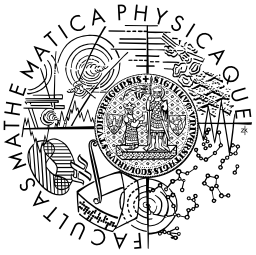

MATEMATICKO-FYZIKÁLNÍ FAKULTA
Univerzita Karlova

**DIPLOMOVÁ PRÁCE**

Adam Zvěřina

# Tateova-Šafarevičova grupa eliptické křivky

Katedra algebry

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

Studijní program: Matematické struktury

Studijní obor: Matematické struktury

Praha 2023

Prohlašuji, že jsem tuto diplomovou práci vypracoval(a) samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů. Tato práce nebyla využita k získání jiného nebo stejného titulu.

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

Děkuji svému vedoucímu docentu Šťovíčkovi za cenné připomínky a laskavé vedení, díky kterým se mi lépe psalo. Svým rodičům děkuji za podporu během celého studia. A nejvíc děkuju Báře za všechno.

Název práce: Tateova-Šafarevičova grupa eliptické křivky

Autor: Adam Zvěřina

Katedra: Katedra algebry

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

Abstrakt: Tato práce se zabývá Tateovou-Šafarevičovou grupou a jejím vztahem k racionálním bodům na křivce a jejímu ranku. Napřed definujeme pojem profinitní grupy a charakterizujeme je jako Galoisovy grupy tělesových rozšíření. Potom definujeme Tateovu-Šafarevičovu grupu pomocí Galoisovy kohomologie a vysvětlíme její vztah k racionálním bodům křivky. Nakonec zformulujeme Birchovu-Swinnerton-Dyerovu domněnku, která dává do souvislosti rank eliptické křivky a řád její Tateovy-Šafarevičovy grupy.

Klíčová slova: Tateova-Šafarevičova grupa, Selmerova grupa, Birchova-Swinnerton-Dyerova domněnka, profinitní grupy, rank eliptické křivky

Title: The Tate-Shafarevich group of an elliptic curve

Author: Adam Zvěřina

Department: Department of algebra

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

Abstract: This thesis deals with the Tate-Shafarevich group and its relation to rational points on the curve and its rank. We first define the notion of profinite groups and characterize them as Galois groups of field extensions. Then we define the Tate-Shafarevich group using Galois cohomology and explain its relation to the rational points on the curve. Finally, we formulate the Birch-Swinnerton-Dyer conjecture, which relates the rank of an elliptic curve and the order of its Tate-Shafarevich group.

Keywords: Tate-Shafarevich group, Selmer group, Birch-Swinnerton-Dyer conjecture, profinite groups, rank of an elliptic curve

# Obsah

# Úvod

Algebraická geometrie se už od svých začátků zabývá hledáním kořenů polynomů ve více proměnných. Mezi těmito polynomy zaujímají významné místo tzv. eliptické křivky, tj. rovnice tvaru $y^2 = f(x)$, kde $f$ je polynom stupně 3 bez násobných kořenů. Už ve třetím století našeho letopočtu se jimi zabýval Diofantos, byť jim tak neříkal a neznal koncept algebraické geometrie.

Problém, kterým se Diofantos ve své *Aritmetice* zabýval, zní takto: „Rozdělit zadané číslo na dvě menší čísla taková, že jejich součin je krychle minus její hrana.“ Pro Diofanta byla čísla jen kladná a racionální a krychlí se myslí třetí mocnina nějakého čísla. Tedy řešil rovnici

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

Když položíme $a = 6$ a od obou stran odečteme 9, dostaneme rovnici

$$6y - y^2 - 9 = x^3 - x - 9.$$

Nakonec substituujeme $y = y' + 3$ a $x = -x'$, což vede na

$$y'^2 = x'^3 - x' + 9,$$

a to je rovnice eliptické křivky.

Další slavný matematik, který zkoumal podobné problémy, byl Fibonacci. Ten nazval přirozené číslo $n$ *kongruentním číslem*, pokud existuje racionální číslo $r$ takové, že $r^2 - n$, $r^2$, $r^2 + n$ jsou nenulové druhé mocniny racionálních čísel.

Je-li $n$ kongruentní číslo, tak součin $(r^2 - n)r^2(r^2 + n)$ je nenulová druhá mocnina racionálního čísla, a pokud položíme $r^2 = x$, dostaneme rovnici

$$y^2 = x(x - n)(x + n)$$

a zase dostáváme rovnici eliptické křivky.

Současný název dostaly eliptické křivky v devatenáctém století – souvisí s problémem hledání obvodu elipsy a obecněji s délkou oblouku.

Mějme elipsu se středem v počátku a uvažujme polopřímku začínající v počátku, která svírá s kladnou částí osy $x$ úhel $\theta$. Pak délka oblouku mezi průsečíkem elipsy s polopřímkou a průsečíkem elipsy s kladnou částí osy $x$ je funkce proměnné $\theta$. Tímto problémem se zabýval hlavně Euler.

Při snaze o zobecnění došli matematici k funkcím tvaru

$$f(x) = \int_c^x R\Big(t, \sqrt{P(t)}\Big)\,dt,$$

kde $c$ je konstanta, $R$ je racionální funkce a $P$ je polynom stupně 3 nebo 4, který nemá násobné kořeny. Těmto funkcím začali říkat *eliptické integrály*.

O pár desítek let později se Jacobi zabýval opačným problémem: Pokud známe délku oblouku, je možné spočítat úhel? Spolu s Abelem přišli s kladnou odpovědí. Přitom našli třídu funkcí, které slouží k invertování eliptických integrálů, a nazvali je *eliptické funkce*.

Rovnice eliptické funkce definované nad nějakým prostorem má v tomto prostoru nějaká řešení. Pokud je nakreslíme, dostaneme obrázek křivky. Nikdo nejspíš nepřišel na lepší jméno, tak se jim začalo říkat *eliptické křivky*.

Další rozvoj teorie eliptických křivek vedl k objevům mnoha aplikací v osmdesátých letech minulého století. Hlavní aplikace jsou v kryptografii a například Lenstrův algoritmus slouží k faktorizaci čísel. O aplikacích široce pojednává Washington.

Tato práce se zaměřuje na teoretické aspekty eliptických křivek, konkrétně na Tateovu-Šafarevičovu grupu a její souvislost s rankem křivky.

V první kapitole zopakujeme základní pojmy a zavedeme značení. Ve druhé kapitole se budeme zabývat základy teorie profinitních grup, jak je vyložil Ribes ve svých poznámkách z přednášek. Úplnější zdroj představuje jeho kniha *Profinite Groups* (Ribes a Zaleskii, 2010). O těch bude řeč především proto, že jedna z nejdůležitějších grup v celé práci, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, je profinitní.

Ve třetí kapitole definujeme ústřední pojem celé práce – Tateovu-Šafarevičovu grupu – a podrobně vysvětlíme, jak souvisí s racionálními body na křivce. V jistém smyslu měří, jak moc daná křivka nesplňuje Hasseho princip. Nakonec ve čtvrté kapitole vyslovíme Birchovu-Swinnerton-Dyerovu domněnku, což je jeden z problémů tisíciletí. Birch a Swinnerton-Dyer v šedesátých letech numerickými výpočty došli k domněnce, která spojuje řád Tateovy-Šafarevičovy grupy a rank eliptické křivky.

# 1. Přípravné práce

## 1.1 Eliptické křivky

**Definice 1.** *Buď $K$ těleso. Množinu $\{(x,y) \mid x,y \in K\}$ značíme $\mathbb{A}^2_K$ a nazýváme ji* afinní rovinou, *popř.* dvourozměrným afinním prostorem. *Uvažujme trojice $(x,y,z)$, kde $x,y,z \in K$ a alespoň jeden prvek je nenulový. Řekneme, že trojice $(x_1,y_1,z_1)$ a $(x_2,y_2,z_2)$ jsou ekvivalentní, což značíme $(x_1,y_1,z_1) \sim (x_2,y_2,z_2)$, pokud existuje nenulový prvek $\lambda \in K$ takový, že $(x_1,y_1,z_1) = (\lambda x_2, \lambda y_2, \lambda z_2)$. Třídu ekvivalence příslušející $(x,y,z)$ značíme $(x : y : z)$ a množinu všech tříd ekvivalence značíme $\mathbb{P}^2_K$ a nazýváme ji* dvourozměrným projektivním prostorem.

Když je $z \neq 0$, tak $(x : y : z) = (x/z : y/z : 1)$. Ale pokud $z = 0$, tak nemůžeme dělit, nebo se můžeme dohodnout, že to odpovídá přiřazení nekonečné hodnoty souřadnici $x$ nebo $y$. Proto prvkům tvaru $(x : y : 0)$ říkáme body v nekonečnu. Ostatním bodům říkame konečné a můžeme je ztotožnit s prvky $\mathbb{A}^2_K$ pomocí zobrazení $(x,y) \mapsto (x : y : 1)$.

**Definice 2.** Eliptickou křivkou *$E$ definovanou nad tělesem $K$ rozumíme množinu bodů $x,y \in K$, které splňují rovnici*

$$y^2 = x^3 + ax + b, \tag{1.1}$$

*kde $a,b \in K$. Té říkáme* Weierstrassova rovnice *eliptické křivky nebo rovnice ve* Weierstrassově tvaru.

Lze ukázat, že diskriminant kubického polynomu na pravé straně rovnice (1.1) je roven $4a^3 + 27b^2$. Požadujeme, aby tento polynom neměl násobné kořeny v žádném nadtělese $K$, tj. $4a^3 + 27b^2 \neq 0$.

Můžeme uvažovat rovnici tvaru

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1.2}$$

kterou nazýváme *zobecněná Weierstrassova rovnice*. Pokud se charakteristika tělesa $K$ nerovná dvěma nebo třem, tak lze snadno převést rovnici (1.2) do tvaru rovnice (1.1).

Uvažujme na chvíli speciální případ – křivku definovanou nad $\mathbb{Q}$. Tedy $E$ je zadaná rovnicí $y^2 = x^3 + a'x + b'$, kde koeficienty $a',b'$ jsou racionální čísla. Zbavíme se jmenovatelů tak, že vynásobíme obě strany rovnice vhodným přirozeným číslem, a dostaneme

$$cy^2 = cx^3 + ax + b,$$

kde $a,b,c$ jsou celá čísla a $c \neq 0$. Vynásobíme obě strany celým číslem $c^5$. Tím dostáváme

$$(c^3y)^2 = (c^2x)^3 + (ac^3)(c^2x) + bc^5,$$

a nakonec substitucí $y_1 = c^3y$, $x_1 = c^2x$ dostaneme Weierstrassovu rovnici s celočíselnými koeficienty, která definuje stejnou křivku. Tedy pro eliptickou křivku definovanou nad racionálními čísly můžeme BÚNO uvažovat rovnici s celočíselnými koeficienty.

Chceme-li uvažovat křivku $E$ v projektivním prostoru, tak musíme homogenizovat rovnici (1.1). Tím dostaneme $y^2z = x^3 + axz^2 + bz^3$. Body tvaru $(x : y : 1)$ na projektivní křivce odpovídají bodům $(x,y)$ na afinní křivce. Abychom objevili nové body, dosadíme $z = 0$ a dostaneme $0 = x^3$. Tedy $x = 0$ a $y$ je libovolné. Bod $(0 : 0 : 0)$ ale není součástí projektivního prostoru, tedy $y \neq 0$. Jenže pro libovolné nenulové $y$ platí $(0 : y : 0) = (0 : 1 : 0)$. Tedy na křivce $E$ je jen jeden bod v nekonečnu.

Nadále budeme křivky uvažovat v afinním prostoru. Bod v nekonečnu k nim jen uměle přidáme a budeme s ním zacházet jako se speciálním případem. Pokud je $E$ křivka definovaná nad tělesem $K$ rovnicí (1.1), tak pro libovolné těleso $L \supseteq K$ definujeme

$$E(L) = \{\mathcal{O}\} \cup \{(x,y) \in L \times L \mid y^2 = x^3 + ax + b\},$$

kde $\mathcal{O} = (0 : 1 : 0)$.

**Definice 3.** *Buď $E$ eliptická křivka nad $K$ a $g \in K[x,y]$. Zobrazení $E(K) \to K$ definované vztahem $(a,b) \mapsto g(a,b)$ nazýváme* regulární funkce *na $E$.*

Označme $f = y^2 - x^3 - ax - b$. Pak $f$ je ireducibilní v $K[x,y]$, tedy $(f)$ je prvoideál a jeho libovolný násobek definuje konstantně nulovou regulární funkci na $E$. Pak z Hilbertovy věty o nulách plyne, že existuje izomorfismus okruhů

$$K[x,y]/(f) \to \{\text{regulární funkce na } E\}$$

definovaný vztahem $g \mapsto ((a,b) \mapsto g(a,b))$. Protože $(f)$ je prvoideál, tak je $K[x,y]/(f)$ obor integrity, který značíme $K[E]$ a nazýváme ho *souřadnicový okruh $E$*.

Označíme $K(E)$ podílové těleso souřadnicového okruhu a uvažujme jeho prvek $\psi = g/h$. Předpokládejme, že $h$ není konstantně nulové. Pak je množina nul funkce $h$, tj. $N = \{(a,b) \in E(K) \mid h(a,b) = 0\}$, konečná, a máme zobrazení

$$E(K) \setminus N \to K$$

definované vztahem $(a,b) \mapsto g(a,b)/h(a,b)$. Takové $\psi$ nazveme *racionální funkcí* na $E$, která je *regulární* na $E \setminus N$.

**Definice 4.** *Buď $K$ perfektní těleso a $E_1, E_2$ eliptické křivky nad $K$. Řekneme, že dvojice $(f_1,f_2)$ regulárních zobrazení na $E_1$ je* regulární zobrazení $\phi : E_1 \to E_2$, *pokud pro každé rozšíření těles $L \supseteq K$ je splněná podmínka*

$$P \in E_1(L) \implies (f_1(P), f_2(P)) \in E_2(L).$$

**Definice 5.** *Buď $\phi : E_1 \to E_2$ regulární zobrazení eliptických křivek nad $K$. Řekneme, že $\phi$ je* konstantní, *pokud pro každé rozšíření těles $L \supseteq K$ platí, že obraz $\phi(L)$ je jednobodový.*

## 1.2 Grupový zákon

Buď $E$ eliptická křivka definovaná rovnicí (1.1) a buďte $P_1 = (x_1,y_1)$, $P_2 = (x_2,y_2)$ body na $E$ takové, že $P_1 \neq \mathcal{O} \neq P_2$. Definujeme bod $P_3 = (x_3,y_3)$, který značíme $P_3 = P_1 + P_2$ následovně:

- Pokud $x_1 \neq x_2$, tak

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

- Pokud $x_1 = x_2$ a $y_1 \neq y_2$, tak $P_1 + P_2 = \mathcal{O}$.
- Pokud $P_1 = P_2$ a $y_1 \neq 0$, tak

$$x_3 = m^2 - 2x_1, \quad y_3 = m(x_1 - x_3) - y_1, \quad \text{kde } m = \frac{3x_1^2 + a}{2y_1}.$$

- Pokud $P_1 = P_2$ a $y_1 = 0$, tak $P_1 + P_2 = \mathcal{O}$.

Navíc pro každý bod $P$ na $E$ definujeme

$$P + \mathcal{O} = P.$$

Na předchozí definici se přirozeně můžeme dívat i geometricky. Máme-li body $P_1$ a $P_2$ na křivce $E$, tak uvažujeme přímku, která těmito body prochází. Tato přímka protíná křivku $E$ ve třetím bodu $P_3'$. Tento zobrazíme v osové souměrnosti podle osy $x$ a dostaneme bod $P_3$. Ostatní případy si lze představit obdobně.

Když jsou souřadnice bodů $P_1$ a $P_2$ prvky tělesa $L$ a toto těleso obsahuje koeficienty $a$,$b$, tak souřadnice bodu $P_1 + P_2$ jsou taktéž v $L$. Tedy $E(L)$ je uzavřená na operaci $+$ a platí následující věta.

**Věta 1.** *Buď $E$ eliptická křivka nad $K$ definovaná rovnicí* (1.1) *a buď $L \supseteq K$ rozšíření těles. Pak $E(L)$ s operací $+$ definovanou výše tvoří komutativní grupu, jejíž neutrální prvek je $\mathcal{O}$.*

Důkaz předchozí věty vynecháme. Spolu s tím jsme vynechali detaily týkající se geometrické představy sčítání bodů. Obojí lze najít v knize *Rational points on elliptic curves* (Silverman a Tate, 1992).

**Definice 6.** *Mějme eliptické křivky $E_1, E_2$ definované nad tělesem $K$ a buď $\phi : E_1 \to E_2$ nekonstantní regulární zobrazení. Když ho složíme s vhodnou translací, dostaneme regulární zobrazení, které pošle neutrální prvek $E_1(K)$ na neutrální prvek $E_2(K)$. Takové zobrazení nazýváme isogenie.*

Lze ukázat, že isogenie je zároveň grupový homomorfismus. Pokud je to izomorfismus, řekneme, že tyto křivky jsou izomorfní. Množinu všech isogenií $\phi : E_1 \to E_2$ značíme $\mathrm{Hom}(E_1,E_2)$. Pokud $E_1 = E_2$, tak skládáním isogenií dostaneme opět isogenii, tedy můžeme značit $\mathrm{End}(E) = \mathrm{Hom}(E,E)$.

Pro $m \in \mathbb{Z}$ definujeme zobrazení $[m] : E \to E$. Pokud $m > 0$, tak pro $P \in E(\mathbb{Q})$ položíme $[m](P) = \underbrace{P + \cdots + P}_{\text{n}}$. Pokud $m < 0$, tak $[m](P) = [-m](-P)$. A nakonec $[0](P) = \mathcal{O}$. Tomu zobrazení budeme říkat *násobení*. Indukcí lze ukázat, že pro každé $m \neq 0$ to je isogenie.

Navíc budeme pro $m \in \mathbb{Z}$ značit

$$E[m] = \{P \in E(\overline{K}) \mid mP = \mathcal{O}\}.$$

**Definice 7.** *Pokud má těleso $K$ nulovou charakteristiku a zobrazení $[\cdot] : \mathbb{Z} \to \mathrm{End}(E)$ není izomorfismus (tj. okruh $\mathrm{End}(E)$ je ostře větší než $\mathbb{Z}$), tak řekneme, že křivka $E$ má* komplexní násobení.

Detaily týkající se zobrazení křivek uvádí Fulton.

## 1.3 Průnik kvadrik

**Definice 8.** *Buď $K$ těleso a $n \in \mathbb{N}$.* Kvadrikou dimenze $n$ *rozumíme množinu tvaru*

$$\{(x_0 : x_1 : \cdots : x_n) \in \mathbb{P}_K^{n+1} \mid q(x_0,x_1,\ldots,x_n) = 0\},$$

*kde $q$ je nenulový homogenní polynom stupně 2 nad $K$ v proměnných $x_0, x_1, \ldots, x_n$.*

Obecně platí, že průnik dvou kvadrik dimenze 2 je eliptická křivka. Důkaz včetně detailního výpočtu s převedením do Weierstrassova tvaru uvádí Knaf a kol.. My se zaměříme na speciální případ, který využijeme později, tak jak ho rozpracoval Washington v sekci 2.5.4.

Buď $K$ těleso charakteristiky různé od dvou a buďte $a$,$b$,$c$,$d$,$e$,$f$ nenulové prvky $K$. Uvažujme rovnice

$$au^2 + bv^2 = e, \quad cu^2 + dw^2 = f,$$

které chápeme jako plochy v prostoru se souřadnicemi $u$,$v$,$w$. Jejich průnik je křivka a dokážeme, že je-li neprázdný, pak je to eliptická křivka definovaná rovnicí ve Weierstrassově tvaru.

Než budeme zkoumat průnik, podíváme se na první rovnici odděleně. Budeme ji chápat tak, že dává křivku $C$ v rovině určené prvky $u$,$v$. Buď $P = (u_0,v_0)$ bod na $C$ a $L$ přímka procházející bodem $P$ mající směrnici $m$, tj.

$$u = u_0 + t, \quad v = v_0 + mt.$$

Chceme najít druhý průsečík $L$ a $C$. Dosazením do rovnice pro $C$ s využitím toho, že $au_0^2 + bv_0^2 = e$, dostaneme

$$a(2u_0t + t^2) + b(2v_0mt + m^2t^2) = 0.$$

Případ $t = 0$ odpovídá $(u_0,v_0)$, takže můžeme vytknout $t$ a dostat tak

$$t = -\frac{2au_0 + 2bv_0m}{a + bm^2},$$

čímž dostáváme souřadnice druhého průsečíku

$$u = u_0 - \frac{2au_0 + 2bv_0m}{a + bm^2} \qquad v = v_0 - \frac{2amu_0 + 2bv_0m^2}{a + bm^2}.$$

Konvencí zavedeme, že případ $m = \infty$ dává bod $(u_0, -v_0)$.

Pokud $(u,v)$ je bod na $C$ se souřadnicemi v $K$, pak směrnice přímky spojující body $(u,v)$ a $P$ je rovněž v $K$, nebo rovná nekonečnu. Tedy máme bijekci mezi hodnotami $m$ včetně nekonečna a body na křivce $C$ včetně bodů v nekonečnu. Tedy jsme křivku $C$ parametrizovali.

Teď pronikneme $C$ s plochou $cu^2 + dw + 2 = f$. Dosadíme do této rovnice výraz pro $u$, který jsme dostali z výpočtu výše, a dostaneme

$$dw^2 = f - c\left(u_0 - \frac{2au_0 + 2bv_0m}{a + bm^2}\right)^2,$$

což můžeme přepsat na

$$d(w(a+bm^2))^2 = (a+bm^2)^2 f - c(bu_0m^2 - 2bv_0m - au_0) = (b^2f - cb^2u_0^2)m^4 + \dots,$$

a to potřebujeme převést na Weierstrassův tvar.

Mějme křivku definovanou rovnicí

$$v^2 = au^4 + bu^3 + cu^2 + du + e,$$

kde $a \neq 0$. Nechť existují $p,q \in K$ takové, že bod $(p,q)$ leží na této křivce. BÚNO můžeme předpokládat $p = 0$ (jinak změníme souřadnici $u$ na $u + p$). Nejprve předpokládejme $q = 0$. Pokud $d = 0$, pak má křivka singularitu v bodu (0,0), takže předpokládáme, že $d \neq 0$. Pak

$$(\frac{v}{u^2})^2 = d(\frac{1}{u})^3 + c(\frac{1}{u})^2 + b(\frac{1}{u}) + a,$$

což snadno převedeme do Weierstrassova tvaru s proměnnými $d/u, dv/u^2$.

Teď uvažujeme případ, kdy $q \neq 0$. Máme následující větu.

**Věta 2.** *Buď $K$ těleso charakteristiky různé od dvou. Uvažujme rovnici*

$$v^2 = au^4 + bu^3 + cu^2 + du + q^2,$$

*kde $a,b,c,d \in K$. Nechť*

$$x = \frac{2q(v+q) + du}{u^2}, \quad y = \frac{4q^2(v+q) + 2q(du + cu^2) - (d^2u^2/2q)}{u^3}.$$

*Položme*

$$a_1 = d/q, \quad a_2 = c - (d^2/4q^2), \quad a_3 = 2qb, \quad a_4 = -4q^2a, \quad a_6 = a_2a_4.$$

*Potom*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

*Inverzní transformace je*

$$u = \frac{2q(x+c) - (d^2/2q)}{y}, \quad v = -q + \frac{u(ux-d)}{2q}.$$

*Důkaz.* Uvádí Washington (2008) (Věta 2.17). □

Tedy podle předchozí věty můžeme přepsat rovnici

$$d(w(a+bm^2))^2 = (b^2f - cb^2u_0^2)m^4 + \dots$$

do Weierstrassova tvaru. Výpočtem navíc lze ukázat, že tato křivka je izomorfní původní křivce $E$.

## 1.4 $p$-adická čísla

Zvolme libovolné prvočíslo $p$ a buď $a \in \mathbb{Z}$ nenulové. Pak existuje jednoznačně určené $n \in \mathbb{N} \cup \{0\}$ takové, že $p^n \mid a$ a $p^{n+1} \nmid a$. Definujeme $v_p(a) = n$ a toto zobrazení nazýváme $p$-valuace. Pro nenulové racionální číslo $a/b$ definujeme jeho $p$-valuaci vztahem $v_p(a/b) = v_p(a) - v_p(b)$. Nakonec definujeme $v_p(0) = \infty$.

**Definice 9.** *Buď $K$ těleso. Řekneme, že zobrazení $|\cdot| : K \to [0,\infty)$ je* norma, *pokud pro všechna $x$,$y \in K$ splňuje:*

- $|x| = 0$ *právě tehdy, když* $x = 0$,
- $|xy| = |x||y|$,
- $|x + y| \leq |x| + |y|$.

Je-li $|\cdot|$ norma na $K$ a položíme-li $d(x,y) = |x-y|$, $x$,$y \in K$, pak je zobrazení $d$ metrika na $K$.

Na množině racionálních čísel definujeme $p$-adickou absolutní hodnotu následovně:

$$|x|_p = \begin{cases} p^{-v_p(x)} & \text{pokud } x \in \mathbb{Q} \setminus \{0\}, \\ 0 & \text{pokud } x = 0. \end{cases}$$

Pro každé prvočíslo $p$ platí, že $|\cdot|_p$ je norma, tedy indukuje $p$-adickou metriku. Navíc platí, že těleso $\mathbb{Q}$ není úplné vzhledem k $p$-adické metrice. Zúplnění značíme $\mathbb{Q}_p$ a říkáme mu těleso $p$-adických čísel. Stejně tak můžeme $\mathbb{Q}$ zúplnit vzhledem k euklidovské metrice a dostaneme těleso reálných čísel, které budeme v tomto kontextu značit $\mathbb{Q}_\infty$.

**Věta 3.** *(Ostrowski) Buď $|\cdot|$ netriviální norma na $\mathbb{Q}$, tj. existuje $a \in \mathbb{Q}$ takové, že $|a| \neq 0$. Označme $\hat{\mathbb{Q}}$ zúplnění $\mathbb{Q}$ vzhledem k indukované metrice. Potom platí buď $\hat{\mathbb{Q}} \cong \mathbb{Q}_\infty$, nebo existuje právě jedno prvočíslo $p$ takové, že $\hat{\mathbb{Q}} \cong \mathbb{Q}_p$.*

Důkazy tvrzení a detaily konstrukce lze najít v poznámkách z přednášek *Algebraic number theory* (Milne, 2020).

## 1.5 Eliptické křivky nad $\mathbb{Q}$

V této části budeme uvažovat eliptické křivky definované nad $\mathbb{Q}$ a vyslovíme dvě zásadní věty – Lutzové-Nagellovu a Mordellovu-Weilovu – které nám umožní zkoumat strukturu grupy $E(\mathbb{Q})$.

Teď už můžeme vyslovit první důležitou větu.

**Věta 4.** *(Mordellova-Weilova) Buď $E$ eliptická křivka definovaná nad $\mathbb{Q}$. Pak je grupa $E(\mathbb{Q})$ konečně generovaná.*

Předchozí věta je neuvěřitelně hluboká a její důkaz by zabral moc místa. Proto uvedeme jen povšechný plán důkazu. První krok je obsažen v následující větě.

**Věta 5.** *Buď $G$ komutativní grupa taková, že index $[G : 2G]$ je konečný. Nechť existuje zobrazení $h : G \to [0,\infty)$ splňující:*

- *Pro každé $M \in \mathbb{R}$ je množina $\{P \in G \mid h(P) \leq M\}$ konečná.*
- *Pro každé $P_0 \in G$ existuje konstanta $\kappa_0$ taková, že pro všechna $P \in G$ platí*

$$h(P_0 + P) \leq 2h(P) + \kappa_0.$$

- *Existuje konstanta $\kappa$ taková, že pro všechna $P \in G$ platí*

$$h(2P) \geq 4h(P) - \kappa.$$

*Pak je $G$ konečně generovaná.*

Důkaz Mordellovy-Weilovy věty pak spočívá v nalezení vhodného zobrazení $h : E(\mathbb{Q}) \to [0,\infty)$ a dokázání požadovaných vlastností. Buď $x = a/b \in \mathbb{Q}$, kde $a/b$ je zlomek v základním tvaru. Definujeme $H(x) = max\{|a|,|b|\}$. Pro $P = (x,y) \in E(\mathbb{Q})$ definujeme $H(P) = H(x)$. Chceme, aby $h$ byla nezáporná funkce a v jistém smyslu aditivní. Tedy definujeme $h(P) = log(H(P))$. Pro libovolné $P$ je $H(P) \geq 1$, tedy $h(P) \geq 0$. Tato zobrazení nazýváme výška a logaritmická výška. Zbytek důkazu lze nalézt v knize Silverman a Tate (1992).

Součástí důkazu Mordellovy-Weilovy věty je i ověření faktu, že grupa $E(\mathbb{Q})/2E(\mathbb{Q})$ je konečná. Ukážeme to jako důsledek Věty 24, kterou uvedeme později. Platí to i obecněji, což říká následující věta, tzv. slabá Mordellova-Weilova.

**Věta 6.** *Buď $K \supseteq \mathbb{Q}$ rozšíření těles konečného stupně a buď $E$ křivka definovaná nad $K$. Pak pro každé přirozené číslo $m \geq 2$ platí, že $E(K)/mE(K)$ je konečná grupa.*

*Důkaz.* Uvádí Silverman (2009) (Věta VIII.1.1).

□

**Věta 7.** *(Lutzové-Nagellova) Buď $E$ eliptická křivka zadaná rovnicí* (1.1)*, kde $a,b \in \mathbb{Z}$. Nechť $P = (x,y)$ je prvek $E(\mathbb{Q})$ konečného řádu. Pak $x,y \in \mathbb{Z}$, a je-li $y \neq 0$, pak $y^2 \mid 4a^3 + 27b^2$.*

Z Lutzové-Nagellovy věty okamžitě plyne, že je torzní podgrupa $E(\mathbb{Q})$ konečná, neboť pro libovolnou eliptickou křivku nad $\mathbb{Q}$ můžeme BÚNO uvažovat její Weierstrassovu rovnici s celočíselnými koeficienty. Totéž plyne rovněž z Mordellovy-Weilovy věty, protože podle ní je torzní podgrupa $E(\mathbb{Q})$ konečně generovaná, a protože má prvky jen konečného řádu, tak je sama konečná.

Víme, že $E(\mathbb{Q})$ je konečně generovaná abelovská grupa. Tedy je izomorfní grupě $\mathbb{Z}^r \oplus \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_i\mathbb{Z}$, kde $r, n_1, \ldots, n_i \in \mathbb{N}$. Navíc podgrupa $E(\mathbb{Q})$ izomorfní $\mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_i\mathbb{Z}$ je právě torzní podgrupa $E(\mathbb{Q})$.

Tedy pro libovolnou eliptickou křivku $E$ definovanou nad $\mathbb{Q}$ existuje přirozené číslo $r$ a konečná grupa $G$ takové, že

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus G.$$

Toto $r$ nazýváme *rank* křivky $E$.

Abychom popsali strukturu grupy $E(\mathbb{Q})$, stačí nalézt torzní podgrupu a rank. V případě torzní podgrupy hledání neuvěřitelně usnadňuje následující věta.

**Věta 8.** *(Mazur) Buď $E$ eliptická křivka definovaná nad $\mathbb{Q}$. Pak je torzní podgrupa $E(\mathbb{Q})$ izomorfní nějaké z následujících grup:*

$$\mathbb{Z}/n\mathbb{Z}, \text{ kde } n \in \{1, \ldots, 10, 12\},$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \text{ kde } n \in \{1, 2, 3, 4\}.$$

*Důkaz.* Lze nalézt v článku Mazur (1978).

□

*Příklad.* Spočítáme torzní podgrupu křivky definované rovnicí

$$y^2 = x^3 - 2.$$

Diskriminant je roven $27 \cdot (-2)^2 = 108$. Pokud $y = 0$, tak hledáme celočíselné kořeny rovnice $x^3 = 2$. Ta ale žádné celočíselné (ani racionální) kořeny nemá. Dále uvažujeme případ, že $y \neq 0$. Tady hledáme celá čísla $y$ taková, že $y \mid 108$. Tedy $y \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$. Pro tyto hodnoty $y$ hledáme celočíselné kořeny $x$ rovnic

$$x^3 - y^2 - 2 = 0.$$

- $x^3 - 3 = 0$ nemá celočíselné kořeny,
- $x^3 - 6 = 0$ nemá celočíselné kořeny,
- $x^3 - 11 = 0$ nemá celočíselné kořeny,
- $x^3 - 38 = 0$ také nemá celočíselné kořeny.

Tím pádem je torzní podgrupa této křivky triviální, tj. obsahje jen bod $\mathcal{O}$.

*Příklad.* Spočítáme torzní podgrupu křivky definované rovnicí

$$y^2 = x^3 + 1.$$

Hodnota diskriminantu je 27. V případě $y = 0$ dostáváme bod $(-1,0)$ jako kandidáta na prvek torzní podgrupy. Když $y \neq 0$, tak $y^2 \mid 27$, tudíž $y \in \{\pm 1, \pm 3\}$, a opět hledáme celočíselné kořeny rovnic.

- $x^3 = 0$ má kořen 0, a tedy máme kandidáty $(0, \pm 1)$,
- $x^3 - 8 = 0$ má kořen 2, a tedy dostáváme kandidáty $(2, \pm 3)$.

Teď postupně u všech kandidátů ověříme, jestli mají konečný řád. Díky Mazurově větě víme, že prvky torzní podgrupy mají řád nejvýše 12. Tedy pokud pro každé $n \in \{1, \ldots, 12\}$ platí $nP \neq \mathcal{O}$, pak $P$ nemá konečný řád.

Z definice okamžitě vidíme, že $2(-1,0) = \mathcal{O}$, tedy tento prvek má řád 2. Bod $(0,1)$ má řád 3, neboť $(0,1) + (0,1) = (0, -1)$ a $(0, -1) + (0,1) = \mathcal{O}$. Pro bod $(0, -1)$ skoro stejným výpočtem zjistíme totéž.

Nakonec se podíváme na body $(2, \pm 3)$. Zjistíme, že násobky bodu $(2,3)$ jsou $(0,1), (-1,0), (0, -1), (2, -3), \mathcal{O}$. Tedy tento prvek má řád 6. Analogicky zjistíme, že i bod $(2, -3)$ je řádu 6.

Torzní podgrupa je v tomto případě šestiprvková. Pohledem na seznam všech možností v tvrzení věty 8 zjistíme, že jediná grupa, která připadá v úvahu, je $\mathbb{Z}/6\mathbb{Z}$.

*Příklad.* Spočítáme torzní podgrupu křivky definované rovnicí

$$y^2 = x^3 - x.$$

V tomto případě je diskriminant $-4$. Pokud $y = 0$, tak máme tři potenciální prvky: $(-1,0), (0,0), (1,0)$. Když $y \neq 0$, tak $y \in \{\pm 1, \pm 2\}$.

- $x^3 - x - 1 = 0$ nemá celočíselné kořeny,
- $x^3 - x - 4 = 0$ nemá celočíselné kořeny.

Tedy máme celkem tři kandidáty. Okamžitě z definice plyne, že všechny tyto prvky jsou řádu 2. Tím pádem se zřejmě jedná o Kleinovu čtyřgrupu, tj. $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

*Příklad.* Spočítáme torzní podgrupu křivky definované rovnicí

$$y^2 = x^3 - 24003x + 1296702.$$

Hodnota diskriminantu je $4 \cdot (-24003)^3 + 27 \cdot 1296702^2 = -9917964518400$. V případě, že $y = 0$, dostáváme tři kandidáty: $(-177,0), (66,0), (111,0)$. Teď prozkoumáme případ $y \neq 0$. Z Lutzové-Nagellovy věty víme, že $y^2 \mid -9917964518400$. Všimneme si, že $3149280^2 = 9917964518400$, tedy $y \mid -3149280$. Tím pádem pro všechny dělitele $d$ čísla 3149280 hledáme celočíselné kořeny rovnice

$$x^3 - 24003x + 1296702 - d^2 = 0.$$

Protože 3149280 má 120 dělitelů, tak z praktických důvodů uvádíme jen ty, kde hledané řešení existuje.

- $x^3 - 24003x + 1296702 - 648^2 = 0$ má celočíselný kořen 39,
- $x^3 - 24003x + 1296702 - 972^2 = 0$ má celočíselný kořen 147,
- $x^3 - 24003x + 1296702 - 1620^2 = 0$ má celočíselný kořen $-69$,
- $x^3 - 24003x + 1296702 - 9720^2 = 0$ má celočíselný kořen 471.

Přímo z definice je vidět, že body $(-177,0), (66,0), (111,0)$ mají řád 2. Tedy zbývá ověřit, jak je to s body $(39, \pm 648), (147, \pm 972), (-69, \pm 1620)$ a $(471, \pm 9720)$.

Násobením bodu (39,648) dostaneme $(147,972), (-177,0), (147, -972), (39, -648), \mathcal{O}$, tedy je řádu 6. Pro bod $(39, -648)$ to spočítáme analogicky.

Výpočtem zjistíme, že $(147, 972) + (147,972) = (147, -972)$, tedy tento prvek je řádu 3. Analogicky to platí pro bod $(147, -972)$.

Násobky bodu $(-69, 1620)$ jsou $(147, -972), (66,0), (147,972), (-69, -1620)$ a $\mathcal{O}$. Stejně tak bod $(-69, -1620)$ je řádu 6.

Body (471,9720) a $(471, -9720)$ jsou rovněž řádu 6. Násobky prvku (471,9720) jsou $(147,972), (111,0), (147, -972), (471, -9720)$ a $\mathcal{O}$.

Torzní podgrupa má celkem 12 prvků. Z věty 8 tedy máme dvě možnosti – $\mathbb{Z}/12\mathbb{Z}$ a $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$. Protože grupa $\mathbb{Z}/12\mathbb{Z}$ obsahuje prvek řádu 4, tak je torzní podgrupa izomorfní $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$.

# 2. Profinitní grupy

**Definice 10.** *Buď $(I, \leq)$ částečně uspořádaná množina, která je navíc nahoru usměrněná, tj. pro libovolné prvky a,b $\in I$ existuje $c \in I$ takový, že $a \leq c$ a zároveň $b \leq c$. Uvažme systém množin indexovaný pomocí prvků $I$, tedy $(G_i)_{i\in I}$, a mějme pro libovolné i,j $\in I$, $i \leq j$ zobrazení $f_{i,j} : G_j \to G_i$.*

*Navíc požadujeme, aby platily následující dvě vlastnosti:*

- *$f_{i,i}$ je identické zobrazení na $G_i$.*
- *Pro všechna $i \leq j \leq k$ platí $f_{i,k} = f_{i,j} \circ f_{j,k}$.*

*Systém $(G_i)_{i\in I}$ splňující tyto podmínky nazveme* inverzním systémem *množin nad $I$.*

Pokud je každé $G_i$ grupa (okruh, modul, topologický prostor) a každé $f_{i,j}$ je homomorfismus grup (okruhů, modulů, popř. spojité zobrazení), tak hovoříme o inverzním systému grup (okruhů, modulů, topologických prostorů).

**Definice 11.** Inverzní limitou *systému $(G_i)_{i\in I}$ rozumíme*

$$\varprojlim G_i = \left\{(x_i)_{i\in I} \in \prod_{i\in I} G_i \mid \forall i,j \in I : i \leq j \implies f_{i,j}(x_j) = x_i\right\}.$$

Je-li $(G_i)_{i\in I}$ inverzní systém grup (okruhů, modulů), tak je $\varprojlim G_i$ podgrupa (podokruh, podmodul) součinu $\prod_{i\in I} G_i$.

**Definice 12.** *Buď $(G, \cdot, ^{-1}, e)$ grupa s topologií na své nosné množině. Na součinu $G \times G$ budeme uvažovat součinovou topologii. Jestliže jsou obě zobrazení $(x,y) \mapsto xy$ a $x \mapsto x^{-1}$ spojitá vzhledem k zadané topologii, řekneme, že $G$ je* topologická grupa. *Tyto dvě podmínky můžeme ekvivalentně nahradit jedinou – požadujeme spojitost zobrazení $(x,y) \mapsto x^{-1}y$.*

Z definice je zřejmé, že libovolná grupa s diskrétní topologií tvoří topologickou grupu. V dalším textu budeme u všech grup uvažovat diskrétní topologii, pokud nebude řečeno jinak.

**Věta 9.** *Nechť $I$ je množina a pro každé $i \in I$ buď $G_i$ topologická grupa. Pak součin grup $\prod_{i\in I} G_i$ spolu se součinovou topologií je rovněž topologická grupa.*

*Důkaz.* Označme $G = \prod_{i\in I} G_i$, $f : G \times G \to G$, $f(x,y) = x^{-1}y$, $f_i : G_i \times G_i \to G_i$, $f_i(x,y) = x^{-1}y$. Chceme dokázat spojitost $f$.

Z předpokladu je pro každé $i \in I$ zobrazení $f_i$ spojité. Tedy máme pro každé $i \in I$ spojité zobrazení $\pi_i \circ f = f_i \circ (\pi_i \times \pi_i)$, kde $\pi_i : G \to G_i$ je kanonická projekce a $\pi_i \times \pi_i : G \times G \to G_i \times G_i$ je po složkách kanonická projekce. Spojitost $f$ plyne z definice.

□

Z předchozího je zřejmé, že můžeme uvažovat inverzní systém topologických grup, kde zobrazení jsou spojité grupové homomorfismy. Můžeme tedy definovat následující pojem.

**Definice 13.** *Řekneme, že topologická grupa je* profinitní (prokonečná)*, pokud je izomorfní inverzní limitě konečných grup s diskrétní topologií.*

**Věta 10.** *Buď $(G_i)_{i\in I}$ inverzní systém Hausdorffových topologických prostorů. Pak inverzní limita $\varprojlim G_i$ je uzavřená podmnožina topologického prostoru $\prod_{i\in I} G_i$.*

*Důkaz.* Dokážeme, že doplněk $\varprojlim G_i$ je otevřená množina. Buď $x \in \prod_{i\in I} G_i$, $x \notin \varprojlim G_i$, tedy existují $i,j \in I$, $i \leq j$ takové, že $f_{i,j}(x_j) \neq x_i$. $G_i$ je Hausdorffův prostor, takže existují disjunktní otevřené množiny $U$,$V$ tak, že $f_{i,j}(x_j) \in U$, $x_i \in V$. Pro každé $k \in I$ definujeme

$$T_k = \begin{cases} U & \text{pokud } k = i, \\ f_{i,j}^{-1}(V) & \text{pokud } k = j, \\ G_k & \text{jinak.} \end{cases}$$

Pak platí, že $\prod_{k\in I} T_k$ je otevřená množina v $\prod_{k\in I} G_k$, obsahuje $x$ a je disjunktní s $\varprojlim G_i$.

□

**Věta 11.** *Každá profinitní grupa je kompaktní.*

*Důkaz.* Konečný topologický prostor je kompaktní. Součin kompaktních prostorů je podle Tichonovovy věty též kompaktní. Tedy podle předchozí věty je inverzní limita uzavřená podmnožina kompaktního prostoru, tudíž je sama kompaktní.

□

**Věta 12.** *Buď $G$ kompaktní topologická grupa a $H$ její podgrupa. Pak je $H$ otevřená právě tehdy, když je uzavřená a má konečný index.*

*Důkaz.* Buď $H$ otevřená. Pak každá rozkladová třída $aH, a \in G$ je také otevřená a z kompaktnosti $G$ plyne, že takových tříd je konečně mnoho. Navíc jsou všechny rozkladové třídy otevřené, a tedy $H$ je doplněk konečného sjednocení otevřených množin. Tudíž je $H$ uzavřená.

Naopak, nechť $H$ je uzavřená s konečným indexem. Každá rozkladová třída $aH, a \in G$ je uzavřená; tím pádem je doplněk $H$ konečné sjednocení uzavřených množin, což je uzavřená množina, tedy je $H$ otevřená.

□

**Věta 13.** *Buď $X$ topologický prostor. Pak NTJE:*

1. *Komponenty souvislosti $X$ jsou jednobodové množiny.*
2. *Pro každé body $x$,$y \in X$, $x \neq y$ existují neprázdné disjunktní otevřené množiny $A, B$ takové, že $x \in A$, $y \in B$ a $A \cup B = X$.*
3. *Pro každé body $x$,$y \in X$, $x \neq y$ existuje obojetná množina $A$ taková, že $x \in A$, $y \notin A$.*

*Důkaz.* 1 $\implies$ 3: Mějme libovolné body $x,y \in X$, $x \neq y$. Množina $\{x,y\}$ je z předpokladu nesouvislá, tedy obsahuje neprázdnou obojetnou množinu. Tím pádem jsou obě množiny $\{x\}$, $\{y\}$ obojetné.

3 $\implies$ 2: Definujeme $B$ jako doplněk $A$, a ihned dostáváme tvrzení.

2 $\implies$ 1: Buď $K$ komponenta $X$ a zvolme libovolné body $x,y \in K$, $x \neq y$. Z předpokladu existují neprázdné disjunktní otevřené množiny $A, B$ takové, že $x \in A$, $y \in B$ a $A \cup B = X$. Tím pádem jsou množiny $A \cap K$, $B \cap K$ neprázdné disjunktní a otevřené v $K$, které splňují $(A \cap K) \cup (B \cap K) = K$. To je spor se souvislostí $K$, a tedy má $K$ jen jeden prvek.

□

**Definice 14.** *Buď $X$ topologický prostor. Řekneme, že $X$ je* totálně nesouvislý*, pokud splnňuje ekvivalentní podmínky z Věty 13.*

**Věta 14.** *Každá profinitní grupa je totálně nesouvislá.*

*Důkaz.* Buď $G_i, i \in I$ projektivní systém konečných grup s diskrétní topologií a $G = \varprojlim G_i$. Dokážeme, že pro každý prvek $g \in G, g \neq 1$ existuje obojetná množina, která obsahuje 1 a neobsahuje $g$. Její doplněk je obojetná množina, která obsahuje $g$ a neobsahuje 1. Z definice topologické grupy plyne, že pro každý prvek $g \in G$ je translace $\rho_g : G \times G \to G$, $\rho_g(x) = g \cdot x$ homeomorfismus. Obojetnou množinu obsahující 1 posuneme o nějaký prvek $h \in G$ a dostaneme neprázdné disjunktní otevřené množiny oddělující libovolné prvky $g,h \in G$.

Zvolme $g \in G, g \neq 1$ a označme $\pi_i, i \in I$ jako přirozenou projekci $\varprojlim G_i \to G_i$. Existuje $i \in I$ takové, že $\pi_i(g) \neq 1$. Tedy $\pi^{-1}(\{1\})$ je otevřená podgrupa $G$, která neobsahuje $g$.

Pro profinitní grupu $G$ platí, že je-li $H$ otevřená podgrupa $G$, pak je $H$ podle věty 12 uzavřená, a tedy obojetná. Tím je důkaz dokončen.

□

**Věta 15.** *Nechť $G$ je Hausdorffova, kompaktní a totálně nesouvislá topologická grupa a buď $\{H_i\}_{i \in I}$ množina všech otevřených normálních podgrup $G$. Pak $\bigcap_{i \in I} H_i = \{1\}$.*

*Důkaz.* Zvolme libovolné $g \in G$, $g \neq 1$. Chceme dokázat, že existuje otevřená normální podgrupa $H \trianglelefteq G$, která neobsahuje $g$. Z totální nesouvislosti $G$ máme obojetnou množinu $U \subseteq G$, která obsahuje 1, ale ne $g$.

Ve zbytku důkazu budeme pro $T \subseteq G$ a $n > 1$ značit

$$T^n = \{t_1 t_2 \dots t_n \mid t_1, \dots, t_n \in T\}, \quad T^{-1} = \{t^{-1} \mid t \in T\}.$$

Uvažme $V = (G \setminus U) \cap U^2$. Protože $U$ je kompaktní, tak je $U \times U$ kompaktní v $G \times G$. Množina $U^2$ je obraz $U \times U$ v zobrazení $(x,y) \mapsto xy$, které je spojité, tedy $U^2$ je též kompaktní. $U$ je otevřená, $G \setminus U$ je uzavřená, tedy kompaktní. Tím pádem je $V$ kompaktní.

Mějme $h \in U$. V zobrazení $(x,y) \mapsto xy$ se $(h,1)$ zobrazí na $h$, což leží v $G \setminus V$. Protože $V$ je kompaktní, tedy i uzavřená, tak je vzor $G \setminus V$ otevřená podmnožina $G \times G$ obsahující $(h,1)$, a tedy obsahuje i $W'_h \times X'_h$, kde $W'_h$ je otevřené okolí

bodu $h$, a $X'_h$ je otevřené okolí bodu 1. Položme $W_h = W'_h \cap U$, $X_h = X'_h \cap U$ a dostáváme $W_h X_h \subseteq (G \setminus V) \cap U^2 \subseteq U$.

Systém $\{W_h \mid h \in U\}$ je otevřené pokrytí $U$, a protože je $U$ uzavřená, tak existují $h_1, \ldots, h_n \in U$ takové, že $\{W_{h_i} \mid i = 1, \ldots, n\}$ je rovněž otevřené pokrytí $U$. Položme $X = \bigcap_{i=1}^n X_{h_i}$ a $Y = X \cap X^{-1}$. Pak $Y$ je otevřené okolí 1 splňující $Y \subseteq U$, a $UY = \bigcup_{i=1}^n W_{h_i} Y \subseteq \bigcup_{i=1}^n W_{h_i} X_{h_i} \subseteq U$. Induktivně platí pro všechna $i \geq 1$, že $UY^i \subseteq U$, tedy $H' = \bigcup_{i=1}^\infty Y^i$ je otevřená podgrupa $G$, a $H' \subseteq U$. Nakonec definujeme $H = \bigcap_{g \in G} g H' g^{-1}$. Protože $H'$ je otevřená, tak má konečný index. $H$ je průnik konečně mnoha otevřených podgrup, a je tudíž sama otevřená, tedy je to podgrupa s požadovanými vlastnostmi.

□

**Věta 16.** *Topologická grupa je profinitní právě tehdy, když je Hausdorffova (jako topologický prostor), kompaktní a totálně nesouvislá.*

*Důkaz.* Z předchozích vět víme, že profinitní grupy mají požadované vlastnosti. Naopak buď $G$ topologická grupa, která je Hausdorffova, kompaktní a totálně nesouvislá. Definujeme grupu $H$ jako projektivní limitu $\varprojlim G/N$, kde $N$ probíhá přes otevřené normální podgrupy $G$. Podle věty 12 mají otevřené podgrupy konečný index, tedy $H$ je profinitní. Dokážeme, že $G \cong H$.

Z univerzální vlastnosti projektivní limity plyne existence přirozeného zobrazení $f : G \to H$. Jak $G$, tak $H$ jsou kompaktní Hausdorffovy prostory. Uzavřené podmnožiny $G$ jsou kompaktní a $f$ je zobrazí na kompaktní, a tedy uzavřené podmnožiny $H$. Stačí dokázat, že $f$ je spojitá bijekce.

V definici $H$ faktorizujeme modulo otevřené podgrupy, tedy sjednocení jejich rozkladových tříd je otevřená množina, a tudíž jsou všechny projekce spojité. Prostota $f$ plyne z Věty 15.

Buď $(g_i G_i)_{i \in I}$ prvek $H$, kde $G_i, i \in I$ jsou otevřené normální podgrupy $G$ a $g_i \in G$. Pak pro každé $i \in I$ je $G_i$, a tedy i $g_i G_i$ je neprázdná uzavřená podmnožina $G$. Chceme dokázat, že $\bigcap_{i \in I} g_i G_i$ je neprázdná. Ať pro spor $\bigcap_{i \in I} g_i G_i = \emptyset$. Pak z kompaktnosti $G$ existují indexy $i_1, \ldots, i_n \in I$ takové, že $\bigcap_{k=1}^n g_{i_k} G_{i_k} = \emptyset$. $G_i, i \in I$ je inverzní systém, takže existuje $i \in I$, $i \geq i_1, \ldots . i_n$, a z definice inverzní limity platí $g_i G_i \subseteq \bigcap_{k=1}^n g_{i_k} G_{i_k} = \emptyset$. Ale $G_i$ je neprázdná, což je spor.

□

Buď $G$ topologická grupa a uvažujme systém

$$\mathcal{N} = \{N \mid N \trianglelefteq G, [G : N] < \infty, N \text{ je otevřená}\},$$

který je částečně uspořádány inkluzí. Navíc, jsou-li $N_1$,$N_2 \trianglelefteq G$ a $[G : N_1], [G : N_2] < \infty$, pak $N_1 \cap N_2 \trianglelefteq G \ \ \& \ \ [G : N_1 \cap N_2] < \infty$. Tedy platí, že $(\mathcal{N}, \subseteq)$ je nahoru usměrněná množina.

Pokud je $G$ obecná grupa bez zadané topologie, tak na $G$ uvažujeme tzv. *profinitní topologii*. To je nejmenší topologie splňující podmínku, že pro každou normální podgrupu $N$ konečného indexu je indukovaná topologie na $G/N$ diskrétní. Báze profinitní topologie je systém rozkladových tříd

$$\{gN \mid g \in G, N \trianglelefteq G, [G : N] < \infty\}.$$

Tím pádem můžeme uvažovat systém $\mathcal{N}$ pro libovolnou grupu $G$.

Původ názvu profinitní topologie v tomto kontextu není nijak záhadný (na rozdíl od názvu eliptických křivek), ale přesto je trochu matoucí. Zdůrazníme tedy, že se nejedná o stejnou topologii, jakou mají profinitní grupy.

Prvky $\{G/N, N \in \mathcal{N}\}$ jsou konečné grupy s diskrétní topologií a přirozená volba homomorfismů splňuje předpoklady inverzního systému.

**Definice 15.** *Inverzní limitu* $\hat{G} = \varprojlim G/N$ *přes všechny podgrupy* $N \in \mathcal{N}$ *značíme* $\hat{G}$ *a říkáme jí* profinitní zúplnění $G$.

Přirozené projekce $G \to G/N$ indukují spojitý homomorfismus $G \to \hat{G}$. Profinitní zúplnění má univerzální vlastnost, což říká následující věta.

**Věta 17.** *Nechť $G$ je libovolná grupa, $H$ profinitní grupa a $f : G \to H$ homomorfismus grup. Označme $\phi : G \to \hat{G}$ přirozený homomorfismus z předchozího odstavce. Pak existuje jednoznačně určený spojitý homomorfismus grup $g : \hat{G} \to H$ takový, že $f = g \circ \phi$.*

**Věta 18.** *Obraz $G$ v homomorfismu $\phi$ je hustá podgrupa $\hat{G}$.*

*Důkaz.* Mějme neprázdnou otevřenou množinu $U \subseteq \hat{G}$. Chceme ukázat, že existuje $g \in G$ takový, že $\phi(g) \in U$. Protože $\hat{G} \subseteq \prod_{N\in\mathcal{N}} G/N$, tak z definice součinové topologie plyne, že $U$ obsahuje neprázdnou podmožinu tvaru $\hat{G} \cap \prod_{N\in\mathcal{N}} U_N$, kde $U_N = G/N$ pro všechny $N \in \mathcal{N}$ až na konečně mnoho výjimek. Tedy můžeme BÚNO předpokládat, že samotná množina $U$ je v tomto tvaru.

Buďte $N_1, \ldots, N_k$ ty prvky $\mathcal{N}$, pro které platí $U_N \neq G/N$. Potom je $N' = N_1 \cap \cdots \cap N_k$ rovněž prvek $\mathcal{N}$. Uvažujme přirozené projekce $G/N' \to G/N_i$, $i = 1, \ldots, k$ a označme $V_1, \ldots, V_k \subseteq G/N'$ vzory $U_{N_i}$ v těchto projekcích. Položme $V = V_1 \cap \cdots \cap V_k$.

Obraz libovolného prvku z $\hat{G} \cap \prod_{n\in\mathcal{N}} U_N$ v $G/H'$ musí z definice inverzní limity ležet ve $V$. A protože je $\hat{G} \cap \prod_{n\in\mathcal{N}} U_N$ neprázdná, tak je neprázdná i $V$. Analogicky zvolme $g$, jehož obraz v $G/H'$ leží ve $V$. Pak $g \in U$, což jsme chtěli. □

Buď $G$ profinitní grupa a $H$ její otevřená podgrupa. $G$ je podle věty 16 kompaktní, a tedy má $H$ podle věty 12 konečný index. Položme $N = \bigcap_{g\in G} g^{-1}Hg$. Pak $N \subseteq H$ a navíc je $N$ normální podgrupa $G$. $G$ je kompaktní, a tedy je $\phi(G)$ také kompaktní. Tím pádem je $\phi(G)$ uzavřená v $\hat{G}$. Tedy, pokud je $G$ profinitní, tak je $\phi(G)$ uzavřená a hustá v $\hat{G}$, tedy $\phi(G) = \hat{G}$ a zobrazení $\phi : G \to \hat{G}$ je na.

Je snadno vidět, že

$$Ker(\phi) = \bigcap\{N \mid N \trianglelefteq G, [G : N] < \infty\},$$

tedy $\phi$ je prosté právě tehdy, když průnik na pravé straně obsahuje jen neutrální prvek grupy $G$. Z vět 15 a 16 plyne, že pro profinitní grupu je $\phi$ prosté. Tím pádem jsme dokázali následující větu.

**Věta 19.** *Buď $G$ profinitní grupa a $\hat{G}$ její profinitní zúplnění. Pak je zobrazení $\phi : G \to \hat{G}$ izomorfismus.*

Zvolme pevné prvočíslo $p$. Uvažme $\mathbb{N}$ jako indexovou množinu s běžným uspořádáním. Pak $(N, \leq)$ je nahoru usměrněná. Pro $i \in \mathbb{N}$ budeme uvažovat okruh $\mathbb{Z}/p^i\mathbb{Z}$. Je-li $i \leq j$, pak chceme definovat homomorfismus $\varphi_{i,j} : \mathbb{Z}/p^j\mathbb{Z} \to \mathbb{Z}/p^i\mathbb{Z}$. Pro $a \in \mathbb{Z}$ definujme $\varphi_{i,j}(a \mod p^j) = a \mod p^i$. Snadno ověříme, že se jedná o okruhový homomorfismus splňující podmínky v definici inverzního systému. Jeho inverzní limita je okruh $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^i\mathbb{Z}$, který se nazývá okruh celých $p$-adických čísel.

Relace dělitelnosti na $\mathbb{N}$ je uspořádání. Zřejmě $(\mathbb{N}, |)$ je nahoru usměrněná množina. Pro $m,n \in \mathbb{N}$ takové, že $m \mid n$, je zobrazení $\varphi_{m,n} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, definované předpisem $\varphi_{m,n}(a \mod n) = a \mod m$, okruhový homomorfismus. Opět se jedná o inverzní systém, tentokrát s inverzní limitou $\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$. Lze ukázat, že $\hat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p$, kde $p$ jde přes všechna prvočísla.

Buď $L \supset K$ Galoisovo rozšíření těles, tj. $L$ je algebraické normální a separabilní rozšíření $K$. Položme

$$\mathcal{F} = \{F \text{ těleso} \mid K \subseteq F \subseteq L, F \supset K \text{ je Galoisovo rozšíření konečného stupně}\}.$$

Pro každé $F \in \mathcal{F}$ je $\mathrm{Gal}(F/K)$ konečná grupa a můžeme na ni uvažovat diskrétní topologii. Platí, že $(\mathcal{F}, \subseteq)$ je nahoru usměrněná množina, kde horní závora prvků $F_1, F_2 \in \mathcal{F}$ je těleso $F_1F_2$. Mějme $F_1 \subseteq F_2$. $K$-automorfismy z $\mathrm{Gal}(F_2/K)$ můžeme zúžit na $F_1$ a tak dostáváme homomorfismus grup $\mathrm{Gal}(F_2/K) \to \mathrm{Gal}(F_1/K)$. Rozšíření tedy tvoří inverzní systém indexovaný množinou $\mathcal{F}$, a tedy můžeme vzít inverzní limitu $\varprojlim \mathrm{Gal}(F/K)$. Lze dokázat přímo, že $\mathrm{Gal}(L/K) \cong \varprojlim \mathrm{Gal}(F/K)$. Speciální případ této konstrukce je grupa $\mathrm{Gal}(\overline{\mathbb{Q}},\mathbb{Q})$.

**Věta 20.** *(Krull) Buď $L \supset K$ Galoisovo rozšíření a označme $G = \mathrm{Gal}(L/K)$. Buď $[L : K]$ svaz všech těles $F$ takových, že $K \subseteq F \subseteq L$ a $[G : 1]$ svaz uzavřených podgrup $G$. Pro $F \in [L : K]$ definujeme $\Phi(F) = \mathrm{Gal}(N/F)$. Pak $\Phi$ je antiizomorfismus svazů $[L : K]$ a $[G : 1]$.*

*Důkaz.* Ribes (2013) (Věta 1.8)

□

**Věta 21.** *(Leptin) Buď $G$ profinitní grupa. Pak existuje Galoisovo rozšíření těles $L \supset K$ takové, že $G = \mathrm{Gal}(L/K)$.*

*Důkaz.* Buď $F$ libovolné těleso. Položme $T$ jako disjunktní sjednocení množin $G/U$, kde $U$ probíhá přes všechny normální otevřené podgrupy $G$. Definujeme těleso $L$ jako $L = F(T)$, tedy těleso všech lomených polynomiálních funkcí s koeficienty z $F$ a proměnnými z $T$. Grupa $G$ působí na $T$ následujícím způsobem: je-li $g \in G$ a $g'U \in G/U$, pak $g(g'U) = gg'U$, což indukuje akci $G$ na $L$. Položme $K = L^G = \{l \in L \mid g(l) = l \ \forall g \in G\}$, což je podtěleso $L$. Dokážeme, že $L \supset K$ je Galoisovo rozšíření s Galoisovou grupou $G$.

Pro $l \in L$ označme $G_l = \{g \in G \mid g(l) = l\} \leq G$ a označme $t_i \in G/U_i$, $i = 1, \ldots, n$ proměnné ve vyjádření prvku $l$. Pak $\bigcap_{i=1}^n U_i \subseteq G_l$.

$G_l$ je otevřená podgrupa $G$, a tedy má konečný index. Tím pádem má orbita prvku $l$ v akci grupy $G$ konečně mnoho prvků. Označme je $\{l = l_1, \ldots, l_r\}$. Uvažme polynom $f(X) = \prod_{i=1}^r (X - l_i)$. Akce $G$ tento polynom zobrazí sám na sebe, takže

$f \in K[X]$. Tedy je $l$ algebraický nad $K$. Navíc má $f$ jen jednoduché kořeny, tudíž je $l$ separabilní nad $K$. Rozšíření $K(l_1, \ldots, l_r) \supset K$ je navíc normální. Tudíž je $L$ sjednocení normálních rozšíření nad $K$, a tedy je $L \supset K$ normální. Dostáváme, že $L \supset K$ je Galoisovo rozšíření.

Označme $H = \mathrm{Gal}(L/K)$. Zřejmě platí $G \leq H$. Zbývá dokázat, že $G = H$. Buď $U$ normální otevřená podgrupa $H$ a $L^U$ ty prvky tělesa $L$, které jsou pevné body všech zobrazení z $U$. Pak $L^U \supset K$ je podle Krullovy věty (Věta 20) konečné Galoisovo rozšíření, označme ho $L^U = K(l'_1, \ldots, l'_s)$, kde $l'_1, \ldots, l'_s \in L$. Pak $\bigcap_{i=1}^{s} G_{l'_i} \subseteq G \cap U$, tedy $G \cap U$ je otevřená v $G$. Tím pádem je inkluze $G \to H$ spojitá a $G$ je uzavřená podgrupa $H$. Protože $G$ a $H$ fixují stejné prvky, tak z Věty 20 plyne $G = H$.

□

# 3. Tateova-Šafarevičova grupa

## 3.1 Abstraktní nonsens

**Definice 16.** *Buď $M$ aditivní abelovská grupa a $G$ libovolná grupa. Řekneme, že $M$ je $G$-*modul*, pokud $G$ působí na $M$, tj. každému $g \in G$ přísluší automorfismus $g : M \to M$, a navíc pro všechna $m \in M$ a $g_1, g_2 \in G$ platí $(g_1 g_2)(m) = g_1(g_2(m))$. Pokud pro každé $g \in G$ je akce prvku $g$ identické zobrazení na $M$, tak řekneme, že akce je triviální.*

Působení $G$ na $M$ můžeme také chápat jako zobrazení $G \times M \to M$ definované vztahem $(g,m) \mapsto g(m)$. Máme-li na $G$ a $M$ zadané topologie, tak požadujeme, aby toto zobrazení bylo spojité vzhledem k topologii na $M$ a součinové topologii na $G \times M$.

Buď $L \supset K$ Galoisovo rozšíření těles a $E$ eliptická křivka definovaná nad $K$. Označme $G = \mathrm{Gal}(L/K)$. Pak $E(L)$ je $G$-modul, kde působení grupou $G$ na $L$ je definované očividně.

**Definice 17.** *Buďte $M_1, M_2$ $G$-moduly. Pokud je $\phi : M_1 \to M_2$ homomorfismus abelovských grup a zachovává akci grupy $G$, tj. pro všechna $g \in G$ a $m_1 \in M_1$ splňuje $\phi(gm_1) = g\phi(m_1)$, tak řekneme, že $\phi$ je* homomorfismus $G$-modulů.

Pro grupu $G$ a $G$-modul $M$ definujeme množinu sestávající z pevných bodů

$$M^G = \{m \in M \mid gm = m \text{ pro všechna } g \in G\}.$$

Pak je z definice snadno vidět, že $M^G$ je podmodul $M$.

**Definice 18.** *Mějme posloupnost $G$-modulů a jejich homomorfismů*

$$\cdots \to M_{n-1} \xrightarrow{\phi_n} M_n \xrightarrow{\phi_{n+1}} M_{n+1} \to \ldots$$

*Řekneme, že posloupnost je* exaktní v $M_n$*, pokud* $\mathrm{Ker}(\phi_{n+1}) = \mathrm{Im}(\phi_n)$*. Posloupnost je* exaktní*, pokud je exaktní všude.*

**Definice 19.** Krátkou exaktní posloupností *rozumíme exaktní posloupnost tvaru*

$$0 \to M_1 \to M_2 \to M_3 \to 0.$$

Až na izomorfismus tato situace nastává právě tehdy, když $M_1 \subseteq M_2$ a $M_3 = M_2/M_1$.

Definujeme nultou kohomologickou grupu následovně: $H^0(G,M) = M^G = \{m \in M \mid gm = m \text{ pro všechna } g \in G\}$. Pokud $G$ působí triviálně, tak $H^0(G,M) = M$. Ve druhém uvedeném příkladě platí $H^0(\mathrm{Gal}(L/K),E(L)) = E(K)$.

**Definice 20.** *Mějme $G$-modul $M$ a zobrazení $f : G \to M$. Řekneme, že $f$ je* zkřížený homomorfismus*, pokud pro všechna $g_1, g_2 \in G$ platí*

$$f(g_1 g_2) = f(g_1) + g_1 f(g_2).$$

*Definujeme pro libovolné $m \in M$ zkřížený homomorfismus $f_m : G \to M$ předpisem*

$$f_m(g) = gm - m.$$

*Zkřížené homomorfismy v tomto tvaru nazýváme* hlavní.

Množinu všech zkřížených homomorfismů $f : G \to M$ označíme $Z(G,M)$, a pokud je na grupách $G$ a $M$ zadaná topologie, tak navíc chceme, aby tato zobrazení byla spojitá. V kontextu kohomologie nazýváme prvky $Z(G,M)$ též kocykly. Zkřížené homomorfismy tvoří aditivní grupu a v případě triviálního působení $G$ platí $Z(G,M) = \mathrm{Hom}(G,M)$.

Množinu všech hlavních zkřížených homomorfismů označíme $B(G,M) = \{f_m \mid m \in M\}$. Prvkům $B(G,M)$ se také říká kohranice.

Definujeme první kohomologickou grupu $H^1(G,M) = Z(G,M)/B(G,M)$. Pokud $G$ působí triviálně, tak pro všechny $g \in G$ a $m \in M$ platí $gm - m = 0$, tedy $B(G,M) = 0$ a $H^1(G,M) = \mathrm{Hom}(G,M)$ je množina grupových homomorfismů z $G$ do $M$.

Kohomologické grupy se dají definovat obecně pro každé $n \in \mathbb{N}$. (Rotman, 2009) Nám budou stačit jen nultá a první.

Buď $\phi : M_1 \to M_2$ homomorfismus $G-$modulů. Pak zúžení $\phi|_{M_1^G}$ je zobrazení kohomologických grup $H^0(G,M_1) \to H^0(G,M_2)$. Vezmeme-li prvek $f \in Z$, pak $\phi_*$ definované předpisem $(\phi_*(f))(g) = \phi(f(g))$ je zobrazení kohomologických grup $H^1(G,M_1) \to H^1(G,M_2)$.

**Věta 22.** *Krátká exaktní posloupnost $G-$modulů $0 \to M_1 \to M_2 \to M_3 \to 0$ indukuje dlouhou exaktní posloupnost kohomologických grup*

$$0 \to H^0(G,M_1) \to H^0(G,M_2) \to H^0(G,M_3) \xrightarrow{\delta}$$
$$\xrightarrow{\delta} H^1(G,M_1) \to H^1(G,M_2) \to H^1(G,M_3).$$

*Důkaz.* Buď $m_3 \in M_3^G$. Existuje $m_2 \in M_2$ takové, že se zobrazí na $m_3$ a pro každé $g \in G$ splňuje $gm_2 - m_2 \in M_1$. Zobrazení $G \to M_1$ dané vztahem $g \mapsto gm_2 - m_2$ je zkřížený homomorfismus a definujeme $\delta(m_3)$ jako třídu ekvivalence $H^1(G,M_1)$ příslušející tomuto zobrazení.

Máme li jiný prvek $m_2' \in M_2$, který se zobrazí na $m_3$, tak se příslušný zkřížený homomorfismus liší od původního o hlavní zkřížený homomorfismus $g \mapsto g(m_2' - m_2) - (m_2' - m_2)$, tedy je $\delta$ dobře definované.

Zbytek důkazu je základní kohomologie.

□

**Věta 23.** *Buď $E$ eliptická křivka a $\alpha \neq 0$ endomorfismus na $E$.Pak $\alpha : E(\overline{K}) \to E(\overline{K})$ je na.*

*Důkaz.* Washington (2008) (Věta 2.22)

□

Položíme-li v předchozí větě $K = \mathbb{Q}$ a uvážíme-li $\alpha$ jako násobení přirozeným číslem $n$, dostaneme krátkou exaktní posloupnost

$$0 \to E[n] \to E(\overline{\mathbb{Q}}) \xrightarrow{n} E(\overline{\mathbb{Q}}) \to 0. \tag{3.1}$$

Položme $G = Gal(\overline{\mathbb{Q}},\mathbb{Q})$. Z druhé kapitoly víme, že je profinitní. Platí

$$H^0(G,E(\overline{\mathbb{Q}})) = E(\overline{\mathbb{Q}})^G = E(\mathbb{Q}).$$

Na grupě $E(\overline{\mathbb{Q}})$ budeme uvažovat diskrétní topologii. Použijeme větu 22 na krátkou exaktní posloupnost z předchozího odstavce a dostaneme exaktní posloupnost

$$0 \to E(\mathbb{Q})[n] \to E(\mathbb{Q}) \xrightarrow{n} E(\mathbb{Q}) \to H^1(G,E[n]) \to H^1(G,E(\overline{\mathbb{Q}})) \xrightarrow{n} H^1(G,E(\overline{\mathbb{Q}})), \tag{3.2}$$

která indukuje krátkou exaktní posloupnost

$$0 \to E(\mathbb{Q})/nE(\mathbb{Q}) \to H^1(G,E[n]) \to H^1(G,E(\overline{\mathbb{Q}}))[n] \to 0. \tag{3.3}$$

Tuto posloupnost nazýváme *Kummerova*.

Totéž platí i v případě, že uvážíme $E$ jako křivku nad $p$-adickými čísly. Reálná čísla budeme značit $\mathbb{Q}_\infty$, a pokud něco platí pro reálná čísla a $p$-adická čísla pro všechna prvočísla $p$, řekneme, že to platí pro $\mathbb{Q}_p$ pro všechna $p \leq \infty$. Dále budeme značit $G_p = \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$. V tomto případě dostáváme krátkou exaktní posloupnost

$$0 \to E(\mathbb{Q}_p)/nE(\mathbb{Q}_p) \to H^1(G_p,E[n]) \to H^1(G_p,E(\overline{\mathbb{Q}_p}))[n] \to 0. \tag{3.4}$$

Vnoření $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ se dá rozšířit na vnoření $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}_p}$. Tedy grupa $G_p$ působí na $\overline{\mathbb{Q}}$ a toto působení definuje homomorfismus $G_p \to G$. Máme-li zkřížený homomorfismus $G \to E(\overline{\mathbb{Q}})$, tak složením s homomorfismem $G_p \to G$ dostaneme zkřížený homomorfismus $G_p \to E(\overline{\mathbb{Q}_p})$. Tím pádem dostáváme homomorfismus grup $H^1(G,E(\overline{\mathbb{Q}})) \to H^1(G_p,E(\overline{\mathbb{Q}_p}))$.

**Definice 21.** *Pro $n \in \mathbb{N}$ definujeme* Selmerovu $n$-grupu *jako*

$$S_n(E/\mathbb{Q}) = \mathrm{Ker}\left(H^1(G,E[n]) \to \prod_{p\leq\infty} H^1(G_p,E(\overline{\mathbb{Q}_p}))\right)$$

*a* Tateovu-Šafarevičovu grupu *jako*

$$Ш(E/\mathbb{Q}) = \mathrm{Ker}\left(H^1(G,E(\overline{\mathbb{Q}})) \to \prod_{p\leq\infty} H^1(G_p,E(\overline{\mathbb{Q}_p}))\right).$$

Je triviální ověřit, že když jsou $A,B,C$ $G$-moduly (abelovské grupy, okruhy) a $\alpha : A \to B$, $\beta : B \to C$ homomorfismy, tak je následující posloupnost exaktní

$$\begin{aligned} 0 \to \mathrm{Ker}(\alpha) \to \mathrm{Ker}(\beta\circ\alpha) \xrightarrow{\alpha} \mathrm{Ker}(\beta) \to \\ \to \mathrm{Coker}(\alpha) \to \mathrm{Coker}(\beta\circ\alpha) \xrightarrow{\alpha} \mathrm{Coker}(\beta) \to 0. \end{aligned}$$

Použijeme to na zobrazení $H^1(G,E[n]) \to H^1(G,E(\overline{\mathbb{Q}}))[n]$ a $H^1(G,E(\overline{\mathbb{Q}}))[n] \to \prod_{p\leq\infty} H^1(G_p,E(\overline{\mathbb{Q}_p}))[n]$ a máme krátkou exaktní posloupnost

$$0 \to E(\mathbb{Q})/nE(\mathbb{Q}) \to S_n(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[n] \to 0. \tag{3.5}$$

Není těžké uvěřit, že definice obou grup jsou korektní a že exaktnost posloupnosti (3.5) je důležitá, mimo jiné třeba proto, že by konečnost grupy $S_n(E/\mathbb{Q})$ implikovala slabou Mordellovu-Weilovu větu. Později se přesvědčíme, že je Selmerova grupa opravdu konečná. Teď by nás ale zajímalo, jak vypadají jejich prvky, a to zejména v případě Tateovy-Šafarevičovy grupy.

## 3.2 2-sestup

Budeme řešit zdánlivě nesouvisející problém. Buďte $e_1, e_2, e_3$ po dvou různá celá čísla a nechť $E$ je eliptická křivka zadaná rovnicí $y^2 = (x-e_1)(x-e_2)(x-e_3)$. Chceme hledat racionální body $(x,y)$ na křivce $E$. Pokud $e_1, e_2, e_3 \in \mathbb{Q}$, tak lze změnou souřadnic převést rovnici na tvar, kde jsou $e_1$,$e_2$,$e_3$ celá čísla, takže tento případ uvažovat nebudeme.

Protože součin $\prod_{i=1}^{3}(x-e_i)$ je čtverec, tak by intuitivně měl každý činitel být „blízko čtverci“, což zapíšeme jako

$$x - e_1 = au^2 \tag{3.6}$$
$$x - e_2 = bv^2 \tag{3.7}$$
$$x - e_3 = cw^2, \tag{3.8}$$

kde $a$,$b$,$c$,$u$,$v$,$w \in \mathbb{Q}$. Pak $y^2 = abc(uvw)^2$, tedy $abc$ je čtverec. Vhodnou volbou $u$,$v$,$w$ lze docílit toho, že $a$, $b$, $c$ jsou bezčtvercová celá čísla. Odečtením rovnic (3.6) dostaneme

$$au^2 - bv^2 = e_2 - e_1$$
$$au^2 - cw^2 = e_3 - e_1.$$

Což jsou dvě kvadriky přesně v tom tvaru, jaké jsme uvažovali v sekci 1.3. Tedy jejich průnikem je eliptická křivka $C_{a,b,c}$, která je izomorfní původní křivce $E$. Tím pádem se původní problém redukuje na hledání racionálních bodů na křivce $C_{a,b,c}$.

Uvažujme zápis čísla $x$ jako zlomku v desítkové soustavě. Je-li délka čitatele i jmenovatele seshora omezena hodnotou $N \in \mathbb{N}$, tak z rovnic (3.6) plyne, že čitatele a jmenovatele čísel $u$,$v$,$w$ by měly být omezeny přibližně hodnotou $N/2$.

Protože hledáme menší řešení, tak Fermat tuto metodu pojmenoval sestup. Používal ho ve dvou podobách. První je, že z existence řešení nějaké rovnice vyvodil existenci menších řešení příbuzné rovnice a tak postupoval dál, dokud nenalezl dostatečně malá řešení, aby mohl ručně ověřit všechny možnosti. Druhá podoba je, že k nějakému řešení nalezl menší řešení téže rovnice. Z toho by ale plynulo, že existuje nekonečná ostře klesající posloupnost přirozených čísel, což je spor s principem dobrého uspořádání. Tedy původní rovnice neměla řešení. Tímto způsobem dokázal Fermat svoji velkou větu v případě $n = 4$. V současné době se tato metoda používá v jiné formě. Hledáme isogenie křivek a menším bodem rozumíme bod s menší výškou $h$.

Vraťme se k původnímu problému. Hledáme trojice $(a,b,c)$ takové, že na křivce $C_{a,b,c}$ leží alespoň jeden bod s racionálními souřadnicemi. K tomu nám pomůže následující věta.

**Věta 24.** *Buď $E$ křivka zadaná rovnicí $y^2 = (x-e_1)(x-e_2)(x-e_3)$, $e_1, e_2, e_3 \in \mathbb{Z}$. Zobrazení*

$$\phi : E(\mathbb{Q}) \to (\mathbb{Q}^*/(\mathbb{Q}^*)^2) \oplus (\mathbb{Q}^*/(\mathbb{Q}^*)^2) \oplus (\mathbb{Q}^*/(\mathbb{Q}^*)^2)$$

*zadané jako*

$$(x,y) \mapsto (x-e_1, x-e_2, x-e_3) \ \textit{když}\ y \neq 0,$$
$$(e_1, 0) \mapsto ((e_1-e_2)(e_1-e_3), e_1-e_2, e_1-e_3),$$

$$(e_2,0) \mapsto (e_2 - e_1, (e_2 - e_1)(e_2 - e_3), e_2 - e_3),$$
$$(e_3,0) \mapsto (e_3 - e_1, e_3 - e_2, (e_3 - e_1)(e_3 - e_2)),$$
$$\infty \mapsto (1,1,1),$$

*je homomorfismus a platí* $\mathrm{Ker}(\phi) = 2E(\mathbb{Q})$.

*Důkaz.* (Washington, 2008)(Věta 8.14)

□

Všimneme si, že dvě nenulová racionální čísla $x_1, x_2$ patří do stejné třídy ekvivalence v $\mathbb{Q}^*/(\mathbb{Q}^*)^2$, pokud je $x_1/x_2$ druhá mocnina racionálního čísla. Z rovnice (3.6) je vidět, že $x - e_1$ je ekvivalentní $a$ modulo $(\mathbb{Q}^*)^2$. Tedy pokud je $(x, y) \in E(\mathbb{Q})$ a není řádu 2, tak zobrazení $\phi$ tento bod pošle na hledanou trojici $(a, b, c)$. Navíc je hledaných trojic jenom konečně mnoho, což říká následující věta.

**Věta 25.** *Položme*

$$S = \{p \mid p \text{ je prvočíslo a } p|(e_1 - e_2)(e_1 - e_3)(e_2 - e_3)\}.$$

*Pokud je $p$ prvočíslo a $p|abc$, pak $p \in S$.*

*Důkaz.* (Washington, 2008)(Věta 8.13)

□

Tedy zobrazení $\phi$ z Věty 24 indukuje prostý homomorfismus

$$E(\mathbb{Q})/2E(\mathbb{Q}) \hookrightarrow (\mathbb{Q}^*/(\mathbb{Q}^*)^2) \oplus (\mathbb{Q}^*/(\mathbb{Q}^*)^2) \oplus (\mathbb{Q}^*/(\mathbb{Q}^*)^2).$$

Jsou-li $a, b, c$ bezčtvercová celá čísla, tak z Věty 25 plyne, že pokud $(a, b, c)$ leží v obrazu $\phi$, tak čísla $a, b, c$ jsou součiny prvočísel z množiny $S$. Protože $S$ je konečná, tak je modulo $(\mathbb{Q}^*)^2$ jen konečně mnoho takových čísel $a, b, c$. Tedy je obraz $\phi$ konečná množina. Což dokazuje slabou Mordellovu-Weilovu větu (Věta 6) pro $K = \mathbb{Q}$ a $m = 2$.

Uvažujme množinu $S_2 \subseteq (\mathbb{Q}^*/(\mathbb{Q}^*)^2) \oplus (\mathbb{Q}^*/(\mathbb{Q}^*)^2) \oplus (\mathbb{Q}^*/(\mathbb{Q}^*)^2)$ všech trojic $(a, b, c)$ takových, že $C_{a,b,c}$ obsahuje $p$-adický bod pro všechna $p \leq \infty$. Trojice $(a, b, c)$ takové, že $C_{a,b,c}$ má racionální bod, určitě patří do $S_2$. Tedy opět zobrazení $\phi$ z věty 24 indukuje prostý homomorfismus

$$\phi : E(\mathbb{Q})/2E(\mathbb{Q}) \hookrightarrow S_2.$$

Pokud definujeme $Ш_2 = S_2/\mathrm{Im}(\phi)$, tak vidíme, že prvky $Ш_2$ odpovídají takovým trojicím $(a, b, c)$, že $C_{a,b,c}$ má $p$-adický bod pro všechna $p \leq \infty$, ale nemá racionální bod.

Je ihned vidět, že posloupnost

$$0 \to E(\mathbb{Q})/2E(\mathbb{Q}) \to S_2 \to Ш_2 \to 0 \tag{3.9}$$

je exaktní a silně připomíná posloupnost (3.5) pro $n = 2$. To není náhoda, a proto zbytek kapitoly věnujeme vysvětlení, jak souvisí kohomologie s hledáním racionálních bodů na křivce. Toho dosáhneme tak, že popíšeme prvky $H^1(G,E(\overline{\mathbb{Q}}))$.

**Definice 22.** *Buď $E$ eliptická křivka nad tělesem $K$.* Homogenním prostorem *křivky $E$ rozumíme dvojici $(C, \mu)$, kde $C$ je hladká křivka nad $K$ a $\mu : C \times E(K) \to C$ je racionální zobrazení definované ve všech bodech, které splňuje*

- $\forall p \in C \quad \mu(p, \mathcal{O}) = p,$
- $\forall p \in C \quad \forall P,Q \in E(K) \quad \mu(\mu(p, P), Q) = \mu(p, P + Q),$
- $\forall p,q \in C \quad \exists! P \in E(K) \quad \mu(p, P) = q.$

Místo $\mu(p, P)$ budeme psát $p + P$. Z kontextu bude jasné, jestli + znamená grupovou operaci na $E(K)$, nebo akci $E(K)$ na $C$.

Můžeme definovat zobrazení $\nu : C \times C \to E(K)$. Jsou-li $p,q \in E$, tak definujeme $\nu(q,p)$ jako ten jednoznačně určený prvek $P \in E(K)$ splňující $\mu(p,P) = q$ a budeme ho značit $\nu(q,p) = q - p$.

**Lemma 26.** *Buď $C$ homogenní prostor křivky $E$ nad $K$. Pak pro všechna $p,q \in C$ a $P,Q \in E(K)$ platí*

- $p + \mathcal{O} = p, \quad p - p = \mathcal{O},$
- $p + (q - p) = p, \quad (p + P) - p = P,$
- $(q + Q) - (p + P) = (q - p) + Q - P.$

*Důkaz.* (Silverman, 2009)(Sekce X.3, Lemma 3.1)

□

**Věta 27.** *Buď $E$ eliptická křivka nad $K$ a $C$ homogenní prostor křivky $E$. Zvolme $p_0 \in C$ a definujme zobrazení $\theta : E(K) \to C$ předpisem $\theta(P) = p_0 + P$. Potom platí*

- $\theta$ *je izomorfismus,*
- $\forall p \in C \quad \forall P \in E(K) \quad p + P = \theta(\theta^{-1}(p) + P),$
- $\forall p,q \in C \quad q - p = \theta^{-1}(q) - \theta^{-1}(p).$

*Důkaz.* (Silverman, 2009)(Sekce X.3, Tvrzení 3.2)

□

**Definice 23.** *Řekneme, že homogenní prostory $C$ a $C'$ křivky $E$ nad $K$ jsou* ekvivalentní*, pokud existuje izomorfismus $\theta : C \to C'$ takový, že pro všechna $p \in C$ a $P \in E(K)$ platí $\theta(p + P) = \theta(p) + P$. Třídu ekvivalence, která obsahuje $E$, nazýváme* triviální*. Později uvidíme, že třídy ekvivalentních homogenních prostorů tvoří grupu. Tu nazýváme* Weilova-Châteletova *a značíme ji $WC(E/K)$.*

**Věta 28.** *Buď $C$ homogenní prostor křivky $E$ nad $K$. Potom $C$ patří do triviální třídy právě tehdy, když obsahuje alespoň jeden bod se souřadnicemi v $K$.*

*Důkaz.* (Silverman, 2009)(Sekce X.3, Tvrzení 3.3)

□

**Věta 29.** *Buď $E$ eliptická křivka nad $K$. Pak existuje bijekce $WC(E/K) \to H^1(\mathrm{Gal}(\overline{K}/K), E(K))$ definovaná následovně. Buď $C$ homogenní prostor $E$ a zvolme $p_0 \in C$. Příslušné třídy ekvivalence značíme hranatými závorkami a definujeme $[C] \mapsto [g \mapsto g(p_0) - p_0]$, kde $g \in \mathrm{Gal}(\overline{K}/K)$.*

*Důkaz.* (Silverman, 2009)(Sekce X.3, Tvrzení 3.6)

□

Tedy vidíme, že $WC(E/K)$ je doopravdy grupa. Navíc můžeme přepsat definice obou dvou grup z předchozí části.

$$S_n(E/\mathbb{Q}) = \mathrm{Ker}\left(H^1(G,E[n]) \to \prod_{p\leq\infty} WC(E/\mathbb{Q}_p)\right)$$

$$Ш(E/\mathbb{Q}) = \mathrm{Ker}\left(WC(E/\mathbb{Q}) \to \prod_{p\leq\infty} WC(E/\mathbb{Q}_p)\right)$$

Tím pádem je $Ш(E/\mathbb{Q})$ podgrupa $WC(E/\mathbb{Q})$. Tedy podle věty 28 prvky $Ш(E/\mathbb{Q})$ odpovídají třídám ekvivalence homogenních prostorů $E$, které obsahují $p$-adický bod pro každé $p \leq \infty$, a netriviální prvky navíc zároveň neobsahují žádný racionální bod. Takže v jistém smyslu grupa $Ш(E/\mathbb{Q})$ měří, jak moc křivka $E$ porušuje Hasseho-Minkowského princip.

Tate a Šafarevič se domnívali, že je $Ш(E/\mathbb{Q})$ konečná. V plné obecnosti je to dosud otevřený problém, ale v příští kapitole uvidíme, že v některých speciálních případech byla tato domněnka potvrzená.

**Věta 30.** *Buď $E$ eliptická křivka nad $\mathbb{Q}$ a nechť $n$ je libovolné přirozené číslo. Pak je $S_n(E/\mathbb{Q})$ konečná.*

*Důkaz.* (Milne, 2006) věnuje důkazu sekci IV.3. V obecnější podobě tuto větu uvádí (Silverman, 2009) (Sekce X.4, Věta 4.2(b)).

□

Následující důsledek okamžitě plyne z toho, že posloupnost (3.5) je exaktní.

*Důsledek.* Pro libovolnou eliptickou křivku $E$ nad $\mathbb{Q}$ a libovolné přirozené číslo $n$ jsou grupy $E(\mathbb{Q})/nE(\mathbb{Q})$ a $Ш(E/\mathbb{Q})[n]$ konečné.

Chtěli bychom nahlédnout, jak spolu souvisejí exaktní posloupnosti (3.5) a (3.9). Tedy znovu uvažujeme eliptickou křivku $E$ definovanou rovnicí $y^2 = (x - e_1)(x - e_2)(x - e_3)$, kde $e_1, e_2, e_3$ jsou po dvou různá celá čísla. Pak pro libovolná racionální čísla $a_1, a_2, a_3$, jejichž součin je čtverec, máme křivku $C_{a_1,a_2,a_3}$ v proměnných $v_1, v_2, v_3$. Ta je definovaná jako průnik kvadrik $a_1v_1^2 - a_jv_j^2 = e_j - e_1$, kde $i \in \{2, 3\}$. Předtím jsme tuto křivku značili $C_{a,b,c}$, ale kvůli přehlednosti značení to teď pozměníme.

Zvolme racionální číslo $d$, které splňuje $d^2 = a_1a_2a_3$ (tzn. zvolíme znaménko). Tedy existuje racionální zobrazení $\psi : C_{a_1,a_2,a_3} \to E(\overline{\mathbb{Q}})$ dané předpisem

$$\psi(v_1, v_2, v_3) = (a_i v_i^2 + e_i, dv_1v_2v_3),$$

které nezávisí na volbě $i \in \{1, 2, 3\}$.

Zobrazení $\psi$ není bijekce. Když dvěma souřadnicím bodu $(v_1, v_2, v_3)$ změníme znaménko, tak ho $\psi$ zobrazí na stejný bod $E$ jako ten původní. Tedy „typický“ bod na $E$ má čtyři vzory v zobrazení $\psi$. Stejnou vlastnost má i násobení dvěma, tedy zobrazení $[2] : E(\overline{\mathbb{Q}}) \to E(\overline{\mathbb{Q}})$, $P \mapsto 2P$.

To plyne z toho, že $E[2]$ obsahuje 4 prvky: kromě $\mathcal{O}$ ještě řešení rovnice (1.1) pro $y = 0$. Protože $E[n]$ uvažujeme se souřadnicemi v $\overline{K}$ a křivka je z definice nesingulární, tak jsou kořeny vždycky tři různé.

Bylo by krásné, kdyby existoval izomorfismus $\varphi : C_{a_1,a_2,a_3} \to E(\overline{\mathbb{Q}})$ takový, že $[2] \circ \varphi = \psi$. Takové $\varphi$ skutečně existuje. Washington ho konstruuje v důkazu Věty 8.14 (v našem číslování jde o Větu 24).

Definujeme $\mu : C_{a_1,a_2,a_3} \times E(\overline{\mathbb{Q}}) \to C_{a_1,a_2,a_3}$ předpisem $\mu(p,P) = \varphi^{-1}(\varphi(p)+P)$. Lze snadno ověřit, že $\mu$ splňuje axiomy v definici 22. Tím pádem je $(C_{a_1,a_2,a_3}, \mu)$ homogenní prostor křivky $E$.

Tedy podle Věty 29 existuje jednoznačně určený kocyklus z $H^1(G,E(\mathbb{Q}))$ příslušející křivce $C_{a_1,a_2,a_3}$, respektive přímo trojici $(a_1, a_2, a_3) \in (\mathbb{Q}^*/(\mathbb{Q}^*)^2) \oplus (\mathbb{Q}^*/(\mathbb{Q}^*)^2) \oplus (\mathbb{Q}^*/(\mathbb{Q}^*)^2)$. Lze ukázat, že příslušný kocyklus má obraz v $E[2]$, tedy je to prvek $H^1(G, E[2])$.

Ztotožnili jsme prvky $(\mathbb{Q}^*/(\mathbb{Q}^*)^2) \oplus (\mathbb{Q}^*/(\mathbb{Q}^*)^2) \oplus (\mathbb{Q}^*/(\mathbb{Q}^*)^2)$ splňující, že součin souřadnic je čtverec s prvky $H^1(G, E[2])$. Odtud už ihned plyne, že existuje bijekce mezi prvky $S_2$ tak, jak jsme ji definovali v této sekci, tj.

$$S_2 = \{(a_1, a_2, a_3) \mid C_{a_1,a_2,a_3} \text{ má } p\text{-adický bod pro všechna } p \leq \infty\},$$

a prvky Selmerovy 2-grupy. Tedy tyto grupy jsou izomorfní. Z exaktnosti posloupností (3.5) a (3.9) plyne, že jsou izomorfní i $Ш_2 = S_2/\operatorname{Im}(\phi)$ s $Ш(E/\mathbb{Q})[2]$.

# 4. Birchova-Swinnerton-Dyerova domněnka

V této kapitole se vrátíme k problému, který jsme zmínili v sekci 1.5 – hledání ranku eliptické křivky. Dosud neexistuje žádný obecný algoritmus na určení ranku, ale jsou heuristiky, které usnadňují ho spočítat v konkrétních případech. Milne uvádí obecný algoritmus, který ale předpokládá konečnost Tateovy-Šafarevičovy grupy.

Zvolíme-li nazdařbůh nějakou eliptickou křivku, tak bude její rank dost malý. Bhargava a Shankar dokázali, že průměrný rank všech eliptických křivek definovaných nad $\mathbb{Q}$ je nanejvýš 3/2. Tento výsledek byl od té doby ještě zpřesněn. V současné době je velice oblíbená domněnka, že průměrný rank je přesně roven 1/2. Přesto se spousta expertů domnívá, že rank není nijak shora omezen, a matematici se věnují hledání křivek s co největším rankem. Současný držitel rekordu je Noam Elkies, jenž našel křivku definovanou rovnicí

$$\begin{aligned} y^2 + xy + y = x^3 - x^2 \\ - 20067762415575526585033208209338542750930230312178956502x \\ + 3448161179503055646703298569039072037485594435931918036126600829629193944873224342 9, \end{aligned}$$

pro kterou platí $r \geq 28$. Tuto rovnici lze převést do Weierstrassova tvaru jen za cenu zvětšení hodnot koeficientů.

Je-li $p$ prvočíslo, tak je $\mathbb{Z}/p\mathbb{Z}$ těleso, které budeme značit $\mathbb{F}_p$. Navíc budeme v této kapitole značit $\#G$ počet prvků konečné grupy (nebo konečné množiny) $G$.

**Definice 24.** *Buď $E$ eliptická křivka definovaná nad $\mathbb{Q}$, tj. $E$ je definovaná rovnicí*

$$y^2 = x^3 + ax + b,$$

*kde a,b jsou BÚNO celá čísla, a buď p prvočíslo. Uvažujeme křivku $E'$ definovanou nad $\mathbb{F}_p$ rovnicí*

$$y^2 = x^3 + cx + d, \tag{4.1}$$

*kde $c = a \mod p$ a $d = b \mod p$. Křivku $E'$ nazýváme* redukcí *křivky $E$ modulo $p$. V případě, že $E'$ je nesingulární eliptická křivka nad $\mathbb{F}_p$, tj. $4c^3 + 27d^2 \not\equiv 0 \pmod p$, tak řekneme, že redukce $E$ modulo $p$ je* dobrá.

Protože v definici eliptické křivky chceme, aby $4a^3 + 27b^2$ bylo nenulové, tak je hned vidět, že pokud $p \neq 2,3$ a zároveň $p \nmid 4a^3 + 27b^2$, tak je redukce $E$ modulo $p$ dobrá. Tedy se $E$ redukuje dobře pro všechna prvočísla, až na konečně mnoho výjimek. Chtěli bychom koeficienty $a'$,$b' \in \mathbb{Z}$ takové, že rovnice $y^2 = x^3 + a'x + b'$ definuje křivku izomorfní původní křivce, a navíc je počet prvočísel $p$ takových, že $p \mid 4a'^3 + 27b'^2$ minimální. Lze ukázat, že takové koeficienty existují, a v tom případě nazýváme $y^2 = x^3 + a'x + b'$ *minimální rovnicí křivky $E$*.

**Definice 25.** *Buď $E$ eliptická křivka definovaná nad $\mathbb{Q}$ rovnicí* (1.1) *a buď $p$ prvočíslo takové, že redukce $E'$ křivky $E$ modulo $p$ není dobrá. Tedy rovnice* (4.1)

*má násobný kořen modulo p. Pokud má kořen násobnosti* 3*, řekneme, že redukce je* aditivní*. Pokud má kořen násobnosti* 2*, tak redukci nazveme* multiplikativní*. V případě multiplikativní redukce navíc rozlišujeme mezi dvěma případy.*

*Pokud jsou směrnice tečen v singulárních bodech prvky* $\mathbb{F}_p$*, tak řekneme, že je redukce E modulo p* štěpící multiplikativní*. V opačném případě je redukce* neštěpící multiplikativní*.*

Je-li $E$ eliptická křivka nad $\mathbb{Q}$ a $p$ je prvočíslo takové, že se $E$ modulo $p$ redukuje dobře, tak položme $N_p = \#E'(\mathbb{F}_p)$, kde $E'$ je redukce $E$ modulo $p$. Protože se $E$ redukuje dobře v nekonečně mnnoha případech, tak můžeme zkoumat limitní chování posloupnosti $N_p$. V padesátých letech napadlo Bryana Birche a Petera Swinnerton-Dyera, že by růst této posloupnosti mohl souviset s rankem křivky $E$. Protože měli přístup k jednomu z mála tehdejších počítačů, tak experimentálně došli k následující domněnce.

**Domněnka 31.** *Pro každou eliptickou křivku* $E$ *nad* $\mathbb{Q}$ *existuje konstanta* $C$ *taková, že*

$$\lim_{P\to\infty} \frac{\prod_{p\leq P} \frac{N_p}{p}}{(\log P)^r} = C,$$

*kde* $r$ *je rank křivky* $E$*.*

Birch a Swinnerton-Dyer tímto postupem ve většině případů dokázali určit rank, ale protože $\prod_{p\leq P} N_p/p$ s rostoucím $p$ osciluje, tak nedokázali dost přesně spočítat $C$. Tedy chtěli tuto domněnku formulovat jinak. (Milne, 2006)(str. 161)

Buď $E$ eliptická křivka nad $\mathbb{Q}$ a $p$ prvočíslo takové, že redukce $E$ modulo $p$ je dobrá. Definujeme koeficienty $a_p$ vztahem $N_p = p + 1 - a_p$. Pokud je redukce $E$ modulo $p$ špatná, tak definujeme

$$a_p = \begin{cases} 0 & \text{je-li redukce } E \text{ modulo } p \text{ aditivní,} \\ 1 & \text{je-li redukce } E \text{ modulo } p \text{ štěpící multiplikativní,} \\ -1 & \text{je-li redukce } E \text{ modulo } p \text{ neštěpící multiplikativní.} \end{cases}$$

**Definice 26.** *Buď* $E$ *eliptická křivka nad* $\mathbb{Q}$ *a koeficienty* $a_p$ *jako výše. Definujeme* $L$-funkci *křivky* $E$ *vztahem*

$$L_E(s) = \Big(\prod_{\text{špatná } p} \frac{1}{1 - a_p p^{-s}}\Big)\Big(\prod_{\text{dobrá } p} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}\Big).$$

Hasseho věta říká, že $|a_p| \leq 2\sqrt{p}$. (Washington, 2008)(Věta 4.2) Tím pádem $L$-funkce konverguje pro $\Re(s) > 3/2$. Platí, že tuto funkci lze analyticky rozšířit na celou komplexní rovinu. Důkaz uvádí Washington ve čtrnácté kapitole jako důsledek tzv. Tanijamovy-Šimurovy domněnky. Tady ji nebudeme vysvětlovat, jen uvedeme, že ji pro křivky, které pro žádné prvočíslo $p$ nemají aditivní redukci, tzv. *semistabilní*, dokázal ve svém slavném článku Andrew Wiles. V úplnosti tuto domněnku dokázali Breuil a kol.

Budeme ignorovat konečně mnoho špatných prvočísel a fakt, že nekonečný součin definující $L_E$ v bodě $s = 1$ nekonverguje. Dosadíme $s = 1$ do definice $L$-funkce a formálními úpravami dostaneme

$$\prod_p \frac{1}{1 - \frac{a_p}{p} + \frac{1}{p}} = \prod_p \frac{1}{\frac{p - a_p + 1}{p}} = \prod_p \frac{p}{p - a_p + 1} = \prod_p \frac{p}{N_p}.$$

Hodně neformálně se dá říct, že když má křivka větší rank, tak má víc bodů modulo $p$ pro víc prvočísel $p$. Birch a Swinnerton-Dyer to na základě experimentálních výpočtů formulovali přesně jako následující domněnku.

**Domněnka 32.** *(Slabá Birchova-Swinnerton-Dyerova) Buď $E$ eliptická křivka nad $\mathbb{Q}$ a buď $r$ její rank. Pak $L_E(s)$ má v bodě $s = 1$ nulu řádu $r$, tj. existuje funkce $g$, která je holomorfní a nenulová na nějakém okolí bodu 1 a splňuje $L_E(s) = (s-1)^r g(s)$.*

Birch a Swinnerton-Dyer se snažili svoji domněnku zpřesnit, aby šlo něco říct nejen o hodnotě $r$, ale i o volné bázi podgrupy $E(\mathbb{Q})$ izomorfní $\mathbb{Z}^r$.

**Definice 27.** *Buď $E$ eliptická křivka nad $\mathbb{Q}$ a buď $P \in E(\mathbb{Q})$. Definujeme zobrazení $\hat{h} : E(\mathbb{Q}) \to [0,\infty)$ vztahem*

$$\hat{h}(P) = \frac{1}{2} \lim_{n\to\infty} \frac{h(2^n P)}{4^n},$$

*kde $h$ je logaritmická výška z diskuze po větě 5. Zobrazení $\hat{h}$ nazýváme* kanonická výška.

Důkaz existence limity z přechozí definice a analogie věty 5 pro zobrazení $\hat{h}$ je obsahem věty 8.18 v knize Washington (2008).

**Definice 28.** *Buď $E$ eliptická křivka nad $\mathbb{Q}$ a buď $\hat{h}$ kanonická výška. Pro body $P,Q \in E(\mathbb{Q})$ definujeme* párování podle výšky *vztahem*

$$\langle P,Q\rangle = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q).$$

**Věta 33.** *Párování podle výšky $\langle\cdot,\cdot\rangle$ je bilineární. Jsou-li navíc $P_1,\dots,P_r \in E(\mathbb{Q})$ takové, že $\det(\langle P_i,P_j\rangle_{i,j=1,\dots,r}) \neq 0$, pak jsou body $P_1,\dots,P_r$ lineárně nezávislé, tj. splňují následující podmínku: Pro libovolná celá čísla $a_1,\dots,a_r$ taková, že $a_1P_1 + \dots + a_rP_r = \mathcal{O}$, platí $a_i = 0$ pro všechna $i = 1,\dots,r$.*

*Důkaz.* (Washington, 2008)(Věta 8.25)

□

Buď $E$ křivka nad $\mathbb{Q}$, $p$ prvočíslo a označme $E'$ redukci $E$ modulo $p$. Definujeme zobrazení $E(\mathbb{Q}) \to E'(\mathbb{F}_p)$. Chceme bodu $P = (x,y) \in E(\mathbb{Q})$ přiřadit bod $P' = (x',y') \in E'(\mathbb{F}_p)$. Pokud $x,y \in \mathbb{Z}$, tak definujeme $x' = x \mod p$, $y' = y \mod p$. Je-li $x = a/b \in \mathbb{Q}$ a $p \nmid b$, tak $b'$ má v $\mathbb{F}_p$ inverzní prvek. Tedy definujeme $x' = a'b'^{-1}$. Pro $y$ to definujeme analogicky. Pokud $p$ dělí jmenovatele $x$ nebo $y$, tak lze ukázat, že dělí oba jmenovatele, a v tom případě definujeme $P'$ jako bod v nekonečnu na křivce $E'$. Pokud je redukce $E$ modulo $p$ dobrá, tak platí, že zobrazení $E(\mathbb{Q}) \to E'(\mathbb{Q}_p)$ je grupový homomorfismus. Dále položme

$$E_0(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) \mid P' \text{ je nesingulární}\}.$$

Je ihned vidět, že $E_0(\mathbb{Q}_p)$ je podgrupa $E(\mathbb{Q}_p)$, protože $\mathcal{O}$ je nesingulární, stejně jako součet dvou nesingulárních bodů. Navíc je faktorgrupa $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$ konečná (Milne, 2006)(Věta 4.1(a)). Označme $c_p = \#(E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p))$.

**Věta 34.** *Buď $E$ eliptická křivka definovaná nad $\mathbb{C}$. Pak existují $\omega_1, \omega_2 \in \mathbb{C}$ takové, že $L = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ je mříž v $\mathbb{C}$ a existuje izomorfismus grup $\mathbb{C}/L \cong E(\mathbb{C})$.*

*Důkaz.* (Washington, 2008)(Věta 9.21)

□

Je-li $E$ definovaná nad $\mathbb{Q}$, můžeme BÚNO předpokládat, že $\omega_2 \in \mathbb{R}$. Pokud $E[2] \subseteq E(\mathbb{R})$, položme $\Omega = 2\omega_2$, a $\Omega = \omega_2$ jinak.

**Domněnka 35.** *(Birchova-Swinnerton-Dyerova) Buď $E$ eliptická křivka nad $\mathbb{Q}$. Nechť $E$ má rank $r$. Potom existují lineárně nezávislé body $P_1, \ldots, P_r \in E(\mathbb{Q})$. V případě, že $r = 0$, klademe $\det(\langle P_i, P_j \rangle) = 1$. Označme $E_T$ torzní podgrupu $E(\mathbb{Q})$. Předpokládejme navíc, že $Ш(E/\mathbb{Q})$ je konečná. Potom platí*

$$\lim_{s \to 1} \frac{L_E(s)}{(s-1)^r} = \frac{\Omega(\prod_p c_p) \# Ш(E/\mathbb{Q}) \det(\langle P_i, P_j \rangle)}{(\# E_T)^2}.$$

V případě, že rank křivky $E$ je nulový, předchozí domněnka předpovídá, že rozvoj funkce $L_E(s)$ na okolí bodu 1 je

$$L_E(s) = \frac{\Omega(\prod_p c_p) \# Ш(E/\mathbb{Q})}{(\# E_T)^2} + \text{členy vyšších řádů.}$$

Pokud $r = 1$ a $P$ generuje $E(\mathbb{Q})/E_T$, tak vypadá rozvoj následovně:

$$L_E(s) = (s-1) \frac{\Omega(\prod_p c_p) \# Ш(E/\mathbb{Q}) \hat{h}(P)}{(\# E_T)^2} + \text{členy vyšších řádů.}$$

Jedním z důsledků této domněnky je i to, že $L_E(1) = 0$ právě tehdy, když $E(\mathbb{Q})$ je nekonečná. Toto tvrzení rovněž není dokázané, ačkoliv bylo dosaženo pokroku. Coates a Wiles dokázali, že když $E(\mathbb{Q})$ má komplexní násobení a $L_E(1) \neq 0$, tak je $E(\mathbb{Q})$ konečná.

V roce 2000 uveřejnil Clayův matematický institut sedm *problémů tisíciletí* a na vyřešení každého vypsal odměnu jeden milion dolarů. Na tento seznam zařadili i Birchovu-Swinnerton-Dyerovu (BSD) domněnku.

Birch a Swinnerton-Dyer svoji domněnku numericky ověřili v mnoha konkrétních případech. K úspěšnému vyřešení je ale potřeba dokázat konečnost Ш. Lze to použít i naopak: předpokládat platnost BSD domněnky a z toho spočítat počet prvků Ш.

I přes desítky let trvající snahu a vypsanou odměnu se podařilo vyřešit jen několik speciálních případů, ve kterých byla zároveň vyřešena i konečnost Ш.

Gross a Zagier dokázali, že pokud má $L_E(s)$ v bodě $s = 1$ nulu řádu 1, tj. $L_E(1) = 0$ a zároveň $L'_E(1) \neq 0$, pak je rank $E$ alespoň 1.

Kolyvagin rozvinul teorii křivek nad racionálními čísly a z výsledků v tomto článku a článku Gross a Zagier (1986) vyplývá, že je-li křivka $E$ definovaná nad $\mathbb{Q}$, tak $L_E(1) \neq 0 \implies r = 0$ a naopak $L_E(1) = 0 \ \& \ L'_E(1) \neq 0 \implies r = 1$.

Jak Kolyvagin, tak Gross se Zagierem tato tvrzení dokázali za předpokladu, že křivka $E$ splňuje Tanijamovu-Šimurovu domněnku. Tím pádem z dříve zmíněného článku (Breuil a kol., 2001) plyne, že tyto výsledky platí pro všechny eliptické křivky nad $\mathbb{Q}$.

Tedy pokud pro eliptickou křivku $E$, jejíž rank je buď 0 nebo 1, existuje nenulová konstanta $k$ splňující

$$\lim_{s\to 1} \frac{L_E(s)}{(s-1)^r} = k,$$

tak BSD domněnka platí. Bohužel ale nejsou známé žádné výsledky pro křivky ranku většího než 1.

V úvodu jsme zmínili kongruentní čísla. Jeden z mnoha důsledků BSD domněnky je řešení problému kongruentních čísel. Ten spočívá v rozhodnutí, je-li zadané číslo kongruentní.

Připomeňme, že přirozené číslo $n$ je *kongruentní*, pokud existuje racionální číslo $r$ takové, že $r^2-n$, $r^2$, $r^2+n$ jsou nenulové druhé mocniny racionálních čísel. Lze ukázat, že $n$ je kongruentní právě tehdy, když existuje pravoúhlý trojúhelník s racionálními délkami stran takový, že jeho obsah je roven $n$. Zároveň jsme v úvodu uvedli, že s tímto problémem souvisí eliptická křivka zadaná rovnicí

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

Připomeňme, že přirozené číslo $n$ je *kongruentní*, pokud existuje racionální číslo $r$ takové, že $r^2 - n$, $r^2$, $r^2 + n$ jsou nenulové druhé mocniny racionálních čísel. Lze ukázat, že $n$ je kongruentní číslo právě tehdy, když existuje pravoúhlý trojúhelník s racionálními délkami stran takový, že jeho obsah je roven $n$. Zároveň jsme v úvodu uvedli, že s tímto problémem souvisí eliptická křivka zadaná rovnicí

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

Fibonacci dokázal, že 5 je kongruentní číslo. Úplně problém vyřešil až Jerrold B. Tunnell v roce 1983, kdy dokázal (v trochu jiné podobě) následující větu.

**Věta 36.** *(Tunnell) Buď $n$ bezčtvercové přirozené číslo a položme*

$$\begin{aligned} f(n) &= \#\{(x,y,z) \in \mathbb{Z}^3 \mid n = x^2 + 2y^2 + 8z^2\}, \\ g(n) &= \#\{(x,y,z) \in \mathbb{Z}^3 \mid n = x^2 + 2y^2 + 32z^2\}, \\ j(n) &= \#\{(x,y,z) \in \mathbb{Z}^3 \mid n/2 = x^2 + 2y^2 + 8z^2\}, \\ k(n) &= \#\{(x,y,z) \in \mathbb{Z}^3 \mid n/2 = x^2 + 2y^2 + 8z^2\}. \end{aligned}$$

*Je-li $n$ kongruentní a liché, pak $f(n) = 2g(n)$. Je-li $n$ kongruentní a sudé, pak $j(n) = 2k(n)$. Navíc, pokud pro křivku definovanou rovnicí $y^2 = x^3 - n^2x$ platí domněnka 32 (slabá BSD), tak platí i opačná implikace.*

*Důkaz.* (Tunnell, 1983)

□

Krása Tunnellovy věty spočívá v tom, že lze snadno ověřit $f(n) \neq 2g(n)$, popř. $j(n) \neq 2k(n)$, a tím pádem rozhodnout, že $n$ není kongruentní.

Pokud máme pravoúhlý trojúhelník s racionálními délkami stran $a$, $b$, $c$ a obsahem $n$, tak ho zobrazíme na racionální bod $(x,y)$ na křivce definované rovnicí $y^2 = x^3 - n^2x$ následujícím předpisem

$$(a,b,c) \longmapsto \left(\frac{nb}{c-a}, \frac{2n^2}{c-a}\right),$$

a opačně definujeme

$$(x, y) \longmapsto (\frac{x^2 - n^2}{y}, \frac{2nx}{y}, \frac{x^2 + n^2}{y}).$$

Lze ukázat, že tato zobrazení jsou vzájemně inverzní bijekce, a tedy $n$ je racionální číslo právě tehdy, když má daná křivka netriviální racionální body.

# Závěr

V práci jsme definovali základní pojmy a uvedli jsme některé vlastnosti eliptických křivek. Nejvýznamnější je ta, že body na křivce tvoří grupu. Mordellova-Weilova věta (Věta 4) říká, že v případě křivek nad racionálními čísly je tato grupa konečně generovaná, tedy se rozkládá na direktní součin konečné grupy a $\mathbb{Z}^r$. Tuto konečnou grupu je snadné popsat (zejména díky Větě 8), a tím pádem se problém hledání racionálních bodů na křivce redukuje na nalezení hodnoty $r$, tzv. ranku.

Definovali jsme Tateovu-Šafarevičovu grupu a vysvětlili jsme, že její prvky odpovídají třídám ekvivalence homogenních prostorů příslušné křivky, které mají $p$-adický bod pro všechna $p$. Triviální prvek Ш navíc odpovídá jediné třídě, která zároveň obsahuje racionální bod.

Hasseho-Minkowského věta říká, že polynomiální rovnice stupně 2 má racionální řešení právě tehdy, když má reálné a $p$-adické řešení pro každé $p$. Eliptické křivky jsou definované rovnicemi stupně 3, tedy tuto vlastnost, tzv. Hasseho-Minkowského princip (též Hasseho nebo lokálně globální princip), vůbec splňovat nemusejí. Tateova-Šafarevičova grupa měří, jak moc daná křivka tento princip porušuje.

Nakonec jsme uvedli pojmy potřebné k formulaci Birchovy-Swinnterton-Dyerovy domněnky (Domněnka 35). Ta říká, jak řád Tateovy-Šafarevičovy grupy souvisí s rankem křivky.

Důsledek netriviálnosti studované látky je, že jsme v průběhu narazili na mnoho otevřených problémů. Vzhledem k tématu práce je nejvýznamnější konečnost Ш. Kladné vyřešení tohoto problému by dokázalo platnost algoritmu pro výpočet ranku a zároveň by znamenalo významný krok k vyřešení Birchovy-Swinnerton-Dyerovy domněnky.

Další otevřený problém v této oblasti je uspokojivý popis grupy $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. O té víme, že je nespočetná a profinitní, ale jediné dva prvky, které umíme popsat, jsou identita a komplexní sdružení.

# Seznam použité literatury


Bhargava, M. a Shankar, A. (2010). Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves. URL https://arxiv.org/abs/1006.1002.

Birch, B. J. a Swinnerton-Dyer, H. P. F. (1963). Notes on elliptic curves. II. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, **1965**, 79 – 108.

Breuil, C., Conrad, B., Diamond, F. a Taylor, R. (2001). On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises. *Journal of the American Mathematical Society*, **14**(4), 843 – 939.

Coates, J. a Wiles, A. (1977). On the conjecture of Birch and Swinnerton-Dyer. *Inventiones mathematicae*, **39**(3), 223–251. ISSN 1432-1297. doi: 10.1007/BF01402975. URL https://doi.org/10.1007/BF01402975.

Elkies, N. D. (2007). Three lectures on elliptic surfaces and curves of high rank. URL https://arxiv.org/abs/0709.2908.

Fulton, W. (2008). *Algebraic Curves: An Introduction to Algebraic Geometry*. URL http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf.

Gross, B. a Zagier, D. (1986). Heegner points and derivatives of L-series. *Inventiones mathematicae*, **84**, 225–320. URL http://eudml.org/doc/143341.

Knaf, H., Selder, E. a Spindler, K. (2019). Explicit transformation of an intersection of two quadrics to an elliptic curve in weierstrass form. URL https://arxiv.org/abs/1906.10230.

Kolyvagin, V. A. (1989). Finiteness of $E(\mathbb{Q})$ and $\text{ш}(E,\mathbb{Q})$ for a subclass of Weil curves. *Izvestiya: Mathematics*, **32**(3), 523–541.

Mazur, B. (1978). Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Inventiones mathematicae*, **44**, 129 – 162.

Milne, J. S. (2020). Algebraic number theory (v3.08). Available at www.jmilne.org/math/.

Milne, J. (2006). *Elliptic Curves*. BookSurge Publishers. ISBN 1-4196-5257-5.

Ribes, L. a Zaleskii, P. (2010). *Profinite Groups*. Second Edition. Springer-Verlag, Berlin Heidelberg. ISBN 978-3-642-01642-4.

Ribes, L. (2013). Introduction to profinite groups. *Travaux mathématiques*, **22**, 179 – 230.

Rotman, J. J. (2009). *An Introduction to Homological Algebra*. Second Edition. Springer, New York, NY. ISBN 978-0-387-68324-9.

Silverman, J. H. (2009). *The Arithmetic of Elliptic Curves*. Second Edition. Springer-Verlag, New York. ISBN 978-0-387-09494-6.

Silverman, J. H. a Tate, J. (1992). *Rational points on elliptic curves*. Corrected second printing. Springer-Verlag, New York. ISBN 0-378-97825-9.

Tunnell, J. (1983). A classical diophantine problem and modular forms of weight 3/2. *Inventiones mathematicae*, **72**, 323–334.

Washington, L. C. (2008). *Elliptic curves: number theory and cryptography*. Second edition. Chapman & Hall/CRC, Boca Raton, FL. ISBN 978-1-4200-7146-7.

Wiles, A. (1995). Modular elliptic curves and Fermat's last theorem. *Annals of Mathematics*, **141**, 443 – 551.