CHALMERS

GÖTEBORGS UNIVERSITET

Riemannhypotesen och Elliptiska Kurvor

Ett sammandrag av Riemannhypotesen för elliptiska kurvor över ändliga kroppar

The Riemann Hypothesis and Elliptic Curves

Examensarbete för kandidatexamen i matematik vid Göteborgs universitet
Kandidatarbete inom civilingenjörsutbildningen Teknisk matematik vid Chalmers

Max Carnesten
Tage Lindahl
Sebastian Miles
Daniel Szybek

Institutionen för Matematiska vetenskaper
CHALMERS TEKNISKA HÖGSKOLA
GÖTEBORGS UNIVERSITET
Göteborg, Sverige 2025

Riemannhypotesen och Elliptiska Kurvor

Ett sammandrag av Riemannhypotesen för elliptiska kurvor över ändliga kroppar

Examensarbete för kandidatexamen i matematik vid Göteborgs universitet
Daniel Szybek

Examensarbete för kandidatexamen i matematik inom Matematikprogrammet vid Göteborgs universitet
Tage Lindahl

Kandidatarbete i matematik inom civilingenjörsprogrammet Teknisk matematik vid Chalmers
Max Carnesten
Sebastian Miles

Handledare: Christian Johansson Institutionen för Matematiska Vetenskaper

Institutionen för Matematiska vetenskaper
CHALMERS TEKNISKA HÖGSKOLA
GÖTEBORGS UNIVERSITET
Göteborg, Sverige 2025

Förord

Vi presenterar i detta arbete en kort genomgång av Riemannhypotesen för elliptiska kurvor över ändliga kroppar. Texten utgår huvudsakligen ifrån *The Arithmetic of Elliptic Curves* av Joseph H. Silverman [1]. Vi utgår från att läsaren besitter goda kunskaper inom grundläggande algebra, inklusive grupp-, ring- och kroppteori. Vi vill även tacka vår handledare Christian Johansson för hans engagemang, rådgivning och förslag till uppsatsens ämne.

Gällande arbetsfördelningen så har vi uppdelat ansvaret för texten på följande vis:

- *Max Carnesten*: Kapitel 1, 4.6 och 5
- *Tage Lindahl*: Populärvetenskapliga presentationen, Sammandrag/Abstract samt kapitel 4.2 - 4.5
- *Sebastian Miles*: Kapitel 3 och 4.1
- *Daniel Szybek*: Kapitel 2

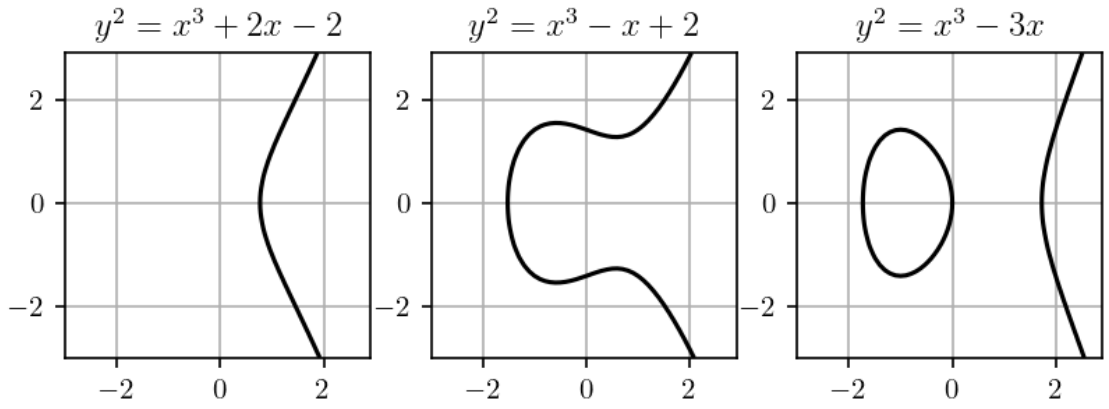
Vidare har Max Carnesten och Tage Lindahl haft ett övergripande ansvar för teori och korrekturläsning. För en mer detaljerad beskrivning av arbetsfördelningen har dagbok och tidslogg förts under arbetets gång.

Populärvetenskaplig presentation

Den 23 juni 1993 vände sig Andrew Wiles mot åhörarna i Isaac Newtons institut på universitetet i Cambridge och yttrade de idag bevingade orden "I think I'll stop there". Med det avslutade han den sista av tre föreläsningar i vilken han hade beskrivit sitt bevis av ett resultat som gäckat matematiker i 357 år, Fermats sista sats. Wiles bevis byggde på en länk mellan Fermats sista sats och *elliptiska kurvor* som upptäcktes av Gerhard Frey och som bevisades av Ken Ribet. Denna länk innebar att ett bevis av ett annat resultat, Taniyama-Shimuras förmodan, även skulle bevisa Fermats sista sats som ett specialfall. Detta är heller inte den enda gången i matematikens historia som elliptiska kurvor har fungerat som en sorts talteorins universalnyckel.

Ett annat liknande exempel finns att hitta inom studien av kongruenta tal. Ett tal n kallas *kongruent* om det finns en rätvinklig triangel med sidor av rationell längd med n som area. Det tog inte lång tid innan matematiker hade hittat flera exempel på kongruenta tal, men någon allmän algoritm för att avgöra om ett tal var kongruent eller inte dröjde, och frågan om dess existens blev känt som det *kongruenta talproblemet*. Än idag är problemet olöst, men matematikern Jerrold B. Tunnell lyckades år 1983 – genom att översätta problemet till elliptiska kurvor – hitta villkor som varje kongruent tal måste uppfylla, och speciellt om ett resultat om elliptiska kurvor – Birch-Swinnerton-Dyers förmodan – stämmer så är varje tal som uppfyller dessa villkor kongruent.

Idag är elliptiska kurvor ett viktigt verktyg inom den moderna talteorin och exemplen ovan är bara ett par av många fall där en översättning av problemet till elliptiska kurvor ger en möjlig väg till en lösning för problem som tillsynes kan verka omöjliga. Elliptiska kurvor spelar även en viktig roll inom IT-säkerhet där deras invecklade struktur ligger till grund för ett flertal viktiga krypteringsscheman.



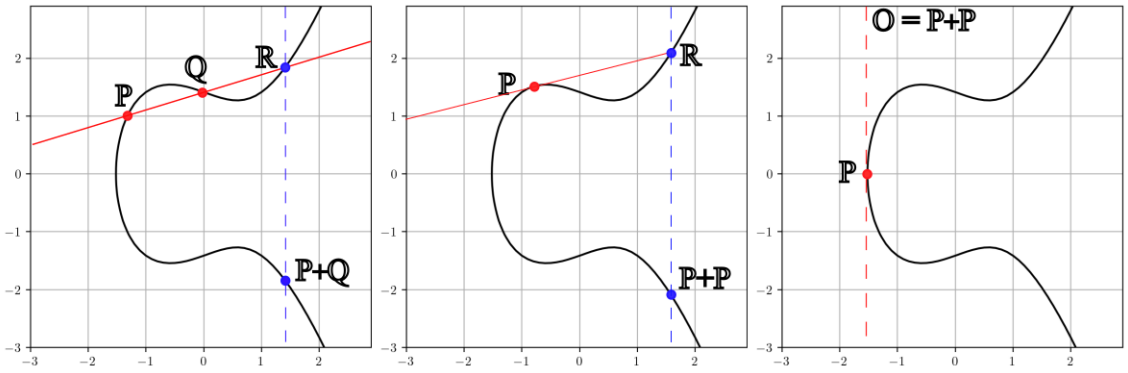
Figur 1: Några exempel på elliptiska kurvpr

Men vad är egentligen elliptiska kurvor och vad gör dem så speciella? En elliptisk kurva ges av en ekvation på formen

$$y^2 = x^3 + Ax + B$$

där A, B är rationella tal – i vilket fall kurvan sägs vara definierad över de rationella talen – eller komplexa tal. Punkter som ligger på den elliptiska kurvan är då precis de par x, y som uppfyller kurvans ekvation. I figur 1 kan vi se tre exempel på elliptiska kurvor.

Det fantastiska med elliptiska kurvor är att man kan skapa något som efterliknar additionen av heltal. Detta följer av att om man har två olika punkter på en elliptisk kurva, säg P och Q, så kommer linjen som passerar genom dem att garanterat passera en tredje punkt i kurvan, som vi kallar R (se figur 2). Vi kallar speglingen av R längst x-axeln för $P + Q$, alltså P "adderat" Q. För att addera en punkt P med sig själv så låter vi linjen istället vara tangentlinjen till kurvan i punkten P. Om man adderar en punkt till sig själv kan man dock få fall där tangenten inte skär den elliptiska kurvan igen, i det fallet säger vi att resultatet är "punkten i oändligheten" som vi betecknar O, och låter linjer som passerar genom O vara linjer parallela med y-axeln.



Figur 2: Figur över additionen på en elliptisk kurva. Till vänster ses additionen för två olika punkter, i mitten additionen för en punkt med sig själv och till höger ett fall där addition med sig själv ger punkten vid oändligheten.

Styrkan med additionen är om den elliptiska kurvan är definierad över rationella tal så ger den ett enkelt recept att hitta alla rationella punkter på kurvan, det vill säga punkter vars koordinater ges av rationella värden eller punkten vid oändligheten. Om man har två rationella punkter så kommer additionen av dessa garanterat ge en rationell punkt. Speciellt kommer additionen av en rationell punkt till sig själv ge en ny rationell punkt. Ett centralt resultat inom studien av elliptiska kurvor – Mordell-Weils sats – ger att det krävs endast ett ändligt antal rationella punkter för att man ska kunna hitta alla rationella punkter genom att addera redan kända rationella punkter, även om de rationella punkterna är oändligt många.

Därmed ges även en del av förklaringen till varför elliptiska kurvor är ett så kraftfullt verktyg inom talteorin. Många av problemen där handlar om att söka rationella lösningar till ekvationer, och genom att översätta den typen av problem till elliptiska kurvor får man tillgång till additionen över elliptiska kurvor och med det receptet för rationella punkter.

Sedan Andrew Wiles publicerade sitt bevis av Fermats Sista Sats har ett nytt problem tagit över rollen som matematikens heliga graal, nämligen Riemannhypotesen. Riemannhypotesen formodades av den tyske matematikern Bernhard Riemann år 1859 och har stora konsekvenser inom studien av primtalen, speciellt hur primtalen är fördelade bland heltalen. Vårt arbete fokuserar på ett parallelt problem till Riemannhypotesen som fås genom att man studerar hur rationella punkter är fördelade över elliptiska kurvor.

Sammandrag

Arbetet är en kort utläggning om Riemannhypotesen för elliptiska kurvor över ändliga kroppar. Texten öppnar med en introduktion till affina och projektiva varieteter inom algebraisk geometri, för att sedan avgränsa och specialisera teorin till kurvor. Huvuddelen av texten behandlar elliptiska kurvor och deras grupplag. Ett särskilt fokus läggs på morfier som bevarar grupplagen och verktyg som används för att studera dessa, bland annat invarianta differentialer. Vi avgränsar sedan teorin till elliptiska kurvor över ändliga kroppar, samt den så kallade Frobeniusendomorfin, som är central inom studien av rationella punkter. Avslutningsvis introducerar vi Tate-modulen och Weils e_m-parning, för att slutligen kombinera våra resultat och bevisa nämnda Riemannhypotesen.

Abstract

This paper is a short exposition of the Riemann hypothesis for elliptic curves over finite fields. Along the way we give a quick introduction to the notions of affine and projective varieties in algebraic geometry before specializing the theory to curves. The main body of the paper is dedicated to the study of elliptic curves and their properties, including their group law, morphisms preserving it and important tools in the study of said morphisms like the invariant differential. Narrowing our focus to elliptic curves over finite fields we consider the Frobenius endomorphism and its importance in the study of rational points. We then conclude the paper by introducing the Tate-module for elliptic curves as well as the Weil e_m-pairing, before combining our results to prove said Riemann hypothesis.

Innehåll

1 Inledning

1.1 Övergripande idé

Talteori studerar aritmetiska egenskaper av ringen $\mathbb{Z}$ av heltal och dess bråkkropp $\mathbb{Q}$. En central del inom talteorin är primtalen, vars egenskaper har drivit forskning framåt genom århundraden. En av de mest kända olösta problemen som handlar om primtalen är Riemannhypotesen. Riemannhypotesen utgår från den så kallade Riemannzetafunktionen $\zeta(s)$ där den får värdet $\sum_{n\geq 1} n^{-s} = \prod_p (1-p^{-s})^{-1}$ då realdelen av s är större än ett, annars används dess analytiska forsättning. Riemannhypotesen säger att alla komplexa rötter till $\zeta(s)$ är antingen av formen $-2n$ för $n \in \mathbb{Z}_+$ eller har realdel $\frac{1}{2}$. Ett känt resultat inom talteori säger att primtalsräknarfunktionen $\pi(x) = \#\{p \leq x \mid p \text{ prim}\}$ växer asymptotiskt med $\frac{x}{\log x}$ och en konsekvens av Riemannhypotesen är en bättre uppskattning, nämligen $\pi(x) = \mathrm{Li}(x) + O(\sqrt{x}\log x)$ där $\mathrm{Li}(x) = \int_2^x \frac{\mathrm{d}t}{\log t}$. Rötterna till Riemannzetafunktionen håller därför mycket information om distributionen av primtalen. [2]

Låt $\mathbb{F}_p$ vara kroppen $\mathbb{Z}/p\mathbb{Z}$ för ett primtal p och betrakta $A = \mathbb{F}_p[T]$ med sin bråkkropp $\mathbb{F}_p(T)$. Mycket av talteorin om heltalen har analoger för dessa polynomringar där primtalen ersätts med irreducibla polynom. Exempelvis så har A sin egna Riemannzetafunktion och Riemannhypotes. För ett ideal $I \subset A$ definierar vi normen $|I|$ att vara p upphöjt till antalet element i ringen A/I. För ett element $f \in A$ så definierar vi $|f| = |(f)|$. Vi vill påminna läsaren om att ett ideal $M \subset A$ är maximalt om det inte finns ideal $I \subset A$ så att $M \subset I \subset A$. Om $\mathrm{mSpec}(A)$ benämner mängden av maximala ideal i A, alltså de ideal som genereras av ett irreducibelt polynom, så kan vi definiera zetafunktionen

$$\zeta_A(s) = \prod_{P \in \mathrm{mSpec}(A)} \frac{1}{1-|P|^{-s}}$$

vilket är lika med serien

$$\zeta_A(s) = \sum_{\substack{f \in A \\ f \, monisk}} \frac{1}{|f|^{-s}}$$

Riemannhypotesen för A säger då att rötterna till $\zeta_A(s)$ har realdel $\frac{1}{2}$. I fallet för A kan man visa att $\zeta_A(s) = \frac{1}{1-p^{1-s}}$ vilket visar att Riemannhypotesen stämmer för polynomringar [3]. Vi kommer förlänga Riemannhypotesen till en annan klass av funktionskroppar som vi definierar utifrån geometriska metoder. Enligt [4, Cor. I.6.12] existerar det en essentiellt unik slät projektiv kurva för varje algebraisk kroppsutvidgning L av $\mathbb{F}_p(T)$ vars funktionskropp är isomorf till L. De kurvor vi kommer studera kallas elliptiska kurvor och för en elliptisk kurva E över en ändlig kropp $\mathbb{F}_p$ så definierar vi dess zetafunktion

$$\zeta(E/\mathbb{F}_p; s) = \exp\left(\sum_{n\geq 1} \#E(\mathbb{F}_{p^n}) \frac{p^{-sn}}{n}\right)$$

Detta låter oss formulera vår huvudsats.

Sats 1.1. *(Riemannhypotesen) Rötterna till $\zeta(E/\mathbb{F}_p; s)$ har realdel $\frac{1}{2}$.*

Vad dessa begrepp betyder och beviset av Riemannhypotesen är vad resten av denna text kommer gå igenom. För detta ändamål använder vi huvudsakligen Joseph H. Silvermans bok *The Arithemetic of Elliptic Curves* [1].

1.2 Strukturen av texten

Vi ger här en bevisidé för beviset av Riemannhypotesen. För en elliptisk kurva E över en ändlig kropp $\mathbb{F}_q$ ges $\mathbb{F}_{q^n}$-rationella punkterna av fixpunkterna av n:te potensen av Frobeniusendomorfin ϕ. Elliptiska kurvor har en gruppstruktur där Frobeniusendomorfin är en grupphomomorfi vilket låter oss omformulera problemet från att räkna fixpunkter till att undersöka kärnan av en grupphomomorfi, nämligen $1-\phi^n$. Endomorfier av grupper har dock en svår struktur att studera. Därför

introducerar vi Tate-modulen vilket låter oss översätta dessa endomorfier till linjära avbildningar och på så sätt använda linjär algebra. Från detta får vi en enkel beskrivning av fixpunkterna från vilken Riemannhypotesen följer enkelt.

I resterande del av kapitel 1 återger vi några grundläggande resultat som behövs för att förstå våran text. Speciellt går vi igenom Galoisteori som kommer användas genom hela texten. Av speciell vikt definieras Galoisgruppen $\mathrm{Gal}(L/K)$ av en kroppsutvidgning som vi kommer använda för att definiera K-rationella punkter på en varietet bland annat.

Kapitel 2 bygger upp den grundläggande teorin av algebraisk geometri. Algebraisk geometri studerar geometrin av rötter till polynom, vilket betyder att vi kommer arbeta med algebraiskt slutna kroppar för en bra teori om varieteter. För att kunna studera algebraisk geometri över icke-algebraiskt slutna kroppar studerar vi hur Galoisgruppen verkar på varieteter vilket leder oss till definitionen av K-rationella punkter. Vi definierar även här funktionskroppen av en varietet.

Kapitel 3 handlar om algebraiska kurvor. Till en del ser vi dualiteten mellan geometri och algebra, där morfier mellan kurvor kan studeras genom de inducerade kroppsutvidgningarna. Vi bygger även upp teorin om divisorer som är en central del av studien av algebraiska kurvor och speciellt för elliptiska kurvor.

I kapitel 4 definierar och studerar vi elliptiska kurvor. Här kommer vi använda mycket av den teori vi byggt upp för att studera strukturen av elliptiska kurvors gruppstruktur och rationella punkter. Det viktigaste resultatet visar hur vi kan räkna fixpunkter av Frobeniusendomorfin via gruppstrukturen och Tate-modulen.

Kapitel 5 sammansätter allt vi gjort för att bevisa Riemannhypotesen.

1.3 Inledande om Galoisteori och ändliga kroppar

I detta delkapitel ger vi några grundläggande resultat om Galoisteori och ändliga kroppar för att läsaren ska enklare förstå våran text.

Låt K och L vara två kroppar så att $K \subseteq L$. Då säger vi att L är en *kroppsutvidgning* av K och betecknar det som L/K. L har en naturlig K-vektorrumstruktur och dess dimension kallas för kroppsutvidgningens *grad* och betecknas $[L : K]$. Om graden är ett ändligt tal kallas det för en ändlig kroppsutvidgning.

Proposition 1.2. *Låt $E/L/K$ vara en kedja av kroppsutvidgninar. E/L och L/K är ändliga kroppsutvidgningar omm E/K är en ändlig kroppsutvidning och det stämmer att*

$$[E : K] = [E : L][L : K].$$

Bevis. Se [5, T.4.3]. □

Om det för ett element $\alpha \in L$ existerar ett polynom $p(X) \in K[X]$ så att $p(\alpha) = 0$ så säger vi att α är *algebraisk* över K, annars är α *transcendental* över K. En kroppsutvidgning L/K där alla element $\alpha \in L$ är algebraiska över K kallas för en *algebraisk kroppsutvidgning*. Om α är algebraisk över K så existerar det ett polynom av minimal grad $p(X) \in K[X]$ med α som rot, unik upp till konstant faktor [5, Thm T.4.1]. Om det polynomet är moniskt kallar vi det för *det minimala polynomet* av α. Ett element $\alpha \in L$ sägs vara *separabel* ifall dess minimala polynom inte har multipla rötter, annars kallar vi det *inseparabelt*. Om alla element i L är separabla så säger vi att L/K är en *separabel kroppsutvidgning*. Speciellt sägs en kropp K vara *perfekt* om varje algebraisk kroppsutvidgning över K är separabel. I kontrast till detta säger vi att en kroppsutvidgning L/K är *helt inseparabelt* ifall alla element i $L \backslash K$ är inseparabla. Om L_s betecknar alla element i L som är separabla så kan vi faktorisera kroppsutvidgningen L/K som $L/L_s/K$ där L_s/K är separabelt och L/L_s är helt inseparabelt. $[L_s : K]$ kallar vi för *den separabla graden* av L/K medans $[L : L_s]$ kallas för *den inseparabla graden*. L_s kallas för det *separabla höljet* av L/K.

Låt $\{\alpha_i\}_{i \in I} \subset L$ vara en samling element i L. Samlingen element sägs vara *algebraiskt oberoende* ifall det inte existerar ett polynom $P(X) \in K[X_i;\ i \in I]$ så att $P(\dots, \alpha_i, \dots) = 0$. Notera att detta implicerar att alla α_i är transcendentala över K. Den största kardinaliteten av en mängd algebraiskt oberoende element kallas för *transcendensgraden* av kroppsutvidgningen L/K [6, s. 9.26].

En kropp L sägs vara algebraiskt sluten om alla algebraiska kroppsutvidgningar E/L är triviala, alltså att $E = L$. Om L/K är en algebraisk kroppsutvidgning och L är algebraiskt sluten så kallas

L för ett *algebraiskt hölje* av K. Gruppen av K-linjära automorfier av L kallas för *Galoisgruppen* av L/K och betecknas $\mathrm{Gal}(L/K)$.

Ändliga kroppar börjar med heltalen $\mathbb{Z}$. Låt $p \in \mathbb{Z}$ vara ett primtal och betrakta kvotkroppen $\mathbb{Z}/p\mathbb{Z}$ som vi betecknar $\mathbb{F}_p$. Eftersom det för alla ringar R existerar en unik ring homomorfi $\mathbb{Z} \to R$ vars kärna är karakteristiken av R så kan man visa att varje ändlig kropp är en ändlig kroppsutvidgning av $\mathbb{F}_p$ för något primtal p. Vi kan dock säga mer om ändliga kroppar utifrån antalet element de har.

Proposition 1.3. *En ändlig kropp är unikt bestämd av hur många element kroppen har, upp till isomorfi, och antalet element är en potens av ett primtal. Vi betecknar kroppen med $q = p^n$ element som $\mathbb{F}_q$.*

Bevis. Se [5, T.5.4] □

Från detta ser vi att ändliga kroppsutvidgningar av $\mathbb{F}_q$ är $\mathbb{F}_{q^n}$ för något $n \in \mathbb{Z}_+$, vilket implicerar att $\mathbb{F}_q$ är perfekt. En explicit beskrivning av $\mathbb{F}_q$ över $\mathbb{F}_p$ är att $\mathbb{F}_q$ är alla rötter till polynomet $X^q - X$. Från denna beskrivning ser vi också följande resultat.

Proposition 1.4. *Galoisgruppen* $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ *genereras av ett element, nämligen* Frobeniusautomorfin $x \mapsto x^q$.

Vi avslutar denna diskussion om ändliga kroppar med det algebraiska höljet av $\mathbb{F}_q$. $\mathbb{F}_q$ har en naturlig identifiering som en delkropp $\mathbb{F}_{q^n}$ och via denna identifiering kan vi bilda kroppen $\bigcup_{n\geq 1} \mathbb{F}_{q^n}$. Denna kropp är algebraiskt sluten och en algebraisk kroppsutvidgning av $\mathbb{F}_q$, med andra ord detta är ett algebraiskt hölje av $\mathbb{F}_q$ som vi betecknar $\overline{\mathbb{F}}_q$. Att beskriva Galoisgruppen $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ är svårt med de verktyg vi har då den inte längre genereras av Frobeniusautomorfin, rent algebraiskt, men vi behöver endast potenser av Frobeniusautomorfin i detta arbete.

2 Varieteter

Algebraiska varieteter utgör en central del i detta arbete. De är mängder av nollställen till system av polynomekvationer, som låter oss studera algebraiska kurvor, och därmed elliptiska kurvor. Vi börjar med *affina varieteter*, men av särskilt intresse är *projektiva varieteter*, som är mängder av nollställen av system av polynomekvationer skrivna i termer av *homogena koordinater*.

2.1 Affina varieteter

Antag att K är en perfekt kropp. Då är det *affina n-rummet* över K mängden

$$\mathbb{A}^n = \mathbb{A}^n(\overline{K}) = \{P = (x_1, \ldots, x_n) : x_i \in \overline{K}\}.$$

När vi nu nämner en kropp K antas det alltid att den är perfekt. För att spara plats så skriver vi $K[X]$ istället för $K[X_1, \ldots, X_n]$, $K[X]$ betecknar alltså polynom i n variabler om vi inte säger annat. När vi hanterar projektiva varieteter skriver vi $K[X]$ för $K[X_0, \ldots, X_n]$ istället.

Definition 2.1. Låt $I \subset \overline{K}[X]$ vara ett ideal. Då definierar vi

$$V(I) = \{P \in \mathbb{A}^n : f(P) = 0 \text{ för alla } f \in I\}.$$

Definition 2.2. En affin algebraisk mängd är en mängd av formen $V(I)$, där $I \subset \overline{K}[X]$ är ett ideal. Om $V \subseteq \mathbb{A}^n$ är en affin algebraisk mängd så definierar vi mängden

$$I(V) = \{f \in \overline{K}[X] : f(P) = 0 \text{ för alla } P \in V\}.$$

Det är lätt att se att $I(V)$ är ett ideal, som vi kallar *idealet av* V. Om $I(V)$ är ett primideal, alltså att $fg \in I(V)$ om och endast om $f \in I(V)$ eller $g \in I(V)$, säger vi att V är en *affin varietet*. Vi säger att en affin varietet V är definierad över K om dess ideal kan genereras av polynom i $K[X]$.

Definition 2.3. Låt V vara en affin varietet. Då är dess *koordinatring*

$$\overline{K}[V] = \overline{K}[X]/I(V).$$

Funktionskroppen $\overline{K}(V)$ av V är bråkkroppen av $\overline{K}[V]$. Om V är definierad över K så kan vi ersätta $\overline{K}$ med K i respektive definition. Detta kommer även gälla för de projektiva varieteterna i nästa del.

Definition 2.4. Låt V vara en affin varietet, och låt $f_0, \ldots, f_m \in \overline{K}[X]$ vara generatorer av $I(V)$ och $P \in V$ en punkt. Då är V *slät* (eller *ickesingulär*) i P om matrisen vars element är

$$\frac{\partial f_i}{\partial X_j}(P),$$

för $1 \leq i \leq m$ och $1 \leq j \leq n$, har maximal rang. Om V är slät (eller ickesingulär) i varje punkt i V så säger vi att V är *slät* (eller *ickesingulär*).

Lägg märke till att detta är mycket likt studier av egenskaper hos ytor i analys på rum av typen $\mathbb{R}^n$, där släthet förknippas med att determinanter lokalt vid punkter på kurvor är inverterbara, eller icke-singulära.

Definition 2.5. För varje $P \in V$ definierar vi idealet

$$M_P = \{f \in \overline{K}[V] : f(P) = 0\}.$$

Proposition 2.6. *M_P är ett maximalideal av $\overline{K}[V]$ (se [1, s. 5]).*

Definition 2.7. Låt V vara en varietet och P en punkt. Den *lokala ringen* av V vid P är

$$\overline{K}[V]_P = \left\{ \frac{f}{g} \in \overline{K}(V) \mid g(P) \neq 0 \right\}.$$

2.2 Projektiva varieteter

På $\mathbb{A}^{n+1} \setminus \{(0, \ldots, 0)\}$ definierar vi ekvivalensrelationen

$$(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n) \iff \exists \lambda \in \overline{K}^* : (x_0, \ldots, x_n) = (\lambda y_0, \ldots, \lambda y_n).$$

Mängden av ekvivalensklasserna av denna relation betecknar vi med $\mathbb{P}^n$, och den kallar vi för det *projektiva n-rummet över K*. Vi betecknar med $[x_0 : \cdots : x_n]$ ekvivalensklassen av $(x_0, \ldots, x_n)$ och kallar det för de *homogena koordinaterna* av ekvivalensklassen. Ett *homogent polynom av grad d* är ett polynom $f \in \overline{K}[X]$ sådan att för varje $\lambda \in \overline{K}$,

$$f(\lambda x_0, \ldots, \lambda x_n) = \lambda^d f(x_0, \ldots, x_n).$$

Ett ideal $I \subset \overline{K}[X]$ är *homogent* om den kan genereras av homogena polynom.

Notera att för ett godtyckligt polynom $f \in \overline{K}[X]$ kan vi inte evaluera det i en punkt $P \in \mathbb{P}^n$ ty f antar olika värden för olika representanter av P. Detta stämmer även för homogena polynom. Fördelen med homogena polynom är att de har väldefinierade nollställen i $\mathbb{P}^n$. Låt $f \in \overline{K}[X]$ vara homogent av grad d och $(x_0, \ldots, x_n)$ en representant för punkten $P \in \mathbb{P}^n$. Om $f(x_0, \ldots, x_n) = 0$ så har vi att

$$f(\lambda x_0, \ldots, \lambda x_n) = \lambda^d f(x_0, \ldots, x_n) = \lambda^d \cdot 0 = 0$$

vilket visar att f har väldefinierade nollställen.

Definition 2.8. Om $I \subset \overline{K}[X]$ är ett homogent ideal så definierar vi

$$V(I) = \{P \in \mathbb{P}^n : f(P) = 0 \text{ för alla homogena } f \in I\}.$$

Definition 2.9. Låt $V \subset \mathbb{P}^n$. V är en *projektiv algebraisk mängd* om det finns ett homogent ideal $I \subset \overline{K}[X]$ sådant att $V = V(I)$. För en projektiv algebraisk mängd V definierar vi $I(V)$ som idealet som genereras av mängden

$$\left\{ f \in \overline{K}[X] \mid f \text{ homogen och } f(P) = 0 \text{ för alla } P \in V \right\}.$$

Om $I(V)$ är ett primideal säger vi att V är en *projektiv varietet*. Kan idealet genereras av polynom i $K[X]$ säger vi att V är definierad över K.

Definition 2.10. Låt V vara en projektiv varietet. Vi definierar den *homogena koordinatringen* av V som $\overline{K}_H[V] = \overline{K}[X]/I(V)$.

Ett element $f \in \overline{K}_H[V]$ sägs vara *homogen av grad d* om det existerar ett homogent polynom $\tilde{f} \in \overline{K}[X]$ så att $f = \tilde{f} + I(V)$.

Definition 2.11. Låt V vara en projektiv varietet. Då är dess *funktionskropp*

$$\overline{K}(V) = \left\{ \frac{f}{g} : f, g \in \overline{K}_H[V] \text{ är homogena av samma grad} \right\}.$$

Definition 2.12. Låt $P \in V$, där V är en projektiv varietet, och $h \in \overline{K}(V)$. Vi säger att h är *reguljär* i P om det finns $f, g \in \overline{K}_H[V]$ homogena av samma grad sådana att $g(P) \neq 0$ och $h = f/g$. Notera att $h(P) = f(P)/g(P)$ då är ett väldefinierat element i $\overline{K}$. Ringen av alla funktioner reguljära i P i $\overline{K}(V)$ betecknas $\overline{K}[V]_P$ med M_p idealet av funktioner $h \in \overline{K}[V]_P$ med $h(P) = 0$.

Med funktionskroppar nu definierade för både affina och projektiva varieteter kan vi nu definiera dimensionen av en varietet.

Definition 2.13. Låt V vara en affin eller projektiv varietet med funktionskropp $\overline{K}(V)$. Dimensionen av V definierar vi som transcendensgraden av kroppsutvidgningen $\overline{K}(V)/\overline{K}$.

2.3 Rationella punkter på en varietet.

Vi har i detta kapitel sett vad som menas med en varietet V som är definierad över en kropp K. I detta delkapitel undersöker vi hur Galoisgruppen $\mathrm{Gal}(\overline{K}/K)$ har en naturlig verkan på varieteter definierade över K och hur detta ger oss så kallade K-rationella punkter. I detta delkapitel antar vi att alla varieteter är definierade över en fixerad kropp K.

Betrakta en punkt $[x_0 : \cdots : x_n] \in \mathbb{P}^n$. Vi ser att ett element $\sigma \in \mathrm{Gal}(\overline{K}/K)$ naturligt verkar på punkten genom $\sigma([x_0 : \cdots : x_n]) = [\sigma(x_0) : \cdots : \sigma(x_n)]$, vilket är väldefinierat eftersom σ är en kroppautomorfi. Om $V \subset \mathbb{P}^n$ är en projektiv varietet med ideal $I(V)$ genererat av de homogena polynomen $f_1, \ldots, f_m \in K[X]$ så kan vi se att Galoisgruppen får en naturlig verkan även på V. Nämligen om $P \in V$ så har vi för alla $\sigma \in \mathrm{Gal}(\overline{K}/K)$ och alla $k = 1, \ldots, m$

$$f_k(\sigma(P)) = \sigma(f_k(P)) = \sigma(0) = 0,$$

vilket visar att $\sigma(P) \in V$. Nu, betrakta ett element $k \in \overline{K}$. Ett känt resultat inom Galoisteori visar att k är ett element i K omm alla $\sigma \in \mathrm{Gal}(\overline{K}/K)$ håller k fixerat, alltså $\sigma(k) = k$. Detta motiverar följande definition

Definition 2.14. En punkt $P \in V$ sägs vara definierad över K om alla $\sigma \in \mathrm{Gal}(\overline{K}/K)$ håller P fixerat, alltså $\sigma(P) = P$. Vi kallar även en sådan punkt för en K-rationell punkt.

I fallet av $\mathbb{P}^n$ ser vi att det följer av denna definition att en punkt $P \in \mathbb{P}^n$ är definierad över K om och endast om P kan representeras med homogena koordinater $[x_0 : \cdots : x_n]$ med $x_i \in K$. Vi betecknar med $V(K)$ mängden av K-rationella punkter i V.

2.4 Morfier mellan varieteter

Precis som grupphomomorfier används för att undersöka relationer mellan grupper behöver vi någon avbildning mellan varieteter som bevarar nån slags struktur. Detta kommer i formen av vad vi kallar morfier mellan varieteter. Morfier mellan varieteter bygger på morfier mellan de projektiva rummen vilket är våran startpunkt.

Betrakta $\mathbb{P}^n$ och $\mathbb{P}^m$. En *morfi* eller en *reguljär avbildning* $F : \mathbb{P}^n \to \mathbb{P}^m$ ges av en samling homogena polynom $(F_0, \dots, F_m)$ av samma grad d som inte har ett gemensamt nollställe i $\mathbb{P}^n$. Dessa polynom samlas då till en funktion $P \mapsto F(P) = [F_0(P) : \cdots : F_m(P)]$. Notera att kraven på F_k kommer från att denna avbildning ska vara väldefinierad. Låt $V \subseteq \mathbb{P}^n$ och $W \subseteq \mathbb{P}^m$ vara två projektiva varieteter. En morfi från V till W ges av en morfi $F : \mathbb{P}^n \to \mathbb{P}^m$ så att $F(V) \subseteq W$.

För att definiera morfier mellan generella varieteter, affina eller projektiva, vill vi kunna betrakta affina varieteter som en slags projektiv varietet. För att göra detta definierar vi funktioner $\mathbb{A}^n \to \mathbb{P}^n$ som vi antar är morfier. Dessa funktioner är morfier utifrån en rimligare definition av morfier, men den använder sig av verktyg vi inte kan använda i denna text.

Proposition 2.15. *Funktionerna $\iota_i : \mathbb{A}^n \to \mathbb{P}^n$ som definieras av*

$$(x_1, \dots, x_n) \mapsto [x_1 : \cdots : x_{i-1} : 1 : x_i : \cdots : x_n]$$

är injektiva och låter oss identifiera $\mathbb{A}^n$ med vissa delmängder av $\mathbb{P}^n$, nämligen $\mathbb{P}^n \setminus V(X_i)$.

Vi tager som ett axiom att ι_i är morfier. Låt $V \subseteq \mathbb{A}^n$ vara en affin varietet. Via en av morfierna ι_i kan vi betrakta V som en delmängd av $\mathbb{P}^n$. När vi betraktar en affin varietet som en delmängd av $\mathbb{P}^n$ kallar vi den för en *kvasiprojektiv varietet*. Kvasiprojektiva varieteter platsar enkelt in i definitionen av morfier.

Anmärkning 2.16. Detta är en okonventionell definition av morfier mellan affina varieteter som inte uppkommer inom litteraturen om algebraisk geometri. Vi har definierat dem på detta vis för en mer kompakt text då morfier mellan affina varieteter inte spelar någon större roll för det vi gör.

Låt $P \in V \subseteq \mathbb{P}^n$ vara en punkt i en projektiv varietet. Om $P \in \iota_i(\mathbb{A}^n) \cap V$ säger vi att $\iota_i(\mathbb{A}^n) \cap V$ är en *affin omgivning* av P. Notera att $\iota_i(\mathbb{A}^n) \cap V$ är en affin varietet. Vi kan då säga att P är en *slät punkt* i V om den är slät i en affin omgivning av P. En projektiv varietet V är *slät* om alla dess punkter är släta.

Definition 2.17. En morfi $\phi : V \to W$ kallas en *isomorfi* om det existerar en morfi $\psi : W \to V$ så att $\phi \circ \psi = \mathrm{id}_W$ och $\psi \circ \phi = \mathrm{id}_V$. Vi betecknar isåfall ψ som ϕ^{-1}.

3 Algebraiska kurvor

3.1 Kurvor

Vi kommer nu studera kurvor med vilket vi menar släta projektiva varieteter av dimension ett. Kapitlet börjar med lite allmän teori om kurvor för att sedan kunna introducera väsentliga verktyg som används för att formulera den berömda satsen Riemann-Roch. Följande två resultat kommer från [1, Thm II.2.3] och [1, Thm II.2.5] respektive.

Sats 3.1. *Låt $\phi : C_1 \to C_2$ vara en morfi av kurvor. Då är ϕ antingen konstant eller surjektiv.*

Proposition 3.2. *Låt $\phi : C_1 \to C_2$ vara en icke-konstant morfi av kurvor. Då finns det en tillhörande injektion av funktionskroppar*

$$\phi^* : K(C_2) \to K(C_1) \quad \text{där} \quad \phi^*(f) = f \circ \phi.$$

Definition 3.3. Låt $\phi : C_1 \to C_2$ vara en morfi av kurvor. Om ϕ är konstant sätter vi graden av ϕ till 0. Annars definieras graden av ϕ som

$$\deg \phi = [K(C_1) : \ \phi^* K(C_2)].$$

Vidare skrivs den separabla graden som

$$\deg_s \phi = [K(C_1)_s : \ \phi^* K(C_2)].$$

Vi hämtar nu följade avbildning på $\overline{K}(C)$ från [7, Prop. 9.2] vilket vi kommer att se är ett viktigt verktyg inom studien av kurvor.

Definition 3.4. Låt C vara en kurva och $P \in C$ en punkt. Vi definierar $\mathrm{ord_P} : \overline{K}(C) \to \mathbb{Z} \cup \{\infty\}$ på funktionskroppen $\overline{K}(C)$ vid P med

$$\mathrm{ord_P}(f) = \sup\left\{d \in \mathbb{Z} : f \in M_P^d\right\}$$

för element i $\overline{K}[C]_P$. För element som inte finns i $\overline{K}[C]_P$ sätts

$$\mathrm{ord_P}(f/g) = \mathrm{ord_P}(f) - \mathrm{ord_P}(g), \quad f, g \in \overline{K}[C]_P.$$

Vidare har $\mathrm{ord_P}$ egenskaperna att för varje $f, g \in \overline{K}(C)$ så uppfylls

$$\mathrm{ord_P}(fg) = \mathrm{ord_P}(f) + \mathrm{ord_P}(g).$$

Intuitionen bakom $\mathrm{ord_P}(f)$ är att f är en rationell funktion $\frac{p(x)}{q(x)}$ där $p(x)$ och $q(x)$ är polynom. $\mathrm{ord_P}(f)$ är multipliciteten vid P i $p(x)$ minus multipliciteten vid P i $q(x)$.

Definition 3.5. Låt C vara en kurva och $P \in C$ en punkt samt $f \in \overline{K}(C)$. Ordningen av f vid P är $\mathrm{ord_P}(f)$. Om $\mathrm{ord_P}(f) > 0$ säger vi att f har ett nollställe vid P och om $\mathrm{ord_P}(f) < 0$ så säger vi att f har en pol vid P. Om $f = 0$ skriver vi $\mathrm{ord_P}(f) = \infty$. Vi säger att en funktion $t \in \overline{K}(C)$ är en *uniformisator* vid P om $\mathrm{ord_P}(t) = 1$. En uniformisator vid P är också detsamma som en generator för maximalidealet i $\overline{K}[C]_P$.

Proposition 3.6. *Låt C vara en kurva och $f \in \overline{K}(C)$ med $f \neq 0$. Då finns det som mest ändligt många punkter i C där f har ett nollställe eller en pol.*

Bevis. Ändligt många nollställen följer direkt från [4, Prop. I.6.5]. För ändligt många poler använder vi samma resultat på $1/f$. □

Vi definierar en term som kommer till användning i ett senare avsnitt när vi jobbar med avbildningar mellan elliptiska kurvor.

Definition 3.7. Låt $\phi : C_1 \to C_2$ vara en icke-konstant avbildning av kurvor och låt $P \in C_1$. Då definierar vi *förgreningsindexet* $e_\phi(P)$ av ϕ vid P som

$$e_\phi(P) = \mathrm{ord_P}(\phi^* t)$$

där $t \in \overline{K}(C_2)$ är en uniformisator vid $\phi(P)$.

Proposition 3.8. *Låt $\phi : C_1 \to C_2$ vara en icke-konstant avbildning av kurvor. För varje $Q \in C_2$ är*

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg \phi.$$

Det gäller också för alla förutom ändligt många $Q \in C_2$ att

$$\#\phi^{-1}(Q) = \deg_s \phi.$$

Bevis. Se [4, Prop. II.6.8, Prop. II.6.9] för ett bevis av båda resultaten. □

3.2 Divisorer

Definition 3.9. *Divisorgruppen* $\mathrm{Div}(C)$ av en kurva C är den fria abelska gruppen genererad av punkter på C. Med andra ord, ett element $D \in \mathrm{Div}(C)$ har formen

$$D = \sum_{P \in C} n_P [P],$$

där $[P]$ är en formell symbol och $n_P \in \mathbb{Z}$ är nollskild för ändligt många punkter. Elementen i $\mathrm{Div}(C)$ kallas för divisorer. Additionen $x + y$ för $x, y \in \mathrm{Div}(C)$ är definierad som termvis addition i den formella summan. Vi säger att graden av D är

$$\deg D = \sum_{P \in C} n_P.$$

Om C är definierad över K definierar vi Galoisgruppens verkan på $\mathrm{Div}(C)$ som

$$\sigma(D) = \sum_{P \in C} n_P [\sigma(P)]$$

för $\sigma \in \mathrm{Gal}(\overline{K}/K)$. D är då definierad över K om $\sigma(D) = D$ för alla $\sigma \in \mathrm{Gal}(\overline{K}/K)$ och vi betecknar *gruppen av divisorer definierad över* K som $\mathrm{Div}_K(C)$. Från Proposition 3.6 kan vi associera en divisor till $f \in \overline{K}(C)^*$ med

$$\mathrm{div}\, f = \sum_{P \in C} \mathrm{ord_P}(f)[P].$$

Notera nu att

$$\mathrm{div} : \overline{K}(C)^* \to \mathrm{Div}(C)$$

är en homomorfi av abelska grupper, vilket följer från egenskaperna av $\mathrm{ord_P}$. Elementen i bilden av div kallar vi för *principiella divisorer*. Två divisorer D_1, D_2 sägs vara linjärt ekvivalenta $D_1 \sim D_2$ om $D_1 - D_2$ är principiell. Eftersom principiella divisorer bildar en delgrupp så är denna relation precis kongruensrelationen för grupper.

Definition 3.10. Vi definierar *Picardgruppen* $\mathrm{Pic}(C)$ av en kurva C som kvotgruppen av $\mathrm{Div}(C)$ med delgruppen av principiella divisorer.

Vi formulerar en identitet från [4, Corollary II.6.10] som kommer visas vara användbar senare i denna texten.

Proposition 3.11. *Låt C vara en kurva och låt $f \in \overline{K}(C)^*$. Då är* $\deg(\mathrm{div}(f)) = 0$.

Vi betecknar delgruppen av alla divisorer av grad 0 som

$$\mathrm{Div}^0(C) = \{D \in \mathrm{Div}(C) : \deg D = 0\}.$$

Tag en principiell divisor $D = \mathrm{div}\, f$ för något $f \in \overline{K}(C)$, då är $\deg D = 0$. Det betyder att gruppen av alla principiella divisorer är en delgrupp av $\mathrm{Div}^0(C)$. Vi kan nu på liknande sätt definiera $\mathrm{Pic}^0(C)$ som $\mathrm{Div}^0(C)$ kvotat med delgruppen av alla principiella divisorer.

Definition 3.12. Låt C vara en kurva. Vi definierar Ω_C som kvotvektorrummet över $\overline{K}(C)$ med symboler dx där $x \in \overline{K}(C)$ under relationerna

(i) $d(x + y) = dx + dy$ för alla $x, y \in \overline{K}(C)$

(ii) $d(xy) = xdy + ydx$ för alla $x, y \in \overline{K}(C)$

(iii) $dx = 0$ då $x \in \overline{K}$.

Ω_C kallas för rummet av alla *meromorfa differentialformer* på C. Ordet differential kommer från att egenskaperna som uppfylls av d efterliknar derivatan inom analysen. För att kunna jobba med differentialformer kan det vara bra med några väsentliga egenskaper. Vi sammanställer [1, Prop II.4.2] och [1, Prop II.4.3] i följande två propositioner.

Proposition 3.13. *Låt C vara en kurva. Då är Ω_C ett endimensionellt $\overline{K}(C)$-vektorrum.*

Proposition 3.14. *Låt C vara en kurva, P en punkt i C och $t \in \overline{K}(C)$ en uniformisator vid P.*

(a) För varje $df \in \Omega_C$ finns det en unik $g \in \overline{K}(C)$ som uppfyller $df = gdt$. Vi skriver att $g = df/dt$.

(b) Låt $df \in \Omega_C$ vara nollskild. Då är $\mathrm{ord_P}(df/dt)$ *oberoende av valet av uniformisator $t \in \overline{K}(C)$. Vi uttnyttar detta och skriver* $\mathrm{ord_P}(df) := \mathrm{ord_P}(df/dt)$.

(c) Låt $df \in \Omega_C$ vara nollskild. Då är

$$\mathrm{ord_P}(df) \neq 0$$

för ändligt många punkter.

Tack vare detta resultat kan vi utöka definitionsmängden av $\mathrm{ord_P}$ för att även täcka in nollskilda differentialer på C.

Definition 3.15. Låt $df \in \Omega_C$ med $df \neq 0$. Vi definierar divisorn till df enligt

$$\operatorname{div} df = \sum_{P \in C} \mathrm{ord_P}(df)[P] \in \operatorname{Div}(C)$$

En divisor $W \in \operatorname{Div}(C)$ sägs vara en *kanonisk divisor* om det finns en differential $df \in \Omega_C$ sådana att $W = \operatorname{div}(df)$.

3.3 Riemann-Roch

Vi börjar med att definiera en så kallad partiell ordning på divisorer.

Definition 3.16. Med $D_1 \geq D_2$ menar vi att alla n_P i $D_1 - D_2$ är icke-negativa. Låt $D \in \operatorname{Div}(C)$ och definiera

$$\mathcal{L}(D) = \{f \in \overline{K}(C)^* : \operatorname{div}(f) \geq -D\} \cup \{0\}$$

En väsentlig egenskap av $\mathcal{L}(D)$ är följande resultat från [1, Prop II.5.2b].

Proposition 3.17. *Låt $D \in \operatorname{Div}(C)$, då är $\mathcal{L}(D)$ ett ändligtdimensionellt $\overline{K}$-vektorrum.*

Eftersom $\mathcal{L}(D)$ är ändligdimensionell betecknar vi dess dimension enligt

$$\ell(D) = \dim_{\overline{K}} \mathcal{L}(D).$$

Vi kan nu formulera Riemann-Rochs sats vilket kommer spela en central roll i nästa kapitel för att studera elliptiska kurvor och dess gruppstruktur. För ett bevis av Riemann-Roch hänvisar vi till [4, Prop. IV.1.1] och [4, Thm. IV.1.3] eller [8, s. 8.6].

Sats 3.18. *(Riemann-Roch) Låt C vara en kurva och låt W vara en kanonisk divisor på C. Då finns det ett heltal $g \geq 0$, kallad för* genuset *av C, sådant att för varje divisor $D \in \operatorname{Div}(C)$,*

$$\ell(D) - \ell(W - D) = \deg D - g + 1.$$

Vi sammanfattar konsekvenser av Riemann-Roch som kommer visas vara användbara i nästa avsnitt då vi ska visa en gruppstruktur på elliptiska kurvor. För ett bevis av detta hänvisas [1, Cor. III.5.5].

Korollarium 3.19.

(a) Om W är en kanonisk divisor på C så är $\deg W = 2g - 2$.

(b) Låt $D \in \operatorname{Div}(C)$, om $\deg D > 2g - 2$, *då är*

$$\ell(D) = \deg D - g + 1.$$

Slutligen formulerar vi en egenskap av baserna i $\mathcal{L}(D)$ och hänvisar till [1, Prop. II.5.8] för ett bevis.

Proposition 3.20. *Låt C vara en kurva över K och låt $D \in \operatorname{Div}_K(C)$. Då har $\mathcal{L}(D)$ en bas av element i $K(C)$.*

4 Om elliptiska kurvor

4.1 Elliptiska Kurvor

En *elliptisk kurva* E är en kurva med genus ett som har en fixerad punkt $O \in E$. En elliptisk kurva är definierad över K om kurvan är definierad över K och $O \in E(K)$. Om inget annat anges kan det antas att kurvan E är definierad över K. Vi ska visa att det finns en bijektion $E \cong \mathrm{Pic}^0(E)$ i Proposition 4.4 vilket innebär en gruppstruktur på E med en identitet $O \in E$. Men innan gruppstrukturer kan visas behövs det en enklare representation av en elliptisk kurva.

Proposition 4.1. *Låt E vara en elliptisk kurva över K.*

(a) Det finns en avbildning

$$\phi : E \to \mathbb{P}^2, \quad \phi = [x : y : 1],$$

med $x, y \in K(E)$ som bildar en isomorfi från E till en kurva som ges av Weierstrassekvationen

$$C : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

med koefficienter $a_1, \ldots, a_6 \in K$ och $\phi(O) = [0 : 1 : 0]$.

(b) Omvänt, varje kurva C given som i (a) är en elliptisk kurva över K med $O = [0 : 1 : 0]$.

Funktionerna $x, y \in K(E)$ i *(a)* kallar vi *koordinatfunktioner*. Vi skissar bevisidén och hänvisar till [1, Prop. 3.1] för det fullständiga beviset. Observera punkterna $n[O]$ för positiva heltal n. Det följer från Korollarium 3.19b) att $\mathcal{L}(n[O])$ är ett vektorrum med dimension n. Från Proposition 3.20 kan vi bilda $x, y \in K(E)$ sådana att $\{1, x\}$ är en bas i $\mathcal{L}(2[O])$ och $\{1, x, y\}$ är en bas i $\mathcal{L}(3[O])$. Vi har nu 7 funktioner i $\mathcal{L}(6[O])$

$$1, x, y, x^2, y^2, xy, x^3$$

som är linjärt beroende, vilket ger att vi har en icke-triviell lösning till

$$A_1 + A_2x + A_3y + A_4x^2 + A_5xy + A_6y^2 + A_7x^3 = 0$$

där $A_i \in K$ för $i = 1, \ldots, 7$. Denna ekvationen kan skrivas om sådan att det finns en surjektiv morfi

$$\phi : E \to C, \qquad \phi = [x : y : 1],$$

för en kurva C som nödvändigtvis inte är slät och beskrivs av en ekvation. Sedan för att visa att $K(E) = K(x, y)$ tolkas graden av avbildningarna $[x : 1] : E \to \mathbb{P}^1$ och $[y : 1] : E \to \mathbb{P}^1$. Detta tvingar att $[K(E) : K(x, y)] = 1$. Sedan för att visa att C är slät antas motsatsen vilket leder till en motsägelse att E har genus ett och $\mathbb{P}^1$ har genus noll.

Nu rör vi oss vidare mot den så kallad *geometriska grupplagen*. Vi motiverar denna genom att vi skriver E som i ekvationen ovan och ser att den har grad tre. Det följer från Bézout's sats [4, Cor. I.7.8] att en linjen kommer skära E exakt tre gånger om man räknar med multiplicitet.

Definition 4.2. Låt $P, Q \in E$ och låt L vara linjen mellan P och Q. Om $P = Q$ då är L tangentlinjen vid P. Låt R vara den tredje skärningspunkten av L i E. Låt l vara linjen mellan R och O. Då skär l en tredje punkt och vi kallar denna punkten för $P + Q$.

Nästa resultat visar att denna geometriska lagen bildar en abelsk grupp genom en isomorfi mellan $\mathrm{Pic}^0(E)$ och E. Vi formulerar först ett lemma som kommer hjälpa oss visa resultatet.

Lemma 4.3. *Om $P, Q \in E$ är punkter då är $P \sim Q$ om och endast om $P = Q$.*

Bevis. Välj först $f \in \overline{K}(C)^*$ sådan att $\operatorname{div} f = [Q] - [P]$ då är $f \in \mathcal{L}([P])$ och av Korollarium 3.19b) är $\ell([P]) = 1$. Det följer att $f \in \overline{K}^*$ eftersom $\mathcal{L}([P])$ har dimension ett. Alltså är $\operatorname{div} f = 0$ och $P = Q$. Omvänt, $[P] - [Q] = 0$ och tag en konstant $f \in \overline{K}^*$. □

Sats 4.4. *Låt E vara en elliptisk kurva,*

(a) För varje divisor $D \in \mathrm{Div}^0(E)$ finns en unik punkt $P \in E$ sådant att

$$D \sim [P] - [O].$$

Vi associerar detta till en funktion

$$\kappa : \mathrm{Div}^0(E) \to E$$

som avbildar D till den unika punkten P.

(b) κ är surjektiv

(c) $\ker \kappa$ är alla principiella divisorer. Från κ induceras en bijektion $\tau : \mathrm{Pic}^0(E) \xrightarrow{\sim} E$. Vi kallar inversen av τ för

$$\iota : E \to \mathrm{Pic}^0(E), \quad P \mapsto [[P] - [O]].$$

(d) ι är en gruppisomorfi mellan E och $\mathrm{Pic}^0(E)$.

Bevis. (a) Notera att $\deg(D + [O]) = 1$ eftersom $D \in \mathrm{Div}^0(E)$. Av Korollarium 3.19b) följer det att $\ell(D + [O]) = 1$ eftersom E har genus 1. Låt $f \in \mathcal{L}(D + [O])$ där $f \neq 0$. Då är f en bas till $\mathcal{L}(D + [O])$. Vidare är $\deg(\mathrm{div}(f)) = 0$ från 3.11 och $\mathrm{div}(f) \geq -D - [O]$ vilket ger att fel termen är en punkt $P \in E$,

$$\mathrm{div} f = -D - [O] + [P]$$

och därmed $D \sim [P] - [O]$. För att visa att denna är unik tag $P' \in E$ med samma egenskap. Då är $P' \sim P$ av transitivitet. Det följer nu direkt av Lemma 4.3.

(b) För varje $P \in E$ har vi $\kappa([P] - [O]) = P$.

(c) Låt $D_1, D_2 \in \mathrm{Div}^0(E)$ och $P_1 = \kappa(D_1), P_2 = \kappa(D_2)$, då är $D_1 - D_2 \sim [P_1] - [P_2]$. Från Lemma 4.3 fås $\kappa(D_1) = \kappa(D_2)$ om och endast om $D_1 \sim D_2$. Vi kan nu tillsammans med (b) bilda en bijektion $\tau : \mathrm{Pic}^0(E) \xrightarrow{\sim} E$ från κ genom att kvota ut gruppen av alla principiella divisorer i $\mathrm{Div}^0(E)$.

(d) Det återstå att visa ι bevarar operationen, dvs

$$\iota(P + Q) = \iota(P) + \iota(Q).$$

Låt

$$f(X, Y, Z) = \alpha X + \beta Y + \gamma Z$$

definiera linjen L i $\mathbb{P}^2$ som går genom P och Q. Låt R vara den tredje skärningspunkten av L. Vidare låt $g(X, Y, Z) = aX + bY + cY$ vara linjen som går mellan R och O. Eftersom $Z = 0$ har multiplicitet 3 vid $[O]$ så är

$$\mathrm{div}(f/Z) = [P] + [Q] + [R] - 3[O],$$

$$\mathrm{div}(g/Z) = [R] + [P + Q] - 2[O]$$

och vidare

$$\mathrm{div}(g/f) = [P + Q] - [P] - [Q] + [O] \sim 0$$

vilket är samma som

$$\iota(P + Q) - \iota(P) - \iota(Q) = 0.$$

□

Detta kopplar den algebraiska grupplagen i $\mathrm{Pic}^0(E)$ till den geometriska grupplagen i definition 4.2. Grupplagen för elliptiska kurvor är ett centralt resultat för att studera elliptiska kurvor.

4.2 Isogenier mellan elliptiska kurvor

Vi har hittills sett att elliptiska kurvor är exempel på varieteter med en tillhörande gruppstruktur. Vi kommer nu att påbörja vår studie av en klass av morfier mellan elliptiska kurvor som kallas *isogenier* som visar sig vara precis de morfier som även bevarar gruppstrukturen.

Definition 4.5. Låt E_1 och E_2 vara två elliptiska kurvor. En *isogeni* är en morfi $\phi : E_1 \to E_2$ sådan att $\phi(O) = O$.

Anmärkning 4.6. Vi kommer hädanefter kalla den konstanta isogenin $P \mapsto O$ som *noll-isogenin* och övriga isogenier som *nollskilda isogenier*.

Genom att notera att noll-isogenin omedelbart uppfyller att den bevarar gruppstrukturen så räcker det att konstatera att nollskilda isogenier bevarar gruppstrukturen. Vi får detta resultat från följande sammanställning av [1, Thm. III.4.8, Cor. III.4.9].

Sats 4.7. *Låt E_1 och E_2 vara elliptiska kurvor och $\phi : E_1 \to E_2$ en icke-konstant isogeni. Då är ϕ en surjektiv grupphomomorfi med ändlig kärna.*

Bevis. Enligt Sats 3.1 är ϕ surjektiv då den är icke-konstant samt enligt Proposition 3.8 så är dess kärna $\ker \phi = \phi^{-1}(O) \leq \deg \phi$ och således ändlig. Vidare så är den inducerade avbildningen

$$\phi_* : \mathrm{Pic}^0(E_1) \to \mathrm{Pic}^0(E_2), \qquad \left[\sum_{P \in E_1} n_P[P]\right] \longmapsto \left[\sum_{P \in E_1} n_P[\phi(P)]\right].$$

en grupphomomorfi. Av Proposition 4.4 har vi gruppisomorfier

$$\iota_i : E_i \to \mathrm{Pic}^0(E_i), \qquad P \mapsto [[P] - [O]].$$

Direkt beräkning ger att

$$\begin{array}{ccc} E_1 & \xrightarrow[\iota_1]{\cong} & \mathrm{Pic}^0(E_1) \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi_*} \\ E_2 & \xrightarrow[\iota_2]{\cong} & \mathrm{Pic}^0(E_2) \end{array}$$

kommuterar, således är ϕ en grupphomomorfi då $\phi = \iota_1 \circ \phi_* \circ \iota_2^{-1}$. □

Sedan får vi även omedelbart att alla morfier som bevarar grupp-strukturen är isogenier i och med att de kommer avbilda $O \mapsto O$. Nu kommer vi definiera två viktiga strukturer av morfier på elliptiska kurvor.

Definition 4.8. Låt E_1 och E_2 vara elliptiska kurvor. Vi definierar gruppen

$$\mathrm{Hom}(E_1, E_2) = \{\phi : E_1 \to E_2 : \phi \text{ är en isogeni}\}$$

med operationen $(\varphi + \psi)(P) := \varphi(P) + \psi(P)$ för $\varphi, \psi \in \mathrm{Hom}(E_1, E_2)$ och $P \in E_1$.

Enligt [1, Thm. III.3.6] är $+$ väldefinierad, och då noll-isogenin tillhör $\mathrm{Hom}(E_1, E_2)$ inducerar gruppstrukturen på den elliptiska kurvan E_2 en abelsk gruppstruktur på $\mathrm{Hom}(E_1, E_2)$.

Definition 4.9. Låt E vara en elliptisk kurva, vi definierar

$$\mathrm{End}(E) := \mathrm{Hom}(E, E).$$

Genom att låta sammansättning agera som en multiplikation på $\mathrm{End}(E)$ får vi en ring-struktur, och kallar mängden för *Endomorfi-ringen* hörande till E.

Sats 4.10. *Låt $\phi : E_1 \to E_2$ vara en nollskild isogeni. För alla $Q \in E_2$ så är $\#\phi^{-1}(Q) = \deg_s \phi$. Speciellt, om ϕ är separabel så är $\#\ker \phi = \deg \phi$.*

Bevis. Se [1, Thm. III.4.10]. □

4.3 Den invarianta differentialen

Låt E vara en elliptisk kurva. Vi vill kunna nyttja rummet av differentialfomer på E, Ω_E, för att utöka vår studie av elliptiska kurvor samt isogenier däremellan. Ett centralt verktyg i studien av Ω_E är den så kallade *invarianta differentialen*. Låt $x, y \in K(E)$ vara två koordinatfunktioner till E samt

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

den tillhörande Weierstrassekvationen med $O = [0 : 1 : 0]$ vid oändligheten. Vi definierar då *invarianta differentialen* hörande till E som

$$\omega = \frac{dx}{2y + a_1x + a_3}.$$

Vi börjar med att undersöka egenskaper hörande till den invarianta differentialen.

Proposition 4.11. *Låt E vara en elliptisk kurva given av en Weierstrassekvation med invariant differential ω. Då saknar ω poler samt nollställen, alltså är div$(\omega) = 0$.*

Bevis. Se [1, Prop. III.1.5] □

Proposition 4.12. *Låt E vara en elliptisk kurva givet av en Weierstrassekvation och ω den invarianta differentialen. Låt τ_Q vara en translation på E, $\tau_Q(P) = P + Q$. Då är $\tau_Q^*\omega = \omega$.*

Bevis. Enligt Proposition 3.13 är Ω_E endimensionell och så finns $r_Q \in \overline{K}(E)$ s.a. $\tau_Q^*\omega = r_Q\omega$. Då τ_Q^* är en isomorfi följer det att $r_Q \neq 0$. Då $\mathrm{Div}(\omega) = 0$ får vi även att

$$\mathrm{Div}(r_Q) = \mathrm{Div}(\tau_Q^*\omega) - \mathrm{Div}(\omega) = \tau_Q^*\mathrm{Div}(\omega) - \mathrm{Div}(\omega) = 0.$$

Enligt [1, Prop. II.1.2] så är $r_Q \in \overline{K}$. Återstår att visa att $r_Q = 1$. Man kan sedan genom att explicit skriva ut $\tau_Q^*\omega(P)$ för ett godtyckligt $P \in E$ se att

$$f : E \longrightarrow \mathbb{P}^1, \qquad Q \mapsto [r_Q : 1]$$

är en rationell funktion på E. Vidare är f inte surjektiv ty $[0 : 1]$ kan ej nås då $r_Q \neq 0$ för alla $Q \in E$. Enligt Sats 3.1 så är f konstant, och således är värdet på r_Q oberoende av valet av Q. Speciellt är $r_Q = r_O = 1$ för alla $Q \in E$. □

Hädanefter innebär en *invariant differential* en differential som uppfyller Proposition 4.12, alltså att de är translationsinvarianta. Man kan i och med det se Proposition 4.11 samt 4.12 som ett existensresultat av invarianta differentialer för elliptiska kurvor, ty en allmän elliptisk kurva är isomorf med en elliptisk kurva given av en Weierstrassekvation som då således har en invariant differential.

Nästa resultat gäller hur invarianta differentialer interagerar med gruppstrukturen på $\mathrm{Hom}(E_1, E_2)$. Om $\psi \in \mathrm{Hom}(E_1, E_2)$ så inducerar den en avbildning

$$\psi^* : \Omega_{E_2} \to \Omega_{E_1} \qquad \psi^*(f\,dx) = \psi^*(f)\,d(\psi^*x)$$

där $\psi^*(f)$ samt $\psi^*(x)$ anger bilden av den inducerade avbildningen på funktionskropparna hörande till E_1 och E_2

Sats 4.13. *Låt E_1 och E_2 vara två elliptiska kurvor, ω en invariant differential på E_2 och $\phi, \psi \in Hom(E_1, E_2)$. Då gäller att*

$$(\phi + \psi)^*\omega = \phi^*\omega + \psi^*\omega.$$

Bevis. Se [1, Thm. III.5.2] □

Alltså ger invarianta differentialer ett sätt att binda samman gruppstrukturen på $\mathrm{Hom}(E_1, E_2)$, som i sig induceras från gruppstrukturen på E_2, med additionen på Ω_E.

4.4 Heltalsmultiplikation och duala isogenier

I detta delkapitel kommer vi att först definiera en av de viktigaste klasserna av endomorfier på en elliptisk kurva – heltalsmultiplikation – och sedan nyttja denna för att utöka våra verktyg i studien av isogenier med så kallade *duala isogenier*. Målet är definiera och sedan avgöra strukturen på *torsionsdelgrupperna* av en elliptisk kurva, som senare är centralt för studien av Tate-modulen.

4.4.1 Heltalsmultiplikation på elliptiska kurvor

Låt E vara en elliptisk kurva och definiera för $m \in \mathbb{Z}$

$$[m] : E \to E, \qquad [m](P) = \begin{cases} \underbrace{P + P + \cdots + P}_{=\text{“}m \text{ gånger P”}} & \text{om} \quad m > 0 \\ O & \text{om} \quad m = 0 \\ \underbrace{(-P) + (-P) + \cdots + (-P)}_{=\text{“}-m \text{ gånger } -P\text{”}} & \text{om} \quad m < 0. \end{cases}$$

Våran förhoppning är att om $m \neq 0$ kommer $[m]$ vara en nollskild isogeni. Av [1, Prop. III.4.2a] ser vi att så är fallet.

Proposition 4.14. *Låt E vara en elliptisk kurva och $m \in \mathbb{Z} \setminus \{0\}$. Då är $[m] \neq [0]$*

Speciellt visar vi nu att om $\text{char}(K) \nmid m$ så kommer heltalsmultiplikationen med m på en elliptisk kurva E vara separabel.

Proposition 4.15. *Låt E vara en elliptisk kurva, ω en invariant differential på E och $m \in \mathbb{Z}$. Då är $[m]^*\omega = m\omega$.*

Bevis. Vi visar resultatet genom induktion. Om $m = 0$ eller $m = 1$ följer resultatet omedelbart ty $[0]$ är noll-isogenin samt $[1] = \text{id}_E$. Det följer från Sats 4.13 att för $m \in \mathbb{Z}$ blir

$$[m + 1]^*\omega = m^*\omega + \omega. \tag{1}$$

Antag nu att satsen stämmer för ett fixt $m \in \mathbb{Z}$. Vi får sedan av (1) att satsen stämmer för både $m + 1$ och $m - 1$ och resultatet följer av tvåsidig induktion. □

Proposition 4.16. *Låt E vara en elliptisk kurva och $m \in \mathbb{Z} \setminus \{0\}$ s.a. $\text{char}(K) \nmid m$. Då är $[m]$ en separabel endomorfi.*

Bevis. För en invariant differential ω på E får vi av Proposition 4.15 samt att $m \neq 0$ i K att $[m]^*\omega = m\omega \neq 0$. Då är $[m]$ en separabel isogeni av [1, Prop. II.4.2(c)]. □

Några resultat vi får direkt från heltalsmultiplikationen är gällande $\text{Hom}(E_1, E_2)$ och $\text{End}(E)$ och deras struktur.

Proposition 4.17. *Låt E_1 och E_2 vara två elliptiska kurvor. Då är $Hom(E_1, E_2)$ en abelsk grupp sådan att för $m \in \mathbb{Z}$ och $\phi \in Hom(E_1, E_2)$ är $[m] \circ \phi = [0]$ om och endast om $m = 0$ eller $\phi = [0]$.*

Bevis. Vi vet sedan tidigare att $\text{Hom}(E_1, E_2)$ är en abelsk grupp. Tag $m \in \mathbb{Z}$ och $\phi \in \text{Hom}(E_1, E_2)$ sådan att $[m] \circ \phi = [0]$. Då har vi att $(\deg[m])(\deg \phi) = \deg[0] = 0$ och alltså måste antingen $\deg[m] = 0$ eller $\deg \phi = 0$, vilket stämmer om och endast om $[m] = [0]$ eller $\phi = [0]$. Av föregående diskussion sammanfaller det första fallet om och endast om $m = 0$. Å andra sidan får vi automatiskt att om $m = 0$ eller $\phi = [0]$ blir $[m] \circ \phi = [0]$. □

Proposition 4.18. *Låt E vara en elliptisk kurva. Då är $End(E)$ en ring av karaktäristik 0 utan nolldelare.*

Bevis. Av Proposition 4.17 samt 4.14 får vi att $\text{End}(E)$ har karaktäristik 0. Tag två nollskilda $\phi, \psi \in \text{End}(E)$. Enligt Sats 3.1 är båda surjektiva, så deras sammansättning $\phi \circ \psi$ är surjektiv, alltså är $\phi \circ \psi \neq [0]$. □

Definition 4.19. Låt E vara en elliptisk kurva och $m \geq 1$ ett heltal. Vi definierar då *m-torsionsdelgruppen* av E som

$$E[m] = \ker[m].$$

4.4.2 Duala isogenier

Vi kommer nu introducera duala isogenier med målet att nyttja dessa för att avgöra strukturen på $E[m]$.

Sats 4.20. *Låt E_1 och E_2 vara två elliptiska kurvor och $\phi : E_1 \to E_2$ en nollskild isogeni av grad m. Då finns en unik isogeni $\hat{\phi} : E_2 \to E_1$ sådan att $\hat{\phi} \circ \phi = [m]$.*

Bevis. Se [1, Thm. III.6.1a]. □

Definition 4.21. Låt $\phi \in \mathrm{Hom}(E_1, E_2)$ vara en isogeni. Om ϕ är nollskild sätt $\hat{\phi} \in \mathrm{Hom}(E_1, E_2)$ som i Sats 4.20, alternativt om ϕ är noll-isogenin sätter vi $\hat{\phi}$ till motsvarande noll-isogeni. Vi kallar $\hat{\phi}$ för den *duala isogenin* till ϕ.

Vi kommer senare se att i kontexten av Weils e_m-parning är duala isogenier en analog till duala operatorer inom studien av inre produktrum.

Vi kommer nu se att isogenier beter sig väl gentemot additionen och sammansättningen på $\mathrm{Hom}(E_1, E_2)$ samt $\mathrm{End}(E)$, för beviset hänvisar vi till [1, Thm. III.6.2abc].

Proposition 4.22. *Låt $\phi : E_1 \to E_2$, $\psi : E_1 \to E_2$ och $\lambda : E_2 \to E_3$ vara isogenier samt E_1, E_2 och E_3 elliptiska kurvor.*

(a) Om $m = \deg \phi$ så är $\phi \circ \hat{\phi} = [m]$ heltalsmultiplikation med m på E_1 samt $\hat{\phi} \circ \phi = [m]$ heltalsmultiplikation med m på E_2.

(b) $\widehat{\lambda \circ \phi} = \hat{\phi} \circ \hat{\lambda}$.

(c) $\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$.

Nu söker vi visa med hjälp av duala isogenier att $\deg[m] = m^2$, för att sedan använda det för att visa att

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

Proposition 4.23. *För alla $m \in \mathbb{Z}$ och en elliptisk kurva E så är $\widehat{[m]} = [m]$ och speciellt är $\deg[m] = m^2$.*

Bevis. Beviset för att $\widehat{[m]} = [m]$ är analogt med beviset för Proposition 4.15 och nyttjar sig av tvåsidig induktion. Vi kan notera att satsen stämmer omedelbart för $m = 0$ och $m = 1$ samt att av Proposition 4.22(c) blir

$$\widehat{[m+1]} = \widehat{[m]} + \widehat{[1]} = \widehat{[m]} + [1]. \tag{2}$$

Antag att satsen stämmer för m. Av (2) så stämmer sedan satsen för $m + 1$ och $m - 1$. Slutligen, låt $d = \deg[m]$. Då kan vi skriva

$$[d] = [m] \circ \widehat{[m]} = [m] \circ [m] = [m^2].$$

Eftersom $\mathrm{End}(E)$ enligt Proposition 4.18 har karakäristik 0 så får vi att $d = m^2$. □

Sats 4.24. *Låt E vara en elliptisk kurva över en kropp K. Om $\mathrm{char}(K) \nmid m$ så blir m-torsionsdelgruppen*

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

Bevis. Av Proposition 4.23 vet vi att $\deg[m] = m^2$ och därmed av Proposition 4.16 samt Sats 4.10 får vi att $\#E[m] = m^2$. Vidare gäller det att för varje $d \mid m$ att $E[d] \subseteq E[m]$ samt $\#E[d] = d^2$. Antag utan inskränkning att $m > 0$ och låt

$$m = \prod_{i=1}^{n} p_i^{e_i}$$

vara primtalsfaktoriseringen av m där $p_1, ..., p_n$ är distinkta primtal samt $e_1, ..., e_n \in \mathbb{Z}_+$. Enligt struktursatsen för ändliga abelska grupper [9, s. 5.2.5] räcker det att visa

$$E[p_i^{e_i}] \cong \frac{\mathbb{Z}}{p_i^{e_i}\mathbb{Z}} \times \frac{\mathbb{Z}}{p_i^{e_i}\mathbb{Z}} \tag{3}$$

ty

$$E[m] \cong E[p_1^{e_1}] \times \cdots \times E[p_n^{e_n}] \tag{4}$$

och således

$$E[m] \cong \left(\frac{\mathbb{Z}}{p_1^{e_1}\mathbb{Z}} \times \frac{\mathbb{Z}}{p_1^{e_1}\mathbb{Z}}\right) \times \cdots \times \left(\frac{\mathbb{Z}}{p_n^{e_n}\mathbb{Z}} \times \frac{\mathbb{Z}}{p_n^{e_n}\mathbb{Z}}\right) \cong \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}.$$

Låt $p_i = p$ och $e_i = N$. Struktursatsen för ändliga abelska grupper samt att $\#E[p^N] = p^{2N}$ ger att

$$E[p^N] \cong \prod_{i=1}^{k} \frac{\mathbb{Z}}{p^{\alpha_i}\mathbb{Z}}$$

där $2N = \alpha_1 + \cdots + \alpha_k$ samt $\alpha_i \geq 1$ för $i = 1, ..., k$. Vi vet att $E[p^d] \leq E[p^N]$ för varje $d \leq N$ och att $\#E[p^d] = p^{2d}$. Speciellt vet vi att $\alpha^i \leq N$ för $i = 1, 2, ..., k$ ty annars kommer det finnas element av ordning större än p^N. Vidare måste $\alpha_i \geq d$ för varje $d \leq N$, då varje $\mathbb{Z}/p^{\alpha_i}\mathbb{Z}$ måste innehålla en delgrupp av element av ordning p^d för att $E[p^N]$ skall innehålla en sådan delgrupp. Alltså får vi att $\alpha_i = N$ för $i = 1, 2, ..., k$, samt då deras summa måste bli $2N$ är $k = 2$, så vi får

$$E[p^N] \cong \frac{\mathbb{Z}}{p^N\mathbb{Z}} \times \frac{\mathbb{Z}}{p^N\mathbb{Z}}.$$

□

4.5 Frobenius-endomorfin

Vi kommer nu att skifta vårt fokus till studien av elliptiska kurvor definierade över ändliga kroppar. Vi har redan tidigare sett att Frobeniusautomorfin spelar en central roll inom studien av ändliga kroppar och deras kroppsutvidgningar. För elliptiska kurvor över ändliga kroppar har Frobeniusautomorfin en naturlig analog, den så kallade *Frobenius-endomorfin*, som är av speciellt intresse för oss då den kommer spela en central roll vid studien av rationella punkter till elliptiska kurvor över ändliga kroppar. Speciellt kommer vi att vara intresserade för den avbildning som Frobeniusendomorfin inducerar på Tate-modulen. Vi kommer vidare genom hela avsnittet anta $q = p^n$ för något primtal p och heltal $n \geq 1$.

Sats 4.25. *Låt E vara en elliptisk kurva definierad över $\mathbb{F}_q$ med Weierstrassekvation $F(X, Y) = 0$. Låt*

$$\phi : E \to E, \qquad [x : y : z] \longmapsto [x^q : y^q : z^q].$$

Då är ϕ en fullständigt inseparabel endomorfi på E med $\deg \phi = q$ vars fixpunkter är exakt $E(\mathbb{F}_q)$.

Definition 4.26. Med E samt ϕ som i Sats 4.25 kallar vi ϕ för *Frobenius-endomorfin* av E.

Bevis. Notera att per definitionen av $\mathbb{F}_q$ så består kroppen av precis de $x \in \overline{\mathbb{F}}_p$ som är rötter till $x^q - x$. Därmed gäller det att $x^q - x = 0$ om och endast om $x \in \mathbb{F}_q$, således kommer avbildningen $x \mapsto x^q$ fixera precis $\mathbb{F}_q$.

Vi ska nu visa att $\phi \in \mathrm{End}(E)$. Vi börjar med att visa att ϕ är en morfi $E \to E$. Enligt [1, Thm 2.4(c)] räcker det att visa att den inducerade kroppsutvidgningen $\overline{\mathbb{F}}_q(E)/\phi^*\overline{\mathbb{F}}_q(E)$ är ändlig och att $\phi^*\overline{\mathbb{F}}_q(E)$ är funktionskroppen till E. Vi börjar med att visa att $\phi^*\overline{\mathbb{F}}_q(E) = \overline{\mathbb{F}}_q(E)^q$. Låt $f \in \overline{\mathbb{F}}_q[X, Y, Z]$ och låt $f^{(q)}$ vara polynomet i $\overline{\mathbb{F}}_q[X, Y, Z]$ vars koefficienter är koefficienterna till f upphöjt till q. Då blir

$$\phi^*(f^{(q)})(P) = f^{(q)}(\phi(P)) = f^{(q)}(x^q, y^q, z^q) = (f(x, y, z))^q.$$

Alltså är $\phi^*\overline{\mathbb{F}}_q[X, Y, Z] = \overline{\mathbb{F}}_q[X, Y, Z]^q$. Vidare, om $f \in I(E)$ får vi då att

$$\phi^*(f^{(q)})(P) = (f(x, y, z))^q = 0.$$

Det följer att $(-)^{(q)}$-konstruktionen kan överföras till $\overline{\mathbb{F}}_{q,H}[E]$. Då E är definierad över $\mathbb{F}_q$ så är $I(E)$ genererad av $F \in \mathbb{F}_q[X,Y,Z]$, därmed är $I(\phi(E)) = I(E)^q = I(E)$. Det följer att $\phi^*\overline{\mathbb{F}}_q(E) = \overline{\mathbb{F}}_q(E)^q$. Vidare, av Definition 2.11 kan vi skriva element i $\overline{\mathbb{F}}_q(E)$ som f/g där $f, g \in \overline{\mathbb{F}}_{q,H}[E]$ har samma grad. Därmed, med notation som ovan får vi för $f/g \in \overline{\mathbb{F}}_q(E)$

$$\phi^*(f/g) = \frac{f(\phi(X,Y,Z))}{g(\phi(X,Y,Z))} = \frac{(f^{(q)}(X,Y,Z))^q}{(g^{(q)}(X,Y,Z))^q} \in \overline{\mathbb{F}}_q(E)^q.$$

Så $\phi^*\overline{\mathbb{F}}_q(E) = \overline{\mathbb{F}}_q(E)^q$. Dessutom så genereras $I(\phi(E))$ av Weierstrassekvationen $F(X,Y,Z) = 0$, så $\phi(E) = E$. Vi visar nu att utvidgningen även är ändlig. Av [1, Cor III.3.1.1] så är $\overline{\mathbb{F}}_q(E) = \overline{\mathbb{F}}_q(x,y)$, där $x, y \in \overline{\mathbb{F}}_q(E)$ är koordinatfunktioner på E. Speciellt kan man visa att $\overline{\mathbb{F}}_q(E)^q = \overline{\mathbb{F}}_q(x^q, y^q)$. Sedan är $\overline{\mathbb{F}}_q(x,y^q)/\overline{\mathbb{F}}_q(x^q,y^q)$ och $\overline{\mathbb{F}}_q(x,y)/\overline{\mathbb{F}}_q(x,y^q)$ två ändliga kroppsutvidgningar, så vi får att $\overline{\mathbb{F}}_q(E)/\overline{\mathbb{F}}_q(E)^q$ är en ändlig kroppsutvidgning och $\phi : E \to E$ är en icke-konstant morfi. Vi får sedan omedelbart att $\phi(O) = O$ då $O = [0:1:0]$, så ϕ är en isogeni och alltså $\phi \in \mathrm{End}(E)$.

Vi visar nu att $\deg \phi = q$. Tag $P \in E$. Då E är per definition slät finns en uniformisator $t \in \overline{\mathbb{F}}_q(E)$ vid P. Enligt [1, Prop. II.1.4] så är $\overline{\mathbb{F}}_q(E)/\overline{\mathbb{F}}_q(t)$ en ändlig separabel kroppsutvidgning. Vi får då en separabel kroppsutvidgning $\overline{\mathbb{F}}_q(E)/\overline{\mathbb{F}}_q(t)$ samt en fullständigt inseparabel kroppsutvidgning $\overline{\mathbb{F}}_q(E)/\overline{\mathbb{F}}_q(E)^q$. Det följer att $\overline{\mathbb{F}}_q(E) = \overline{\mathbb{F}}_q(E)^q(t)$ då $\overline{\mathbb{F}}_q(E)/\overline{\mathbb{F}}_q(E)^q(t)$ är separabel samt fullständigt inseparabel utvidgning, och måste således vara trivial. Så

$$\deg \phi = [\overline{\mathbb{F}}_q(E)^q(t) : \overline{\mathbb{F}}_q(E)^q].$$

Vi får då att $1, t, ..., t^{\deg\phi - 1}$ blir en bas till $\overline{\mathbb{F}}_q(E)^q(t)$ sedd som ett $\overline{\mathbb{F}}_q(E)^q$-vektorrum, där $\deg\phi$ är det minsta värdet p^m för vilket $t^{p^m} - a = 0$ för något $a \in \overline{\mathbb{F}}_q(E)^q$ och $m \geq 1$ av [10, Lem. 5.1.20]. För att visa att $\deg\phi = q$ så räcker att visa att $t^{p^{n-1}} \notin \overline{\mathbb{F}}_q(E)^q$, ty då måste $m \geq n$ vilket ger att $n = m$ ty enligt [10, Lem. 2.3.1] måste $\deg\phi = p^m$ dela $q = p^n$. Om $t^{p^{m-1}} = t^{q/p} \in \overline{\mathbb{F}}_q(E)^q$ så finns $f \in \overline{\mathbb{F}}_q(E)$ sådan att $f^q = t^{q/p}$, således blir

$$\frac{q}{p} = \mathrm{ord}_P(t^{q/p}) = q\,\mathrm{ord}_P(f),$$

alltså är $\mathrm{ord}_P(f) = p^{-1}$ vilket är absurt. Därmed är $\deg\phi = q$. □

Vi kommer senare att vilja utnyttja Sats 4.10 tillsammans med Frobenius-endomorfin ϕ för att studera kardinaliteten av $E(\mathbb{F}_q)$, speciellt kommer vi att utnyttja $1 - \phi^m$, så vi behöver visa att $1 - \phi^m$ är separabel.

Sats 4.27. *Låt E vara en elliptisk kurva definierad över en ändlig kropp $\mathbb{F}_q$ och $\phi : E \to E$ Frobenius-endomorfin på E. Då är $1 - \phi^m$ en separabel isogeni för alla $m \geq 1$.*

Bevis. Av [1, Prop. II.4.2c] så är en ändlig morfi $\psi : E \to E$ separabel om och endast om den inducerade avbildningen

$$\psi^* : \Omega_E \to \Omega_E, \qquad \psi^*(f\,dx) = \psi^*(f)\,d(\psi^* x)$$

är injektiv. Av Proposition 3.13 är $\dim \Omega_E = 1$, således är en morfi separabel om och endast om ψ är nollskild. Låt $\omega \in \Omega_E$ vara en invariant differential på E, vi får då att $\psi^*\omega \neq 0$ om och endast om ψ är separabel. Då räcker det alltså att visa att $(1 - \phi^m)^*\omega \neq 0$. Då ϕ är fullständigt inseparabel av Sats 4.25 så är även ϕ^m fullständigt inseparabel av [10, Thm. 5.1.26], och så blir $(\phi^m)^*\omega = 0$. Vi får därmed av Sats 4.13 och Proposition 4.15 att

$$(1 - \phi^m)^*\omega = [1]^*\omega + [-1]^* \circ (\phi^m)^*\omega = [1]^*\omega \neq 0$$

ty [1] anger identiteten på E. □

4.6 Tate-modulen

Som vi tidigare sett bär Frobeniusendomorfin ϕ informationen om $\mathbb{F}_q$-rationella punkter i E genom dess fixpunkter, som man kan se från faktumet att $\#E(\mathbb{F}_q) = \#\ker(1 - \phi) = \deg(1 - \phi)$ via satser

4.10 och 4.27. Vi kan därför studera rationella punkter på E genom att studera Galoisgruppens verkan på kurvan. Ett problem med detta är att E är en abelsk grupp och dess automorfigrupp har därför en relativt komplex struktur. Det vi vill ha är en enklare kontext där vi kan studera Galoisgruppens verkan. Därför introducerar vi följande.

Definition 4.28. Låt A vara en abelsk grupp och $\ell \in \mathbb{Z}$ ett primtal. Vi definierar Tate-modulen $T_\ell(A)$ som

$$T_\ell(A) = \left\{ (x_i) \in \prod_{n=1}^{\infty} A[\ell^n] : \ell x_i = x_{i-1} \right\}$$

med elementvis addition. $A[m]$ betecknar m-torsion elementen i A.

Tate-modulen av en abelsk grupp bildar naturligt en modul över de ℓ-adiska talen $\mathbb{Z}_\ell$, som definieras som

$$\mathbb{Z}_\ell := \left\{ (x_i) \in \prod_{i=1}^{\infty} \mathbb{Z}/\ell^i\mathbb{Z} \mid \ell x_i = x_{i-1} \right\}.$$

Definitionen visar inte fördelen med att introducera Tate-modulen men senare visar vi varför vi vill introducera den.

Sats 4.29. *Låt E vara en elliptisk kurva över K och $\ell \neq \mathrm{char}(K)$ ett primtal. Då är Tate-module $T_\ell(E)$ en fri modul av rang 2, alltså $T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$.*

Bevis. Från tidigare resultat vet vi att $E[\ell^n] \cong \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z}$. Elementen i $E[\ell^n]$ har alltså formen av ett par av element (a, b). Resultatet följer från faktumet att ett par av sekvenser är ekvivalent med en sekvens av par. □

Sats 4.30. *Endomorfier $\phi \in \mathrm{End}(E)$ inducerar endomorfier $\phi_\ell \in \mathrm{End}(T_\ell(E))$.*

Bevis. Låt $\phi \in \mathrm{End}(E)$ vara en endomorfi. Då vet vi att $\phi([\ell]T) = [l]\phi(T)$ och från detta ser vi att ϕ inducerar en linjär transformation $\phi_\ell \in \mathrm{End}(T_\ell(E))$ via att komponentvis applicera ϕ. □

Vi har alltså en gruppverkan av $\mathrm{Gal}(\overline{K}/K)$ på en fri modul över $\mathbb{Z}_\ell$ vilket öppnar möjligheten att använda linjär algebra för att studera Galoisgruppens verkan på E. Mer specifikt kan vi nyttja determinanten och spåret av den inducerade transformationen.

Sats 4.31. *Låt $\phi \in \mathrm{End}(E)$ vara en endomorfi på en elliptisk kurva E och $\phi_\ell : T_\ell(E) \to T_\ell(E)$ den inducerade avbildningen på Tate-modulen. Då gäller det att*

$$\begin{aligned} \det(\phi_\ell) &= \deg(\phi) \\ \mathrm{tr}(\phi_\ell) &= 1 + \deg(\phi) - \deg(1 - \phi). \end{aligned}$$

För att bevisa detta behöver vi ett tekniskt verktyg som kallas *Weils e_m-parning*. Till att börja med, låt $\boldsymbol{\mu} \subset \overline{K}^*$ vara gruppen av enhetsrötter, alltså de element x så att $x^n = 1$ för något $n \in \mathbb{Z}_+$. Weils e_m-parning är en bilinjär avbildning $e_m : E[m] \times E[m] \to \boldsymbol{\mu}[m]$ mellan abelska grupper som uppfyller

1. Den är alternerande:

$$e_m(T, T) = 1, \quad \forall T \in E[m]$$

2. Den är icke-degenererad:

$$\forall S \in E[m],\ e_m(S, T) = 1 \implies T = O$$

3. Den är Galois-ekvivariant:

$$e_m(S^\sigma, T^\sigma) = e_m(S, T)^\sigma \quad \forall \sigma \in \mathrm{Gal}(\overline{K}/K)$$

4. Weils e_m-parningar är kompatibla för varierande m:

$$e_{mm'}(S,T) = e_m([m']S,T) \;\; \forall S \in E[mm'],\; T \in E[m]$$

För mer detaljer om e_m-parningen, se [1, s. III.8].

Sats 4.32. *e_m-parningen inducerar en bilinjär avbildning $e : T_\ell(E) \times T_\ell(E) \to T_\ell(\boldsymbol{\mu})$ som uppfyller analoga egenskaper till e_m.*

Bevis. För att visa detta vill vi visa att diagrammet

$$\begin{array}{ccc} E[\ell^{n+1}] \times E[\ell^{n+1}] & \xrightarrow{\cdot \ell} & E[\ell^n] \times E[\ell^n] \\ \Big\downarrow{\scriptstyle e_{\ell^{n+1}}} & & \Big\downarrow{\scriptstyle e_{\ell^n}} \\ \boldsymbol{\mu}[\ell^{n+1}] & \xrightarrow[(-)^\ell]{} & \boldsymbol{\mu}[\ell^n] \end{array}$$

kommuterar, alltså att de två vägarna genom diagrammet sammansätts till samma homomorfi. Om diagrammet kommuterar så blir den inducerade parningen komponentvis applicerad e_m, alltså $e : ((x_i),(y_i)) \mapsto (e_{\ell^i}(x_i, y_i))$, väldefinierad. Från bilinjäriteten av e_m ser vi att $e_{\ell^{n+1}}(S,T)^\ell = e_{\ell^{n+1}}(S, [\ell]T)$ och kommutativiteten av diagrammet följer nu från kompatibiliteten av e_m. □

Proposition 4.33. *Låt $\phi : E \to E$ vara en isogeni med dual $\hat{\phi} : E \to E$. Då gäller det att $e_m(\phi(S), T) = e_m(S, \hat{\phi}(T))$.*

Bevis. Se [1, Prop. III.8.2] □

Från denna proposition följer det att $e(\phi_\ell S, T) = e(S, \hat{\phi}_\ell T)$ vilket nu låter oss bevisa sats 4.31.

Bevis. Välj en bas $\{v_1, v_2\} \subset T_\ell(E)$ och låt $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ vara matrisen som representerar ϕ_ℓ i denna bas. Då ser vi

$$\begin{aligned} e(v_1,v_2)^{\deg \phi} &= e([\deg \phi]v_1, v_2) \\ &= e(\hat{\phi}_\ell \phi_\ell v_1, v_2) \\ &= e(\phi_\ell v_1, \phi_\ell v_2) \\ &= e(av_1 + bv_2, cv_1 + dv_2) \\ &= e(v_1,v_2)^{ad-bc} \end{aligned}$$

där det sista steget följer från bilinjäriteten och alternerandet av e. $ad - bc$ känns igen som determinanten av ϕ_ℓ vilket är oberoende av valet av bas. Detta visar att $\det(\phi_\ell) = \deg \phi$. Formeln involverandes spåret följer från standard linjär algebra och håller för alla 2×2 matriser. □

5 Bevis av Riemannhypotesen

Nu har vi resultaten vi behöver för att kunna bevisa Riemannhypotesen för elliptiska kurvor över ändliga kroppar. Genom detta kapitel kommer vi anta att ϕ betecknar Frobeniusendomorfin och att alla elliptiska kurvor är definierade över $\mathbb{F}_q$. Vi återger definitionen av Zetafunktionen för en elliptisk kurva här.

Definition 5.1. Låt E vara en elliptisk kurva. Zetafunktionen $Z(E/\mathbb{F}_q; T)$ definieras som

$$Z(E/\mathbb{F}_q; T) = \exp\left(\sum_{n=1}^{\infty} \#E(\mathbb{F}_{q^n}) \frac{T^n}{n}\right).$$

Notera här att vi ger en annorlunda definition av Zetafunktionen än i inledningen. Vi kan återfå $\zeta(E/\mathbb{F}_q; s)$ via variabelbytet $T \mapsto q^{-s}$ men för dem beräkningar vi kommer göra finns det ingen mening att göra variabelbytet än.

Anmärkning 5.2. I inledningen definierade vi Zetafunktioner utifrån maximalideal av en ring medans här definierar vi dem utifrån punkter på varieteten. Motivationen till detta kommer från följande faktum. Givet en affin varietet V över en algebraiskt sluten kropp K så finns det en en-till-en korrespondens mellan punkter i V och maximala ideal i $K[V]$.

Vi kommer bevisa ett starkare resultat än att rötterna till $\zeta(E/\mathbb{F}_q; s)$ har realdel $\frac{1}{2}$, nämligen att $Z(E/\mathbb{F}_q; T)$ är en rationell funktion med en väldigt specifik form.

Sats 5.3. *Zetafunktionen $Z(E/\mathbb{F}_q; T)$ för en elliptisk kurva E är en rationell funktion och det finns ett heltal $a \in \mathbb{Z}$ med $|a| \leq 2\sqrt{q}$ så att*

$$Z(E/\mathbb{F}_q; T) = \frac{1 - aT + qT^2}{(1-T)(1-qT)}.$$

Vi behöver ett till resultat innan vi kan bevisa Sats 5.3. Som vi tidigare noterat så stämmer det att $\#E(\mathbb{F}_{q^n}) = \deg(1 - \phi^n)$ för alla $n \in \mathbb{Z}_+$. Via Tate-modulen kan vi då bevisa följande.

Proposition 5.4. *Det existerar komplexkonjugater $\alpha, \beta \in \mathbb{C}$ med magnitud $\sqrt{q}$ som uppfyller $\#E(\mathbb{F}_{q^n}) = 1 + q^n - \alpha^n - \beta^n$ för alla $n \in \mathbb{Z}_+$.*

Bevis. Vi låter α och β vara rötterna till det karakteristiska polynomet $\det(T - \phi_\ell)$ från vilket resultatet kommer följa. För varje rationellt tal $\frac{x}{y} \in \mathbb{Q}$ så gäller det att

$$\det\left(\frac{x}{y} - \phi_\ell\right) = \frac{\det(x - y\phi_\ell)}{y^2} = \frac{\deg(x - y\phi)}{y^2} \geq 0,$$

vilket visar att polynomet $\det(T - \phi_\ell) \in \mathbb{Z}[T]$ har en dubbelrot eller komplexkonjugater till rötter. Detta tillsammans med att $\det(\phi_\ell) = q$ visar den första delen av propositionen. Via beräkning ser vi att $\operatorname{tr}(\phi_\ell^n) = \alpha^n + \beta^n$ och $\det(\phi_\ell^n) = q^n$. Från sats 4.31 följer det nu att

$$\#E(\mathbb{F}_{q^n}) = \det(1 - \phi_\ell^n) = 1 + \det(\phi_\ell^n) - \operatorname{tr}(\phi_\ell^n) = 1 + q^n - \alpha^n - \beta^n.$$

□

Låt oss nu bevisa sats 5.3.

Bevis. Vi får

$$\begin{aligned}
\log(Z(E/\mathbb{F}_q; T)) &= \sum_{n=1}^{\infty} \frac{\#E(\mathbb{F}_{q^n})T^n}{n} \\
&= \sum_{n=1}^{\infty} \frac{(1 + q^n - \alpha^n - \beta^n)T^n}{n} \\
&= -\log(1-T) - \log(1-qT) + \log(1-\alpha T) + \log(1-\beta T).
\end{aligned}$$

Alltså är $Z(E/\mathbb{F}_q; T) = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)} = \frac{1-(\alpha+\beta)T+qT^2}{(1-T)(1-qT)}$. Notera att $\alpha+\beta = \operatorname{tr}(\phi_\ell) = 1+q-\#E(\mathbb{F}_q)$ och därför ett heltal. □

Vi ser nu alltså att $\zeta(E/\mathbb{F}_q; s)$ har samma rötter som funktionen $(1 - \alpha q^{-s})(1 - \beta q^{-s})$ vilket implicerar att s måste ha realdel $\Re(s) = \frac{1}{2}$. Detta bevisar Riemannhypotesen.

Referenser

[1] J. H. Silverman, *The Arithmetic of Elliptic Curves* (Applications of Mathematics). Springer, 1986, ISBN: 9780387962030. DOI: https://doi.org/10.1007/978-0-387-09494-6.

[2] E. Bombieri, "Problems of the Millennium: the Riemann Hypothesis", 2000.

[3] M. Rosen, *Number Theory in Function Fields*. Springer New York, 2002, ISBN: 9781475760460. DOI: 10.1007/978-1-4757-6046-0. URL: http://dx.doi.org/10.1007/978-1-4757-6046-0.

[4] R. Hartshorne, *Algebraic Geometry* (Graduate Texts in Mathematics). Springer, 1977, ISBN: 9780387902449.

[5] J. Brzeziński, *Galois Theory Through Exercises* (Graduate Texts in Mathematics), 1. utg. Springer Cham, 2018, ISBN: 978-3-319-72325-9. DOI: https://doi.org/10.1007/978-3-319-72326-6.

[6] T. Stacks project authors, *The Stacks project*, https://stacks.math.columbia.edu, 2025.

[7] M. Atiyah och I. MacDonald, *Introduction To Commutative Algebra* (Addison-Wesley series in mathematics). Avalon Publishing, 1994, ISBN: 9780813345444.

[8] W. Fulton, *Algebraic Curves: An Introduction to Algebraic Geometry*. 2008, ISBN: 9780805330816.

[9] S. Dummit och R. M. Foote, *Abstract Algebra*, 3. utg. John Wiley & Sons Inc., 2004, ISBN: 978-0-471-43334-7.

[10] S. H. Weintraub, *Galois Theory* (Universitext), 1. utg. Springer New York, 2006, ISBN: 978-0-387-28917-5. DOI: https://doi.org/10.1007/0-387-28917-8.

Användning av AI i arbetet

AI har inte använts för detta arbete.

A Appendix 1 – Notationsindex

K	Perfekt kropp
$\mathbb{F}_q$	En ändlig kropp av ordning q
$\overline{K}$	Algebraiskt hölje av K
$\mathrm{Gal}(L/K)$	Galoisgruppen av kroppsutvidgningen L/K
K^*	Multiplikativa gruppen av K
$\mathbb{A}^n$	Det affina n-rummet
$\mathbb{P}^n$	Det projektiva n-rummet
$V(K)$	K-rationella punkterna för en varietet V
$\overline{K}[V]$	Koordinatringen av en affin varietet V
$\overline{K}(V)$	Funktionskroppen av en varietet V
M_P	maximalidealet av $\overline{K}[V]$ hörande till $P \in V$.
$\overline{K}[V]_P$	lokala ringen vid $P \in V$.
$\overline{K}_H[V]$	Homogena koordinatringen av en projektiv varietet V.
$\deg \phi$	Graden av en morfi mellan kurvor.
$\mathrm{Div}(C)$	Divisorgruppen hörande till en kurva C
$\mathrm{Div}^0(C)$	Delgruppen av $\mathrm{Div}(C)$ med divisorer av grad 0.
$\mathrm{Div}^0_K(C)$	Delgruppen av $\mathrm{Div}^0(C)$ som är invariant under $\mathrm{Gal}(\overline{K}/K)$-verkan.
$\mathrm{ord_P}$	Räknar multipliciteten av en funktion $f \in \overline{K}(E)$ i punkten P.
$\mathrm{Pic}(C)$	Picardgruppen av en kurva C
$\mathrm{Pic}^0(C)$	delgruppen av $\mathrm{Pic}(C)$ av grad 0-divisorer
$f\ dx$	En differentialform på en kurva C, $f, x \in \overline{K}(C)$
Ω_C	Rummet av differentialformer på en kurva C
$\mathcal{L}(D)$	Vektorrummet av funktioner f med $\mathrm{Div}(f) \geq -D$.
$\ell(D)$	Dimensionen av $\mathcal{L}(D)$.
$\mathrm{Hom}(E_1, E_2)$	Gruppen av isogenier mellan två elliptiska kurvor
$\mathrm{End}(E)$	Rummet av endomorfier på en elliptisk kurva
$[m]$	Heltalsmultiplikatiom på en elliptisk kurva
$\hat{\phi}$	Duala isogenin för någon isogeni ϕ
$A[m]$	m-torsionsdelgruppen av en abelsk grupp A
$T_\ell(A)$	Tate-modulen över en abelsk grupp A
$\mathbb{Z}_\ell$	De ℓ-adiska talen
e_m	Weils e_m-parning
$Z(E/\mathbb{F}_q; T)$	Zetafunktionen av $E/\mathbb{F}_q$.