (Grupový zákon)**.** Ať E je eliptická křivka nad tělesem K daná rovnicí $y^2 = x^3 + Ax + B$. Dále ať $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ jsou body na E. Definujeme součet $P_1 + P_2$ následovně.

1. $P_1 \neq P_2$, $P_1' \neq P_2$:

$$\begin{gathered} P_1 + P_2 = (x_3, y_3), \\ x_3 = m^2 - x_1 - x_2, \\ y_3 = m(x_1 - x_3) - y_1 = -m^3 + m(2x_1 + x_2) - y_1, \\ \text{kde } m = (y_2 - y_1)/(x_2 - x_1). \end{gathered} \tag{a}$$

2. $P_1 \neq P_2$, $P_1' = P_2$:

$$P_1 + P_2 = \mathcal{O}.$$

3. $P_1 = P_2$, $P_1' \neq P_2$:

$$\begin{gathered} P_1 + P_2 = (x_3, y_3), \\ x_3 = m^2 - 2x_1, \\ y_3 = m(x_1 - x_3) - y_1 = -m^3 + m(3x_1) - y_1, \\ \text{kde } m = (3x_1^2 + A)/(2y_1). \end{gathered} \tag{b}$$

4. $P_1 = P_2$, $P_1' = P_2$:

$$P_1 + P_2 = \mathcal{O}.$$

Nakonec definujeme $P + \mathcal{O} = \mathcal{O} + P = P$ pro libovolný bod P na E (speciálně $\mathcal{O} + \mathcal{O} = \mathcal{O}$).

Věta 2. *Ať E je eliptická křivka nad tělesem K daná rovnicí $y^2 = x^3 + Ax + B$, ať L je těleso splňující $K \subseteq L$. Pak množina $E(L)$ spolu s operací $+$ definovanou jako výše tvoří komutativní grupu.*

Důkaz. Uzavřenost množiny $E(L)$ vzhledem k operaci $+$ plyne přímo z rozboru v sekci 1.4.1. Totéž platí pro komutativitu (přímka procházející dvěma body je totožná bez ohledu na pořadí bodů). Jako neutrální prvek vezmeme $\mathcal{O}$. Jako opačný prvek k prvku $P \neq \mathcal{O}$ vezmeme P', jako opačný prvek k $\mathcal{O}$ vezmeme $\mathcal{O}$. Zbývá asociativita; tato vlastnost zdaleka není zřejmá, dokážeme ji v kapitole 2. □

Poznámka. Přímo z definice 3 plyne, že opačné prvky jsou určené jednoznačně; opačný bod k bodu P budeme značit $-P$. Máme tedy

$$\begin{gathered} -(x_0, y_0) = (x_0, -y_0), \\ -\mathcal{O} = \mathcal{O}. \end{gathered}$$

Jednoznačnost neutrálního prvku zřejmá není, tu dokážeme v rámci důkazu asociativity (viz lemma 8).

2. Důkaz asociativity

Dokazujeme, že

$$(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3) \tag{2.1}$$

pro libovolné body $P_1, P_2, P_3 \in E(L)$. Budeme vycházet přímo z definice 3. Pro ověření (2.1) potřebujeme provést celkem čtyřikrát operaci $+$. Důkaz provedeme rozborem případů – pro každé sečtení dvou bodů musíme rozlišit následující situace (pro ilustraci uvažujme součet $P_1 + P_2$).

1. Je-li jeden z bodů roven $\mathcal{O}$, pak je součet roven druhému bodu.
2. Jinak, platí-li $P_1 = -P_2$, pak je součet roven $\mathcal{O}$.
3. Jinak, platí-li $P_1 = P_2$, pak se použije formulka (b) z definice 3.
4. Jinak se použije formulka (a) z definice 3.

V sekci 2.1 dokážeme tři konkrétní případy za pomocí programu vytvořeného v počítačové aplikaci *Mathematica*[1]. Vycházíme z článku [5], kde je dokázán jeden z těchto tří případů. Zdrojový kód a výstupy z programu se nachází v příloze A; samotný program, jejž lze spustit v Mathematice, se nachází v příloze elektronické verze práce. Mathematicu použijeme pro práci s výrazy a polynomy; výpočty jsou příliš složité na to, abychom je provedli ručně.

Ve zbytku důkazu se obejdeme bez počítače. Nejprve dokážeme sérii technických tvrzení (sekce 2.2), ty následně použijeme k důkazu zbývajících případů (sekce 2.3). Budeme čerpat z článku [6], kde je uveden prakticky celý postup; většinu důkazů ovšem doplníme o detaily, případně některé kroky zformulujeme jinak (zejména důkazy lemmat 6, 9, 12 doplníme o výpočty s formulkami (a) a (b), v důkazu lemmatu 8 ukážeme jiným způsobem fakt, že $y_2 = 0$).

V celé kapitole budeme předpokládat, že P_1, P_2, P_3 jsou libovolně zvolené prvky $E(L)$. Pro jednoduchost budeme dodržovat následující značení: pokud bod P_i není roven $\mathcal{O}$, pak $P_i = (x_i, y_i)$.

2.1 Tři případy s pomocí počítače

Každý případ zformulujeme jako samostatné lemma s vlastními předpoklady. Ve všech třech případech budeme navíc předpokládat, že platí:

- $P_1, P_2, P_3 \neq \mathcal{O}$;
- $P_1 \neq -P_2$, $P_2 \neq -P_3$, $P_1 + P_2 \neq -P_3$, $P_1 \neq -(P_2 + P_3)$.

Lemma 3. *Předpokládejme, že P_1, P_2, P_3 jsou po dvou různé, $P_1 + P_2 \neq P_3$, $P_1 \neq P_2 + P_3$. Pak platí $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$.*

Důkaz. Při výpočtu $(P_1+P_2)+P_3$, $P_1+(P_2+P_3)$ se pro všechny čtyři součty použije formulka (a). Označme $P_1+P_2 = (x_4, y_4)$, $(P_1+P_2)+P_3 = (s, t)$; $P_2+P_3 = (x_5, y_5)$, $P_1 + (P_2 + P_3) = (u, v)$. Ukážeme, že $s - u = t - v = 0$.

[1] Wolfram Mathematica, verze 11.2. `https://www.wolfram.com/mathematica/`.

Nejprve spočítáme hodnoty s, t, u, v podle definice 3.

- $(P_1 + P_2) + P_3$:

$$m_1 = \frac{y_2 - y_1}{x_2 - x_1}, \qquad x_4 = m_1^2 - x_1 - x_2, \qquad y_4 = m_1(x_1 - x_4) - y_1,$$
$$\widetilde{m}_1 = \frac{y_3 - y_4}{x_3 - x_4}, \qquad s = \widetilde{m}_1^2 - x_4 - x_3, \qquad t = \widetilde{m}_1(x_4 - s) - y_4;$$

- $P_1 + (P_2 + P_3)$:

$$m_2 = \frac{y_3 - y_2}{x_3 - x_2}, \qquad x_5 = m_2^2 - x_2 - x_3, \qquad y_5 = m_2(x_2 - x_5) - y_2,$$
$$\widetilde{m}_2 = \frac{y_5 - y_1}{x_5 - x_1}, \qquad u = \widetilde{m}_2^2 - x_1 - x_5, \qquad v = \widetilde{m}_2(x_1 - u) - y_1.$$

Dále postupujeme s využitím počítače (v textu níže pro přehlednost neuvádíme mezivýpočty, kompletní postup je uveden v příloze A). Postupným dosazováním vyjádříme hodnoty s, t, u, v jako výrazy v proměnných x_i, y_i, $i = 1, 2, 3$; každý z těchto výrazů následně upravíme do tvaru jednoho zlomku. Jmenovatelé výrazů s a t se příliš neliší: jmenovatel s je roven p^2, jmenovatel t je roven p^3, kde

$$p = \cdots = -(x_1 - x_2)^2(x_1 + x_2 + x_3) + (y_1 - y_2)^2.$$

Podobně jmenovatel výrazu u je q^2, jmenovatel výrazu v je q^3, kde

$$q = \cdots = (x_2 - x_3)^2(x_1 + x_2 + x_3) - (y_2 - y_3)^2.$$

Výrazy p, q můžeme chápat jako polynomy v proměnných x_i, y_i, $i = 1, 2, 3$; všechny koeficienty jsou navíc celočíselné. Jinými slovy, p a q jsou prvky okruhu $R \coloneqq \mathbb{Z}[x_1, x_2, x_3, y_1, y_2, y_3]$.

Nyní uvažujme výrazy $p^2q^2(s-u)$, $p^3q^3(t-v)$; oba výrazy jsou opět polynomy s celočíselnými koeficienty. Spočítáme největší společný dělitel těchto polynomů, označíme jej r (počítáme v Gaussově oboru R, největší společný dělitel tedy jistě existuje):

$$r = \cdots = (x_1 - x_2)(x_2 - x_3)(x_1 - x_3)(x_1 + x_2 + x_3) + \\ + (x_3 - x_2)y_1^2 + (x_1 - x_3)y_2^2 + (x_2 - x_1)y_3^2.$$

Potom pro nějaké $k, l \in R$ můžeme psát

$$s - u = \frac{k}{p^2q^2}r, \qquad t - v = \frac{l}{p^3q^3}r.$$

Uvědomíme si, že platí následující identity: $y_i^2 = x_i^3 + Ax_i + B$, $i = 1, 2, 3$. Zbývá poslední krok – za využití těchto identit ověřit, že $r = 0$. Formálněji řečeno chceme ukázat, že $r = 0$ ve faktorokruhu R/I, kde I je ideál

$$I = (y_1^2 - x_1^3 - Ax_1 - B,\, y_2^2 - x_2^3 - Ax_2 - B,\, y_3^2 - x_3^3 - Ax_3 - B).$$

To lze provést nahrazením y_i^2 za $x_i^3 + Ax_i + B$ ve výrazu r a následnou přímočarou úpravou tohoto výrazu (viz příloha A). □

Lemma 4. *Předpokládejme, že* $P_1 = P_2$, $P_2 \neq P_3$, $P_1 + P_2 \neq P_3$, $P_1 \neq P_2 + P_3$. *Pak platí* $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$.

Důkaz. Při výpočtu $(P_1 + P_2) + P_3$ se použije nejprve formulka (b), poté formulka (a); při výpočtu $P_1 + (P_2 + P_3)$ se pro oba součty použije formulka (a). Použijeme stejné značení jako v důkazu lemmatu 3; navíc máme $x_1 = x_2$, $y_1 = y_2$. Výpočet hodnot s, t, u, v pak vypadá následovně.

- $(P_1 + P_2) + P_3$:

$$m_1 = \frac{3x_1^2 + A}{2y_1}, \qquad x_4 = m_1^2 - 2x_1, \qquad y_4 = m_1(x_1 - x_4) - y_1,$$
$$\widetilde{m}_1 = \frac{y_3 - y_4}{x_3 - x_4}, \qquad s = \widetilde{m}_1^2 - x_4 - x_3, \qquad t = \widetilde{m}_1(x_4 - s) - y_4;$$

- $P_1 + (P_2 + P_3)$:

$$m_2 = \frac{y_3 - y_1}{x_3 - x_1}, \qquad x_5 = m_2^2 - x_1 - x_3, \qquad y_5 = m_2(x_1 - x_5) - y_1,$$
$$\widetilde{m}_2 = \frac{y_5 - y_1}{x_5 - x_1}, \qquad u = \widetilde{m}_2^2 - x_1 - x_5, \qquad v = \widetilde{m}_2(x_1 - u) - y_1.$$

Zbytek důkazu je analogický k důkazu lemmatu 3 (v příloze A je uveden kompletní postup). □

Lemma 5. *Předpokládejme, že* $P_1 = P_2$, $P_2 \neq P_3$, $P_1 + P_2 = P_3$, $P_1 \neq P_2 + P_3$. *Pak platí* $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$.

Důkaz. Při výpočtu $(P_1 + P_2) + P_3$ se pro oba součty použije formulka (b); při výpočtu $P_1 + (P_2 + P_3)$ se pro oba součty použije formulka (a). Použijeme stejné značení jako v důkazu lemmatu 3; navíc máme $x_1 = x_2$, $y_1 = y_2$, $x_4 = x_3$, $y_4 = y_3$. Výpočet hodnot s, t, u, v pak vypadá následovně.

- $(P_1 + P_2) + P_3$:

$$m_1 = \frac{3x_1^2 + A}{2y_1}, \qquad x_4 = m_1^2 - 2x_1, \qquad y_4 = m_1(x_1 - x_4) - y_1,$$
$$\widetilde{m}_1 = \frac{3x_4^2 + A}{2y_4}, \qquad s = \widetilde{m}_1^2 - 2x_4, \qquad t = \widetilde{m}_1(x_4 - s) - y_4;$$

- $P_1 + (P_2 + P_3)$:

$$m_2 = \frac{y_4 - y_1}{x_4 - x_1}, \qquad x_5 = m_2^2 - x_1 - x_4, \qquad y_5 = m_2(x_1 - x_5) - y_1,$$
$$\widetilde{m}_2 = \frac{y_5 - y_1}{x_5 - x_1}, \qquad u = \widetilde{m}_2^2 - x_1 - x_5, \qquad v = \widetilde{m}_2(x_1 - u) - y_1.$$

V tomto případě závěr dostaneme přímým výpočtem hodnot $s - u$, $t - v$ v Mathematice (jinak bychom mohli důkaz dokončit analogicky k důkazu lemmatu 3). □

2.2 Technická tvrzení

Budeme používat následující značení: $P_1 - P_2 \coloneqq P_1 + (-P_2)$. Dále budeme využívat následující pozorování.

- $-(-P_1) = P_1$;
- $P_1 = P_2$, právě když $-P_1 = -P_2$;
- $P_1 + P_2 = \mathcal{O}$, právě když $P_1 = -P_2$;
- ať $P_1 \neq \mathcal{O}$, pak platí: $P_1 = -P_1$, právě když $y_1 = 0$;
- ať $P_1, P_2 \neq \mathcal{O}$, pak platí: $P_1 \neq \pm P_2$, právě když $x_1 \neq x_2$.

Lemma 6. *$-P_1 - P_2 = -(P_1 + P_2)$.*

Důkaz. Situace $P_1 = \mathcal{O}$, $P_2 = \mathcal{O}$ a $P_1 = -P_2$ jsou zřejmé. Předpokládejme tedy, že $P_1, P_2 \neq \mathcal{O}$, $P_1 \neq -P_2$.

Označme $-P_1 - P_2 = (x_4, y_4)$, $-(P_1 + P_2) = (x_5, y_5)$. Nejprve předpokládejme, že $P_1 \neq P_2$; pak se při výpočtu součtů $P_1 + P_2$, $-P_1 - P_2$ použije formulka (a). Potom platí:

$$\begin{aligned} m &= \frac{-y_2 + y_1}{x_2 - x_1} = -\frac{y_2 - y_1}{x_2 - x_1}, \\ x_4 &= m^2 - x_1 - x_2, \\ y_4 &= m(x_1 - x_4) - (-y_1) = m(x_1 - x_4) + y_1; \end{aligned}$$

$$\begin{aligned} \widetilde{m} &= \frac{y_2 - y_1}{x_2 - x_1} = -m, \\ x_5 &= \widetilde{m}^2 - x_1 - x_2 = m^2 - x_1 - x_2 = x_4, \\ y_5 &= -(\widetilde{m}(x_1 - x_5) - y_1) = m(x_1 - x_4) + y_1 = y_4. \end{aligned}$$

Nyní ať $P_1 = P_2$; v tomto případě se použije formulka (b). Opět platí $\widetilde{m} = -m$, postup tedy lze provést stejně jako v předchozím případě. □

Lemma 7. *Ať $P_1 + P_2 = P_1 - P_2$, $P_1 \neq -P_1$. Pak $P_2 = -P_2$.*

Důkaz. Z předpokladu $P_1 \neq -P_1$ plyne, že $P_1 \neq \mathcal{O}$. Situace $P_2 = \mathcal{O}$ je zřejmá. V situaci $P_1 = \pm P_2$ dostaneme z prvního předpokladu, že $P_1 + P_1 = \mathcal{O}$, potom $P_1 = -P_1$, a tedy není splněn druhý předpoklad. Dále tedy můžeme předpokládat, že $P_1, P_2 \neq \mathcal{O}$, $P_1 \neq \pm P_2$.

Využijeme předpokladu $P_1 + P_2 = P_1 - P_2$, porovnáním prvních složek dostaneme

$$\begin{aligned} \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 &= \left(\frac{-y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2, \\ -2y_1y_2 &= 2y_1y_2, \\ 4y_1y_2 &= 0. \end{aligned}$$

Charakteristika tělesa je různá od 2, proto $y_1 = 0$ nebo $y_2 = 0$. Předpoklad $P_1 \neq -P_1$ nám dá $y_1 \neq 0$; pak nutně $y_2 = 0$, a tedy $P_2 = -P_2$. □

Lemma 8 (Jednoznačnost neutrálního prvku)**.** *Ať $P_1 + P_2 = P_1$. Pak $P_2 = \mathcal{O}$.*

Důkaz. Situace $P_1 = \mathcal{O}$, $P_1 = -P_2$ jsou zřejmé. Předpokládejme tedy, že $P_1 \neq \mathcal{O}$, $P_1 \neq -P_2$; pro spor navíc předpokládejme, že $P_2 \neq \mathcal{O}$.

Označme $P_1 + P_2 = (x_4, y_4)$. Využijeme předpoklad $P_1 = P_1 + P_2$, porovnáním prvních složek dostaneme $x_1 = x_4$, následně porovnáním druhých složek dostaneme

$$\begin{aligned} y_1 &= y_4, \\ y_1 &= m(x_1 - x_4) - y_1, \\ y_1 &= -y_1, \end{aligned}$$

a tedy $y_1 = 0$ (v tuto chvíli ještě nevíme, jaká je hodnota m ve výpočtu výše). Platí tedy $P_1 = -P_1$, toto společně s předpokladem ze znění lemmatu využijeme v následující úvaze: kdyby $P_1 = P_2$, pak

$$P_2 = P_1 = P_1 + P_2 = P_1 + P_1 = P_1 - P_1 = \mathcal{O}.$$

Dále tedy můžeme předpokládat, že $P_1 \neq P_2$; to znamená, že při výpočtu $P_1 + P_2$ se použije formulka (a). Opět využijeme předpoklad $P_1 = P_1 + P_2$:

$$\begin{aligned} x_1 &= x_4, \\ x_1 &= \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2. \end{aligned} \tag{2.2}$$

Nyní dokážeme, že $y_2 = 0$. Víme, že $y_1 = 0$, zároveň můžeme využít vztah $y_2^2 = x_2^3 + Ax_2 + B$. Pracujeme dále s rovností (2.2):

$$\begin{aligned} x_1 &= \left(\frac{y_2}{x_2 - x_1}\right)^2 - x_1 - x_2, \\ (2x_1 + x_2)(x_2 - x_1)^2 &= y_2^2, \\ (2x_1 + x_2)(x_2 - x_1)^2 &= x_2^3 + Ax_2 + B, \\ 2x_1^3 - x_2(3x_1^2 + A) - B &= 0. \end{aligned} \tag{2.3}$$

Ověříme, že $3x_1^2 + A \neq 0$. Označme $f(x) \coloneqq x^3 + Ax + B$, zderivováním dostaneme $f'(x) = 3x^2 + A$. Máme vztah

$$x_1^3 + Ax_1 + B = y_1^2 = 0,$$

neboli x_1 je kořenem polynomu $f(x)$. Pokud $3x_1^2 + A = 0$, pak x_1 je společný kořen polynomů $f(x)$ a $f'(x)$, a tedy podle [7, věta 11.2] je x_1 vícenásobný kořen $f(x)$. To je spor s předpokladem, že $\Delta \neq 0$.

Z rovnosti (2.3) tedy dostáváme, že

$$x_2 = (2x_1^3 - B)/(3x_1^2 + A),$$

a nakonec přímým výpočtem

$$y_2^2 = x_2^3 + Ax_2 + B = \left(\frac{2x_1^3 - B}{3x_1^2 + A}\right)^3 + A\left(\frac{2x_1^3 - B}{3x_1^2 + A}\right) + B =$$

$$= \frac{(x_1^3 + Ax_1 + B)^2(2Ax_1 - B + 8x_1^3)}{(3x_1^2 + A)^3} = \frac{y_1^4(2Ax_1 - B + 8x_1^3)}{(3x_1^2 + A)^3} = 0,$$

neboli $y_2 = 0$.

Vraťme se k rovnosti (2.2), nyní dostáváme

$$x_1 = -x_1 - x_2.$$

Známe dva kořeny polynomu $x^3 + Ax + B$: x_1 a $x_2 = -2x_1$. Třetí kořen potom je $x_3 = -x_1 - x_2 = -x_1 + 2x_1 = x_1$. To znamená, že x_1 je dvojnásobný kořen; to je spor s předpokladem, že $\Delta \neq 0$. □

Lemma 9. $(P_1 + P_1) - P_1 = P_1$.

Důkaz. Situace $P_1 = \mathcal{O}$, $P_1 = -P_1$ jsou zřejmé. Pokud $P_1 + P_1 = P_1$, pak $P_1 = \mathcal{O}$ z lemmatu 8. Pokud $P_1 + P_1 = -P_1$, pak za použití lemmatu 6 máme

$$(P_1 + P_1) - P_1 = -P_1 - P_1 = -(P_1 + P_1) = -(-P_1) = P_1.$$

Můžeme tedy předpokládat, že $P_1 \neq \mathcal{O}$, $P_1 \neq -P_1$, $P_1 + P_1 \neq \pm P_1$.

Označme $P_1 + P_1 = (x_4, y_4)$, $(P_1 + P_1) - P_1 = (x_5, y_5)$. Pak máme:

$$\begin{aligned} m &= (3x_1^2 + A)/(2y_1), \\ x_4 &= m^2 - 2x_1, \\ y_4 &= m(x_1 - x_4) - y_1; \end{aligned}$$

$$\widetilde{m} = \frac{-y_1 - y_4}{x_1 - x_4} = \frac{-y_1 - (m(x_1 - x_4) - y_1)}{x_1 - x_4} = -m,$$

$$x_5 = \widetilde{m}^2 - x_4 - x_1 = m^2 - (m^2 - 2x_1) - x_1 = x_1.$$

Zjistili jsme, že body $(P_1 + P_1) - P_1$ a P_1 mají stejnou první složku. Nutně se tedy rovnají nebo je jeden opačný k druhému. Kdyby $(P_1 + P_1) - P_1 = -P_1$, pak $P_1 + P_1 = \mathcal{O}$ z lemmatu 8, což je spor s předpokladem; proto $(P_1 + P_1) - P_1 = P_1$. □

Lemma 10. *Ať* $P_1 + P_2 = -P_1$. *Pak* $P_2 = -P_1 - P_1$.

Důkaz. Situace $P_1 = \mathcal{O}$, $P_2 = \mathcal{O}$, $P_1 = -P_2$ jsou zřejmé. Pokud $P_1 = P_2$, pak

$$-P_1 - P_1 = -P_1 - P_2 = -(P_1 + P_2) = -(-P_1) = P_1 = P_2.$$

Pokud $P_1 = -P_1$, pak z předpokladu máme $P_1 + P_2 = P_1$, a tedy z lemmatu 8 dostáváme $P_2 = \mathcal{O}$. Můžeme tedy předpokládat, že $P_1, P_2 \neq \mathcal{O}$, $P_1 \neq \pm P_2$, $P_1 \neq -P_1$.

Provedeme několik úprav; některé z nich jsou na pohled netriviální, všechny lze ovšem ověřit přímým výpočtem za použití identit $y_i^2 = x_i^3 + Ax_i + B$, $i = 1, 2$. Vyjdeme z předpokladu $-P_1 = P_1 + P_2$, porovnáním prvních složek dostaneme

$$\begin{aligned} x_1 &= \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2, \\ 2y_1y_2 &= y_1^2 + Ax_2 + B - 2x_1^3 + 3x_1^2x_2, \end{aligned}$$

umocněním na druhou pak dostaneme

$$\begin{aligned}(2y_1y_2)^2 - (y_1^2 + Ax_2 + B - 2x_1^3 + 3x_1^2x_2)^2 &= 0,\\ (8y_1^2x_1 + 4y_1^2x_2 - (3x_1^2 + A)^2)(x_2 - x_1)^2 &= 0,\\ \left(2x_1 + x_2 - \left(\frac{3x_1^2 + A}{2y_1}\right)^2\right)(x_2 - x_1)^2 &= 0.\end{aligned}$$

Víme, že $x_1 \neq x_2$, a proto

$$\begin{aligned}2x_1 + x_2 - \left(\frac{3x_1^2 + A}{2y_1}\right)^2 &= 0,\\ x_2 &= \left(\frac{3x_1^2 + A}{2y_1}\right)^2 - 2x_1.\end{aligned}$$

Tím jsme zjistili, že body P_2 a $P_1 + P_1$ mají stejnou první složku. Platí tedy $P_2 = P_1 + P_1$ nebo $P_2 = -(P_1 + P_1) = -P_1 - P_1$.

Pokud $P_2 = -P_1 - P_1$, pak jsme hotovi. Pokud $P_2 = P_1 + P_1$, pak z předpokladu ze znění lemmatu dostáváme, že $P_1 + (P_1 + P_1) = -P_1$; dále z lemmatu 9 víme, že $P_1 + (-P_1 - P_1) = -P_1$; dohromady potom máme

$$P_1 + (P_1 + P_1) = P_1 + (-P_1 - P_1) = P_1 - (P_1 + P_1).$$

Nakonec využijeme lemma 7 (předpoklad $P_1 \neq -P_1$ je splněn); dostáváme, že $P_1 + P_1 = -(P_1 + P_1)$, a tedy $P_2 = P_1 + P_1 = -(P_1 + P_1) = -P_1 - P_1$. □

Lemma 11. *Ať $P_1 + P_2 = P_1 + P_3$. Pak $P_2 = P_3$.*

Důkaz. Situace $P_1 = \mathcal{O}$ je zřejmá. Pokud $P_2 = \mathcal{O}$, pak $P_1 = P_1 + P_3$, a tedy $P_3 = \mathcal{O}$. Situace $P_3 = \mathcal{O}$ je obdobná. Pokud $P_1 = -P_2$, pak $P_1 + P_2 = P_1 + P_3 = \mathcal{O}$, a tedy $P_2 = -P_1$, $P_3 = -P_1$. Situace $P_1 = -P_3$ je obdobná. Pokud $P_1 + P_2 = -P_1$, pak $P_2 = -P_1 - P_1$, $P_3 = -P_1 - P_1$ z lemmatu 10. Navíc pokud $P_1 + P_2 = P_1$, pak $P_2 = \mathcal{O}$. Můžeme tedy předpokládat, že $P_1, P_2, P_3 \neq \mathcal{O}$; $P_1 \neq -P_2$, $P_1 \neq -P_3$; $P_1 + P_2 \neq \pm P_1$.

Označme $P_1 + P_2 = P_1 + P_3 = (x_4, y_4)$. Hodnoty x_4, y_4 pak lze vyjádřit následovně:

$$x_4 = m^2 - x_1 - x_2 = \widetilde{m}^2 - x_1 - x_3, \tag{2.4}$$
$$y_4 = m(x_1 - x_4) - y_1 = \widetilde{m}(x_1 - x_4) - y_1; \tag{2.5}$$

hodnoty m, $\widetilde{m}$ zatím neznáme. Předpokládáme $P_1 + P_2 \neq \pm P_1$, neboli $x_4 \neq x_1$. Z (2.5) proto dostáváme, že $m = \widetilde{m}$; z (2.4) potom dostáváme, že $x_2 = x_3$. Nutně tedy $P_2 = P_3$ nebo $P_2 = -P_3$.

Rozlišíme dva případy – podle toho, zda $P_1 = -P_1$. Nejprve ať $P_1 = -P_1$. Potom jistě $P_1 \neq P_2, P_3$ (toto plyne přímo z předpokladů výše); hodnoty m, $\widetilde{m}$ tedy odpovídají formulce (a). Proto dostáváme

$$m = \frac{y_2 - y_1}{x_2 - x_1}, \qquad \widetilde{m} = \frac{y_3 - y_1}{x_3 - x_1} = \frac{y_3 - y_1}{x_2 - x_1};$$

ze vztahu $m = \widetilde{m}$ potom plyne, že $y_2 = y_3$. Nyní ať $P_1 \neq -P_1$. Předpokládejme, že $P_2 = -P_3$ (jinak $P_2 = P_3$ a jsme hotovi); pak $P_1 + P_2 = P_1 + P_3 = P_1 - P_2$. Použijeme lemma 7; dostáváme, že $P_2 = -P_2$, a tedy $P_3 = -P_2 = P_2$. □

Lemma 12. $(P_1 + P_2) - P_2 = P_1$.

Důkaz. Situace $P_1 = \mathcal{O}$, $P_2 = \mathcal{O}$, $P_1 = -P_2$ jsou zřejmé. V situaci $P_1 = P_2$ máme závěr přímo z lemmatu 9. Pokud $P_1 + P_2 = -P_2$, pak z lemmatu 10 dostáváme, že $P_1 = -P_2 - P_2$; potom $(P_1 + P_2) - P_2 = -P_2 - P_2 = P_1$. Předpokládejme tedy, že $P_1, P_2 \neq \mathcal{O}$, $P_1 \neq \pm P_2$, $P_1 + P_2 \neq -P_2$; navíc jistě $P_1 + P_2 \neq P_2$.

Označme $P_1 + P_2 = (x_4, y_4)$, $(P_1 + P_2) - P_2 = (x_5, y_5)$. Důkaz dokončíme následujícím výpočtem:

$$\begin{aligned} m &= \frac{y_2 - y_1}{x_2 - x_1}, \\ x_4 &= m^2 - x_1 - x_2, \\ y_4 &= m(x_1 - x_4) - y_1; \end{aligned}$$

$$\widetilde{m} = \frac{-y_2 - y_4}{x_2 - x_4} = \frac{-y_2 - (m(x_1 - x_4) - y_1)}{x_2 - x_4} = \frac{y_1 - y_2 - \frac{y_2 - y_1}{x_2 - x_1}(x_1 - x_4)}{x_2 - x_4} =$$

$$= \frac{(y_1 - y_2)(x_2 - x_1) - (y_2 - y_1)(x_1 - x_4)}{(x_2 - x_4)(x_2 - x_1)} = \frac{(y_1 - y_2)(x_2 - x_4)}{(x_2 - x_1)(x_2 - x_4)} = \frac{y_1 - y_2}{x_2 - x_1} =$$

$$= -m,$$

$$\begin{aligned} x_5 &= \widetilde{m}^2 - x_4 - x_2 = m^2 - (m^2 - x_1 - x_2) - x_2 = x_1, \\ y_5 &= \widetilde{m}(x_4 - x_5) - y_4 = -m(x_4 - x_1) - (m(x_1 - x_4) - y_1) = y_1. \end{aligned}$$

□

Důsledek 13. *Ať $P_1 + P_2 = P_3$. Pak $P_1 = P_3 - P_2$.*

Důkaz. Využijeme předpoklad a lemma 12, dostaneme

$$P_1 + P_2 = P_3 = (P_3 - P_2) + P_2;$$

závěr potom plyne z lemmatu 11. □

2.3 Dokončení důkazu

Věta 14. $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$.

Důkaz. Situace $P_1 = \mathcal{O}$, $P_2 = \mathcal{O}$, $P_3 = \mathcal{O}$ jsou zřejmé. Pokud $P_1 = -P_2$, potom

$$\begin{aligned} (P_1 + P_2) + P_3 &= \mathcal{O} + P_3 = P_3, \\ P_1 + (P_2 + P_3) &= P_1 + (-P_1 + P_3) = P_3. \end{aligned}$$

Pokud $(P_1 + P_2) = -P_3$, pak

$$(P_1 + P_2) + P_3 = \mathcal{O},$$
$$P_1 + (P_2 + P_3) = P_1 + (P_2 - (P_1 + P_2)) = P_1 - P_1 = \mathcal{O}.$$

Situace $P_2 = -P_3$ a $P_1 = -(P_2 + P_3)$ jsou obdobné. Dále tedy můžeme předpokládat, že $P_1, P_2, P_3 \neq \mathcal{O}$, $P_1 \neq -P_2$, $P_2 \neq -P_3$, $P_1 + P_2 \neq -P_3$, $P_1 \neq -(P_2 + P_3)$.

Nyní ukážeme, že věta platí v případě, kdy se některé z bodů P_1, P_2, P_3 rovnají. Situace $P_1 = P_3$ je zřejmá; dále předpokládejme, že $P_1 \neq P_3$. Nyní ať $P_1 = P_2$; v tomto případě dokazujeme, že

$$(P_1 + P_1) + P_3 = P_1 + (P_1 + P_3). \tag{2.6}$$

Rozlišíme dva případy – pokud $P_1 + P_1 \neq P_3$, pak závěr plyne z lemmatu 4; pokud $P_1 + P_1 = P_3$, pak závěr plyne z lemmatu 5 (předpoklady ze znění lemmat je snadné ověřit). Situace $P_2 = P_3$ je obdobná. Dále tedy můžeme navíc předpokládat, že body P_1, P_2, P_3 jsou po dvou různé.

Nyní předpokládejme, že $P_1 + P_2 = P_3$; v tomto případě dokazujeme, že

$$(P_1 + P_2) + (P_1 + P_2) = P_1 + (P_2 + (P_1 + P_2)). \tag{2.7}$$

V následující úvaze použijeme již dokázaný vztah (2.6) a lemma 12:

$$\begin{aligned}((P_1 + P_2) + (P_1 + P_2)) - P_1 &= (P_1 + P_2) + ((P_1 + P_2) - P_1) = \\ &= (P_1 + P_2) + P_2 = (((P_1 + P_2) + P_2) + P_1) - P_1,\end{aligned}$$

dokazovaný vztah (2.7) pak plyne z lemmatu 11. Situace $P_1 = P_2 + P_3$ je obdobná.

Nakonec zbývá situace, kdy $P_1 + P_2 \neq P_3$ a $P_1 \neq P_2 + P_3$; tato situace plyne z lemmatu 3. □

3. Frobeniův endomorfismus a Hasseho věta

V celé kapitole budeme uvažovat eliptickou křivku E definovanou nad konečným tělesem $\mathbb{F}_q$. Grupa $E(\mathbb{F}_q)$ je potom konečná; důležitou vlastností je řád této grupy, značíme $\#E(\mathbb{F}_q)$. Hasseho věta poskytuje odhad na $\#E(\mathbb{F}_q)$, k důkazu této věty budeme směřovat ve zbytku práce. Vycházíme z [1, sekce 2.9, 4.1, 4.2]. Výsledky představené v sekci 3.2 dávají smysl pro eliptické křivky definované nad libovolným tělesem, my však budeme pro přehlednost pracovat pouze s konečnými tělesy.

3.1 Konečná tělesa

V této sekci uvedeme některé pojmy a výsledky z teorie konečných těles. Jednotlivé výsledky přímo potřebné v dalším textu uvedeme i s důkazy, vynecháme ovšem detaily; jde o látku pokrytou na přednáškách Konečná tělesa na MFF UK, kromě toho lze využít např. přehled [1, Appendix C].

Ať p je prvočíslo a $q = p^n$ pro nějaké kladné celé číslo n. Pak existuje (až na izomorfismus) jediné konečné těleso o q prvcích, budeme jej značit $\mathbb{F}_q$; charakteristika tohoto tělesa je p. Dále uvažujme algebraický uzávěr $\overline{\mathbb{F}}_q$ tělesa $\mathbb{F}_q$ (i toto těleso má charakteristiku p).

Tvrzení 15. *Těleso $\overline{\mathbb{F}}_q$ je nekonečné.*

Důkaz. Ať $\overline{\mathbb{F}}_q$ je konečné. Pak máme $\overline{\mathbb{F}}_q = \{a_1, \ldots, a_m\}$ pro nějaké m, polynom $(x - a_1) \cdots (x - a_m) + 1$ potom nemá v $\overline{\mathbb{F}}_q$ kořen. To je spor. □

Definujeme zobrazení

$$\begin{aligned} \varphi_q : \overline{\mathbb{F}}_q &\to \overline{\mathbb{F}}_q, \\ a &\mapsto a^q, \end{aligned}$$

nazýváme je *Frobeniův endomorfismus*.

Poznámka. Zobrazení φ_q je skutečně endomorfismus. Vlastnost $(a \cdot b)^q = a^q \cdot b^q$ je zřejmá; vlastnost $(a + b)^q = a^q + b^q$ plyne indukcí z rovnosti $(a + b)^p = a^p + b^p$, tu lze ověřit použitím binomické věty a faktu, že $p \mid \binom{p}{i}$ pro $i = 1, \ldots, p - 1$.

Ať a je prvek $\overline{\mathbb{F}}_q$. Pokud $a \in \mathbb{F}_q$, pak $\varphi_q(a) = a^q = a$. Toto tvrzení platí i naopak, neboli platí následující.

Tvrzení 16. $\mathbb{F}_q = \{a \in \overline{\mathbb{F}}_q \mid a^q = a\}$.

Důkaz. Zvolme $a \in \mathbb{F}_q$. Pro $a \neq 0$ máme $a^{q-1} = 1$ v $\mathbb{F}_q^*$, a tedy $a^q = a$ (symbolem $\mathbb{F}_q^*$ rozumíme multiplikativní grupu tělesa $\mathbb{F}_q$); pro $a = 0$ zřejmě $a^q = a$. Tím jsme ukázali, že $\mathbb{F}_q \subseteq \{a \in \overline{\mathbb{F}}_q \mid a^q = a\}$.

Nyní uvažujme polynom $f(x) \coloneqq x^q - x$. Tento polynom nemá vícenásobné kořeny, neboť $f'(x) = -1$, a tedy má v $\overline{\mathbb{F}}_q$ právě q různých kořenů. Tím jsme zjistili, že množina $\{a \in \overline{\mathbb{F}}_q \mid a^q = a\}$ má q prvků, a proto nutně $\mathbb{F}_q = \{a \in \overline{\mathbb{F}}_q \mid a^q = a\}$. □

3.2 Endomorfismy eliptické křivky

Definice 4. Zobrazení $\alpha : E(\overline{\mathbb{F}}_q) \to E(\overline{\mathbb{F}}_q)$ nazveme *endomorfismus eliptické křivky* E, pokud je to homomorfismus daný racionálními funkcemi.

Poznámka. Homomorfismem rozumíme zobrazení α takové, že pro libovolné body P_1, P_2 na E platí $\alpha(P_1 + P_2) = \alpha(P_1) + \alpha(P_2)$. Zobrazení α je dáno racionálními funkcemi, pokud pro libovolný bod (x, y) na E platí

$$\alpha(x, y) = (R_1(x, y), R_2(x, y)), \tag{3.1}$$

kde $R_1(x, y), R_2(x, y)$ jsou racionální funkce (neboli podíly dvou polynomů v proměnných x, y). Pokud některá z funkcí R_1, R_2 není v bodě (x_0, y_0) definovaná, pak píšeme $\alpha(x_0, y_0) = \mathcal{O}$ (k této situaci se vrátíme níže). Pro každý endomorfismus α jistě platí $\alpha(\mathcal{O}) = \mathcal{O}$; jako *triviální endomorfismus* označujeme zobrazení α takové, že $\alpha(P) = \mathcal{O}$ pro každý bod P.

Nyní ukážeme, jakým způsobem lze racionální funkce z definice endomorfismu převést do jistého „standardního“ tvaru. Uvažujme nějakou racionální funkci $R(x, y)$; tato funkce je definovaná nějakým předpisem v proměnných x, y. Využijeme vztah $y^2 = x^3 + Ax + B$, ten nám umožní nahradit v předpisu pro $R(x, y)$ výraz y^2 výrazem $x^3 + Ax + B$; každý výskyt y v sudé mocnině tedy nahradíme nějakým polynomem $f(x)$, každý výskyt y v liché mocnině nahradíme výrazem tvaru $y \cdot g(x)$ pro nějaký polynom $g(x)$. Dostáváme, že

$$R(x, y) = \frac{p_1(x) + y \cdot p_2(x)}{p_3(x) + y \cdot p_4(x)}$$

pro nějaké polynomy $p_1(x), \ldots, p_4(x)$. Tento zlomek můžeme rozšířit výrazem $p_3(x) - y \cdot p_4(x)$, dostaneme

$$R(x, y) = \frac{(p_1(x) + y \cdot p_2(x))(p_3(x) - y \cdot p_4(x))}{p_3(x)^2 - y^2 \cdot p_4(x)^2} = \frac{q_1(x) + y \cdot q_2(x)}{q_3(x)} \tag{3.2}$$

pro nějaké polynomy $q_1(x), \ldots, q_3(x)$.

Uvažujme endomorfismus α daný předpisem (3.1). Využijeme fakt, že α je homomorfismus, dostaneme

$$\begin{aligned} \alpha(x, -y) &= \alpha(-(x, y)) = -\alpha(x, y), \\ (R_1(x, -y), R_2(x, -y)) &= (R_1(x, y), -R_2(x, y)). \end{aligned}$$

Vyjádříme funkce R_1, R_2 ve tvaru (3.2). Pro R_1 dostaneme

$$\begin{aligned} R_1(x, -y) &= R_1(x, y), \\ \frac{q_1(x) - y \cdot q_2(x)}{q_3(x)} &= \frac{q_1(x) + y \cdot q_2(x)}{q_3(x)}, \end{aligned}$$

neboli $q_2(x)$ je nutně[1] nulový polynom. Obdobně pro funkci R_2, v tomto případě dostaneme, že $q_1(x)$ je nulový polynom. Zjistili jsme tedy, že $R_1(x, y) = r_1(x)$, $R_2(x, y) = y \cdot r_2(x)$ pro nějaké racionální funkce r_1, r_2.

[1] Pro libovolné $x \in \overline{\mathbb{F}}_q$ existuje bod $(x, y) \in E(\overline{\mathbb{F}}_q)$, přitom jen pro konečně mnoho takových bodů může být $y = 0$; zároveň jen pro konečně mnoho různých x může být $q_3(x) = 0$. Proto $q_2(x) = 0$ pro nekonečně mnoho hodnot x, a tedy je to nulový polynom.

Dále tedy budeme endomorfismus chápat jako zobrazení α dané předpisem

$$\alpha(x, y) = (r_1(x), y \cdot r_2(x)), \tag{3.3}$$

kde r_1, r_2 jsou nějaké racionální funkce. Můžeme psát

$$r_1(x) = p(x)/q(x), \qquad r_2(x) = s(x)/t(x),$$

kde $p(x)$ a $q(x)$, resp. $s(x)$ a $t(x)$ jsou polynomy bez společného faktoru. Pokud pro nějaký bod (x_0, y_0) platí $q(x_0) = 0$, pak definujeme $\alpha(x_0, y_0) = \mathcal{O}$; říkáme, že funkce r_1 není v bodě (x_0, y_0) definovaná. Následující lemma nám říká, že je-li funkce r_1 v nějakém bodě definovaná, pak je v tomto bodě definovaná i funkce r_2.

Lemma 17 ([1], cvičení 2.19)**.** *Ať α, $r_1(x) = p(x)/q(x)$, $r_2(x) = s(x)/t(x)$ jsou definovány jako výše. Pokud $t(x_0) = 0$, pak také $q(x_0) = 0$.*

Důkaz. Zvolme libovolný bod (x, y) z $E(\overline{\mathbb{F}}_q)$. Potom i $\alpha(x, y)$ leží v $E(\overline{\mathbb{F}}_q)$, neboli platí

$$\left(y \cdot \frac{s(x)}{t(x)}\right)^2 = \left(\frac{p(x)}{q(x)}\right)^3 + A\left(\frac{p(x)}{q(x)}\right) + B,$$

$$\frac{(x^3 + Ax + B)s(x)^2}{t(x)^2} = \frac{p(x)^3 + A \cdot p(x)q(x)^2 + B \cdot q(x)^3}{q(x)^3}.$$

Označme $u(x) \coloneqq p(x)^3 + A \cdot p(x)q(x)^2 + B \cdot q(x)^3$, potom

$$(x^3 + Ax + B)s(x)^2 q(x)^3 = u(x)t(x)^2.$$

Předpokládáme, že $t(x_0) = 0$; proto x_0 je aspoň dvojnásobný kořen polynomu $u(x)t(x)^2$, a tedy také polynomu $(x^3 + Ax + B)s(x)^2 q(x)^3$. Polynom $x^3 + Ax + B$ nemá vícenásobný kořen a polynomy $s(x), t(x)$ nemají společný kořen; to dohromady znamená, že x_0 je kořenem polynomu $q(x)^3$, a tedy i polynomu $q(x)$. □

Definice 5. Definujeme *stupeň endomorfismu* α jako maximum ze stupňů polynomů $p(x), q(x)$:

$$\deg \alpha = \max\{\deg p(x),\ \deg q(x)\};$$

stupeň triviálního endomorfismu definujeme jako 0. Dále o netriviálním endomorfismu řekneme, že je *separabilní*, pokud $r_1'(x)$ není nulová funkce.

V dalším textu bude klíčové využití derivací. Budeme používat následující standardní značení:

- $\dfrac{\mathrm{d}}{\mathrm{d}x} f(x) = f'(x)$ pro derivaci funkce jedné proměnné,
- $\dfrac{\partial}{\partial x} f(x, y, \ldots)$ pro parciální derivaci funkce více proměnných.

Navíc budeme potřebovat formální derivaci $\mathrm{d}/\mathrm{d}x$ pro funkce více proměnných. Níže stručně shrneme, jakým způsobem je tato derivace definovaná. Vycházíme z textu [8, sekce 4.1].

Funkčním tělesem eliptické křivky dané rovnicí $y^2 = x^3 + Ax + B$ rozumíme podílové těleso oboru $\mathbb{F}_q[x, y]/(y^2 - x^3 - Ax - B)$; označme jej K. *Formální derivace podle* x je $\mathbb{F}_q$-lineární zobrazení

$$\mathrm{d}/\mathrm{d}x : \ K \to K$$

splňující

- $(\mathrm{d}/\mathrm{d}x)(u \cdot v) = u \cdot (\mathrm{d}/\mathrm{d}x)(v) + (\mathrm{d}/\mathrm{d}x)(u) \cdot v$ pro každé $u, v \in K$,
- $(\mathrm{d}/\mathrm{d}x)(x) = 1$.

Teorie v [8] říká, že zobrazení $\mathrm{d}/\mathrm{d}x$ je určeno jednoznačně, dále toto zobrazení splňuje následující vlastnosti (jde o standardní vlastnosti derivace):

- $(\mathrm{d}/\mathrm{d}x)(k) = 0$ pro každé $k \in \mathbb{F}_q$,
- $(\mathrm{d}/\mathrm{d}x)(y^n) = ny^{n-1}(\mathrm{d}/\mathrm{d}x)(y)$ pro každé $y \in K$, $n \geq 0$,
- $(\mathrm{d}/\mathrm{d}x)(y/z) = ((\mathrm{d}/\mathrm{d}x)(y) \cdot z - y \cdot (\mathrm{d}/\mathrm{d}x)(z))/(z^2)$ pro každé $y, z \in K$, $z \neq 0$.

Pro jednoduchost budeme používat značení $\mathrm{d}f/\mathrm{d}x = (\mathrm{d}/\mathrm{d}x)(f)$ pro $f \in K$. Z vlastností výše plyne tzv. *řetízkové pravidlo*:

- $\dfrac{\mathrm{d}f}{\mathrm{d}x} = \dfrac{\mathrm{d}f}{\mathrm{d}y}\dfrac{\mathrm{d}y}{\mathrm{d}x}$ pro $f \in K$,
- $\dfrac{\mathrm{d}f}{\mathrm{d}x} = \dfrac{\partial f}{\partial y_1}\dfrac{\mathrm{d}y_1}{\mathrm{d}x} + \dfrac{\partial f}{\partial y_2}\dfrac{\mathrm{d}y_2}{\mathrm{d}x}$ pro $f = f(y_1, y_2)$, $f, y_1, y_2 \in K$.

Poznámka. Uvažujme rovnici $y^2 = x^3 + Ax + B$. Aplikujeme řetízkové pravidlo pro $f(x, y) = y^2 - x^3 - Ax - B$:

$$\frac{\mathrm{d}f}{\mathrm{d}x} = \frac{\partial f}{\partial x}\frac{\mathrm{d}x}{\mathrm{d}x} + \frac{\partial f}{\partial y}\frac{\mathrm{d}y}{\mathrm{d}x} = \frac{\partial f}{\partial x} + \frac{\partial f}{\partial y}\frac{\mathrm{d}y}{\mathrm{d}x} = -3x^2 - A + 2yy'.$$

Víme, že $f = 0$ v K, dostáváme tedy

$$2yy' = 3x^2 + A.$$

Nyní dokážeme několik výsledků potřebných pro důkaz Hasseho věty v sekci 3.4. Budeme používat značení $\operatorname{Ker}\alpha$ pro jádro homomorfismu α.

Tvrzení 18. *Ať α je netriviální endomorfismus eliptické křivky E. Pokud je α separabilní, pak*

$$\deg\alpha = \#\operatorname{Ker}\alpha.$$

Důkaz. Ať je α dáno racionálními funkcemi $r_1(x) = p(x)/q(x)$, $r_2(x) = s(x)/t(x)$ jako výše. Definujme polynom $f(x) \coloneqq (p'q - pq')(x)$. Zobrazení α je separabilní, proto $r_1'(x) = f(x)/q(x)^2$ není nulová funkce; z toho plyne, že $f(x)$ není nulový polynom. Ať S je množina všech prvků x z $\overline{\mathbb{F}}_q$ takových, že $f(x) = 0$ nebo $q(x) = 0$; podmínka $q(x) = 0$ nám zajistí, že pro $x \notin S$ jsou hodnoty $r_1(x), r_2(x)$ definované. Dále zvolme prvek (a, b) z $E(\overline{\mathbb{F}}_q)$ takový, že

1. $a, b \neq 0$,
2. $\deg(p(x) - a \cdot q(x)) = \max\{\deg p(x),\ \deg q(x)\}$,
3. $a \notin r_1(S)$,
4. $(a, b) \in \alpha(E(\overline{\mathbb{F}}_q))$.

Musíme ověřit, že takový prvek (a, b) existuje. Nejprve ukážeme, že množina $r_1(\overline{\mathbb{F}}_q)$ je nekonečná. Kdyby tomu tak nebylo, pak by díky nekonečnosti $\overline{\mathbb{F}}_q$ existovala konstanta c taková, že $r_1(x) = p(x)/q(x) = c$ pro nekonečně mnoho různých x. To by ovšem znamenalo, že polynomy $p(x)$ a $q(x)$ se liší pouze o konstantu c, a tedy mají společný faktor (r_1 jistě není konstantní); to je spor s předpokladem. Dále pro každé x existuje y takové, že (x, y) leží na E. To dohromady znamená, že množina $\alpha(E(\overline{\mathbb{F}}_q))$ je nekonečná. Na druhou stranu, polynomy $f(x), q(x)$ nejsou nulové, a tedy množina S je konečná; proto je konečná i množina $r_1(S)$. Zbývá si uvědomit, že předpoklady $1, 2$ nejsou splněny pouze pro konečně mnoho bodů (a, b); bod (a, b) splňující všechny předpoklady tedy jistě lze najít.

Dokážeme, že (a, b) má právě $\deg \alpha$ vzorů při zobrazení α. Ať x_0 splňuje $r_1(x_0) = a$; hledáme y_0 takové, že $\alpha(x_0, y_0) = (a, b)$. Kdyby $r_2(x_0) = 0$, pak by bod $(a, 0)$ ležel na E, což nelze (víme, že na E již leží bod (a, b) pro $b \neq 0$). Chceme, aby $r_2(x_0)y_0 = b$; z toho máme $y_0 = b/r_2(x_0)$. Zjistili jsme, že hodnota x_0 jednoznačně určuje hodnotu y_0, dále tedy místo vzorů bodu (a, b) při zobrazení α můžeme počítat vzory prvku a při zobrazení r_1. Všimneme si, že tyto vzory jsou právě kořeny polynomu $p(x) - a \cdot q(x)$ z předpokladu 2. Tento polynom má stupeň roven $\deg \alpha$, a tedy má $\deg \alpha$ kořenů. Zbývá ukázat, že tyto kořeny jsou po dvou různé, neboli že polynom $p(x) - a \cdot q(x)$ nemá vícenásobný kořen.

Kdyby x_1 byl vícenásobný kořen, pak platí

$$\begin{aligned} p(x_1) &= a \cdot q(x_1), \\ p'(x_1) &= a \cdot q'(x_1). \end{aligned}$$

Přehozením levé a pravé strany jedné z rovnic a následným vynásobením obou rovnic dostaneme

$$a \cdot p(x_1)q'(x_1) = a \cdot p'(x_1)q(x_1).$$

Předpokládáme, že $a \neq 0$, proto x_1 je kořenem polynomu $f(x) = (p'q - pq')(x)$. To ovšem znamená, že x_1 je prvkem S, a tedy $r_1(x_1) = a$ je prvkem $r_1(S)$; to je spor s předpokladem 3.

Dokázali jsme, že existuje právě $\deg \alpha$ vzorů bodu (a, b) při zobrazení α. Toto nutně znamená, že existuje právě $\deg \alpha$ vzorů bodu $\mathcal{O}$ (toto plyne přímo z faktu, že α je homomorfismus); platí tedy $\#\mathrm{Ker}\, \alpha = \deg \alpha$. □

Lemma 19. *Ať (u, v) je pevně zvolený bod na eliptické křivce E. Předpokládejme, že pro každý bod $(x, y) \neq \pm(u, v)$ na E platí*

$$(x, y) + (u, v) = (f(x, y), g(x, y)),$$

kde f, g jsou racionální funkce. Pak

$$y \cdot \frac{\mathrm{d}}{\mathrm{d}x} f(x, y) = g(x, y).$$

Důkaz. Z formulky pro součet bodů na eliptické křivce dostaneme

$$f(x,y) = \left(\frac{v-y}{u-x}\right)^2 - x - u,$$
$$g(x,y) = -\left(\frac{v-y}{u-x}\right)^3 + \left(\frac{v-y}{u-x}\right)(2x+u) - y.$$

Spočítáme derivaci pomocí řetízkového pravidla:

$$\frac{\mathrm{d}}{\mathrm{d}x} f(x,y) = \frac{\partial f}{\partial x} + \frac{\partial f}{\partial y}\frac{\mathrm{d}y}{\mathrm{d}x} = \left(\frac{-2(y-v)^2}{(x-u)^3} - 1\right) + \frac{2(y-v)}{(x-u)^2}\cdot y'.$$

Víme, že platí identity $v^2 = u^3 + Au + B$, $y^2 = x^3 + Ax + B$; navíc máme identitu $2yy' = 3x^2 + A$. Přímočarým výpočtem za použití uvedených identit lze ověřit, že platí následující (nejprve použijeme třetí identitu, poté první a druhou identitu):

$$\begin{aligned}
&(x-u)^3\left(y\cdot\frac{\mathrm{d}}{\mathrm{d}x}f(x,y) - g(x,y)\right) = \\
&= -2y(y-v)^2 + 2yy'(y-v)(x-u) + (y-v)^3 - (y-v)(x-u)^2(2x+u) = \\
&= (y-v)\Big((3x^2+A)(x-u) - (x-u)^2(2x+u) + (y-v)^2 - 2y(y-v)\Big) = \\
&= (y-v)(x^3 - u^3 + Ax - Au - y^2 + v^2) = \\
&= (y-v)(-B+B) = 0,
\end{aligned}$$

a tedy $y\cdot\frac{\mathrm{d}}{\mathrm{d}x}f(x,y) - g(x,y) = 0$. □

Lemma 20. *Ať $\alpha_1, \alpha_2, \alpha_3$ jsou netriviální endomorfismy takové, že $\alpha_1 + \alpha_2 = \alpha_3$. Pro $i = 1, 2, 3$ můžeme endomorfismus α_i zapsat ve tvaru* (3.3)*:*

$$\alpha_i(x,y) = (R_i(x), y\cdot S_i(x)),$$

kde R_i, S_i jsou nějaké racionální funkce. Předpokládejme, že existují konstanty c_1, c_2 takové, že

$$\frac{R_1'(x)}{S_1(x)} = c_1, \qquad \frac{R_2'(x)}{S_2(x)} = c_2.$$

Potom

$$\frac{R_3'(x)}{S_3(x)} = c_1 + c_2.$$

Důkaz. Použijeme následující značení. Ať $(x_1, y_1) = \alpha_1(x,y)$, $(x_2, y_2) = \alpha_2(x,y)$; dále ať $(x_3, y_3) = \alpha_3(x,y) = \alpha_1(x,y) + \alpha_2(x,y) = (x_1, y_1) + (x_2, y_2)$. Potom x_3, y_3 můžeme chápat jako racionální funkce v proměnných x_1, x_2, y_1, y_2; ty pak můžeme chápat jako racionální funkce v proměnných x, y.

Můžeme přepsat předpoklad ze znění lemmatu, pro $j = 1, 2$ dostaneme

$$R_j'(x) = c_j\cdot S_j(x),$$
$$\frac{\mathrm{d}x_j}{\mathrm{d}x} = c_j\cdot\frac{y_j}{y}.$$

Dále použijeme lemma 19 pro $(x, y) \coloneqq (x_1, y_1)$, $(u, v) \coloneqq (x_2, y_2)$, dostaneme

$$\frac{\mathrm{d}}{\mathrm{d}x_1} x_3(x_1, y_1) = \frac{y_3}{y_1},$$
$$\frac{\partial x_3}{\partial x_1} + \frac{\partial x_3}{\partial y_1}\frac{\mathrm{d}y_1}{\mathrm{d}x_1} = \frac{y_3}{y_1};$$

podobně pro $(x, y) \coloneqq (x_2, y_2)$, $(u, v) \coloneqq (x_1, y_1)$ dostaneme

$$\frac{\partial x_3}{\partial x_2} + \frac{\partial x_3}{\partial y_2}\frac{\mathrm{d}y_2}{\mathrm{d}x_2} = \frac{y_3}{y_2}.$$

Nyní můžeme provést následující výpočet (použijeme řetízkové pravidlo a vztahy odvozené výše):

$$\begin{aligned}
\frac{\mathrm{d}x_3}{\mathrm{d}x} &= \frac{\partial x_3}{\partial x_1}\frac{\mathrm{d}x_1}{\mathrm{d}x} + \frac{\partial x_3}{\partial y_1}\frac{\mathrm{d}y_1}{\mathrm{d}x} + \frac{\partial x_3}{\partial x_2}\frac{\mathrm{d}x_2}{\mathrm{d}x} + \frac{\partial x_3}{\partial y_2}\frac{\mathrm{d}y_2}{\mathrm{d}x} = \\
&= \frac{\partial x_3}{\partial x_1}\frac{\mathrm{d}x_1}{\mathrm{d}x} + \frac{\partial x_3}{\partial y_1}\frac{\mathrm{d}y_1}{\mathrm{d}x_1}\frac{\mathrm{d}x_1}{\mathrm{d}x} + \frac{\partial x_3}{\partial x_2}\frac{\mathrm{d}x_2}{\mathrm{d}x} + \frac{\partial x_3}{\partial y_2}\frac{\mathrm{d}y_2}{\mathrm{d}x_2}\frac{\mathrm{d}x_2}{\mathrm{d}x} = \\
&= \left(\frac{\partial x_3}{\partial x_1} + \frac{\partial x_3}{\partial y_1}\frac{\mathrm{d}y_1}{\mathrm{d}x_1}\right)\frac{\mathrm{d}x_1}{\mathrm{d}x} + \left(\frac{\partial x_3}{\partial x_2} + \frac{\partial x_3}{\partial y_2}\frac{\mathrm{d}y_2}{\mathrm{d}x_2}\right)\frac{\mathrm{d}x_2}{\mathrm{d}x} = \\
&= \frac{y_3}{y_1}\frac{y_1}{y}\cdot c_1 + \frac{y_3}{y_2}\frac{y_2}{y}\cdot c_2 = \frac{y_3}{y}(c_1 + c_2).
\end{aligned}$$

Nakonec se vrátíme ke značení ze znění lemmatu:

$$\frac{\mathrm{d}x_3}{\mathrm{d}x} = \frac{y_3}{y}(c_1 + c_2),$$
$$R_3'(x) = S_3(x)(c_1 + c_2).$$

□

3.3 Frobeniův endomorfismus

V sekci 3.1 jsme definovali Frobeniův endomorfismus $\varphi_q : \overline{\mathbb{F}}_q \to \overline{\mathbb{F}}_q$ předpisem $\varphi(a) = a^q$. Analogicky můžeme definovat *Frobeniův endomorfismus eliptické křivky* E:

$$\begin{aligned}
\phi_q :\ & E(\overline{\mathbb{F}}_q) \to E(\overline{\mathbb{F}}_q), \\
& (x, y) \mapsto (x^q, y^q).
\end{aligned}$$

Poznámka. Frobeniův endomorfismus ϕ_q je skutečně endomorfismus. Využijeme fakt, že φ_q je homomorfismus, který funguje jako identita na $\mathbb{F}_q$; připomeňme, že uvažujeme eliptickou křivku definovanou nad $\mathbb{F}_q$.

Ověřme, že $\phi_q(x, y)$ leží v $E(\overline{\mathbb{F}}_q)$. Vyjdeme z rovnice eliptické křivky E, závěr dostaneme umocněním na q:

$$\begin{aligned}
y^2 &= x^3 + Ax + B, \\
(y^q)^2 &= (x^q)^3 + A^q x^q + B^q, \\
(y^q)^2 &= (x^q)^3 + Ax^q + B.
\end{aligned}$$

Přímo z definice vidíme, že ϕ_q je určeno racionálními funkcemi. Zbývá ověřit, že ϕ_q je homomorfismus. Zvolme nějaké body (x_1, y_1), (x_2, y_2) z $E(\overline{\mathbb{F}}_q)$, označme $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$. Ověřujeme, že

$$(x_3^q, y_3^q) = (x_1^q, y_1^q) + (x_2^q, y_2^q).$$

Předpokládejme, že $(x_1, y_1) \neq \pm(x_2, y_2)$. Vyjdeme z definice sčítání bodů na E, závěr dostaneme umocněním na q:

$$x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1, \quad \text{kde } m = \frac{y_2 - y_1}{x_2 - x_1},$$

$$x_3^q = \widetilde{m}^2 - x_1^q - x_2^q, \quad y_3^q = \widetilde{m}(x_1^q - x_3^q) - y_1^q, \quad \text{kde } \widetilde{m} = \frac{y_2^q - y_1^q}{x_2^q - x_1^q}.$$

Případ $(x_1, y_1) = (x_2, y_2)$ se ověří analogicky. Situace, kdy $(x_1, y_1) = -(x_2, y_2)$ nebo je jeden z bodů roven bodu v nekonečnu, jsou zřejmé.

Pro zobrazení φ_q jsme v sekci 3.1 dokázali, že $a \in \overline{\mathbb{F}}_q$ leží v $\mathbb{F}_q$ právě tehdy, když $\varphi_q(a) = a$. Analogické tvrzení opět platí pro zobrazení ϕ_q.

Poznámka. Ať (x, y) je prvek $E(\overline{\mathbb{F}}_q)$. Potom

$$(x, y) \in E(\mathbb{F}_q) \iff \phi_q(x, y) = (x, y).$$

Stačí si uvědomit, že (x, y) leží v $E(\mathbb{F}_q)$, právě když x, y leží v $\mathbb{F}_q$; toto ovšem nastává, právě když $x^q = x$, $y^q = y$.

V dalším textu budeme kromě Frobeniova endomorfismu potřebovat ještě endomorfismus násobení celým číslem. Ať P je bod na eliptické křivce E a n je celé číslo. Pro kladné n definujeme nP jako součet $P + \cdots + P$ s n sčítanci, pro záporné n definujme nP jako součet $(-P) + \cdots + (-P)$ s $-n$ sčítanci, pro $n = 0$ definujeme $nP = \mathcal{O}$. Definujeme zobrazení $n : \ E(\overline{\mathbb{F}}_q) \to E(\overline{\mathbb{F}}_q)$ dané předpisem $n(P) = nP$. Množina bodů na E tvoří komutativní grupu, definice nP je tedy korektní a zobrazení n je endomorfismus E.

Dále budeme pracovat se zobrazeními tvaru $a\alpha + b\beta : \ E(\overline{\mathbb{F}}_q) \to E(\overline{\mathbb{F}}_q)$, kde α, β jsou endomorfismy E a a, b jsou celá čísla; toto zobrazení je dané předpisem

$$(a\alpha + b\beta)(P) = a(\alpha(P)) + b(\beta(P)).$$

Není těžké ověřit, že zobrazení $a\alpha + b\beta$ je opět endomorfismus E.

Následující dvě tvrzení budou klíčová v sekci 3.4.

Tvrzení 21. *Endomorfismus $\phi_q - 1$ je separabilní.*

Důkaz. Vyjádříme zobrazení ϕ_q a (-1) ve tvaru (3.3):

$$\phi_q(x, y) = (R_{\phi_q}(x), y \cdot S_{\phi_q}(x)) = (x^q, y^q) = (x^q, y \cdot (x^3 + Ax + B)^{(q-1)/2}),$$
$$(-1)(x, y) = (R_{-1}(x), y \cdot S_{-1}(x)) = (x, -y) = (x, y \cdot (-1)),$$

Potom máme

$$c_{\phi_q} \coloneqq \frac{R'_{\phi_q}(x)}{S_{\phi_q}(x)} = \frac{(x^q)'}{S_{\phi_q}(x)} = \frac{q \cdot x^{q-1}}{S_{\phi_q}(x)} = 0,$$

$$c_{-1} \coloneqq \frac{R'_{-1}(x)}{S_{-1}(x)} = \frac{1}{-1} = -1.$$

Nakonec použijeme lemma 20, dostaneme

$$\frac{R'_{\phi_q-1}(x)}{S_{\phi_q-1}(x)} = c_{\phi_q} + c_{-1} = 0 - 1 = -1.$$

Proto R'_{ϕ_q-1} není nulová funkce, a tedy zobrazení $\phi_q - 1$ je separabilní. □

Tvrzení 22. $\mathrm{Ker}(\phi_q - 1) = E(\mathbb{F}_q)$.

Důkaz. Ať $(x, y) \in E(\overline{\mathbb{F}}_q)$. Definice jádra homomorfismu říká, že (x, y) leží v $\mathrm{Ker}(\phi_q - 1)$, právě když $(\phi_q - 1)(x, y) = \mathcal{O}$, neboli $\phi_q(x, y) = (x, y)$. Toto pak nastává právě tehdy, když (x, y) leží v $E(\mathbb{F}_q)$. Nakonec bod $\mathcal{O}$ zřejmě leží v obou množinách. □

3.4 Hasseho věta

Posledním pojmem, který potřebujeme pro důkaz Hasseho věty, je *Weilovo párování*. Výklad odpovídající teorie je nad rámec práce, definici Weilova párování proto jen nastíníme a potřebný výsledek (tvrzení 23) použijeme jako fakt. Vycházíme z [1, kapitola 3].

Ať K je nyní obecné těleso. Bod P na eliptické křivce E nad K nazveme *torzní*, pokud $nP = \mathcal{O}$ pro nějaké kladné celé číslo n; torzní body jsou tedy právě prvky grupy $E(\overline{K})$, jejichž řád je konečný. Ať n je nějaké kladné celé číslo takové, že charakteristika tělesa K jej nedělí. Uvažujme množinu

$$E[n] = \{P \in E(\overline{K}) \mid nP = \mathcal{O}\},$$

tato množina se v angličtině nazývá výmluvně *n-torsion*. Dále uvažujme množinu všech n-tých odmocnin z jedné v $\overline{K}$:

$$\mu_n = \{x \in \overline{K} \mid x^n = 1\}.$$

Weilovo párování pro dané n je zobrazení

$$e_n : \ E[n] \times E[n] \to \mu_n$$

splňující vlastnosti uvedené ve znění věty [1, věta 3.9]; tato věta navíc říká, že zobrazení e_n existuje. Z definice Weilova párování potom lze odvodit následující (pro nás klíčový) výsledek.

Tvrzení 23 ([1], tvrzení 3.16)**.** *Ať α, β jsou endomorfismy eliptické křivky E a a, b jsou celá čísla. Pro endomorfismus $a\alpha + b\beta : \ E(\overline{K}) \to E(\overline{K})$ pak platí*

$$\deg(a\alpha + b\beta) = a^2 \deg\alpha + b^2 \deg\beta + ab(\deg(\alpha + \beta) - \deg\alpha - \deg\beta).$$

Nyní nám již nic nebrání ve zformulování a dokázání Hasseho věty.

Věta 24 (Hasseho věta)**.** *Pro grupu $E(\mathbb{F}_q)$ platí*

$$|q + 1 - \#E(\mathbb{F}_q)| \leq 2\sqrt{q}.$$

Důkaz. Tvrzení 22 nám říká, že $\mathrm{Ker}(\phi_q - 1) = E(\mathbb{F}_q)$. Podle tvrzení 21 je endomorfismus $\phi_q - 1$ separabilní, můžeme tedy použít tvrzení 18; dostáváme $\#\mathrm{Ker}(\phi_q - 1) = \deg(\phi_q - 1)$. Dohromady tedy máme

$$\#E(\mathbb{F}_q) = \deg(\phi_q - 1).$$

Označme $a \coloneqq q + 1 - \#E(\mathbb{F}_q) = q + 1 - \deg(\phi_q - 1)$. Nyní použijeme tvrzení 23 pro endomorfismus $r\phi_q - s$, kde r, s jsou celá čísla, $s \neq 0$. Endomorfismus $r\phi_q - s$ chápeme jako $r\phi_q + s(-1)$, navíc zřejmě $\deg \phi_q = q$, $\deg(-1) = 1$; dostáváme

$$\begin{aligned}\deg(r\phi_q - s) = r^2 \deg \phi_q + s^2 \deg(-1) + rs(\deg(\phi_q - 1) - \deg \phi_q - \deg(-1)) = \\ = r^2 q + s^2 + rs(\deg(\phi_q - 1) - q - 1) = r^2 q + s^2 - rsa.\end{aligned}$$

Přímo z definice stupně endomorfismu plyne, že $\deg(r\phi_q - s) \geq 0$. Proto

$$\begin{aligned}r^2 q + s^2 - rsa \geq 0, \\ q\left(\frac{r}{s}\right)^2 - a\left(\frac{r}{s}\right) + 1 \geq 0.\end{aligned}$$

Jinými slovy jsme zjistili, že

$$qx^2 - ax + 1 \geq 0 \tag{3.4}$$

pro libovolné racionální číslo x. Nyní využijeme známý fakt, že množina $\mathbb{Q}$ je hustá v množině $\mathbb{R}$; z toho plyne, že vztah (3.4) je splněn pro každé reálné číslo x. Posledním krokem je výpočet diskriminantu kvadratického polynomu $qx^2 - ax + 1$. Tento diskriminant je díky vztahu (3.4) menší nebo roven 0, máme tedy

$$\begin{aligned}a^2 - 4q \leq 0, \\ |a| \leq 2\sqrt{q},\end{aligned}$$

což jsme měli dokázat. □

Závěr

V práci jsme se věnovali studiu eliptických křivek, tj. křivek daných rovnicí tvaru $y^2 = x^3 + Ax + B$ nad nějakým tělesem K; pro těleso L splňující $K \subseteq L$ jsme potom symbolem $E(L)$ označili množinu bodů na eliptické křivce, jejichž koeficienty leží v L. Volba tělesa, nad nímž křivky uvažujeme, je klíčová – pro různá tělesa dostaneme různá využití eliptických křivek. V této práci jsme se zajímali o eliptické křivky nad konečnými tělesy (ty se používají mimo jiné v mnoha kryptografických algoritmech). V celém textu jsme se snažili o co možná nejelementárnější přístup, pozornost jsme přitom věnovali zejména algebraickým, nikoli geometrickým aspektům eliptických křivek.

Nejprve jsme představili základní teorii eliptických křivek, při tom jsme se nevyhnuli několika technickým aspektům (vliv charakteristiky tělesa na tvar rovnice eliptické křivky, singulární křivky jakožto křivky s násobným bodem); poté jsme odvodili a zformulovali grupový zákon, tj. definici operace sčítání na $E(L)$.

Dále jsme dokázali známý fakt, že množina $E(L)$ společně s operací sčítání tvoří komutativní grupu; tento fakt je zásadní pro další využití eliptických křivek. K důkazu jsme přistoupili elementárně, vycházeli jsme tedy přímo z definice operace sčítání. Ukázalo se, že takový přístup je technicky velmi náročný; důkaz je nutné provést rozborem případů, přičemž pro některé případy jsou výpočty velmi komplikované (pracuje se s polynomy se stovkami členů). Z tohoto důvodu jsme odpovídající část důkazu provedli pomocí počítačového programu Mathematica, zdrojový kód a výsledky výpočtů jsme pak pro přehlednost umístili do přílohy práce.

Nakonec jsme dokázali Hasseho větu – důležité tvrzení, jež nám dává horní i dolní odhad na řád grupy $E(\mathbb{F}_q)$. K tomu jsme potřebovali několik výsledků o endomorfismech eliptických křivek (to jsou homomorfismy na množině $E(\overline{\mathbb{F}}_q)$ zadané racionálními funkcemi), klíčový pro nás byl Frobeniův endomorfismus ϕ_q daný předpisem $\phi_q(x, y) = (x^q, y^q)$.

Poznamenejme, že existují metody, jak počet bodů na eliptické křivce nad konečným tělesem spočítat přesně; těmito metodami jsme se nezabývali (jde o rozsáhlé téma, které by zřejmě vydalo na samostatnou práci).

Seznam použité literatury

[1] Lawrence C. Washington. *Elliptic curves: number theory and cryptography.* Chapman & Hall/CRC, second edition, 2008.

[2] Joseph H. Silverman. An introduction to the theory of elliptic curves. `https://www.math.brown.edu/~jhs/Presentations/WyomingEllipticCurve.pdf`, 2006. Citováno: 15. 6. 2018.

[3] Joseph H. Silverman. *The arithmetic of elliptic curves.* Springer-Verlag, second edition, 2009.

[4] Todd Rowland. Elliptic discriminant. `http://mathworld.wolfram.com/EllipticDiscriminant.html`. Citováno: 15. 6. 2018.

[5] Kazuyuki Fujii and Hiroshi Oike. An algebraic proof of the associative law of elliptic curves. *Advances in pure mathematics*, 7:649–659, 2017.

[6] Stefan Friedl. An elementary proof of the group law for elliptic curves. `http://math.rice.edu/~friedl/papers/AAELLIPTIC.PDF`. Citováno: 21. 6. 2018.

[7] David Stanovský. *Základy algebry.* Matfyzpress, 2010.

[8] Henning Stichtenoth. *Algebraic function fields and codes.* Springer-Verlag, second edition, 2008.

A. Program v Mathematice

Lemma 3

```
(* výpočet s, t, u, v *)
m1 = (y2 - y1)/(x2 - x1);
x4 = m1^2 - x1 - x2;
y4 = m1(x1 - x4) - y1;
m2 = (y3 - y4)/(x3 - x4);
s = m2^2 - x4 - x3;
t = m2(x4 - s) - y4;

m3 = (y3 - y2)/(x3 - x2);
x5 = m3^2 - x2 - x3;
y5 = m3(x2 - x5) - y2;
m4 = (y5 - y1)/(x5 - x1);
u = m4^2 - x1 - x5;
v = m4(x1 - u) - y1;

Print[s]
```

$$x1 + x2 - x3 - \frac{(-y1 + y2)^2}{(-x1 + x2)^2} + \frac{\left(y1 - \frac{(-y1+y2)\left(2\,x1+x2-\frac{(-y1+y2)^2}{(-x1+x2)^2}\right)}{-x1+x2} + y3\right)^2}{\left(x1 + x2 + x3 - \frac{(-y1+y2)^2}{(-x1+x2)^2}\right)^2}$$

```
Print[t]
```

$$y1 - \frac{(-y1 + y2)\left(2\,x1 + x2 - \frac{(-y1+y2)^2}{(-x1+x2)^2}\right)}{-x1 + x2} + \frac{1}{x1 + x2 + x3 - \frac{(-y1+y2)^2}{(-x1+x2)^2}}\left(y1 - \frac{(-y1 + y2)\left(2\,x1 + x2 - \frac{(-y1+y2)^2}{(-x1+x2)^2}\right)}{-x1 + x2} + y3\right)$$

$$\left(-2\,x1 - 2\,x2 + x3 + \frac{2\,(-y1 + y2)^2}{(-x1 + x2)^2} - \frac{\left(y1 - \frac{(-y1+y2)\left(2\,x1+x2-\frac{(-y1+y2)^2}{(-x1+x2)^2}\right)}{-x1+x2} + y3\right)^2}{\left(x1 + x2 + x3 - \frac{(-y1+y2)^2}{(-x1+x2)^2}\right)^2}\right)$$

```
Print[u]
```

$$x3 - \frac{(-y1 + y3)^2}{(-x1 + x3)^2} + \frac{\left(-2\,y1 + \frac{(-y1+y3)\left(2\,x1+x3-\frac{(-y1+y3)^2}{(-x1+x3)^2}\right)}{-x1+x3}\right)^2}{\left(-2\,x1 - x3 + \frac{(-y1+y3)^2}{(-x1+x3)^2}\right)^2}$$

```
Print[v]
```

$$-y1+\frac{1}{-2\,x1-x3+\frac{(-y1+y3)^2}{(-x1+x3)^2}}\left(-2\,y1+\frac{(-y1+y3)\left(2\,x1+x3-\frac{(-y1+y3)^2}{(-x1+x3)^2}\right)}{-x1+x3}\right)$$

$$\left(x1-x3+\frac{(-y1+y3)^2}{(-x1+x3)^2}-\frac{\left(-2\,y1+\frac{(-y1+y3)\left(2\,x1+x3-\frac{(-y1+y3)^2}{(-x1+x3)^2}\right)}{-x1+x3}\right)^2}{\left(-2\,x1-x3+\frac{(-y1+y3)^2}{(-x1+x3)^2}\right)^2}\right)$$

```
(* s, t ve tvaru zlomku; pro přehlednost vytiskneme pouze jmenovatele *)

jmenovatelS = Denominator[Together[s]];
Print[jmenovatelS]
```

$$\left(x1^3-x1^2\,x2-x1\,x2^2+x2^3+x1^2\,x3-2\,x1\,x2\,x3+x2^2\,x3-y1^2+2\,y1\,y2-y2^2\right)^2$$

```
jmenovatelS = Denominator[Together[t]];
Print[jmenovatelT]
```

$$\left(-x1^3+x1^2\,x2+x1\,x2^2-x2^3-x1^2\,x3+2\,x1\,x2\,x3-x2^2\,x3+y1^2-2\,y1\,y2+y2^2\right)^3$$

```
jmenovatelS = Denominator[Together[u]];
Print[jmenovatelU]
```

$$\left(x1\,x2^2+x2^3-2\,x1\,x2\,x3-x2^2\,x3+x1\,x3^2-x2\,x3^2+x3^3-y2^2+2\,y2\,y3-y3^2\right)^2$$

```
jmenovatelS = Denominator[Together[v]];
Print[jmenovatelV]
```

$$\left(x1\,x2^2+x2^3-2\,x1\,x2\,x3-x2^2\,x3+x1\,x3^2-x2\,x3^2+x3^3-y2^2+2\,y2\,y3-y3^2\right)^3$$

```
(* upravíme jmenovatele do přijatelnějšího tvaru *)

Print[FullSimplify[jmenovatelS]]
```

$$\left(-(x1-x2)^2\,(x1+x2+x3)+(y1-y2)^2\right)^2$$

```
Print[FullSimplify[jmenovatelT]]
```

$$\left(-(x1-x2)^2\,(x1+x2+x3)+(y1-y2)^2\right)^3$$

```
Print[FullSimplify[jmenovatelU]]
```

$$\left(-(x2-x3)^2\,(x1+x2+x3)+(y2-y3)^2\right)^2$$

```
Print[FullSimplify[jmenovatelV]]
```

$$\left((x2-x3)^2\,(x1+x2+x3)-(y2-y3)^2\right)^3$$

```
(* na základě výstupů výše definujeme p, q *)
p = -(x1 - x2)^2(x1 + x2 + x3) + (y1 - y2)^2;
q = (x2 - x3)^2(x1 + x2 + x3) - (y2 - y3)^2;

(* výpočet největšího společného dělitele p^2 q^2(s - u), p^3 q^3(t - v) *)
gcd = PolynomialGCD[p^2 q^2(s - u), p^3 q^3(t - v)];
Print[gcd]
```

$$x1^3\,x2 - x1\,x2^3 - x1^3\,x3 + x2^3\,x3 + x1\,x3^3 - x2\,x3^3 - x2\,y1^2 + x3\,y1^2 + x1\,y2^2 - x3\,y2^2 - x1\,y3^2 + x2\,y3^2$$

```
(* upravíme gcd do přijatelnějšího tvaru *)
Print[Factor[x1^3 x2 - x1 x2^3 - x1^3 x3 + x2^3 x3 + x1 x3^3 - x2 x3^3]
        + Collect[-x2 y1^2 + x3 y1^2 + x1 y2^2 - x3 y2^2 - x1 y3^2 + x2 y3^2,
        {y1, y2, y3}]]
```

$$(x1 - x2)\,(x1 - x3)\,(x2 - x3)\,(x1 + x2 + x3) + (-x2 + x3)\,y1^2 + (x1 - x3)\,y2^2 + (-x1 + x2)\,y3^2$$

```
(* na základě výstupu výše definujeme r *)
r = (x1 - x2)(x2 - x3)(x1 - x3)(x1 + x2 + x3)
        + (x3 - x2)y1^2 + (x1 - x3)y2^2 + (x2 - x1)y3^2;

(* nyní ověříme, že platí r = 0,
        pokud předpokládáme yi^2 = xi^3 + A xi + B, i = 1, 2, 3 *)
rId = Expand[r/.{y1^2 -> x1^3 + A x1 + B, y2^2 -> x2^3 + A x2 + B,
        y3^2 -> x3^3 + A x3 + B}];
Print[rId]
```

```
0
```

Lemma 4

```
(* výpočet s, t, u, v *)

m1 = (3x1^2 + A)/(2y1);
x4 = m1^2 - 2x1;
y4 = m1 (x1 - x4) - y1;
m2 = (y3 - y4)/(x3 - x4);
s = m2^2 - x4 - x3;
t = m2(x4 - s) - y4;

m3 = (y3 - y1)/(x3 - x1);
x5 = m3^2 - x1 - x3;
y5 = m3(x1 - x5) - y1;
m4 = (y5 - y1)/(x5 - x1);
u = m4^2 - x1 - x5;
v = m4(x1 - u) - y1;

Print[s]
```

$$2\,x1 - x3 - \frac{\left(A + 3\,x1^2\right)^2}{4\,y1^2} + \frac{\left(-\frac{\left(A+3\,x1^2\right)\left(3\,x1-\frac{\left(A+3\,x1^2\right)^2}{4\,y1^2}\right)}{2\,y1} + y1 + y3\right)^2}{\left(2\,x1 + x3 - \frac{\left(A+3\,x1^2\right)^2}{4\,y1^2}\right)^2}$$

```
Print[t]
```

$$-\frac{\left(A + 3\,x1^2\right)\left(3\,x1 - \frac{\left(A+3\,x1^2\right)^2}{4\,y1^2}\right)}{2\,y1} + y1 +$$

$$\frac{1}{2\,x1 + x3 - \frac{\left(A+3\,x1^2\right)^2}{4\,y1^2}}\left(-\frac{\left(A + 3\,x1^2\right)\left(3\,x1 - \frac{\left(A+3\,x1^2\right)^2}{4\,y1^2}\right)}{2\,y1} + y1 + y3\right)$$

$$\left(-4\,x1 + x3 + \frac{\left(A + 3\,x1^2\right)^2}{2\,y1^2} - \frac{\left(-\frac{\left(A+3\,x1^2\right)\left(3\,x1-\frac{\left(A+3\,x1^2\right)^2}{4\,y1^2}\right)}{2\,y1} + y1 + y3\right)^2}{\left(2\,x1 + x3 - \frac{\left(A+3\,x1^2\right)^2}{4\,y1^2}\right)^2}\right)$$

```
Print[u]
```

$$x3 - \frac{(-y1 + y3)^2}{(-x1 + x3)^2} + \frac{\left(-2\,y1 + \frac{(-y1+y3)\left(2\,x1+x3-\frac{(-y1+y3)^2}{(-x1+x3)^2}\right)}{-x1+x3}\right)^2}{\left(-2\,x1 - x3 + \frac{(-y1+y3)^2}{(-x1+x3)^2}\right)^2}$$

```
Print[v]
```

$$-y1 + \frac{1}{-2\,x1 - x3 + \frac{(-y1+y3)^2}{(-x1+x3)^2}}\left(-2\,y1 + \frac{(-y1 + y3)\left(2\,x1 + x3 - \frac{(-y1+y3)^2}{(-x1+x3)^2}\right)}{-x1 + x3}\right)$$

$$\left(x1 - x3 + \frac{(-y1 + y3)^2}{(-x1 + x3)^2} - \frac{\left(-2\,y1 + \frac{(-y1+y3)\left(2\,x1+x3-\frac{(-y1+y3)^2}{(-x1+x3)^2}\right)}{-x1+x3}\right)^2}{\left(-2\,x1 - x3 + \frac{(-y1+y3)^2}{(-x1+x3)^2}\right)^2}\right)$$

```
(* s, t ve tvaru zlomku; pro přehlednost vytiskneme pouze jmenovatele *)

jmenovatelS = Denominator[Together[s]];
Print[jmenovatelS]
```

$$\left(A^2 + 6\,A\,x1^2 + 9\,x1^4 - 8\,x1\,y1^2 - 4\,x3\,y1^2\right)^2$$

```
jmenovatelS = Denominator[Together[t]];
Print[jmenovatelT]
```

$$\left(A^2 + 6\,A\,x1^2 + 9\,x1^4 - 8\,x1\,y1^2 - 4\,x3\,y1^2\right)^3$$

```
jmenovatelS = Denominator[Together[u]];
Print[jmenovatelU]
```

$$\left(2\,x1^3 - 3\,x1^2\,x3 + x3^3 - y1^2 + 2\,y1\,y3 - y3^2\right)^2$$

```
jmenovatelS = Denominator[Together[v]];
Print[jmenovatelV]
```

$$\left(-2\,x1^3 + 3\,x1^2\,x3 - x3^3 + y1^2 - 2\,y1\,y3 + y3^2\right)^3$$

```
(* upravíme jmenovatele do přijatelnějšího tvaru *)

Print[FullSimplify[jmenovatelS]]
```

$$\left(\left(A + 3\,x1^2\right)^2 - 4\,(2\,x1 + x3)\,y1^2\right)^2$$

```
Print[FullSimplify[jmenovatelT]]
```

$$\left(\left(A + 3\,x1^2\right)^2 - 4\,(2\,x1 + x3)\,y1^2\right)^3$$

```
Print[FullSimplify[jmenovatelU]]
```

$$\left(-(x1 - x3)^2\,(2\,x1 + x3) + (y1 - y3)^2\right)^2$$

```
Print[FullSimplify[jmenovatelV]]
```

$$\left(-(x1 - x3)^2\,(2\,x1 + x3) + (y1 - y3)^2\right)^3$$

```
(* na základě výstupů výše definujeme p, q *)
p = (A + 3x1^2)^2 - 4y1^2(2x1 + x3);
q = -(x1 - x3)^2(2x1 + x3) + (y1 - y3)^2;

(* výpočet největšího společného dělitele p^2 q^2(s - u), p^3 q^3(t - v) *)
gcd = PolynomialGCD[p^2 q^2(s - u), p^3 q^3(t - v)];
Print[gcd]
```

$$2\,\left(A\,x1\,y1 + x1^3\,y1 - A\,x3\,y1 - x3^3\,y1 - y1^3 + y1\,y3^2\right)$$

```
(* upravíme gcd do přijatelnějšího tvaru *)
Print[FullSimplify[2(A x1 y1 + x1^3 y1 - A x3 y1 - x3^3 y1 - y1^3 + y1 y3^2)]]
```

$$2\,y1\,\left(x1^3 + A\,(x1 - x3) - x3^3 - y1^2 + y3^2\right)$$

```
(* na základě výstupu výše definujeme r *)
r = 2y1(x1^3 + A(x1 - x3) - x3^3 - y1^2 + y3^2);

(* nyní ověříme, že platí r = 0,
        pokud předpokládáme yi^2 = xi^3 + A xi + B, i = 1, 2, 3 *)
rId = Expand[r/.{y1^2 -> x1^3 + A x1 + B, y2^2 -> x2^3 + A x2 + B,
        y3^2 -> x3^3 + A x3 + B}];
Print[rId]
```

```
0
```

Lemma 5

```
(* výpočet s, t, u, v *)

m1 = (3x1^2 + A)/(2y1);
x4 = m1^2 - 2x1;
y4 = m1(x1 - x4) - y1;
m2 = (3x4^2 + A)/(2y4);
s = m2^2 - 2x4;
t = m2(x4 - s) - y4;

m3 = (y4 - y1)/(x4 - x1);
x5 = m3^2 - x1 - x4;
y5 = m3(x1 - x5) - y1;
m4 = (y5 - y1)/(x5 - x1);
u = m4^2 - x1 - x5;
v = m4(x1 - u) - y1;

(* přímý výpočet s - u, t - v *)

Print[Simplify[s - u]]
```

```
0
```

```
Print[Simplify[t - v]]
```

```
0
```