CHALMERS

GÖTEBORGS UNIVERSITET

Uniformisering av elliptiska kurvor

Examensarbete för kandidatexamen i matematik vid Göteborgs universitet

Tomas Forssmark
Douglas Molin

Institutionen för Matematiska vetenskaper
CHALMERS TEKNISKA HÖGSKOLA
GÖTEBORGS UNIVERSITET
Göteborg, Sverige 2019

Uniformisering av elliptiska kurvor

Examensarbete för kandidatexamen i matematik vid Göteborgs universitet

Tomas Forssmark Douglas Molin

Handledare: Per Salberger
Examinator: Maria Roginskaya & Ulla Dinger

Institutionen för Matematiska vetenskaper
CHALMERS TEKNISKA HÖGSKOLA
GÖTEBORGS UNIVERSITET
Göteborg, Sverige 2019

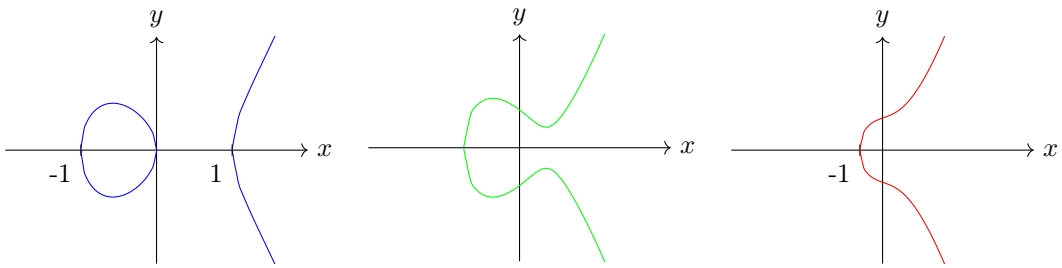
Populärvetenskaplig presentation

Kurvor definierade av polynomekvationer har intresserat matematiker i århundraden. Ekvationer kan se ut på många sätt. Denna uppsats handlar om en speciell typ av kurva som blivit centralgestalt inom den moderna matematiken. Bland annat användes de på 90-talet för att bevisa Fermats stora sats, ett av matematikens mest berömda problem. De går under namnet *elliptiska kurvor*, inte att förväxla med ellipser.

Vad är en elliptisk kurva? Det kan beskrivas på flera sätt. Ett av dessa är genom en ekvation på formen

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

där a och b är fixa tal. Olika val av a och b svarar mot olika ekvationer, och därmed olika kurvor. En lösning består av två tal x och y så att ekvationen uppfylls. Varje sådant par kan nu tolkas som koordinater i xy-planet och ritar vi allihop får vi en kurva.

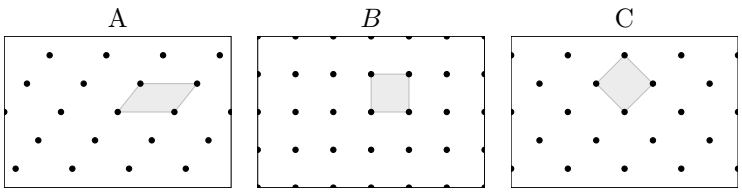


$y^2 = x^3 - x$ $\quad$ $y^2 = x^3 - \frac{3}{2}x + 1$ $\quad$ $y^2 = x^3 + x + 2$

Figur 1: Några exempel på elliptiska kurvor och deras ekvationer.

Målet med denna uppsats är att betrakta samlingen av alla elliptiska kurvor på en gång och försöka hitta en övergripande struktur. Det visar sig att en elliptisk kurva på sätt och vis är samma sak som ett *gitter*. Detta kallas för uniformisering av elliptiska kurvor, vilket är denna uppsats titel.

Vad är då ett gitter? Det är i kontrast till elliptiska kurvor ett relativt enkelt objekt. Vad ett gitter är kan förklaras genom att tänka sig ett kaklat golv med skeva plattor (parallellogram). Gittret är hörnpunkterna där plattorna möts, som punkterna i figur 2.



Figur 2: Tre exempel på gitter i planet.

Vissa par av gitter är mer lika än andra. Exempelvis i figur 2 är gitter C likadant som gitter B om man snurrar det 45° mot- eller medurs. Å andra sidan så kan man inte på något sätt snurra eller skala gitter A för att få gitter B eller C. Matematiskt så är B och C väsentligen samma gitter, men A är ett helt annat.

I denna uppsats visar vi att det i princip finns lika många olika (i det avseende som beskrivs ovan) gitter som det finns olika elliptiska kurvor. Tack vare detta kan vi dra slutsatser om kurvans ekvation genom att istället titta på ett motsvarande gitter. Detta gör att vi kan omformulera svåra frågor om kurvor till enkla frågor om kakelplattor.

Sammanfattning

I denna uppsats formuleras och bevisas Uniformiseringssatsen för elliptiska kurvor över $\mathbb{C}$. Detta resultat är av betydelse för klassificering av komplexa algebraiska kurvor samt studiet av diofantiska ekvationer. Beviset bygger på teorin för elliptiska funktioner, särskilt Weierstrass $\wp$-funktion. I sista kapitlet undersöks förhållandet mellan den analytiska och den algebraiska beskrivningen av elliptiska kurvor vidare. Dessutom dras slutsatser om ändliga delgrupper och endomorfiringar.

Abstract

In this paper the Uniformization theorem for elliptic curves over $\mathbb{C}$ is formulated and proved. This is an important result for the classification of complex algebraic curves and the study of Diophantine equations. The proof relies on the theory of elliptic functions, in particular Weierstrass' $\wp$-function. In the last chapter, we further examine the relation between the algebraic and the analytic description of elliptic curves. In addition, we draw conclusions concerning finite subgroups and endomorphism rings.

Innehåll

Förord

Denna uppsats har skrivits i syfte att presentera klassisk teori på ett tillgänligt och läsarvänligt sätt. Uppsatsen behandlar Uniformiseringssatsen och framställningen följer Silverman och Sutherland (se bibliografi). Läsaren förväntas vara bekant med grundläggande komplex analys och abstrakt algebra. Vi gör inga anspråk på originalitet då resultaten är välkända och lättillgängliga i litteraturen. Vi vill också passa på att tacka professor Per Salberger för ämnesförslag samt handledning.

Under arbetets gång har dag- och loggbok förts över samtliga bidrag till uppsatsen. Inlärningen av materialet har skett gemensamt och beslut kring innehåll och framställning har tagits tillsammans. På det stora hela har ansvaret varit gemensamt, men Tomas har varit ansvarig för figurer samt den populärvetenskapliga texten medan Douglas står som ensam författare till s.15-20.

1 Inledning

Kurvor definierade av polynomekvationer har intresserat många av tidernas bästa matematiker. Att hitta punkter på kurvor är ekvivalent med att lösa deras definierande ekvationer. Studiet av *diofantiska ekvationer* behandlar hur man kan hitta heltalslösningar till polynomekvationer, vilket ofta är mycket svårt. Denna uppsats handlar om *elliptiska kurvor* över de komplexa talen $\mathbb{C}$. Dessas ekvationer är på formen

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

där $a, b \in \mathbb{C}$. När vi tillåter komplexa x, y handlar detta inte geometriskt sett om en kurva utan en yta över de reella talen och kallas även en Riemannyta. Inom algebraisk geometri betraktas det som en kurva då den lokalt beskrivs av en komplex parameter. Elliptiska kurvor har en märkvärdig egenskap i det att vi givet ett antal lösningar till ekvationen kan hitta nya på ett systematiskt vis. Vi jämför med cirkeln.

Enhetscirkeln består av alla punkter $(x, y) \in \mathbb{R}^2$ så att $x^2 + y^2 = 1$. Givet två stycken punkter P_1, P_2 så kan vi hitta en tredje punkt genom att addera vinklarna hos P_1, P_2. Vi får nu en tredje punkt P_3 och vi kan fortsätta hitta nya punkter genom att addera vinklar på detta vis. Om vi till varje punkt väljer en representerande vinkel i intervallet $[0, 2\pi)$ får vi nu en bijektion, och vi har definierat en gruppstruktur på enhetscirkeln S^1. Hur gör vi då för att gå mellan dessa två? Som bekant kan vi använda trigonometriska funktioner och få en bijektion

$$\begin{aligned} \mathbb{R}/_{2\pi\mathbb{Z}} = [0, 2\pi) &\to S^1 \\ \theta &\mapsto (\cos\theta, \sin\theta). \end{aligned}$$

I denna uppsats gör vi en motsvarande konstruktion för elliptiska kurvor. Det kommer istället att röra sig om dubbelt periodiska funktioner i en komplex variabel. Den gruppstruktur på elliptiska kurvor som vi nämnde ovan definieras i kapitel 2, och kommer kunna återföras på addition i $\mathbb{C}$ (modulo Λ) för $\mathbb{C}/\Lambda$ för ett 2-dimensionellt gitter $\Lambda \subset \mathbb{C}$.

Denna *uniformisering* ger oss möjlighet att dra slutsatser om gruppstrukturen på elliptiska kurvor. Detta är av central betydelse för studiet av diofantiska ekvationer. Ett djupt resultat från 1929 är Mordells sats, som säger att vi bara behöver ett ändligt antal rationella punkter på en elliptisk kurva för att kunna generera samtliga rationella punkter. Ett av millennieproblemen, Birch och Swinnerton-Dyers förmodan, handlar om hur många som behövs.

2 Elliptiska kurvor

I detta kapitel introducerar vi begreppet *elliptisk kurva* (över $\mathbb{C}$) och definierar en gruppstruktur på dessa. För att få en fullständig förståelse för det som pågår i detta kapitel krävs en del allmän teori om algebraiska kurvor. Då detta inte är syftet med denna uppsats presenterar vi bara det absolut nödvändigaste utan bevis. Vår förhoppning är att läsaren skall kunna ta till sig innebörden utan att behöva se detaljer. En fullständig redogörelse för teorin nedan finns i [Sil].

Vi börjar med en affin ekvation $f(x, y) = y^2 - x^3 - ax - b = 0$ där $a, b \in \mathbb{C}$. Denna definierar en kurva i $\mathbb{C}^2$ och genom homogenisering gör vi den kompakt. Med andra ord betraktar vi lösningsmängden till den homogena ekvationen

$$F(X, Y, Z) := Y^2Z - X^3 + -aXZ^2 - bZ^3 = 0 \qquad (\star)$$

där vi för $Z \neq 0$ återfår den affina ekvationen genom att låta $x = \frac{X}{Z}, y = \frac{Y}{Z}$. Eftersom F är homogen gäller för alla $\lambda \in \mathbb{C}$ att

$$F(a, b, c) = 0 \implies F(\lambda a, \lambda b, \lambda c) = \lambda^3 F(a, b, c) = 0.$$

Vi inför homogena koordinater genom att identifiera punkter utanför origo som ligger på samma linje genom origo:

$$(x_1, x_2, x_3) \sim (y_1, y_2, y_3) \iff \exists \lambda \in \mathbb{C}^\times : (\lambda x_1, \lambda x_2, \lambda x_3) = (y_1, y_2, y_3).$$

Det resulterande kvotrummet skrivs $\mathbb{P}^2(\mathbb{C}) = \big(\mathbb{C}^3 \setminus (0,0,0)\big)/\sim$ (se 6.1). Ekvivalensklasserna kallas punkter samt betecknas $[x_1 : x_2 : x_3]$ för något val av koordinater. Om vi begränsar oss till de punkter vars tredje koordinat är nollskild fås att varje klass har en unik representant på formen

$$\left[\frac{x_1}{x_3} : \frac{x_2}{x_3} : 1\right]$$

och i vår ursprungliga ekvation $(\star)$ gäller alltså $x = \frac{x_1}{x_3}, y = \frac{x_2}{x_3}$. Vi sätter in $z = 0$ i $(\star)$ och får lösningen $[0 : 1 : 0]$ som inte fanns med i den affina ekvationen. Genom att lägga till denna "punkt i oändligheten" har vi fått en kompakt mängd.

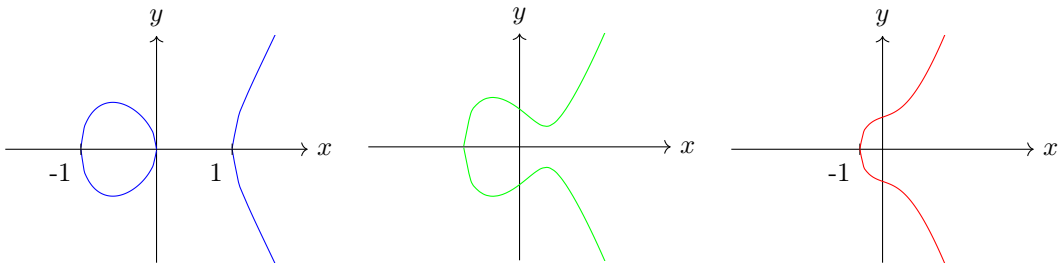
Definition 2.1. *En **elliptisk kurva** över $\mathbb{C}$ är en mängd*

$$\{[x : y : z] \in \mathbb{P}^2 \mid F(x, y, z) = 0\} = \{(x, y) \in \mathbb{C}^2 \mid f(x, y) = 0\} \cup \{O\},$$

där $F(x, y, z) = y^2 z - x^3 + -xz^2 - bz^3 \in \mathbb{C}[x, y, z]$, $4a^3 + 27b^2 \neq 0$ och $f(x, y) = F(x, y, 1)$.

Det går att visa att villkoret $4a^3 + 27b^2 \neq 0$ är ekvivalent med att kurvan är ickesingulär, det vill säga har en väldefinierad tangentlinje i varje punkt. Vi kommer genomgående att använda oss av den affina ekvationen $y^2 = x^3 + ax + b$ men det är viktigt att inte glömma den tillagda punkten i oändligheten som vi betecknar O. Notera att användningen av ordet *kurva* syftar på den algebraiska dimensionen, 1, men att det över $\mathbb{R}$ rör sig om ytor.

Låt nu E vara en elliptisk kurva. Eftersom $E \subset \mathbb{C}^2$ kan vi inte visualisera hela kurvan, men vi kan titta på $E(\mathbb{R}) = \{(x, y) \in E \mid x, y \in \mathbb{R}\}$. Detta kommer vara till hjälp för att illustrera gruppstrukturen vi skall införa. Några exempel på hur $E(\mathbb{R})$ ser ut för olika val av a, b ses i Figur 3.



$y^2 = x^3 - x$ $\quad$ $y^2 = x^3 - \frac{3}{2}x + 1$ $\quad$ $y^2 = x^3 + x + 2$

Figur 3: $E(\mathbb{R})$ för några elliptiska kurvor E.

Som med alla matematiska objekt så är det användbart att titta på avbildningar mellan dessa samt att införa ett ekvivalensbegrepp.

Definition 2.2. *Låt E_1, E_2 vara elliptiska kurvor och $\mathbb{C}(E_1)$ funktionskroppen till E_1 (se Appendix 6.2). En **isogeni** $\psi : E_1 \to E_2$ är en icke-konstant trippel*

$$\psi = [r_1 : r_2 : r_3] \in \mathbb{P}^2(\mathbb{C}(E_1))$$

som uppfyller $\psi(O_{E_1}) = O_{E_2}$.

Att vi tar r_1, r_2, r_3 ur $\mathbb{P}^2(\mathbb{C}(E_1))$ istället för $\mathbb{C}(E_1)$ innebär att vi för något P kan ha $r_1(P) = r_2(P) = r_3(P) = 0$ men att det finns $s \in \mathbb{C}(E_1)$ så att minst en av $s(P)r_1(P), \ldots$ är nollskild.

Definition 2.3. *Två elliptiska kurvor E_1, E_2 sägs vara* ***isomorfa*** *om det finns isogenier $\psi_1 : E_1 \to E_2,\ \psi_2 : E_2 \to E_1$ sådana att*

$$\psi_1 \circ \psi_2 = \psi_2 \circ \psi_1 = \mathrm{id}\,.$$

I detta fall kallas ψ_1, ψ_2 för isomorfier.

En explicit isomorfi som figurerar i denna uppsats är mellan kurvorna $E_1 : y^2 = 4x^3 - g_2x - g_3$ och $E_2 : y^2 = x^3 + ax + b$ där $-4a = g_2$ och $-4b = g_3$. Isogenin ges av $[x : y : z] \mapsto [x : \frac{y}{2} : z]$ och det är tydligt att det är en isomorfi.

Vi inför nu ett mycket användbart verktyg, j-invarianten till en elliptisk kurva. Denna kommer att vara av central betydelse i kapitel 4.

Definition 2.4. *Låt $E : y^2 = x^3 + ax + b$ vara en elliptisk kurva. Vi definierar j-****invarianten*** *till E som*

$$j(E) = 1728\frac{4a^3}{4a^3 + 27b^2}.$$

Nedan följer tre fakta om isomorfa kurvor som kommer att behövas längre fram.

Sats 2.1. *(a) Två elliptiska kurvor E_1 och E_2 är isomorfa om och endast om $j(E_1) = j(E_2)$.*

(b) Varje komplext tal är j-invariant till minst en elliptisk kurva. Med andra ord, j definierar en surjektiv funktion

$$j : \{^{Elliptiska}_{kurvor}\} \twoheadrightarrow \mathbb{C}$$

(c) Två elliptiska kurvor $E_1 : y^2 = x^3 + a_1x + b_1$ och $E_2 : y^2 = x^3 + a_2x + b_2$ är isomorfa om och endast om det finns ett $\mu \in \mathbb{C}^*$ sådant att

$$a_2 = \mu^4 a_1 \text{ och } b_2 = \mu^6 b_1.$$

Bevis. (a)-(c) [Su14, Sats 12,13,14]. □

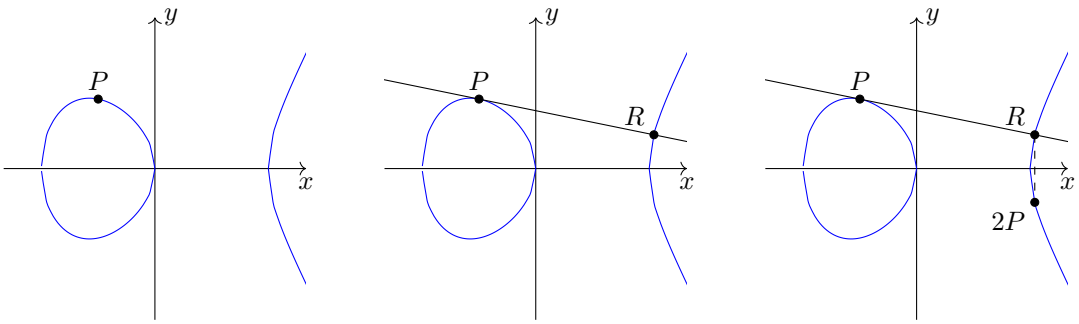
En del av motiveringen till att studera elliptiska kurvor är talteoretisk. Talteoretiker är intresserade av att lösa polynomekvationer över $\mathbb{Q}$ och $\mathbb{Z}$, och elliptiska kurvor har egenskapen att vi givet ett antal punkter på kurvan (det vill säga lösningar till dess definierande ekvation) kan generera nya punkter på ett systematiskt vis. Mer precist finns det på varje elliptisk kurva[1] en gruppstruktur. Ett av våra mål i denna uppsats är att hitta en enklare beskrivning av denna struktur.

Definition 2.5. *Låt $P, Q \in E$, L vara linjen mellan P och Q (om $P = Q$, tag tangentlinjen) och R vara den tredje skärningspunkten mellan L och E. Låt L' vara linjen mellan R och O. Vi låter $P + Q$ vara den tredje skärningspunkten till L'.*

Att det alltid finns exakt tre skärningspunkter (medräknat multiplicitet) följer av Bézouts sats[2]. För reella punkter har vi en tydlig bild av hur kompositionslagen ser ut, se figur 4 och 5. För komplexa punkter fungerar additionen lika bra, men blir svår att visualisera.

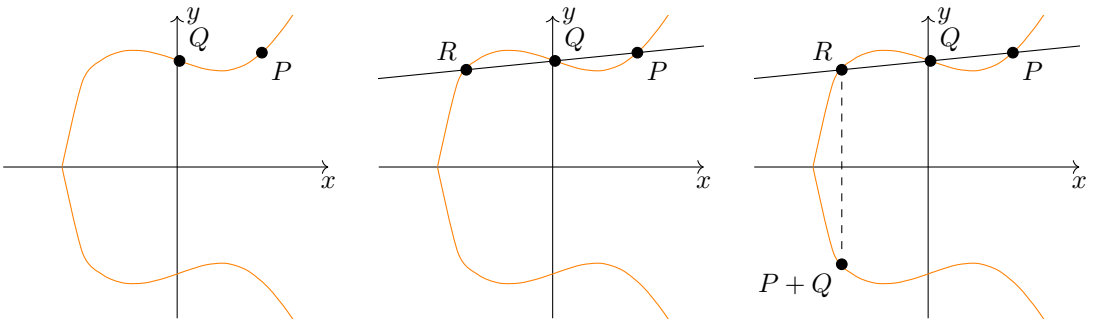
[1] Det räcker att kurvan är ickesingulär och kubisk.

[2] Här behövs att kurvan är projektiv, det vill säga att vi lagt till punkter i oändligheten. Annars garanterar Bézouts sats inte 3 skärningspunkter.



(a) Tag en punkt P. (b) Drag en tangentlinje och finn skärningspunkten R. (c) Spegla i x-axeln för att erhålla $2P$.

Figur 4: Uträkning av $2P = P + P$ för $P \in E(\mathbb{R})$.



(a) Tag två punkter P och Q (b) Drag en sekant och finn skärningspunkten R. (c) Spegla i $x-$axeln för att erhålla $P + Q$.

Figur 5: Uträkning av $P + Q$ för $P, Q \in E(\mathbb{R})$.

Sats 2.2.

(a) Operationen som definieras i Definition 2.5 *gör E till en abelsk grupp med O som neutralt element.*

(b) För $P = (x, y) \in E$ gäller $-P = (x, -y)$

(c) Isogenier är homomorfier, det vill säga om $\psi : E_1 \to E_2$ är en isogeni gäller

$$\psi(P + Q) = \psi(P) + \psi(Q) \ \forall P, Q \in E_1.$$

Bevis. (a) [Sil, Prop. III.2.2], (b) [Sil, s.53], (c) [Sil, Sats III.4.8]. □

Observera att associativitet är långt ifrån självklart med denna definition av gruppoperationen. Tack vare 2.2c behöver vi inte skilja på isomorfi av elliptiska kurvor (som i Definition 2.3) och isomorfi av grupper.

3 Elliptiska funktioner

I detta kapitel introduceras begreppet *elliptiska funktioner*. Detta är dubbelt periodiska funktioner i en komplex variabel. Kapitlet följer framställningen i [Sil, VI.2-3].

Definition 3.1. *Ett **gitter** är en diskret delgrupp $\Lambda \subset \mathbb{C}$ som innehåller en $\mathbb{R}$-bas för $\mathbb{C}$, det vill säga en mängd på formen*

$$\Lambda = \{m\omega_1 + n\omega_2 \in \mathbb{C} \mid m, n \in \mathbb{Z}\}$$

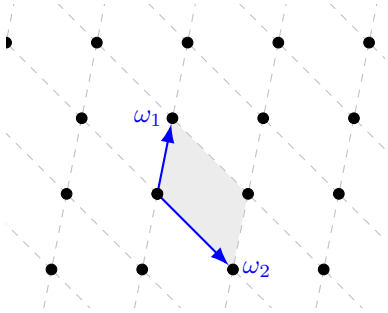
för $\mathbb{R}$-linjärt oberoende $\omega_1, \omega_2 \in \mathbb{C}$.

För våra ändamål kommer det vara nyttigt att ha ett ekvivalensbegrepp för gitter. Vi säger att två gitter Λ_1, Λ_2 är **homotetiska** och skriver $\Lambda_1 \cong \Lambda_2$ om det finns ett $\alpha \in \mathbb{C}$, $\alpha \neq 0$, sådant att $\alpha\Lambda_1 = \{\alpha\omega \mid \omega \in \Lambda_1\} = \Lambda_2$. Geometriskt innebär multiplikation med komplexa tal dels en skalning och dels en rotation. Två gitter är alltså homotetiska om det finns en rotationsvinkel och en skalningsfaktor som tar det förstas punkter till det andras.

Definition 3.2. *En **fundamentalparallellogram** till ett gitter Λ är en mängd på formen*

$$D = \{a + t_1\omega_1 + t_2\omega_2 \mid 0 \leq t_1, t_2 < 1\}$$

där $a \in \mathbb{C}$ och $\omega_1, \omega_2 \in \Lambda$ en bas.



Figur 6: Gittret $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. Det skuggade området är en fundamentalparallellogram.

Definition 3.3. *Låt Λ vara ett gitter. En **elliptisk funktion** (med avseende på gittret Λ) är en meromorf funktion f definierad på $\mathbb{C}$ sådan att*

$$f(z + \omega) = f(z) \text{ för alla } \omega \in \Lambda,\ z \in \mathbb{C}.$$

För ett gitter Λ skriver vi $\mathbb{C}(\Lambda)$ för mängden av alla elliptiska funktioner med avseende på Λ. Notera att $\mathbb{C}(\Lambda)$ bildar en kropp under punktvis addition och multiplikation.

Proposition 3.1. *En elliptisk funktion som saknar poler eller nollställen är konstant.*

Bevis. Antag att $f \in \mathbb{C}(\Lambda)$ saknar poler, det vill säga är holomorf. Låt D vara en fundamentalparallellogram för Λ. Eftersom f är periodisk fås

$$\sup_{z\in\mathbb{C}} |f(z)| = \sup_{z\in\bar{D}} |f(z)|,$$

men $|f|$ är kontinuerlig och $\bar{D}$ kompakt, så $|f|$ är begränsad på $\bar{D}$ och därmed på hela $\mathbb{C}$. Vi drar med hjälp av Liouvilles sats slutsaten att f är konstant. Om f saknar nollställen kan vi tillämpa samma resonemang på $1/f$ och satsen följer. □

För en meromorf funktion f och $w \in \mathbb{C}$ skriver vi $\mathrm{ord}_w(f)$ och $\mathrm{res}_w(f)$ för multipliciteten av nollstället w (0 om $f(w) \neq 0$) respektive residyn. I följande sats skriver vi $\sum_{w\in\mathbb{C}/\Lambda}$ för en summa över en fundamentalparallellogram D. Eftersom vi behandlar elliptiska funktioner kommer dessa summor vara oberoende av val av D.

Sats 3.1. *Låt f vara elliptisk med avseende på Λ. Då gäller att*

$$\sum_{w\in\mathbb{C}/\Lambda} \mathrm{res}_w(f) = 0 \tag{a}$$

$$\sum_{w\in\mathbb{C}/\Lambda} \mathrm{ord}_w(f) = 0 \tag{b}$$

$$\sum_{w\in\mathbb{C}/\Lambda} \mathrm{ord}_w(f)w \in \Lambda. \tag{c}$$

Bevis. Låt D vara en fundamentalparallellogram för Λ sådant att f saknar poler eller nollställen på randen ∂D. Alla tre påståenden följer av residysatsen och argumentprincipen.

(a) Residysatsen ger

$$\sum_{w\in\mathbb{C}/\Lambda} \operatorname{res}_w(f) = \frac{1}{2\pi i}\int_{\partial D} f(z)dz.$$

Eftersom f är periodisk tar integralerna längs motsatta sidor av D ut varandra. Därmed blir hela integralen 0.
(b) Eftersom f är periodisk är även f' periodisk. Vi tillämpar (a) på den elliptiska funktionen f'/f och utnyttjar argumentprincipen:

$$\sum_{w\in\mathbb{C}/\Lambda} \operatorname{ord}_w(f) = \frac{1}{2\pi i}\int_{\partial D} \frac{f'(z)}{f(z)}dz = 0.$$

(c) Residysatsen tillämpad på $\frac{zf'(z)}{f(z)}$ ger

$$\begin{aligned}\sum_{w\in\mathbb{C}/\Lambda} \operatorname{ord}_w(f)w &= \frac{1}{2\pi i}\int_{\partial D} \frac{zf'(z)}{f(z)}dz \\ &= \frac{1}{2\pi i}\left(\int_a^{a+\omega_1} + \int_{a+\omega_1}^{a+\omega_1+\omega_2} + \int_{a+\omega_1+\omega_2}^{a+\omega_2} + \int_{a+\omega_2}^{a}\right)\frac{zf'(z)}{f(z)}dz\end{aligned}$$

I den andra och tredje integralen gör vi variabelsubstitutionerna $z \to z-\omega_1$ respektive $z \to z-\omega_2$. Sedan används periodiciteten hos integranden för att få

$$\sum_{w\in\mathbb{C}/\Lambda} \operatorname{ord}_w(f)w = \frac{\omega_2}{2\pi i}\int_a^{a+\omega_1} \frac{f'(z)}{f(z)}dz + \frac{\omega_1}{2\pi i}\int_a^{a+\omega_2} \frac{f'(z)}{f(z)}dz.$$

Argumentprincipen ger nu att integralerna är lika med $2\pi ik$ där k är ett heltal, och satsen följer. □

Definition 3.4. ***Ordningen*** *av en elliptisk funktion är dess antal poler (räknade med multiplicitet) i någon fundamentalparallellogram.*

Även denna definition är oberoende av val av parallellogram. Vi anmärker att vi lika gärna kunnat definiera ordning som antalet nollställen (enligt Sats 3.1b ovan). Sats 3.1a och Proposition 3.1 ger oss följande korollarium som är ett första steg mot en klassificering av alla elliptiska funktioner.

Korollarium 3.1. *Ordningen av en ickekonstant elliptisk funktion är åtminstone* 2.

Bevis. Om f är elliptisk och bara har en pol, av ordning 1, i en punkt w så följer det av Sats 3.1a att $\operatorname{res}_w(f) = 0$. Därmed är f holomorf, och Proposition 3.1 ger att f måste vara konstant. □

Ännu har vi inte sett några icketriviala exempel på elliptiska funktioner. Nu introducerar vi en första kandidat som kommer följa med i resten av uppsatsen.

Definition 3.5. *Låt Λ vara ett gitter.* ***Weierstrass $\wp$-funktion*** *(med avseende på Λ) definieras som*

$$\wp_\Lambda : \mathbb{C}\setminus\Lambda \to \mathbb{C},\ z \mapsto \frac{1}{z^2} + \sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right).$$

Det följer direkt från definitionen att $\wp_\Lambda$ är en Λ-periodisk jämn funktion. Gittret Λ kommer alltid vara fixt, så vi skriver ibland bara $\wp(z)$. Vi vill nu visa att $\wp$ är meromorf och därmed elliptisk. För att kunna göra detta så behöver vi följande lemma från komplex analys (för ett bevis, se [Ahl, §5 Sats 1]).

Lemma 3.1. *Antag att $\{f_n\}$ är en följd av holomorfa funktioner på en öppen mängd $\Omega \subseteq \mathbb{C}$, och att $f_n \to f$ likformigt på varje kompakt delmängd av Ω. Då är f holomorf på Ω.*

Sats 3.2. *$\wp$ är holomorf på $\mathbb{C} \setminus \Lambda$ och därmed elliptisk.*

Bevis. Vi visar att $\wp$ konvergerar absolut och likformigt. Tag $\omega \in \mathbb{C}$ så att $|\omega| > 2|z|$. Då har vi

$$\left| \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right| = \left| \frac{\omega^2 - \omega^2 + 2z\omega - z^2}{\omega^2(z-\omega)^2} \right| \leq \frac{|z|(2|\omega| + |z|)}{|\omega|^2(|\omega| - |z|)^2} \leq \frac{10|z|}{|\omega|^3}.$$

Detta ger

$$\wp(z) = \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \left| \frac{1}{(z-\omega)^2} - \frac{1}{w^2} \right| \leq \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0 \\ |\omega| \leq 2|z|}} \left| \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right| + 10|z| \sum_{\substack{\omega \in \Lambda \\ |\omega| > 2|z|}} \frac{1}{|\omega|^3}.$$

Notera att den första summan är ändlig och därmed konvergent. Om även den andra summan konvergerar kan vi tillämpa Weierstrass M-test ihop med Lemma 3.1 för att avsluta beviset. Till detta behövs följande lemma:

Lemma 3.2. *Det finns en konstant $c > 0$ och ett $R_0 > 0$ så att*

$$\#\{\omega \in \Lambda \mid R < |\omega| \leq R + 1\} \leq cR \text{ för alla } R \geq R_0.$$

Med andra ord, antalet gitterpunkter i en skiva växer linjärt i radien.

Bevis. Låt ω_1, ω_2 vara en bas till Λ med minimal längd, det vill säga för varje annan bas ω_1', ω_2' så gäller $|\omega_1| \leq |\omega_1'|, |\omega_2| \leq |\omega_2'|$ upp till omindexering. Låt A beteckna arean av fundamentalparallellogrammen till detta val av bas, och d diametern. Vi definierar

$$f(R) = \#\{\omega \in \Lambda \mid |\omega| \leq R\},$$

som är växande och noterar att $\#\{\omega \in \Lambda \mid R < \omega \leq R + 1\} = f(R+1) - f(R)$. Vi får följande:

$$\begin{aligned} f(R) &\leq \frac{\pi(R+d)^2}{A} \\ &= \frac{\pi R^2}{A} + \frac{\pi}{A}\left((R+d)^2 - R^2\right) \\ &= \frac{\pi}{A}R^2 + \mathcal{O}(R) \\ \implies f(R+1) - f(R) &= \frac{\pi}{A}\left((R+1)^2 - R^2 + \mathcal{O}(R+1) + \mathcal{O}(R)\right) \\ &= \mathcal{O}(R), \end{aligned}$$

vilket bevisar Lemma 3.2. Vi tillämpar detta på summan vi är intresserade av:

$$\sum_{\substack{\omega \in \Lambda \\ |\omega| > 2|z|}} \frac{1}{|\omega|^2} \leq \sum_{R=1}^{\infty} \frac{cR}{R^3} < \infty.$$

Därmed är $\wp$ absolut- och likformigt konvergent på hela $\mathbb{C} \setminus \Lambda$ och således elliptisk. □

Med ett liknande resonemang visas att vi kan derivera $\wp$ termvis för att finna dess derivata:

$$\wp'(z) = -\frac{2}{z^3} - 2\sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \frac{1}{(z-\omega)^3}.$$

Innebörden i följande sats är att $\wp$ och $\wp'$ är de byggstenar som tillsammans kan bilda alla icke-konstanta elliptiska funktioner. Vi inför här begreppet *divisor* till en elliptisk funktion, definierat som en formell (ändlig!) summa

$$\operatorname{div}(f) = \sum_{w \in \mathbb{C}/\Lambda} \operatorname{ord}_w(f)\langle w \rangle,$$

av element $\langle w \rangle$ där w är punkter[3]. Om vi känner till en funktions divisor känner vi alltså till dess nollställen och poler med sina multipliciteter, och vi inför begreppet i syfte att göra resonemanget i följande bevis tydligare.

Sats 3.3. *Varje elliptisk funktion kan uttryckas som en rationell funktion i $\wp$ och $\wp'$. Därmed gäller*

$$\mathbb{C}(\Lambda) = \mathbb{C}(\wp, \wp').$$

Bevis. Att varje rationell kombination av $\wp, \wp'$ är elliptisk är tydligt. Vi bevisar den andra inklusionen. Låt $f \in \mathbb{C}(\Lambda)$. Det räcker att visa påståendet för jämna och udda funktioner eftersom

$$f(z) = \frac{1}{2}\big(f(z) + f(-z)\big) + \frac{1}{2}\big(f(z) - f(-z)\big).$$

Om f är udda så kommer produkten $\wp' f$ vara jämn, så vi kan anta att f är jämn. Vi har då att

$$\operatorname{ord}_w(f) = \operatorname{ord}_{-w}(f) \quad \forall w \in \mathbb{C}.$$

Om $2w \in \Lambda$ kan vi derivera $f(-z) = f(z)$ upprepade gånger och få

$$f^k(z) = (-1)^k f^k(-z)$$

alltså kommer $f^k(w) = 0$ för alla udda k. Alltså måste ord_w vara ett jämnt tal. Om nu D är en fundamentalparallellogram till Λ låter vi H vara "halva" D (ersätt ω_1 med $\frac{1}{2}\omega_1$). Av att f är jämn och att $\operatorname{ord}_w(f)$ är jämn om $2w \in \Lambda$ följer att

$$\operatorname{div}(f) = \sum_{w \in H} n_w \left(\langle w \rangle + \langle -w \rangle\right) \text{ för några } n_w \in \mathbb{Z}.$$

Definiera nu g enligt följande:

$$g(z) = \prod_{\substack{w \in H \\ w \neq 0}} \left(\wp(z) - \wp(w)\right)^{n_w}.$$

Eftersom $\wp(z) - \wp(w)$ har divisor $\langle w \rangle + \langle -w \rangle - 2\langle 0 \rangle$ så kommer f och g ha identiska nollställen och poler i alla $w \in H \setminus \{0\}$. Den enda punkt som kvarstår är $z = 0$, men det följer av Sats 3.1 att $\operatorname{ord}_0(f) = \operatorname{ord}_0(g)$. Betrakta nu den elliptiska funktionen $\frac{f}{g}$. Eftersom nollställen och poler i täljare respektive nämnare överensstämmer så är detta en holomorf funktion. Enligt Proposition 3.1 kommer därför $\frac{f(z)}{g(z)} = c$ vilket ger oss

$$f(z) = cg(z) = c \prod_{\substack{w \in H \\ w \neq 0}} \left(\wp(z) - \wp(w)\right)^{n_w} \in \mathbb{C}(\wp(z), \wp'(z)). \qquad \square$$

Vi vill härleda en särskild ekvation med $\wp$ och $\wp'$ som kopplar elliptiska funktioner till elliptiska kurvor. För att göra detta behöver vi skriva om funktionerna som Laurentutvecklingar. Vi börjar med att införa följande definition som förenklar notationen.

Definition 3.6. *Låt $\Lambda \subset \mathbb{C}$ vara ett gitter och $k > 2$ ett heltal.* ***Eisensteinserien av vikt*** *k till Λ definieras som*

$$G_k(\Lambda) = \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \frac{1}{\omega^k}.$$

Ett resonemang som det i beviset till Sats 3.2 visar att G_k konvergerar absolut för $k > 2$. Observera att G_k är 0 för udda k.[4]

[3] För den som känner till *fria abelska grupper*: div definierar en homomorfi från $\mathbb{C}(\Lambda)$ till $F(\mathbb{C}/\Lambda)$, den fria abelska gruppen genererad av punkterna i C/Λ.

[4] Eisensteinserien är det enklaste exemplet på en så kallad *modulär form*.

Proposition 3.2. *Laurentserien till $\wp$ ges av*

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty}(2n+1)G_{2n+2}(\Lambda)z^{2n}.$$

Bevis. För $|z| < |\omega|$ har vi att varje i term i $\wp$ ges av

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{1}{\omega^2}\left(\frac{1}{(1-z/\omega)^2} - 1\right) = \sum_{n=1}^{\infty}(n+1)\frac{z^n}{\omega^{n+2}}.$$

Alltså har vi

$$\begin{aligned}
\wp(z) &= \frac{1}{z^2} + \sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}}\sum_{n=1}^{\infty}(n+1)\frac{z^n}{\omega^{n+2}} \\
&= \frac{1}{z^2} + \sum_{n=1}^{\infty}(n+1)z^n \sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}}\frac{1}{\omega^{n+2}} \\
&= \frac{1}{z^2} + \sum_{n=1}^{\infty}(n+1)z^n G_{n+2}(\Lambda) \\
&= \frac{1}{z^2} + \sum_{n=1}^{\infty}(2n+1)z^{2n} G_{2n+2}(\Lambda),
\end{aligned}$$

eftersom $G_k = 0$ för udda k. □

Följande sats är kanske den viktigaste i hela uppsatsen och är anledningen till varför $\wp$ intresserar oss.

Sats 3.4. *Låt $\Lambda \subset \mathbb{C}$ vara ett gitter, $\wp = \wp_\Lambda$, $g_2 = 60G_4(\Lambda)$ och $g_3 = 140G_6(\Lambda)$. Då gäller att*

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

Bevis. I en omgivning till 0 har vi enligt Proposition 3.2 följande Laurentutvecklingar:

$$\wp(z) = \frac{1}{z^2} + z^2 h_1(z), \quad \wp'(z) = -\frac{2}{z^3} + z h_2(z),$$

där h_1, h_2 är holomorfa i en omgivning av 0. Vi får följande (här betecknar "..."högre ordningens termer, holomorfa i en omgivning av 0):

$$\begin{aligned}
f(z; g_2, g_3) &= 4(\wp(z))^3 - g_2\wp(z) - g_3 - (\wp'(z))^2 \\
&= 4\left(\frac{1}{z^6} + \frac{3h_1(z)}{z^2} + \dots\right) - g_2\left(\frac{1}{z^2} + \dots\right) \\
&\quad - g_3 - \left(\frac{4}{z^6} - \frac{4h_2(z)}{z^2} + \dots\right) \\
&= \frac{h_3(z) - g_2}{z^2} - g_3 + h_4(z),
\end{aligned}$$

där h_3, h_4 är holomorfa nära 0. Vi väljer nu g_2 så att $h_3(0) - g_2 = 0$, och g_3 så att f har ett nollställe någonstans. Valet av g_2 medför att f har en hävbar singularitet i 0 och definierar alltså en holomorf Λ-periodisk funktion. Därmed är f konstant enligt Sats 3.1, och vårt val av g_3 ger att f är identiskt 0. För den exakta uträkningen av g_2 och g_3, se Appendix 6.3. □

4 Uniformisering

Detta kapitel är baserat på [Su15], [Su16]. Låt $\Lambda \subset \mathbb{C}$ vara ett gitter och E_Λ vara kurvan (inte nödvändigtvis icke-singulär) bestämd av

$$y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda).$$

Kom ihåg att $E_\Lambda \cong E : y^2 = x^3 + ax + b$ där $-4a = g_2(\Lambda)$ och $-4b = g_3(\Lambda)$ via isogenin $[x : y : z] \mapsto [x : \frac{y}{2} : z]$. Eftersom E är icke-singulär då $4a^3 + 27b^2 \neq 0$ får vi villkoret $g_2^3 - 27g_3^2 \neq 0$ på E_Λ. Sats 3.4 ger oss en avbildning (eftersom $\wp$ är elliptisk)

$$\begin{aligned} \phi_\Lambda : \mathbb{C}/\Lambda &\to E_\Lambda \\ [z] &\mapsto [\wp_\Lambda(z) : \wp'_\Lambda(z) : 1]. \end{aligned}$$

Vi kallar ϕ för den **uniformiserande avbildningen**, och vi skall visa att det är en gruppisomorfi. Detta innebär två saker. För det första kan vi parametrisera den elliptiska kurvan E_Λ, och en naturlig fråga (som besvaras längre fram) är vilka elliptiska kurvor som kan parametriseras på detta vis. För det andra innebär det att den tämligen invecklade grupplagen vi infört på elliptiska kurvor kan beskrivas som addition av komplexa tal modulo Λ, åtminstone för de kurvor som vi kan parametrisera. Vi börjar med två tekniska observationer.

Lemma 4.1. *Låt $\Lambda' = \frac{1}{2}\Lambda \setminus \Lambda$. Då gäller*

$$\wp'(\lambda) = 0 \iff \lambda \in \Lambda' \tag{a}$$

$$\wp''(\lambda) \neq 0 \quad \textit{för} \quad \lambda \in \Lambda'. \tag{b}$$

Bevis. Antag att $\lambda \in \Lambda'$. Då gäller för alla $h \in \mathbb{C}$ att

$$\wp(\lambda + h) = \wp(\lambda + h - 2\lambda) = \wp(-\lambda + h) = \wp(\lambda - h)$$

eftersom $\wp$ är Λ-periodisk och jämn. Vi får att

$$\wp'(\lambda) = \lim_{h \to 0} \frac{\wp(\lambda + h) - \wp(\lambda - h)}{2h} = 0.$$

Eftersom $\wp'$ är av ordning 3 med endast en pol måste då dessa nollställen vara av ordning 1 enligt Proposition 3.1, det vill säga $\wp'' \neq 0$ där. □

Lemma 4.2. *För varje gitter $\Lambda \subset \mathbb{C}$ gäller*

$$\Delta(\Lambda) := g_2(\Lambda)^3 - 27g_3(\Lambda)^2 \neq 0,$$

där g_2, g_3 är definierade som i Sats 3.4.

Konstanten $\Delta(\Lambda)$ kallas för gittrets **diskriminant** och kommer spela en viktig roll längre fram. Innebörden i Lemma 4.2 är alltså att E_Λ alltid är elliptisk.

Bevis. Låt $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ och sätt

$$\lambda_1 = \frac{\omega_1}{2}, \quad \lambda_2 = \frac{\omega_2}{2}, \quad \lambda_3 = \frac{\omega_1 + \omega_2}{2}.$$

Enligt Lemma 4.1 de enda nollställena till $\wp'$, upp till kongruens modulo Λ. Från Sats 3.4 fås att $\wp(r_1),\ \wp(r_2),\ \wp(r_3)$ är nollställen till det kubiska polynomet

$$f(x) = 4x^3 - g_2 x - g_3.$$

Vi har att $\Delta(f) = 16(\Delta(\Lambda))$, och får

$$\Delta(\Lambda) = \frac{1}{16} \prod_{i<j} \left(\wp(r_i) - \wp(r_j)\right)^2.$$

Vi vill alltså visa att ingen faktor $\wp(r_i) - \wp(r_j)$ är 0. Låt $g_i(z) = \wp(z) - \wp(r_i)$. Då är g_i elliptiska funktioner av ordning 2, så de har 2 nollställen i varje fundamentalparallellogram. Eftersom $g_i(r_i) = 0$ och $g_i'(r_i) = \wp'(r_i) = 0$ så saknar g_i andra nollställen. Det följer att ingen faktor i produkten är 0, och därmed gäller $\Delta(\Lambda) \neq 0$. □

Sats 4.1. *(Uniformiseringssatsen, del 1)*
Låt $\Lambda \subset \mathbb{C}$ vara ett gitter och $E_\Lambda : y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$. Då är avbildningen

$$\begin{aligned} \phi_\Lambda : \mathbb{C}/\Lambda &\to E_\Lambda \\ [z] &\mapsto [\wp_\Lambda(z) : \wp'_\Lambda(z) : 1] \end{aligned}$$

en gruppisomorfi.

Bevis. Låt $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. Det finns tre element av ordning 2 i $\mathbb{C}/\Lambda$: $\frac{\omega_1}{2}, \frac{\omega_2}{2}$ och $\frac{\omega_1+\omega_2}{2}$. Enligt Lemma 4.1 så har $\wp'$ nollställen i dessa punkter, och därmed avbildar ϕ punkter av ordning 2 på punkter av ordning 2, eftersom dessa är de som uppfyller $y = 0$ (se Sats 2.2b). Vidare är ϕ injektiv på punkter av ordning 2 eftersom dessa avbildas på distinkta rötter till $4\wp(z)^3 - g_2\wp(z) - g_3$ enligt beviset av Lemma 4.2. Vi skriver $(\mathbb{C}/\Lambda)[2]$ respektive $E_\Lambda[2]$ för delgrupperna bestående av punkter av ordning 2 samt noterar att $\phi(0) = O$ eftersom $[\wp_\Lambda(z) : \wp'_\Lambda(z) : 1] = [\frac{\wp_\Lambda(z)}{\wp'_\Lambda(z)} : 1 : \frac{1}{\wp'_\Lambda(z)}]$ så $[0] \overset{\phi_\Lambda}{\mapsto} [0 : 1 : 0] = O$. Restriktionen $\phi|_{(\mathbb{C}/\Lambda)[2]}$ ger alltså en isomorfi

$$\begin{array}{ccc} (\mathbb{C}/\Lambda)[2] & \longleftrightarrow & E_\Lambda[2] \\ \| & & \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} & & \end{array}$$

Vi visar nu surjektivitet. Låt $(x_0, y_0) \in E_\Lambda$, och D vara en fundamentalparallellogram till Λ. Funktionen $f(z) = \wp(z) - x_0$ är elliptisk av ordning 2 och har därmed 2 nollställen i D. Eftersom f har en pol i 0 kan den inte ha ett nollställe där, så låt $z_0 \neq 0$ vara ett nollställe till f i D. Då fås

$$\wp(z_0) = x_0 \implies \phi(z_0) = (x_0, \pm y_0) \implies (x_0, y_0) = \phi(\pm z_0),$$

och ϕ är alltså surjektiv.
Låt nu $z_1, z_2 \in D$ och antag $\phi(z_1) = \phi(z_2)$. Om $2z_1 \in \Lambda$ så är z_1 av ordning 2, och enligt ovan fås $z_1 = z_2$. Om $2z_1 \notin \Lambda$ har vi $\wp'(z_1) \neq 0$ och på samma sätt som tidigare har vi att rötterna till $f(z) = \wp(z) - \wp(z_1)$ i D är $\pm z_1$ vilket ger

$$z_2 \equiv \pm z_1 \pmod{\Lambda},$$

men eftersom $\wp'(z_1) = \wp'(z_2)$ enligt antagande och $\wp'(z_1) \neq 0$ fås

$$\wp'(-z_1) = -\wp'(z_1) \neq \wp'(z_1).$$

Detta ger $z_1 \equiv z_2 \pmod{\Lambda}$ och ϕ är alltså injektiv.

Det återstår att visa att ϕ är en grupphomomorfi. Låt $z_1, z_2 \in D$. Vi vill visa att $\phi(z_1 + z_2) = \phi(z_1) + \phi(z_2)$ för alla $z_1, z_2 \in \mathbb{C}$. Om någon av z_1, z_2 tillhör Λ följer påståendet direkt eftersom Λ avbildas på identitetselementet O. Även fallet då $z_1 + z_2$ ligger i Λ är enkelt, ty då fås att $z_2 = -z_1 + \omega$ för något $\omega \in \Lambda$ och alltså

$$\phi(z_1 + z_2) = O = \phi(z_1) + \phi(-z_1 + \omega) = \phi(z_1) + \phi(z_2).$$

Antag nu $z_1, z_2, z_1 + z_2 \notin \Lambda$, och skriv

$$P_1 = \phi(z_1), \quad P_2 = \phi(z_2).$$

Observera att $P_1, P_2 \neq O$. Skriv $y = mx + b$ för linjen mellan P_1 och P_2, och låt P_3 vara den tredje skärningspunkten. Då gäller enligt definitionen av grupplagen på E att $P_1 + P_2 + P_3 = O$. Betrakta nu funktionen

$$\ell(z) = -\wp'(z) + m\wp(z) + b.$$

Detta är en elliptisk funktion av ordning 3 med en trippelpol i 0, så den har 3 nollställen i D (inklusive multiplicitet) varav z_1 och z_2 är två. Skriv z_3 för det tredje nollstället i D. Då gäller att

$\phi(z_3) =$ ligger både på linjen ℓ och E, och är alltså lika med någon av P_1, P_2, P_3. Eftersom vi har en bijektion

$$\{z_1, z_2, z_3\} \longrightarrow \{P_1, P_2, P_3\}$$

så måste $\phi(z_3) = P_3$ om $P_3 \neq P_1, P_2$. Om P_3 sammanfaller med P_1 (säg) så fås att ℓ har en dubbelrot i z_1 och alltså $z_1 = z_3$. Om $P_1 = P_2 = P_3$ måste även $z_1 = z_2 = z_3$. Vi drar slutsatsen att $P_3 = \phi(z_3)$.

Eftersom $P_1 + P_2 + P_3 = O$ räcker det att visa $z_1 + z_2 + z_3 \in \Lambda$, ty

$$\phi(z_1 + z_2) = \phi(-z_3) = -\phi(z_3) = -P_3 = P_1 + P_2 = \phi(z_1) + \phi(z_2).$$

Detta följer direkt av Proposition 3.1 tillämpad på ℓ, det vill säga $\sum_{w \in \mathbb{C}/\Lambda} \mathrm{ord}_w(\ell) w \in \Lambda$. □

Vårt mål är nu att visa varje elliptisk kurva parametriseras enligt ovan. Detta kräver mer avancerat maskineri än vi hittills infört. Kom ihåg att j-invarianten som vi införde i kapitel 2 klassificerar alla elliptiska kurvor upp till isomorfi (Sats 2.1a). Denna invariant kommer att stå i fokus i resten av kapitlet, och vi börjar med att införa en motsvarande kvantitet för gitter.

Definition 4.1. *Låt $\Lambda \subset \mathbb{C}$ vara ett gitter. Vi definierar j-**invarianten** associerad till Λ som*

$$j(\Lambda) = 1728 \frac{g_2(\Lambda)^3}{\Delta(\Lambda)}.$$

Observera att $j(\Lambda)$ alltid är definierad enligt Proposition 4.2. Som bekant har vi en isomorfi av kurvor

$$y^2 = 4x^3 - g_2 x - g_3 \quad \cong \quad y^2 = x^3 + ax + b,$$

där $g_2(\Lambda) = -4a$ och $g_3(\Lambda) = -4b$. Detta ger att

$$j(\Lambda) = 1728 \frac{g_2(\Lambda)^3}{g_2(\Lambda)^3 - g_3(\Lambda)^2} = 1728 \frac{(-4a)^3}{(-4a)^3 - (-4b)^2} = 1728 \frac{4a^3}{4a^3 + 27b^2} = j(E_\Lambda),$$

så j-invarianten till ett gitter sammanfaller med j-invarianten till den motsvarande kurvan. Vi gör därför följande definition.

Definition 4.2. ***Diskriminanten** till en elliptisk kurva $y^2 = x^3 + ax + b$ definieras som*

$$\Delta(E) = -16(4a^3 + 27b^2).$$

Notera att en kubisk kurva på formen $y^2 = x^3 + ax + b$ är icke-singulär (och därmed elliptisk) om och endast om dess diskriminant är nollskild. Vi påminner om att två gitter Λ_1, Λ_2 är homotetiska om det finns ett nollskilt $c \in \mathbb{C}$ så att $c\Lambda_1 = \Lambda_2$. Följande sats ger oss ett annat villkor.

Sats 4.2. *Två gitter $\Lambda_1, \Lambda_2 \subset \mathbb{C}$ är homotetiska om och endast om $j(\Lambda_1) = j(\Lambda_2)$.*

Bevis. ($\Longrightarrow$) Antag att $c\Lambda_1 = \Lambda_2$. Då har vi enligt Sats 3.4 att

$$g_2(\Lambda_2) = 60 \sum_{\substack{\omega \in \Lambda_2 \\ \omega \neq 0}} \frac{1}{\omega^4} = 60 \sum_{\substack{\omega \in \Lambda_1 \\ \omega \neq 0}} \frac{1}{(c\omega)^4} = c^{-4} g_2(\Lambda_1),$$

och på samma sätt fås $g_3(\Lambda_2) = c^{-6} g_3(\Lambda_1)$. Vi jämför j-invarianter:

$$j(\Lambda_2) = 1728 \frac{(c^{-4} g_2(\Lambda_1))^3}{(c^{-4} g_2(\Lambda_1))^3 - 27(c^{-6} g_3(\Lambda_1))^2} = \frac{g_2(\Lambda_1)^3}{g_2(\Lambda_1)^3 - 27 g_3(\Lambda)^2} = j(\Lambda_1).$$

($\Longleftarrow$) Antag att $j(\Lambda_1) = j(\Lambda_2)$ och skriv E_1, E_2 för de motsvarande kurvorna. Enligt ovan har vi att $j(E_1) = j(E_2)$. Vi skriver

$$E_1 : y^2 = x^3 + a_1 x + b_1$$
$$E_2 : y^2 = x^3 + a_2 x + b_2,$$

där $-4a_1 = g_2(\Lambda_1),\ -4b_1 = g_3(\Lambda_1)$ och motsvarande för E_2. Enligt Sats 2.1b existerar ett nollskilt $\mu \in \mathbb{C}$ så att

$$a_2 = \mu^4 a_1, \quad b_2 = \mu^6 b_1,$$

och om vi låter $\lambda = \mu^{-1}$ får vi

$$\begin{aligned} g_2(\Lambda_2) &= \lambda^{-4} g_2(\Lambda_1) = g_2(\lambda\Lambda_1), \\ g_3(\Lambda_2) &= \lambda^{-6} g_3(\Lambda_1) = g_3(\lambda\Lambda_1). \end{aligned} \tag{$\triangle$}$$

Vi har enligt Sats 3.4 att

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

och derivering på bägge sidor ger

$$\begin{aligned} 2\wp'\wp'' &= 12\wp^2\wp' - g_2\wp' \\ \wp'' &= 6\wp^2 - \frac{g_2}{2}. \end{aligned} \tag{$\star$}$$

Enligt Proposition 3.2 så har vi i en omgivning till 0 att

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty}(2n+1)G_{2n+2}z^{2n} = \frac{1}{z^2} + \sum_{n=1}^{\infty} a_n z^{2n},$$

där $a_1 = \frac{g_2}{20}$ och $a_2 = \frac{g_3}{28}$. Vi jämför koefficienter i ($\star$) och får

$$\begin{aligned} (2n+2)(2n+1)a_{n+1} &= 6\left(\sum_{k=1}^{n-1} a_k a_{n-k} + 2a_{n+1}\right) \\ \implies a_{n+1} &= \frac{6}{(2n+2)(2n+1) - 12}\sum_{k=1}^{n-1} a_k a_{n-k}. \end{aligned}$$ □

Denna rekursionsformel bestämmer entydigt Laurentserien till $\wp(z) = \wp_{\Lambda_1}(z)$ och därmed hela funktionen. Vi använder oss av detta i ($\triangle$) och får att

$$\wp_{\Lambda_2}(z) = \wp_{\lambda\Lambda_1}(z) \implies \Lambda_2 = \lambda\Lambda_1 \implies \Lambda_2 \cong \Lambda_1.$$

En direkt tillämpning av detta resultat ger nu följande korollarium.

Korollarium 4.1. *Två gitter Λ_1 och Λ_2 är homotetiska om och endast om de motsvarande elliptiska kurvorna E_1 respektive E_2 är isomorfa. Med andra ord har vi en injektiv funktion*

$$\{\substack{\textit{Homotetiklasser} \\ \textit{av gitter } \Lambda\subset\mathbb{C}}\} \hookrightarrow \{\substack{\textit{Isomorfiklasser av} \\ \textit{elliptiska kurvor} \\ \textit{över } \mathbb{C}.}\}.$$

Vårt mål är att visa att detta är en bijektion, så det som kvarstår är att visa surjektivitet. Vi formulerade utan bevis i Sats 2.1c att varje komplext tal är j-invariant till en elliptisk kurva. Det räcker alltså om vi kan visa samma sak för j-invarianter till gitter.

Låt $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ vara ett gitter, orienterat så att $\operatorname{Im}\frac{\omega_1}{\omega_2} > 0$. Då gäller att

$$\Lambda \cong \mathbb{Z}\frac{\omega_1}{\omega_2} + \mathbb{Z},$$

och för $\tau \in \mathbb{H} = \{z \in \mathbb{C} \mid \operatorname{Im}(z) > 0\}$ så skriver vi $\Lambda_\tau = \mathbb{Z}\tau + \mathbb{Z}$. Detta möjliggör följande definition.

Definition 4.3. ***j-funktionen*** *är funktionen*

$$\begin{aligned} j : \mathbb{H} &\to \mathbb{C} \\ \tau &\mapsto j(\mathbb{Z}\tau + \mathbb{Z}). \end{aligned}$$

Funktionerna g_2, g_3, Δ definieras analogt.

Notera att om τ ligger i $\mathbb{H}$ så gör även $-\frac{1}{\tau}$ och $\tau+1$ det.

Sats 4.3. *Funktionen j definerad ovan är holomorf på hela $\mathbb{H}$ och uppfyller*

$$j(-\frac{1}{\tau}) = j(\tau) \text{ och } j(\tau+1) = j(\tau).$$

Bevis. Låt $\Lambda = \mathbb{Z}\tau + \mathbb{Z}$. Från definitionerna av j, g_2, g_3 har vi att

$$j(\tau) = 1728\frac{g_2(\tau)^3}{g_2(\tau)^3 - 27g_3(\tau)^2},$$

och vi kan skriva

$$g_2(\tau) = 60 \sum_{\substack{m,n\in\mathbb{Z}\\(m,n)\neq(0,0)}} \frac{1}{(m+n\tau)^4}, \quad g_3(\tau) = 140 \sum_{\substack{m,n\in\mathbb{Z}\\(m,n)\neq(0,0)}} \frac{1}{(m+n\tau)^6}.$$

Ett argument analogt med det i Sats 3.2 visar att $g_2(\tau)$ och $g_3(\tau)$ konvergerar absolut på hela $\mathbb{H}$, och likformigt på varje kompakt delmängd till $\mathbb{H}$. Alltså är g_2 samt g_3 och därmed Δ holomorfa funktioner, och eftersom $\Delta(\tau) \neq 0$ enligt Proposition 4.2 måste även j vara holomorf.

Den andra delen av satsen följer direkt av Sats 4.2 och observationerna

$$\mathbb{Z}\tau + \mathbb{Z} \cong \mathbb{Z} + \frac{1}{\tau}\mathbb{Z}, \quad \mathbb{Z}(\tau+1) + \mathbb{Z} = \mathbb{Z}\tau + \mathbb{Z}. \qquad \square$$

Lemma 4.3. *(a) Om $\Lambda \subset \mathbb{C}$ är ett gitter med två baser ω_1, ω_2 och ω_1', ω_2', orienterade så att $\frac{\omega_1}{\omega_2}, \frac{\omega_1'}{\omega_2'} \in \mathbb{H}$, gäller att*

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix} = \begin{bmatrix} \omega_1' \\ \omega_2' \end{bmatrix}$$

för någon matris $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) = \{A \in \mathbb{Z}^{2\times 2} \mid \det A = 1\}$.

(b) Låt $\tau_1, \tau_2 \in \mathbb{H}$. Då gäller $\Lambda_{\tau_1} \cong \Lambda_{\tau_2}$ om och endast om det finns en matris $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ sådan att $\tau_2 = \frac{a\tau_1+b}{c\tau_1+d}$.

Bevis. Antag att Λ har två baser, orienterade som innan:

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \mathbb{Z}\omega_1' + \mathbb{Z}\omega_2'.$$

Då finns $a, b, c, d, a', b', c', d' \in \mathbb{Z}$ så att

$$\begin{aligned} \omega_1' &= a\omega_1 + b\omega_2, \quad \omega_1 = a'\omega_1' + b'\omega_2' \\ \omega_2' &= c\omega_1 + d\omega_2, \quad \omega_2 = c'\omega_1' + d'\omega_2'. \end{aligned}$$

Genom substitution och vårt antagande att ω_1, ω_2 är linjärt oberoende fås

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \implies \det \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \pm 1,$$

men en snabb räkning ger (tack vare vårt val av orientering) att

$$0 < \mathrm{Im}\left(\frac{\omega_1'}{\omega_2'}\right) = \frac{(ad-bc)\,\mathrm{Im}(\omega_1/\omega_2)}{|c(\omega_1/\omega_2)+d|^2} \tag{1}$$

så determinanten måste vara positiv, vilket bevisar (a). Vi använder (a) för att visa (b). Låt $\Lambda_{\tau_1} \cong \Lambda_{\tau_2}$. Då finns en matris $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ så att

$$\left.\begin{aligned} \tau_2 &= a\alpha\tau_1 + b\alpha \\ 1 &= c\alpha\tau_1 + d\alpha \end{aligned}\right\} \implies \tau_2 = \frac{a\tau_1+b}{c\tau_1+d}.$$

Omvänt fås att om $\tau_2 = \frac{a\tau_1+b}{c\tau_1+d}$ att

$$(c\tau_1 + d)\,(\mathbb{Z}\tau_2 + \mathbb{Z}) = \mathbb{Z}(a\tau_1 + b)\mathbb{Z}(c\tau_1 + d) = \mathbb{Z}\tau_1 + \mathbb{Z},$$

så $\Lambda_{\tau_1} \cong \Lambda_{\tau_2}$ och beviset är klart. □

Efter detta resultat är det naturligt att definiera en gruppverkan av $\mathrm{SL}_2(\mathbb{Z})$ på $\mathbb{H}$:

$$\gamma\tau = \frac{a\tau + b}{c\tau + d} \text{ för } \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Att $\gamma\tau$ ligger i $\mathbb{H}$ följer av (1) ovan. Vi kontrollerar att detta definierar en gruppverkan, det vill säga att vi har en grupphomomorfi $\mathrm{SL}_2(\mathbb{Z}) \to \operatorname{Sym}\mathbb{H}$. Låt γ_1, γ_2 vara matriserna $\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$ respektive $\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$ och τ vara en punkt i $\mathbb{H}$. Då gäller att

$$\gamma_2(\gamma_1(\tau)) = \frac{a_2\frac{a_1\tau+b_1}{c_1\tau+d_1} + b_2}{c_2\frac{a_1\tau+b_1}{c_1\tau+d_1} + d_2} = \frac{(a_1a_2 + b_2c_1)\tau + (a_2b_1 + b_2d_1)}{(a_1c_2 + c_1d_2)\tau + (b_1c_2 + d_1d_2)} = (\gamma_2\gamma_1)(\tau).$$

I och $-I$ är de enda matriser som har trivial verkan på $\mathbb{H}$, eftersom

$$\gamma\tau = \tau\ \forall\tau \in \mathbb{H} \implies c\tau^2 - (d-a)\tau - b = 0\ \forall\tau \in \mathbb{H} \implies\ c = b = 0,\ d = a,$$

och $\det\gamma = 1$ så $d = a = \pm 1$. Detta leder oss till följande viktiga definition.

Definition 4.4. *Den **modulära gruppen** definieras som*

$$\Gamma = \mathrm{SL}_2(\mathbb{Z})\big/\{\pm 1\}.$$

Efter denna definition kan vi direkt formulera följande korollarium till Lemma 4.3b och Sats 4.2.

Korollarium 4.2. *Låt $\tau, \tau' \in \mathbb{H}$. Då gäller att*

$$j(\tau) = j(\tau') \iff \gamma\tau = \tau' \text{ för något } \gamma \in \Gamma.$$

Γ innehåller två extra viktiga element, $S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ och $T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ med motsvarande transformationer $\tau \mapsto -\frac{1}{\tau}$ respektive $\tau \mapsto \tau + 1$ som vi behandlade i Sats 4.3. Dessa element genererar Γ, det vill säga varje matris i Γ kan skrivas som en produkt av S, T och dessas inverser. Vi skriver $\Gamma = \langle S, T\rangle$.

Sats 4.4. *S och T, definierade som ovan, genererar gruppen Γ.*

Bevis. Låt $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma$. Vi vill visa att γ kan skrivas som en produkt av S, S^{-1}, T och T^{-1}. Vi delar upp beviset i tre fall:
$\underline{a = 0}$: Om $a = 0$ fås $bc = -1 \implies b = -c = \pm 1 \implies \gamma\tau = \frac{\pm 1}{\pm\tau+d} \implies \gamma = ST^{\pm d}$.
$\underline{a = \pm 1}$: Vi kan anta $a = 1$ eftersom $\frac{-a\tau-b}{-c\tau-d} = \frac{a\tau+b}{c\tau+d}$. Då har vi $d - bc = 1$, och vi får att

$$T^cS\gamma\tau = T^cS\left(\frac{\tau + b}{c\tau + d}\right) = T^c\left(\frac{-c\tau - d}{\tau + b}\right) = -\frac{1}{z + b},$$

och nu kan vi tillämpa resonemanget från första fallet.
$\underline{|a| > 1}$: Vi kan anta att $|a| > |c|$ (ersätt annars γ med $S\gamma$). Vårt mål är att bryta ut faktorer i γ på ett sådant sätt att vi får $\gamma = A\gamma_1$ för någon $A \in \langle S, T\rangle$ där $\gamma_1 = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$ uppfyller $|a_1| < |a|$ och $|c_1| < |c|$. Om vi upprepar denna process kommer vi till sist få $|a|, |c| = \pm 1$ och vara tillbaka på andra fallet. Låt $n = \left[\frac{a}{c}\right] = \frac{a}{c} - \left\{\frac{a}{c}\right\}$, avrundning nedåt till närmsta heltal. Då fås

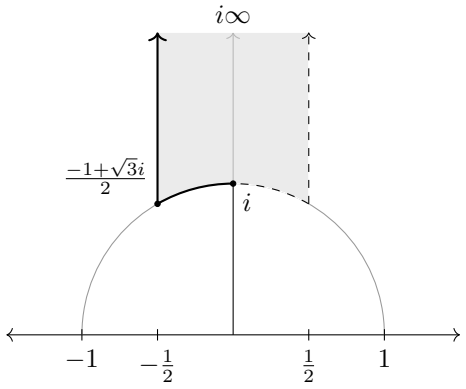
$$|a - nc| = |c\left\{\frac{a}{c}\right\}| < |c| < |a|.$$

För detta n får vi

$$T^{-n}\gamma\tau = T^{-n}\left(\frac{a\tau+b}{c\tau+d}\right) = \frac{(a-nc)\tau+(b-nd)}{c\tau+d}.$$

Slutligen multiplicerar vi med S för att byta plats på a och c, och får alltså

$$\gamma_1 = ST^{-n}\gamma. \qquad \square$$



Figur 7: Ett fundamentalområde till Γ.

Proposition 4.1. *Definiera (se Figur 7)*

$$\mathcal{F} = \{\tau \in \mathbb{H} \mid |\tau| \geq 1,\ \mathrm{Re}(\tau) \in [-1/2,\ 1/2),\ \mathrm{Re}(\tau) > 0 \implies |\tau| > 1\}.$$

Då finns för varje τ en unik Γ-representant (ett element ur $\mathrm{Orb}(\tau)$) i $\mathcal{F}$. Med andra ord, $\mathcal{F}$ är ett fundamentalområde för Γ:s verkan på $\mathbb{H}$.

Bevis. Låt $\tau \in \mathbb{H}$. Vi vill visa att det finns ett unikt $\tau' \in \mathcal{F}$ sådant att $\gamma\tau = \tau'$ för något $\gamma \in \Gamma$. Vi börjar med att visa existens. För alla $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma$ gäller som i beviset till Lemma 4.3a) att

$$\mathrm{Im}(\gamma\tau) = \frac{\mathrm{Im}(\tau)}{|c\tau+d|^2}. \qquad (\star)$$

Låt $c\tau + d \in \Lambda_\tau$ ha minimal längd bland gitterelementen utanför origo. Då måste c och d vara relativt prima, och vi kan därför hitta a, d sådana att $ad - bc = 1$. Då gäller att matrisen $\gamma_0 = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma$ maximerar $\mathrm{Im}(\gamma\tau)$. Välj nu $\gamma = T^k\gamma_0$ sådant att $\mathrm{Re}(\gamma\tau) \in [1/2,\ 1/2)$. Då är $\mathrm{Im}(\gamma\tau) = \mathrm{Im}(\gamma_0\tau)$ fortfarande maximal, och vi måste ha att $|\gamma\tau| \geq 1$ eftersom vi annars får $\mathrm{Im}(S\gamma\tau) > \mathrm{Im}(\gamma\tau)$ vilket motsäger vårt val av γ_0. Slutligen, om $\gamma\tau \notin \mathcal{F}$ så måste $|\gamma\tau| = 1$ och $\mathrm{Re}(\tau) > 0$, men då fås $S\gamma\tau \in \mathcal{F}$, vilket avslutar beviset av existens.

Det återstår att visa entydighet. Vi visar att två punkter $\tau_1\tau_2 \in \mathcal{F}$ som hör till samma Γ-klass måste sammanfalla. Antag $\tau_2 = \gamma_1\tau_1$ för något $\gamma_1 = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma$ och $\mathrm{Im}(\tau_1) \leq \mathrm{Im}(\tau_2)$. Enligt $(\star)$ gäller $|c\tau_1 + d|^2 \leq 1$, och vi får

$$1 \geq |c\tau_1+d|^2 = c^2|\tau_1|^2 + d^2 + 2cd\,\mathrm{Re}(\tau_1) \geq c^2|\tau_1|^2 + d^2 - |cd| \geq 1, \qquad (\star\star)$$

där den sista olikheten följer av att $|\tau_1| \geq 1$ och att c, d är heltal, åtminstone en av dem nollskild. Alltså är olikheterna likheter, och vi har $|c\tau_1 + d| = 1$. Vi använder detta i $(\star)$ och $(\star\star)$ för att få

$$\mathrm{Im}(\tau_2) \overset{(\star)}{=} \mathrm{Im}(\tau_1), \quad |c|, |d| \overset{(\star\star)}{\leq} 1.$$

Vi kan anta att $c \geq 0$ eftersom $\gamma = -\gamma$ i Γ. Vi får tre fall som vi behandlar separat.
$\underline{c = 0}$: Vi får $|d| = 1$ och $a = d$. Med andra ord, $\tau_1 = \tau_2 \pm b$ men

$$|\operatorname{Re}(\tau_1) - \operatorname{Re}(\tau_2)| < 1 \implies b = 0 \implies \tau_1 = \tau_2.$$

$\underline{c = 1,\ d = 0}$: I detta fall måste $b = -1$ och enligt ovan har vi $|c\tau_1 + d| = |\tau_1| = 1$. Detta ger $\tau_2 = a - \frac{1}{\tau_1}$, och vi får antingen $\tau_1 = \tau_2 = i$ om $a = 0$ eller $\tau_1 = \tau_2 = e^{2\pi i/3}$ om $a = -1$.
$\underline{c = 1,\ |d| = 1}$: Här gäller $|\tau_1 + d| = 1$ så $\tau_1 = e^{2\pi i/3}$ och eftersom $\operatorname{Im}(\tau_1) = \operatorname{Im}(\tau_2) = \frac{\sqrt{3}}{2}$ fås $\tau_1 = \tau_2$.
I samtliga fall gäller alltså $\tau_1 = \tau_2$, vilket är vad vi ville visa. □

Sats 4.5. *Restriktionen $j|_{\mathcal{F}}$ definierar en bijektion $\mathcal{F} \to \mathbb{C}$.*

Bevis. Injektivitet följer direkt av Korollarium 4.2 och Proposition 4.1. Det återstår att visa surjektivitet. Vi har att

$$g_2(\tau) = 60 \sum_{\substack{m,n\in\mathbb{Z}\\(m,n)\neq(0,0)}} \frac{1}{(m+n\tau)^4} = 60\left(2\sum_{m=1}^{\infty}\frac{1}{m^4} + \sum_{\substack{m,n\in\mathbb{Z}\\n\neq 0}}\frac{1}{(m+n\tau)^4}\right).$$

Den andra termen går mot 0 då $\operatorname{Im}(\tau) \to \infty$. Detta ger att

$$\lim_{\operatorname{Im}(\tau)\to\infty} g_2(\tau) = 120\sum_{m=1}^{\infty}\frac{1}{m^4} = 120\zeta(4) = 120\frac{\pi^4}{90} = \frac{4\pi^4}{3},$$

där $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ är Riemanns ζ-funktion. På samma sätt fås

$$\lim_{\operatorname{Im}(\tau)\to\infty} g_3(\tau) = 280\zeta(6) = 280\frac{\pi^6}{945} = \frac{8\pi^6}{27},$$

och därmed följer även

$$\lim_{\operatorname{Im}(\tau)\to\infty} \Delta(\tau) = \left(\frac{4\pi^4}{3}\right)^3 - 27\left(\frac{8\pi^6}{27}\right)^2 = 0.^5$$

Vi har alltså att

$$j(\tau) = \frac{g_2(\tau)^3}{\Delta(\tau)} \to \infty \text{ då } \operatorname{Im}(\tau) \to \infty.$$

Eftersom j är holomorf och icke-konstant så ger satsen om öppna avbildningar att $j(\mathbb{H})$ är en öppen delmängd till $\mathbb{C}$. Vi visar att $j(\mathbb{H})$ även är sluten för att kunna dra slutsatsen $j(\mathbb{H}) = \mathbb{C}$. Låt $\{j(\tau_k)\}$ vara en konvergent följd i $j(\mathbb{H})$, $\lim j(\tau_k) = w \in \mathbb{C}$. Eftersom j är Γ-invariant så kan vi anta att alla $j(\tau_k)$ ligger i $\mathcal{F}$. Eftersom $\{j(\tau_k)\}$ är konvergent och $j(\tau) \to \infty$ då $\operatorname{Im}(\tau) \to \infty$ så måste följden $\{\operatorname{Im}(\tau_k)\}$ vara begränsad, säg $|\operatorname{Im}(\tau_k)| \leq M\ \forall k$. Vi får alltså att

$$\tau_k \in \Omega = \{\tau \in \mathbb{H} \mid \operatorname{Re}(\tau) \in [-1/2, 1/2],\ \operatorname{Im}(\tau) \in [1/2, M]\}.$$

Ω är kompakt, och det följer att det finns en konvergent delföljd till $\{\tau_k\}$ som konvergerar mot något $\tau \in \Omega$. Eftersom j är kontinuerlig får vi $j(\tau) = w$. Vi har alltså visat att $j(\mathbb{H})$ innehåller alla sina hopningspunkter och är därmed sluten. Det följer att $j(\mathbb{H}) = \mathbb{C}$ och Proposition 4.1 ger att $j(\mathcal{F}) = \mathbb{C}$, vilket avslutar beviset. □

Vi sammanfattar våra resultat i följande korollarium.

Korollarium 4.3. *(Uniformiseringssatsen, del 2)*
Till varje elliptisk kurva E över $\mathbb{C}$ finns ett gitter $\Lambda \subset \mathbb{C}$ sådant att $E = E_\Lambda$.

[5] Detta förklarar varför 60 och 140 dyker upp i definitionerna av g_2, g_3. Det är det minsta paret av heltal som gör att gränsvärdet ovan går mot 0.

Bevis. Låt E vara en elliptisk kurva och tag $\tau \in \mathbb{H}$ så att $j(\tau) = j(E)$. Låt $\Lambda_1 = \mathbb{Z}\tau + \mathbb{Z}$. Vi får att

$$j(E) = j(\tau) = j(\Lambda_1) = j(E_{\Lambda_1})$$

så $E \cong E_{\Lambda_1}$ enligt sats 2.1a. □

Vi kan nu kombinera del 1 och 2 för att få följande sats som är huvudresultatet i denna uppsats.

Sats 4.6. *(Uniformiseringssatsen)*
Det finns en bijektion

$$\{\textit{Homotetiklasser av gitter } \Lambda \subset \mathbb{C}\} \to \{\textit{Isomorfiklasser av elliptiska kurvor över } \mathbb{C}\}$$
$$[\Lambda] \to [E_\Lambda],$$

och till varje Λ *(eller* E_Λ*) en gruppisomorfi*

$$\mathbb{C}/\Lambda \to E_\Lambda$$
$$z \mapsto [\wp_\Lambda(z) : \wp'_\Lambda(z) : 1].$$

5 Korollarier

I detta kapitel diskuterar vi följder av Uniformiseringssatsen. Alla resultat finns i [Su17], bortsett från Sats 5.3 som är [Sil, Sats VI.5.5]. Vi börjar med att undersöka relationen mellan den algebraiska och den analytiska beskrivningen av elliptiska kurvor närmre.

Låt Λ_1 och Λ_2 vara gitter. Vi har inte definierat begreppet komplex mångfald, än mindre vad en holomorf avbildning mellan sådana är, men för funktioner $\mathbb{C}/\Lambda_1 \xrightarrow{\psi} \mathbb{C}/\Lambda_2$ innebär det att det finns en holomorf funktion f som gör följande diagram kommutativt:

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{f} & \mathbb{C} \\ {\scriptstyle \pi_1}\downarrow & & \downarrow{\scriptstyle \pi_2} \\ \mathbb{C}/\Lambda_1 & \xrightarrow{\psi} & \mathbb{C}/\Lambda_2 \end{array} \tag{D}$$

Att diagrammet kommuterar innebär att $\psi \circ \pi_1 = \pi_2 \circ f$. Här betecknar π_1, π_2 projektionerna $z \mapsto [z]$. Vi noterar att om det existerar ψ, f enligt (D) så finns det alltid f^* med $f^*(0) = 0$ som ger att (D) kommuterar. Mängden av holomorfa avbildningar $\mathbb{C}/\Lambda_1 \xrightarrow{\psi} \mathbb{C}/\Lambda_2$ med $\psi([0]) = [0]$ skrivs $\mathrm{Hom}(\mathbb{C}/\Lambda_1, \mathbb{C}/\Lambda_2)$.

Låt nu $\alpha \in \mathbb{C}$. Vi definierar en grupphomomorfi

$$\psi_\alpha : \mathbb{C} \to \mathbb{C}$$
$$z \to \alpha z.$$

Om nu $\alpha\Lambda_1 \subseteq \Lambda_2$ så inducerar ψ_α en väldefinierad holomorf homomorfi

$$\psi_\alpha : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$$
$$[z] \to [\alpha z].$$

Sats 5.1. *Låt* Λ_1, Λ_2 *vara gitter. Med notation som ovan har vi en bijektion*

$$\{\alpha \in \mathbb{C} \mid \alpha\Lambda_1 \subseteq \Lambda_2\} \to \mathrm{Hom}(\mathbb{C}/\Lambda_1, \mathbb{C}/\Lambda_2)$$
$$\alpha \mapsto \psi_\alpha.$$

Bevis. Vi bevisar att tilldelningen $\alpha \mapsto \psi_\alpha$ är bijektiv. Om $\psi_\alpha = \psi_\beta$ så har vi för alla z att

$$\alpha z \equiv \beta z \pmod{\Lambda_2},$$

vilket ger att $\psi_{\alpha-\beta}(\mathbb{C}) \subseteq \Lambda_2$, men Λ_2 är diskret och $\psi_{\alpha-\beta}$ kontinuerlig. Därmed är $\psi_{\alpha-\beta}(z) = 0$ så $\alpha - \beta = 0$ vilket visar injektivitet.

Det återstår att visa surjektivitet. Låt ψ vara en holomorf funktion med $\psi(0) = 0$. Enligt ovan kan vi lyfta ψ till en holomorf funktion $f : \mathbb{C} \to \mathbb{C}$ med $f(0) = 0$ och vi erhåller ett diagram som (D) ovan. Av kommutativitet följer att

$$f(z + \omega) \equiv f(z) \pmod{\Lambda_2} \ \forall z \in \mathbb{C},\ \omega \in \Lambda_1.$$

Vi får att $f(z + \omega) - f(z) \in \Lambda_2$ för alla z och eftersom Λ_2 är diskret måste $f(z + \omega) - f(z)$ vara konstant (som funktion av z). Vi deriverar och får

$$f'(z + \omega) = f'(z) \quad \forall z \in \mathbb{C},\ \omega \in \Lambda_1,$$

så f' är en holomorf elliptisk funktion och därmed konstant enligt 3.1. Vi får att $f(z) = \alpha z + \beta$, men eftersom $f(0) = 0$ så har vi $\beta = 0$, och eftersom $f(\Lambda_1) \subseteq \Lambda_2$ gäller $\alpha\Lambda_1 \subseteq \Lambda_2$. Med andra ord har vi

$$\psi = \psi_\alpha,$$

vilket bevisar surjektivitet. □

Kom ihåg att isogenier är rationella avbildningar mellan elliptiska kurvor som bevarar identitetselementet O. Skriv $\mathrm{Hom}(E_1, E_2) = \{\text{Isogenier } E_1 \xrightarrow{\rho} E_2\}$. Vi visar nu att dessa står i bijektiv korrespondens med holomorfa avbildningar.

Sats 5.2. *Låt Λ_1, Λ_2 vara gitter och E_1, E_2 de motsvarande elliptiska kurvorna. Då är inklusionen*

$$\mathrm{Hom}(E_1, E_2) \hookrightarrow \mathrm{Hom}(\mathbb{C}/\Lambda_1, \mathbb{C}/\Lambda_2)$$

en bijektion.

Bevis. Isogenier ges lokalt av överallt definierade rationella funktioner och definierar därför holomorfa funktioner $\mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$, alltså är den påstådda bijektionen väldefinierad. Vidare är den injektiv ty två isogenier definierar samma holomorfa funktion om och endast om de överensstämmer på varje punkt, det vill säga är samma funktion.

Det återstår att visa att funktionen är surjektiv. Låt därför $\psi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ vara holomorf och uppfylla $\psi(0) = 0$. Enligt (a) kan vi skriva $\psi = \psi_\alpha$ för något $\alpha \in \mathbb{C}$ sådant att $\alpha\Lambda_1 \subseteq \Lambda_2$, definierad enligt ovan. Låt $\wp_1 = \wp_{\Lambda_1},\ \wp_2 = \wp_{\Lambda_2}$. Vi får en inducerad avbildning

$$\begin{aligned} E_1 &\to E_2 \\ [\wp_1(z) : \wp_1'(z) : 1] &\mapsto [\wp_2(\alpha z) : \wp_2'(\alpha z) : 1], \end{aligned}$$

som vi vill visa ges av rationella funktioner. Med andra ord vill vi visa att

$$\wp_2(\alpha z),\ \wp_2'(z) \in \mathbb{C}(\wp_1(z), \wp_1'(z)).$$

Men eftersom $\alpha\Lambda_1 \subseteq \Lambda_2$ så har vi för $\omega \in \Lambda_1$ att

$$\wp_2(\alpha(z + \omega)) = \wp_2(\alpha z + \alpha\omega) = \wp_2(\alpha z).$$

Samma resonemang för $\wp'$ ger nu ihop med Sats 3.3 att

$$\wp_2(\alpha z),\ \wp_2'(\alpha z) \in \mathbb{C}(\Lambda_1) = \mathbb{C}(\wp_1(z), \wp_1'(z)).$$ □

Vi återvänder till E som grupp. Vi nämnde i inledningen att det är önskvärt att förstå gruppstrukturen hos elliptiska kurvor. Uniformiseringssatsen ger oss en beskrivning som är enkel att förstå sig på. Den möjliggör bland annat följande karakterisering av ändliga delgrupper.

Korollarium 5.1. *Låt E vara en elliptisk kurva, $m \geq 2$ samt $E[m] = \{P \in E \mid mP = O\}$. Då gäller*

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Bevis. Låt E vara en elliptisk kurva och $m \geq 2$. Då gäller $E \cong \mathbb{C}/\Lambda$ för något $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. Vi får

$$\begin{aligned} E[m] &= (\mathbb{C}/\Lambda)[m] \\ &= \{[z] \in \mathbb{C}/\Lambda \mid mz \in \Lambda\} \\ &= \{\left[\frac{a\omega_1 + b\omega_2}{m}\right] \in \mathbb{C}/\Lambda \mid a, b \in \mathbb{Z}\} \\ &= \{\left[\frac{a}{m}\omega_1\right] + \left[\frac{b}{m}\omega_2\right] \in \mathbb{C}/\Lambda \mid a, b \in \mathbb{Z}\} \\ &\cong \mathbb{Z}/_{m\mathbb{Z}} \times \mathbb{Z}/_{m\mathbb{Z}}. \end{aligned}$$

□

Utöver att förstå delgrupper kan vi undersöka endomorfier, det vill säga grupphomomorfier $E \to E$. Under punktvis addition bildar dessa en grupp som vi betecknar $\mathrm{Hom}(E, E)$ eller $\mathrm{End}(E)$. Detta kapitels resultat möjliggör en klassificering av endomorfiringar till elliptiska kurvor. Kom ihåg att en kvadratisk utvidgning av $\mathbb{Q}$ är en kroppsutvidgning $\mathbb{Q} \subset \mathbb{Q}(\sqrt{d})$ där $d \neq 0, 1$ är ett kvadratfritt heltal. Om $d < 0$ kallas utvidgningen för imaginär. En **ordning** till en kvadratisk utvidgning $\mathcal{K}$ är en delring $\mathcal{O} \subseteq \mathcal{K}$ där den underliggande additiva delgruppen är genererad av två element. Exempelvis har vi att $\mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}]$ och $\mathbb{Z}[2i]$ är ordningar till $\mathbb{Q}(i)$.

Sats 5.3. *Låt E vara en elliptisk kurva och $\mathbb{Z}\tau + \mathbb{Z}$ dess associerade gitter. Då gäller en av följande:*

(a) $\mathrm{End}(E) \cong \mathbb{Z}$.

(b) $\mathbb{Q}(\tau)$ *är en kvadratisk imaginär utvidgning och*

$$\mathrm{End}(E) \cong \mathcal{O} \text{ för någon ordning } \mathcal{O} \subset \mathbb{Q}(\tau).$$

Bevis. Låt $\mathcal{O} = \{\alpha \mid \alpha\Lambda \subseteq \Lambda\} \cong \mathrm{End}(E)$ enligt tidigare resultat. För varje $\alpha \in \mathcal{O}$ gäller då att det finns $a, b, c, d \in \mathbb{Z}$ så att

$$\alpha = a + b\tau, \quad \alpha\tau = c + d\tau.$$

Vi eliminerar τ och får:

$$\alpha^2 - (a + d)\alpha - (ad - bc) = 0,$$

så varje $\alpha \in \mathcal{O}$ är helt över $\mathbb{Z}$, det vill säga är rot till ett moniskt polynom med koefficienter i $\mathbb{Z}$. Antag nu att $\mathcal{O} \neq \mathbb{Z}$ och välj $\alpha \in \mathcal{O} \setminus \mathbb{Z}$. Då måste b ovan vara nollskild, och om vi eliminerar α fås

$$b\tau^2 + (a - d)\tau - c = 0,$$

så $\mathbb{Q}(\tau)$ är en kvadratisk imaginär utvidgning. Slutligen fås eftersom $\mathcal{O}$ är hel över $\mathbb{Z}$ att $\mathcal{O} = \mathbb{Z}(n\tau) + \mathbb{Z}$. □

Innebörden i Sats 5.3 är enklast att förstå geometriskt genom att betrakta fundamentalparallellogrammen som spänns av $\{\tau, 1\}$ och identifiera motstående sidor. Det finns alltid endomorfier $m_* : z \mapsto mz$ med $\mathrm{Ker}\, m_* = E[m]$ som svarar mot skalningar av gittret. I vissa fall finns ytterligare endomorfier som ges av rotationer ihop med skalningar. Vi illustrerar med tre exempel. De Gaussiska heltalen, $\mathbb{Z}i + \mathbb{Z}$, har en avbildning $i_* : z \mapsto iz$ som roterar gittret 90° moturs. Notera att detta är en bijektion och således en automorfi. Tittar vi istället på det liknande exemplet $\mathbb{Z}(2i) + \mathbb{Z}$ har vi endomorfin $(2i)_*$ som inte är en automorfi. Sats 5.3 säger oss att $\mathbb{Z}(\pi i) + \mathbb{Z}$ inte har några endomorfier förutom m_* för $m \in \mathbb{Z}$.

6 Appendix

6.1 Projektiva rum

Låt k vara en kropp. Betrakta följande ekvivalensrelation på k^{n+1}

$$(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n) \iff \exists \lambda \in k^\times : \ (\lambda x_0, \ldots, \lambda x_n) = (y_0, \ldots, y_n).$$

Att $\sim$ definierar en ekvivalensrelation bevisar vi inte här.

Definition 6.1. *Låt k vara en kropp. Vi definierar **projektiva n-rummet** (över k) som*

$$\mathbb{P}^n(k) = {}^{k^{n+1} - (0,\ldots,0)}\!/_{\sim}$$

där $\sim$ definieras som ovan.

Det följer av definitionen att varje element i $\mathbb{P}^n$ har representanter $[x_0 : \cdots : x_n]$ (där åtminstone en $x_j \neq 0$). Detta kallas för *homogena koordinater*. Vi noterar slutligen att punkter i

$$U_n = \mathbb{P}^n - \{[x_0 : \cdots : x_n] \in \mathbb{P}^n \mid x_n \neq 0\}$$

kan skalas ned med x_n vilket ger oss unika representanter $[x_0/x_n : x_1/x_n, \ldots, 1]$.

6.2 Funktionskroppar

Låt $F(X, Y, Z) = Y^2Z - X^3 - aXZ^2 - bZ^3 \in \mathbb{C}[X, Y, Z]$, och skriv E för kurvan bestämd av $F(X, Y, Z) = 0$ som i kapitel 2. Vi är intresserade av att studera polynomfunktioner samt rationella funktioner definierade på E. Eftersom vi infört homogena koordinater behövs ett visst mått av försiktighet då vi gör detta.

Kvotringen $\mathbb{C}[E] = {}^{\mathbb{C}[X,Y,Z]}\!/_{(F)}$ kallas för E:s **homogena koordinatring**. Eftersom F är irreducibelt är (F) ett primideal. Således är $\mathbb{C}[E]$ ett integritetsområde. Notera att $g \in \mathbb{C}[E]$ inte är väldefinierade som funktioner på homogena koordinater. Ett element $g \in \mathbb{C}[E]$ kallas för en **form** av grad d om det finns ett homogent polynom $G \in \mathbb{C}[X, Y, Z]$ av grad d så att $g = G + (F)$. Vi skriver $\deg g = d$.

Eftersom $\mathbb{C}[E]$ är ett integritetsområde kan vi bilda bråkkroppen $\mathrm{Frac}(\mathbb{C}[E])$. Vi definierar nu **funktionskroppen** till E som

$$\mathbb{C}(E) = \left\{ \frac{g}{h} \in \mathrm{Frac}(\mathbb{C}[E]) \mid g, h \text{ former av samma grad} \right\} \subset \mathrm{Frac}(\mathbb{C}[E]).$$

Detta är väldefinierade rationella funktioner på homogena koordinater, ty vi kan välja g, h homogena vilket ger

$$\frac{g(\lambda a, \lambda b, \lambda c)}{h(\lambda a, \lambda b, \lambda c)} = \frac{\lambda^d g(a, b, c)}{\lambda^d h(a, b, c)} = \frac{g(a, b, c)}{h(a, b, c)}.$$

Som namnet antyder bildar $\mathbb{C}(E)$ en kropp.

6.3 Härledning av g_2, g_3

Antag att vi har visat att

$$\wp'(z) = 4(\wp(z))^3 + g_2\wp(z) + g_3. \qquad (\star)$$

Vi påstår att denna ekvation bestämmer g_2, g_3 entydigt. Betrakta Laurentutvecklingarna till $\wp(z)$ och $\wp'(z)$ runt 0 (G_k är Eisensteinserien):

$$\wp(z) = \frac{1}{z^2} + z^2 \sum_{k=1}^{\infty} (2k+1) G_{2k+2} z^{2k-2},$$

$$\wp(z) = -\frac{2}{z^3} + z \sum_{k=1}^{\infty} (2k+1)(2k) G_{2k+2} z^{2k-2}.$$

Vi skriver ut termerna i ($\star$): (H_j betecknar holomorfa funktioner i en omgivning till 0)

$$\begin{aligned}
(\wp'(z))^2 &= \left(-\frac{2}{z^3} + z\sum_{k=1}^{\infty}(2k+1)(2k)G_{2k+2}z^{2k-2}\right)^2 \\
&= \frac{4}{z^6} + 2\frac{-2}{z^3}z\sum_{k=1}^{\infty}(2k+1)(2k)G_{2k+2}z^{2k-2} + z^2H_1(z) \\
&= \frac{4}{z^6} - \frac{4}{z^2}\left(6G_4 + 20G_6z^2 + z^4H_2(z)\right) + z^2H_1(z) \\
&= \frac{4}{z^6} - \frac{24G_4}{z^2} - 80G_6 + z^2H_3(z) \\
4(\wp(z))^3 &= 4\left(\frac{1}{z^2} + z^2\sum_{k=1}^{\infty}(2k+1)G_{2k+2}z^{2k-2}\right)^3 \\
&= \frac{4}{z^6} + 12\frac{1}{z^4}z^2\sum_{k=1}^{\infty}(2k+1)G_{2k+2}z^{2k-2} \\
&\quad + 12\frac{1}{z^2}z^4\left(\sum_{k=1}^{\infty}(2k+1)G_{2k+2}z^{2k-2}\right)^2 + 4z^6\left(\sum_{k=1}^{\infty}(2k+1)G_{2k+2}z^{2k-2}\right)^3 \\
&= \frac{4}{z^6} + \frac{12}{z^2}\left(3G_4 + 5G_6z^2 + z^4H_4(z)\right) + z^6H_5(z) \\
&= \frac{4}{z^6} + \frac{36G_4}{z^2} + 60G_6 + z^2H_6(z) \\
g_2\wp(s) &= \frac{g_2}{z^2} + z^2H_7(z)
\end{aligned}$$

Vi stoppar nu in dessa i ($\star$) och får

$$\begin{aligned}
\wp'(z) &= 4(\wp(z))^3 + g_2\wp(z) + g_3 \\
\frac{4}{z^6} - \frac{24G_4}{z^2} - 80G_6 + z^2H_3(z) &= \frac{4}{z^6} + \frac{36G_4}{z^2} + 60G_6 + z^2H_6(z) + \frac{g_2}{z^2} + z^2H_7(z) + g_3 \\
\frac{60G_4 + g_2}{z^2} + g_3 + 140G_6 + z^2H_8(z) &= 0,
\end{aligned}$$

så om ekvationen skall hålla måste $g_2 = -60G_4$ och $g_3 = -140G_6$. □

Referenser

[Ahl] L. Ahlfors, *Complex analysis*, tredje utgåvan, McGraw Hill, 1979.

[Sil] J.H. Silverman. *The Arithmetic of Elliptic Curves*, andra utgåvan, Springer, 1986.

[Su14] A. Sutherland. *Ordinary and supersingular elliptic curves*, föreläsningsanteckningar MIT. Tillgänglig: https://math.mit.edu/classes/18.783/2019/LectureNotes14.pdf [2019-05-02]

[Su15] A. Sutherland. *Elliptic curves over* $\mathbb{C}$ *(Part 1)*, föreläsningsanteckningar MIT. Tillgänglig: https://math.mit.edu/classes/18.783/2019/LectureNotes15.pdf [2019-05-02]

[Su16] A. Sutherland. *Elliptic curves over* $\mathbb{C}$ *(Part 2)*, föreläsningsanteckningar MIT. Tillgänglig: https://math.mit.edu/classes/18.783/2019/LectureNotes16.pdf [2019-05-02]

[Su17] A. Sutherland. *Complex multiplication*, föreläsningsanteckningar MIT. Tillgänglig: https://math.mit.edu/classes/18.783/2019/LectureNotes17.pdf [2019-05-02]