



**MATEMATICKO-FYZIKÁLNÍ
FAKULTA**
Univerzita Karlova

BAKALÁŘSKÁ PRÁCE

Adam Zvěřina

Komplexní algebraické křivky

Katedra algebry

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

Studijní program: Matematika

Studijní obor: Obecná matematika

Praha 2020

Prohlašuji, že jsem tuto bakalářskou 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 doc. RNDr. Janu Šťovíčkovi, Ph.D., za čas, který mi poskytl, a za rady, kterými mě zásobil.

Název práce: Komplexní algebraické křivky

Autor: Adam Zvěřina

Katedra: Katedra algebry

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

Abstrakt: Práce popisuje vztah mezi algebraickými křivkami a Riemannovými plochami. Zavedeme Weierstrassovu $\wp$ -funkci a dokážeme některé její vlastnosti. Dále nahlédneme, že každou komplexní algebraickou křivku lze chápat jako Riemannovu plochu. Nakonec ukážeme, že eliptickou křivku lze parametrizovat pomocí Weierstrassovy $\wp$ -funkce.

Klíčová slova: eliptická křivka, Riemannova plocha, komplexní torus, Weierstrassova $\wp$ -funkce

Title: Complex algebraic curves

Author: Adam Zvěřina

Department: Department of algebra

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

Abstract: The thesis describes the relationship between algebraic curves and Riemann surfaces. We define Weierstrass $\wp$ -function and prove some of its properties. We further prove that every complex algebraic curve can be regarded as a Riemann surface. Finally, we demonstrate that an elliptic curve can be parametrised with Weierstrass $\wp$ -function.

Keywords: elliptic curve, Riemann surface, complex torus, Weierstrass $\wp$ -function

Obsah

Úvod	2
1 Weierstrassova $\wp$ -funkce	3
2 Riemannovy plochy	10
3 Eliptické křivky	17
Závěr	24
Seznam použité literatury	25

Úvod

Uvažujme pyramidu sestavenou z koulí. V nejvyšší vrstvě je jedna koule, v další čtyři, ve třetí vrstvě devět koulí atd. Když pyramida spadne, je možné koule přeskládat do tvaru čtverce? V pyramidě o x vrstvách je

$$1^2 + 2^2 + \dots + x^2 = \frac{x(x+1)(2x+1)}{6}$$

koulí. Chceme vědět, jestli je tento výraz roven druhé mocnině přirozeného čísla, tj. hledáme celočíselná řešení rovnice

$$y^2 = \frac{x(x+1)(2x+1)}{6}.$$

Rovnicemi tohoto druhu, tzv. diofantickými rovnicemi, se zabývali už staří Řekové. Pokud se neomezíme jen na celočíselná řešení, pak polynomiální rovnice definují algebraické křivky, jeden ze základních pojmů algebraické geometrie. Rovnice z předchozího odstavce představuje speciální typ křivky – eliptickou křivku. Ty jsou předmětem obsáhlého výzkumu a mají aplikace v kryptografii, o kterých pojednává např. Washington (2008).

Geometrické výsledky, jichž bylo dosaženo v 19. století zejména v oblastech projektivní a neeukleidovské geometrie, umožnily propojení algebry a geometrie.

Chceme ukázat souvislost mezi algebraickými křivkami a Riemannovými plochami. Vyložíme pátou kapitolu z knihy Kirwan (1992) a doplníme některé důkazy. Konkrétním cílem je dokázat, že nesesingulární algebraická křivka má holomorfní atlas, a to dále použít k důkazu, že eliptické křivky lze parametrizovat pomocí zobrazení z komplexního toru.

1. Weierstrassova $\wp$ -funkce

Definice 1. *Bud' $z_0 \in \mathbb{C}$ a f funkce definovaná na nějakém okolí bodu z_0 . Řekneme, že f je holomorfní v z_0 , pokud existuje vlastní limita $\lim_{h \rightarrow 0} \frac{f(z_0+h)-f(z_0)}{h}$, a tuto limitu nazveme derivací f v bodu z_0 . Když $G \subset \mathbb{C}$ je otevřená a $f : G \rightarrow \mathbb{C}$, řekneme, že f je holomorfní na G , pokud je holomorfní v každém bodu množiny G .*

Definice 2. *Bud' $W \subset \mathbb{C}$ otevřená. Řekneme, že množina P je izolovaná v W , pokud pro každý bod $x \in W$ existuje jeho prstencové okolí $O \subset W$ takové, že $P \cap O = \emptyset$.*

Definice 3. *Funkci $f : W \rightarrow \mathbb{C} \cup \{\infty\}$ nazveme meromorfní na W , jestliže f je spojitá a existuje množina P izolovaná v W taková, že f je holomorfní v $W \setminus P$ a v každém bodu množiny P má pól.*

V této situaci existuje pro libovolný bod $a \in P$ nějaké $m > 0$ takové, že můžeme f rozvinout do Laurentovy řady

$$f(z) = \sum_{n=-m}^{\infty} c_n(z-a)^n, \quad 0 < |z-a| < r,$$

kde $c_{-m} \neq 0$. Hodnotu m nazýváme násobností pólu. Hodnotu koeficientu c_{-1} nazýváme reziduem funkce f v bodě a a značíme ho $\text{res}(f(z), a)$.

Bud' $[a, b] \subset \mathbb{R}$ interval. Spojité zobrazení $\gamma : [a, b] \rightarrow \mathbb{C}$ nazveme křivkou v $\mathbb{C}$. Pokud lze γ rozšířit na nějaký otevřený interval obsahující $[a, b]$ tak, že γ' je na tomto otevřeném intervalu spojitá, řekneme, že γ je hladká. Pokud $\gamma(a) = \gamma(b)$, řekneme, že γ je uzavřená; pokud $\gamma|_{[a, b]}$ je prosté, řekneme, že γ je jednoduchá.

Když existuje dělení $a = a_0 < a_1 < \dots < a_n = b$ intervalu $[a, b]$ a hladká zobrazení $\gamma_i : [a_{i-1}, a_i] \rightarrow W$, $1 \leq i \leq n$ takové, že $\gamma(t) = \gamma_i(t)$, $t \in [a_{i-1}, a_i]$, řekneme, že γ je po částech hladká.

Ať $f : W \rightarrow \mathbb{C}$ je spojitá funkce a $\gamma : [a, b] \rightarrow W$ je po částech hladká křivka, pak definujeme integrál f podle křivky γ předpisem

$$\int_{\gamma} f(z) dz = \int_a^b f(\gamma(t)) \gamma'(t) dt.$$

Ve zbytku kapitoly se budeme zabývat speciálním druhem křivek. Speciální křivkou budeme rozumět jednoduchou uzavřenou křivku, která je po částech úsečka, tj. zobrazení γ_i jsou úsečky v $\mathbb{C}$. Pak podle Jordanovy věty (Veselý, 2000, str. 36) existuje souvislá omezená množina $\text{Int}(\gamma)$ taková, že γ je její hranice. Tuto množinu nazýváme vnitřkem γ .

Věta 4 (Cauchyho věta). *Bud' γ speciální křivka v $\mathbb{C}$ a necht' f je funkce holomorfní na nějaké otevřené množině $W \subset \mathbb{C}$ obsahující $\overline{\text{Int}(\gamma)}$. Potom*

$$\int_{\gamma} f(z) dz = 0.$$

Věta 5 (Cauchyho reziduová věta). *Bud' γ speciální křivka v $\mathbb{C}$ a necht' funkce f je meromorfní na nějaké otevřené množině obsahující $\overline{\text{Int}(\gamma)}$ s konečně mnoha*

póly $a_1, \dots, a_n$ tak, že $\{a_1, \dots, a_n\} \subset \text{Int}(\gamma)$ a navíc žádný z pólů neleží na γ . Potom platí

$$\int_{\gamma} f(z) dz = \pm 2\pi i \sum_{j=1}^n \text{res}(f, a_j).$$

Věta 6 (Moreroova věta). Ať $W \subset \mathbb{C}$ je otevřená a $f : W \rightarrow \mathbb{C}$ spojitá. Jestliže

$$\int_{\gamma} f(z) dz = 0$$

pro každou speciální křivku γ v konvexní otevřené podmnožině W , pak f je holomorfní na W .

Všechny tyto věty se dají zobecnit pro větší množinu křivek. Jejich důkazy uvádí Veselý (2000). S jejich pomocí lze dokázat následující větu.

Věta 7. Ať $W \subset \mathbb{C}$ je otevřená a buď $(f_n : W \rightarrow \mathbb{C})_{n=1}^{\infty}$ posloupnost holomorfních funkcí, která stejnoměrně konverguje k funkci $f : W \rightarrow \mathbb{C}$. Potom f je holomorfní na W a derivace f'_n konvergují stejnoměrně k f' na W .

Důkaz. (Veselý, 2000, str. 109)

□

Snadným důsledkem Věty 7 je tzv. Weierstrassův M-test.

Důsledek. Ať $W \subset \mathbb{C}$ je otevřená a $(f_n : W \rightarrow \mathbb{C})_{n=1}^{\infty}$ je posloupnost funkcí holomorfních na W . Označme $|f_n| = \sup\{|f_n(z)| : z \in W\}$. Necht existují kladná reálná čísla M_n taková, že $|f_n| \leq M_n$ pro každé $n \in \mathbb{N}$ a řada $\sum_{n=1}^{\infty} M_n$ konverguje. Potom řada $\sum_{n=1}^{\infty} f_n(z)$ konverguje stejnoměrně na W k holomorfní funkci $f(z)$ splňující $f'(z) = \sum_{n=1}^{\infty} f'_n(z)$.

Důkaz. Označme s_n n -tý částečný součet řady $\sum f_k$. Pak pro $m > n$ platí odhad

$$\sup\{|f_m(z) - f_n(z)| : z \in W\} \leq M_{n+1} + \dots + M_m,$$

a protože $\sum M_n$ konverguje, tak je posloupnost $\{s_n\}$ stejnoměrně Cauchyovská. Tedy $\sum_{k=1}^{\infty} f_k$ konverguje stejnoměrně a zbytek tvrzení přímo plyne z věty 7.

□

Definice 8. Budte ω_1, ω_2 nenulová komplexní čísla lineárně nezávislá nad $\mathbb{R}$. Pak $\Lambda = \{n\omega_1 + m\omega_2 : n, m \in \mathbb{Z}\}$ nazveme mříží v $\mathbb{C}$.

Lemma 9. Existuje $\delta > 0$ takové, že pro všechna $x, y \in \mathbb{R}$ platí

$$|x\omega_1 + y\omega_2| \geq \delta \sqrt{x^2 + y^2}.$$

Důkaz. Definujme funkci $f : [0, 2\pi] \rightarrow \mathbb{R}$ předpisem $f(\varphi) = |(\cos \varphi)\omega_1 + (\sin \varphi)\omega_2|$. Interval $[0, 2\pi]$ je kompaktní a f je spojitá. Tedy f je omezená a nabývá svých extrémů. Protože ω_1 a ω_2 jsou lineárně nezávislá nad $\mathbb{R}$, tak $f(\varphi) > 0$ pro všechna $\varphi \in [0, 2\pi]$. Tedy existuje $\delta > 0$ takové, že $f(\varphi) > \delta$ pro všechna $\varphi \in [0, 2\pi]$.

Pro libovolná $x, y \in \mathbb{R}$ obě nenulová existuje právě jedno $r > 0$ a $\varphi \in [0, 2\pi]$ takové, že $x = r \cos \varphi$ a $y = r \sin \varphi$. Tedy $|x\omega_1 + y\omega_2| = |r(\cos \varphi)\omega_1 + r(\sin \varphi)\omega_2| \geq |\delta r| = \delta \sqrt{x^2 + y^2}$.

□

Věta 10. *Bud Λ mříž v $\mathbb{C}$. Pak existuje meromorfní funkce $\wp(z)$ na $\mathbb{C}$ definovaná vztahem*

$$\wp(z) = z^{-2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left((z - \omega)^{-2} - \omega^{-2} \right),$$

pro jejíž derivaci platí

$$\wp'(z) = \sum_{\omega \in \Lambda} -2(z - \omega)^{-3}.$$

Důkaz. Zvolme $R > 0$ libovolné a položme $\Lambda_R = \{\omega \in \Lambda : |\omega| \leq 2R\}$. Potom z Lemmatu 9 plyne, že $\Lambda_R \subset \{n\omega_1 + m\omega_2 : n, m \in \mathbb{Z}, n^2 + m^2 \leq 4R^2\delta^{-2}\}$, a tedy $\Lambda_R \subset \Lambda$ je konečná.

$$z^{-2} + \sum_{\Lambda \setminus \{0\}} (z - \omega)^{-2} - \omega^{-2} = \left(z^{-2} + \sum_{\Lambda_R \setminus \{0\}} (z - \omega)^{-2} - \omega^{-2} \right) + \left(\sum_{\Lambda \setminus \Lambda_R} (z - \omega)^{-2} - \omega^{-2} \right) \quad (1.1)$$

První sčítanec na pravé straně rovnice 1.1 je meromorfní. Dokážeme-li, že druhý sčítanec konverguje absolutně stejnoměrně na množině $\{z \in \mathbb{C} : |z| \leq R\}$, pak je tato suma podle Weierstrassova M-testu holomorfní, a tedy je celá pravá strana rovnice meromorfní na množině $\{z \in \mathbb{C} : |z| < R\}$. Z M-testu navíc plyne, že lze řadu derivovat člen po členu, a tím dostaneme i druhou část tvrzení.

Zvolme $\omega = n\omega_1 + m\omega_2 \in \Lambda \setminus \Lambda_R$. Je-li navíc $|z| \leq R$, pak $|z| \leq \frac{1}{2}|\omega|$, a tedy $|z - \omega| \geq \frac{1}{2}|\omega|$. Kdyby $|z - \omega| < \frac{1}{2}|\omega|$, pak $|\omega| \leq |z| + |z - \omega| < \frac{1}{2}|\omega| + \frac{1}{2}|\omega|$, což je spor. Tedy $|z - \omega|^{-2} \leq 4|\omega|^{-2}$. Navíc $|2\omega - z| \leq |2\omega| + |-z| = |2\omega| + |z| \leq 2|\omega| + \frac{1}{2}|\omega| = \frac{5}{2}|\omega|$.

Celkem dostáváme

$$\begin{aligned} |(z - \omega)^{-2} - \omega^{-2}| &= |z(2\omega - z)(z - \omega)^{-2}\omega^{-2}| \\ &\leq (5R|\omega|/2)/(|\omega|^4/4) \\ &= 10R/|\omega|^3 \\ &\leq 10R\delta^{-3}(n^2 + m^2)^{-3/2}. \end{aligned}$$

Konvergenci členů na pravé straně dostaneme ze srovnávacího kritéria

$$\begin{aligned} \sum_{(n,m) \neq (0,0)} (n^2 + m^2)^{-3/2} &= \sum_{k=1}^{\infty} \sum_{\max(|n|, |m|)=k} (n^2 + m^2)^{-3/2} \\ &\leq 8 \sum_{k=1}^{\infty} k^{-2} < \infty, \end{aligned}$$

neboť $\sum_{\max(|n|, |m|)=k} (n^2 + m^2)^{-3/2}$ má $8k$ sčítanců a platí

$$(n^2 + m^2)^{-3/2} \leq (k^2)^{-3/2} = k^{-3},$$

takže celkem

$$\sum_{\max(|n|, |m|)=k} (n^2 + m^2)^{-3/2} \leq 8k \cdot k^{-3} = 8k^{-2}.$$

Tedy pro libovolné $z \in \mathbb{C}$ lze zvolit $R > 0$ tak, že nějaké okolí z je v množině $\{z \in \mathbb{C} : |z| \leq R\}$, a tedy je $\wp(z)$ na tomto okolí meromorfní. Tím pádem je $\wp(z)$ meromorfní na $\mathbb{C}$.

□

Definice 11. $\wp(z)$ se nazývá Weierstrassova $\wp$ -funkce mřížě Λ .

Lemma 12. $\wp(z) = \wp(-z) = \wp(z + \zeta)$ pro každé $z \in \mathbb{C}$ a $\zeta \in \Lambda$.

Důkaz. Když $\zeta \in \Lambda$, pak $\wp'(z + \zeta) = -2 \sum_{\omega \in \Lambda} (z + \zeta - \omega)^{-3}$. Protože řada konverguje absolutně a $\omega - \zeta$ probíhá přes Λ , když ω probíhá Λ , tak můžeme řadu přerovnat a substituovat ω za $\omega - \zeta$ a tím dostaneme

$$\wp'(z + \zeta) = \wp'(z), z \in \mathbb{C}.$$

Z toho plyne

$$\wp(z + \zeta) = \wp(z) + c(\zeta),$$

kde $c(\zeta)$ nezávisí na z . Dosazením $z = -\frac{1}{2}\zeta$ dostaneme

$$c(\zeta) = \wp\left(\frac{1}{2}\zeta\right) - \wp\left(-\frac{1}{2}\zeta\right).$$

Podle definice je $\wp(-z) = z^{-2} + \sum_{\omega \in \Lambda \setminus \{0\}} (z + \omega)^{-2} - \omega^{-2}$ a opět můžeme řadu přerovnat a substituovat ω za $-\omega$ a tím dostaneme $\wp(-z) = \wp(z)$, $z \in \mathbb{C}$.

Tedy speciálně $c(\zeta) = \wp\left(\frac{1}{2}\zeta\right) - \wp\left(-\frac{1}{2}\zeta\right) = 0$, a tedy

$$\wp(z + \zeta) = \wp(z), z \in \mathbb{C}.$$

Což jsme chtěli dokázat. □

Protože $\wp(z)$ má v nule pól násobnosti 2, tak má tím pádem póly násobnosti 2 ve všech mřížových bodech. Navíc je $\wp$ holomorfní v libovolném bodě $z \in \mathbb{C} \setminus \Lambda$, takže mřížové body jsou jediné póly $\wp$.

Definice 13. Funkci $f : \mathbb{C} \rightarrow \mathbb{C}$ splňující $\forall z \in \mathbb{C}, \forall \zeta \in \Lambda : f(z + \zeta) = f(z)$ ekvivalentně $\forall z \in \mathbb{C} : f(z + \omega_1) = f(z) = f(z + \omega_2)$ nazveme dvojité periodickou funkcí s periodami ω_1, ω_2 .

Věta 14 (Liouvillova věta). Necht $f : \mathbb{C} \rightarrow \mathbb{C}$ je na $\mathbb{C}$ omezená a holomorfní. Pak je f konstantní.

Důkaz. (Veselý, 2000, str. 116) □

Lemma 15. Ať f je dvojité periodická funkce holomorfní na $\mathbb{C}$. Pak f je konstantní.

Důkaz. Rovnoběžník $P = \{s\omega_1 + t\omega_2 : s, t \in [0, 1]\}$ je omezená a uzavřená podmnožina $\mathbb{C}$. Tedy P je kompaktní. Funkce f je na $\mathbb{C}$ holomorfní, a tím pádem i spojitá, takže f je na P omezená.

Pro dané $z \in \mathbb{C}$ najdeme $\zeta \in \Lambda$ takové, že $z + \zeta \in P$, a protože f je dvojité periodická, tak $f(z + \zeta) = f(z)$, a tedy je f omezená na $\mathbb{C}$. Tvrzení tedy plyne z Liouvillovy věty. □

Lemma 16. *Označme*

$$g_2 = 60 \sum_{\omega \in \Lambda \setminus \{0\}} \omega^{-4}$$

a

$$g_3 = 140 \sum_{\omega \in \Lambda \setminus \{0\}} \omega^{-6}.$$

Potom $\wp(z)$ splňuje vztah:

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3.$$

Důkaz. Funkce $f(z) = \wp(z) - z^{-2} = \sum_{\omega \in \Lambda \setminus \{0\}} ((z - \omega)^{-2} - \omega^{-2})$ nabývá nulové hodnoty v bodě $z = 0$ a je na nějakém okolí nuly holomorfní. Navíc je to sudá funkce, takže její Taylorův rozvoj kolem nuly obsahuje jen sudé mocniny z . To znamená, že na nějakém okolí nuly platí

$$\wp(z) = z^{-2} + \lambda z^2 + \mu z^4 + z^6 h(z), \quad (1.2)$$

kde h je holomorfní na nějakém okolí nuly. Zderivováním dále dostaneme

$$\wp'(z) = -2z^{-3} + 2\lambda z + 4\mu z^3 + 6z^5 h(z) + z^6 h'(z). \quad (1.3)$$

Mějme funkci

$$k(z) = \wp'(z)^2 - 4\wp(z)^3 + 20\lambda\wp(z) + 28\mu. \quad (1.4)$$

Umocněním 1.2 a 1.3 dostaneme

$$\begin{aligned} \wp(z)^3 &= z^{-6} + 3\lambda z^{-2} + 3\mu + 3(\lambda^2 + h(z))z^2 + 6\lambda\mu z^4 + (\lambda^3 + 3\mu^2 + 6\lambda h(z))z^6 \\ &\quad + 3(\lambda^2\mu + 2\mu h(z))z^8 + 3(\lambda\mu^2 + \lambda^2 h(z) + h(z)^2)z^{10} + (\mu^3 + 6\lambda\mu h(z))z^{12} \\ &\quad + 3(\mu^2 h(z) + \lambda h(z)^2)z^{14} + 3\mu h(z)^2 z^{16} + h(z)^3 z^{18} \end{aligned} \quad (1.5)$$

a

$$\begin{aligned} \wp'(z)^2 &= 4z^{-6} - 8\lambda z^{-2} - 16\mu + 4(\lambda^2 - 6h(z))z^2 - 4h'(z)z^3 + 16\lambda\mu z^4 \\ &\quad + 8(2\mu^2 + 3\lambda h(z))z^6 + 4\lambda h'(z)z^7 + 48\mu h(z)z^8 + 8\mu h'(z)z^9 \\ &\quad + 36h(z)^2 z^{10} + 6h(z)h'(z)z^{11} + h'(z)^2 z^{12}. \end{aligned} \quad (1.6)$$

Dosadíme 1.2, 1.5 a 1.6 do 1.4 a dostaneme

$$\begin{aligned} k(z) &= 12(\lambda^2 - 3h(z))z^2 - 4h'(z)z^3 + 12\lambda\mu z^4 - 4(\lambda^3 - \mu^2 - 5\lambda h(z))z^6 \\ &\quad + 4\lambda h'(z)z^7 - 12(\lambda^2\mu - 2\mu h(z))z^8 + 8\mu h'(z)z^9 \\ &\quad - 12(\lambda\mu^2 + \lambda^2 h(z) - 2h(z)^2)z^{10} + 6h(z)h'(z)z^{11} \\ &\quad + (h'(z)^2 - 4\mu^3 - 24\lambda\mu h(z))z^{12} - 12(\mu^2 h(z) + \lambda h(z)^2)z^{14} \\ &\quad - 12\mu h(z)^2 z^{16} - 4h(z)^3 z^{18}. \end{aligned}$$

Tedy $k(z)$ je holomorfní na nějakém otevřeném okolí nuly a $k(0) = 0$. Protože $\wp$ i $\wp'$ jsou dvojité periodické funkce holomorfní na $\mathbb{C} \setminus \Lambda$, tak $k(z)$ je holomorfní na okolí každého $\zeta \in \Lambda$. To znamená, že $k(z)$ je dvojité periodická funkce holomorfní na $\mathbb{C}$, a tedy podle Lemmatu 15 je $k(z)$ konstantní, tj. pro každé $z \in \mathbb{C}$ platí $k(z) = k(0) = 0$.

Funkci $f(z)$ můžeme v bodě $z = 0$ derivovat člen po členu. Tedy

$$f''(z) = 6 \sum_{\omega \in \Lambda \setminus \{0\}} (z - \omega)^{-4}$$

a

$$f^{(4)}(z) = 120 \sum_{\omega \in \Lambda \setminus \{0\}} (z - \omega)^{-6}.$$

Pro členy Taylorova rozvoje platí

$$\lambda = \frac{f''(0)}{2} = 3 \sum_{\omega \in \Lambda \setminus \{0\}} \omega^{-4}$$

a

$$\mu = \frac{f^{(4)}(0)}{24} = 5 \sum_{\omega \in \Lambda \setminus \{0\}} \omega^{-6}.$$

Takže

$$20\lambda = 60 \sum_{\omega \in \Lambda \setminus \{0\}} \omega^{-4} = g_2$$

a

$$28\mu = 140 \sum_{\omega \in \Lambda \setminus \{0\}} \omega^{-6} = g_3.$$

□

Věta 17. *Weierstrassova funkce $\wp : \mathbb{C} \setminus \Lambda \rightarrow \mathbb{C}$ je na. Navíc $\wp(z) = \wp(w)$ právě tehdy, když $w \in \Lambda \pm z$.*

Důkaz. Zvolme $c \in \mathbb{C}$ libovolné a položme $f(z) = \wp(z) - c$. Funkce $f'(z)/f(z)$ je meromorfní na $\mathbb{C}$. Když f má v bodě z_0 pól násobnosti m , tak Laurentův rozvoj f na okolí z_0 je

$$f(z) = \frac{c_{-m}}{(x-z)^m} + \frac{c_{-(m-1)}}{(x-z)^{m-1}} + \dots$$

a rozvoj f' na tomtéž okolí je

$$f'(z) = \frac{-mc_{-m}}{(x-z)^{m+1}} + \frac{-(m-1)c_{-(m-1)}}{(x-z)^m} + \dots$$

Dělením polynomů dostáváme rozvoj $f'/f = -m/(z - z_0) + \dots$, a tedy f'/f má v z_0 jednoduchý pól s hodnotou rezidua $-m$. Analogicky, když f má kořen násobnosti m , tak f'/f má jednoduchý pól s hodnotou rezidua m . Navíc f'/f nemá jiné póly. Když γ je křivka v $\mathbb{C}$, na které neleží žádný kořen ani pól f , tak podle Cauchyho reziduové věty (Věta 5) platí

$$\frac{1}{2\pi i} \int_{\gamma} \frac{f'(z)}{f(z)} dz = \pm(N - P),$$

kde N je počet nul a P počet pólů ve vnitřku γ včetně násobností.

Kořeny f tvoří izolovanou množinu (Veselý, 2000, Věta 8.1.8) a póly f jsou právě v mřížových bodech, takže množina všech nul a pólů funkce f je izolovaná v $\mathbb{C}$. Když je množina v $\mathbb{C}$ izolovaná, pak je spočetná (Veselý, 2000, Lemma 7.1.2).

Zvolme $a \in \mathbb{C}$, položíme $P(a) = \{a + s\omega_1 + t\omega_2 : s, t \in [0, 1]\}$. Pokud na hranici $P(a)$ jsou kořeny nebo póly f , tak uvažíme rovnoběžníky $P(a + x\omega_1)$, $x \in \mathbb{R}$. Takových rovnoběžníků je nespočetně mnoho, protože množina $\mathbb{R}$ je nespočetná, tedy mezi nimi můžeme vybrat takový rovnoběžník, že na jeho hranách rovnoběžných s vektorem ω_2 není žádný kořen ani pól. To lze, protože je množina kořenů a pólů spočetná. Analogicky se posunutím ve směru ω_2 můžeme zbavit kořenů a pólů na hranách rovnoběžných s ω_1 . Tedy existují $x, y \in \mathbb{R}$ taková, že na hranici $P(a + x\omega_1 + y\omega_2)$ neleží žádný kořen ani pól funkce f a za γ zvolíme hranici tohoto rovnoběžníku.

Ve vnitřku γ leží právě jeden mřížový bod $\zeta \in \Lambda$. Z dvojité periodicity f plyne, že $\int_{\gamma} \frac{f'(z)}{f(z)} dz = 0$, protože se odečtou integrály přes protější strany rovnoběžníku. Tedy $N = P$.

Stejně jako $\wp$ i f má póly násobnosti dva právě v mřížových bodech, takže $P = 2$. Tedy i $N = 2$ a existuje nějaké $w_0 \in P(a)$ takové, že $f(w_0) = 0$, tj. $\wp(w_0) = c$. Protože c bylo libovolné, tak $\wp : \mathbb{C} \setminus \Lambda \rightarrow \mathbb{C}$ je na.

Protože $\wp(z)$ je sudá a dvojitě periodická, tak platí $\wp(z) = \wp(w_0) = c$ pro každé $z \in \Lambda \pm w_0$. Označme $w_1 \in \Lambda - w_0$ druhý kořen funkce f uvnitř γ . Pokud $w_0 \neq w_1$, pak to jsou jediné kořeny f ve vnitřku γ , a tedy pro kořeny platí $z \in \Lambda \pm w_0$. Zbývá ukázat, že když naopak $w_0 = w_1$, tak f má dvojnásobný kořen v bodě w_0 , tj. $f'(w_0) = 0$. Ale když $w_0 = w_1$, tak $\Lambda + w_0 = \Lambda - w_1$, a protože $\wp'(z)$ je lichá dvojitě periodická funkce, tak $\wp'(w_0) = -\wp'(-w_0) = -\wp'(w_0)$. Tedy $\wp'(w_0) = 0$ a $f'(w_0) = 0$, což jsme chtěli.

□

2. Riemannovy plochy

Buď $f(x,y)$ nekonstantní bezčtvercový polynom ve dvou proměnných s komplexními koeficienty. Pak afinní algebraická křivka C v $\mathbb{C}^2$ definovaná polynomem f je množina $C = \{(x,y) \in \mathbb{C}^2 : f(x,y) = 0\}$. Když $f(x,y,z)$ je nekonstantní bezčtvercový polynom ve třech proměnných s komplexními koeficienty, a navíc f je homogenní, tak projektivní křivka C v $\mathbb{P}^2$ definovaná polynomem f je množina $C = \{(x : y : z) \in \mathbb{P}^2 : f(x,y,z) = 0\}$. Je-li navíc polynom f stupně 3, pak křivku definovanou polynomem f nazveme kubickou křivkou.

Bod (a,b) na afinní křivce C se nazývá singulární, pokud platí

$$\frac{\partial f}{\partial x}(a,b) = \frac{\partial f}{\partial y}(a,b) = 0.$$

Analogicky bod $(a : b : c)$ projektivní křivky C je singulární, pokud

$$\frac{\partial f}{\partial x}(a,b,c) = \frac{\partial f}{\partial y}(a,b,c) = \frac{\partial f}{\partial z}(a,b,c) = 0.$$

Body, které nejsou singulární, nazýváme nesingulární. Pokud jsou všechny body křivky C nesingulární, tak řekneme, že C je nesingulární křivka.

Ať C je křivka a buď N množina jejích nesingulárních bodů. Definujme zobrazení $\nu : C \rightarrow \mathbb{C}^2$ předpisem $(a,b) \mapsto (\frac{\partial f}{\partial x}(a,b), \frac{\partial f}{\partial y}(a,b))$. Potom ν je spojitý. Platí $\nu^{-1}(\{(0,0)\}) = C \setminus N$. $\{(0,0)\}$ je uzavřená v $\mathbb{C}^2$, a tedy je $C \setminus N$ uzavřená v C . Takže N je otevřená v C .

Definice 18. Buď (X,τ) topologický prostor. Řekneme, že X je Hausdorffův, pokud pro libovolné body $x,y \in X, x \neq y$ existují otevřené množiny $X,Y \in \tau$ splňující $x \in X, y \in Y$ a $X \cap Y = \emptyset$.

Definice 19. Ať S je Hausdorffův topologický prostor. Řekneme, že S je plocha, pokud pro každý bod $x \in S$ existuje jeho otevřené okolí $U \subset S$, otevřená množina $V \subset \mathbb{C}$ a homeomorfismus $\phi : U \rightarrow V$. Takový homeomorfismus nazveme mapou na S . Atlasem nazveme množinu $\Phi = \{\phi_\alpha : U_\alpha \rightarrow V_\alpha : \alpha \in A\}$ map na S splňující $S = \bigcup_{\alpha \in A} U_\alpha$.

Když $\phi_\alpha : U_\alpha \rightarrow V_\alpha$ a $\phi_\beta : U_\beta \rightarrow V_\beta$ jsou mapy, pak $\phi_\alpha(U_\alpha \cap U_\beta)$ je zřejmě otevřená podmnožina V_α .

Definice 20. Buď $\Phi = \{\phi_\alpha : U_\alpha \rightarrow V_\alpha : \alpha \in A\}$ atlas na S . Homeomorfismus $\phi_{\alpha\beta} = \phi_\alpha \circ \phi_\beta^{-1} : \phi_\beta(U_\alpha \cap U_\beta) \rightarrow \phi_\alpha(U_\alpha \cap U_\beta)$ otevřených podmnožin $\mathbb{C}$ nazveme přechodovou funkcí atlasu Φ . Řekneme, že atlas je holomorfní, pokud jsou všechny jeho přechodové funkce holomorfní v obvyklém smyslu jako funkce na $\mathbb{C}$.

Dále budeme potřebovat komplexní verzi věty o implicitní funkci.

Věta 21. Buď $P(x,y)$ polynom ve dvou proměnných s komplexními koeficienty a $x_0, y_0 \in \mathbb{C}$ splňující

$$P(x_0, y_0) = 0 \neq \frac{\partial P}{\partial y}(x_0, y_0).$$

Pak existuje otevřené okolí $U \subset \mathbb{C}$ bodu x_0 , otevřené okolí $V \subset \mathbb{C}$ bodu y_0 a holomorfní funkce $f : U \rightarrow V$ taková, že $f(x_0) = y_0$, a pokud pro $x \in U, y \in V$ platí $f(x) = y$, pak $P(x,y) = 0$.

Důkaz. Kirwan (1992, Věta B.1)

□

Věta 22. *At C je afinní algebraická křivka v $\mathbb{C}^2$. Označme N množinu nesesingulárních bodů C . Pak N má holomorfní atlas.*

Důkaz. Označme $P(x,y)$ polynom, který definuje křivku C . At $(a,b) \in N$, tj. $P(a,b) = 0$, a navíc předpokládejme $\frac{\partial P}{\partial y}(a,b) \neq 0$. Z věty o implicitní funkci existují otevřené okolí V bodu a , otevřené okolí W bodu b a holomorfní funkce $g : V \rightarrow W$ takové, že když $x \in V$ a $y \in W$, pak $P(x,y) = 0 \iff y = g(x)$. N je otevřená podmnožina C , tak můžeme zvolit V a W dostatečně malé, aby $U = \{(x,y) \in C : x \in V, y \in W\}$ bylo okolí bodu (a,b) otevřené v N . Zobrazení $\phi : U \rightarrow V$ definované vztahem $\phi(x,y) = x$ je spojitě a jeho inverz $x \mapsto (x, g(x))$ je také spojitá funkce.

Analogicky když $\frac{\partial P}{\partial x}(a,b) \neq 0$, tak existuje okolí U bodu (a,b) otevřené v N takové, že zobrazení $\psi : U \rightarrow C$ definované vztahem $\psi(x,y) = y$ je homeomorfismus na otevřenou množinu $V \subset \mathbb{C}$ s inverzním zobrazením $y \mapsto (h(y), y)$, kde h je holomorfní.

Tedy existuje atlas na N takový, že každá mapa je tvaru ϕ nebo ψ . Přejchodové funkce jsou buď identická zobrazení, nebo jeden z tvarů

$$x \mapsto (x, g(x)) \mapsto g(x),$$

$$y \mapsto (h(y), y) \mapsto h(y),$$

kde g a h jsou holomorfní. Tedy takový atlas je holomorfní.

□

Věta platí i pro projektivní křivky, ale k důkazu potřebujeme následující lemma.

Lemma 23. *At $F(x,y,z)$ je homogenní polynom stupně d . Potom*

$$x \cdot \frac{\partial F}{\partial x}(x,y,z) + y \cdot \frac{\partial F}{\partial y}(x,y,z) + z \cdot \frac{\partial F}{\partial z}(x,y,z) = d \cdot F(x,y,z).$$

Důkaz. Pro homogenní polynom platí rovnost

$$F(tx, ty, tz) = t^d F(x, y, z).$$

Zderivováním podle t dostaneme:

$$x \frac{\partial F}{\partial x}(tx, ty, tz) + y \frac{\partial F}{\partial y}(tx, ty, tz) + z \frac{\partial F}{\partial z}(tx, ty, tz) = dt^{d-1} F(x, y, z),$$

a když položíme $t = 1$, dostáváme požadovanou rovnost.

□

Věta 24. *At C je projektivní křivka v $\mathbb{P}^2(\mathbb{C})$ a označme N množinu nesesingulárních bodů C . Pak N má holomorfní atlas.*

Důkaz. Označme $P(x,y,z)$ homogenní polynom, který definuje křivku C . Bud $(a : b : c) \in C$, tj. $P(a,b,c) = 0$, a necht $\frac{\partial P}{\partial y}(a,b,c) \neq 0$. Podle Lemmatu 23 platí

$$a \cdot \frac{\partial P}{\partial x}(a,b,c) + b \cdot \frac{\partial P}{\partial y}(a,b,c) + c \cdot \frac{\partial P}{\partial z}(a,b,c) = 0.$$

Tedy $a = c = 0 \implies a = b = c = 0$, což nejde z definice $\mathbb{P}^2$. Takže $a \neq 0$ nebo $c \neq 0$. Předpokládejme, že $c \neq 0$.

Z homogeneity P plyne

$$\frac{\partial P}{\partial y}\left(\frac{a}{c}, \frac{b}{c}, 1\right) = c^{-(d-1)} \frac{\partial P}{\partial y}(a,b,c),$$

kde $d = \deg(P)$. Můžeme použít větu o implicitní funkci na polynom $P(x,y,1)$, a tedy máme okolí V a W bodů a/c a b/c otevřená v $\mathbb{C}$ a holomorfní funkci $g : V \rightarrow W$ takové, že pro $x \in V$ a $y \in W$ platí $P(x,y,1) = 0 \iff y = g(x)$.

Můžeme zvolit V a W dost malá, aby

$$\begin{aligned} U &= \{(x : y : z) \in C : z \neq 0, x/z \in V, y/z \in W\} \\ &= \{(x : y : 1) \in C : x \in V, y \in W\} \end{aligned}$$

bylo okolí bodu $(a : b : c)$ otevřené v N . Zobrazení $\phi : U \rightarrow V$ definované vztahem $\phi(x : y : z) = x/z$ je homeomorfismus s inverzem $w \mapsto (w : g(w) : 1)$.

Analogicky když $(a : b : c) \in C$ a $\frac{\partial P}{\partial y}(a,b,c) \neq 0 \neq a$ nebo když $\frac{\partial P}{\partial x}(a,b,c) \neq 0$ nebo $\frac{\partial P}{\partial z}(a,b,c) \neq 0$, pak existuje homeomorfismus $\phi : U \rightarrow V$, kde U je otevřené okolí $(a : b : c)$ v N , takový, že $\phi(x : y : z)$ je roven jednomu z následujících: $z/x, y/z, z/y, x/y, y/x$. Inverz ϕ je také jedno z následujících zobrazení:

$$w \mapsto (1 : g(w) : w), (g(w) : w : 1), (g(w) : 1 : w), (w : 1 : g(w)), (1 : w : g(w)),$$

kde $g : V \rightarrow C$ je holomorfní.

Tedy na N máme holomorfní atlas takový, že každá přechodová funkce je jednoho z tvarů: $w \mapsto w, \frac{1}{w}, g(w), \frac{1}{g(w)}, \frac{w}{g(w)}, \frac{g(w)}{w}$, kde g je holomorfní a jmenovatel je nenulový na definičním oboru přechodové funkce. Takže atlas je holomorfní. $\square$

Definice 25. Bud $\Phi = \{\phi_\alpha : U_\alpha \rightarrow V_\alpha : \alpha \in A\}$ holomorfní atlas na ploše S . Spojité zobrazení $f : S \rightarrow \mathbb{C}$ se nazývá holomorfní vzhledem k Φ v $x \in S$, pokud existuje mapa $\phi_\alpha : U_\alpha \rightarrow V_\alpha$ v Φ taková, že $x \in U_\alpha$ a $f \circ \phi_\alpha^{-1} : V_\alpha \rightarrow \mathbb{C}$ je holomorfní v bodě $\phi_\alpha(x)$. Zobrazení f se nazývá holomorfní vzhledem k Φ , pokud je holomorfní v každém bodě $x \in S$.

Holomorfnost v předchozí definici nezávisí na volbě mapy ϕ_α . Je-li $x \in U_\alpha \cap U_\beta$ a $\phi_\alpha : U_\alpha \rightarrow V_\alpha, \phi_\beta : U_\beta \rightarrow V_\beta$ jsou mapy ve Φ , pak $\phi_\alpha(U_\beta \cap U_\alpha)$ je otevřená podmnožina V_α obsahující $\phi_\alpha(x)$ a platí

$$f \circ \phi_\alpha^{-1}|_{\phi_\alpha(U_\beta \cap U_\alpha)} = (f \circ \phi_\beta^{-1}) \circ (\phi_\beta \circ \phi_\alpha^{-1})|_{\phi_\alpha(U_\beta \cap U_\alpha)}.$$

Protože $\phi_\beta \circ \phi_\alpha^{-1}$ a jeho inverz $\phi_\alpha \circ \phi_\beta^{-1}$ jsou holomorfní a složení holomorfních funkcí je holomorfní funkce, tak $f \circ \phi_\alpha^{-1}$ je holomorfní ve $\phi_\alpha(x)$ právě tehdy, když $f \circ \phi_\beta^{-1}$ je holomorfní v $\phi_\beta(x)$.

Z předchozího odstavce vyplývá, že spojitá funkce $f : S \rightarrow \mathbb{C}$ je holomorfní vzhledem k holomorfnímu atlasu Φ na S právě tehdy, když $f \circ \phi_\alpha^{-1} : V_\alpha \rightarrow \mathbb{C}$ je holomorfní pro každou mapu $\phi_\alpha : U_\alpha \rightarrow V_\alpha$ ve Φ .

Definice 26. Budte S a T plochy s holomorfními atlasy Φ a Ψ . Spojité zobrazení $f : S \rightarrow T$ nazveme holomorfní vzhledem k Φ a Ψ , jestliže

$$\psi_\beta \circ f \circ \phi_\alpha^{-1} : \phi_\alpha(U_\alpha \cap f^{-1}(W_\beta)) \rightarrow Y_\beta$$

je holomorfní pro každou mapu $\phi_\alpha : U_\alpha \rightarrow V_\alpha$ ve Φ a každou mapu $\psi_\beta : W_\beta \rightarrow Y_\beta$ v Ψ .

Lemma 27. Budte S, T, R plochy s holomorfními atlasy Φ, Ψ, Θ . Jestliže $f : S \rightarrow T$ a $g : T \rightarrow R$ jsou holomorfní vzhledem k daným holomorfním atlasům, pak $g \circ f : S \rightarrow R$ je holomorfní vzhledem k holomorfním atlasům Φ, Θ na S a R .

Důkaz. Buď $x \in S$. Chceme ukázat, že $g \circ f$ je holomorfní v x . Zvolme mapy $\phi_\alpha : U_\alpha \rightarrow V_\alpha$ na S , $\psi_\beta : W_\beta \rightarrow X_\beta$ na T a $\theta_\gamma : Y_\gamma \rightarrow Z_\gamma$ na R takové, že $x \in U_\alpha$, $f(x) \in W_\beta$, $g(f(x)) \in Y_\gamma$.

Stačí ukázat, že $\theta_\gamma \circ g \circ f \circ \phi_\alpha^{-1}$ je holomorfní v bodě $\phi_\alpha(x) \in V_\alpha$. Množina $\phi_\alpha(U_\alpha \cap f^{-1}(W_\beta) \cap g^{-1}(f^{-1}(Y_\gamma)))$ je otevřené okolí bodu $\phi_\alpha(x)$ a platí na ní

$$\theta_\gamma \circ g \circ f \circ \phi_\alpha^{-1} = (\theta_\gamma \circ g \circ \psi_\beta^{-1}) \circ (\psi_\beta \circ f \circ \phi_\alpha^{-1}),$$

což je složení dvou holomorfních funkcí, a tedy holomorfní funkce. □

Definice 28. Buď S plocha se dvěma holomorfními atlasy Φ a Ψ . Atlasy nazveme kompatibilní, pokud je identické zobrazení $1_S : S \rightarrow S$ holomorfní jako zobrazení z plochy S s atlasem Φ do plochy S s atlasem Ψ i jako zobrazení z plochy S s atlasem Ψ do plochy S s atlasem Φ .

Zřejmě platí, že relace „být kompatibilní“ na množině atlasů je ekvivalence. Navíc platí následující tvrzení.

Tvrzení 29 (Kirwan, Cvičení 5.7 (a)). Buď S plocha se dvěma kompatibilními atlasy Φ a Ψ . Pak $\Phi \cup \Psi$ je holomorfní atlas na S .

Důkaz. Budte ϕ, ψ mapy v $\Phi \cup \Psi$. Pokud jsou obě mapy ze stejného atlasu, pak je jejich přechodová funkce kompatibilní z definice. Předpokládejme, že $\phi : U \rightarrow V \in \Phi$ a $\psi : W \rightarrow Y \in \Psi$, a necht $U \cap W \neq \emptyset$ (kdyby $U \cap W = \emptyset$, pak je přechodová funkce prázdné zobrazení a všechny podmínky splňuje triviálně).

Přechodová funkce je $\psi \circ \phi^{-1} : \phi(U \cap W) \rightarrow \psi(U \cap W)$. Platí, že $\psi \circ \phi^{-1} = \psi \circ 1_S \circ \phi^{-1}$ a funkce $\psi \circ 1_S \circ \phi^{-1}$ je holomorfní, protože Φ a Ψ jsou kompatibilní atlasy.

Situace, kdy $\psi \in \Phi$ a $\phi \in \Psi$, je zcela analogická a přechodové funkce atlasu $\Phi \cup \Psi$ jsou holomorfní, tedy je to holomorfní atlas. □

Definice 30. Riemannovou plochou nazveme plochu S spolu s třídou ekvivalence $\mathcal{H}$ na množině holomorfních atlasů na S . Jinými slovy, dva holomorfní atlasy na ploše S definují stejnou Riemannovu plochu právě tehdy, když jsou kompatibilní.

Příklad (Kirwan, Cvičení 5.7 (b)). Řekneme, že holomorfní atlas Φ plochy S je úplný, pokud každý holomorfní atlas Ψ plochy S splňuje podmínku: Ψ je kompatibilní s $\Phi \implies \Psi \subset \Phi$. Ukažte, že každá třída ekvivalence $\mathcal{H}$ na množině holomorfních atlasů na S obsahuje právě jeden úplný holomorfní atlas.

Důkaz. Jednoznačnost přímo plyne z Tvzení 29. Jsou-li $\Phi \neq \Psi$ dva různé úplné atlasy v $\mathcal{H}$, pak jsou kompatibilní a jejich sjednocení je holomorfní atlas v $\mathcal{H}$. Sjednocení navíc obsahuje oba tyto atlasy, což je spor s úplností Φ a Ψ .

Třída $\mathcal{H}$ je částečně uspořádaná inkluzí. Chceme dokázat, že má maximální prvek. Buď $\{\Phi_i : i \in I\}$ řetězec holomorfních atlasů v $\mathcal{H}$. Položme $\Phi = \bigcup_{i \in I} \Phi_i$. Pro libovolné mapy $\phi_\alpha, \phi_\beta \in \Phi$ existují $i_1, i_2 \in I$ taková, že $\phi_\alpha \in \Phi_{i_1}, \phi_\beta \in \Phi_{i_2}$. Protože $\{\Phi_i : i \in I\}$ je řetězec, tak buď $\Phi_{i_1} \subset \Phi_{i_2}$, nebo $\Phi_{i_2} \subset \Phi_{i_1}$. BÚNO $\Phi_{i_1} \subset \Phi_{i_2}$. Tedy $\phi_\alpha, \phi_\beta \in \Phi_{i_2}$. Přejchodová funkce $\phi_\alpha \circ \phi_\beta^{-1}$ je tedy holomorfní, a tím pádem je Φ holomorfní atlas. Každý řetězec v $\mathcal{H}$ má horní závorku, a z Zornova lemmatu tedy plyne, že v $\mathcal{H}$ existuje maximální prvek. □

Definice 31. *Riemannovy plochy S, T nazveme biholomorfní, pokud existuje holomorfní bijekce $f : S \rightarrow T$ taková, že její inverz je holomorfní.*

Požadavek, že inverzní funkce je také holomorfní, můžeme vynechat. Je-li $f : W \rightarrow \mathbb{C}$ holomorfní na W a prostá, pak její inverzní funkce $f^{-1} : f(W) \rightarrow \mathbb{C}$ je holomorfní na $f(W)$. Zvolme $z \in W$ a $h \neq 0$. Pak

$$\begin{aligned} 1 &= \frac{z + h - z}{h} = \frac{f^{-1}(f(z + h)) - f^{-1}(f(z))}{h} \\ &= \frac{f^{-1}(f(z + h)) - f^{-1}(f(z))}{f(z + h) - f(z)} \frac{f(z + h) - f(z)}{h}. \end{aligned}$$

Limita výrazu v prvním řádku napravo pro $h \rightarrow 0$ je jedna, tedy existuje limita výrazu na druhém řádku. Protože f je v z holomorfní, tak

$$\lim_{h \rightarrow 0} \frac{f(z + h) - f(z)}{h}$$

je vlastní, a tedy je vlastní i

$$\lim_{h \rightarrow 0} \frac{f^{-1}(f(z + h)) - f^{-1}(f(z))}{f(z + h) - f(z)}.$$

Z věty o limitě složené funkce vyplývá, že

$$\lim_{f(z+h) \rightarrow f(z)} \frac{f^{-1}(f(z + h)) - f^{-1}(f(z))}{f(z + h) - f(z)}$$

je také vlastní, takže f^{-1} je v $f(z)$ holomorfní.

Afinní prostor je zřejmě Hausdorffův, tedy i afinní křivka je Hausdorffův prostor, a nesesingulární afinní křivka je podle Věty 22 Riemannova plocha. Jak dokazuje Kirwan (1992) na straně 42, projektivní křivka v $\mathbb{P}^2$ je rovněž Hausdorffův prostor. Věta 24 tedy říká, že když C je projektivní algebraická křivka v $\mathbb{P}^2$, tak je to Riemannova plocha.

Dále budeme potřebovat následující větu.

Věta 32 (o otevřenosti zobrazení). *Nechť je funkce f nekonstantní a holomorfní na otevřené souvislé množině $G \subset \mathbb{C}$. Pak je f otevřené zobrazení G do $\mathbb{C}$.*

Důkaz. (Veselý, 2000, Věta 5.8.2)

□

Navíc použijeme i větu o jednoznačnosti (Veselý, 2000, Věta 5.7.1). Ta říká, že funkce holomorfní na podmnožině otevřené souvislé množiny se na tuto množinu rozšíří jednoznačně.

Příklad (Kirwan, Cvičení 5.1). Budte R, S Riemannovy plochy a budte $f, g : R \rightarrow S$ holomorfní zobrazení. Nechť navíc R je souvislá a existuje neprázdná otevřená podmnožina $V \subset R$ taková, že pro každé $z \in V$ platí $f(z) = g(z)$. Ukažte, že pak pro všechna $z \in R$ platí $f(z) = g(z)$.

Důkaz. Budte $f, g : R \rightarrow S$ holomorfní zobrazení a označme $V = \{z \in R : \text{existuje okolí } U_z \text{ bodu } z \text{ takové, že } (\forall x \in U_z) f(x) = g(x)\}$. Pokud $z \in V$, pak $\forall u \in U_z$ je $u \in V$, takže je V otevřená. Ukážeme-li, že množina V je uzavřená, pak pokud je V neprázdná, ze souvislosti R plyne $V = R$.

Zvolme $y \in R$ takové, že leží v uzavěru V . Zobrazení f, g jsou spojitá, a protože se rovnají na V , tak $f(y) = g(y)$. Vezmeme nějaké otevřené okolí $Y \subset S$ obrazu $f(y) = g(y)$ a homeomorfismus $\psi : Y \rightarrow \psi(Y)$ z atlasu S a nějaké otevřené okolí W bodu y tak, že $f(W) \subset Y$, $g(W) \subset Y$ a existuje $\phi : W' \rightarrow \phi(W')$, kde $W \subset W'$. Navíc můžeme zvolit W souvislé (stačí to okolí dostatečně zmenšit).

Definujme $\tilde{f} : \psi(W) \rightarrow \phi(Y)$ předpisem $\tilde{f} = \psi \circ f \circ \phi^{-1}$ a $\tilde{g} : \psi(W) \rightarrow \phi(Y)$ předpisem $\tilde{g} = \psi \circ g \circ \phi^{-1}$.

Protože $y \in \overline{V}$, tak má W neprázdný průnik s V . Tedy existuje $z \in V \cap W$. Tedy $f(x) = g(x)$ pro každé $x \in U_z \cap W$. Takže $\tilde{f} : \phi(W) \rightarrow \psi(Y)$ a $\tilde{g} : \phi(W) \rightarrow \psi(Y)$ se shodují na neprázdné otevřené podmnožině $\phi(W)$, a tedy z Věty (Veselý, 2000, Věta 5.7.1) se shodují na celém $\phi(W)$. Tím pádem se f a g shodují na celém W , a protože $W \subset R$ je otevřené okolí bodu y v R , tak z definice V plyne $y \in V$.

□

Příklad (Kirwan, Cvičení 5.2). Nechť R, S jsou Riemannovy plochy, R je souvislá (v obvyklém smyslu jako topologický prostor) a $f : R \rightarrow S$ je nekonstantní holomorfní zobrazení. Ukažte, že $f(R)$ je otevřená v S .

Důkaz. Zvolme $x \in R$ libovolné a označme $y = f(x) \in S$. Pak existují $U \subset R$ otevřená taková, že $x \in U$, $V \subset \mathbb{C}$ otevřená a homeomorfismus $\phi : U \rightarrow V$. Stejně tak existují $W \subset S$ otevřená taková, že $y \in W$, $Y \subset \mathbb{C}$ otevřená a homeomorfismus $\psi : W \rightarrow Y$.

Položme $U' = U \cap f^{-1}(W)$. Definujme $\tilde{f} : \phi(U') \rightarrow \psi(W)$ předpisem $\tilde{f} = \psi \circ f|_{U'} \circ \phi^{-1}$. Zřejmě je $\tilde{f}$ holomorfní zobrazení na $\mathbb{C}$.

Dokážeme nekonstantnost $\tilde{f}$ ze souvislosti R . Použijeme větu o jednoznačnosti (Veselý, 2000, Věta 5.7.1). Kdyby $\tilde{f}$ bylo konstantní, pak by bylo konstantní i zúžení f na U' . Tedy existuje $p \in S$ takové, že $(\forall z \in U') f(z) = p$. Definujme zobrazení $g : R \rightarrow S$ předpisem $(\forall r \in R) g(r) = p$. Zřejmě je g holomorfní. Protože $(\forall x \in U') f(x) = g(x)$, pak se podle cvičení 5.1 shodují f a g na celém R , což je spor s nekonstantností f .

Zvolme $x \in \phi(U')$ a jeho souvislé okolí U'' takové, že $U'' \subset \phi(U')$. Pak $\tilde{f}|_{U''}$ je nekonstantní a holomorfní na souvislé množině U'' , tedy z věty o otevřenosti zobrazení víme, že pro každou otevřenou podmnožinu $G \subset U''$ je $f|_{U''}(G)$ otevřená.

Zvolme $r \in R$ libovolné. Existuje okolí U_r a homeomorfismus $\phi_r : U_r \rightarrow V_r$. Zvolme $V'_r \subset V_r$ tak, aby byla V'_r souvislá a $\phi_r(r) \in V'_r$. Zřejmě je $\phi^{-1}(V'_r)$ otevřená a souvislá. Stejně tak existuje otevřené okolí $W_{f(r)} \subset S$ bodu $f(r)$ a homeomorfismus $\psi : W_{f(r)} \rightarrow \psi(W_{f(r)})$. Položme $W' = W \cap f(\phi^{-1}(V'_r))$. Zvolme souvislé okolí $Y' \subset \psi(W)$ bodu $\psi(y)$. Pak $\psi^{-1}(Y')$ je souvislá a otevřená a platí $f(\psi^{-1}(V_r)) = \psi^{-1}(Y')$. Tedy f zobrazuje otevřené okolí bodu r na otevřenou množinu. Tím pádem je f otevřený. Speciálně $f(R)$ je otevřená v S .

□

Definice 33. Buď (X, τ) Hausdorffův topologický prostor. Řekneme, že $Y \subset X$ je kompaktní, pokud lze z každého otevřeného pokrytí $A \subset \tau$ množiny Y vybrat konečné podpokrytí, tj. existuje $F \subset A$ konečná taková, že $\bigcup F = Y$.

Příklad (Kirwan, Cvičení 5.3). Necht R, S jsou souvislé Riemannovy plochy a R je neprázdná a kompaktní. Buď $f : R \rightarrow S$ nekonstantní holomorfní zobrazení. Pak f je na a S je kompaktní.

Důkaz. Z předchozího příkladu víme, že $f(R)$ je otevřená v S . Protože f je spojitý a R je kompaktní, tak je $f(R)$ kompaktní v S . Navíc je S Hausdorffův prostor, a tedy je každá jeho kompaktní podmnožina uzavřená. Tedy $f(R)$ je otevřená i uzavřená v S . Protože S je souvislý prostor, tak buď $f(R) = \emptyset$, nebo $f(R) = S$. Ale f je nekonstantní a R je neprázdná, tedy $f(R) = S$, tzn. f je na a S je kompaktní.

□

Příklad (Kirwan, Cvičení 5.4). Necht R je kompaktní souvislá Riemannova plocha. Pak neexistuje žádné nekonstantní holomorfní zobrazení $f : R \rightarrow \mathbb{C}$.

Důkaz. Pro spor mějme nekonstantní holomorfní $f : R \rightarrow \mathbb{C}$. Prostor $\mathbb{C}$ je souvislý, a podle předchozího příkladu je tedy f na a $\mathbb{C}$ je kompaktní. Ale množina v $\mathbb{C}$ je kompaktní právě tehdy, když je uzavřená a omezená. $\mathbb{C}$ není omezená, což je spor.

□

3. Eliptické křivky

Buď Λ mříž v $\mathbb{C}$ a definujme g_2 a g_3 jako v Lemmatu 16. Pak označíme C_Λ křivku v $\mathbb{P}^2$ definovanou polynomem

$$Q_\Lambda(x, y, z) = y^2z - 4x^3 + g_2xz^2 + g_3z^3.$$

Lemma 34. *Křivka C_Λ je nesesingulární.*

Důkaz. Položme $\alpha = \wp(\omega_1/2)$, $\beta = \wp(\omega_2/2)$, $\gamma = \wp((\omega_1 + \omega_2)/2)$. Ukážeme, že α , β a γ jsou různá komplexní čísla a že platí vztah

$$Q_\Lambda(x, y, z) = y^2z - 4(x - \alpha z)(x - \beta z)(x - \gamma z). \quad (3.1)$$

Potom $\frac{\partial Q_\Lambda}{\partial y} = 2yz$, tedy pokud $(x : y : z)$ je singulární bod, tak $y = 0$ nebo $z = 0$. Nejprve uvažujme případ $z = 0$. Platí

$$\frac{\partial Q_\Lambda}{\partial x}(x, y, z) = -4(3x^2 - 2xz(\alpha + \beta + \gamma) + z^2(\alpha(\beta + \gamma) + \beta\gamma)),$$

tedy pokud $z = 0$, tak $\partial Q_\Lambda / \partial x = -12x^2$, a tím pádem $x = 0$. Navíc

$$\frac{\partial Q_\Lambda}{\partial z} = y^2 + 4\gamma(x - \alpha z)(x - \beta z) + 4\beta(x - \alpha z)(x - \gamma z) + 4\alpha(x - \beta z)(x - \gamma z),$$

a pokud dosadíme $x = z = 0$, dostaneme $\partial Q_\Lambda / \partial z = y^2$, a tedy $x = y = z = 0$. Ale $(0 : 0 : 0) \notin \mathbb{P}^2$.

Dále rozebereme případ $y = 0$. Protože $(x : 0 : z) \in C_\Lambda$, tak $x = \alpha z$, βz nebo γz . Pokud $x = \alpha z$, tak dosazením do $\partial Q_\Lambda / \partial z$ dostaneme $x = \beta z$ nebo $x = \gamma z$. Tedy pokud $x = \alpha z = \gamma z$, tak protože α a γ jsou různá, platí $x = z = 0$. Analogicky pro $x = \beta z$ a $x = \gamma z$. Ale opět $(0 : 0 : 0) \notin \mathbb{P}^2$.

Tedy stačí ukázat vztah 3.1 a z toho plyne, že C_Λ je nesesingulární. Že α , β a γ jsou různá, plyne ihned z Věty 17. Protože $\wp$ je sudá, dvojitě periodická funkce, tak její derivace je lichá, dvojitě periodická funkce se stejnými periodami ω_1, ω_2 . Tedy stejně jako v důkazu Věty 17 platí

$$\wp'(\omega_1/2) = \wp'(\omega_1/2 - \omega_1) = \wp'(-\omega_1/2) = -\wp'(\omega_1/2).$$

Tím pádem $\wp'(\omega_1/2) = 0$.

Z Lemmatu 16 vyplývá vztah

$$4\alpha^3 - g_2\alpha - g_3 = \wp'(\omega_1/2)^2 = 0,$$

tedy α a analogicky i β a γ jsou kořeny polynomu $4x^3 - g_2x - g_3$. Takže

$$4x^3 - g_2x - g_3 = 4(x - \alpha)(x - \beta)(x - \gamma). \quad (3.2)$$

Odtud už snadno plyne, že

$$Q_\Lambda(x, y, z) = y^2z - 4(x - \alpha z)(x - \beta z)(x - \gamma z),$$

kde α , β , γ jsou různá.

□

Definice 35. *Nesingulární kubickou křivku v $\mathbb{P}^2$ nazveme eliptickou křivkou.*

Podle Lemmatu 34 je C_Λ eliptická křivka. Totéž Lemma navíc využijeme k řešení následujícího příkladu.

Příklad (Kirwan, Cvičení 5.12). Buď Λ mříž v $\mathbb{C}$. Dokažte, že $g_2^3 - 27g_3^2 \neq 0$.

Důkaz. Ze vztahu 3.2 vyplývá, že

$$x^3 - \frac{g_2}{4}x - \frac{g_3}{4} = (x - \alpha)(x - \beta)(x - \gamma).$$

Diskriminant polynomu $x^3 - \frac{g_2}{4}x - \frac{g_3}{4}$ je roven $(g_2^3 - 27g_3^2)/16$, a protože má tento polynom tři různé kořeny, tak je jeho diskriminant nenulový. □

Když Λ je mříž v $\mathbb{C}$, tak $(\Lambda, +) \leq (\mathbb{C}, +)$. Definujme faktorgrupu $\mathbb{C}/\Lambda = \{\Lambda + a : a \in \mathbb{C}\}$. Tato faktorgrupa má topologii indukovanou euklidovskou topologií na $\mathbb{C}$. Buď $\pi : \mathbb{C} \rightarrow \mathbb{C}/\Lambda$ projekce definovaná vztahem $\pi(a) = \Lambda + a$. Pak řekneme, že U je otevřená v $\mathbb{C}/\Lambda$, pokud její vzor $\pi^{-1}(U)$ je otevřená v $\mathbb{C}$.

Množina $P = \{s\omega_1 + t\omega_2 : s, t \in [0, 1]\}$ je kompaktní v $\mathbb{C}$ a restrikce π na P je surjektivní. Tedy $\mathbb{C}/\Lambda$ je kompaktní. Protože $\mathbb{C}/\Lambda$ můžeme ztotožnit s rovnoběžníkem P , kterému navíc „slepíme“ protější strany, budeme $\mathbb{C}/\Lambda$ nazývat komplexním torem.

Definujme zobrazení $u : \mathbb{C}/\Lambda \rightarrow \mathbb{P}^2$ předpisem

$$u(\Lambda + z) = \begin{cases} (\wp(z) : \wp'(z) : 1), & \text{je-li } z \notin \Lambda, \\ (0 : 1 : 0), & \text{je-li } z \in \Lambda. \end{cases}$$

Je-li $z_1 \neq z_2$, ale $\Lambda + z_1 = \Lambda + z_2$ a navíc $z_1, z_2 \notin \Lambda$, pak existuje $\zeta \in \Lambda$ takové, že $z_1 = z_2 + \zeta$. Tedy z Lemmatu 12 plyne

$$u(\Lambda + z_1) = (\wp(z_1) : \wp'(z_1) : 1) = (\wp(z_2) : \wp'(z_2) : 1) = u(\Lambda + z_2).$$

Jsou-li $z_1 \neq z_2$, ale $z_1, z_2 \in \Lambda$, pak $u(z_1) = (0 : 1 : 0) = u(z_2)$.

Tedy $u : \mathbb{C}/\Lambda \rightarrow \mathbb{P}^2$ je dobře definované zobrazení. Dosadíme-li souřadnice $u(\Lambda + z)$ do rovnice Q_Λ , dostaneme

$$Q_\Lambda(\wp(z), \wp'(z), 1) = \wp'(z)^2 - 4\wp(z)^3 + g_2\wp(z) + g_3$$

a výraz na pravé straně je podle Lemmatu 16 roven nule. Tedy $u(\Lambda + z) \in C_\Lambda$.

Věta 36. *Zobrazení $u : \mathbb{C}/\Lambda \rightarrow C_\Lambda$ je homeomorfismus.*

Důkaz. Chceme ukázat, že u je spojitá bijekce a že u^{-1} je spojitý. Nejprve ověříme, že u je prosté. Budte $z, w \in \mathbb{C} \setminus \Lambda$ a $u(z) = u(w)$. Pak $\wp(z) = \wp(w)$, tedy podle Věty 17 platí $z \in \Lambda \pm w$. Chceme ukázat, že $z \in \Lambda + w$. Ať $z \in \Lambda - w$. Protože $\wp'$ je lichá, dvojitě periodická funkce, tak $\wp'(z) = -\wp'(w)$. Ale z toho, že $u(z) = u(w)$, plyne $\wp'(z) = \wp'(w)$. Tedy $\wp'(z) = \wp'(w) = 0$. Z důkazu Lemmatu 34 je vidět, že když $\wp'(w) = 0$, tak $\wp(w)$ je rovno α , β , nebo γ , kde $\alpha = \wp(\omega_1/2)$, $\beta = \wp(\omega_2/2)$, $\gamma = \wp((\omega_1 + \omega_2)/2)$. Potom z Věty 17 plyne $w \in \frac{1}{2}\Lambda$, tj. $\Lambda + w = \Lambda - w$. Tedy $z \in \Lambda + w$ a ukázali jsme, že u je prosté.

Ted dokážeme, že u je na. Buď $(a : b : c) \in C_\Lambda$. Když $c = 0$, tak z definice C_Λ je nutně $a = 0$, tedy $(a : b : c) = (0 : 1 : 0)$. V opačném případě můžeme předpokládat, že $c = 1$. Pak z Věty 17 existuje $z \in \mathbb{C}$ takové, že $\wp(z) = a$. Z Lemmatu 16 a předpokladu $(a : b : c) \in C_\Lambda$ plyne

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3 = 4a^3 - g_2a - g_3 = b^2.$$

Tedy $\wp'(z) = \pm b$. Protože $\wp'$ je lichá funkce, tak buď $u(\Lambda + z) = (a : b : 1)$, nebo $u(\Lambda - z) = (a : b : 1)$. Takže u je na.

Na $\mathbb{C} \setminus \Lambda$ jsou $\wp$ a $\wp'$ holomorfní, a tedy spojité. Takže u je zřejmě spojitá s jedinou možnou výjimkou v $\Lambda + 0$. Protože $\wp$ má v nule pól násobnosti 2 a $\wp'$ pól násobnosti 3, tak platí $\wp(z) = g(z)/z^2$, $\wp'(z) = h(z)/z^3$, kde g a h jsou holomorfní na okolí nuly a $g(0) \neq 0 \neq h(0)$. Tedy když z je v nějakém prstencovém okolí nuly, tak platí

$$u(\Lambda + z) = (\wp(z) : \wp'(z) : 1) = \left(\frac{g(z)}{z^2} : \frac{h(z)}{z^3} : 1\right) = (zg(z) : h(z) : z^3).$$

Tím pádem, když z jde k nule, tak $u(\Lambda + z)$ jde k $(0 : 1 : 0)$. Takže u je v nule spojitá.

Ukázali jsme, že u je spojitá bijekce. Zbývá dokázat, že u^{-1} je spojitá. K tomu budeme potřebovat následující lemma.

Lemma 37. *Budte X, Y topologické prostory a $f : X \rightarrow Y$. Je-li X kompaktní, Y Hausdorffův a f spojitá bijekce, pak f je otevřené zobrazení z X do Y .*

Důkaz. Ať U je otevřená v X . Tedy U^C je uzavřená v X . Protože X je kompaktní a U^C uzavřená, tak U^C je kompaktní v X . Protože f je spojitá, tak $f(U^C)$ je kompaktní v Y . Protože Y je Hausdorffův a $f(U^C)$ kompaktní, tak $f(U^C)$ je v Y uzavřená. Platí $f(U^C) = (f(U))^C$. Takže $(f(U))^C$ je uzavřená, tedy $f(U)$ je otevřená. Tedy f je otevřené zobrazení. □

Protože $\mathbb{C}/\Lambda$ je kompaktní a C_Λ je Hausdorffův, tak $u : \mathbb{C}/\Lambda \rightarrow C_\Lambda$ je otevřené. Ať G je otevřená v $\mathbb{C}/\Lambda$. Chceme ukázat, že $(u^{-1})^{-1}(G)$ je otevřená v C_Λ . Protože u je bijekce, tak $(u^{-1})^{-1}(G) = u(G)$. Ale u je otevřené, tedy $u(G)$ je otevřená v C_Λ .

Tedy u^{-1} je spojitá, a tím pádem je u homeomorfismus. □

C_Λ je Hausdorffův prostor, a protože $u : \mathbb{C}/\Lambda \rightarrow C_\Lambda$ je homeomorfismus, tak je $u^{-1} : C_\Lambda \rightarrow \mathbb{C}/\Lambda$ také homeomorfismus. Homeomorfní obraz Hausdorffova prostoru je Hausdorffův, tedy $\mathbb{C}/\Lambda$ je Hausdorffův prostor. Abychom ukázali, že $\mathbb{C}/\Lambda$ je Riemannova plocha, stačí najít holomorfní atlas.

Z Lemmatu 9 víme, že existuje $\delta > 0$ takové, že $|n\omega_1 + m\omega_2| \geq \delta$ pro libovolná celá čísla n, m obě nenulová. Když $a \in \mathbb{C}$, tak zúžení projekce $\pi : \mathbb{C} \rightarrow \mathbb{C}/\Lambda$ na množinu $U_a = \{z \in \mathbb{C} : |z - a| < \delta/2\}$ je homeomorfismus na množinu $\pi(U_a)$ otevřenou v $\mathbb{C}/\Lambda$. Je-li $\pi(U_a) \cap \pi(U_b) \neq \emptyset$, pak existuje právě jeden mřížový bod $n\omega_1 + m\omega_2 \in \Lambda$ takový, že $|n\omega_1 + m\omega_2 + a - b| < \delta/2$. Tedy zobrazení

$$(\pi|_{U_b})^{-1} \circ \pi|_{U_a \cap \pi^{-1}(\pi(U_b))} : U_a \cap \pi^{-1}(\pi(U_b)) \rightarrow U_a$$

je translace. Tudiž mapy $\{\phi_a = (\pi|_{U_a})^{-1} : \pi(U_a) \rightarrow U_a : a \in \mathbb{C}\}$ tvoří holomorfní atlas na $\mathbb{C}/\Lambda$.

Věta 38. *Homeomorfismus $u : \mathbb{C}/\Lambda \rightarrow C_\Lambda$ je holomorfní ve smyslu definice 26.*

Důkaz. Buď $\Lambda + w \in \mathbb{C}/\Lambda$. Chceme ukázat, že $\psi_\beta \circ u \circ \psi_\alpha^{-1} : \psi_\alpha(U_\alpha \cap u^{-1}(W_\beta)) \rightarrow Y_\beta$ je holomorfní v obvyklém smyslu pro nějaké holomorfní mapy $\psi_\alpha : U_\alpha \rightarrow V_\alpha$ na $\mathbb{C}/\Lambda$ a $\psi_\beta : W_\beta \rightarrow Y_\beta$ na C_Λ takové, že $\Lambda + w \in U_\alpha$ a $u(\Lambda + w) \in W_\beta$.

Zvolme V_α jako dostatečně malou otevřenou kouli v $\mathbb{C}$ a položme $U_\alpha = \pi(V_\alpha)$. Za ψ_α můžeme zvolit inverzní zobrazení k π .

Když $w \notin \Lambda$, tak $u(\Lambda + w) = (\wp(z) : \wp'(z) : 1)$, tedy z důkazu Věty 24 vyplývá, že můžeme za ψ_β zvolit buď $(x : y : z) \mapsto x/z$, nebo $(x : y : z) \mapsto y/z$. Tedy $\psi_\beta \circ u \circ \phi_\alpha^{-1}$ je zúžení buď $\wp$, nebo $\wp'$, ale obě funkce jsou holomorfní na okolí w .

Když $w \in \Lambda$, tak $u(\Lambda + w) = (0 : 1 : 0)$, a opět z důkazu Věty 24 můžeme za ψ_β zvolit $(x : y : z) \mapsto x/y$, protože $\frac{\partial Q_\Lambda}{\partial z}(0, 1, 0) \neq 0$. Tedy

$$\psi_\beta \circ u \circ \phi_\alpha^{-1}(z) = \begin{cases} \wp(z)/\wp'(z), & \text{je-li } z \notin \Lambda, \\ 0, & \text{je-li } z \in \Lambda. \end{cases}$$

Tato funkce je holomorfní na okolí nuly (a z dvojité periodicity na okolí každého mřížového bodu), protože $\wp$ má v nule pól, stejně jako $\wp'$.

Tedy u je holomorfní ve smyslu definice 26. □

Z diskuze za definicí 31 vyplývá, že i u^{-1} je holomorfní. Tedy plochy $\mathbb{C}/\Lambda$ a C_Λ jsou biholomorfní.

Tvrzení 39 (Kirwan, Cvičení 5.13). *Budte $\Lambda, \tilde{\Lambda}$ mříže v $\mathbb{C}$ a necht $F : \mathbb{C}/\Lambda \rightarrow \mathbb{C}/\tilde{\Lambda}$ je holomorfní zobrazení. Pak existují $a, b \in \mathbb{C}$ taková, že $a\Lambda \subset \tilde{\Lambda}$, a pro každé $x \in \mathbb{C}$ platí $F(\Lambda + x) = \tilde{\Lambda} + (ax + b)$.*

Důkaz. Označme $\pi : \mathbb{C} \rightarrow \mathbb{C}/\Lambda$ a $\tilde{\pi} : \mathbb{C} \rightarrow \mathbb{C}/\tilde{\Lambda}$ přirozené projekce, tj. $\pi(z) = \Lambda + z$, $\tilde{\pi}(z) = \tilde{\Lambda} + z$.

Zvolme $\tilde{z} \in \mathbb{C}$ libovolné a nalezneme jeho okolí $U_{\tilde{z}} \subset \mathbb{C}$ takové, že $\tilde{\pi}|_{U_{\tilde{z}}} : U_{\tilde{z}} \rightarrow \tilde{\pi}(U_{\tilde{z}})$ je homeomorfismus. Potom existuje $\tilde{\psi} : \tilde{\pi}(U_{\tilde{z}}) \rightarrow U_{\tilde{z}}$ takové, že $\tilde{\pi} \circ \tilde{\psi} = id_{\tilde{\pi}(U_{\tilde{z}})}$.

Toto $\tilde{\psi}$ je určené až na konstantu z $\tilde{\Lambda}$. Vezmeme $\tilde{z} \in \mathbb{C}$ libovolné a jeho otevřené okolí U takové, že $\tilde{\pi}|_U : U \rightarrow \tilde{\pi}(U)$ je homeomorfismus a U je souvislé. Uvažujme libovolná $\psi_1, \psi_2 : \tilde{\pi}(U) \rightarrow \mathbb{C}$ spojitá tak, že $\tilde{\pi} \circ \psi_1 = \tilde{\pi} \circ \psi_2$. Pak existuje konstanta $\tilde{\lambda} \in \tilde{\Lambda}$ taková, že pro každé $\tilde{\Lambda} + x \in \tilde{\pi}(U)$ je $\psi_1(\tilde{\Lambda} + x) = \psi_2(\tilde{\Lambda} + x) + \tilde{\lambda}$.

Definujme totiž zobrazení $\delta : \tilde{\pi}(U) \rightarrow \mathbb{C}$ předpisem $\delta(\tilde{\Lambda} + x) = \psi_1(\tilde{\Lambda} + x) - \psi_2(\tilde{\Lambda} + x)$. Pro každé $\tilde{\Lambda} + x$ se $\psi_1(\tilde{\Lambda} + x)$ a $\psi_2(\tilde{\Lambda} + x)$ liší o nějakou konstantu z $\tilde{\Lambda}$, takže obraz δ je obsažen v diskrétní množině $\tilde{\Lambda}$. Množina U je souvislá a $\tilde{\pi}(U)$ je homeomorfní U , takže je $\tilde{\pi}(U)$ také souvislá. Zobrazení δ je spojitě, takže je obraz $\tilde{\pi}(U)$ při zobrazení δ taktéž souvislý. Protože obraz δ leží v $\tilde{\Lambda}$, což je izolovaná množina, tak je obraz δ jednoprvkový. Tím je dokázána jednoznačnost $\tilde{\psi}$ až na konstantu.

Zvolme $z \in \mathbb{C}$ libovolné. K němu nalezneme $\tilde{z} \in \mathbb{C}$ takové, že $F(\pi(z)) = F(\Lambda + z) = \tilde{\Lambda} + \tilde{z}$. K tomuto $\tilde{z}$ nalezneme okolí $U_{\tilde{z}}$ jako ve druhém odstavci důkazu.

Ze spojitosti F nalezneme okolí $U_z \subset \mathbb{C}$ bodu z takové, že $(F \circ \pi)(U_z) \subset \tilde{\pi}(U_{\tilde{z}})$. Definujme zobrazení $G_z : U_z \rightarrow \tilde{\psi}(\tilde{\pi}(U_{\tilde{z}}))$ vztahem $G_z = \tilde{\psi} \circ F \circ \pi$, kde $\tilde{\psi}$ je jako ve druhém odstavci důkazu. Funkce G_z je holomorfní a určená jednoznačně až na přičtení konstanty $\tilde{\lambda} \in \tilde{\Lambda}$. Tato nejednoznačnost je způsobená výběrem $\tilde{\psi}$.

Uvažujme derivaci $G'_z : U_z \rightarrow \tilde{\psi}(\tilde{\pi}(U_{\tilde{z}}))$. Konstanta se zderivuje na nulu, tedy je G'_z určená jednoznačně.

Buď $z \in \mathbb{C}$, $\lambda \in \Lambda$ a označme $y = z + \lambda$. Chceme ukázat, že $G'_z(z) = G'_y(y)$. Dosazením do definice dostáváme $G_z = \psi_z \circ F \circ \pi : U_z \rightarrow \mathbb{C}$, $G_y = \psi_y \circ F \circ \pi : U_y \rightarrow \mathbb{C}$, kde ψ_z, ψ_y jsou inverze k π jako ve druhém odstavci důkazu. Z definice π plyne $\pi(z) = \Lambda + z = \Lambda + y = \pi(y)$, speciálně $\tilde{\Lambda} + \tilde{z} = F(\lambda + z) = F(\lambda + y) = \tilde{\Lambda} + \tilde{y}$. Položme $V = \tilde{\pi}(U_{\tilde{z}}) \cap \tilde{\pi}(U_{\tilde{y}})$; pak V je otevřené okolí $\tilde{\Lambda} + \tilde{z} = \tilde{\Lambda} + \tilde{y}$. Podle jednoznačnosti až na konstantu výše existuje $\tilde{\lambda} \in \tilde{\Lambda}$ taková, že pro každé $x \in V$ je $\psi_z(x) = \psi_y(x) + \tilde{\lambda}$. Dosazením do definic G_z, G_y dostáváme $G_z(x) = G_y(x + \lambda) + \tilde{\lambda}$ pro každé $x \in U_z \cap (U_y - \lambda)$. Zderivováním dostaneme požadovanou rovnost $G'_z(z) = G'_y(y)$.

Definujme funkci $G' : \mathbb{C} \rightarrow \mathbb{C}$ předpisem $G'(x) = G'_z(x)$, pokud $x \in U_z$. Dokážeme korektnost definice. Zvolme $x \in \mathbb{C}$ libovolné. Buďte $z_1, z_2 \in \mathbb{C}$, $z_1 \neq z_2$ taková, že $x \in U_{z_1} \cap U_{z_2}$. Pak existuje konstanta $\tilde{\lambda} \in \tilde{\Lambda}$ taková, že pro každé $x \in U_{z_1} \cap U_{z_2}$ platí $G_{z_1}(x) = G_{z_2}(x) + \tilde{\lambda}$. Tedy $G'_{z_1}(x) = G'_{z_2}(x)$ pro každé $x \in U_{z_1} \cap U_{z_2}$.

Zvolme $z \in \mathbb{C}$, $\lambda \in \Lambda$ a označme $y = z + \lambda$. Jak jsme dokázali výše, platí $G'(z) = G'_z(z) = G'_y(y) = G'(y)$. Tedy je G' dvojité periodická vzhledem k mříži Λ . Navíc je zřejmě holomorfní a podle Lemmatu 15 je G' konstantní.

Funkce G' je na $\mathbb{C}$ konstantní. Tedy pro každé $z \in \mathbb{C}$ je G_z restrikce lineárního zobrazení, tzn. existuje b_z takové, že $G_z(x) = ax + b_z$. Takže pro každé $x \in \mathbb{C}$ platí $\tilde{\psi} \circ F \circ \pi(x) = ax + b_z$. Když obě strany rovnosti složíme s $\tilde{\pi}$, dostáváme $\tilde{\pi} \circ \tilde{\psi} \circ F \circ \pi(x) = \tilde{\pi}(ax + b_z)$, a protože $\tilde{\pi} \circ \tilde{\psi} = id$, tak $F \circ \pi(x) = \tilde{\pi}(ax + b_z)$, tedy $F(\Lambda + x) = \tilde{\Lambda} + (ax + b_z)$.

Zvolme $z_1, z_2 \in \mathbb{C}$, $z_1 \neq z_2$ taková, že $U_{z_1} \cap U_{z_2} \neq \emptyset$. Pro každé $x \in U_{z_1} \cap U_{z_2}$ je hodnota $F \circ \pi(x)$ určena jednoznačně, tedy existuje $\tilde{\lambda} \in \tilde{\Lambda}$ takové, že $b_{z_1} + \tilde{\lambda} = b_{z_2}$. Takže můžeme zvolit libovolné $z \in \mathbb{C}$ a položit $b = b_z$. Pak pro $z_1 \in \mathbb{C}$ libovolné existuje $\tilde{\lambda} \in \tilde{\Lambda}$ takové, že platí $F(\Lambda + z_1) = \tilde{\Lambda} + (az_1 + b_{z_1}) = \tilde{\Lambda} + (az_1 + b + \tilde{\lambda}) = \tilde{\Lambda} + (az_1 + b)$.

Zbývá dokázat, že $a\Lambda \subset \tilde{\Lambda}$. Buď $z \in \Lambda$. Pak $\tilde{\Lambda} + b = F(\Lambda) = F(\Lambda + z) = \tilde{\Lambda} + (az + b)$, tedy $az \in \tilde{\Lambda}$.

□

V předešlém příkladu navíc platí, že zobrazení F je invertibilní právě tehdy, když $a\Lambda = \tilde{\Lambda}$ a navíc $a \neq 0$. Pokud platí $a\Lambda \subsetneq \tilde{\Lambda}$, pak existuje nějaké $\tilde{\lambda} \in \tilde{\Lambda}$ takové, že $\tilde{\lambda}/a \notin \Lambda$, ale $F(\Lambda + \tilde{\lambda}/a) = \tilde{\Lambda} + b = F(\Lambda)$. Pokud $a\Lambda = \tilde{\Lambda}$, pak $\Lambda = (1/a)\tilde{\Lambda}$ a zobrazení $F^* : \mathbb{C}/\tilde{\Lambda} \rightarrow \mathbb{C}/\Lambda$ zadané předpisem $F^*(\tilde{\Lambda} + \tilde{\lambda}) = \tilde{\Lambda} + (\tilde{\lambda} - b)/a$ je inverzní k F .

Příklad (Kirwan, Cvičení 5.14). Buďte $\Lambda, \tilde{\Lambda}$ mříže v $\mathbb{C}$. Uvažujme křivky $C_\Lambda, C_{\tilde{\Lambda}}$. Ukažte, že existuje projektivní transformace $\mathbb{P}^2(\mathbb{C})$ daná diagonální maticí zobrazující C_Λ na $C_{\tilde{\Lambda}}$ právě tehdy, když $J(C_\Lambda) = J(C_{\tilde{\Lambda}})$, kde

$$J(C_\Lambda) = \frac{g_2^3}{g_2^3 - 27g_3^2}.$$

Důkaz. Jak víme ze cvičení 5.12 (první příklad za definicí 35), $g_2^3 - 27g_3^2 \neq 0$, takže je definice $J(C_\Lambda)$ korektní.

Transformace $\mathbb{P}^2(\mathbb{C})$ diagonální maticí jsou zobrazení $f : \mathbb{P}^2(\mathbb{C}) \rightarrow \mathbb{P}^2(\mathbb{C})$ tvaru $f((x : y : z)) = (ax : by : cz)$, kde $a, b, c \in \mathbb{C} \setminus \{0\}$.

Ať existuje projektivní transformace $\mathbb{P}^2(\mathbb{C})$ tvaru $f((x : y : z)) = (ax : by : cz)$, $a, b, c \in \mathbb{C} \setminus \{0\}$. BÚNO můžeme předpokládat, že $c = 1$ (toho lze docílit vhodnou volbou homogenních souřadnic). Dosadíme $(ax : by : z)$ do polynomu Q_Λ a porovnáme koeficienty s polynomem $Q_{\tilde{\Lambda}}$. Dostaneme $a^3 = b^2$, $ag_2 = b^2\tilde{g}_2$ a $g_3 = b^2\tilde{g}_3$. Položme $t = b/a$, pak $a = t^2$, $b = t^3$, $g_2 = t^4\tilde{g}_2$, $g_3 = t^6\tilde{g}_3$. Tedy:

$$J(C_\Lambda) = \frac{(t^4\tilde{g}_2)^3}{(t^4\tilde{g}_2)^3 - 27(t^6\tilde{g}_3)^2} = \frac{t^{12}\tilde{g}_2^3}{t^{12}\tilde{g}_2^3 - 27t^{12}\tilde{g}_3^2} = J(C_{\tilde{\Lambda}}).$$

Naopak předpokládejme, že $J(C_\Lambda) = J(C_{\tilde{\Lambda}})$. Tedy:

$$\begin{aligned} \frac{g_2^3}{g_2^3 - 27g_3^2} &= \frac{\tilde{g}_2^3}{\tilde{g}_2^3 - 27\tilde{g}_3^2} \\ g_2^3(\tilde{g}_2^3 - 27\tilde{g}_3^2) &= \tilde{g}_2^3(g_2^3 - 27g_3^2) \\ g_2^3\tilde{g}_2^3 - 27g_2^3\tilde{g}_3^2 &= g_2^3\tilde{g}_2^3 - 27\tilde{g}_2^3g_3^2, \end{aligned}$$

odečteme $g_2^3\tilde{g}_2^3$ od obou stran rovnice, vydělíme -27 a dostaneme $g_2^3\tilde{g}_3^2 = \tilde{g}_2^3g_3^2$.

Tím pádem když $g_2 = 0$, tak $J(C_\Lambda) = 0$, a tedy $J(C_{\tilde{\Lambda}}) = 0$, a musí být $\tilde{g}_2 = 0$. Opačná implikace je analogická, a tedy $g_2 = 0$ právě tehdy, když $\tilde{g}_2 = 0$. Když $g_3 = 0$, pak buď $g_2 = 0$, nebo $\tilde{g}_3 = 0$. Kdyby $g_2 = 0$, pak $g_2^3 - 27g_3^2 = 0$, což nelze. Tedy $\tilde{g}_3 = 0$. Opačná implikace je opět analogická, takže $g_3 = 0$ právě tehdy, když $\tilde{g}_3 = 0$.

Na začátku uvažujeme případ, kdy $g_2, \tilde{g}_2, g_3, \tilde{g}_3$ jsou všechny nenulové. Pak $(\tilde{g}_3/g_3)^2 = (\tilde{g}_2/g_2)^3$. Položme $t = \sqrt[3]{(\tilde{g}_3/g_3)/(\tilde{g}_2/g_2)}$. Pak $\tilde{g}_3/g_3 = t^6$ a $\tilde{g}_2/g_2 = t^4$. Tedy $\tilde{g}_3 = t^6g_3$ a $\tilde{g}_2 = t^4g_2$. Je-li $(x : y : z) \in C_\Lambda$, pak $y^2z = x^3 - g_2xz^2 - g_3z^3$. Vynásobíme obě strany rovnosti t^6 a dostaneme $(t^3y)^2z = (t^2x)^3 - \tilde{g}_2(t^2x)z^2 - \tilde{g}_3z^3$, tedy $(t^2x : t^3y : z) \in C_{\tilde{\Lambda}}$.

Pokud $g_2 = \tilde{g}_2 = 0$ a $g_3, \tilde{g}_3$ jsou nenulová, položme $t = \sqrt[6]{\tilde{g}_3/g_3}$. Opět platí $\tilde{g}_3 = t^6g_3$ a $\tilde{g}_2 = t^4g_2$ a zbytek jako v předchozím případě.

Pokud $g_3 = \tilde{g}_3 = 0$ a $g_2, \tilde{g}_2$ jsou nenulová, tak položme $t = \sqrt[4]{\tilde{g}_2/g_2}$ a situace je analogická předchozímu případu.

□

Věta 40 (Kirwan, Cvičení 5.15). *Budte $\Lambda, \tilde{\Lambda}$ mříže v $\mathbb{C}$. Ukažte, že následující tvrzení jsou ekvivalentní.*

- (i) $\mathbb{C}/\Lambda$ je biholomorfní $\mathbb{C}/\tilde{\Lambda}$.
- (ii) Existuje $a \in \mathbb{C} \setminus \{0\}$ takové, že $\Lambda = a\tilde{\Lambda}$.
- (iii) $J(C_\Lambda) = J(C_{\tilde{\Lambda}})$

Důkaz. (i) $\implies$ (ii): Zobrazení $F : \mathbb{C}/\Lambda \rightarrow \mathbb{C}/\tilde{\Lambda}$ je holomorfní bijekce. Tedy podle Tvrzení 39 existují $a, b \in \mathbb{C}$ taková, že pro každé $x \in \mathbb{C}$ je $F(\Lambda + x) = \tilde{\Lambda} + (ax + b)$

a navíc $a\Lambda \subset \tilde{\Lambda}$. Protože F má holomorfní inverz, tak platí $a\Lambda = \tilde{\Lambda}$, jak víme z odstavce za tímto tvrzením. Kdyby $a = 0$, tak $a\Lambda = \{0\}$, což nelze.

(ii) $\implies$ (iii): Pro každé $\lambda \in \Lambda$ existuje právě jedno $\tilde{\lambda} \in \tilde{\Lambda}$ takové, že $\lambda = a\tilde{\lambda}$. Tedy platí:

$$\begin{aligned} g_2 &= 60 \sum_{\lambda \in \Lambda \setminus \{0\}} \lambda^{-4} = 60 \sum_{\lambda \in \Lambda \setminus \{0\}} a^4 a^{-4} \lambda^{-4} = a^4 60 \sum_{a\lambda \in \Lambda \setminus \{0\}} (a\lambda)^{-4} \\ &= a^4 60 \sum_{\tilde{\lambda} \in \tilde{\Lambda} \setminus \{0\}} \tilde{\lambda}^{-4} = a^4 \tilde{g}_2. \end{aligned}$$

Analogicky dostaneme $g_3 = a^6 \tilde{g}_3$, a tudíž

$$J(C_\Lambda) = \frac{g_2^3}{g_2^3 - 27g_3^2} = \frac{(a^4 \tilde{g}_2)^3}{(a^4 \tilde{g}_2)^3 - 27(a^6 \tilde{g}_3)^2} = \frac{a^{12} \tilde{g}_2^3}{a^{12} \tilde{g}_2^3 - a^{12} 27 \tilde{g}_3^2} = J(C_{\tilde{\Lambda}}).$$

(iii) $\implies$ (i): Podle předešlého cvičení existuje transformace $\mathbb{P}^2(\mathbb{C})$ daná diagonální maticí, označme ji d . Uvažujeme zobrazení $u_\Lambda : \mathbb{C}/\Lambda \rightarrow C_\Lambda$, $u_{\tilde{\Lambda}} : \mathbb{C}/\tilde{\Lambda} \rightarrow C_{\tilde{\Lambda}}$ tak, jak byla definovaná před Větou 36. Z Věty 38 víme, že u_Λ i $u_{\tilde{\Lambda}}$ jsou biholomorfní. Uvažujme zobrazení $u_{\tilde{\Lambda}}^{-1} \circ d \circ u_\Lambda : \mathbb{C}/\Lambda \rightarrow \mathbb{C}/\tilde{\Lambda}$. To je zřejmě holomorfní a jeho inverzní zobrazení $u_\Lambda^{-1} \circ d^{-1} \circ u_{\tilde{\Lambda}}$ je taktéž holomorfní. Tedy $\mathbb{C}/\Lambda$ je biholomorfní $\mathbb{C}/\tilde{\Lambda}$.

□

Závěr

Ve větě 38 jsme ukázali, že eliptická křivka tvaru C_Λ je biholomorfní komplexnímu toru. Dá se navíc ukázat, že lze v $\mathbb{P}^2(\mathbb{C})$ definovat změnu souřadnic takovou, že převede libovolný nesesingulární homogenní polynom stupně tři do tvaru Q_Λ (Kirwan, 1992, Corollary 3.34), a ke koeficientům g_2, g_3 lze nalézt mříž Λ v $\mathbb{C}$ takovou, aby platily rovnice v Lemmatu 16. Weierstrassova $\wp$ -funkce této mříže výslednou křivku parametrizuje, a tedy je libovolná eliptická křivka v $\mathbb{P}^2(\mathbb{C})$ biholomorfní komplexnímu toru (Kirwan, 1992, Cvičení 6.13, 6.14).

Navíc jsme ve větě 40 dokázali, že dvě mříže v $\mathbb{C}$ určují biholomorfní tory právě tehdy, když jsou stejnohlé. Hodnota $J(C_\Lambda)$ z bodu iii této věty, tzv. j -invariant, je důležitý nástroj při zkoumání eliptických křivek.

Tento invariant je navíc speciální případ modulární formy – analytické funkce na horní polorovině komplexní roviny splňující určitou funkcionální rovnici. Modulární formy se objevují v mnoha odvětvích matematiky, ale například i v teorii strun.

Seznam použité literatury

- KIRWAN, F. (1992). *Complex algebraic curves*. First published. Cambridge University press, Cambridge. ISBN 0 521 41251 X.
- VESELÝ, J. (2000). *Komplexní analýza pro učitele*. 1. Vydání. Nakladatelství Karolinum, Praha. ISBN 80-246-0202-4.
- WASHINGTON, L. C. (2008). *Elliptic Curves: Number Theory and Cryptography*. Second edition. Taylor & Francis Group, University of Maryland. ISBN 978-1-4200-7146-7.