Uvod u aritmetiku eliptičkih krivulja

1. Uvod i motivacija - 1. lekcija

Začetci ideje o eliptičkim krivuljama mogu se nazrijeti kod Diofanta (vjerojatno u 3. stoljeću) u postupku rješavanja jednadžba u racionalnim brojevima (diofantskih jednadžba). Nakon stoljeća zaborava Bachet je u 17. stoljeću ponovno otkrio slične postupke, a Newton ih geometrijski interpretirao. Preko Fermata (17. st.), Poincarea (19.-20. st.), Mordella, Weila, Serra i drugih, razvoj te ideje doveo je koncem 20. stolječa do rješenja Fermatova teorema (Wiles). Uz taj, aritmetički aspekt eliptičkih krivulja, postoji i onaj geometrijski i analitički, koji se kroz razvoj pojma eliptičkih integrala i eliptičkih funkcija može pratiti od 17. st. (Wallis, Newton), preko 18. st. (J.Bernoulli, MacLaurin, Fagnano, Euler), 19. st. (Legendre, Gauss, Abel, Jacobi, Riemann, Weierstrass, Klein, Poincare), do današnjih dana.

Integrali racionalnih funkcija

Racionalna funkcija je funkcija F koja se može zapisati kao kvocijent dvaju polinoma, dakle

$$F = \frac{g}{h}$$

gdje su f, g polinomi (koeficijenti mogu biti u bilo kojem polju, ali, u ovom kontekstu smatramo da su to realni brojevi; takodjer, racionalne funkcije mogu biti u jednoj, dvjema ili u više varijabla). Poznato je da se

$$\int \frac{g(x)}{h(x)} dx \tag{1}$$

može uvijek izraziti u terminima elementarnih funkcija. Na primjer,
$\int \frac{dx}{1+x^2} = arctg(x) + C$ i $\frac{dx}{x} = \ln x + C$, za $x > 0$.

Integrali oblika $\int R(x, \sqrt{ax^2 + bx + c})dx$

Po složenosti, nakon integrala racionalnih funkcija, dolaze integrali koji se mogu zapisati pomoću x i $\sqrt{ax + b}$, za neke realne brojeve a, b. Oni se, nakon jednostavne zamjene varijabla, svode na integrale racionalnih fukcija. Nešto su složeniji integrali koji se mogu zapisati u obliku

$$\int R(x, \sqrt{ax^2 + bx + c})dx \tag{2}$$

gdje je R racionalna funkcija u dvjema varijablama, primjerice $\int \frac{x+1}{2+\sqrt{3x^2-4x+5}}dx$. I ti se integrali mogu **racionalizirati**, tj. prikladnom zamjenom varijabla svesti na integrale racionalnih funkcija (tu je bitno da se racionalizacija može provesti pomoću racionalnih funkcija). Jedna od metoda su **Eulerove supstitucije**, koje se na dijele na one:
(I) vrste, za $a > 0$,
(II) vrste, za $D > 0$, gdje je D diskriminanta polinoma $f(x) := ax^2 + bx + c$, i
(III) vrste, ako je $c > 0$.

Na primjer, za (III) vrstu zamjena je: $\sqrt{ax^2 + bx + c} = tx + \sqrt{c}$, odakle se dobije $x = \frac{2\sqrt{c}t-b}{a-t^2}$ i $dx = \frac{2\sqrt{c}t^2-2bt+2a\sqrt{c}}{(a-t^2)^2}dt$ (tu se vidi da je x racionalna funkcija od t).

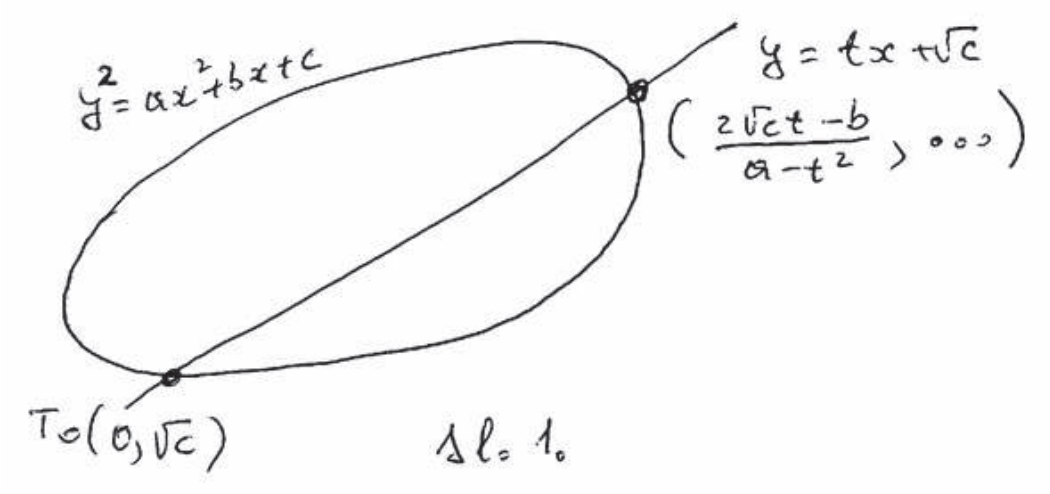
Pokazuje se da se te supstitucije temelje na geometrijskim svojstvima krivulje

$$y^2 = ax^2 + bx + c \tag{3}$$

koja se prirodno pojavljuje uz ovakav integral, odnosno na činjenici da je to krivulja 2. reda - **konika** (tu zanemarujemo trivijalni slučaj, kad je $D = 0$). Naime, uvjet $c > 0$ osigurava postojanje točke s realnim koordinatama $T_0(0, \sqrt{c})$ na krivulji, a

$$y = tx + \sqrt{c} \tag{4}$$

za $t \in \mathbf{R}$ je jednadžba pramena pravaca kroz T_0 (osim jednog pravca). Kako je krivulja konika, svaki od tih pravaca (osim tangente) presijeca krivulju u još jednoj točki T, koja nužno ima realne koordinate, čime se uspostavlja bijekcija izmedju točaka konike i realnih parametara t (osim jednog izuzetka); kažemo da smo **parametrizirali** koniku. Lako se vidi da je prva koordinata točke T upravo $x = \frac{2\sqrt{c}t-b}{a-t^2}$ kao u (III) Eulerovoj supstituciji, a za $y \geq 0$ je $y = \sqrt{ax^2 + bx + c}$, pa (4) postaje zamjena $\sqrt{ax^2 + bx + c} = tx + \sqrt{c}$ (sl.1.).



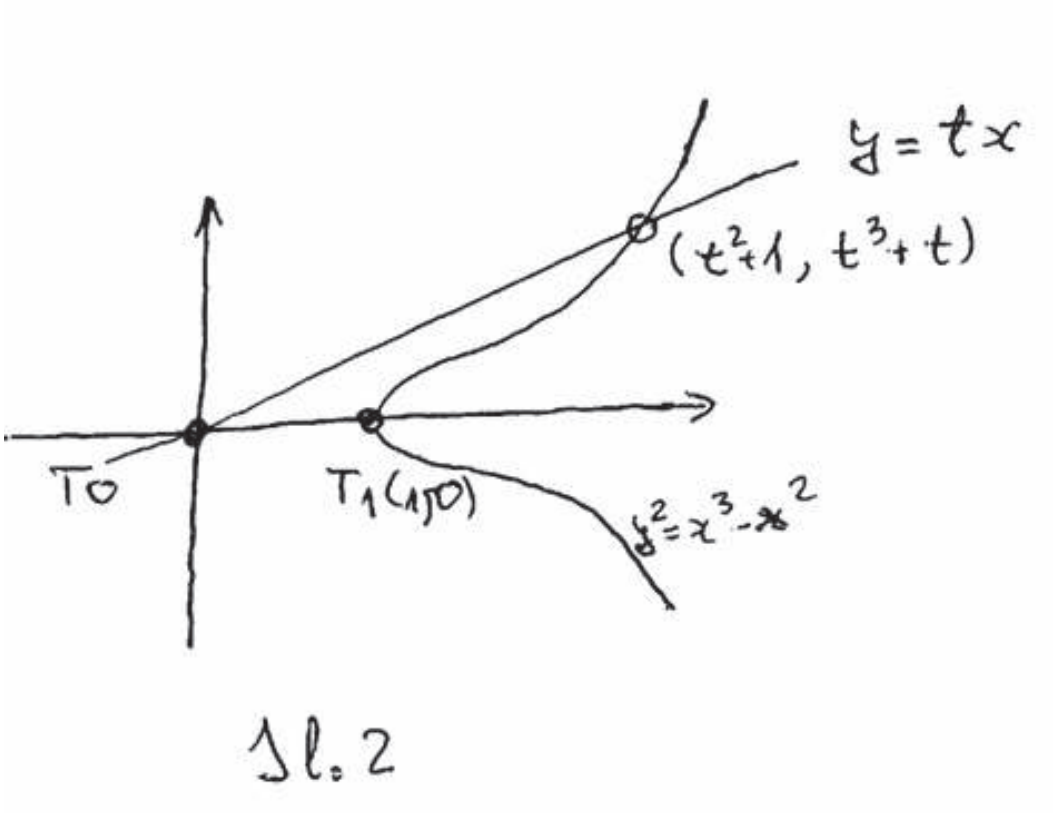
Uočite da su tu x i y racionalne funkcije od t; takodjer (inverzna transformacija) t je racionalna funkcija od x i y.

Eliptički integrali

Situacija se bitno usložnjava za integrale oblika $\int R(x, \sqrt{f(x)}dx$ gdje je f polinom 3. stupnja: $f(x) := ax^3 + bx^2 + cx + d$, te a, b, c, d realni brojevi i $a \neq 0$.

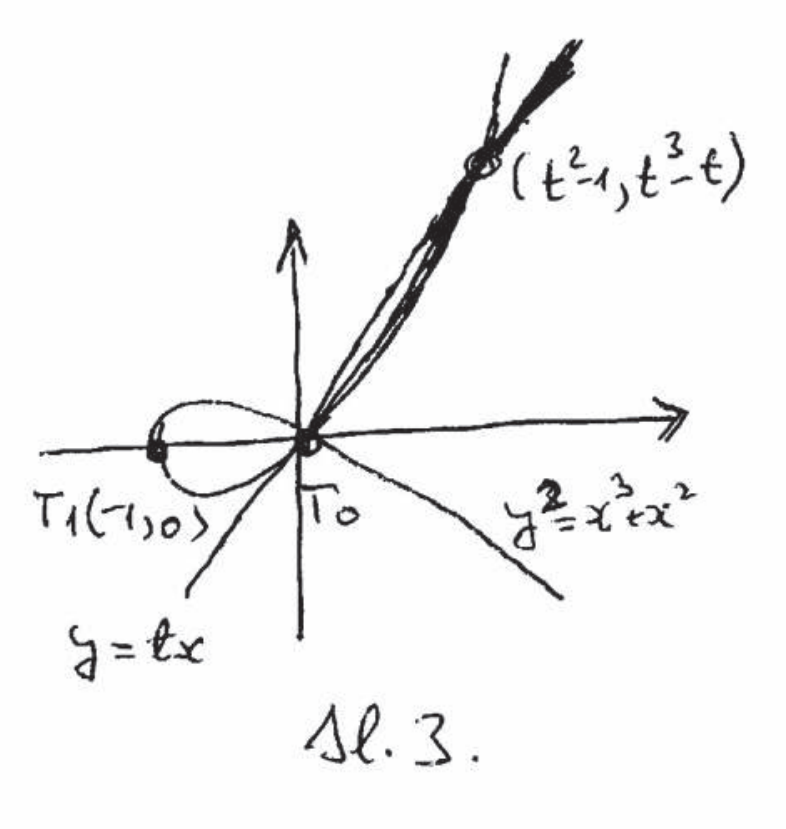
Napomena 1. Polinom f može se zamjenom $X := \sqrt[3]{a}x$ svesti na oblik $f(X) = X^3 - 3AX^2 + BX + C = (X - A)^3 - (3A^2 - B)X + (C + A^3)$, a ovaj, dalje, zamjenom $X - A := u$, na oblik $f(u) = u^3 + pu + q$, za realne p, q. Imajući to na pameti, obično ćemo kubni polinom pisati u obliku $f(x) = x^3 + ax + b$.
Neki integrali s $\sqrt{x^3 + ax + b}$ su poput onih iz (2).

Primjer 1. (a) $\int \frac{dx}{\sqrt{x^3 - x^2}}$ racionalizirat ćemo tako da pogledamo pripadnu krivulju $y^2 = x^3 - x^2$ (sl.2) i uočimo izoliranu točku $T_0(0.0)$.



Sl. 2

Vidimo da pravci $y = tx$ kroz T_0 parametriziraju tu krivulju, uvrštavanjem u jednadžbu krivulje i kraćenjem dobije se $x = t^2 + 1$ pa se integral racionalizira: $\int \frac{2t}{t(t^2+1}dt$. Uočite da analogon postupak s pravcima kroz točku $T_1(1, 0)$ ne bi urodio plodom (za razliku od integrala (2) gdje nije bitan izbor točke). (b) Uz $\int \frac{dx}{\sqrt{x^3+x^2}}$, prirodno ide krivulja $y^2 = x^3 + x^2$, kojoj se odmah uočavaju dvije točke: $T_0(0, 0)$ i $T_1(-1, 0)$. Kao i u a), parametrizacija pravcima kroz T_0 uspijeva, a kroz T_1 ne uspijeva (sl. 3.).



Sl. 3.

Ono što je uspjelo s integralima iz Primjera 1, nikako nije uspijevalo matematičarima 18. st. općenito s integralima poput

$$\int \frac{dx}{\sqrt{x^3 + ax + b}} \tag{5}$$

Slično je bilo i s integralima $\int \frac{dx}{\sqrt{f(x)}}$ za polinome f četvrtog stupnja, na primjer $\int \frac{dx}{\sqrt{x^4-1}}$. Takvi integrali i integrali (5), uz uvjet da podintegralni polinomi nemaju višestrukih korijena, primjeri su **eliptičkih integrala**. Koncem 18. st. shvatilo se da se takvi integrali ne mogu riješiti u terminima elementarnih funkcija (puno objašnjenje tek je od sredine 19. st.). Uspjeh u Primjeru 1 omogućen je upravo činjenicom što su podintegralni polinomi višestruke korijene, a točka kroz koju se provlače pravci bila ona koja odgovara tim dvostrukim korijenima. Na jeziku krivulja to je bila **singularna točka**. O tome čemo više govoriti poslije.

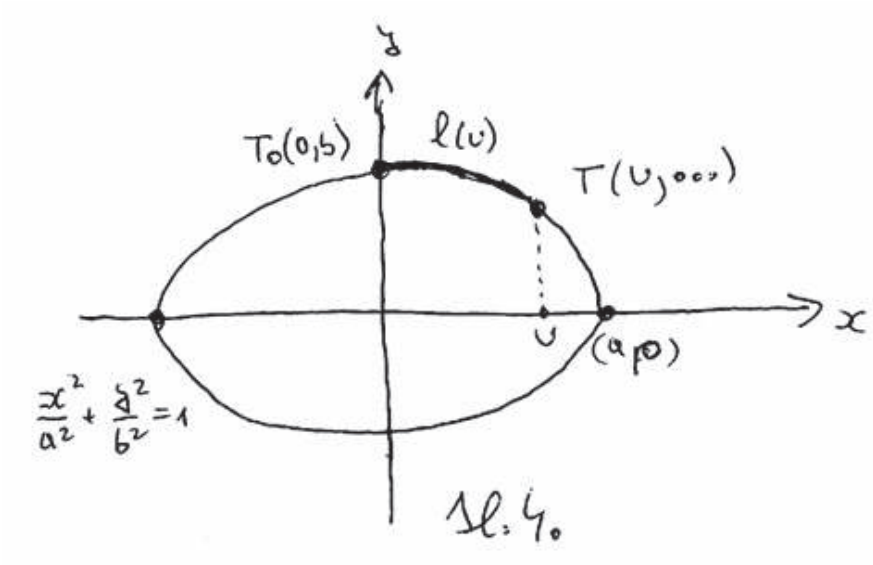
Naziv Eliptički integral

Taj naziv nastaje od *elipse*, zato što se pojavljuje u problemu odredjivanja duljine luka elipse. Problem odredjivanja opsega elipse još je iz starogrčkih vremena, a naročito je postao aktualan nakon Keplerovih zakona (početkom 17. st.). Za razliku od formule za površinu unutar elipse $P = \pi ab$ koja je prirodno poopćenje formule za površinu kruga $P = \pi r^2 = \pi r \cdot r$, a ostvaruje se zamjenom jednog r u a, a drugog u b, tako se nešto ne dogadja s opsegom: izraz $2\pi r$ tj. $\pi(r + r)$ pri analognom postupku prelazi u $\pi(a + b)$, što je uvijek, osim za $a = b = r$ manje od opsega elipse. U 17. st. uočeno je da je odredjivanje formule za opseg elipse problem integralnog računa i prva rješenja (u obliku beskonačnog reda) dali su Wallis, Newton i, poslije njih, MacLaurin. Red s vrlo brzom konvergencijom čekao je 19. st. Takav je Gauss-Kummerov red:

$$O = \pi(a + b) \sum_{n \geq 0} [\binom{\frac{1}{2}}{n}^2 h^n]$$

gdje je $h := (\frac{a-b}{a+b})^2$. Ramanujan je pronašao vrlo preciznu približnu formulu $O \approx \pi(a + b)(3 - \sqrt{4 - h})$.

Za odredjivanje duljine luka krivulje, predpostavimo da je $a > b$ i pogledajmo sl.4.



Tu je:
$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$ - jednadžba elipse,
$y = \frac{b}{a}\sqrt{a^2 - x^2}$ - jednadžba gornje poluelipse
$y' = -\frac{b}{a}\frac{x}{\sqrt{a^2-x^2}}$,
$l(u)$ - duljina lika elipse od točke $T_0(0, b)$ do točke $T(u, ...)$.
Kako je
$l(u) = \int_0^u \sqrt{1 + y'^2}dx$, dobijemo

$$l(u) = a\int_0^{\frac{u}{a}} \sqrt{\frac{1 - k^2t^2}{1 - t^2}}dt \tag{6}$$

gdje je $t = ax$ i $k^2 = 1 - \frac{b^2}{a^2}$. Posebno je opseg elipse

$$O = 4a\int_0^1 \sqrt{\frac{1 - k^2t^2}{1 - t^2}}dt$$

Ako stavimo $t = \sin\phi$, što je dio prirodne parametrizacije elipse $x = a\sin\phi$, dobijemo $l(u) = a\int_0^{arcsin\frac{u}{a}} \sqrt{1 - k^2\sin^2\phi}d\phi$, odnosno $O = 4a\int_0^{\frac{\pi}{2}} \sqrt{1 - k^2\sin^2\phi}d\phi$. Drugi korijen se može rastaviti u red potencija i integrirati član po član. Tako imamo MacLaurinov rezultat iz 1742.

$$O = 2\pi a(1 - \frac{1}{4}k^2 - \frac{3}{64}k^4 - \frac{5}{256}k^6 - ...)$$

Integral (6), samo bez granica (radi jednostavnosti), dalje se može napisati kao $a\int \frac{1-k^2t^2}{\sqrt{(1-t^2)(1-k^2t^2)}}dt$, odnosno kao

$$a\int \frac{dt}{\sqrt{(1 - t^2)(1 - k^2t^2)}} - ak^2\int \frac{t^2dt}{\sqrt{(1 - t^2)(1 - k^2t^2)}}$$

Prvi od ovih integrala obično se zove **eliptički integral prve vrste**, a drugi **eliptički integral treće vrste** (ako su u tim integralima granice od 0 do 1 kaže se da su **potpuni**).

Svodjenje $\int \frac{dt}{\sqrt{(1-t^2)(1-k^2t^2)}}$ na oblik $\int \frac{dz}{\sqrt{f(z)}}$, $degf = 3$.

Pokazuje se da se integrali gornjeg tipa s polinomom 4. stupnja pod korijenom uvijek mogu svesti na one s s polinomom 3. stupnja pod korijenom (ali daljnja redukcija općenito nije moguća). Stavimo:

$z = \frac{1}{1-t},\ t = 1 - \frac{1}{z},\ dt = \frac{1}{z^2}dz$ i dobit ćemo:
$\int \frac{dt}{\sqrt{(1-t^2)(1-k^2t^2)}} = \int \frac{dz}{\sqrt{\frac{1+t}{1-t}\frac{1-kt}{1-t}\frac{1+kt}{1-t}}} = \int \frac{dz}{\sqrt{(2z-1)((1-k)z+k)((k+1)z-k)}}.$

Tu se pojavljuje slična situacija onoj s formulama za rješenje algebarskih jednadžba u radikalima:
(I) za $n = 1$ i $n = 2$, tj. za jednadžbe $ax + b = 0$ i $ax^2 + bx + c = 0$ formule su poznate od davnina.
(II) Za $n = 3$ čekalo se gotovo do polovice 16. st., a slučaj $n = 4$ reducira se na kubni. Pokazalo se da je za uporabu formule (u slučaju realnih rješenja) presudno uvodjenje kompleksnih brojeva.
(III) Za $n \geq 5$ nema općenite formule i za zapis rješenja treba uvesti nove funkcije.

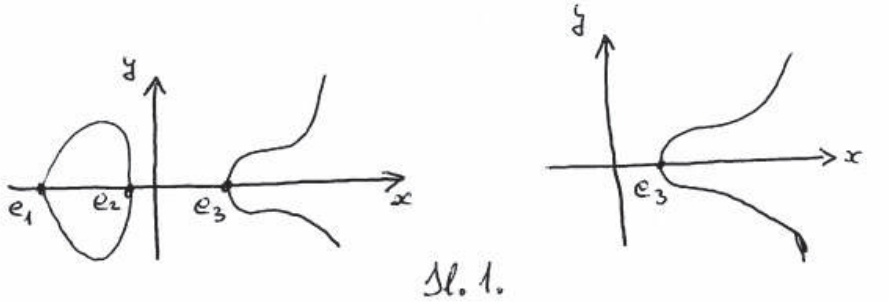
Za integrale $\int \frac{dx}{\sqrt{f(x)}}$ uz $n = degf$ vrijedi:
(I) za $n = 1$ i $n = 2$ integral se racionalizira racionalnim funkcijama, pa se izražava elementarnim funkcijama.
(II) za $n = 3$ integral se općenito ne racionalizira racionalnim funkcijama, već tzv. eliptičkim funkcijama (uniformizacija) i nije elementaran (o tome ćemo više reći poslije). Slučaj $n = 4$ svodi se na $n = 3$. Pokazuje se da je za pravilno tretiranje potrebno uvodjenje kompleksnih brojeva.
(III) za $n \geq 5$ za uniformizaciju su potrebne druge vrste funkcija.

Uvod u aritmetiku eliptičkih krivulja

1. Uvod i motivacija 2. lekcija

Genus (rod) orijentirane kompaktne plohe

Pokazalo se da je za proučavanje integrala oblika $\int \frac{dx}{\sqrt{f(x)}}$ (i njima sličnih, već nakon $degf \geq 3$ gotovo nemoguće izbjeći kompleksne brojeve. Abel je, da bi razriješio problem dvoznačnosti kompleksnog drugog korijena, uveo njegovo razmatranje na tzv. *dvolistnom natkrivanju* skupa kompleksnih brojeva. To u biti znači da je gledao pripadnu ravninsku krivulje $El : y^2 = f(x)$ (koja je, kako smo vidjeli u prvoj lekciji, tijesno povezana s integralom) i da je razmatrao sve kompleksne točke (oznaka $El(\mathbf{C})$).
Neka je, na primjer, $f(x) = x^3 + ax + b$ polinom bez višestrukih korijena, s realnim koeficijentima a, b. Tada se pripadna krivulja $y^2 = f(x)$ zove **eliptička krivulja**. Kako $El(\mathbf{C})$ ima kompleksnu dimenziju 1, njena je realna dimenzija 2, pa je riječ o plohi (to se može izravno dobiti rastavljajući realni i imaginarni dio od x i y). Na primjer, ako stavimo $x = x_1 + ix_2$ i $y = y_1 + iy_2$, onda svaka kompleksna točka krivulje (u, v) postaje realna (u_1, u_2, v_1, v_2) čije koordinate povezuju dvije nezavisne jednadžbe (svaka od njih dimenziju spušta za 1). Svaka točka od $El(\mathbf{C})$ ima bazu okolina koje su homeomorfne otvorenim krugovima u $\mathbf{C}$ (tu je bitno da f nema višestrukih korijena), što u koordinatama (x_1, x_2, y_1, y_2) znači da svaka točka ima bazu okolina homeomorfnih otvorenim krugovima u realnoj ravnini.
Skup realnih točaka $El(\mathbf{R})$ možemo predočiti kao na sl.1. (tu smo uzeli da je $x^3 + ax + b = (x - e_1)(x - e_2)(x - e_3)$ i posebno nacrtali slučaj kad su svi korijeni realni - tada postoje dvije komponente, a posebno kad je samo e_1 realan - jedna komponenta povezanosti).

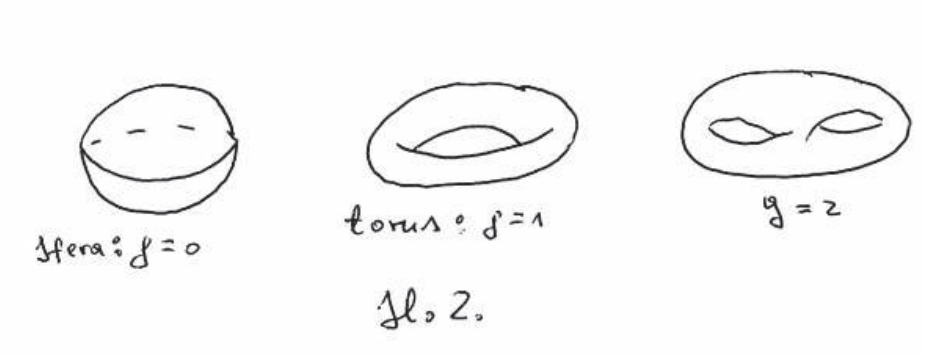


Sl. 1.

Možemo zamisliti da smo onoj nezatvorenoj komponenti dodali beskonačno daleku točku O (u kojoj se sijeku svi pravci usporedni s y osi) tako da je i ona postala zatvorena. O tome čemo potanje govoriti kad budemo obradjivali projektivne koordinate.
Skup $El(\mathbf{C})$ teže je predočiti, ali ga možemo zamisliti kao dvostruko natkrivanje kompleksnog pravca (kompleksne ravnine) preko projekcije na prvu koordinatu (abelovo dvolistno natkrivanje):

$$(x, y) \mapsto x$$

Tu iznad svake točke kompleksnog pravca postoje dvije točke krivulje (upravo one koje se u nju projiciraju; iznad x je $(x, \pm\sqrt{x^3 + ax + b})$ gdje je $\sqrt{}$ odabran po volji kompleksni drugi korijen), osim za $x = e_1$ ili $x = e_2$ ili $x = e_3$, kada je samo jedna (na primjer iznad $x = e_1$ nalazi se samo $(e_1, 0)$). Zato takvo natkrivanje zovemo **razgranatim**, ono se **grana** iznad točaka e_i pravca (u ovom slučaju su **indeksi grananja** 2). Abel je uočio potrebu da se kompleksnim brojevima doda znak ∞; tako se pravac **kompaktificira** (upotpuni **beskonačno dalekom točkom** i dobije **Riemannova sfera**). $El(\mathbf{C})$ se upotpuni onom istom točkom O od prije i pri tom se projicira u ∞ (znači da je i tu grananje). Pokazat ćemo poslije, pomoću homogenih koordinata, da se na oba objekta može uvesti prirodna topologija pri kojoj je ova projekcija neprekinuto preslikavanje (i više od toga).
Riemannova sfera je homeomorfna običnoj sferi u realnom trodimenzionalnom prostoru. Manje je očito da je $El(\mathbf{C}) \cup O$ homeomorfna torusu. Poznata je klasifikacija dvodimenzionalnih kompaktnih orijentiranih (realnih, povezanih) ploha, prema broju rupa - genusu (rodu). Na primjer, sfera ima genus 0, a torus genus 1 (sl.2.).



Sl. 2.

Smisao je da su dvije takve plohe homeomorfne ako i samo ako imaju jednake genuse. Orijentiranost izbacuje projektivnu ravninu i analogne konstrukcije pomoću nje. Standardno se proučavanje ploha temelji na činjenici da se mogu **triangulirati**. To je jedan od načina da se dokaže da je genus od $El(\mathbf{C}) \cup O$ jednak 1. Mi će mo to izvesti iz **Hurwitzove formule** za Riemannove plohe (koja se može dokazati upravo pomoću triangulacije):
Ako su X i Y kompaktne Riemannove plohe s genusima g_X i g_Y i $f : X \to Y$ surjektivno (tj. netrivijalno) analitičko preslikavanje, onda je;

$$2g_X - 2 = n(2g_Y - 2) + \sum_{P \in Y} (e_P - 1) \tag{1}$$

gdje je n stupanj od f i e_P indeksi grananja u točkama od Y.

Kod nas je $X = El(\mathbf{C}) \cup O$, Y je Riemannova sfera, $g_Y = 0$, f je projekcija na prvu koordinatu, $n = 2$, indeksi grananja su 1 (tj. nema grananja), osim u točkama e_1, e_2, e_3 i ∞ u kojima je indeks grananja 2. Zato je:
$2g_X - 2 = 2(0 - 2) + 4$, odakle dobijemo $g_X = 1$.

Aritmetika i geometrija

U geometriji algebarskih krivulja razmatramo sve kompleksne točke, dok nas u aritmetici zanimaju samo točke s racionalnim koordinatama (ili cijelim). Na primjer, jednadžba

$$f(x, y) = 0$$

gdje je f ireducibilan polinom s racionalnim koeficijentima definira algebarsku krivulju, a skup svih kompleksnih rješenja (uključujući beskonačno daleke točke) topološka je kompaktna povezana orijentirana ploha (uz uvjet da nema singularnih točaka, a ako ih ima treba malo modificirati). Pripadni je diofantski (aritmetički) problem odredjivanje racionalnih rješenja, što je obično vrlo težak problem (i ne postoji algoritam koji ga općenito rješava). Ipak, pokazuje se da geometrija dobro opisuje aritmetiku. Naime, diofantska složenost ovisi o genusu g pripadne algebarske krivulje:
(i) ako je $g = 0$, tj. ako je pripadna ploha Riemannova sfera, diofantski problemi su načelno rješivi; može biti da nema ni jedno racionalno rješenje, ali ako ima bar jedno, ima ih beskonačno mnogo.
(ii) ako je $g = 1$, onda je situacija najbogatija, matematički najzanimljivija i,

općenito daleko od završetka; može se dogoditi da nema racionalnih rješenja, da ih ima konačno mnogo ili beskonačno mnogo.
(iii) ako je $g \geq 2$ za pripadne se krivulje kaže da su **općeg tipa** i po mnogo čemu imaju sličnu geometriju; pripadna jednadžba ima konačno mnogo rješenja.

Eliptički se integral ne može racionalizirati racionalnim funkcijama

Tu je činjenicu naslutio J.Bernoulli koncem 17. st., ali je postala jasna činjenica tek početkom 19. st. Racionalna racionalizacija znači i racionalnu parametrizazaciju pripadne eliptičke krivulje

$$x = \phi(t),\ y = \psi(t),\ \text{tj. } t \mapsto (\phi(t), \psi(t)) \tag{2}$$

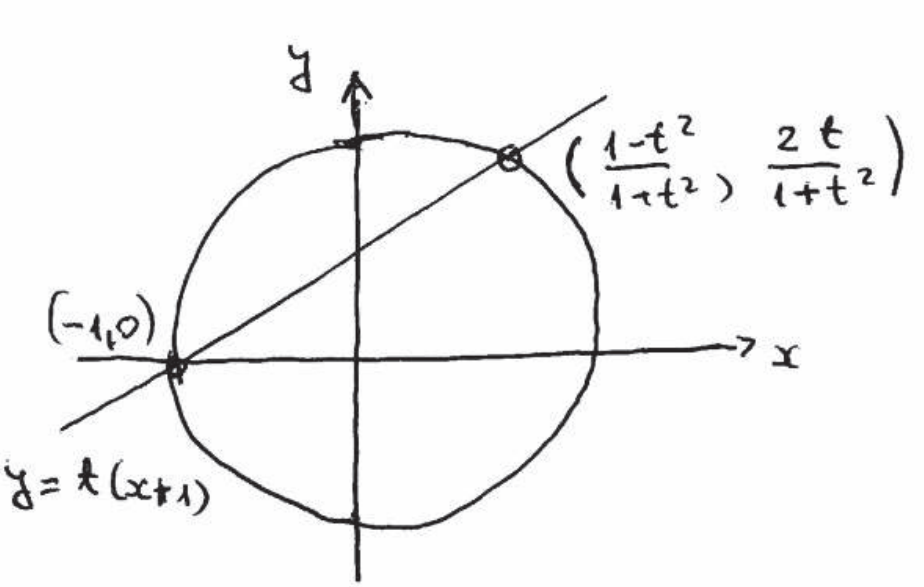
gdje su ϕ i ψ racionalne funkcije od t. Za zaključak o nemogućnosti potrebne su nam sljedeće činjenice:
(i) ta se parametrizacija prosiruje, po istoj formuli, na kompleksne brojeve t i kompleksne točke na eliptičkoj krivulji
(ii) ova nova parametrizacija proširuje se do neprekinute bijekcije (čak i više) s Riemannove sfere na $El(\mathbf{C}) \cup O$.
ovo (ii) je nemoguće jer su genusi različiti.
Napominjemo da ovo ne znači da se eliptički integral ne može racionalizirati (nekim drugim funkcijama). Takodjer, ovo gore nije dokaz da je eliptički integral neelemantaran (što je zaista istina i pokazuje se na više načina, a proizlazi i iz jednog Liouvillovog teorema iz 1833.).

Uniformizacija eliptičke krivulje

Integral $\int \frac{dx}{\sqrt{1-x^2}}$ može se racionalno racionalizirati na pr. pomoću formula za racionalizaciju jedinične kružnice (**stereografska projekcija**). Evo formula za stereografsku projekciju iz točke $(-1, 0)$ (sl.3.):

$$y = t(x+1);\ x = \frac{1-t^2}{1+t^2},\ y = \frac{2t}{1+t^2};\ dx = \frac{-4t}{(1+t^2)^2}dt$$

Sad je:
$\int \frac{dx}{\sqrt{1-x^2}} = \int \frac{-2dt}{1+t^2} = -2arctg(t) + C = -2arctg\sqrt{\frac{1-x}{1+x}} + C.$



Sl. 3.

Vidjeli smo da takvo nešto nije moguće za eliptički integral, medjutim moguće je nešto drugo. Vratimo se opet na jediničnu kružnicu i njenu parametrizaciju trigonometrijskim funkcijama

$$t \mapsto (\sin(t), \cos(t)), \ -\pi \leq t < \pi$$

Sad je $\int \frac{dx}{\sqrt{1-x^2}} = \int dt = arcsinx + C$ (provjerite da ste dobili isti rezultat kao i racionalnom parametrizacijom). Postavlja se pitanje može li se ovo prenijeti i na eliptičke krivulje. Ideja kojom se to realiziralo potječe od Abela (a i Jacobija), a to je tzv. **invertiranje eliptičkog integrala**. Naime, kako eliptički integral nisu mogli zapisati pomoću elementarnih funkcija, matematičari 18. st. su ih tretirali kao nove funkcije od gornje granice, tako da su gledali, na primjer

$$g(u) := \int_{\alpha}^{u} \frac{dx}{\sqrt{x^3 + ax + b}}$$

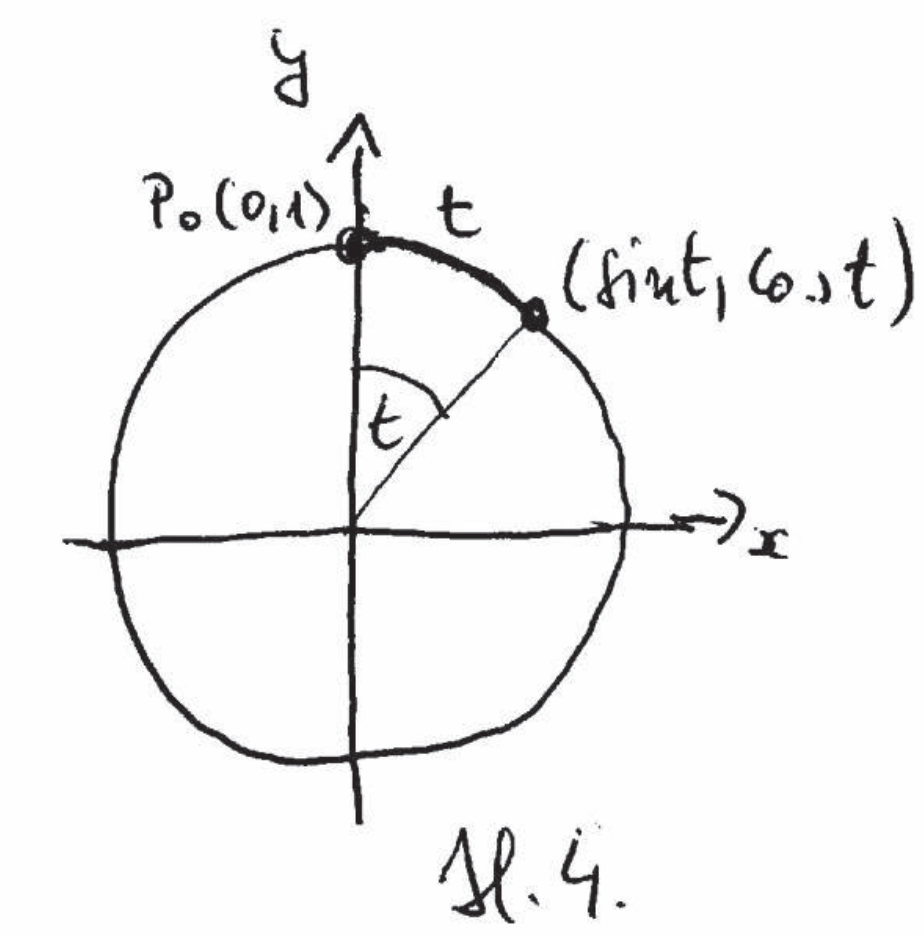
za neki zgodno odabrani fiksirani α i varijabilni u. Abel je uveo novinu da gornja granica bude funkcija od rezultata, tj.

$$\int_{\alpha}^{h(t)} \frac{dx}{\sqrt{x^3 + ax + b}} = t$$

Koristnost takvog pristupa vidi se kod jednakosti

$$\int_0^{h(t)} \frac{dx}{\sqrt{1-x^2}} = t \tag{3}$$

kojoj je rješenje $h(t) = \sin t$ za $-\frac{\pi}{2} \leq t < \frac{\pi}{2}$. Sad je $t \mapsto (h(t), h'(t))$ parametrizacija gornje polukružnice, koja se proširuje na parametrizaciju kružnice $t \mapsto (\sin t, \cos t)$, dalje se funkcije sin i cos po periodnosti proširuju na cijeli $\mathbf{R}$ (sl.4.).



Sl. 4.

Ako analogno postupimo za eliptički integral dobijemo $\int_\alpha^{h(t)} \frac{dx}{\sqrt{f(x)}} = t$. Neka je $S(x)$ primitivna funkcija od podintegralne funkcije, tj. $S(h(t)) -$

$S(\alpha) = t$, a odavde $S'(h(t))h'(t) = 1$, tj. $h'(t) = \sqrt{f(h(t))}$, pa je $t \mapsto (h(t), h'(t))$, za t iz nekog realnog intervala, parametrizacija jednog dijela (realne) eliptičke krivulje. Na tom dijelu imamo i racionalizaciju eliptičkog integrala. Naime zamjenom $x = h(t)$, $\sqrt{f(h(t))} = h'(t)$, $dx = h'(t)dt$ dobijemo

$$\int \frac{dx}{\sqrt{f(x)}} = \int dt = t + C = h^{-1}(x) + C.$$

Uočite da sve ovo vrijedi za svaki polinom f, a ne samo za one 3. stupnja. I za integral i za ovakvu parametrizaciju krivulje postavljaju se dva pitanja:
1. Može li se h proširiti kao u slučaju jedinične kružnice, tako da $t \mapsto (h(t), h'(t))$ bude parametrizacija cijele krivulje?
2. Kako se h može analitički definirati?

Odgovor na 1. pitanje je niječan ako ostanemo na realnim parametrima (i krivuljama). Abel je problem riješio tako da je prešao na kompleksne parametre i pokazao da se h može definirati kao meromorfna dvostruko periodna funkcija (s dva realno nezavisna perioda). Njegova metoda je oponašanje situacije kod jedinične kružnice $\mathbf{T}$ i trigonometrijskih funkcija. Za njihovo pravilno tumačenje, umjesto parametrizacije, pogledajmo preslikavanje

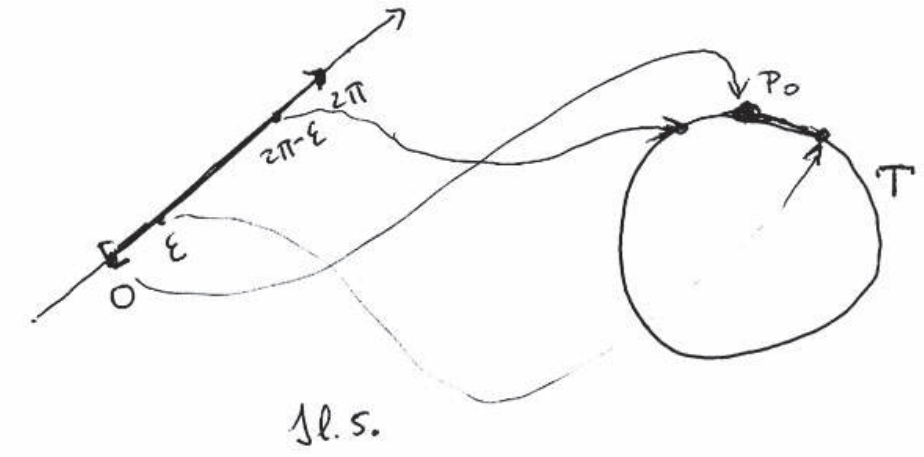
$$\mathbf{R} \mapsto \mathbf{T},\ t \mapsto (\sin t, \cos t).$$

To je homomorfizam aditivne grupe realnih brojeva i multiplikativne grupe (realnih) točaka na $\mathbf{T}$ s grupnom operacijom $(x_1, y_1) \cdot (x_2, y_2) = (x_1y_2 + y_1x_2, y_1y_2 - x_1x_2)$ (ta se grupna operacija na $\mathbf{T}$ razlikuje od one standardne naslijedjene od formule $|z_1z_2| = |z_1||z_2|$ ako točke od $\mathbf{T}$ shvatimo točkama jedinične kompleksne kružnice što bi bilo pogodno ako bismo imali preslikavanje $t \mapsto (\cos t, \sin t)$; u našem slučaju neutralni je element $P_0(0, 1)$, a u standardnom $(1, 0)$). Jezgra tog homomorfizma je diskretne podgrupa $2\pi\mathbf{Z}$ od $\mathbf{R}$. Zato imamo izomomorfizam

$$\mathbf{R}/2\pi\mathbf{Z} \cong \mathbf{T},\ t + 2\pi\mathbf{Z} \mapsto (\sin t, \cos t) \tag{4}$$

(to je i topološki i realno analitički izomorfizam ako na $\mathbf{R}/2\pi\mathbf{Z}$ uvedemo kvocijentnu topologiju i prirodnu analitičku strukturu; $\mathbf{R}/2\pi\mathbf{Z}$ možemo predočiti kao interval $[0, 2\pi >$, s topologijom kod koje je baza okolina svake nutarnje točke naslijedjena iz $\mathbf{R}$, samo 0 ima bazu okolina oblika $[0, \epsilon > \cup < 2\pi epsilon, 1 >$ za male $\epsilon > 0$ - tako je $\lim_{\epsilon \to 0}(2\pi - \epsilon) = 0$, pa je taj kvocijent

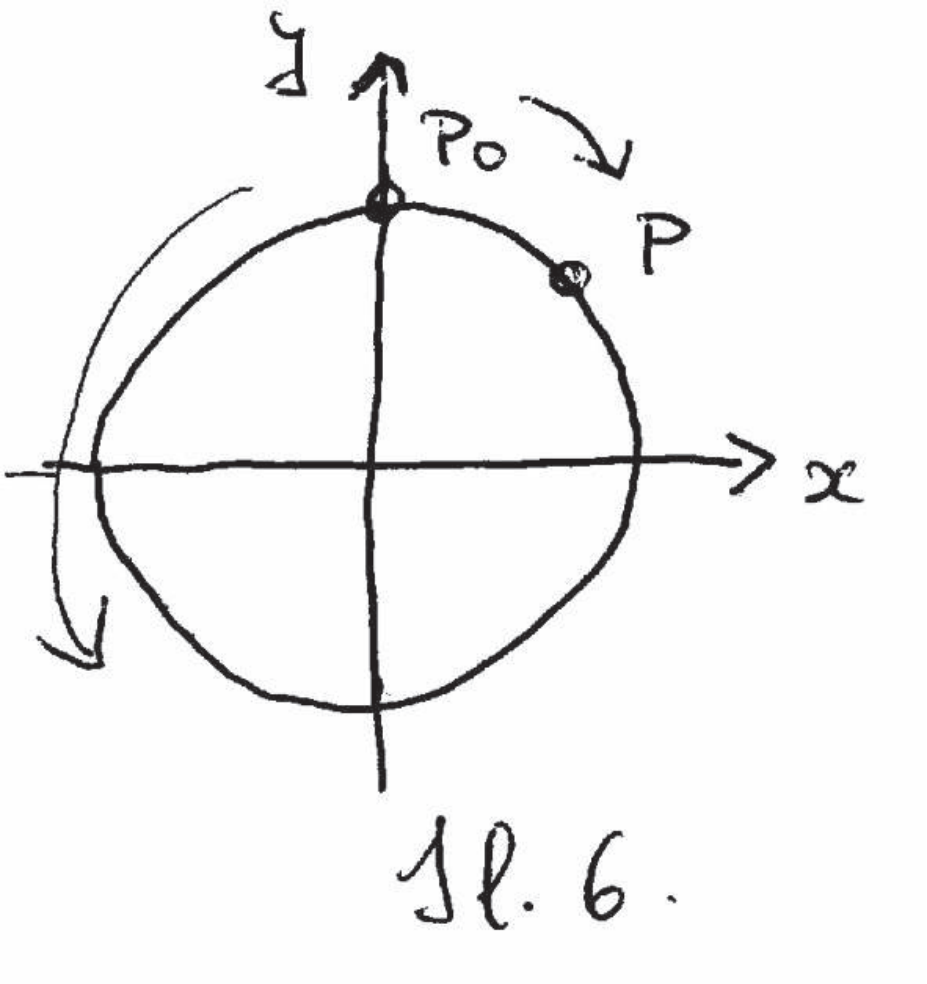
topološki kružnica) (sl.5.).



Prema tome periodne funkcije sin i cos dobiju se iz inverza izomorfizma (4).

Rekonstrukcija trigonometrijske parametrizacije.

Postavlja se pitanje kako se taj inverz može rekonstruirati iz samog $\mathbf{T}$. Kako smo vidjeli, dio funkcije sinus rekonstruira se iz (3). Ako želimo dobiti čitav sinus, možemo postupiti ovako: umjesto integrala po segmentu prijedjemo na krivuljni integral $\int_{P_0}^{P} \frac{dx}{y}$, za $P_0(0,1)$ i P na $\mathbf{T}$. Značenje tog integrala je $\int_{\alpha}^{\beta} \frac{u'(t)dt}{v(t)}$, gdje je $t \mapsto (u(t), v(t))$ diferencijabilno preslikavanje realnog segmenta $[\alpha, \beta]$ u $\mathbf{T}$, uz $(u(\alpha), v(\alpha)) = P_0$ i $(u(\beta), v(\beta)) = P$. Problem je što je taj integral definiran samo do na $2\pi k,\ k \in \mathbf{Z}$ (ovisno o parametrizaciji kojom smo od P_0 došli do P - integral po jednom obilasku u smjeru kazaljke sata jednak je 2π (sl.6.)).



Sl. 6.

Tako smo dobili inverzni izomorfizam

$$P \mapsto \int_{P_0}^{P} \frac{dx}{y} \in \mathbf{R}/2\pi\mathbf{Z} \tag{5}$$

Ako je $\int_{P_0}^{P} \frac{dx}{y} = \bar{t}$, gdje je $\bar{t}$ oznaka za klasu $t + 2\pi\mathbf{Z}$, onda možemo pisati $P = (\bar{h}(\bar{t}), \bar{r}(\bar{t}))$ za funkcije $\bar{h},\ \bar{r} : \mathbf{R}/2\pi\mathbf{Z} \to \mathbf{T}$. Komponirajući te funkcije s prirodnom projekcijom $\mathbf{R} \mapsto \mathbf{R}/2\pi\mathbf{Z}$ dobijemo parametrizaciju

$$t \mapsto (h(t), r(t))$$

od $\mathbf{T}$ (tu su $h(t) = \bar{h}(\bar{t})$ i $r(t) = \bar{r}(\bar{t})$ periodne funkcije perioda 2π). Tvrdimo da je $h = \sin$ i $r = \cos$. Iz definicije proizlazi da je $(h(0), r(0)) = (0, 1)$ i neka

je $P = (h(t), r(t))$, dakle je

$$\bar{t} = \int_{P_0}^{P} \frac{dx}{y} = \int_0^t \frac{h'(t)dt}{r(t)} + 2\pi\mathbf{Z}.$$

Odavde dobijemo $\int_0^t \frac{h'(t)dt}{r(t)} - t \in \{2\pi\mathbf{Z}\}$ za sve t. Kako je na lijevoj strani neprekinuta funkcija, zaključujemo da je konstanta. Uvrstivši $t = 0$ vidimo da je ta konstanta 0 pa je $r = h'$. S druge strane iz $h^2 + r^2 = 1$ dobijemo $hh' + rr' = 0$, a odatle $r' = -h$. Dobili smo diferencijalnu jednadžbu 2. reda s početnim uvjetima:

$$h'' + h = 0,\ h(0) = 0,\ h'(0) = 1$$

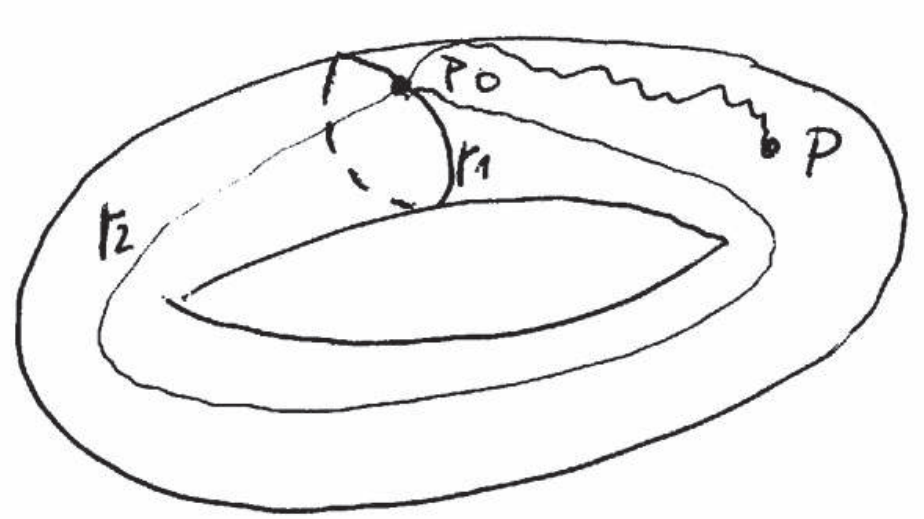
s jedinstvenim rješenjem $h = \sin$, a odavde $r = \cos$, kako smo i tvrdili.

Proširenje ideje na eliptičke krivulje.

Abelova ideja za racionalizaciju eliptičkog integrala u biti je analogno definiranje funkcija kojima se parametrizira pripadna eliptička krivulja. Pokazalo se da je to općenito nemoguće ako se zadržimo na realnim parametrima. To je uvjetovalo uvodjenje kompleksnih brojeva i gledanje kompleksnih točaka tj. $El(\mathbf{C})$. Takodjer, treba dodati beskonačno daleku točku O. Sad se potpuno analogno gleda

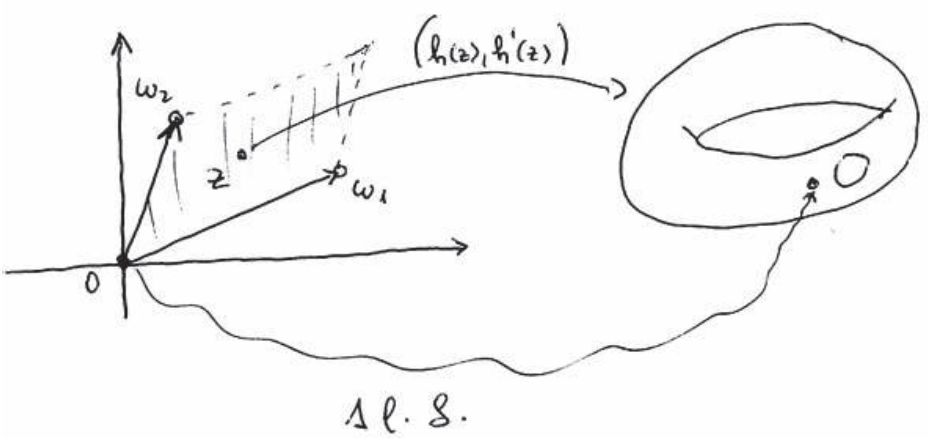
$$P \mapsto \int_O^P \frac{dx}{y} \tag{6}$$

po torusu $El(\mathbf{C}) \cup \mathbf{O}$, što nije jednoznačno definirano već do na izraz $m\omega_1 + n\omega_2$ za $m, n \in \mathbf{Z}$ gdje su **periodi** ω_1 i ω_2 integrali po dvama izabranim jednostavnim ciklima γ_1, γ_2 (kao na sl.7.) - izvodnicama prve grupe homologije $H_1(torus, \mathbf{Z})$.



Sl. 7.

Ti su periodi linearno nezavisni nad $\mathbf{R}$ i generiraju rešetku $L := \{m\omega_1 + n\omega_2\}$. Kao i prije, dobiju su kompleksne funkcije h, r uz $r = h'$ samo sad dvostrukoperiodne (s osnovnim periodima ω_1, ω_2), ali ne analitičke, već meromorfne s polovima u L, koje parametriziraju eliptičku krivulju: $z \mapsto (h(z), h'(z))$ i ostvaruju analitički izomorfizam $\mathbf{C}/L \cong El(\mathbf{C}) \cup \mathbf{O}$ (ako se na desnoj strani grupni zakon definira tako da je zbroj triju točaka nula ako se nalaze na jednom pravcu). Kažemo da smo **uniformizirali** eliptičku krivulju (sl.8.).



Sl. 8.

Uvod u aritmetiku eliptičkih krivulja

1. Eliptičke krivulje nad $\mathbf{C}$ (skica) - 3. lekcija

Već smo vidjeli da se eliptička krivulja (točnije skup svih njenih kompleksnih točaka, uključujući i beskonačno daleku točku) može parametrizirati (uniformizirati) dvostrukoperiodnim kompleksnim funkcijama h, h', koje se dobiju integriranjem po torusu $E(\mathbf{C})$ (od sad ćemo eliptičku krivulju zadanu jednadžbom $y^2 = x^3 + ax + b$ označavati kao E, skup njenih kompleksnih točaka, uključujući i beskonačno daleku točku, kao $E(\mathbf{C})$, skup realnih točaka kao $E(\mathbf{R})$ i sl.). Do baze za rešetku perioda Abel je izvorno došao integriranjem po pripadnom torusu. Einsensteinova je ideja da se krene od $\mathbf{C}$ i od po volji odabrane dvodimenzionalne rešetke

$$L = \{m\omega_1 + n\omega_2\},\ m, n \in \mathbf{Z}$$

gdje su ω_1, ω_2 $\mathbf{R}$-linearno nezavisni kompleksni brojevi koji čine bazu rešetke, pa da se konstruiraju meromorfne funkcije kojima je L skup perioda. On je dao i prijedlog kako se tako funkcije mogu konstruirati. Eisenstein je umro mlad, a njegovu ideju razradio je Weierstrass.

Weierstarssove $\mathcal{P}$ i $\mathcal{P}'$ funkcija

Neka je $L = \mathbf{Z}\omega_1 \oplus \mathbf{Z}\omega_2$ fiksirana rešetka u $\mathbf{C}$ (gdje su ω_1, ω_2 linearno nezavisni nad $\mathbf{R}$). **Weierstrassova $\mathcal{P}$ funkcija** (pridužena rešetki L) je funkcija zadana redom:

$$\mathcal{P}(z) := \frac{1}{z^2} + \sum_{\omega \in L \setminus \{0\}} [\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}] \tag{1}$$

Da bi se naglasilo o kojoj je rešetki riječ često se piše $\mathcal{P}_L(z)$ ili slično. Vrijedi sljedeće (a dokaže se standardnim postupkom):
(I) Red (1) konvergira apsolutno na $\mathbf{C} \setminus L$.
(II) Red (1) konvergira uniformno na kompaktima od $\mathbf{C} \setminus L$.

Svojstvo (I) potvrdjuje da je (1) dobro definirano tj. da ne ovisi o redoslijedu zbrajanja, a skupa s (II) da je $\mathcal{P}$ analitička funkcija na $\mathbf{C} \setminus L$, koja se može derivirati član po član. Dalje, vrijedi (što ćemo i dokazati):

(i) $\mathcal{P}$ je parna funkcija. Naime, $\mathcal{P}(-z) := \frac{1}{z^2} + \sum_{\omega \in L \setminus \{0\}} [\frac{1}{(z-(-\omega))^2} - \frac{1}{(-\omega)^2}] = \mathcal{P}(z)$, jer je $-L = L$.

(ii) $\mathcal{P}'(z) := -2\sum_{\omega\in L}\frac{1}{(z-\omega)^3}$ je L-periodna (tj. za periode ima sve elemente iz L, odnodno ima dva nezavisna perioda pa je dvostruko periodna) neparna analitička na $\mathbf{C}\setminus L$ funkcija. Zato kažemo da je $\mathcal{P}'$ **eliptička funkcija** (ili, preciznije, L-eliptička funkcija). Periodnost ide izravnim uvrštavanjem i korištenjem $-L = L$, a neparnost kao i u (i).
(iii) $\mathcal{P}$ takodjer je periodna, pa je eliptička. Naime, iz
$\mathcal{P}'(z+\omega) = \mathcal{P}'(z)$, za svaki fiksirani $\omega \in L$ i svaki $z \in \mathbf{C}$ (uz interpretaciju da je vrijednost u točkama rešetke beskonačna), integriranjem se dobije $\mathcal{P}(z+\omega) = \mathcal{P}(z) + C$, za svaki fiksirani $\omega \in L$ i svaki $z \in \mathbf{C}$, gdje je C kompleksna konstanta ovisna samo o izabranom ω. Uvrštavanjem $z = -\frac{\omega}{2}$ iz parnosti od $\mathcal{P}$ proizlazi da je $C = 0$. Kako sve vrijedi za bilo koji ω, $\mathcal{P}$ je eliptička.
(iv) (Laurentov razvoj od $\mathcal{P}$ oko ishodišta). Za $z \neq 0$ sa svojstvom $|z| < \min\{|\omega|,\ \omega \in L\setminus\{0\}\}$ vrijedi

$$\mathcal{P}(z) = \frac{1}{z^2} + 3G_4 z^2 + 5G_6 z^4 + 7G_8 z^6 + ...$$

gdje je

$$G_k := \sum{}' \frac{1}{\omega^k}$$

za $k \geq 3$ Eisensteinov red (znak sume s crticom znači da se sumira po svim ne-nul elementima rešetke - uočite da za neparne indekse k je $G_k = 0$, a za parne ≥ 4 red apsolutno konvergira). Za dokaz je dovoljno razmotriti:

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{1}{\omega^2}[\frac{1}{(1-\frac{z}{\omega})^2} - 1]\frac{1}{\omega^2}\sum_{n=1}^{\infty}(n+1)\frac{z^n}{\omega^n}$$

Sumirajući po svim $\omega \neq 0$ dobijemo traženi razvoj.
(v) $\mathcal{P}$ je meromorfna na $\mathbf{C}$ s polovima 2. reda u L, a $\mathcal{P}'$ je meromorfna na $\mathbf{C}$ s polovima 3. reda u L. Naime, iz razvoja (iv) se vidi da je u 0 pol 2. reda, a zbog eliptičnosti (tj. L-periodnosti) tako je u svakoj točki rešetke.
(vi) Vrijedi

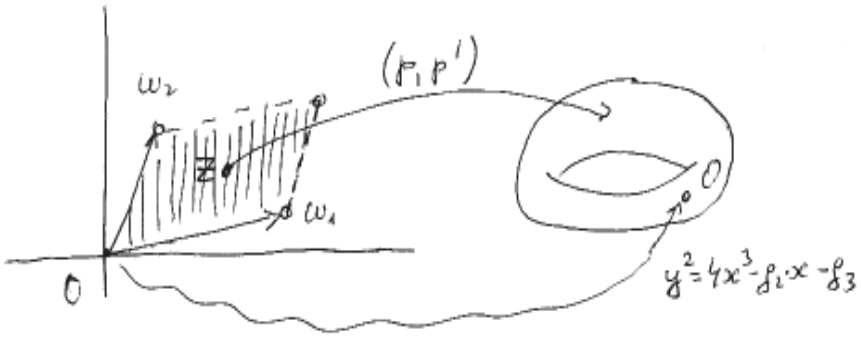
$$\mathcal{P}'(z)^2 = 4\mathcal{P}(z)^3 - g_2\mathcal{P}(z) - g_3$$

gdje je $g_2 := 60G_4,\ g_3 := 140G_6$. Naime, iz razvoja (iv) dobije se:
$\mathcal{P}'(z)^2 = \frac{4}{z^6} - \frac{24G_4}{z^2} - 80G_6 + ...$

$\mathcal{P}(z)^3 = \frac{1}{z^6} + \frac{9G_4}{z^2} + 15G_6 + ...,$
pa je $H(z) := \mathcal{P}'(z)^2 - 4\mathcal{P}(z)^3 + g_2\mathcal{P}(z) + g_3$ analitička L-periodna funkcija na $\mathbf{C}$ sa svojstvom $H(0) = 0$. Ona je omedjena na fundamentalnom periodu, pa i na cijelom $\mathbf{C}$, pa je konstanta. Kako joj je jedna vrijednost 0 ona je nula-funkcija, što smo i trebali.
(vii) preslikavanje $\mathbf{C} \mapsto E(\mathbf{C})$, $z \mapsto (\mathcal{P}(z), \mathcal{P}'(z))$, $L \mapsto O$,

gdje je $E : y^2 = 4x^3 - g_2x - g_3$ pripadna eliptička krivulja s beskonačno dalekom točkom O, je dobro definirana surjekcija (da je preslikavanje dobro definirano slijedi iz (vi)). Ona inducira bijekciju

$$\mathbf{C}/L \cong E(\mathbf{C})$$



Sl. 1.

Time smo dobili uniformizaciju eleptičke krivulje E eliptičkim funkcijama $\mathcal{P}, \mathcal{P}'$ (sl.1). Za preciznu formulaciju ove tvrdnje i dokaz trebalo bi uvesti nekoliko novih pojmova i dokazati nekoliko (standardnih) činjenica, što izostavljamo. Posebno gornja bijekcija je analitički izomorfizam grupa, što će imati smisla tek kad definiramo grupnu operaciju na $\mathbf{C}$.
Umjesto toga podrobno ćemo sve ilustrirati na jednom primjeru. Najprije bez dokaza navodimo još jednu dobro poznatu formulu.

(IV) Kako je $G_k := \sum' \frac{1}{(m\omega_1+n\omega_2)^k} = \frac{1}{(\omega_1)^k} \sum' \frac{1}{(m+n\tau)^k}$, gdje je $\tau := \frac{\omega_2}{\omega_1}$ i možemo smatrati da je iz gornje poluravnine $\mathcal{H}$, vidimo da je gotovo dovoljno razmatrati Eisensteinove redove za rešetke razapete bazom $\{1, \tau\}$ za $\tau \in \mathcal{H}$, definirane kao:

$$G_k(\tau) := \sum' \frac{1}{(m + n\tau)^k}.$$

Vrijedi:

$$G_{2k}(\tau) = 2\zeta(2k) + 2\frac{(2\pi i)^{2k}}{(2k-1)!} \sum_{k=1}^{\infty} \sigma_{2k-1}(n) e^{2\pi i n\tau}, \tag{2}$$

gdje je ζ Riemannova zeta funkcija, a $\sigma_r(n) := \sum_{d|n} d^r$, funkcija koja zbraja r-te potencije djelitelja broja n.

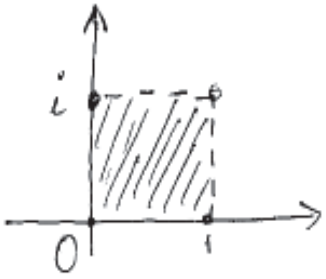
Primjer. Neka je $L := \mathbf{Z} \oplus \mathbf{Z}i$ rešetka razepeta s $\{1, i\}$ (vidi sl.2. gdje je predočen fundamentalni paralelogram). Tada je:

$\mathcal{P}(z) = \frac{1}{z^2} + \sum{}' [\frac{1}{(z-m-ni)^2} - \frac{1}{(m+ni)^2}]$,

$\mathcal{P}'(z) = \frac{-2}{z^3} - 2\sum{}' \frac{1}{(z-m-ni)^3}$,

$g_2 := 60G_4 = 60\sum{}' \frac{1}{(m+ni)^4}$,

$g_3 := 140G_6 = \sum{}' \frac{1}{\quad} - \frac{140}{6}\sum{}' \frac{1}{(n-mi)^6} = -g_3$, pa je $g_3 = 0$.

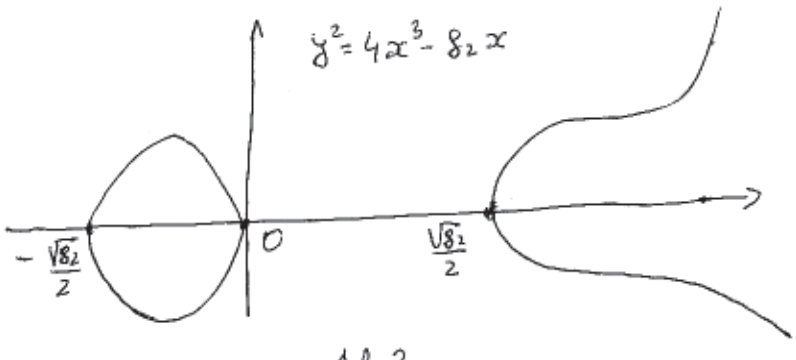


Sl.2.

Nadalje, izravnim uvrštavanjem u (2) dobije se $g_2 > 0$, pa je eliptička krivulja

$$E : y^2 = 4x^3 - g_2 x$$

definirana jednadžbom s realnim koeficijentima i $E(\mathbf{R})$ ima dvije komponente povezanosti, kao na sl.3. Želimo razjasniti koje se točke fundamentalnog paralelograma preko uniformizacije $z \mapsto (\mathcal{P}(z), \mathcal{P}'(z))$ preslikavaju u ove realne točke od E.



Sl.3.

a) Točke presjeka s x-osi: one karakterizirane uvjetom $y = 0$, tj. $\mathcal{P}'(z) = 0$, pa treba naći nultočke te funkcije. Kako je općenito $\mathcal{P}'(\frac{\omega}{2}) = \mathcal{P}'(\frac{\omega}{2} - \omega) =$

$\mathcal{P}'(-\frac{\omega}{2}) = -\mathcal{P}'(\frac{\omega}{2})$ vidimo da je u našem fundamentalnom paralelogramu

$$\mathcal{P}'(\frac{1}{2}) = \mathcal{P}'(\frac{i}{2}) = \mathcal{P}'(\frac{1+i}{2}) = 0$$

To su, očito, jedina rješenja jednadžbe $\mathcal{P}'(z) = 0$ u fundamentalnom periodu (a poslije se sve ponavlja).
b) Tražimo z za koje je $\mathcal{P}(z)$ realno. Kako definicijske redove možemo zbrajati po volji i kako je rešetka invarijantna na konjugiranje (pri konjugiranju prelazi u sebe), vrijedi

$$\overline{\mathcal{P}(z)} = \mathcal{P}(\bar{z})$$

(tj. konjugiranje je "homomorfizam" za beskonačnu sumu). Zato je za sve t za koje je $0 < t < 1$:
$\overline{\mathcal{P}(t)} = \mathcal{P}(t)$
$\overline{\mathcal{P}(ti)} = \mathcal{P}(-ti) = \mathcal{P}(ti)$, zbog parnosti
$\overline{\mathcal{P}(\frac{1}{2} + ti)} = \mathcal{P}(\frac{1}{2} - ti) = \mathcal{P}(-\frac{1}{2} + ti) = \mathcal{P}(\frac{1}{2} + ti)$, zbog parnosti i periodnosti
$\overline{\mathcal{P}(\frac{i}{2} + t)} = \mathcal{P}(-\frac{i}{2} + t) = \mathcal{P}(\frac{i}{2} + t)$, zbog periodnosti
Tako smo našli 4 intervala u fundamentalnom periodu koje funkcija $\mathcal{P}$ preslikava u 4 realna intervala na koje $-\frac{\sqrt{g_2}}{2}$, 0 i $\frac{\sqrt{g_2}}{2}$ dijeli realnu os. Funkcija $\mathcal{P}$ na tim intervalima nije injektivna, već svaku vrijednost osim $-\frac{\sqrt{g_2}}{2}$, 0 i $\frac{\sqrt{g_2}}{2}$ postiže dva puta (u točkama simetričnim s obzirom na $\frac{1}{2}, \frac{i}{2}, \frac{1+i}{2}$). To izravno proizlazi iz identiteta

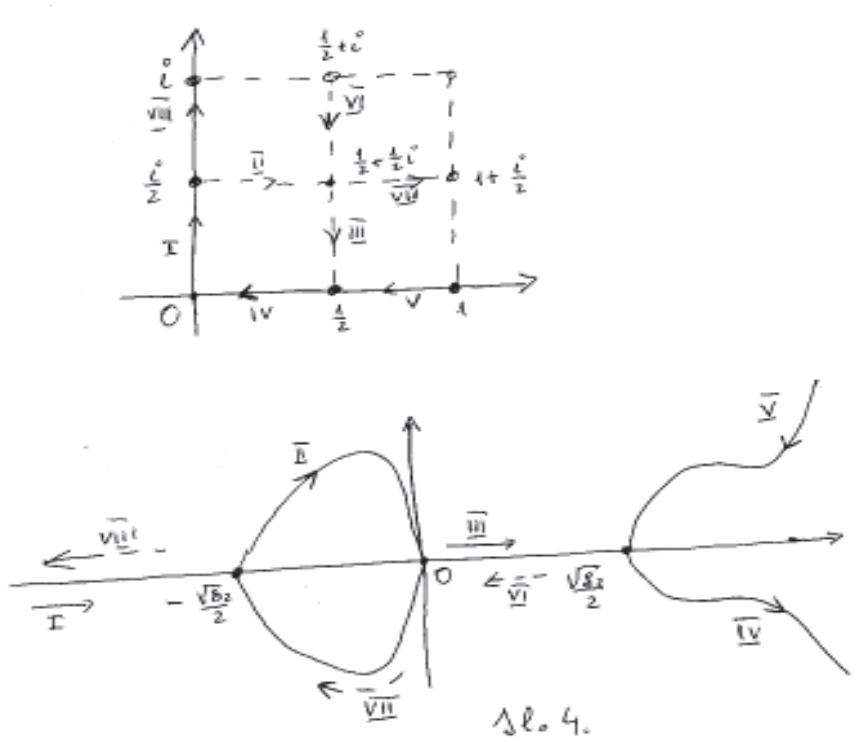
$$\mathcal{P}(\frac{\omega}{2} - z) = \mathcal{P}(\frac{\omega}{2} + z)$$

koji vrijedi za svaki z i svaki period ω (za bilo koju rešetku). Uočite, takodjer da vrijedi

$$\mathcal{P}'(\frac{\omega}{2} - z) = -\mathcal{P}'(\frac{\omega}{2} + z)$$

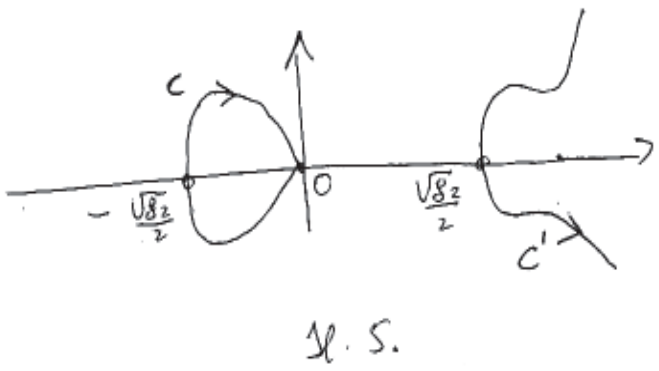
pa u gornjim točkama $\mathcal{P}'$ prima suprotne vrijednosti.
Zato u prvom dijelu svakog od tih intervala $\mathcal{P}$ primi svaku vrijednost iz odredjenog intervala na x-osi, a u drugom dijelu iste te vrijednosti u suprotnom redoslijedu, pri čemu $\mathcal{P}'$ postiže suprotne vrijednosti (u slučaju realnih vrijednosti jednom ispod osi x, a jednom iznad). Zato smo ta 4 intervala podijelili na 8 poluintervala kao na sl.4. i predočili ponašanje $\mathcal{P}$ i $\mathcal{P}'$ funkcije (tu $\mathcal{P}$ u prva četiri intervala prima redom sve realne vrijednosti od $-\infty$ do $+\infty$, a druga četiri u suprotnom redoslijedu, a $\mathcal{P}'$ prima suprotne vrijednosti). Pri odredjivanju putanje sluv zili smo se programskim paketom Mathematica, pune oznake odnose se na prve 4 poluintervala, a iscrtkane na druga 4. Na onim dijelovima nad kojima su druge koordinate imaginarne (tj. prve negativne) oznaku putanje stavljamo iznad x-osi ako su imaginarni dijelovi

pozitivni.



Sl. 4.

Rekonstrukcija perioda $1, i$ **integriranjem po torusu**.
Uvedimo sljedeće oznake (vidi sl.5.):



Sl. 5.

Realni ciklus koji ne sadrži O označimo kao c (dobije se preslikavan-

jem intervala $II \cup VII$), a onaj drugi kao c' (dobije se preslikavanjem intervala $IV \cup V$, c, c' su suprotno orijentirani). Nevidljive imaginarne cikluse označimo kao γ (dobije se preslikavanjem intervala $III \cup VI$), odnosno kao γ' (dobije se preslikavanjem intervala $I \cup VIII$). Tada je (uz zamjenu $x = \mathcal{P}(z),\ y = \mathcal{P}'(z);\ dx = \mathcal{P}'(z)dz$)

$$\int_c \frac{dx}{y} = \int_{\frac{i}{2}}^{\frac{1}{2}+\frac{i}{2}} dz + \int_{\frac{1}{2}+\frac{i}{2}}^{1+\frac{i}{2}} dz = 1.$$

U prijevodu na standardno integriranje po x osi, značenje je:

$$\int_{-\frac{\sqrt{g_2}}{2}}^{0} \frac{dx}{\sqrt{4x^3-g_2x-g_3}} + \int_{0}^{-\frac{\sqrt{g_2}}{2}} \frac{dx}{-\sqrt{4x^3-g_2x-g_3}} = 2\int_{-\frac{\sqrt{g_2}}{2}}^{0} \frac{dx}{\sqrt{4x^3-g_2x-g_3}} = 1.$$

Lako se vidi da se integriranjem po c' dobije -1 (što je logično jer su c i $-c'$ homologni).

Slično se dobije:

$$\int_{\gamma'} \frac{dx}{y} = \int^{\frac{i}{}}$$

Uvod u aritmetiku eliptičkih krivulja

Homogene (projektivne) kordinate - 4. lekcija

Za pravilno definiranje mnogih pojmova i formuliranje mnogih tvrdnja često je potrebno upotpuniti (proširiti) područje razmatranja. Tipične konstrukcije tog tipa su
(1) proširivanje brojnog područja do polja kompleksnih brojeva (ili do nekog algebarski zatvorenog polja)
(ii) upotpunjenje (do potpunog prostora - u kojemu Cauchyjevi nizovi konvergiraju) (iii) kompaktifikacija.

Uvodjenje homogenih koordinata odnosno dodavanje geometrijskim objektima "beskonačno dalekih točaka" u biti je proširenje tipa (iii) iako je nastalo daleko prije topologije. Razmotrit ćemo dva aspekta homogenih koordinata: aritmetički i geometrijski.
Aritmetički aspekt. Razmotrimo jednadžbu

$$x^2 + y^2 = 1 \tag{1}$$

gdje rješenja gledamo u skupu racionalnih brojeva (ta je jednadžba **nehomegena**). Zamjenom $x = \frac{X}{Z},\ y = \frac{Y}{Z}$, gdje su X, Y, Z cijeli brojevi i množenjem s nazivnikom dobijemo **homogenu jednadžbu**

$$X^2 + Y^2 = Z^2 \tag{2}$$

čija rješenja razmatramo u skupu cijelih brojeva. Ako želimo uspostaviti korespodenciju medju rješenjima jednadžba (1) i (2) prirodno je:
(i) izbaciti trivijalno rješenje $(0, 0, 0)$ koje je rješenje svake homogene jednadžbe.
(ii) poistovjetiti ekvivalentna rješenja, tj. rješenja (a, b, c) i $(ka, kb, kc),\ k \neq 0$ homogene jednadžbe (na primjer, rješenja $(3, 4, 5)$ i $(30, 40, 50)$) jer oni odgovaraju istom rješenju nehomogene jednadžbe.
Slično bismo postupili s jednadžbom

$$x^2 - y^2 = 1 \tag{3}$$

i pripadnom homogenom jednadžbom

$$X^2 - Y^2 = Z^2 \tag{4}$$

samo što bi se tu javila jedna novina: homogena jednadžba ima i klasu cjelobrojnih rješenja za koje je $Z = 0$, to je klasa rješenja ekvivalentnih $(1, -1, 0)$ koja ne dolazi od rješenja nehomogene jednadžbe.
Zaključimo: Svakoj polinomijalnoj jednadžbi $f(x, y) = 0$ s cjelobrojnim koeficijentima može pridružiti homogena polinomijalna jednadžba $F(X, Y, Z)$ s cjelobrojnim koeficijentima. Rješenje homogene jednadžbe je klasa ekvivalentnosti trojaka (a, b, c), različitih od $(0, 0, 0)$, tako da je $F(a, b, c) = 0$ (da bismo naznačili da je riječ o klasi često pišemo $[a, b, c]$). Tako see skup racionalnih rješenja od $f(x, y) = 0$ prirodno ulaže u skup rješenja jednadžbe $F(X, Y, Z) = 0$. Medjutim, to ulaganje općenito nije surjekcija, tj. postoji (najviše konačno) dodatnih rješenja homogene jednadžbe (sa svojstvom $Z = 0$).
Geometrijski aspekt. Ako jednadžbe (1)-(4) ili, općenito, jednadžbu

$$f(x, y) = 0$$

shvatimo geometrijski, onda su njihova rješenja točke na pripadnoj (afinoj, ravninskoj) krivulji, pa se postavlja pitanje kako geometrijski treba interpretirati moguća nova rješenja homogene jednadžbe

$$F(X, Y, Z) = 0.$$

Pri tom ne moramo ostati samo na racionalnim rješenjima već i na realnim, kompleksnim i sl. Odgovor je da ih treba interpretirati u **projektivnoj ravnini** koja je proširenje **afine ravnine** beskonačno dalekim točkama. Ta je konstrukcija nastala neovisno o postavljenom problemu, iz čisto geometrijskih razloga, odnosno problema s perspektivom koju su započeli slikari talijanske renesanse.
U **afinoj ravnini** $\mathbf{A}^2$ dvije točke odredjuju točno jedan pravac (koji njima prolazi), dok dva pravca gotovo uvijek odredjuju jednu točku (njihovo sjecište - postoji ako pravci nisu usporedni). Da bi se otklonila ta nesimetrija, geometri su uveli dodatne (beskonačno daleke) točke kao sjecišta usporednih pravaca, za svaki smjer po točku i dobili projektivnu ravninu $\mathbf{A}^2$. Same beskonačno daleke točke organizirane su u **projektivni pravac** $\mathbf{P}^1$ koji je upotpunjenje afinog pravca $\mathbf{A}^1$ beskonačno dalekom točkom ∞. Dakle, na skupovnoj razini:

$$\mathbf{P}^2 = \mathbf{A}^2 \cup \mathbf{P}^1, \ \mathbf{P}^1 = \mathbf{A}^1 \cup \infty$$

Naime smjerovi u ravnini u korespodenciji su s koeficijentima smjerova, a to su svi realni brojevi i ∞ kao koeficijent smjera y-osi.

Sve ovo vrijedi ako gledamo realne točke, kada pišemo $\mathbf{A}^1(\mathbf{R})$, $\mathbf{P}^1(\mathbf{R})$ $\mathbf{A}^2(\mathbf{R})$, $\mathbf{P}^2(\mathbf{R})$, kompleksne $\mathbf{A}^1(\mathbf{C})$, $\mathbf{P}^1(\mathbf{C})$ $\mathbf{A}^2(\mathbf{C})$, $\mathbf{P}^2(\mathbf{C})$, racionalne $\mathbf{A}^1(\mathbf{Q})$, $\mathbf{P}^1(\mathbf{Q})$ $\mathbf{A}^2(\mathbf{Q})$, $\mathbf{P}^2(\mathbf{Q})$ itd.

Veza homogenih koordinata i projektivnog pravca. Možemo pisati:
$\mathbf{P}^1(\mathbf{R})$ = skup svih smjerova u afinoj ravnini $\mathbf{A}^2(\mathbf{R})$
= skup svih pravaca kroz ishodište u $\mathbf{A}^2(\mathbf{R})$
$= \{Au - Bv = 0 : \ A, B \in \mathbf{R}, \ A \neq 0 \ ili \ B \neq 0\}/\sim$, gdje se $\sim$ odnosi na ekvivalentne jednadžbe
$= \{(A, B) \in \mathbf{R}^2, \ A \neq 0 \ ili \ B \neq 0\}/\sim$.
Vidimo da smo dobili homogene koordinate (samo sad su dvije). Klasa koordinata $[1, 0]$ odgovara beskonačno dalekoj točki pravca (ili koeficijentu smjera ∞, dok afinim točkama odgovara koeficijent smjera $\frac{A}{B}$). Uočite ulaganje afinog pravca u projektivni pravac formulom

$$x \mapsto [x, 1]$$

gdje je x afina koordinata, dok za homogene koordinate X, Z imamo vezu

$$x = \frac{X}{Z}$$

za afine točke (tj. za $Z \neq 0$).
Analogno, projektivna ravnina zadaje se homogenim koordinatama X, Y, Z, gdje je $Z = 0$ jednadžba beskonačno dalekog pravca (to je projektivni pravac i svaki se afini pravac nadopunjuje po jednom točkom beskonačno dalekog pravca i tako se dobije projektivni pravac). U analogiji s tim pravcem imamo ulaganje afine ravnine u homogenu formulom

$$(x, y) \mapsto [x, y, 1]$$

a za afine točke (tj. za $Z \neq 0$) imamo

$$x = \frac{X}{Z}, \ y = \frac{Y}{Z}.$$

Zaključak. "Nova" rješenja iz homogene jednadžbe interpretiraju se kao rješenja u projektivnoj ravnini, tj. rješenja u beskonačnosti (odnosno na beskonačno dalekom pravcu).

Primjer 1. $E_0 : y^2 = x^3 + Ax + B$ tipična je jednadžba afine eliptičke krivulje. Pripadna homogena jednadžba je $E : Y^2Z = X^3 + AXZ^2 + BZ^3$.

Ako želimo odrediti "nove" točke, u tu jednadžbu stavimo $Z = 0$ i dobijemo $X = 0$, a odatle $Y \neq 0$, pa možemo staviti $Y = 1$, tj. $O = [0, 1, 0]$ jedina je beskonačno daleka točka, što pišemo kao $E = E_0 \cup O$. Možemo zamišljati da beskonačno daleki pravac $Z = 0$ siječe krivulju E u jednoj točki (taj pravac je tangenta, a O je trostruka točka - kažemo da je to **točka infleksije** ili **fleks**).

Afini pokrivači projektivnog pravca i ravnine.
Skup zadan jednadžbom $Z \neq 0$ na projektivnom pravcu obični je afini pravac $\mathcal{U}$ s prirodnom koordinatom $x = \frac{X}{Z}$. Slično je sa skupom $\mathcal{V} : X \neq 0$ - i to je afini pravac koji sadrži ∞, a na njemu je prirodna koordinata $t = \frac{Z}{X}$. Uočite da na $\mathcal{U} \cap \mathcal{V}$ vrijedi $t = \frac{1}{x}$. Sjetite se Riemannove sfere kod koje je $\frac{1}{z}$ koordinata "oko ∞". Skupovi $\mathcal{U}, \mathcal{V}$ su najjednostavniji otvoreni afini pokrivač projektivnog pravca u **topologiji Zariskog**. U toj topologiji zatvoreni su: prazni skup, cijeli pravac i konačni skupovi točaka.
Slično, skup zadan jednadžbom $Z \neq 0$ u projektivnoj ravnini, obična je afina ravnina $\mathcal{U}$ s prirodnim koordinatama $x = \frac{X}{Z},\ y = \frac{Y}{Z}$. Slično je sa skupovima $\mathcal{V} : X \neq 0$ i $\mathcal{W} : Y \neq 0$ - i to su afine ravnine, a na njima su prirodne koordinate $r = \frac{Y}{X},\ w = \frac{Z}{X}$, odnosno $u = \frac{X}{Y},\ v = \frac{Z}{Y}$. Uočite da na $\mathcal{U} \cap \mathcal{V}$ vrijedi $r = \frac{y}{x}$ *i* $w = \frac{1}{x}$, dok na $\mathcal{U} \cap \mathcal{W}$ vrijedi $u = \frac{x}{y}$ *i* $v = \frac{1}{y}$. Skupovi $\mathcal{U}, \mathcal{V}, \mathcal{W}$ su najjednostavniji otvoreni afini pokrivač projektivne ravnine u **topologiji Zariskog**. U toj topologiji zatvoreni su: prazni skup, cijeli pravac, konačni skupovi točaka, konačne unije krivulja i njihove konačne unije.

Singularne točke .
Ravninskom krivuljom smatramo skupom (kompleksnih) rješenja u projektivnoj ravnini jednadžbe

$$F(X, Y, Z) = 0$$

gdje je F nerastavljiv (ireducibilan) homogeni polinom različit od 0. Pripadna afina krivulja ima jednadžbu

$$f(x, y) = 0$$

gdje je $f(x, y) := F(x, y, 1)$. Naravno da ima i drugih izbora za afinu jednadžbu, na primjer $g(u, v) = 0$, gdje je $g(u, v) := F(u, 1, v)$. Projektivna krivulja može imati najviše *novih* točaka koliki je stupanj polinoma F.
Intuitivno, točka na krivulji je **nesingularna** ako je u njoj jednoznačno definirana tangenta, inače je **singularna**. Za afinu krivulju, to znači:
Točka $P = (a, b)$ na $C_0 : f(x, y) = 0$ je nesingularna ako je $\frac{\partial f}{\partial x}(a, b) \neq 0$ ili

$\frac{\partial f}{\partial y}(a,b) \neq 0$. Tada je jednadžba tangente

$$\frac{\partial f}{\partial x}(a,b)(x-a) + \frac{\partial f}{\partial y}(a,b)(y-b) = 0 \tag{5}$$

Drugim riječima, ako f rastavimo u Taylorov red oko (a,b) kao

$$f = f_0 + f_1 + ... + f_d,$$

gdje je f_i homogeni dio i-tog stupnja po $x-a$ i $y-b$, onda je:
(i) $P(a,b)$ je na krivulji akko $f_0 = 0$,
(ii) $P(a,b)$ je nesingularna akko $f_0 = 0$ i $f_1 \neq 0$. Uočite da je, općenito, $f_1 =$ lijeva strana od (5), tj. jednadžba tangente je $f_1 = 0$.

Primjer 2. (i) Točka $(0,0)$ singularna je točka krivulje $C_0 : y^2 = x^3 - x^2$. To se vidi izravno iz funkcije $f(x,y) := y^2 + x^2 - x^3$ što je razvoj oko $(0,0)$ pa vidimo da je linearni dio jednak nuli, ali i iz $\frac{\partial f}{\partial x}(0,0) = \frac{\partial f}{\partial y}(0,0) = 0$.
(ii) Točka $O = [0,1,0]$ na krivulji $E : Y^2Z = X^3 + AXZ^2 + BZ^3$ je nesingularna. Da to dokažemo, afinu jednadžbu gledamo u ravnini $Y \neq 0$:

$$v = u^3 + Auv^2 + Bv^3, \ tj. \ v - u^3 - Auv^2 - Bv^3 = 0$$

gdje je $u = \frac{X}{Y}, \ v = \frac{Z}{Y}$, a O postaje $(0,0)$. Vidimo da je linearni dio u rastavu po u, v različit od 0, točnije, jednak je v pa je $v = 0$ jednadžba tangente, što bismo dobilio i parcijalnim integriranjem (formula (5)). Ako želimo jednadžbu tangente u projektivnim (homogenim) koordinatama, pišemo $\frac{Z}{Y} = 0$, tj. $Z = 0$ (beskonačno daleki pravac - što je i logično).

Umjesto (5) možemo se služiti formulom za jednadžbu tangente u homogenim koordinatama. Točka P krivulje $F(X,Y,Z) = 0$ je nesingularna akko $\frac{\partial F}{\partial X}(P) \neq 0$ ili $\frac{\partial F}{\partial Y}(P) \neq 0$ ili $\frac{\partial F}{\partial Z}(P) \neq 0$. Ako je tako, jednadžba tangente je

$$X\frac{\partial F}{\partial X}(P) + Y\frac{\partial F}{\partial Y}(P) + Z\frac{\partial F}{\partial Z}(P) = 0 \tag{6}$$

Kažemo da je krivulja nesingularna ako su joj sve točke nesingularne. Krivulja može imati najviše konačno singularnih točaka (objasnite).

Afine i projektivne zamjene koordinata.

Dvije ravninske krivulje $F(X,Y,Z) = 0$ i $G(X,Y,Z) = 0$ jednake su kao skupovi ako i samo ako su F i G proporcionalni polinomi (slično je za afine

jednadžbe $f(x,y)=0$ i $g(x,y)=0$). Postoje medjusobno različite krivulje koje "nisu bitno različite", pa ih smatramo ekvivalentnim. Najjednostavniji primjeri ekvivalentnih krivulja jesu onih dobivenih linearnom zamjenom koordinata.

Afina zamjena koordinata - afina transformacija ravnine. To je zamjena:

$$x = ax' + by' + r,\ y = cx' + dy' + s$$

gdje su a, b, c, d, r, s koeficijenti, a da bi inverzna transformacija postojala determinanta matrice

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

treba biti različita od nule.

Takva transformacija prebacuje krivulju $f(x,y)=0$ u njoj **afino ekvivalentnu** $g(x',y')=0$. Pri tom se zadržava stupanj, nesingularnost, tangente itd.

Afinu transformaciju možemo shvatiti i kao transformaciju afine ravnine zadane formulom

$$(x,y) \mapsto (x',y').$$

Primjer 3. Afina transformacija $x = x' + y',\ y = x' - y'$ krivulju $xy = 1$ prebacuje u krivulju $x'^2 - y'^2 = 1$. Takjodjer, tu transformaciju možemo interpretirati kao preslikavanje afine ravnine zadane formulom

$$(x,y) \mapsto (x',y'),\ tj.\ (x,y) \mapsto (\frac{x+y}{2}, \frac{x-y}{2}).$$

Pri tom preslikavanju krivulja $xy = 1$ prelazi u krivulju $x^2 - y^2 = 1$ (tu nema crtica).

Afinoj zamjeni koordinata (transformaciji ravnine) pridružena je projektivna:

$$X = aX' + bY' + rZ',\ Y = cX' + dY' + sZ',\ Z = Z'$$

To nisu sve projektivne transformacije ravnine (već samo one koje čuvaju standardnu afinu ravninu, tj. standardni beskonačno daleki pravac). Općenito, projektivna transformacija ravnine je oblika

$$X = aX' + bY' + rZ',\ Y = cX' + dY' + sZ',\ Z = mX' + nY' + kZ'.$$

Uvod u aritmetiku eliptičkih krivulja

Grupni zakon na eliptičkoj krivulji - 5. lekcija

Kubične krivulje (kubike). To su krivulje zadane jednadžbom oblika

$$F(X, Y, Z) = 0$$

gdje je F homogeni polinom trećeg stupnja (kubična forma). Napominjemo da rješenja gledamo u projektivnoj ravnini (prvenstveno s kompleksnim koordinatama, ali i iz bilo kojega algebarski zatvorenog polja), tj. izbacujemo trivijalno rješenje $(0, 0, 0)$, a netrivijalna proporcionalna rješenja poistovjećujemo. Pripadna afina krivulja zadana je afinom jednadžbom $f(x, y) = 0$.

Primjer 1. Evo nekoliko projektivnih kubika i njihovih pridruženih afinih:
(i) $X^3 + Y^3 - \alpha Z^3 = 0,\ (i)'\ x^3 + y^3 - \alpha = 0$
(ii) $X^3 - X^2Z - Y^2Z = 0,\ (ii)'\ x^3 - x^2 - y^2 = 0,\ tj.\ y^2 = x^3 - x^2$
(iii) $X^3 + AXZ^2 + BZ^3 - Y^2Z = 0,\ (iii)'\ x^3 + Ax + B - y^2 = 0,\ tj.\ y^2 = x^3 + Ax + B$.

Skupovna razlika izmedju projektivne i afine krivulje najviše je u 3 točke. Postoji jednostavna korespodencija izmedju svojstava forme F (odnosno polinoma f) i geometrije pripadne krivulje C:
(I) $F = L^3$, za linearnu formu L —- C je trostruki pravac.
(II) $F = L_1^2 L_2$ —- C je unija dvostrukog pravca i pravca.
(III) $F = L_1 L_2 L_3$ —- C je unija triju pravaca.
(IV) $F = KL$, gdje je K kvadratna forma —- C je unija konike i pravca.
To su bili slučajevi **reducibilnih** krivulja, u nastavku su **ireducibilne**.
(V) F je ireducibilan polinom, ali pripadna krivulja $C : F(X, Y, Z) = 0$ ima singularnu točku. Vidjet ćemo da se taj slučaj svodi na konike; tu je genus (rod) jednak 0.
(VI) F je ireducibilan polinom, a C je nesingularna. U nastavku će nas u pravilu zanimati samo takve krivulje. Tu je genus jednak 1, a pripadne krivulje eliptičke (nakon izbora jedne točke).

Geometrija i aritmetika. Kažemo da je kubika $C : F(X, Y, Z) = 0$ definirana nad $\mathbf{Q}$ (ili nad nekim drugim poljem) ako postoji $\lambda \neq 0$, tako da

svi koeficijenti od λF budu iz $\mathbf{Q}$, a onda je moguće i da budu iz $\mathbf{Z}$ (ili tog drugog polja). Ako je C definirana nad $\mathbf{Q}$, onda je pripadni aritmetički (diofantski) problem, problem odredjivanja $\mathbf{Q}$-racionalnih točaka, tj. rješenja jednadžbe $F(X,Y,Z) = 0$ za koje postoji reprezentant (a,b,c) gdje su svi a,b,c racionalni brojevi (a onda je moguće i da budu cijeli). Za pripadnu afinu krivulju $C_0 : f(x,y) = 0$ s cjelobrojnim koeficijentima ima smisla i problem odredjivanja cjelobrojnih točaka.

Primjer 2. Kubika $Y^2Z = X^3 + 17Z^3$ definirana je nad $\mathbf{Q}$. Lako se vidi da je nesingularna. Točka O u beskonačnosti očito je definirana nad $\mathbf{Q}$, jer je $O = [0,1,0]$. Kako su ostale točke afine, gledamo jednadžbu $y^2 = x^3 + 17$. Vidimo da su $(-1, \pm 4)$ i $(2, \pm 5)$ definirane nad $\mathbf{Q}$ (ujedno i nad $\mathbf{Z}$). Pokušajte odgovoriti na pitanja:
(1.) Je su li ove četiri točke jedine cjelobrojne?
(2.) Postoji li neka druga $\mathbf{Q}$-racionalna točka različite od ovih 5 navedenih?

Zašto singularna točka pojednostavljuje krivulju? Neka je $C : F(X,Y,Z) = 0$ ireducibilna kubika i neka je P neka njena točka. Nakon jednostavne projektivne zamjene koordinata, možemo smatrati da je to točka $[0,0,1]$ (objasnite). Zato možemo preći na afinu jednadžbu $f(x,y) = 0$ i njenu točku $P(0,0)$. Razvoj $f = f_3 + f_2 + f_1 + f_0$ oko P ima $f_0 = 0$ (jer krivulja prolazi ishodištem). Zato možemo pisati:

$$f(x,y) = (a_0x^3 + a_1x^2y + a_2xy^2 + a_3y^3) + (b_0x^2 + b_1xy + b_2y^2) + (c_0x + c_1y).$$

Stavimo zamjenu $y = tx$ i dobit ćemo jednadžbu:

$$x^3g_3(t) + x^2g_2(t) + xg_1(t) = 0$$

Ako je $P(0,0)$ singularna, onda je $g_1 = 0$, pa nakon dijeljenja s x^2 dobijemo $xg_3(t) + g_2(t) = 0$, odakle dobijemo parametrizaciju

$$x = -\frac{g_2(t)}{g_3(t)},\ y = -\frac{g_2(t)}{g_3(t)} \cdot t$$

što izravno pokazuje da je krivulja C racionalna (ima genus 1).

Ireducibilne nesingularne kubike - grupni zakon. Na svaku takvu krivulju C možemo uvesti tzv. grupni "sekantno-tangentni" zakon koji se

zasniva na:
(I) Činjenici da svaki pravac siječe kubiku u tri točke (ako pravilno brojimo kratnosti). Preciznije, pravac općenito ciječe C u trima različitim točkama. Iznimno, ako je pravac tangenta u nekoj točki krivulje, tu brojimo dvostruko, a pravac siječe C u još jednoj točki. Konačno, može se dogoditi da tangenta ne siječe krivulju ni u jednoj drugoj točki. Tada tu točku brojimo trostruko, zovemo je infleksijskom točkom (fleksom). Pokazuje se da svaka kubika ima točno 9 fleksova. Primjer fleksa je beskonačno daleka točka $O[0,1,0]$ na kubici $C : X^3 + AXZ^2 + BZ^3 - Y^2Z = 0$, gdje tangenta $Z = 0$ u toj točki dira krivulju trostruko.
(II) Činjenici (jedinstvena tangenta - nesingularnost) da pri fiksiranoj točki krivulje, svi pravci koji njome prolaze sijeku krivulju u dvjema novim točkama (ili u dvostrukoj točki), a samo je jedan tangenta.
Za grupni zakon najprije biramo po volji točku O krivulje. Time će zakon biti jednoznačno odredjen.
Sad zbroj $P \oplus Q$ točaka P, Q definiramo ovako (za slike pogledajte [Silverman-Tate, str. 16-21]):
1. korak. Neka je R treća točka presjeka pravca kroz P i Q s krivuljom. Tu točku označavat ćemo kao $P * Q$.
2. korak. $P \oplus Q$ definiramo kao treću točku presjeka pravca kroz R i O s krivuljom.
Tom načelnom zakonu treba dodati sljedeće posebne slučajeve:
(i) ako je $P = Q$, onda $P \oplus Q$ postaje $P \oplus P = 2P$ tako da u 1. koraku povlačimo tangentu u P; iznimno, ako je P fleks, definiramo $P * P = P$ (treća točka presjeka opet je P).
(ii) ako bude $P * Q = O$, onda u 2. koraku povlačimo tangentu kroz O.
Sad je lako pokazati sljedeće:
(G_0) $(P, Q) \mapsto P \oplus Q$ dobro je definirano.
(G_1) $\oplus$ je komutativna operacija.
(G_2) O je neutralni element: $P \oplus O = P$.
(G_3) Za svaki P jednoznačno je definiran suprotni element ovako: neka je S treća točka presjeka tangente u O s krivuljom; $-P$ je treća točka presjeka pravca kroz P i S s krivuljom. Iznimno, ako je O fleks, onda je $S = O$ pa su P, O i $-P$ na istom pravcu.
Jedino je netrivijalan zakon asocijativnosti
(G_4) $P \oplus (Q \oplus R) = (P \oplus Q) \oplus R$ za sve P, Q, R,
i izgleda da se ne može elementarno geometrijski dokazati.
Lagani dio zakona asocijativnosti. Zakon asocijativnosti očit je u poseb-

nim slučajevima:

$$P \oplus (Q \oplus R) = (P \oplus Q) \oplus R \text{ ako je } P, Q, \text{ ili } R \text{ jednako } O \tag{1}$$

$$-P \oplus (P \oplus R) = R = (-P \oplus P) \oplus R \tag{2}$$

Radi jednostavnosti, (2) ćemo obrazložiti ako je O fleks. Uočimo sljedeće: Ako je $P \oplus R = T$ onda su P, R i $-T$ na istom pravcu. Zato su $-P, -R$ i $-(-T) = T$ na istom pravcu, pa je $-P \oplus T = -(-R) = R$. Dakle, $-P \oplus (P \oplus R) = R$.
Tipičan geometrijski dokaz zakona asocijativnosti je pomoću tzv. "teorema o devet točaka", koji se izvodi iz Bezout-ova teorema, a za koji je potrebno razviti teoriju presjeka ravninskih krivulja (vidi [Silverman-Tate, Appendix]). Taj dokaz je revizija dobrog dijela klasične projektivne geometrije u ravnini 17. i 18. stoljeća. Moderniji dokaz koristi se teorijom divizora na algebarskim krivuljama i teoremom Riemanna-Rocha (vidi [Silverman, III, Prop.3.4.]). Mi ćemo dati jedan drugi dokaz nakon uvodjenja Weierstrassova modela.

Weierstrassov model.
Neka je $C : F(X, Y, Z) = 0$ ireducibilna nesingularna kubika s istaknutom točkom O. Tada se pokazuje:
(I) Ako je O fleks onda se C projektivnim transformacijama ravnine može dovesti u oblik

$$E : Y^2Z = X^3 + AXZ^2 + BZ^3, \text{ uz } 4A^3 + 27B^2 \neq 0 \tag{3}$$

Pri tom flex O prelazi u beskonačno daleku točku $O[0, 1, 0]$.
Pripadna afina jednadžba je

$$E_0 : y^2 = x^3 + Ax + B \tag{4}$$

(II) Ako O nije fleks, opet se C dovodi u oblik (3) samo što nisu dovoljne projektivne transformacije, već tzv. "biracionalne transformacije" (kvocijenti polinoma).
(3) se naziva Weierstrassova jednadžba eliptičke krivulje (ili Weierstrassov model) i postoji u svakoj karakteristici različitoj od 2 i 3; uvjet $4A^3+27B^2 \neq 0$ je uvjet nesingularnosti (to znači da se i ostale ireducibilne kubike svode na ovaj oblik, ali su nesingularne akko zadovoljavaju taj uvjet).

(I) ćemo ilustrirati primjerom.

Primjer 3. **[Silverman-Tate, str. 24]** Neka je $C : X^3 + Y^3 - \alpha Z^3 = 0$. Uz (projektivnu) zamjenu koordinata

$$X = W + V,\ Y = W - V,\ Z = U$$

dobijemo jednadžbu

$$4V^2W = \frac{\alpha}{6}U^3 + \frac{1}{3}W^3$$

ili, nakon dijeljenja s W^3, afinu jednadžbu

$$v^2 = \frac{\alpha}{6}u^3 - \frac{1}{3}.$$

Sad, množenjem s $6^4\alpha^2$ (za $\alpha \neq 0$) dobijemo $(6^2\alpha v)^2 = (6\alpha)^3 - 432\alpha^2$, odnosno afinu jednadžbu eliptičke krivulje

$$y^2 = x^3 - 432\alpha^2.$$

Pripadna homogena jednadžba je:

$$E : Y^2Z = X^3 - 432\alpha^2Z^3.$$

Krivulje C i E su projektivno ekvivalentne (izomorfne). Pri tom je flex $[-1, 1, 0]$ na C prešao u flex $[0, 1, 0]$ na E.
Uočite da je za $\alpha = 0$ početna krivulja reducibilna, a ova završna je ireducibilna. To se dogodilo zbog množenja nulom; lako je vidjeti da je C tada ekvivalentna krivulji, $C' : V^2W = \frac{1}{3}W^3$ (takodjer reducibilnoj).

Napomena. Lako je vidjeti da je E iz (3) nesingularna akko je polinom $f(x) := x^3 + Ax + B$ iz (4) bez višestrukih nultočaka. Naime, već znamo da je $O[0, 1, 0]$ nesingularna pa treba gledati samo afine točke. Dalje, za polinom $g(x, y) := y^2 - f(x)$ vrijedi: sustav $\frac{\partial g}{\partial x} = \frac{\partial g}{\partial y} = 0$ akko sustav $f(x) = f'(x) = 0$ ima rješenje, a to je akko f ima višestruku nultočku.

Zadatak. Dokažite da je uvjet nesingularnosti krivulje E (iz (3)), odnosno E_0 (iz (4)) upravo $4A^3 + 27B^2 \neq 0$.

Aritmetički slučaj.
Ako je $C : F(X, Y, Z) = 0$ definirana nad $\mathbf{Q}$, onda imamo dva slučaja:
1. slučaj. Postoji bar jedna $\mathbf{Q}$ racionalna točka na C. Tada C ima Weierstrassov model i riječ je o **eliptičkoj krivulji nad Q**. Postoje dva slučaja

tehnički različita:
(i) ako je bar jedan od fleksova O definiran nad $\mathbf{Q}$, onda se do Weiersstrasova modela nad $\mathbf{Q}$ dolazi projektivnim transformacijama ravnine s koeficijentima iz $\mathbf{Q}$ i pri tom se može izabrati da taj flex prelazi u beskonačno daleku W. modela $[0, 1, 0]$ (tako je bilo u primjeru 3. uz racionalan $\alpha \neq 0$).
(ii) ako ni jedan od fleksova nije definiran nad $\mathbf{Q}$, onda se do W. modela dolazi biracionalnim transformacijama ravnine s koeficijentima iz $\mathbf{Q}$.
(II) C nema ni jednu $\mathbf{Q}$-racionalnu točku. Tada C nema Weierstrassov model nad $\mathbf{Q}$, i nije eliptička krivulja nad $\mathbf{Q}$ (već samo nad $\mathbf{C}$, odnosno nad nekim algebarskim proširenjem od $\mathbf{Q}$), iako je C krivulja genusa 1 nad $\mathbf{Q}$.

Primjer 4. (Selmer) Neka je $C : 3X^3 + 4Y^3 + 5Z^3 = 0$. Tada C nema $\mathbf{Q}$-racionalnu točku i nije eliptička krivulja nad $\mathbf{Q}$ (već samo nad nekim proširenjem nad kojim ima $\mathbf{Q}$-racionalnu točku, pa i W. model, na primjer nad $\mathbf{Q}(\sqrt[3]{6})$).

Uvod u aritmetiku eliptičkih krivulja

Grupni zakon na eliptičkoj krivulji II - 6. lekcija

Analitički zapis grupnog zakona.
Od sad nadalje, ako drukčije ne kažemo, eliptička krivulja E je zadana afinom Weierstrassovom jednadžbom

$$y^2 = x^3 + ax^2 + bx + c$$

gdje je $f(x) := x^3 + ax^2 + bx + c = (x - e_1)(x - e_2)(x - e_3)$ kubni polinom s različitim korijenima (ili, u skraćenom obliku $y^2 = x^3 + Ax + B$). U oba slučaja $O = [0, 1, 0]$ je jedina točka u beskonačnosti i nju smatramo istaknutom. Zato pod grupnim zakonom mislimo na onaj u kojemu je O neutralni element. Napominjemo da se u O sijeku afini pravci usporedni s y-osi. Naime, pravac

$$\alpha X + \beta Y + \gamma Z = 0$$

sadrži O ako i samo ako je $\beta = 0$, pa to može biti beskonačno daleki pravac $Z = 0$ ili pravci $X = -\frac{\gamma}{\alpha}Z$, tj. $x = -\frac{\gamma}{\alpha}$.
Zato za grupni zakon vrijedi:
(I) Ako je $P(x, y)$ afina točka, onda je $-P(x, -y)$ suprotna točka.
(I) Ako su P, Q afine točke onda se $P \oplus Q$ dobije kao točka presjeka krivulje i usporednice s y-osi kroz $P * Q$. Rezultat je afina točka, osim ako je $Q = -P$, posebno ako je $P = Q = (e_i, 0)$ za neki $i = 1, 2, 3$.
Uočite, takodjer, da su točke $O, (e_1, 0), (e_2, 0), (e_3, 0)$ rješenja jednadžbe $2P = 0$.

Teorem 1. (i) Neka su $P(x_1, y_1), Q(x_2, y_2)$ afine točke i $Q \neq -P$. Tada je i $(P \oplus Q)(x_3, y_3)$ afina i vrijedi:

$$x_3 = -x_1 - x_2 + \lambda^2 - a, \;\; y_3 = \lambda(x_1 - x_3) - y_1$$

gdje je $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ ako je $P \neq Q$, i $\lambda = \frac{f'(x_1)}{2y_1}$ ako je $P = Q$.
(ii) Ako je krivulja E definirana nad $\mathbf{Q}$ i ako su P, Q definirane nad $\mathbf{Q}$, onda je i $P \oplus Q$ definirana nad $\mathbf{Q}$, odnosno $2P$ je definirana nad $\mathbf{Q}$..
Dokaz. (i) Riješimo sustav jednadžba

$$y^2 = x^3 + ax^2 + bx + c, \;\; y = \lambda x + \nu$$

gdje je druga jednadžba jednadžba pravca kroz P, Q. Kako taj pravac siječe krivulju u točkama s prvim koordinatama x_1, x_2, x_3, nakon eliminiranja varijable y iz Vieteovih formula dobijemo

$$x_1 + x_2 + x_3 = \lambda^2 - a$$

, sto smo i trebali. Sad samo treba primijeniti činjenicu da za $P \neq Q$ vrijedi $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$, a ako je $P = Q$, pravac je tangenta u (x_1, y_1) pa je $\lambda = \frac{f'(x_1)}{2y_1}$.
(ii) vidi se iz formula.

Napomena Ako označimo koordinate afine točke T kao $x(T), y(T)$ onda je

$$x(2P) = \frac{1}{4} \frac{x^4 - 2bx^2 - 8cx + (b^2 - 4ac}{x^3 + ax^2 + bx + c}$$

To se dobije izravnim računanjem.

Važnost grupnog zakona na eliptičkoj krivulji prvenstveno je u tomu što se iz dviju točaka može dobiti nova točka, odnosno iz zadane točke nova (dvostruka) točka. To je, na neki način, u dalekoj prošlosti otkrio i primijenio Diofant.
Primjer 1. Neka je E zadana afinom jednadžbom $y^2 = x^3 + 17$. Očite točke su $P(-1, 4)$ i $Q(2, 5)$. Neka je $(P \oplus Q)(x_3, y_3)$. Tada je, prema teoremu 1 $(x_3, y_3) = (-\frac{8}{9}, \frac{109}{27}$. Takodjer je $2P(\frac{137}{64}, -\frac{2651}{51})$. Postavlja se pitanje možemo li pomoću P, Q povlačenjem sekanata i tangenata dobiti svaku točku krivulje E se racionalnim koordinatama (**Q**-racionalne točke).

Dokaz zakona asocijativnosti.
Definicija 1. Neka su C_1, C_2 dvije (ne nužno ravninske) algebarske krivulje. Kažemo da je $\phi : C_1 \to C_2$ racionalno preslikavanje, ako se lokalno može zadati racionalnim funkcijama. Kažemo da je ϕ morfizam ako definirana na cijelom C_1 (ili ako se može proširiti).

Primjer 2. Ako je E eliptička krivulja onda je $\phi : E \to E$, $\phi(P) = 2P$ racionalno preslikavanje. Naime, na afinom dijelu je ϕ, ako je $2P \neq O$, prema teoremu 1, zadano kao $\phi(x, y) = (\phi_1(x, y), \phi_2(x, y)$ gdje su ϕ_1, ϕ_2 racionalne funkcije od x, y, tj. one su racionalne funkcije na E.

Za dokaz asocijativnosti potrebna nam je standardna (iako ne elementarna) lema o preslikavanjima algebarskih krivulja.

Lema 1. Neka su C_1, C_2 nesingularne projektivne krivulje. Tada:
(i) Svako racionalno preslikavanje $\phi : C_1 \to C_2$ proširuje se do morfizma.
(ii) Morfizam ϕ je konstanta ili surjekcija.
(iii) Ako je ψ drugi morfizam i $\psi \neq \phi$, onda je skup svih P tako da je $\phi(P) = \psi(P)$ konačan.
Ovu lemu nećemo dokazivati.

Prije dokaza napominjemo opet već poznatu činjenicu da je asocijativnost

$$P \oplus (Q \oplus R) = (P \oplus Q) \oplus R$$

evidentna ako je neka od točaka fleks O ili u posebnom slučaju

$$-P \oplus (P \oplus R) = R = (-P \oplus P) \oplus R, \tag{1}$$

odakle, kao poseban slučaj vidimo da je $P \oplus (-Q) = O$ akko $P = Q$.

Dokaz asocijativnosti. Iz (1) slijedi da možemo predpostaviti da je $Q, R \neq O$ i $Q \oplus R \neq O$. Definirajmo (za sad skupovno) preslikavanje

$$h : E \to E,\ h(P) := [P \oplus (Q \oplus R)] \oplus [-(P \oplus Q) \oplus R] \tag{2}$$

Iz (1) izlazi da je dovoljno dokazati da je $h(P) = O$ za sve P. Očito je $h(O) = O$. Takodjer, h ne postiže $-R$. Naime iz jednakosti $h(P) = -R$ i (1) slijedi

$$P \oplus (Q \oplus R) = ((P \oplus Q) \oplus R) \oplus (-R) = P \oplus Q$$

a odavde, $Q \oplus R = Q$, tj. $R = O$, što je kontradikcija.
Iz Leme (i) i (ii), vidi se da je za dokazivanje zakona, dovoljno dokazati da je h racionalno preslikavanje. Prvo uočite da je $\phi : E \to E$ definirano kao $P \mapsto P \oplus (Q \oplus R)$ morfizam algebarskih krivulja. Naime, iz (4)-(5), ϕ je racionalno preslikavanje regularno za $P \neq O, \pm(Q \oplus R)$, pa je po Lemi (i), ϕ definirano na cijelom E. Slično, preslikavanje $\psi : E \to E$ definirano kao $P \mapsto (P \oplus Q) \oplus R$ je morfizam algebarskih krivulja.
Sad, ako je $\phi = \psi$ sve je u redu.
Ako je pak $\phi = -\psi$, onda je, prema (6)-(7) h racionalno preslikavanje .
Predpostavimo konačno da je $\phi \neq \psi$ i $\phi \neq -\psi$. Onda iz Leme (iii) slijedi da je $\phi(P) \neq \pm\psi(P)$ za gotovo sve P. Sad iz (4)-(5) vidimo da je h racionalno preslikavanje.

Uvod u aritmetiku eliptičkih krivulja

Izomorfizmi, automorfizmi, izogenije - 7.lekcija

Izomorfni Weierstrassovi modeli - jednadžbe.

Neka su eliptičke krivulje $(E_1, O_1), (E_2, O_2)$ zadane Weierstrassovim jednadžbama (ako ih zadamo u istoj projektivnoj ravnini onda je $O_1 = O_2 = O = [0, 1, 0]$). Projektivne transformacije ravnine koje fiksiraju O, ujedno preslikavaju afine dijelove u afine, pa možemo razmatrati samo afine transformacije. Načelno bi se moglo dogoditi da jedna Weierstrassova jednadžba prelazi u drugu i transformacijama koje nisu afine. Pokazat ćemo da to nije moguće, tj. da su dva Weierstrassova modela izomorfna ako i samo ako su afino izomorfna.
Neka su, radi jednostavnosti, eliptičke krivulje zadane afinim jednadžbama:

$$E_1 : y^2 = x^3 + Ax + B,\ E_2 : y'^2 = x'^3 + A'x' + B'$$

i neka je

$$\phi : E_1 \to E_2$$

izomorfizam algebarskih krivulja (grupni zakon privremeno zaboravljamo) koji neutralni element preslikava u neutralni, tj. $\phi(O) = O$. Tada je, za $P(x, y) \in E_1$:

$$\phi(x, y) = (\phi_1(x, y), \phi_2(x, y)) \in E_2$$

gdje su ϕ_1, ϕ_2 racionalne funkcije na E_1. Kako je ϕ izomorfizam afinih dijelova, te su funkcije regularne (svugdje definirane), pa su, prema definiciji, restrikcije polinoma dviju varijabla (na E_1). Zbog izomorfizma, postoje inverzno preslikavanje, tj.

$$\psi : E_2 \to E_1;\ \psi = (\psi_1, \psi_2)$$

gdje su ψ_1, ψ_2 restrikcije polinoma dviju varijabla (na E_2), tako da bude:

$$\psi_1(\phi_1(x, y), \phi_2(x, y)) = x \text{ i } \psi_2(\phi_1(x, y), \phi_2(x, y)) = y \tag{1}$$

što treba shvatiti kao jednakost regularnih funkcija na E_1. Osnovna poteškoća kod razmatranja ovakvih identiteta jest u tome što prsten restrikcija polinoma na afinu eliptičku krivulju E_1 nema jednoznačnu faktorizaciju, a i

inače, zapisi tih funkcija nisu jednoznačni (za razliku od jednozačnog zapisa polinoma dviju varijabla i jednoznačne faktorizacije). Uočite da svaku regularnu funkciju r na afinom dijelu od E_1 možemo jednoznačno zapisati kao $r(x,y) = r_1(x) + r_2(x)y$, gdje su r_1, r_2 polinomi i $y^2 = x^3 + Ax + B$, što dobijemo tako da y^2 sustavno zamijenimo s $x^3 + Ax + B$ itd. (slično je za regularne funkcije na afinom dijelu od E_2). Zato zapišimo:
$\phi_1(x,y) = f_1(x) + f_2(x)y;\ \phi_2(x,y) = g_1(x) + g_2(x)y,$
$\psi_1(x',y') = h_1(x') + h_2(x')y',\ \psi_2(x',y') = k_1(x') + k_2(x')y'$
gdje su $f_1, f_2, g_1, g_2, h_1, h_2, k_1, k_2$ polinomi jedne varijable (i $y'^2 = x'^3 + A'x' + B'$). Sad (1), uz ispuštanje varijable x u zapisu postaje

$$h_1(f_1 + f_2 \cdot y) + h_2(f_1 + f_2 y) \cdot (g_1 + g_2 \cdot y) = x \tag{2}$$

i

$$k_1(f_1 + f_2 \cdot y) + k_2(f_1 + f_2 y) \cdot (g_1 + g_2 \cdot y) = y. \tag{3}$$

Iako nam intuicija govori da tu mora biti da su:
f_1 i h_1 linearni, $f_2 = h_2 = g_1 = k_1 = 0$, g_2, k_2 ne-nul konstante (*),
ipak to nije tako lako izravno dokazati. Prigodna metoda za to je usporedjivanje valuacija v_O u beskonačno dalekoj točki, tj. razmatranje razvoja u beskonačni red po lokalnoj varijabli u toj točki. Ako bismo imali osnovna znanja o prstenima diskretne valuacije pridruženim nesingularnim točkama algebarske krivulje, lako bismo zaključili da je da je $v_O(x) = -2$ i $v_O(y) = -3$. Mi ćemo to sad izvesti izravno.

Valuacija u beskonačno dalekoj točki.
Jednadžbu $y^2 = x^3 + Ax + B$, kako smo već vidjeli, zamjenom $y = \frac{1}{v},\ x = \frac{u}{v}$ (što su koordinate oko O), postaje

$$v = u^3 + Auv^2 + Bv^3 \tag{4}$$

a O u (u,v) koordinatama postaje $(0,0)$. Gornju bismo jednadžbu mogli predočiti kao

$$v = \frac{u^3}{1 - Auv - Bv^2}$$

što u terminima lokalnih prstena znači da je u lokalni parametar u O, v je treća potencija od u pomnožena invertibilnom funkcijom u tom prstenu (naime $(1 - Auv - Bv^2)(0,0) = 1 \neq 0$); sve skupa znači da u ima valuaciju 1, a v valuaciju 3, što znači da $y = \frac{1}{v}$ ima valuaciju -3, a $x = \frac{u}{v}$ valuaciju $1 - 3 = -2$. Ako želimo izbjeći takvo razmatranje, primijenimo teorem o implicitnoj funkciji, prema kojemu je, oko točke $(0,0)$ jednadžbom (4) zadana

funkcija v u ovisnosti o u (tj. $v = v(u)$, tako da je $v(0) = 0$, a Taylorov razvoj te funkcije počinje s u^3. Naime, iz (4) dobijemo (u nastavku se crtice odnose na derivacije po u):
$v' = 3u^2 + Av^2 + 2Auvv' + 3Bv^2v'$, odakle je $v'(0) = 0$. Slično se dobije:
$v'' = 6u + 2Avv' + 2Avv' + 2Auv'^2 + 2Auvv'' + 6Bvv'^2 + 3Bv^2v''$, odakle je $v''(0) = 0$. Derivirajući još jednom dobijemo $v'''(0) = 6$. Zato je
$v(u) = u^3+$ članovi višeg reda
(kako smo već ranije najavili). Sad definiramo $v_O(u) = 1$, pa je $v_0(v) = 3$, odakle je $v_O(x) = -2,\ v_O(y) = -3$ itd.
U nastavku demonstriramo snagu razmatranja valuacije u beskonačnosti. Prije dokaza od $*$, ilustrirajmo kako bi dokaz izgledao na jednom višem jeziku, kojeg, nažalost, nismo razvili. Pridruživanje $x' \mapsto \phi_1(x, y);\ y' \mapsto \phi_2(x, y)$ je izomorfizam polja racionalnih funkcija na E_2 i E_1. Pri tom izomorfizmu lokalni prsteni koji odgovaraju točkama u beskonačnosti prelaze jedan u drugi. Zato mora biti $v_O(\phi_1) = -2,\ v_O(\phi_2) = -3$, odakle lako dobijemo $\phi_1(x, y) = ax + b\ phi_2(x, y) = ex + cy + d$ itd.

Izravan dokaz relacija (*)

Pri ovom dokazu, temeljni argument je da za racionalne funkcije r_1, r_2 na E_1 (odnosno E_2) očito vrijedi $v_O(r_1 + r_2) = \min\{v_O(r_1), v_O(r_2)\}$ uz uvjet da je $v_O(r_1) \neq v_O(r_2)$ (u stvari to nam je dovoljno za regularne funkcije na afinom dijelu od E_1). Kako (ϕ_1, ϕ_2) zadovoljava jednadžbu od E_2, vrijedi:

$$(g_1 + g_2 \cdot y)^2 = (f_1 + f_2 \cdot y)^3 + A'(f_1 + f_2 \cdot y) + B'. \tag{5}$$

Svaki od f_1, f_2, g_1, g_2 je ili 0 ili ima stupanj $d_1, d_2, \delta_1, \delta_2$ pa je valuacija u O lijeve strane parna (vidimo čak da je jednaka $-4\delta_1$ ili $-4\delta_2 - 6$), pa mora takva biti i na desnoj. Na desnoj strani treba gledati samo kubni dio, pa je tamo valuacija jednaka $-6d_1$ ili $-6d_2 - 9$, dakle ono prvo. To posebno za sobom povlači da je $f_1 \neq 0$ i da je valuacija od f_1 manja od valuacije od $f_2 \cdot y$. Takodjer, analogno, zbog simetrije, vrijedi za h_1 i $h_2 \cdot y$.
Sad, ako je $h_2 = 0$, onda iz (2) slijedi da je $f_2 = 0$, h_1, f_1 linearni, a onda iz (3) proizlazi da su k_2, g_2 ne-nul konstante i da je $k_1 = g_1 = 0$.
Pokažimo da predpostavka $h_2 \neq 0$ vodi u kontradikciju. Prvo, iz (2) slijedi da je valuacija od $g_1 + g_2 \cdot y$ parna, a to znači da je u (5) na lijevoj strani valuacija jednaka $-4\delta_1$, tj. $2\delta_1 = 3d_1$ pa je $\delta_1 = 3s,\ d_1 = 2s$. Još uvedimo D_1, D_2 kao stupnjeve od h_1, h_2. Sad je razlika valuacija pribrojnika s lijeve strane od (3) broj: $-2[2s(D_1 - D_2) - 3] \neq 0$, što znači da je valuacija lijeve

strane parna, a to je kontradikcija s činjenicom da je $v_O(y) = -3$.

Teorem. Neka je $E_1 : y^2 = x^3 + Ax + B,\ E_2 : y^2 = x^3 + A'x + B'$ i neka je $\phi : E_1 \to E_2$ izomorfizam algebarskih krivulja takav da je $\phi(O) = O$. Tada postoji broj $\mu \neq 0$ tako da je
$\phi(x, y) = (\mu^2 x, \mu^3 y)$. Pri tom je $A' = \mu^4 A,\ B' = \mu^6 B$.
Dokaz. Lako je provjeriti da je ovo gore izomorfizam krivulja. Obratno, prema predhodnim razmatranjima vrijedi $\phi(x, y) = (ax + b, cy + d)$. Odavde se lako dobije tvrdnja. Dovoljno je gledati relaciju

$$(cy + d)^2 = (ax + b)^3 + A'(ax + b) + B'$$

i iz nje zaključiti da je $b = d = 0$ i $c^2 = a^3$, tj. $c = \mu^3,\ a = \mu^2$ za neki μ itd.

Napomena. Slična tvrdnja vrijedi za eliptičke krivulje s Weierstrassovim modelom oblika $y^2 = x^3 + ax^2 + bx + c$. Za to je dovoljno gledati redom kompoziciju preslikavanja: prvo koje E_1 preslikava u oblik iz teorema (kratka Weierstrassova jednadžba), potom preslikavanje kao u teoremu, potom preslikavanje koje kratku W. jednadžbu vraća u običnu. Izvedite formule!

Korolar 1. Svaki izomorfizam eliptičkih krivulja (kao algebarskih krivulja) koji O preslikava u O, ujedno je i izomorfizam grupa.
I to ćemo ilustrirati za kratke W. jednadžbe (a vrijedi općenito). Sjetimo se formula iz predhodne lekcije:

$$x_3 = -x_1 - x_2 + \lambda^2 - a,\ y_3 = \lambda(x_1 - x_3) - y_1$$

gdje je $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ ako je $P \neq Q$, i $\lambda = \frac{f'(x_1)}{2y_1}$ ako je $P = Q$.
Tu je $a = 0$ i $f'(x) = 3x^2 + A$, pa uz gornja ograničenja, i uz napomenu da, ako s λ_μ označimo pripadni koeficijent smjera za točke $\phi(x_1, y_1)$ i $\phi(x_2, y_2)$, onda je $\lambda_\mu = \mu\lambda$, dobijemo:
$\phi((x_1, y_1) \oplus (x_2, y_2)) = \phi(-x_1 - x_2 + \lambda^2, \lambda(x_1 - x_3) - y_1)$
$= (\mu^2(-x_1 - x_2 + \lambda^2), \mu^3(\lambda(x_1 - x_3) - y_1)) = (-\mu^2 x_1 - \mu^2 x_2 + \lambda_\mu^2, ...)$.
Tu smo, uz gornja ograničenja, tvrdnju pokazali za prvu koordinatu. Dokažite je i za drugu i bez gornjih ograničenja.

Korolar 2. Grupa automorfizama eliptičke krivulje (kao algebarske krivulje i grupe, tj. kao algebarske grupe u karakteristici različitoj od $2, 3$) je, u pravilu grupa drugog reda $(x, y) \mapsto (x, \pm y)$, iznimno je ciklička grupa 4. ili 6. reda.

Kako svaka eliptička krivulja u karakteristici različitoj od $2, 3$ ima kratku W. jednadžbu, možemo iskoristiti teorem. Zato, iz $A' = A$ i $B' = B$ slijedi $\mu^4 = \mu^6 = 1$ (uz uvjet $A, B \neq 0$), tj. $\mu = \pm 1$, kako smo i tvrdili.
Ako je, pak, $B' = B = 0$, onda je $\mu = \pm 1, \pm i$, a ako je $A' = A = 0$, onda je $\mu = \pm 1, \pm\rho, \pm\rho^2$, gdje je ρ treći korijen iz jedinice. Pokažite da se ove grupe zaista realiziraju.

Definicija 1. Homomorfizam eliptičkih krivulja je svaki homomorfizam pripadnih grupa, koji je ujedno i morfizam algebarskih krivulja. Izogenija eliptičkih krivulja je homomorfizam koji nije nula preslikavanje. Ako postoji izogenija medju dvjema eliptičkim krivuljama, onda kažemo da su izogene. Endomorfizam je homomorfizam eliptičke krivulje u sebe. Skup svih endomorfizama od E označavamo kao End$E$.

Uočite da je End$E$ prsten s obzirom na standardno zbrajanje: $(\phi_1 + \phi_2)(P) = \phi_1(P) \oplus \phi_2(P)$; $(\phi_1 \circ \phi_2)(P) = \phi_1(\phi_2(P))$.

Napomena. (i) Sjetite se da je svaki homomorfizam surjektivan ili nula-homomorfizam - iako to nismo dokazali.
(ii) Ako primijeninimo Hurwitzowu formulu za $\phi : E_1 \to E_2$ uz standradne oznake za genus (koji je tu jednak 1) i n za stupanj morfizma, iz $2g_1 - 2 = n(2g_2 - 2) + R$, dobijemo $0 = n \cdot 0 + R$, tj. $R = 0$, pa ϕ nema grananja, tj. svaka točka iz E_2 ima točno n originala. Ta je činjenica karakteristična samo za krivulje genusa 1.
(iii) Kako je bilo za izomorfizam (iz korolara 1.), tako je za svaki morfizam eliptičkih krivulja, koji neutralni element preslikava u neutralni; može se pokazati da je on automatski i homomorfizam grupa.

Primjer 1. - homomorfizmi $[m] : E \to E$**.**
Preslikavanje $[m]$ za $m \in \mathbf{Z}$ definirano je kao

$$[m](P) = mP = P + P + ... + P \ (m \text{ puta}).$$

Iz definicije zbrajanja vidi se da su ovo homomorfizmi eliptičkih krivulja. Tvrdimo da su to različiti homomorfizmi, tj. da je $h : \mathbf{Z} \to \text{End}E;\ m \mapsto [m]$ Već smo vidjeli, da za eliptičke krivulje s jednadžbom $y^2 = f(x) := (x - e_1)(x - e_2)(x - e_3)$ vrijedi $[2](P) = O$ akko $P = O, (e_1, 0), (e_2, 0), (e_3, 0)$ što znači da $[2]$ nije konstanta pa je surjekcija (naravno, to možemo izravno

pokazati iz formula za zbrajanje). S druge, strane, ako je m neparan, a P točka 2. reda, onda je $[m]P = P$. Koristeći te dvije činjenice dokazujemo tvrdnju.

Primjer 2. Neka je $E : y^2 = x^3 + x^2 + x$; $\bar{E} = y^2 = x^3 - 2x^2 - 3x$. Definirajmo $\phi : E \to \bar{E}$ lokalno formulom $\phi(x, y) = (\frac{y^2}{x^2}, y\frac{x^2-1}{x^2})$, za $P \neq T := (0, 0)$ i $P \neq O$. Tada je ϕ definirano za svaki P i vrijedi $\phi(T) = \phi(O) = O$ pa je ϕ je izogenija eliptičkih krivulja. Pokažimo prvi dio tvrdnje izravno, a izravni dokaz druge ostavljamo vama, kao i dokaz da je gornje preslikavanje dobro definirano, tj. da je slika u $\bar{E}$.
Dokaz da je $\phi(O) = O$. ϕ proširimo na homogene koordinate:

$$\phi[X, Y, Z] = [Y^2Z, Y(X^2 - Z^2), X^2Z].$$

U lokalnim koordinatama oko O, koje smo već uveli, $u := \frac{X}{Y}$, $v := \frac{Z}{Y}$, jednadžba krivulje E je

$$v = u^3 + u^2v + uv^2,$$

a O je $(0, 0)$. Nadalje, naše preslikavanje (dijeljenjem sa srednjim v clanom, potom brojnika i nayivnika s Y^3) postaje

$$\phi(u, v) = (\frac{v}{u^2 - v^2}, \frac{u^2v}{u^2 - v^2}).$$

Iz jednadžbe dobijemo $v = u^3+u^2v+uv^2 = u^3+u^2(u^3+u^2v+uv^2)+u(u^3+u^2v+uv^2)^2 = u^3[1+(u^2+uv+v^2)+(u^2+uv+v^2)^2]$. Ako to sustavno uvrstimo u formulu za ϕ dobijemo da je $\phi(0, 0) = (0, 0)$ kako smo i tvrdili.
Slično dobijemo za preslikavanje oko $(x, y) = (0, 0)$ u (u, v) koordinate (opet nakon dijeljenja homogenih koordinata sa srednjom, potom dijeljenja brojnika i nayivnika sa Z^3) : $\phi(x, y) = (\frac{y}{x^2-1}, \frac{x^2}{y(x^2-1}) = (\frac{y}{x^2-1}, \frac{y^3}{(x^2-1)(x^2+x+1)^2})$ (nakon zamjene $x = \frac{y^2}{x^2+x+1}$ na odgovarajućem mjestu). Zato je $\phi(T) = \phi(0, 0) = (0, 0) = O$.

Uvod u aritmetiku eliptičkih krivulja

Točke konačnog reda. Lutz-Nagell teorem - 8.lekcija

Ako je E bilo koja abelova grupa (s aditivnim zapisom i neutralnim elementom O) i P njen element, onda za niz elemenata

$$P, 2P, 3P, ...$$

mogu nastupiti dvije mogućnosti.
Prva je da su u tom nizu svi elementi različiti. Tada kažemo da je P element **beskonačnog reda**. Uočite da je tada $< P >:= \{..., -2P, -P, O, P, 2P, ...\}$ beskonačna ciklička grupa generirana s P (onosno $-P$), koja je izomorfna grupi $\mathbf{Z}$ (jedan od izomorfizama preslikava P u 1; ima li još koji?).
Druga je da je $mP = O$ za neki $m \in \mathbf{N}$. Tada ako je m najmanji prirodni broj s tim svojstvom kažemo da je P (konačnog) reda m i tada je skup $< P >= \{O, P, 2P, ..., (m-1)P\}$ ciklička grupa m-tog reda (s generatorom P; što možete reći o drugim generatorima?), koja je izomorfna grupi $\mathbf{Z}/m\mathbf{Z}$ (koja se pak može realizirati kao skup $\{0, 1, 2, ..., (m-1)\}$ uz zbrajanje modulo m).
Lako se vidi da elementi kojima red dijeli m (tj. rješenja jednadžbe $mT = O$) čine podgrupu u E. Naime, ako je $mT = O$, onda je i $m(-T) = O$,i ako je $mT_1 = mT_2 = O$, onda je $m(T_1 + T_2) = O$.
Takodjer svi elementi konačnog reda čine podgrupu u E (torzijska podgrupa, oznaka E_{tors}).
Ako je E eliptička krivulja potrebna je dodatna napomena. Na primjer, ako gledamo eliptičke krivulje nad $\mathbf{C}$ i njihove točke nad $\mathbf{C}$, onda ima jedna točka 1. reda - to je O, vidjeli smo da ima 3 točke 2. reda, koje skupa s O čine grupu rješenja jednadžbe $2T = O$, lako se može pokazati da ima 8 točaka 3. reda, koje skupa s O čine grupu rješenja jednadžbe $3T = O$. Jednadžba $4T = O$ ima 16 rješenja: O, 3 točke 2. reda i 12 točaka 4. reda. Općenito, jednadžba $mT = O$ na eliptičkoj krivulji ima m^2 kompleksnih rješenja koje čine grupu izomorfnu $\mathbf{Z}/m\mathbf{Z} \oplus \mathbf{Z}/m\mathbf{Z}$ (direktna suma abelovih grupa).
Na primjer, ako je E zadana standardnom afinom jednadžbom

$$y^2 = x^3 + ax^2 + bx + c \tag{1}$$

gdje je $x^3+ax^2+bx+c = (x-e_1)(x-e_2)(x-e_3)$, onda su $O, (e_1, 0), (e_2, 0), (e_3, 0)$ rješenja jednadžbe $2T = O$. Uočite da je $(e_1, 0) + (e_2, 0) = (e_3, 0)$ i analogno

za ostale mogućnosti, odakle se vidi da je ta grupa izomorfna direktnoj sumi grupa drugog reda. Slično, rješenja jednadžbe $3T = O$ su 9 fleksova krivulje itd. Isto vrijedi općenito u karakteristici 0 nad algebarski zatvorenim poljem, a uz neke izuzetke, i u svakoj karakteristici.

Podgrupa racionalnih točaka konačnog reda eliptičke krivulje nad Q.

Nas ovdje zanima **aritmetički**, tj. **diofantski** aspekt problema. Zato u (1) predpostavljamo da je E zadana nad $\mathbf{Q}$, tj. da su a, b, c, d iz (1) racionalni brojevi i da razmatramo samo točke krivulje definirane nad $\mathbf{Q}$, tj. iz $E(\mathbf{Q})$, tj. s racionalnim koordinatama. Tada opet **racionalna** rješenja jednadžbe

$$mT = O$$

čine podgrupu, samo ne mora biti m^2 racionalnih točaka (i u pravilu je tako). Uvedimo ovakve oznake:
$E[m]$:= podgrupa svih točaka koje su rješenja jednadžbe $mT = O$.
$E[m](\mathbf{Q})$:= podgrupa svih točaka iz $E[m]$ definiranih nad $\mathbf{Q}$.
$E_{\text{tors}}(\mathbf{Q})$:= podgrupa svih $\mathbf{Q}$-racionalnih točaka konačnog reda (torzijska podgrupa).

Primjer 1. (i) Neka je $E : y^2 = x^3 - x$. Tada je $E[2] = E[2](\mathbf{Q}) = \{O, (0,0), (1,0)(-1,0)\}$.
(ii) Neka je $E : y^2 = x^3 + x$. Tada je $E[2] = \{O, (0,0), (i,0)(-i,0)\}$ i $E[2](\mathbf{Q}) = \{O, (0,0)\}$.
Pokušajte u ovim primjerima odgovoriti na pitanje što je $E_{\text{tors}}(\mathbf{Q})$. Je li ta grupa konačna ili beskonačna?

Prirodno pojednostavljenje - eliptičke krivulje definirane nad Z.

Za razmatranje racionalne torzije dovoljno je gledati eliptičke krivulje definirane nad $\mathbf{Z}$. Na primjer

$$E : y^2 = x^3 - \frac{3}{2}x^2 + \frac{11}{16}x - \frac{3}{32}$$

nakon množenja s 64 postaje

$$(8y)^2 = (4x)^3 - 6(4x)^2 + 11(4x) - 6$$

odnosno

$$E' : y'^2 = x'^3 - 6x'^2 + 11x' - 6.$$

Vidimo da je E' definirana nad $\mathbf{Z}$ i da je preslikavanje

$$\phi : E \to E';\ (x, y) \mapsto (4x, 8y)$$

izomorfizam tih krivulja definiran nad $\mathbf{Q}$. Uočite da pri tom izomorfizmu
(i) $E(\mathbf{Q})$ prelazi u $E'(\mathbf{Q})$
(ii) $E[m](\mathbf{Q})$ prelazi u $E'[m](\mathbf{Q})$, za sve m.
(iii) $E(\mathbf{Q})_{tors}$ prelazi u $E'(\mathbf{Q})_{tors}$.

Tako nešto možemo napraviti općenito, a ne samo u ovom primjeru. Na primjer, ako jednadžbu

$$y^2 = x^3 + \frac{a}{d}x^2 + \frac{b}{d}x + \frac{c}{d}$$

pomnožimo s d^6, dobit ćemo

$$(d^3y)^2 = (d^2x)^3 + ad(d^2x)^2 + bd^3(d^2x) + cd^5$$

, pa je početna krivulja $\mathbf{Q}$-izomorfna krivulji

$$y'^2 = x'^3 + adx'^2 + bd^3x' + cd^5$$

(uz izomorfizam $(x, y) \mapsto (d^2x, d^3y)$).
Zato ćemo, kad nam zatreba smatrati da je Weierstrassov model eliptičke krivulje definiran nad $\mathbf{Z}$, tj. da su koeficijenti a, b, c iz (1) cijeli brojevi.

O torzijskim točkama eliptičke krivulje nad $\mathbf{Q}$ izreć ćemo nekoliko tvrdnja. Najgrublja od njih je sljedeća.

(I) Skup $\mathbf{Q}$-racionalnih točaka konačnog reda eliptičke krivulje nad $\mathbf{Q}$ je konačan.

Za jednu suptilniju tvrdnju potreban je cjelobrojni model.

(II) Neka je E eliptička krivulja s cjelobrojnim koeficijentima. Tada svaka $\mathbf{Q}$-racionalna točka konačnog reda ima cjelobrojne koordinate.

Napomenimo da ovo ne znači da je i svaka točka s cjelobrojnim koordinatama automatski torzijska. Medjutim, ako naidjemo na racionalnu necjelobrojnu točku (na cjelobrojnom W. modelu), onda znamo da je to točka

beskonačnog reda.

Primjer 2. (i) Neka je $E : y^2 = x^3 + 3x$ i uočimo njenu točku $P(\frac{1}{4}, \frac{7}{8})$. Ta je točka, prema tvrdniji (II), beskonačnog reda.
(ii) Točka $Q(3, 6)$ takodjer je na krivulji i ima cjelobrojne koordinata. Ona nije konačnog reda jer $2Q$ nema cjelobrojne koordinate (pokažite), pa $2Q$ nije konačnog reda (zato nije ni Q).

Još preciznija tvrdnja o torzijskim točkama je Lutz-Nagellov teorem iz 1937. odnosno 1935. godine (prema francuskoj matematičarki Elisabeth Lutz i norveškom matematičaru Trygve Nagell-u). Za tu tvrdnju podsjetimo na pojam diskriminante D polinoma $f(x) := x^3 + ax^2 + bx + c = (x - e_1)(x - e_2)(x - e_3)$, koja je definirana kao

$$D = (e_1 - e_2)^2(e_2 - e_3)^2(e_3 - e_1)^2$$

Izravnim računanjem dobije se

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$$

(uočite posljednja dva pribrojnika - već smo na njih nailazili).

Lutz-Nagell-ov teorem. Neka je E s cjelobrojnim koeficijentima i neka je D diskriminanta od E. Tada svaka $\mathbf{Q}$-racionalna točka konačnog reda ima cjelobrojne koordinate. Ako je $P(x, y)$ takva afina točka, onda je ili $y = 0$ ili je $y^2|D$.

Uočite da je tvrdnja (II) sadržana u teoremu, a da je drugi dio teorema konstruktibilna varijanta tvrdnje (I). Zato je taj teorem dobra osnova algoritma za odredjivanje torzijskih točaka.

Primjer 3. Neka je $E : y^2 = x^3 - x^2 + x$. Tada je $D = -3$ pa su jedine $\mathbf{Q}$-racionalne torzijske točke $O, (0, 0)$ i možda neke od onih (x, y) za koje je $y = \pm 1$ ili ± 3. Za $y = \pm 1$ dobijemo $x = 1$ i lako provjerimo da za $P(1, 1)$ vrijedi $2P = (0, 0)$ pa su $(1, \pm 1)$ takodjer torzijske. Za $y \pm 3$ dolazimo do jednadžbe $x^3 - x^2 + x - 9 = 0$ koja nema cjelobrojnih rješenja. Zato je $E(\mathbf{Q})_{tors} = \{O, (0, 0), (1, \pm 1)\}$. Pokažite da je ta grupa izomorfna $\mathbf{Z}/4\mathbf{Z}$.

Zadatak. Odredite racionalne torzijske točke i torzijsku podgrupu krivulja zadanih afinim jednadžbama:

(i) $y^2 = x^3 + 2$,
(ii) $y^2 = x^3 + x$,
(iii) $y^2 = x^3 + 4$,
(iv) $y^2 = x^3 + 4x$,
(v) $y^2 = x^3 - x^2 + \frac{1}{4}$,
(vi) $y^2 = x^3 + 1$,
(vii) $y^2 = x^3 + \frac{9}{4}x^2 - x + 1$,
(viii) $y^2 = x^3 - x$,
(ix) $y^2 = x^3 + 5x^2 + 4x$,
(x) $y^2 = x^3 + 337x^2 + 20736x$,

Iako izgleda da je s L-N teoremom problem torzije riješen, treba napomenuti da ja za velike D problem faktorizacije često vrlo mukotrpan ili praktično nemoguć (to je problem subeksponencijalne, a ne polinomijalne složenosti). Zato se za odredjivanje torzije (do na izomorfizam) često koristi jedan kriterij koji ćemo upoznati kad budemo obradjivali eliptičke krivulje nad konačnim poljem i redukciju eliptičke krivulje. S duge strane, iz L-N teorema, informaciju o torziji dobivamo samo za konkretnu krivulju, a malo toga možemo reći za sve krivulje (ili familije krivulja). Na primjer za familiju krivulja

$$y^2 = x^3 - n^2 x,$$

za $n \in \mathbf{N}$ (koja je povezano s problemom kongruentnih brojeva - o tome ćemo više poslije), dobijemo $D = 4n^6$, odakle nije lako izvesti činjenicu da se za sve ove krivulje torzijska podgrupa poklapa s podgrupom $\{O, (0,0), (\pm n, 0)\}$.

Problem mogućih racionalnih torzija (za sve eliptičke krivulje nad $\mathbf{Q}$) riješio je Mazur (1977-1978.).

Mazurov teorem. Neka je P racionalna točka m-tog reda na eliptičkoj krivulji E nad $\mathbf{Q}$. Tada je

$$1 \leq m \leq 10, \text{ ili } m = 12.$$

Moguće torzijske podgrupe su
(I) cikličke grupe reda m za $1 \leq m \leq 10$, ili $m = 12$.
(II) direktni produkt cikličkih grupa reda 2 i reda $2n$ za $1 \leq n \leq 4$.

O svim $\mathbf{Q}$-racionalnim točkama govori Mordellov teorem iz 1922. godine. Jednostavnim riječima on tvrdi da se sve racionalne točke mogu povlačenjem tangenata i sekanata dobiti iz konačnog skupa takvih točaka (generatora).

Mordellov teorem. Neka je E eliptička krivulja nad $\mathbf{Q}$. Tada je $E(\mathbf{Q})$ konačno generirana abelova grupa.

Lutz-Nagellov teorem dokazat ćemo u sljedećoj lekciji. Taj je dokaz složen, ali elementaran. U nastavku ćemo dokazati i Mordellov teorem (uz neka ograničenja). Taj je dokaz relativno elementaran, ali još uvijek nije pronadjen algoritam za odredjivanje generatora (iako postoje vrlo uspješne metode). Dokaz Mazurova teorema je vrlo složen i neelementaran (potrebna su duboka znanja iz algebarske geometrije i algebarske teorije brojeva)i nećemo ga dokazivati.

Uvod u aritmetiku eliptičkih krivulja

Dokaz Lutz-Nagell-ova teorema - 9.lekcija

Vidjeli smo da se Lutz-Nagell-ov teorem sastoji od dva dijela. Pokazuje se da je teži onaj dio koji govori da su torzijske točke na cjelobrojnom W. modelu nužno cjelobrojne. To je upravo tvrdnja (II) iz predhodne lekcije. Da pokažemo kako iz tog dijela teorema slijedi drugi dio potrebna je samo jedna dobro poznata činjenica o diskriminanti D polinoma

$$f(x) := x^3 + ax^2 + bx + c = (x - e_1)(x - e_2)(x - e_3),$$

naime da postoje polinomi h_1, h_2 s cjelobrojnim koeficijentima tako da bude

$$h_1(x)f(x) + h_2(x)g(x) = D, \tag{1}$$

gdje je g brojnik u duplikacijskoj formuli (iz 6. lekcije - tamo je $x = x(P)$ i $y = y(P)$)

$$x(2P) = \frac{x^4 - 2bx^2 - 8cx + (b^2 - 4ac)}{4y^2}. \tag{2}$$

Pokušajte sami naći h_1, h_2 uz napomenu da je h_1 drugog, a h_2 trećeg stupnja.

Dokaz kriterija iz L-N teorema, modulo tvrdnja (II).
Neka je P točka konačnog reda za koju je $y(P) \neq 0$. Tada je $2P \neq O$ i $2P$ je takodjer torzijska, pa su, prema tvrdnji (II), brojevi $x(P), y(P), x(2P), y(2P)$ cijeli. Prema formuli (2) vrijedi $y(P)^2 | g(x(P))$, a kako je $y(P)^2 = f(x(P))$, iz (1) slijedi $y(P)^2 | D$, kako smo i htjeli.

Priprema za dokaz tvrdnje II.
Sad vidimo da je za dokaz Lutz-Nagell-ova teorema dovoljno pokazati da su torzijske točke na cjelobrojnom W. modelu cjelobrojne. Za dokaz se podsjetimo diskretne valuacije u prostom broju p. Ako se racionalni broj q različit od nule napiše kao $q = p^r \frac{m}{n}$ gdje su m, n, p medjusobno relativno prosti, onda definiramo $v_p(q) := r$.
Sad se dokaz provodi tako da se pokaže, da za svaku racionalnu torzijsku točku $P(x, y)$, uz $y \neq 0$, eliptičke krivulje $E : y^2 = x^3 + ax^2 + bx + c$ uz cjelobrojne a, b, c, i svaki prosti broj p vrijedi $v_p(x) \geq 0$ i $v_p(y) \geq 0$.
Dokaz se provodi kontradikcijom, pa razmotrimo što znači da je $v_p(x) < 0$ ili

$v_p(y) < 0$ za neki p. Iz jednadžbe eliptičke krivulje evidentno je da vrijedi: $v_p(x) < 0$ akko $v_p(y) < 0$, i tada je $3v_p(x) = 2v_p(y)$, tj. $v_p(x) = -2k,\ i\ v_p(y) = -3k$, za $k \in \mathbf{N}$ (*).
Da lakše provedemo razmatranje uvodimo sljedeće oznake:

$$E(p^k) := \{(x,y) \in E(\mathbf{Q}) : v_p(x) \leq -2k\} \cup \{O\},\ k = 1,2,3,...$$

Napominjemo da je prema (*) gornji uvjet ekvivalentan s $v_p(y) \leq -3k$ (jer točke očito nisu reda 2). Takodjer napominjemo da smo dodali O da bi $E(p^k)$ bila grupa, što je za dokaz vrlo važno i što ćemo dokazati poslije.
Vidi se da vrijedi: $E(\mathbf{Q}) \supset E(p) \supset E(p^2) \supset ....$
Vidi se takodjer da je naš cilj pokazati da torzijska točka ne može biti niti u jednom $E(p)$. Pokazuje se da je za provodjenje dokaza vrlo korisno iz afinih x, y koordinata na krivulji prijeći na t, s koordinate oko O, gdje je:

$$s := \frac{1}{y},\ t := \frac{x}{y}$$

koje smo već upoznali (uz druge oznake: u, v).
Odmah se vidi da su $E(p^k)$ jednostavno zadani, naime:

$$E(p^k) := \{(t,s) \in E(\mathbf{Q}) : v_p(t) \geq k\} \cup \{O\},\ k = 1,2,3,...$$

(naravno, gornji je uvjet ekvivalentan s $v_p(s) \geq 3k$).
Uvedimo sad još jednu korisnu oznaku (relaciju): za racionalne brojeve pišemo $q_1 \equiv q_2 \pmod{p^k}$ ako $v_p(q_2 - q_1) \geq k$.

Dokaz tvrdnje II uz jednu predpostavku.

Predpostavimo da znademo da su skupovi $E(p^k)$ grupe i da za svake dvije točke $P_1, P_2 \in E(p^k)$ vrijedi

$$t(P_1 \oplus P_2) \equiv t(P_1) + t(P_2)\ (mod\ p^{3k}), \tag{3}$$

gdje su $t(P), s(P)$ oznake za t, s koordinate točke P. Neka je sad P torzijska točka reda m koja je u $E(p)$ (podsjetimo da iz te predpostavke treba izvesti kontradikciju). Tada postoji k tako da je $P \in E(p^k)$, ali $P \notin E(p^{k+1})$. Iz (3) zaključujemo da mora biti (sjetite se da je $O(0,0)$ u t, s koordinatama)

$$0 = t(O) = t(mP) \equiv mt(P)\ (mod\ p^{3k}).$$

Sad smo gotovi ako p ne dijeli m, jer bi to značilo da $t(P) \equiv 0 \ (mod\ p^{3k})$, što bi značilo da je $p \in E(p^{3k})$, što je u kontradikciji s $P \notin E(p^{k+1})$.
Slučaj $p|m$ samo je tehnički nešto složeniji. Naime, tada je $m = pn$ i točka $P' = nP$ ima red p. Sad ponavljamo gornji postupak, ali s točkom P'. Najprije treba napomenuti da je $P' \in E(p)$ (jer je $P \in E(p)$ i $P' = nP$ i $E(p)$ je grupa), pa postoji $l \in \mathbf{N}$ tako da je $P' \in E(p^l)$, ali $P' \notin E(p^{l+1})$. Sad provodimo prijašnji postupak, ali uz P' umjesto P, uz p umjesto m i uz l umjesto k. Dobijemo

$$0 = t(O) = t(pP') \equiv pt(P') \ (mod\ p^{3l}),$$

odakle zaključujemo da je $P' \in E(p^{3l-1})$, što je u kontradikciji s $3l-1 \geq l+1$.

Dokaz da su svi $E(p^k)$ grupe i da vrijedi (3) - skica - detalji u [S-T, str. 49-56]
Priprema dokaza.
Pažljivijom analizom vidimo da je dovoljno pokazati da su skupovi $E(p^k)$ zatvoreni na zbrajanje, medjutim oni su zatvoreni i na promjenu predznaka. Pokazuje se da je puno pogodnije razmatranje provoditi u t, s koordinatama. Opet podsjetimo da u t, s koordinatama E ima jednadžbu

$$s = t^3 + at^2s + bts^2 + cs^3 \tag{4}$$

i da je $O(0, 0)$. Uočite da u ovom afinom modelu od E nema točaka $(e_i, 0),\ i = 1, 2, 3$ (u x, y koordinatama), medjutim ako neke od njih i jesu racionalne, tj. ako je neki od e_i racionalan, onda su i cjelobrojne, pa nisu u $E(p)$ niti za jedan p.
Transformacije prijelaza iz x, y u t, s koordinate su projektivne, pa pravci prelaze u pravce, pa se grupni zakon provjerava kao i prije (naravno vidi se i izravno da jednadžba $y = \lambda x + \mu$ prelazi u $s = -\frac{\lambda}{\mu}t + \frac{1}{\mu}$)
Ako (4) presječemo s pravcem $s = \alpha t + \beta$, dobijemo, kao i prije, kubnu jednadžbu, i ako su $P_i(t_i, s_i),\ i = 1, 2, 3$ tri točke presjeka (vidi sl.2.7 u [S-T] i detalje), onda je

$$t_1 + t_2 + t_3 = -\frac{a\beta + 2b\alpha\beta + 3c\alpha^2\beta}{1 + a\alpha + b\alpha^2 + c\alpha^3} \tag{5}$$

Ako, kako je i prije bilo, predpostavimo da P_1, P_2 imamo, a tražimo P_3, onda je (nakon lakog računa)

$$\alpha = \frac{t_2^2 + t_1t_2 + t_1^2 + a(t_2 + t_1)s_2 + bs_2^2}{1 - at_1^2 - bt_1(s_2 + s_1) - c(s_2^2 + s_1s_2 + s_1^2)} \tag{6}$$

(to je za $P_1 \neq P_2$), a ako je $P_1 = P_2$, onda je

$$\alpha = \frac{3t_1^2 + 2at_1s_1 + bs_1^2}{1 - at_1^2 - 2bt_1s_1 - 3cs_1^2} \tag{7}$$

a uvijek je $\beta = s_1 - \alpha t_1$.
Uočite takodjer da ako je (t_0, s_0) na krivulji, onda je $(-t_0, -s_0)$ na krivulji i spojnica kroz te dvije točke prolazi ishodištem $(0, 0)$. Zato je (u t, s koordinatama) $-(t, s) = (-t, -s)$.
Dokaz.
Prtedpostavimo da su P_1, P_2 iz $E(p^k)$, tj. $v_p(t_i) \geq k$ i $v_p(s_i) \geq 3k$ za $i = 1, 2$. Tada zahvaljujući jedinici u nazivniku od (6), odnosno (7), dobijemo da je

$$v_p(\alpha) \geq 2k, \ \textit{a onda} \ \ v_p(\beta) \geq 3k.$$

Sad, opet zahvaljujući jedinici u nazivniku od (5) dobijemo

$$v_p(t_1 + t_2 + t_3) \geq 3k$$

što dokazuje relaciju (3), a i grupoidnost. Naime iz te relacije slijedi $v_p(-t_3) = v_p(t_3) \geq k$, a za s koordinatu dobije se slično.

Uvod u aritmetiku eliptičkih krivulja

Mordell-ov teorem - 10.lekcija

Sjetimo se formulacije.
Mordellov teorem. Neka je E eliptička krivulja nad $\mathbf{Q}$. Tada je $E(\mathbf{Q})$ konačno generirana abelova grupa.

Primjer 1. (i) Grupa $\mathbf{Z}$ je konačno generirana. Točnije, ima jedan generator (broj 1 ili -1); kažemo da ima rang 1 (to je slobodna abelova grupa ranga 1).
(ii) Grupa $\mathbf{Z}[i] := \{a + bi : a, b \in \mathbf{Z}\}$ je konačno generirana, točnije to je slobodna abelova grupa ranga 2 (generatori su, na primjer, $1, i$).
(iii) Skup svih cjelobrojnih rješenja pellove jednadžbe $x^2 - 2y^2 = 1$ je abelova grupa G s obzirom na operaciju $*$ definiranu kao

$$(x_1, y_1) * (x_2, y_2) = (x_1x_2 + 2y_1y_2, x_1y_2 + x_2y_1).$$

Uočite da je $e := (1, 0)$ neutralni element i $(x, y)^{-1} = (x, -y)$. Ta je grupa konačno generirana ranga 1, ali nije slobodna, jer ima torzijski element $\epsilon := (-1, 0)$. Rješenje $t := (3, 2)$ ima beskonačan red i vrijedi

$$G = \{e, \epsilon\} \times < t >$$

gdje je $< t >$ ciklička grupa generirana s t (to je direktni produkt ili suma, svejedno, podgrupa), tj. kao apstraktna grupa G je izomorfna grupi $\mathbf{Z} \oplus \mathbf{Z}_2$.
(iv) Abelova grupa $(\mathbf{Q}, +)$ nije konačno generirana.
(v) Abelova grupa $(\mathbf{Q}^*, \cdot)$ nije konačno generirana.
(vi) Abelova grupa $\mathbf{Q}^*/\mathbf{Q}^{*2}$ nije konačno generirana - ta je grupa kao skup u prirodnoj bijekciji sa skupom svih prirodnih kvadratno slobodnih brojeva kojima je dodan broj -1, a skup generatora je skup svih prostih brojeva skupa s -1 (dokažite).

Visina točke eliptičke krivulje.
Tipičan dokaz Mordellova teorema koristi pojam visine (koji izvorno potječe od Fermata). Za racionalan broj

$$x = \frac{m}{n}$$

gdje je gornji zapis maksimalno skračen, definiramo visinu kao

$$H(x) = H(\frac{m}{n}) := \max\{|m|, |n|\}.$$

Ako je $P(x, y)$ afina racionalna točka na eliptičkoj krivulji

$$E : y^2 = x^3 + ax^2 + bx + c$$

definiranoj nad $\mathbf{Q}$, onda visinu od P definiramo kao visinu njene prve koordinate, tj.

$$H(P) := H(x).$$

Često se umjesto H koristi logaritamska visina h definirana kao

$$h(P) := logH(P)$$

gdje je log bilo koji logaritam s bazom većom od 1(a u pravilu smatramo da je prirodni).
Još se definira $H(O) = 1$, tj. $h(O) = 0$.

Kako ćemo h primjenjivati na eliptičku krivulju, bit će potrebno proučiti kako se visina ponaša prema operaciji zbrajanja. Radi toga podsjetimo na formule za x koordinatu zbroja. Neka je $P_0(x_0, y_0)$, $P(x, y)$ i $(P + P_0)(w, \omega)$. Tada je, za $P \neq P_0$,

$$w = -x - x_0 - a + \frac{(y - y_0)^2}{(x - x_0)^2} = \frac{Ay + Bx^2 + Cx + D}{Ex^2 + Fx + G} \tag{1}$$

gdje smo najprije sveli na zajednički nazivnik, potom $y^2 - x^3$ u brojniku zamijenili polinomom 2. stupnja u x i, konačno, uredili da koeficijenti $A, B, ..., G$ budu cijeli.
Slično, ako je $2P(u, v)$, onda je, kako smo vidjeli

$$u = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c} \tag{2}$$

Sad se odmah vidi da je za točke P dovoljno velike visine vrijedi $h(y) \approx \frac{3}{2}h(x),\ h(P + P_0) \approx 2h(P),\ h(2P) \approx 4h(P)$. (jer se kvadriranjem racionalna broja njegova visina udvostručuje itd.). Za dokaz Mordellova teorema te ćemo činjenice morati nešto preciznije zapisati ovako:

(I) Za svaki realan broj M je $\{P \in E(\mathbf{Q}) : h(P) \leq M\}$ je konačan.
(II) Za svaku racionalnu točku P_0 postoji konstanta k_0 tako da za svaku racionalnu točku P vrijedi

$$h(P + P_0) \leq 2h(P) + k_0.$$

(III) Postoji konstanta k tako da za svaku racionalnu točku P vrijedi

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

Tim trima svojstvima visine treba dodati još jedno, čisto algebarsko
(IV) Podgrupa $2E(\mathbf{Q})$ ima konačan indeks u grupi $E(\mathbf{Q})$, tj. $E(\mathbf{Q})/\mathbf{2E}(\mathbf{Q})$ je konačna grupa.
Pokazat ćemo kako se iz ova četiri svojstva izvodi Mordellov teorem. Prije toga napomenimo da je samo (I) tvrdnja trivijalna (jer uz zadane uvjete ima samo konačno mnogo mogućnosti za brojnike i nazivnike od $x := x(P)$). Medjutim ostale su tvrdnje netrivijalne, (II) i (III) su elementarne, a (IV) vrlo zaguljena. Taj je zahtjev vrlo jak. Na primjer $\mathbf{Q} = \mathbf{2Q}$ pa je kvocijent poput onog iz (IV) trivijalan, tj. jednočlan. Ipak je $(\mathbf{Q}, +)$ daleko od konačne generiranosti. S druge strane, primjer (vi) pokazuje da takav kvocijent ne mora biti konačan.
Sad trenutno možemo zaboraviti eliptičke krivulje i koncentrirati se na bilo koju abelovu grupu Γ.

Teorem 1. Neka je Γ abelova grupa i $h : \Gamma \to [0, \infty >$ funkcija visine koja zadovoljava svojstva (I), (II) i (III), i neka Γ zadovoljava i svojstvo (IV), tj. neka je $\Gamma/2\Gamma$ konačna grupa. Tada je Γ konačno generirana.
Dokaz. Iz svojstva (IV) slijedi da je skup reprezentanata iz Γ s obzirom na 2Γ konačan, recimo da je to skup

$$A = \{Q_1, Q_2, ..., Q_n\}.$$

To znači da je

$$(Q_1 + 2\Gamma) \cup (Q_2 + 2\Gamma) \cup ... \cup (Q_n + 2\Gamma) = \Gamma. \tag{3}$$

Neka su $k_i,\ i = 1, 2, ..., n$ konstante koje postoje prema (II) (za $-Q_i$ umjesto P_0), i neka je k' najveća od tih konstanata. Definirajmo skup B (koji je konačan prema (I)) kao:

$$B := \{R \in \Gamma : h(R) \leq k + k'\}.$$

Tvrdimo: skup $A \cup B$ generira Γ, posebice Γ je konačno generirana.
Da to pokažemo, neka je $P \in \Gamma$ bilo koji element. Tada, prema (3), postoji $Q_{i_1} \in A$ tako da je $P - Q_{i_1} \in 2\Gamma$, što se moze zapisati i kao
$P - Q_{i_1} = 2P_1$, za neki $P_1 \in \Gamma$. Sad možemo nastaviti s P_1 umjesto P itd.
$P_1 - Q_{i_2} = 2P_2$
$P_2 - Q_{i_3} = 2P_3$
. . .
$P_{m-1} - Q_{i_m} = 2P_m$
Ako drugu jednakost pomnožimo s 2, treću s 4, četvrtu s 8 itd., pa zbrojimo, dobijemo

$$P = Q_{i_1} + 2Q_{i_2} + 4Q_{i_3} + ... + 2^{m-1}Q_{i_m} + 2^m P_m \tag{4}$$

Tvrdimo da bez obzira na P, ako je m dovoljno velik onda je $P_m \in B$.
Za to uočimo neki P_j i vidimo (prema (II) i (III) i definiciji od k_i i k':
$4h(P_j) \leq h(2P_j) + k = h(P_{j-1} - Q_{i_j}) + k \leq 2h(P_{j-1}) + k + k'$, pa je $h(P_j) \leq \frac{3}{4}h(P_{j-1}) - \frac{1}{4}(h(P_{j-1} - (k + k'))$.
Sad vidimo, u nizu $P_1, P_2, P_3, ...$, dok god je $h(P_i) \geq k + k'$, sljedeći element ima visinu bar 75 posto manju od $h(P_i)$, pa jednom visina mora pasti ispod $k + k'$. Dokaz je gotov.

Dakle, da bismo dokazali Mordell-ov teorem, **jedino** treba dokazati tvrdnje (II), (III) i (IV).

Skica dokaza tvrdnje (II). Podsjetimo se najprije da u (1) možemo staviti $x = \frac{m}{e^2}$, $y = \frac{n}{e^3}$ i da su ti prikazi maksimalno skraćeni, pa je $|m| \leq H(P)$ i $e^2 \leq H(P)$. Sad (1)postaje

$$w = \frac{Ane + Bm^2 + Cme^2 + De^4}{Em^2 + Fme^2 + Ge^4}.$$

Takodjer tu zamjenu možemo staviti u jednadžbu krivulje, pa dobijemo

$$n^2 = m^3 + ae^2m^2 + be^4m + ce^6.$$

Sad izravnim uvrštavanjem dobijemo $|n| \leq KH(P)^{\frac{3}{2}}$, gdje je $K := \sqrt{1 + |a| + |b| + |c|}$, a nakon toga i
$|Ane + Bm^2 + Cme^2 + De^4| \leq (|AK| + |B| + |C| + |D|)H(P)^2$ i $|Em^2 + Fme^2 + Ge^4| \leq (|E| + |F| + |G|)H(P)^2$.
Zato je $H(P + P_0) := H(w) \leq K_0H(P)^2$, gdje je K_0 veća od konstanta na desnim stranama (uočite da nam tu nije bilo važno što brojnik i nazivnik od w možda nisu maksimalno skraćeni). Tako smo, nakon logaritmiranja,

dokazali (II) i dobili ocjenu za $k_0 := logK_0$.

Skica dokaza tvrdnje (III).
Tu gledamo (2)i stavljamo $x = \frac{m}{n}$ gdje je taj prikaz maksimalno skraćen. Zato je

$$u = \frac{\Phi(m,n)}{\Psi(m,n)} := \frac{m^4 - 2bm^2n^2 - 8cmn^3 + (b^2 - 4ac)n^4}{4m^3n + 4am^2n^2 + 4bmn^3 + 4cn^4}.$$

Za razliku od (II), sad nam je važno imaju li $\Phi(m,n)$ i $\Psi(m,n)$ zajedničke faktore (jer želimo dobiti ocjenu oblika $H(u) \geq ...$). Tvrdimo da postoji prirodni broj R tako da zajednička mjera od $\Phi(m,n)$ i $\Psi(m,n)$ dijeli R, bez obzira o kojima m, n je riječ (tj. da takvih mjera ima konačno mnogo pa za R možemo staviti njihov višekratnik). Za tren predpostavimo da je tako i sjetimo se da je $H(P) = \max\{|m|, |n|\}$. Tada je
$H(2P) := H(u) \geq \frac{1}{R}\max\{|\Phi(m,n)|, |\Psi(m,n)|\} \geq \frac{1}{2R}(|\Phi(m,n)| + |\Psi(m,n)|)$
$\geq \frac{1}{2R}H(P)^4 \frac{|\Phi(m,n)|+|\Psi(m,n)|}{\max\{|m|^4,|n|^4\}} = \frac{1}{2R}H(P)^4 \frac{|x^4-2bx^2-8cx+b^2-4ac|+|4x^3+4ax^2+4bx+4c|}{\max\{|x|^4,1\}}$
$\geq \frac{C}{2R}H(P)^4$ (pogledajte odgovarajuće mjesto u [S-T]).
Sad se rezultat ostvaruje logaritmiranjem.
Da bi dokaz završili potrebno je dokazati tvrdnju o broju R. Već smo u dokazu Lutz-Nagell-ova teorema (9. lekcija formula (1)) vidjeli da brojnik $g(x)$ i nazivnik $4f(x)$ od (2) generiraju diskriminantu, naime da postoje polinomi h_1, h_2 s cjelobrojnim koeficijentima (stupnja 3 odnosno 2) tako da bude

$$h_1(x)f(x) + h_2(x)g(x) = D \tag{5}$$

(za naše potrebe dovoljno je bilo znati da su f i g relativno prosti, ali iskoristimo ovo od prije). Sad vidimo, ako $d|\Phi(m,n)$ i $d|\Psi(m,n)$, onda $d|4Dn^7$. Medjutim, ako $d|\Phi(m,n)$, onda $d|4n^5\Phi(m,n)$, pa $d|4m^4n^5$, a kako su m, n relativno prosti, sad $d|4Dn^5$. Daljnjim ponavljanjem dobit ćemo, konačno da $d|4D$. Znači, možemo uzeti $R = 4D$.

Uvod u aritmetiku eliptičkih krivulja

Slabi Mordell-ov teorem - 11.lekcija

Za dokaz Mordellova teorema preostala nam je tvrdnja (IV), koja se katkad naziva **slabi mordellov teorem.** To je najteži i najvažniji dio teorema. Dakle, treba dokazati:
(IV) Podgrupa $2E(\mathbf{Q})$ ima konačan indeks u grupi $E(\mathbf{Q})$.
Radi jednostavnosti, grupu $E(\mathbf{Q})$ označit ćemo kao Γ. Dakle, treba dokazati da je $\Gamma/2\Gamma$ konačna grupa. Iako bi se dokaz mogao provesti u punoj općenitosti (medjutim, tada bi morali prijeći na razmatranje u poljima algebarskih brojeva), najjednostavniji je dokaz ako su sva tri korijena e_1, e_2, e_3 polinoma f cijeli brojevi. Mi tu nećemo napraviti takvu restrikciju, već ćemo predpostaviti samo da polinom f ima bar jedan racionalan korijen (pa onda i cjelobrojan). Nakon jednostavne zamjene varijabla možemo predpostaviti da je taj korijen jednak 0, pa možemo smatrati da je

$$E : y^2 = x^3 + ax^2 + bx.$$

Uočite da je tada $T(0,0)$ racionalna točka na E i da je $2T = O$. Takodjer, tu je $D = b^2(a^2 - 4b)$ pa treba biti $b \neq 0$ i $a^2 \neq 4b$ (što se vidi i izravno).

Primjer. Neka je $E : y^2 = x^3 - x^2 + x - 1$. Tu je $x = 1$ racionalan korijen od f. Razvojem po $x - 1$ dobijemo $y^2 = (x-1)^3 + 2(x-1)^2 + 2(x-1)$, pa je E izomorfna nad $\mathbf{Q}$ eliptičkoj krivulji $E' : y^2 = x^3 + 2x^2 + 2x$, koja je gornjeg oblika.

Priprema za slabi mordell-ov teorem, homomorfizmi ϕ i ψ.
Put za dokazivanje da je $\Gamma/2\Gamma$ konačna ide posredno preko jedne druge eliptičke krivulje koja je tijesno povezana s E. To je krivulja

$$\bar{E} : y^2 = x^3 + \bar{a}x^2 + \bar{b}x,$$

gdje je $\bar{a} := -2a$ i $\bar{b} = a^2 - 4b$ (uočite da je $\bar{E}$ zaista eliptička krivulja).
Te dvije krivulje su izogene, tj. postoji netrivijalni homomorfizam medju njima. O tome govori:
Teorem 1. (i) Racionalno preslikavanje $\phi : E \to \bar{E}$ zadano lokalno kao

$$\phi(x,y) := (\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}),\ za\ (x,y) \neq (0,0)$$

proširuje se do homomorfizma eliptičkih krivulja sa svojstvom $\phi(0,0) = \bar{O}$.
(ii) Racionalno preslikavanje $\psi : \bar{E} \to E$ zadano lokalno kao

$$\psi(\bar{x}, \bar{y}) := (\frac{\bar{y}^2}{4\bar{x}^2} \frac{\bar{y}(\bar{x}^2 - \bar{b})}{8\bar{x}^2}),\ za\ (\bar{x}, \bar{y}) \neq (0,0)$$

proširuje se do homomorfizma eliptičkih krivulja sa svojstvom $\psi(0,0) = O$.
(iii) $(\psi \circ \phi)(P) = 2P$ za sve $P \in E$ i $(\phi \circ \psi)(\bar{P}) = 2\bar{P}$, za sve $\bar{P} \in \bar{E}$.
Dokaz. Da su ϕ i ψ dobro definirani dokazuje se izravno (a može se, kao i za ostale detalje, pogledati [S-T, str. 76-82]). Da se te funkcije proširuju do morfizma za koje je $\phi(O) = \bar{O}$ i $\psi(\bar{O}) = O$ vidjeli smo u ranijem primjeru. Tada možemo primijeniti opći rezultat, dovoljno je napomenuti da su to racionalna preslikavanja koja neutralni element preslikavaju u neutralni, pa su onda to homomorfizmi grupa, a može se lako sve to i izravno dokazati, samo treba strpljenja (vidi [S-T]). Jednako tako, izravno se dokazuje da je kompozicija tih preslikavanja množenje s 2.

Djelovanje od ϕ i ψ na racionalne točke.
Kao i prije, grupu racionalnih točaka na E označimo kao Γ, a analogno tome pripadnu grupu na $\bar{E}$ označimo kao $\bar{\Gamma}$. Na svim točkama i ϕ i ψ su surjekcije, medjutim, općenito to nije istina za racionalne točke. Naravno, ta su preslikavanja definirana nad $\mathbf{Q}$ pa racionalne točke preslikavaju u racionalne. Zato je
(a) $\phi(\Gamma)$ je podgrupa od $\bar{\Gamma}$, a mi želimo pokazati da je konačna indeksa.
(b) $\psi(\bar{\Gamma})$ je podgrupa od Γ, a mi želimo pokazati da je konačna indeksa
(podsjetimo da je indeks $(A : B)$ podgrupe B abelove grupe A broj elemenata u kvocijentnoj grupi A/B; za nekomutativne je grupe slično, ali to nas tu ne zanima).
Zašto je važno da su gornji indeksi konačni?
Kad bismo to znali, odmah bi $\Gamma/2\Gamma$ bila konačna grupa. Naime, indeksi se ponašaju poput dvostrukih razlomaka (uz neke uvjete), pa je (sjetimo se da je $2\Gamma = \psi(\phi(\Gamma))$)

$$(\Gamma : 2\Gamma) = (\Gamma : \psi(\bar{\Gamma})) \cdot (\psi(\bar{\Gamma}) : \psi(\phi(\Gamma)) \leq (\Gamma : \psi(\bar{\Gamma})) \cdot (\bar{\Gamma} : \phi(\Gamma)) < \infty$$

(izravan dokaz u [S-T], lema na str. 87.).
Opis grupa $\phi(\Gamma)$ i $\psi(\bar{\Gamma})$.
Taj je opis načelno zaista jednostavan. Naime, za $(\bar{x}, \bar{y}) \in \bar{\Gamma}$ različit od $(0,0)$ vrijedi sljedeće:

$(\bar{x}, \bar{y}) \in \phi(\Gamma)$ akko $\bar{x} = w^2$ za neki racionalni w.
Tome treba dodati da je $(0,0) \in \phi(\Gamma)$ akko $\bar{b} = a^2 - 4b$ kvadrat prirodna broja.
Za $\psi(\bar{\Gamma})$ vrijedi potpuno analogna tvrdnja. Naime, ψ se definira potpuno analogno kao ϕ samo što treba komponirati s izomorfizmom $(x, y) \mapsto (\frac{x}{4}, \frac{y}{8})$.
Dokaz tvrdnje. Jedan je smjer očit, zato predpostavimo da je $\bar{x} = w^2$ za racionalan w i $\bar{x} \neq 0$. Tražimo $(x, y) \in \Gamma$ tako da bude $\phi(x, y) = (\bar{x}, \bar{y})$. Kako mora biti $\frac{y^2}{x^2} = w^2$, vidimo da tražimo točku oblika $(x, \pm wx)$. Da bi ta točka bila u Γ mora biti $w^2x^2 = x^3 + ax^2 + bx$, a kako je $x \neq 0$, dobijemo $x^2 + (a - w^2)x + b = 0$, odakle je $x = w^2 - a \pm \frac{\bar{y}}{w}$ (iskoristite jednadžbu od $\bar{E}$).
Sad uočimo točke iz Γ:
(x_1, wx_1) gdje je $2x_1 = w^2 - a + \frac{\bar{y}}{w}$ i
(x_2, wx_2) gdje je $2x_2 = w^2 - a - \frac{\bar{y}}{w}$.
Još treba pokazati da se te točke preslikavaju u $(\bar{x}, \bar{y})$, a dovoljno je za prvu. Očito je $\frac{y_1^2}{x_1^2} = w^2$, dok je $\frac{y_1(x_1^2 - b)}{{x_1}^2} = \frac{wx_1(x_1^2 - x_1x_2)}{{x_1}^2} = w(x_1 - x_2) = \bar{y}$.

Dokaz da je $(\Gamma : \psi(\bar{\Gamma}))$ i $(\bar{\Gamma} : \phi(\Gamma))$ konačno.
Vidjeli smo da te činjenice dokazuju slabi mordellov teorem. Kako su one simetrične, dovoljno je pokazati jednu od njih, na primjer prvu.
Odgovor će biti vrlo jednostavan:$(\Gamma : \psi(\bar{\Gamma})) \leq 2^{k+1}$, gdje je k broj prostih djelitelja od b. Za drugi kvocijent vrijedi analogno, samo s $\bar{b}$ umjesto b.
Za dokaz najprije podsjetimo na grupu $\mathbf{Q}^*$ racionalnih brojeva bez nule i njenu podgrupu $\mathbf{Q}^{*\mathbf{2}}$ koja se sastoji od kvadrata racionalnih bojeva koji nisu nula, te na kvocijentnu grupu $\mathbf{Q}^*/\mathbf{Q}^{*\mathbf{2}}$ kojoj su reprezentanti $-1, 1$ i prirodni brojevi koji u rastavu nemaju viših potencija. Neka tilda označava klase u $\mathbf{Q}^*/\mathbf{Q}^{*2}$. Tada vrijedi $(\tilde{t})^2 = \tilde{1}$ za sve $t \in \mathbf{Q}$.
Definirajmo preslikavanje

$$\alpha : \Gamma \to \mathbf{Q}^*/\mathbf{Q}^{*\mathbf{2}}$$

ovako

$$\alpha(O) = \tilde{1},\ \alpha(0,0) = \tilde{b},\ \alpha(x,y) = \tilde{x}\ za\ x \neq 0.$$

Mi želimo pokazati da je α homomorfizam grupa i dokazati da je jezgra tog homomofizma upravo $\psi(\bar{\Gamma})$. To će biti presudno za dokaz. Napomenimo da za dokaz da je α homomorfizam ne možemo koristiti rezultate algebarske geometrije, jer to nije preslikavanje medju algebarsko-geometrijskim objektima, već to moramo pokazati izravno. Takodjer, napomenimo da je u $\mathbf{Q}^*/\mathbf{Q}^{*2}$)

grupni zakon multiplikativan. Idemo redom.
(1) α je homomorfizam grupa.
Naime $\alpha(-P) = \alpha(x,-y) = \tilde{x} = (\frac{\tilde{1}}{x}) = \alpha(P)^{-1}$. Za preostale dvije točke je očito.
Ostaje pokazati, ako je $P_1 \oplus P_2 \oplus P_3 = O$ onda je $\alpha(P_1)\alpha(P_1)\alpha(P_1) = \tilde{1}$.
To slijedi izravno iz jednadžbe za x koordinate triju točaka presjeka pravca $y = \lambda x + \mu$ i E:

$$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\mu)x - \mu^2 = 0.$$

Sad iz $x_1x_2x_3 = \mu^2$ izravno slijedi naša tvrdnja za afine točke različite od $(0,0)$. Ostali se slučajevi lako provjere.
(2). Jezgra od α je $\psi(\bar{\Gamma})$.
To je očito iz karakterizacije $\psi(\bar{\Gamma})$ - sastoji se od svih (x,y) takvih da je x kvadrat racionalna broja, itd.
To govori da α inducira ulaganje $\Gamma/\psi(\bar{\Gamma}) \hookrightarrow \mathbf{Q}^*/\mathbf{Q}^{*2}$.
Ocjena slike od α.
Nećemo odgovoriti točno što je slika od α već samo približno, ali i to će biti dovoljno. Neka su $p_1, p_2, ..., p_k$ prosti brojevi koji dijele b. Tada je $\alpha(\Gamma)$ podgrupa podgrupe od $\mathbf{Q}^*/\mathbf{Q}^{*2}$ koja se sastoji od klasa elemenata oblika $\pm p_1^{\epsilon_1} \cdot p_2^{\epsilon_2} \cdot ... \cdot p_k^{\epsilon_k}$ gdje su ϵ_i jednaki 1 ili 0. Kako ta podgrupa ima 2^{k+1} elemenata, vrijedi $(\Gamma : \psi(\bar{\Gamma})) \leq 2^{k+1}$.
Da bismo ocijenili sliku od α najprije razmotrimo kako izgledaju $(x,y) = (\frac{m}{e^2}, \frac{n}{e^3}) \in \Gamma$, gdje su prikazi maksimalno skraćeni.
Stavljajući to u jednadžbu od E dobijemo (za $(x,y) \neq (0,0)$)

$$n^2 = m(m^2 + ame^2 + be^4).$$

Zapišimo $m = \pm m'^2 \cdot q_1 \cdot q_2 \cdot ... \cdot q_s$, gdje su q_j različiti prosti brojevi. Tada $q_1 \cdot q_2 \cdot ... \cdot q_s | (m^2 + ame^2 + be^4)$ pa $q_1 \cdot q_2 \cdot ... \cdot q_s | b$ (jer su m i e relativno prosti).
Zato su q_j djelitelji od b pa su neki p_i. To znači da je

$$\alpha(x,y) = \pm \bar{p_1}^{\epsilon_1} \cdot \bar{p_2}^{\epsilon_2} \cdot ... \cdot \bar{p_k}^{\epsilon_k}$$

kako smo i tvrdili.

Uvod u aritmetiku eliptičkih krivulja

Eksplicitna formula za rang - kvazialgoritam 12.lekcija

Napomenimo da smo u posljednje dvije lekcije dokazali da je grupa racionalnih točaka $\Gamma := E(\mathbf{Q})$ konačno generirana. Istina, potpun dokaz smo proveli samo za eliptičke krivulje $\mathbf{Q}$-izomorfne eliptičkim krivuljama

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

iako sve vrijedi općenito (štoviše, analogna tvrdnja vrijedi za svako polje algebarskih brojeva konačna stupnja nad $\mathbf{Q}$ - to se zove Mordell-Weilov teorem; takodjer, analogno vrijedi za višedimenzionalne analogone eliptičkih krivulja - za jakobijane algebarskih krivulja i općenito, za abelove mnogostrukosti).
U dokazu smo koristili visine i ocjenu za broj elemenata u $\Gamma/2\Gamma$. Sad ćemo pokazati da možemo zaboraviti na visine (one su svoju ulogu odigrale) i koncentrirati se samo na kvocijent $\Gamma/2\Gamma$.
Dogovor. Od sad ćemo operaciju zbrajanja na eliptičkoj krivulji označavati jednostavno znakom $+$, a znak $\oplus$ koristit ćemo na standardan način, kao znak za **direktnu sumu**.

Kao prvi korak iskoristimo općepoznatu činjenicu da je svaka konačno generirana abelova grupa izomorfna umnošku slobodne abelove grupe ranga r (direktna suma r kopija grupe cijelih brojeva) i torzijske podgrupe. Za nas to znači:

$$\Gamma \cong \mathbf{Z}^r \oplus \mathbf{Z}/p_1^{n_1}\mathbf{Z} \oplus ... \oplus \mathbf{Z}/p_k^{n_k}\mathbf{Z} \tag{1}$$

gdje je r jednoznačno definiran i zove se **rang** od Γ, a p_j su (ne nužno različiti) prosti brojevi.

Primjer. (i) Neka je $E : y^2 = x^3 - 5x$ i $\Gamma := E(\mathbf{Q})$ njena grupa $\mathbf{Q}$-racionalnih točaka (**Mordell-Weilova grupa**). Pokazat ćemo da je $r = 1$. Takodjer, uz pomoć Lutz-Nagell-ova teorema dobije se da je torzijska podgrupa drugog reda. Zato je $\Gamma \cong \mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$.
Malo podrobnija analiza pokazuje da je Γ generirana točkom $P(-1, 2)$ beskonačna reda i točkom $T(0, 0)$ reda 2. Zato je $\Gamma = \{mP + nT\}$ gdje su $m \in \mathbf{Z}$ i $n = 0$ *ili* 1 jednoznačni.
Uočite razliku izmedju izomorfizma i jednakosti.

(ii) Neka je $E : y^2 = x^3 - x$. Pokazat ćemo da je $r = 0$, a već smo vidjeli da se torzijska podgrupa sastoji samo od točaka 2 reda, tj. $\Gamma_{\text{tors}} = \{O, (0,0), (1,0), (-1,0)\}$. Te su točke organizirane u grupu četvrtog reda izomorfnu direktnoj sumi grupa 2. reda, tj. $\Gamma[2] \cong \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$.

Općenito, za svaku eliptičku krivulju nad $\mathbf{Q}$, grupa racionalnih točaka drugog reda $\Gamma[2]$ ili je trivijalna ili drugog reda ili direktna suma grupa 2. reda. To znači da se u (1) u torzijskom dijelu broj 2 ne pojavljuje, pojavljuje se jednom ili dva puta. Iz Mazurova teorema lako možemo izvesti koji se prosti brojevi i s kojim eksponentima mogu pojavljivati u (1), medjutim to nam nije potrebno.
$\Gamma[2]$ možemo općenito opisati, za grupe iz (1), a ne nužno samo one koje dolaze od eliptičkih krivulja. Naime za $p \neq 2$ množenje s 2 u abelovoj grupi neparnog reda je izomorfizam, a u cikličkoj grupi koja ima red potenciju broja 2 to je homomorfizam s dvočlanom jezgrom, izomorfnom dakle s $\mathbf{Z}/2\mathbf{Z}$. Zato je, za grupe (1),

$$\Gamma[2] \cong (\mathbf{Z}/2\mathbf{Z})^s$$

gdje je s broj indeksa j u (1) za koje je $p_j = 2$.

Iz (1) slijedi izravno (uočite razliku izmedju 2Γ i $\Gamma[2]$)

$$2\Gamma \cong 2\mathbf{Z}^r \oplus 2(\mathbf{Z}/p_1^{n_1}\mathbf{Z}) \oplus ... \oplus 2(\mathbf{Z}/p_k^{n_k}\mathbf{Z}) \tag{2}$$

Zato je

$$\Gamma/2\Gamma \cong (\mathbf{Z}/2\mathbf{Z})^r \oplus (\mathbf{Z}/p_1^{n_1}\mathbf{Z}/2(\mathbf{Z}/p_1^{n_1}\mathbf{Z})) \oplus ... \oplus (\mathbf{Z}/p_k^{n_k}\mathbf{Z}/2(\mathbf{Z}/p_k^{n_k}\mathbf{Z})). \tag{3}$$

Izravno iz definicije se vidi da je $\mathbf{Z}/p_j^{n_j}\mathbf{Z}/2(\mathbf{Z}/p_j^{n_j}\mathbf{Z})$ trivijalna grupa osim u slučaju kad je $p_j = 2$, tada je ta grupa izomorfna cikličkoj grupi 2. reda $\mathbf{Z}/2\mathbf{Z}$ (argument smo već rekli).
Sad dobivamo važnu formulu

$$(\Gamma : 2\Gamma) = 2^r \cdot 2^s$$

gdje je, opet, s broj indeksa j za koje je $p_j = 2$.
Zato vrijedi

$$(\Gamma : 2\Gamma) = 2^r \cdot |\Gamma[2]| \tag{4}$$

To je već dosta dobra eksplicitna formula za rang Kako smo vidjeli gore, s općenito može biti $0, 1$ ili 2, pa $|\Gamma[2]|$ može biti $1, 2$ ili 4. Medjutim ako se ograničimo samo na krivulje

$$E : y^2 = x^3 + ax^2 + bx$$

onda je $|\Gamma[2]| = 2$ ako $a^2 - 4b$ nije kvadrat, a $|\Gamma[2]| = 4$ ako jest (dok je $|\Gamma[2]| = 1$ za sve ostale eliptičke krivulje nad $\mathbf{Q}$, tj. za one koje nisu $\mathbf{Q}$-izomorfne ovima gore).

Zaključak. Ako bismo u (4) znali odrediti lijevu stranu, znali bismo odrediti i rang. Nažalost, ne postoji algoritam za odredjivanje $(\Gamma : 2\Gamma)$ (bar za sad) i to je jedan od najitrigantnijih problema suvremene matematike.

Kvazialgoritam za odredjivanje ranga za $E : y^2 = x^3 + ax^2 + bx$.
Iz (4) vidimo da je $2^r = \frac{(\Gamma:2\Gamma)}{|\Gamma[2]|}$.
Sjetimo se, da smo za krivulje gornjeg oblika izveli

$$(\Gamma : 2\Gamma) \leq (\Gamma : \psi(\bar{\Gamma})) \cdot (\bar{\Gamma} : \phi(\Gamma))$$

Može se pokazati (pogledajte [S-T, str.91)]da ova nejednakost nije daleko od jednakosti. Naime to je jednakost ako E ima četiri $\mathbf{Q}$-racionalne točke 2. reda (tj. ako je $a^2 - 4b$ puni kvadrat, tj. ako je $|\Gamma[2]| = 4$), a lijeva je strana 2 puta manja od desne inače (tj. ako je $|\Gamma[2]| = 2$). To znači da je

$$2^r = \frac{(\Gamma : \psi(\bar{\Gamma})) \cdot (\bar{\Gamma} : \phi(\Gamma))}{4} = \frac{|\alpha(\Gamma)| \cdot |\bar{\alpha}(\bar{\Gamma})|}{4}$$

gdje je $\alpha : \Gamma \to \mathbf{Q}^*/\mathbf{Q}^{*2}$ homomorfizam grupa definiran prije i sjetimo se da je $\alpha(0, 0) = \tilde{b}$, $\alpha(O) = \tilde{1}$ i za sve ostale točke $\alpha(x, y) = \tilde{x}$,
dok je $\bar{\alpha} : \bar{\Gamma} \to \mathbf{Q}^*/\mathbf{Q}^{*2}$ definiran potpuno analogno, samo što umjesto a, b stavljamo $\bar{a} : -2a$, a umjesto b stavljamo $\bar{b} := a^2 - 4b$.
Dakle, problem bi bio riješen ako bismo znali odredjivati slike od α i $\bar{\alpha}$. Mi ćemo pokazati postupak (ne algoritam), kojim ćemo, ako budemo imali sreće, moći odrediti sliku od α (a za $\bar{\alpha}$ sve je analogno).
Slika od α. Znamo da je $\tilde{1}$ u slici, jer je $\alpha(O) = \tilde{1}$. Sjetimo se da se afine točke $(x, y) \in \Gamma$ mogu predočiti u skraćenom zapisu

$$x = \frac{m}{e^2}, \ y = \frac{n}{e^3}$$

uz $e > 0$ (naravno m, n, e su cijeli te m, e relativno prosti ili $m = 0$, i n, e relativno prosti ili $n = 0$).

Slučaj $n = 0$.
Postoje dvije mogućnosti. Prva je da $a^2 - 4b$ nije kvadrat. Tada je $m = 0$ i $\alpha(0, 0) = \tilde{b}$. Naravno, to je novi element slike ako b nije kvadrat, inače je $\tilde{b} = \tilde{1}$.
Druga je, ako je $a^2 - 4b = d^2$ puni kvadrat. Tada su i $(\frac{-a\pm d}{2}, 0) \in \Gamma$ pa su i klase od $(\frac{-a\pm d}{2})$ u slici.
Slučaj $n \neq 0$**, tada je i** $m \neq 0$**.** Tada gledamo u jednadžbu

$$n^2 = m(m^2 + ame^2 + be^4). \tag{5}$$

U toj (diofantskoj) jednadžbi nepoznanice su m, n, e, a rješenja tražimo u cijelim brojevima, ali tako da bude $e > 0$, zatim da m, e te n, e budu relativno prosti (m i n ne moraju biti relativno prosti). Sad definiramo nove veličine b_1, b_2 ovako:
Neka b_1 bude hipotetska najveća zajednička mjera od m i b, ali tako da bude $mb_1 > 0$, i neka bude $b_1b_2 = b$ i $b_1m_1 = m$ (uočite da je $m_1 > 0$).
Ako to stavimo u jednadžbu (1) vidimo da $b_1^2|n^2$, tj. $b_1|n$ pa stavljamo $n = b_1n_1$. Ako sad u toj jednadžbi skratimo s b_1^2 dolazimo do jednadžbe

$$n_1^2 = m_1(b_1m_1^2 + am_1e^2 + b_2e^4), \tag{6}$$

u kojoj su b_2 i m_1 te e i m_1 relativno prosti, pa je desna strana umnožak relativno prostih brojeva, a kako je $m_1 > 0$, vidimo da je svaki od njih puni kvadrat, dakle
$m_1 = M^2$, $b_1m_1^2 + am_1e^2 + b_2e^4 = N^2$, pa nakon eliminacije m_1 dobijemo diofantsku jednadžbu

$$N^2 = b_1M^4 + aM^2e^2 + b_2e^4 \tag{7}$$

u kojoj koeficijenti zadovoljavaju uvjet $b_1b_2 = b$, a nepoznanice su M, e, N. Rješenja tražimo u cijelim brojevima, ali tako da bude:
(1) $e > 0$
(2) M i e, N i e, b_1 i e, b_2 i M, te M i N su relativno prosti
(ovo (2) nije tako presudno za postupak (iako je katkad korisno), na primjer, uz svako rješenje $((M, e, N)$ od (7) i (kM, ke, k^2N) je rješenje, pa uvijek možemo doći do rješenja kod kojega su M i e relativno prosti, ali sad se nećemo upuštati u tu analizu).
Gledamo sve takve mogućnosti za b_1 i b_2, i za svaku takvu jednadžbu gledamo ima li rješenja (M, e, N) ili ne. Ako nema, idemo dalje, a ako ima dobili smo

racionalnu točku $P(x,y)$ gdje je:

$$x = \frac{b_1 M^2}{e^2},\ y = \frac{b_1 MN}{e^3}.$$

Tu nam je bitan samo x, točnije bitan je samo b_1 jer je $\alpha(P) = \tilde{x} = \tilde{b_1}$, i tako smo dobili vrijednost u slici od α. Uočite da je ta vrijednost iz slike neovisna o tome koje smo rješenje od (7) našli, jer ona osvisi samo o b_1. Uočite i tako da slika od α ima samo konačno mnogo vrijednosti (to znamo od prije).
Sad se sve ovo ponovi s $\bar{E}$ i $\bar{\alpha}$ i primijenimo formulu $2^r = \frac{|\alpha(\Gamma)|\cdot|\bar{\alpha}(\bar{\Gamma})|}{4}$.
Osnovni problem ovog postupka (a zato to i nije algoritam) što, bar za sad, nema nikakve eksplicitne metode ili algoritma za odlučivanje ima li jednadžba (7) rješenje traženog oblika ili ne, odnosno odredjivanje bar jednog rješenja (ukoliko postoji).
Napomena. U (7) je diofantska jednadžba s trima nepoznanicama i gledamo cjelobrojna rješenja. Medjutim, ako podijelimo s e^4 dobijemo jednadžbu krivulje

$$v^2 = b_1 u^4 + au^2 + b_2$$

i gledamo racionalna rješenja (kao i do sada).
Uvjet $a^2 - 4b_1 b_2 = a^2 - 4b \neq 0$ govori da je pripadna afina krivulja C_0 nesingularna. Medjutim (jedina) beskonačno daleka točka $[0,1,0]$ je singularna (provjerite) i snjom se dobije krivulja C. Opća je činjenica da je C $\mathbf{Q}$-biracionalno izomorfna nesingularnoj krivulji A genusa 1 (koja obavezno ima model u obliku nesigularne projektivne kubične krivulje). Ne samo to već je preslikavanje s A u C morfizam (nad $\mathbf{Q}$) i bijekcija osim u dvjema točkama koje idu u $[0,1,0]$. Ovdje se sve, čak i više, može izravno pokazati (vidi [Silverman, The arithmetic of elliptic curves, Prop.2.5.2]). Naime, eksplicitno se može napisati jednadžba od A kao prostorne krivulje u projektivnom prostoru $\mathbf{P^3(C)}$ (točnije, to je sustav dviju jednadžba) tako da je A bez dviju točaka (definiranih nad $\mathbf{Q}(\sqrt{b_1})$) izomorfna nad $\mathbf{Q}$ s C_0, a te dvije točke odlaze u singularnu točku $[0,1,0]$ od A. Te izuzetne točke su racionalne akko je b_1 puni kvadrat, ali taj nam slučaj nije zanimljiv jer je onda slika od α jednaka $\tilde{1}$ (što nije nova vrijednost - za taj dio pogledajte odgovarajući dio u Washingtonu o "quartic curves"). Ako pak b_1 nije kvadrat, onda su racionalne točke od C_0 i A u bijekciji (ako ih uopće i ima).
Može se pokazati da postoji izomorfizam s koeficijentima iz $\mathbf{Q}$ izmedju A i neke nesingularne kubike. Sad se problem odredjivanja bar jednog cjelobrojnog netrivijalnog rješenja od (7) svodi na problem odredjivanja bar jedne

racionalne točke na toj kubici (ako postoji). Opet smo se vratili na nesingularne kubike (krivulje genusa 1) definirane nad $\mathbf{Q}$ i pitamo se imaju li one $\mathbf{Q}$-racionalnu točku, tj. jesu li to eliptičke krivulje nad $\mathbf{Q}$. Ne postoji algoritam za takvo nešto, a mnogi bi ga htjeli naći.

Uvod u aritmetiku eliptičkih krivulja

Odredjivanje ranga - 13. lekcija

Ponovimo već poznato. Neka je:
$E : y^2 = x^3 + ax^2 + bx$, $\bar{E} : y^2 = x^3 + \bar{a}x^2 + \bar{b}x$, gdje je $\bar{a} : -2a$ i $\bar{b} := a^2 - 4b$.
Označimo:
$\Gamma := E(\mathbf{Q})$, $\bar{\Gamma} := \bar{E}(\mathbf{Q})$,
$\alpha : \Gamma \to \mathbf{Q}^*/\mathbf{Q}^{*2}$ homomorfizam grupa definiran kao
$\alpha(0,0) = \tilde{b}$,
$\alpha(O) = \tilde{1}$
$\alpha(x,y) = \tilde{x}$, za sve ostale točke
dok je $\bar{\alpha} : \bar{\Gamma} \to \mathbf{Q}^*/\mathbf{Q}^{*2}$ definiran potpuno analogno, samo što umjesto a, b stavljamo $\bar{a}$, a umjesto b stavljamo $\bar{b}$. Tilda označava klasu racionalnog broja različitog od nule u $\mathbf{Q}^*/\mathbf{Q}^{*2}$.
Tada je

$$2^r = \frac{|\alpha(\Gamma)| \cdot |\bar{\alpha}(\bar{\Gamma})|}{4} \tag{1}$$

Kvazialgoritam za odredjivanje slike od α (i analogno za $\bar{\alpha}$) .

(I) $\tilde{1}$ i $\tilde{b}$ uvijek su slici (s tim da su jednaki ako je b kvadrat).
Dodatak: ako je $a^2 - 4b = d^2$ puni kvadrat, onda su i klase od $\frac{-a \pm d}{2}$ u slici.
(II) (netrivijalni dio) Za svaku mogućnost $b_1 b_2 = b$ gledamo diofantsku jednadžbu

$$N^2 = b_1 M^4 + aM^2 e^2 + b_2 e^4 \tag{2}$$

s nepoznanicama M, e, N. Rješenja tražimo u cijelim brojevima, ali tako da bude:
(1) $e > 0$
(2) M i e, N i e, b_1 i e, b_2 i M, te M i N su relativno prosti
Ako nema takvog rješenja (M, e, N), biramo drugi par b_1, b_2, a ako ima dobili smo racionalnu točku $P(x,y)$ gdje je:

$$x = \frac{b_1 M^2}{e^2},\ y = \frac{b_1 MN}{e^3}$$

i $\alpha(P) = \tilde{x} = \tilde{b_1}$, i tako smo dobili vrijednost u slici od α (ta vrijednost osvisi samo o b_1, a ne o rješenju (M, e, N)).

Napomena. U [S-T] (I) je djelomično uključeno u (II) jer se dopušta $e = 0$ i $N = 0$, a mi ćemo u (II) priznavati samo rješenja kojima su sve koordinate različite od nule. Takodjer, u (II) ne treba gledati $b_1 = 1$, jer, ako i bude dobrog rješenja, u slici će dati $\tilde{1}$.

Primjeri.

Primjer 1. $E : y^2 = x^3 - x$.

Tu je $a = 0,\ b = -1$, pa je $\bar{a} = 0,\ \bar{b} = 4$, pa je $\bar{E} : y^2 = x^3 + 4x$.

Odredjujemo sliku od α.

Mogućnosti za b_1 jesu ± 1. Kako su obje u (I) ne treba gledati (II) i imamo dva elementa u slici (jer -1 nije kvadrat). Dodatak u (I) daje $d = 2$, zato treba razmotriti $\frac{\pm 2}{2} = \pm 1$, pa ne dobivamo ni jednu novu vrijednost u slici od α. Zaključujemo:

$|\alpha(\Gamma)| = 2$.

Sad odredjujemo sliku od $\bar{\alpha}$.

(I) Daje samo $\tilde{1}$ jer je 4 kvadrat, a dodatak ne nastupa.

(II). Mogućnosti za b_1 jesu $\pm 1, \pm 2, \pm 4$. Brojeve 1 i 4 možemo odbaciti jer su kvadrati i već su u (I), pa ostaju samo $-1, 2, -2, -4$ (i odgovarajuće vrijednosti $-4, 2, -2, -1$ za b_2), pa su pripadne diofantske jednadžbe

(i) $N^2 = -M^4 - 4e^4$

(ii) $N^2 = 2M^4 + 2e^4$

(iii) $N^2 = -2M^4 - 2e^4$

(iv) (i) $N^2 = -4M^4 - e^4$

Vidimo da ni (i) ni (iii) ni (iv) nemaju rješenja (ne dopuštamo nule), pa ostaje (ii) koja ima očito rješenje $(M, e, N) = (1, 1, 2)$ Zaključujemo da je $|\bar{\alpha}(\bar{\Gamma})| = 2$.

Uvrštavajući u (1) dobijemo $2^r = \frac{2 \cdot 2}{4} = 1$, tj. $r = 0$.

Napomene. 1. Rješenje $(1, 1, 2)$ dolazi od točke $(2, 4)$ iz $\bar{\Gamma}$.

(2.) Usput smo dokazali i da $\bar{E}$ ima rang 0.

(3.) Zaključujemo da su racionalne točke na E i $\bar{E}$ torzijske, pa ih eksplicitno možemo odrediti. Pomoću Lutz-Nagell-ova teorema dobije se

$E(\mathbf{Q}) \cong \mathbf{Z}/\mathbf{2Z} \otimes \mathbf{Z}/\mathbf{2Z}$, i $\bar{E}(\mathbf{Q}) \cong \mathbf{Z}/\mathbf{4Z}$, što su neizomorfne grupe. E i $\bar{E}$ su $\mathbf{Q}$-izogene, a rang je invarijanta $\mathbf{Q}$-izogenije, dok torzijska podgrupa nije (izogene krivulje mogu čak imati različito mnogo torzijskih točaka - što tu nije slučaj).

(4.) Jednadžbe (i) i (iv) pripadaju vrijednostima $-1, -4$ od b_1, koji su u istim klasama od $\mathbf{Q}^*/\mathbf{Q}^{*2}$. Tu ni jedna od pripadnih diofantskih jednadžba nije imala rješenje. Općenito može se dogoditi da jedna od njih nema, a druga

ima rješenje koje zadovoljava sve uvjete (pa unaprijed ni jednu ne možemo odbaciti; ako jedna ima rješenje drugu ne moramo gledati, ali ako jedna nema treba provjeriti i drugu). Na primjer, za $y^2 = x^3 - 52x$ i vrijednosti $b_1 = -1, -4$, pripadne su jednadžbe (i) $N^2 = -M^4 + 52e^4$ i (ii) $N^2 = -4M^4 + 13e^4$. Ako sad u (i) uzmemo u obzir uvjet $(M, b_2) = (M, 52) = 1$, dopuštamo samo neparne M, pa nakon redukcije modulo 4 dobijemo jednadžbu $N^2 = -M^4$, koja nema rješenja, pa ni (i) nema dobrog rješenja. Sad bi bilo pogrješno zaključiti da klasa od -1 nije u slici od α. Naime, (ii) ima očito dobro rješenje $(M, e, N) = (1, 1, 3)$. Uočite, takodjer da (i) ima rješenje $(2, 1, 6)$ (koje ne zadovoljava dodatne uvjete iz kvazialgoritma).

Primjer 2. $E : y^2 = x^3 + x$.
Tu je $a = 0,\ b = 1$, pa je $\bar{a} = 0,\ \bar{b} = -4$, pa je $\bar{E} : y^2 = x^3 - 4x$.
Odredjujemo sliku od α.
Tu je $|\alpha(\Gamma)| = 1$.
Jedinu vrijednost - $\tilde{1}$ - dobijemo iz (I), drugih novih nema. Ostaje provjeriti (II) za $b_1 = -1$ čemu korespondira diofantska jednadžba

$$N^2 = -M^4 - e^4.$$

Ta jednadžba nema rješenja. Naime, radimo samo s prirodnim M i e.
Odredimo sliku od $\bar{\alpha}$.
(I) daje $\pm\tilde{1}$ jer -4 nije kvadrat, a dodatak za $d = 4$ daje ± 2, ukupno 4 vrijednosti.
(II). Mogućnosti za b_1 jesu $\pm 1, \pm 2, \pm 4$ i sve su bile u (I). Zaključujemo da je $|\bar{\alpha}(\bar{\Gamma})| = 4$.
Uvrštavajući u (1) dobijemo $2^r = \frac{1 \cdot 4}{4} = 1$, tj. $r = 0$.
Napomena. Opet zaključujemo da su racionalne točke na E i $\bar{E}$ torzijske, pa ih eksplicitno možemo odrediti. Pomoću Lutz-Nagell-ova teorema dobije se
$E(\mathbf{Q}) \cong \mathbf{Z/2Z}$, i $\bar{E}(\mathbf{Q}) \cong \mathbf{Z/2Z} \otimes \mathbf{Z/2Z}$, pa su torzije različitih kardinalnosti.
Nas ovdje više zanima E za koju smo dobili da ima samo dvije racionalne točke: O i $(0, 0)$.
Posebice, diofantska jednadžba $N^2 = M^4 + e^4$ (inače dobivena za $b_1 = 1$) ne može imati rješenje (osim trivijalnih koja uključuju nule), jer bi inače eliptička krivulja E imala racionalnu točku različitu od $(0, 0)$. To je dokaz poznate Fermatove tvrdnje (jedine iz teorije brojeva za koju je Fermat dao dokaz).

Primjer 3. $E : y^2 = x^3 - 5x$.
Tu je $a = 0,\ b = -5$, pa je $\bar{a} = 0,\ \bar{b} = 20$, pa je $\bar{E} : y^2 = x^3 + 20x$.
Odredjujemo sliku od α.
(I) Daje $\tilde{1}, \tilde{-5}$ jer -5 nije kvadrat, a dodatak ne nastupa.
(II) Mogućnosti za b_1 jesu $\pm 1, \pm 5$. Kako su 1 i -5 u (I) ostaju $-1, 5$ i pripadne diofantske jednadžbe
(i) $N^2 = -M^4 + 5e^4$
(ii) $N^2 = 5M^4 - e^4$.
Obje imaju očita rješenja $(M, e, N) = (1, 1, 2)$. Zaključujemo:
$|\alpha(\Gamma)| = 4$.
Sad odredjujemo sliku od $\bar{\alpha}$.
(I) Daje $\tilde{1}$ i $\tilde{5}$ jer je 20 u istoj klasi kao i 5, a dodatak ne nastupa.
(II). Mogućnosti za b_1 jesu $\pm 1, \pm 2, \pm 4, \pm 5, \pm 10, \pm 20$. Brojeve 1 i 5 možemo odbaciti jer su u (I), potom i $4, 20$ jer su u njihovim klasama, zatim uočimo da su $-1, -4$ i $-5, -20$ u istim klasama. Konačno ostaju $-1, -4, \pm 2, -5, -20, \pm 10$, pa su pripadne diofantske jednadžbe
(i) $N^2 = -M^4 - 20e^4$
(i)' $N^2 = -4M^4 - 5e^4$
(ii) $N^2 = 2M^4 + 10e^4$
(iii) $N^2 = -2M^4 - 10e^4$
(iv) $N^2 = -5M^4 - 4e^4$
(iv)' $N^2 = -20M^4 - 4e^4$
(v) $N^2 = 10M^4 + 2e^4$
(vi) $N^2 = -10M^4 - 2e^4$
Tu smo stavili (i),(i)' te (iii),(iii)' jer su $-1, -4$ te $-5, -20$ u istim klasama. Medjutim, s njima neće biti problema. Naime, odmah odbacujemo (i),(i)' (iii), (iii)', (iv) i (vi) zbog oba minusa (a tu ne dopuštamo nule), ostaje (ii) i (v). Tvrdimo da ni one nemaju dobra rješenja.
U (ii) možemo predpostaviti da M nije djeljiv s 5, pa jednadžba nema rješenja modulo 5. Sad vidimo da ni (v) nema rješenja, jer je $\tilde{5}$ u slici, a $\tilde{2}$ nije, pa nije ni $\tilde{10}$ (zbog grupne strukture).
Zaključujemo da je $|\bar{\alpha}(\bar{\Gamma})| = 2$.
Uvrštavajući u (1) dobijemo $2^r = \frac{4 \cdot 2}{4} = 2$, pa je $r = 1$.

Često imamo sreću s konkretnim krivuljama, medjutim još smo uvijek nemoćni s familijama, pa čak i s onim najjednostavnijim - parametriziranim prostim brojevima.

Primjer 4. Familija krivulja $E_p : y^2 = x^3 + px$, za proste p.
Tu je $a = 0,\ b = p$, pa je $\bar{E}_p : y^2 = x^3 - 4px$. Odredjivanje slike od α je jednostavno. U (I) dobijemo $\tilde{1}$ i $\tilde{p}$, dok su u (II) preostale mogućnosti za b_1 brojevi $-1, -p$, pa su i vrijednosti b_2 negativne. Tako je $|\alpha(\Gamma)| = 2$.
Kod $\bar{E}_p$ nastaju problemi. U (I) dobijemo $\tilde{1}$ i $\tilde{-p}$. U (II) su mogućnosti $\pm 1, \pm 2, \pm 4, \pm p, \pm 2p, \pm 4p$. Odbacujemo $1, 4, -p, -4p$, jer već postoje u (I), zatim uočavamo da su u istoj klasi $-1, -4$, te $p, 4p$ pa ostaju $-1, -4, \pm 2, p, 4p \pm 2p$. Ima osam jednadžba koje treba razriješiti:
(i) $N^2 = -M^4 + 4pe^4$
(i)' $N^2 = -4M^4 + pe^4$
(ii) $N^2 = 2M^4 - 2pe^4$
(iii) $N^2 = -2M^4 + 2pe^4$
(iv) $N^2 = pM^4 - 4e^4$
(iv)' $N^2 = 4pM^4 - e^4$
(v) $N^2 = 2pM^4 - 2e^4$
(vi) $N^2 = -2pM^4 + 2e^4$
Odmah vidimo samo to da u isto vrijeme (ii) i (vi) te (iii) i (v) imaju ili nemaju rješenje, takodjer da (i) nema rješenje modulo 4 (uz legitimni uvjet da je M neparan), i slično da (iv)' nema rješenja uz legitimni uvjet da je e neparan, pa ostaje gledati samo (i)', (ii), (iii),(iv). Medjutim to je lako reći, ali teško provesti. Vidimo da uz dvije moguńosti iz (I) ima najviše 8 elemenata u slici od $\bar{\alpha}$ (jer svaki od (ii), (iii) daju 0 ili 2), Tako za r ostaju mogućnosti $0, 1$ ili 2 i pokazuje se da sve mogućnosti nastupaju. Izgleda da dosta toga ovisi o ostatcima prostog broja p modulo 16.
Znade se sljedeće:
(A) Ako je $p \equiv 7, 11$ modulo 16 onda je $r = 0$.
(B) Ako je $p \equiv 3, 5, 13, 15$ modulo 16 onda je **slutnja** da je $r = 1$.
(C) Ako je $p \equiv 1, 9$ modulo 16 onda je **slutnja** da je $r = 0$ ili $r = 2$. Kad je jedno, a kad drugo izgleda da se ne može opisati kongruencijama.
Na primjer, kako je $p = 17 \equiv 1$ modulo 16, slutnja predvidja da je $r = 0$ ili $r = 2$. Kako smo vidjeli α ima 2 vrijednosti, a $\bar{\alpha}$ takodjer 2 u dijelu (I). U (II) dobijemo
(i)' $N^2 = -4M^4 + 17e^4$
(ii) $N^2 = 2M^4 - 34e^4$
(iii) $N^2 = -2M^4 + 34e^4$
(iv) $N^2 = 17M^4 - 4e^4$
jer, kako smo vidjeli, ostale ne treba gledati, ali treba znati da (ii) i (iii) vrijede dvostruko. To dvostruko je ništa, a ni (i)' niti (iv) nemaju rješenja,

iako to nije lako pokazati. Na primjer, (iv) ima rješenje po svakom modulu i nad $\mathbf{R}$, a ipak se pokazuje da (iv) nema rješenja (to je primjer jednadžbe koja pokazuje da u ovakvim okolnostima općenito ne vrijedi lokalno-globalni princip Minkowski-Hasse). Zaključujemo da je $r = 0$, u skladu sa slutnjom. Situacija kad dobivena diofantska jednadžba ima rješenje po svakom modulu i nad $\mathbf{R}$, povezan je s tzv. Selmerovom grupom. Takva jednadžba može, ali ne mora imati cjelobrojno rješenje, i za sad nema algoritma koji odgovara na to pitanje, dok je reduciranje problema na takve jednadžbe algoritamsko.

Zadatak. Odredite rang sljedećih krivulja.
(i) $y^2 = x^3 + 2x$
(ii) $y^2 = x^3 + 3x$
(iii) $y^2 = x^3 + 5x$
(iv) $y^2 = x^3 + 13x$
(v) $y^2 = x^3 + 73x$.

Evo i primjera u kojemu nije $a = 0$.
Primjer 5. Neka je $E : y^2 = x^3 + x^2 + x$. Tada je $a = b = 1$, pa je $\bar{a} = -2$ i $\bar{b} = -3$, dakle $\bar{E} :: y^2 = x^3 - 2x^2 - 3x$.
Slika od ϕ je trivijalna, jer (I) daje samo klasu od 1; naime $b = 1$, a dodatak ne nastupa. U (II) ostaje samo $b_1 = -1$ s pripadnom jednadžbom

$$N^2 = -M^4 + M^2e^2 - e^4$$

Kako je $-M^4 + M^2e^2 - e^4 = -(M^2 - e^2)^2 - M^2e^2 < 0$, jednadžba nema rješenja.
Kod $\bar{E}$ u (I) dobijemo 4 vrijednosti: najprije $1, -3$, a u dodatku $-1, 3$ (uočite da je $x^3 - 2x^2 - 3x = x(x + 1)(x - 3)$). Kako su to sve moguće vrijednosti za b_1 u (II), to je sve. Sad je $2^r = \frac{1 \cdot 4}{4} = 1$, pa je $r = 0$.

Uvod u aritmetiku eliptičkih krivulja

Eliptičke krivulje nad konačnim poljem - 14. lekcija

Konačna polja. Za svaki prost p, postoji polje od p elemenata, a može se realizirati kao

$$\mathbf{F}_p := \{0, 1, ..., p-1\}$$

uz zbrajanje i množenje modulo p. Analogna je realizacija kao kvocijentnog prstena $\mathbf{F}_p :\cong \mathbf{Z}/p\mathbf{Z}$.
Za svaki prirodan broj n postoji i konačno polje $\mathbf{F}_{p^n}$ od p^n elemenata, koje je proširnje stupnja n polja $\mathbf{F}_p$. To su sva, do na izomorfizam, konačna polja. Uobičajeno je pisati $q := p^n$ i $\mathbf{F}_q$ za pripadno polje.
Ako fiksiramo jedno algebarsko zatvorenje $\bar{\mathbf{F}}_p$ polja $\mathbf{F}_p$, onda su polja $\mathbf{F}_q$ jedina (kao skupovi) polja koja sadrže $\mathbf{F}_p$ i vrijedi

$$\mathbf{F}_q = \{x \in \bar{\mathbf{F}}_p : \ x^q = x\}.$$

Konkretna realizacija polja $\mathbf{F}_q$ ostvaruje se biranjem ireducibilnog polinoma f nad $\mathbf{F}_p$ i biranjem nekog njegovog korijena η. Tada je

$$\mathbf{F}_q = \{a_0 + a_1\eta + ... + a_{n-1}\eta^{n-1} : \ a_j \in \mathbf{F}_p\}$$

uz pokomponentno zbrajanje i množenje polinoma uz uvjet $f(\eta) = 0$.

Primjer 1. Polinom $f(x) := x^2 + 1$ ireducibilan je nad $\mathbf{F}_3$ pa je

$$\mathbf{F}_{3^2} = \{a + b\eta : \ a, b \in \mathbf{F}_3\},$$

uz uvjet $\eta^2 = -1$ i ima 9 elemenata.

Eliptičke krivulje nad $\mathbf{F}_p$.

Ograničujemo se na krivulje E s jednadžbama oblika

$$y^2 = x^3 + ax^2 + bx + c \tag{1}$$

gdje su $a, b, c \in \mathbf{F}_p$, a točke (x, y) gledamo da x, y budu u algebarskom zatvorenju $\bar{\mathbf{F}}_p$. Vidi se da je $O[0, 1, 0]$, kao i u karakteristici 0, jedina beskonačno

daleka točka. Tu točku i afine točke s koordinatama u $\mathbf{F}_p$ zovemo racionalnima. Zanimaju nas samo nesingularne krivulje. Zato odmah odbacujemo $p = 2$, jer je tada E singularna, tj. ima singularnu točku. Naime, ako stavimo $F(x, y) := y^2 - x^3 - ax^2 - bx - c$, onda je $\frac{\partial F}{\partial y} = 2y = 0$ za sve (x, y). Dalje, $\frac{\partial F}{\partial x} = -3x^2 - 2ax - b = x^2 + b$ (jer je karakteristika $p = 2$). Jednadžba $x^2 + b = 0$ ima jedinstveno rješenje $x = b$, takodjer, postoji jedinstvena točka na E s prvom koordinatom b, i ta je točka singularna.
Od sad je $p \neq 2$ i E je nesingularna ako i samo ako je $D \neq 0$, gdje je D, kao i prije, diskriminanta kubnog polinoma u varijabli x, tj.

$$D := -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$$

. Tada kažemo da je E **eliptička krivulja** nad $\mathbf{F}_p$.
Grupni zakon na eliptičkoj krivulji E definira se analogno kao i u karakteristici nula, kao:
$P_1 + P_2 + P_3 = O$ ako su P_1, P_2, P_3 na jednom pravcu.
Podsjetimo, ako je $y = \lambda x + \mu$ jednadžba pravca kroz $P_1(x_1, y_1),\ P_2(x_2, y_2)$, onda je
$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ za $x_2 \neq x_1$, i $\lambda = \frac{3x_1^2 + 2ax_1 + b}{2y_1}$ za $x_2 = x_1$.
Vidimo da da formula nema smisla za $p = 2$. Dalje, ako je $P_3(x_3, y_3$ onda je $x_3 = \lambda^2 - a - x_1 - x_2;\ y_3 = \lambda x_3 + \mu$ dok $P_1 + P_2$ ima koordinate $(x_3, -y_3)$.
Jasno je da je E abelova grupa s neutralnim elementom elementom O, nadalje skup racionalnih točaka $E(\mathbf{F}_p)$ je **konačna abelova grupa**. Evo nekoliko primjera.
Primjer 2. (i) $E : y^2 = x^3 + x + 1$ nad $\mathbf{F}_5$. Tu je $D = 4$ pa je E eliptička krivulja. Kvadrati u $\mathbf{F}_5$ su $0, 1, 4$ pa se lako dobije da je
$E(\mathbf{F}_5) = \{O, (0, \pm 1), (2, \pm 1), (3, \pm 1), (4, \pm 2)\}$, dakle $|E(\mathbf{F}_5)| = 9$. Lako se provjeri da je riječ o cikličkoj grupi reda 9 (a ne o produktu grupa reda 3).
(ii) $E : y^2 = x^3 - x$ nad $\mathbf{F}_5$. Tu je, opet, $D = 4$ pa je E eliptička krivulja. Dobije se $|E(\mathbf{F}_5)| = 8$.
(iii) $E : y^2 = x^3 + x$ nad $\mathbf{F}_5$. Dobije se $|E(\mathbf{F}_5)| = 4$.

Općenito, stavimo $N_p := |E(\mathbf{F}_p)|$ za eliptičku krivulju E nad konačnim poljem $\mathbf{F}_p$. Kako u $\mathbf{F}_p$ ima pola kvadrata i pola nekvadrata (ne računajući nulu), a E ima jednadžbu oblika $y^2 = f(x)$ za kubni polinom f, intuitivno je jasno da će f (u prosjeku) jednako mnogo puta postizati kvadrate kao i nekvadrate. Dakle, možemo očekivati $2\frac{p-1}{2} = p - 1$ takvih racionalnih točaka. Tome treba dodati beskonačno daleku točku i još jednu (f prosječno postiže

jednom vrijednost nulu) i to je $p+1$ točaka. Kako je to tek u prosjeku, očekujemo da bude

$$p+1-\epsilon \leq N_p \leq p+1+\epsilon$$

za neku grješku ϵ, što se može zapisati i kao

$$|p+1-N_p| \leq \epsilon.$$

Pokazuje se da je zaista tako i da je $\epsilon = 2\sqrt{p}$, što je "zanemarivo" u usporedbi s p (za velike p). Ta je činjenica poznata kao **Hasseova ocjena** ili **Hasse-Weilova ocjena** i može se pokazati da je analogna (još ne dokazanoj **Riemannovoj slutnji**). Dakle vrijedi:

$$|p+1-N_p| \leq 2\sqrt{p}.$$

Naravno da tu jednakost nikad ne nastupa, ali taj se obliki tradicionalno piše jer vrijedi i za svako konačno polje s $q := p^n$ elemenata

$$|q+1-N_q| \leq 2\sqrt{q}.$$

To je specijalni slučaj tvrdnje za krivulje genusa g:

$$|q+1-N_q| \leq 2g\sqrt{q}.$$

(tu je tvrdnju prvi dokazao A.Weil).

Redukcija modulo p.
Vratimo se na eliptičke krivulje nad $\mathbf{Q}$, tj. na krivulje

$$E : y^2 = x^3 + ax^2 + bx + c$$

gdje možemo izabrati da a, bc budu cijeli brojevi. Neka je, kao i prije, D diskriminanta od E.
Podsjetimo da postoji homomorfizam redukcije modulo p sa $\mathbf{Z}$ na $\mathbf{F}_p$, zadan kao $m \mapsto m$ modulo p, što kraće pišemo kao $m \mapsto \bar{m}$ (to vrijedi i za $p = 2$, ali taj slučaj tu ne razmatramo).
Redukcijom modulo p koeficijenata, od E nastaje krivulja nad $\mathbf{F}_p$

$$\bar{E} : y^2 = x^3 + \bar{a}x^2 + \bar{b}x + \bar{c}.$$

To općenito nije eliptička krivulja (jer ne mora biti nesingularna), ali ako je $\bar{D} \neq 0$ u $\mathbf{F}_p$, onda jest. Kako uvjet $\bar{D} \neq 0$ znači da D nije djeljiv s p vidimo

da vrijedi:
Ako p ne dijeli D, onda je $\bar{E}$ eliptička krivulja.
Posebno, $\bar{E}$ je eliptička krivulja za gotovo sve p.
Ne možemo govoriti općenito o redukciji točaka eliptičke krivulje, ali ako su točke s cjelobrojnim koordinatama, onda je to vrlo prirodan postupak (čak ako su i racionalne, ali sad nas to ne zanima). Naime, ako je $(x, y) \in E(\mathbf{Q})$ i $x, y \in \mathbf{Z}$, onda je $(\bar{x}, \bar{y}) \in E(\mathbf{F}_p)$ (bez obzira je li reducirana krivulja nesingularna, naravno uz uvjet da su a, b, c cijeli brojevi).
Kako su racionalne torzijske točke na E nužno s cjelobrojnim koordinatama (opet uz uvjet da su a, b, c cijeli), one se mogu reducirati na $\bar{E}$. Nije teško vidjeti da je preslikavanje redukcije s $E(\mathbf{Q})_{tors}$ u $\bar{E}(\mathbf{F}_p)$ homomorfizam (naravno uz uvjet da je reducirana krivulja $\bar{E}$ nesingularna, tj. eliptička). Razlog je jednostavan: ako su tri točke od E (s cjelobrojnim koordinatama) na jednom pravcu, onda su njihove redukcije takodjer na jednom pravcu (za detalje vidite [S-T]). Zato vrijedi:

Teorem. Preslikavanje redukcije $E(\mathbf{Q})_{tors} \to \bar{E}(\mathbf{F}_p)$ definirano kao

$$(x, y) \mapsto (\bar{x}, \bar{y}),\ i\ O \mapsto \bar{O},$$

je injektivni homomorfizam grupa (uz uvjet da p ne dijeli $2D$).
Dokaz. Sve smo komentirali osim injektivnosti, a ona izravno slijedi iz toga što je preslikavanje redukcije homomorfizam (naime, jezgra je očito samo O).

Teorem govori da za sve osim konačno mnogo prostih p (djelitelja od D) grupu $E(\mathbf{Q})_{tors}$ možemo smatrati podgrupom grupe $E(\mathbf{F}_p)$. Kako je ovu drugu grupu relativno lako računati, tako često dobijemo korisne informacije o torzijskoj grupi. To je naročito korisno kod razmatranja familija eliptičkih krivulja (o čemu će više riječi biti poslije). Sad razmotrimo dva konkretna primjera.

Primjer 3. Za $E : y^2 = x^3 + 3$ je $D = -3^5$ pa je $E(\mathbf{Q})_{tors} \hookrightarrow \bar{E}(\mathbf{F}_p)$ za $p \geq 5$. Nije teško vidjeti da je $|\bar{E}(\mathbf{F}_5)| = 6$ i $|\bar{E}(\mathbf{F}_7)| = 13$. Zato je racionalna torzijska grupa od E trivijalna (Lutz-Nagellovom metodom postupak bi bio složeniji).

Primjer 4. Za $E : y^2 = x^3/43x + 166$ je $D = -2^{15} \cdot 13$ pa je Lutz-Nagellov postupak dosta složen. Nije teško vidjeti da je $|\bar{E}(\mathbf{F}_3)| = 7$, a

kako točka $(3, 8)$ ima red 7 (provjerite), zaključujemo da je $E(\mathbf{Q})_{tors} = \{O, (3, \pm 8), (-5, \pm 16), (11, \pm 32)\}$.

Uvod u aritmetiku eliptičkih krivulja

Točke konačnog reda - 15. lekcija

Vraćamo se na eliptičke krivulje nad poljem racionalnih brojeva, tj. na E s jednadžbama oblika

$$y^2 = x^3 + ax^2 + bx + c = (x - e_1)(x - e_2)(x - e_3) \tag{1}$$

gdje su $a, b, c \in \mathbf{Z}$, a e_j su medjusobno različiti kompleksni brojevi. Sjetimo se oznake

$$E[n] = \{P \in E(\mathbf{C}) : nP = O\}.$$

Već smo vidjeli da su točke O, E_1, E_2, E_3, gdje su $E_i = (e_i, 0)$, rješenja jednadžbe $2P = O$. Lako se vidi da je $E_1 + E_2 = E_3$ itd. pa je $E[2]$ produkt cikličkih grupa drugog reda. Jednako tako, mogli bismo pokazati da je

$$E[3] \cong \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}$$

i da se, kao skup, $E[3]$ sastoji od inleksijskih točaka (fleksova) na E. Geometrijski opisi grupe $E[n]$ za veće n bili bi vrlo složeni. Ipak, vrijedi općenito

$$E[n] \cong \mathbf{Z}/n\mathbf{Z} \oplus \mathbf{Z}/n\mathbf{Z}.$$

Dakle, jednadžba $nP = O$ ima n^2 rješenja koji čine grupu izomorfnu produktu cikličkih grupa reda n. Zato postoje rješenja P_1, P_2 te jednadžbe tako da bude

$$E[n] = \{rP_1 + sP_2 : \ r, s = 0, 1, ..., n - 1\}$$

tj. r, s su cijeli brojevi jednoznačno zadani modulo n.
To najlakše vidimo ako iskoristimo činjenicu da je grupa $E(\mathbf{C})$ izomorfna grupi $\mathbf{C}/L$ za neku rešetku

$$L := \{k\omega_1 + m\omega_2\},$$

gdje su ω_1, ω_2 dva $\mathbf{R}$-linearno nezavisna kompleksna broja. Sad odmah vidimo da je

$$E[n] \cong \{r\frac{\omega_1}{n} + s\frac{\omega_1}{n} : \ r, s = 0, 1, ..., n - 1\},$$

kako smo i trebali.
Nedostatak ovog pristupa jest o tomu što vrijedi samo u karakteristici nula. Ista tvrdnja vrijedi u svakoj karakteristici p, uz uvjet da p ne dijeli n (ako p dijeli n onda vrijedi nešto slično). Za dokaz te tvrdnje (koja vrijedi i u karakteristici 0), analizira se formula za grupni zakon, pa se rekurzivno definiraju ireducibilni polinomi ϕ_n, ψ_n, ω_n u dvije varijable, s cjelobrojnim koeficijentima, tako da ϕ_n i ω_n budu relativno prostis ψ_n, a da za afinu točku $P(x, y)$ bude

$$nP = (\frac{\phi_n(P)}{\psi_n^2(P)}, \frac{\omega_n(P)}{\psi_n^3(P)}).$$

Sad se koristi činjenica da je $nP = O$ ako i samo ako je $\psi_n(P) = 0$ (vidi [S-T] ili [S]).
Vratimo se nad eliptičke krivulje nad $\mathbf{Q}$ i najavimo važan rezultat:
Za takve krivulje E točke iz $E[n]$ imaju za koordinate **algebarske brojeve**. To smo izravno vidjeli za $n = 2$, a relativno lako bismo vidjeli i za $n = 3$. Ako bismo iskoristili one rekurzivno definirane polinome, to bismo lako dokazali i općenito, medjutim dat ćemo drugi dokaz.
Prije dokaza podsjetimo na neke činjenice iz algebarske teorije brojeva.
Za broj $\alpha \in \mathbf{C}$ postoje dvije moguć nosti:
(I) Skup $\{1, \alpha, \alpha^2, ...\}$ nezavisan je nad $\mathbf{Q}$, tj. ako je $f(\alpha) = 0$ i f polinom s racionalnim koeficijentima, onda je $f = 0$.
Tada kažemo da je α **transcendentalan** Na primjer, π je transcendentalan.
(II) Skup $\{1, \alpha, \alpha^2, ...\}$ linearno je nezavisan nad $\mathbf{Q}$. Tada postoji najmanji prirodni broj n tako da $\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ bude linearno nezavisan nad Q, tj. postoji **ireducibilan polinom** f stupnja n nad $\mathbf{Q}$ tako da bude $f(\alpha) = 0$ (taj je f jednoznačno definiran do na umnožak, tj. jedinstven je uz predpostavku da mu je vodeći koeficijent jednak 1 - uočite i to da mu je, zbog ireducibilnosti, slobodni koeficijent različit od nule).
Tada kažemo da je α **algebarski broj** (stupnja n). Algebarski brojevi čine polje - **polje svih algebarskih brojeva**.
Podjela na algebarske i transcendentalne brojeve α ima karakterizaciju i u terminima polja $\mathbf{Q}(\alpha)$. Sjetimo se:
$\mathbf{Q}(\alpha) = [$ **najmanje polje koje sadrži** $\alpha] = \{\frac{g(\alpha)}{h(\alpha)}\}$,
gdje su g, h polinomi nad $\mathbf{Q}$ i $g(\alpha) \neq 0$. Vrijedi:
(I) Ako je α transcendentalan, onda je polje $\mathbf{Q}(\alpha)$ izomorfno polju racionalnih funkcija jedne varijable $\mathbf{Q}(t)$ nad $\mathbf{Q}$. To znači da su za svaka dva transcendalna broja α, β polja $\mathbf{Q}(\alpha)$ i $\mathbf{Q}(\beta)$ izomorfna. Piosebno, to znači da ima

beskonačno mnogo ulaganja polja $\mathbf{Q}(\alpha)$ u polje kompleksnih brojeva.
(II) Ako je α transcendentalan, onda je polje $\mathbf{Q}(\alpha)$ izomorfno prstenu
$\mathbf{Q}[\alpha] =[$ **najmanji prsten koji sadrži** $\alpha] = \{g(\alpha)\}$,
gdje su g polinomi nad $\mathbf{Q}$, što je jednako skupu svih brojeva oblika
$b_0 + b_1\alpha + b_2\alpha^2 + ... + b_{n-1}\alpha^{n-1}$; $bj \in \mathbf{Q}$, uz uvjet $f(\alpha) = 0$ za pripadni ireducibilni poliniom f stupnja n (drugim riječima, svi se nazivnici mogu racionalizirati).

Primjer 1. (i) $\mathbf{Q}(i) = \{a + bi : a, b \in \mathbf{Q}\}$. Tu je $\alpha := i$, $f(x) = x^2 + 1$. Tu je $\frac{1}{a+bi} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i$, pa se svaki nazivnik racionalizira.
(ii) $\mathbf{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbf{Q}\}$. Tu je $\alpha := \sqrt[3]{2}$, $f(x) = x^3 - 2$ (kako se tu svaki nazivnik racionalizira?).
(iii) Ciklotomsko polje generirano petim korijenima iz jedinice je polje $\mathbf{Q}(\zeta) := \{b_0+b_1\zeta+b_2\zeta^2+b_3\zeta^3\}$, gdje su b_j racionalni brojevi, a ζ neki primitivni peti korijen iz jedinice (u ovom slučaju netrivijalni), na primjer $\zeta := \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}$. Tu je $f(x) = x^4+x^3+x^2+x+1$. Analogno je za svaki p-ti korijen iz jedinice, za prosti p, a za složeni je slično.

Za razliku od transcendentalnog slučaja tu je polje $\mathbf{Q}(\alpha)$ (konačnog) stupnja n nad $\mathbf{Q}$ (kao vektorski prostor) i postoji konačno, točnije točno n ulaganje polja $\mathbf{Q}(\alpha)$ u polje $\mathbf{C}$. Naime, neka je

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdot ... \cdot (x - \alpha_n).$$

Tada je α jedan od ovih α_i, a ko je

$$\sigma : \mathbf{Q}(\alpha) \hookrightarrow \mathbf{C}$$

neko ulaganje polja, tj. preslikavanje različito od nule za koje vrijedi $\sigma(x + y) = \sigma(x) + \sigma(y)$ i $\sigma(xy) = \sigma(x)\sigma(y)$ - tj. netrivijalni homomorfizam, onda je:
$0 = \sigma(0) = \sigma(f(\alpha)) = f(\sigma(\alpha))$,
pa je $\sigma(\alpha)$ neki od α_i, dakle n moguńosti. Kako je svako ulaganje σ jednoznačno odredjeno s vrijednošću $\sigma(\alpha)$ vidimo da ima konačno i to točno n ulaganja polja $\mathbf{Q}(\alpha)$ u $\mathbf{C}$.

Primjer 2.(i) Polje $\mathbf{Q}(i) = \{a + bi : a, b \in \mathbf{Q}\}$ ima dva ulaganja u $\mathbf{C}$:
(a) identitet $a + bi \mapsto a + bi$ i (b) konjugiranje $a + bi \mapsto a - bi$.

(ii) Polje $\mathbf{Q}(\sqrt[3]{2})$ ima tri ulaganja u $\mathbf{C}$:
(a) identitet
(b) $a+b\sqrt[3]{2}+c\sqrt[3]{4} \mapsto a+b\sqrt[3]{2}\rho+c\sqrt[3]{4}\bar{\rho}$, odredjeno preslikavanjem $\sqrt[3]{2} \mapsto \sqrt[3]{2}\rho$, gdje je ρ netrivijalni treći korijen iz jedinice.
(c) $a+b\sqrt[3]{2}+c\sqrt[3]{4} \mapsto a+b\sqrt[3]{2}\bar{\rho}+c\sqrt[3]{4}\rho$, odredjeno preslikavanjem $\sqrt[3]{2} \mapsto \sqrt[3]{2}\bar{\rho}$.
(iii) Polje $\mathbf{Q}(\zeta)$ iz prvog primjera ima 4 ulaganja u $\mathbf{C}$, koja se mogu opisati djelovanjem na ζ kao $\sigma_a(\zeta) := \zeta^a$, za $a = 1, 2, 3, 4$.
To je zato što je

$$x^4 + x^3 + x^2 + x + 1 = (x - \zeta)(x - \zeta^2)(x - \zeta^3)(x - \zeta^4).$$

Primjeri (i) i (iii) razlikuju se od (ii). Naime u njima je svaki σ **automorfizam** polja, tj. ulaganje u sama sebe, dok je u (2) to samo identitet, dok druga dva preslikavaju početno polje u dva druga podpolja od $\mathbf{C}$, različita od njega, ali njemu izomorfna.
U prvom slučaju kažemo da je polje **Galoisovo**. Pokazuje se da za svako polje K konačnog stupnja nad $\mathbf{Q}$ (kao vektorski prostor), postoji algebarski broj α stupnja n, tako da bude $K = \mathbf{Q}(\alpha)$ (to je **teorem o primitivnom elementu**). Zato svako Galoisovo polje K stupnja n ima točno n automorfizama. Ti automorfizmi čine grupu s obzirom na **kompoziciju** kao operaciju, to je Galoisova grupa $Gal(K/\mathbf{Q})$.

Primjer 3. U 2. primjeru (i) galoisova grupa je ciklička reda 2, a galoisova grupa u (iii) je ciklička reda 4.
Općenito Galoisove grupe ne moraju biti ni abelove, a kamoli cikličke.

Djelovanje Galoisove grupe na točke eliptičke krivulje.
Ako je

$$E : y^2 = x^3 + ax^2 + bx + c$$

definirana nad $\mathbf{Q}$, K neko Galoisovo polje (konačnog stupnja nad $\mathbf{Q}$) i $P(x, y)$ točka od E s koordinatama iz K (tj. iz $E(K)$), onda za svaki $\sigma \in Gal(K/\mathbf{Q}$ definiramo djelovanje

$$\sigma(P) := (\sigma x, \sigma y).$$

Uz dodatak $\sigma(O) = O$, to je zaista preslikavanje

$$\sigma : E(K) \to E(K).$$

Za to treba dokazati da je $\sigma(P) \in E(K)$. To je lako, naime samo treba znati da σ aditivna i multiplikativna funkcija, te da racionalne brojeve ostavlja na

miru:
$(x, y) \in E(K)$ znači da je $E = y^2 = x^3 + ax^2 + bx + c$ i $x, y \in K$. Zato je $\sigma(y^2) = \sigma(x^3 + ax^2 + bx + c)$, tj. $\sigma(y)^2 = \sigma(x)^+ a\sigma(x)^2 + b\sigma(x) + c$,
što upravo znači da je $(\sigma(x), \sigma(y)) \in E(K)$.

Dakle, σ je dobro definirano preslikavanje, medjutim vrijedi puno više: svaki σ je automorfizam grupe $E(K)$. To znači da je

$$\sigma(P + Q) = \sigma(P) + \sigma(Q)$$

za sve $P, Q \in E(K)$ (to izlazi izravno iz definicije zbrajanja točaka, samo što dosta toga treba provjeriti - vidi [S-T]),
i da je σ injektivan (to je očito jer afine točke preslikava u afine, pa jedino O preslikava u O).

Teorem. Ako je $P \in E(K)$ i $P \in E[n]$, onda je $\sigma P \in E[n]$ za svaki $\sigma \in Gal(K/\mathbf{Q}$.
Dokaz. $P \in E[n]$ znači $nP = O$, pa je $O = \sigma(O) = \sigma(nP) = n\sigma(P)$, jer je σ automorfizam grupe $E(K)$, što znači da $\sigma(P) \in E[n]$.

Uvod u aritmetiku eliptičkih krivulja

Galoisova reprezentacija - 16. lekcija

Polje $K = \mathbf{Q}(E[n])$.
Polazimo od eliptičke krivulje nad poljem racionalnih brojeva, tj. od E s jednadžbom oblika

$$y^2 = x^3 + ax^2 + bx + c \tag{1}$$

gdje su $a, b, c \in \mathbf{Z}$. Njoj je pridružena grupa

$$E[n] = \{P \in E(\mathbf{C}) : nP = O\}.$$

koja ima n^2 elemenata Dakle,

$$E[n] = \{O, (x_1, y_1), (x_2, y_2), ..., (x_m, y_m)$$

za neke kompleksne brojeve $x_1, y_1, x_2, y_2, ..., x_m, y_m$ (tu je $m = n^2 - 1$).
Tim točkama konačnog reda pridruženo je polje K generirano njenim koordinatama

$$K = \mathbf{Q}(E[n]) := \mathbf{Q}(x_1, y_1, x_2, y_2, ..., x_m, y_m).$$

To je polje **konačno generirano nad Q**, ali nije odmah jasno da je ono **konačna stupnja nad Q**, naime nije jasno da su svi x_i, y_i algebarski brojevi. Takodjer, nije odmah jasno da je K Galoisovo. Pokazat ćemo i jedno i drugo.

Teorem 1. (i) Svi x_i, y_i su algebarski brojevi. Posebno, $K = \mathbf{Q}(E[n])$ je polje algebarskih brojeva (konačna stupnja nad $\mathbf{Q}$).
(ii) Polje K je Galoisovo.
Dokaz. (i) Neka je (x, y) bilo koja točka iz $E(\mathbf{C})$. Tada mogu nastupiti dvije mogućnosti. Prva je da su i x i y algebarski brojevi, a druga je da su oba transcendentna. Naime, ako je x algebarski, onda je $\mathbf{Q}(x)$ polje algebarskih brojeva konačna stupnja, a y je drugog stupnja nad tim poljem, pa je i on algebarski (to je standardna činjenica iz teorije proširenja polja). Slično je x trećeg stupnja nad $\mathbf{Q}(y)$, pa je x algebarski ukoliko je to y.
Predpostavimo sad da su x, y oba transcendentna. Tvrdimo da ima beskonačno mnogo ulaganje polja $\mathbf{Q}(x, y)$ u $\mathbf{C}$. Naime, kako je $\mathbf{Q}(x, y) = \{A(x)+B(x)y\}$, gdje su $A(x), B(x)$ racionalne funkcije u varijabli x s racionalnim keficijentima, uz uvjet $y^2 = x^3 + ax^2 + bx + c$ (i taj je prikaz jednoznačan), za svaki

kompleksni transcendentni broj t i $s := \sqrt{t^3 + at^2 + bt + c}$ (gdje po volji biramo jedan od drugih korijena), preslikavanje

$$A(x) + B(x)y \mapsto A(t) + B(t)s$$

je ulaganje (tu $x \mapsto t;\ y \mapsto s$).
Neka je sad $(x, y) \in E[n]$ i neka je $\sigma : \mathbf{Q}(x, y) \hookrightarrow \mathbf{C}$ neko ulaganje. Tada je, kako smo vidjeli, $(\sigma(x), \sigma(y)) \in E[n]$. Zato je $\sigma x = x_i$ i $\sigma y = y_i$, za neke x_i, y_i iz gornjeg popisa. Kako ima samo konačno mogućnosti za $\sigma(x)$ i $\sigma(y)$, postoji samo konačno mnogo takvih σ. Zato x, y ne mogu biti transcendentni, pa su oba algebarski brojevi, kako smo i tvrdili.
Sad je i K konačna stupnja nad $\mathbf{Q}$, jer je generiran s konačno mnogo algebarskih brojeva (standardan zaključak) (ii) Neka je $\sigma : K \hookrightarrow \mathbf{C}$ neko ulaganje. Ono je jednoznačno odredjeno vrijednostima $\sigma(x_i), \sigma(y_i)$ za sve i. Kako su te vrijednosti opet neki x_j, y_j, vrijedi $\sigma(K) = K$, a to upravo znači da je K Galoisovo proširenje.

Analogija izmedju jedinične kružnice $\mathbf{S^1}$ i eliptičkih krivulja.
Postavlja se pitanje zašto je za matematiku relevantno razmatranje polja $K = \mathbf{Q}(E[n])$. Pokušat ćemo skicirati odgovor na to pitanje. Riječ je o jednoj manifestaciji analogije izmedju jedinične kružnice i eliptičkih krivulja, prema kojoj su ta polja viši analogoni ciklotomskih polja.
Topološka razina. Za svaki E, topološki prostor $E(\mathbf{C})$ je torus pa je $E(\mathbf{C}) \cong S^1 \times S^1$ (topološki izomorfizam).
Geometrijska razina. S^1 možemo realizirati u kompleksnoj Gaussovoj ravnini kao skup T kompleksnih rješenja jednadžbe $|z| = 1$. Multiplikativnost apsolutne vrijednosti $|z_1 z_2| = |z_1||z_2|$ uvjetuje grupnu strukturu na T (obično množenje kompleksnih brojeva).
Takodjer, S^1 se može realizirati kao skup **realnih** rješenja $C(\mathbf{R})$ jednadžbe

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

C je afina krivulja definirana nad $\mathbf{Q}$. Prirodna bijekcija izmedju točaka tih dviju realizacija $(x, y) \leftrightarrow x + iy$ prenosi grupnu strukturu na C, tako da vrijedi $(x_1, y_1)(x_2, y_2) = (x_1y_1 - x_2y_2, x_1y_2 + x_2y_1)$.
S obzirom na to da je C definirana nad $\mathbf{Q}$, prirodno je razmatrati eliptičke krivulje E definirane nad $\mathbf{Q}$. I skup E ima grupnu strukturu, ali tek nakon dodavanja beskonačno daleke točke.
Analizom točaka konačnog reda na ovim grupama vidimo:

$T[n] := \{z \in \mathbf{C} : z^n = 1\} \cong \mathbf{Z}/n\mathbf{Z}$ (izomorfizam apstraktnih grupa, ostvaruje se biranjem primitivnog n-tog korijena ζ iz 1 (na primjer $\zeta = e^{\frac{2\pi i}{n}}$), pa pridruživanja $\zeta \mapsto 1$ modulo n ; prva je grupa multiplikativna, a druga aditivna).
Potpuno je analogno s $C(\mathbf{R})[n]$, tj. $C(\mathbf{R})[n] \cong T[n] \cong \mathbf{Z}/n\mathbf{Z}$ (tu samo treba uočiti da na C gledamo samo realne točke).
Kako smo vidjeli, za svaku E (bez obzira je li definirana nad $\mathbf{Q}$ ili nad nekim većim poljem) vrijedi:
$E[n] \cong \mathbf{Z}/n\mathbf{Z} \oplus \mathbf{Z}/n\mathbf{Z}$.
Vidimo da se tu topološka analogija nastavlja i na geometrijskoj razini (uz pravilnu interpretaciju).
Aritmetička razina. Sad ćemo razmatrati koordinate točaka konačnog reda na ovim krivuljama i pripadna polja koja generiraju.
Kod T dobivamo ciklotomska polja $\mathbf{Q}(\zeta)$ koja odavno zauzimaju važno mjesto u aritmetici (na primjer, Gauss ih je iskoristio za rješenje problema konstrukcije pravilnih mnogokuta). U terminima tih polja Kronecker i Weber su u drugoj polovici 19. st. opisali abelova proširenja od $\mathbf{Q}$, tj. takva Galoisova polja L za koje je Galoisova grupa $Gal(L/\mathbf{Q})$ abelova:
$L/\mathbf{Q}$ je abelovo ako i samo ako je sadržano u nekom ciklotomskom polju $\mathbf{Q}(\zeta)$.
Viši analogoni ciklotomskih polja $\mathbf{Q}(\zeta)$ trebala bi biti polja $K = \mathbf{Q}(E[n])$ (ili njima vrlo bliska). Kronecker je, s obzirom na uočenu analogiju, puno očekivao od $\mathbf{Q}(E[n])$ za eliptičke krivulje nad $\mathbf{Q}$ - njegov *Jugendtraum* (mladenački san) bio je da pomoću njih opiše abelova proširenja kvadratno imaginarnih polja (i znao je to provesti na primjerima). Tako je nastala **teorija kompleksnog množenja** kojim je to i ostvareno.
Napomenimo da nije odmah jasno da baš $\mathbf{Q}(E[n])$ pravilno poopćuju ciklotomska polja $\mathbf{Q}(\zeta)$. Na primjer, eliptičke krivulje E (odnosno njihove jednadžbe) više sliče krivulji C, medjutim kod nje gledamo samo realne točke konačnog reda a kod E gledamo sve. Ako usporedjujemo $C[n]$ i $T[n]$ aritmetički (a ne samo kao apstraktne grupe), i ako svaku točku $(x, y) \in C[n]$ gledamo pridruženu točku $z = x + iy \in T[n]$, onda je prirodno usporedjivati polja $\mathbf{Q}(x, y)$ i $\mathbf{Q}(z)$ koja su bliska, ali ne jednaka. Vidimo da je $\bar{z} \in T[n]$, takodjer, pa je

$$x = \frac{1}{2}(z + \bar{z});\ y = \frac{1}{2i}(z - \bar{z})$$

pa je $\mathbf{Q}(i, x, y) = \mathbf{Q}(i, z)$.
Jošu veća očekivanja od polja $\mathbf{Q}(E[n])$ imali matematičari druge polovice

20. st. Nadali su se da će ih ona dovesti do netrivijalnih opisa **neabelovih proširanja** od **Q** i do tzv. neabelovih **zakona reciprociteta**. U okviru toga bilo je i rješenje slutnje Taniyama-Shimure, koja je za posljedicu imala rješenje Fermatova problema.

Reprezentacija Galoisove grupe $Gal(K/\mathbf{Q}$ **na** $E[n]$.
U ovome dijelu je fiksirana eliptička krivulja E nad $\mathbf{Q}$ i prirodan broj n. Kako smo vidjeli, postoji Galoisovo polje $\mathbf{Q}(E[n])$, generiran koordinatama točaka iz $E[n]$. Fiksirajmo i dva nezavisna rješenja P_1, P_2 jednadžbe $nP = O$ tako da je

$$E[n] = \{rP_1 + sP_2 : \ r, s = 0, 1, ..., n-1\}$$

tj. r, s su cijeli brojevi jednoznačno zadani modulo n.
Zato $E[n]$ možemo identificirati skupom svih dvodimenzionalnih vektora stupaca

$$\begin{bmatrix} \text{r} \\ \text{s} \end{bmatrix}.$$

Tako, na primjer, točkama P_1, P_2 odghovaraju vektori $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$, $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$.

Kako vrijedi $\sigma(P+Q) = \sigma(P) + \sigma(Q)$, a onda i $\sigma(mR) = m\sigma(R)$ za sve točke $P, Q, R \in E[n]$ i svaki $\sigma \in Gal(K/\mathbf{Q}$, vidimo da je $\sigma(rP_1 + sP_2) = r\sigma(P_1) + s\sigma(P_2)$, za sve $r, s \in \mathbf{Z}/n\mathbf{Z}$, pa svaki σ djeluje poput **linearnog operatora** na gornjem vektorskom prostoru (točnije na slobodnom $\mathbf{Z}/n\mathbf{Z}$-modulu ranga 2).
Zato svakom σ jednoznačno pridružujemo 2×2 matricu $\rho_n(\sigma)$ s koeficijentima iz $\mathbf{Z}/n\mathbf{Z}$. Naime, jednoznačno su odredjeni $\alpha, \beta, \gamma, \delta \in \mathbf{Z}/n\mathbf{Z}$, tako da bude

$$\sigma(P_1) = \alpha P_1 + \gamma P_2; \ i \ \sigma(P_2) = \beta P_1 + \delta P_2.$$

Sad definiramo

$$\rho_n(\sigma) := \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$$

Djelovanje od σ na vektoru

$$\begin{bmatrix} \text{r} \\ \text{s} \end{bmatrix}$$

ostvaruje se običnim množenjem matrica

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} \mathrm{r} \\ \mathrm{s} \end{bmatrix}$$

sad vidimo da vrijedi

$$\rho_n(\tau \circ \sigma) = \rho_n(\tau) \cdot \rho_n(\sigma).$$

Takodjer vidimo da je

$$\rho_n(\sigma_0) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

gdje je σ_0 identički automorfizam.

Odavde dobijemo $I = \rho_n(\sigma^{-1} \circ \sigma) = \rho_n(\sigma^{-1}) \cdot \rho(\sigma)$, pa su sve $\rho_n(\sigma)$ invertibilne matrice tj. iz $Gl_2(\mathbf{Z}/n\mathbf{Z})$ i vrijedi

$$\rho_n(\sigma^{-1}) = (\rho_n\sigma)^{-1}.$$

Treba napomenuti da ovdje, za razliku od matrica nad poljem, uvjet invertibilnosti matrice A nije $det(A) \neq 0$ već $det(A) \in (\mathbf{Z}/n\mathbf{Z})^\star$, tj. da je $det(A)$ invertibilan, (izravne račune pogledajte u [S-T]).

Formuliramo važan teorem.
Teorem 2. $\rho_n : Gal(K/\mathbf{Q}) \to Gl_2(\mathbf{Z}/n\mathbf{Z})$ je injektivna **reprezentacija grupa**.

Da je ρ_n reprezentacija upravo znači $\rho_n(\tau \circ \sigma) = \rho_n(\tau) \cdot \rho_n(\sigma)$, za svaka dva τ, σ i $\rho_n(\sigma_0) = I$, što smo već vidjeli. Ostaje pokazati injektivnost, što je gotovo očito, jer ako je $\rho_n(\sigma) = I$, onda je $\sigma(P_1) = P_1$ i $\sigma(P_2) = P_2$ pa je $\sigma(P) = P$ za sve P, tj. $\sigma = \sigma_0$.

Uvod u aritmetiku eliptičkih krivulja

Galoisova reprezentacija, primjeri - 17. lekcija
Eliptičke krivulje s kompleksnim množenjem 18. lekcija

Opisat ćemo primjere Galoisovih grupa $G = Gal(K/\mathbf{Q}$ pridruženih točkama drugog ili četvrtog reda nekih eliptičkih krivulja, i pripadne grupe matrica.

Primjer 1. Neka je $E : y^2 = x^3 - x$ i $n = 2$. Tada je $E[2] = \{O, (0,0), (1,0), (-1,0),$ pa je $K = \mathbf{Q}(E[2]) = \mathbf{Q}$ i $G = \sigma_0$ je jedinična grupa. Takodjer $\rho_2(\sigma_0) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, bez obzira koje smo P_1, P_2 izabrali.

Primjer 2. Neka je $E : y^2 = x^3 + x$ i $n = 2$. Tada je $E[2] = \{O, (0,0), (i,0), (-i,0),$ pa je $K = \mathbf{Q}(E[2]) = \mathbf{Q}(i)$ i $G = \sigma_0, \sigma$, gdje je σ kompleksno konjugiranje. Znamo da je $\rho_2(\sigma_0) = I$ bez obzira koje smo P_1, P_2 izabrali. Neka je $P_1 = (0,0)$ i $P_2 = (i,0)$. Tada je $\sigma(P_1) = P_1$ i $\sigma P_2 = (-i,0) = P_1 + P_2$ pa je $\rho_2(\sigma) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$.
Da smo izabrali $P_1 = (i,0),\ P_2 = (-i,0)$, bilo bi $\sigma P_1 = P_2$ i $\sigma P_2 = P_1$ pa bi bilo $\rho_2(\sigma) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.

Primjer 3. Neka je $E : y^2 = x^3 + x$ i $n = 4$. Da bismo odredili $E[4]$ napišimo formulu za dupliciranje. Dobijemo, ako je $P(x,y)$, onda je

$$2P = (\frac{x^4 - 2x^2 + 1}{4y^2}, \frac{x^6 + 5x^4 - 5x^2 - 1}{8y^3}).$$

Sad zaključujemo ovako: $4P = O$ akko $2(2P) = O$ a to je akko $y(2P) = 0$ tj. $x^6+5x^4-5x^2-1 = 0$. Rješenja te jednadžbe jesu $1, -1$ te rješenja bikvadratne jednadžbe $x^4 + 6x^2 + 1 = 0$, tj. $\pm\alpha, \pm\alpha^{-1}$, gdje je $\alpha := (\sqrt{2} - 1)i$. Ako još stavimo $\beta := (1 + i)(\sqrt{2} - 1)$, dobijemo:
$E[4] = \{O, (0,0), (\pm i, 0), (1, \pm\sqrt{2}),$
$(-1, \pm i\sqrt{2}), (\alpha, \pm\beta), (-\alpha, \pm i\beta), (\alpha^{-1}, \pm\alpha^{-2}\beta), (-\alpha^{-1}, \pm i\alpha^{-2}\beta)\}$.
Vidimo da je

$$K = \mathbf{Q}(E[4]) = \mathbf{Q}(i, \sqrt{2}) = \{a + bi + c\sqrt{2} + d\sqrt{2}i : a, b, c, d \in \mathbf{Q}\},$$

proširenje četvrtog stupnja. Vidimo dalje da je

$$G := Gal(K/\mathbf{Q} = \{\sigma_0, \sigma, \tau, \sigma\tau\},$$

umnožak cikličkih grupa drugog reda σ_0, σ i σ_0, τ, gdje je:
$\sigma(i) = -i,\ i\ \sigma(\sqrt{2}) = \sqrt{2}$ i $\tau(i) = i,\ i\ \tau(\sqrt{2}) = -\sqrt{2}$.
Vidimo da vrijedi $\sigma\tau = \tau\sigma$ i da taj automorfizam mijenja predznak i od i i od $\sqrt{2}$.
Da bismo odredili ρ_4 treba izabrati bazu P_1, P_2. Prve tri navedene točke su iz $E[2]$ pa nisu dobre. Neka je $P_1 = (1, \sqrt{2})$ i $P_2 = (\alpha, \beta)$. To je baza od $E[4]$.
Naime, $2P_1 = (0, 0),\ 3P_1 = (1, -\sqrt{2}) = -P_1,\ 4P_1 = O$. Takodjer,
$2P_2 = (i, 0),\ 3P_2 = (\alpha, -\beta) = -P_2,\ 4P_2 = O$.
Vidimo dalje $\sigma P_1 = P_1,\ \sigma P_2 = (-\alpha, -i\beta)$, dok je
$\tau P_1 = -P_1,\ \tau P_2 = (\alpha^{-1}, \alpha^{-2}\beta)$.
Odredite $\rho_4(\sigma)$ i $\rho_4(\tau)$ u toj bazi.

Primjer 4. Neka je $E : y^2 = x^3 - 2$ i $n = 2$. Vidimo da je
$E[2] = \{O, (\sqrt[3]{2}, 0), (\rho\sqrt[3]{2}, 0), (\bar{\rho}\sqrt[3]{2}, 0)\}$,
gdje je ρ primitivni treći korijen iz jedinice, na primjer $\rho = -\frac{1}{2} + \frac{\sqrt{-3}}{2}$ (uočite da je $\bar{\rho} = \rho^2$ - taj broj treba razlikovati od reprezentacije ρ_n). Tada je
$K = \mathbf{Q}(E[2]) = \mathbf{Q}(\rho, \sqrt[3]{2}) = \mathbf{Q}(\sqrt{-3}, \sqrt[3]{2})$. To je proširenje šestog stupnja (kompozit proširenja drugog i trećeg stupnja). Galoisova grupa je simetrična grupa S_3, konkretnije:
$Gal(K/\mathbf{Q} = \{\sigma_0, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$, gdje su σ, τ definirani tako da bude:
$\sigma(\sqrt[3]{2}) := \rho\sqrt[3]{2},\ \sigma(\sqrt{-3}) = \sqrt{-3}$ i $\tau(\sqrt[3]{2}) := \sqrt[3]{2},\ \tau(\sqrt{-3}) = -\sqrt{-3}$
Izravno se provjeri da je $\sigma^3 = \tau^2 = \sigma_0$, i da je $\tau\sigma = \sigma^2\tau$ i $\tau\sigma^2 = \sigma\tau$.
Na primjer, $\tau\sigma^2(\sqrt[3]{2}) = \tau\sigma(\rho\sqrt[3]{2}) = \tau(\rho^2\sqrt[3]{2}) = (\bar{\rho})^2\sqrt[3]{2} = \rho\sqrt[3]{2}$, dok je $\sigma\tau(\sqrt[3]{2})\sigma(\sqrt[3]{2} = \rho\sqrt[3]{2}$, pa se ta dva automorfizma poklapaju na $\sqrt[3]{2}$. Slično bismo dobili s $\sqrt{-3}$ itd.
Stavimo $P_1 = (\sqrt[3]{2}, 0)$ i $P_2 = (\rho\sqrt[3]{2}, 0)$. Tada je P_1, P_2 baza od $E[2]$ i $P_1 + P_2 = (\bar{\rho}\sqrt[3]{2}, 0)$.
Vidimo da je $\sigma(P_1) = P_2,\ \sigma(P_2) = P_1 + P_2$ i da je $\tau(P_1) = P_1 + P_2$. Zato je
$\rho_2(\sigma) = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ i $\rho_2(\tau) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$.
Sad se lako dobije da je $\rho_2(\sigma^2) = (\rho_2(\sigma))^2 = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$, $\rho_2(\sigma\tau) = \rho_2(\sigma)\rho_2(\tau) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, i, konačno $\rho_2(\sigma^2\tau) = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$.

Vidimo da smo dobili da je $\rho_2(G) = Gl_2(\mathbf{Z}/2\mathbf{Z})$, odnosno da su u slici sve moguće matrice nmad poljem od dva elementa.
Sad je relativno lako provjeriti da je G simetrična grupa S_3, točnije da je njoj izomorfna (tako što se pokaže da je $\rho_2(G)$ izomorfna S_3). Što se tiče strukture podgrupa od G, element σ generira cikličku grupu (koja odgovara alternativnoj grupi A_3 i ona je normalna), dok $\tau, \sigma\tau, \sigma^2\tau$ generiraju cikličke poodgrupe 2. reda (koje nisu normalne). Na primjer,
$(\sigma\tau)^2 = \sigma\tau\sigma\tau = \sigma\sigma^2\tau\tau = \sigma_0$.
Izravna realizacija grupe G kao S_3, jest da ona permutira skup $\{\sqrt[3]{2}, \sqrt[3]{2}\rho, \sqrt[3]{2}\rho^2\}$.

To je bio prvi primjer u kojemu konstruirano polje K nije bilo abelovo. Naime, kako smo vidjeli, grupa S_3 nije abelova (to je najmanja neabelova grupa). To je ujedno bio i prvi primjer kad je slika grupe G pri reprezentaciji ρ_n čitava opća linearna grupa nad brojevima modulo n. Može se pokazati (iako ne lako) da je to pravilo, a ne izuzetak (s obzirom na eliptičke krivulje, a na neki način, i na brojeve n). Naime, eliptičke krivulje dijelimo na one s **kompleksnim množenjem**, tj. koje imaju netrivijalne homomorfizme (endomorfizme)

$$\phi : E \to E$$

(nad $\mathbf{Q}$, a i općenito, one su rijetkost), i ostale. Trivijalni homomorfizmi su oni oblika $P \mapsto mP$ za $m \in \mathbf{Z}$. J.P.Serre je dokazao da za svaku eliptičku krivulju nad $\mathbf{Q}$ bez kompleksnog množenja postoji prirodan broj N tako da za sve $n \geq N$ koji su relativno prosti s N vrijedi $\rho_n(G) = Gl_2(\mathbf{Z}/n\mathbf{Z})$.
Kako su grupe $Gl_2(\mathbf{Z}/n\mathbf{Z})$ neabelove (osim za $n = 1$), tako smo dobili mnogo neabelovih proširenja od $\mathbf{Q}$ (pridruženih eliptičkim krivuljama).

Treba napomenuti da Primjer 4 nije dobar za ilustraciju Serreova rezultata. Naime, $E : y^2 = x^3 - 2$ je eliptička krivulja s kompleksnim množenjem. Zaista, preslikavanje

$$\phi : E \to E;\ (x, y) \mapsto (\rho x, y)$$

je automorfizam od E, što se izravno provjeri (tu je, opet, ρ primitivni treći korijen iz 1).
On je zato različit od svakog preslikavanja $P \mapsto mP$, pa je to primjer kompleksnog množenja.
Ovdje treba uočiti da je polje $\mathbf{Q}(E[3])$ abelovo nad poljem $\mathbf{Q}(\rho)$ (upravo poljem nad kojim je definirano kompleksno množenje). Može se pokazati da

slično vrijedi za sve eliptičke krivulje s kompleksnim množenjem, naime da su pripadne grupe abelove ili "gotovo abelove".

Sad ćemo samo skicirati jedan primjer, koji upotpunjuje Primjere 1, 2 i 3. Za detalje pogledajte [S-T, str. 191].

Primjer 5. Neka je $E : y^2 = x^3 + x$ i $n = 3$. Koristeći se duplikacijskom formulom iz Primjera 3. i činjenicom da $3P = O$ ako i samo ako je $2P = -P$, dobije se da je G nekomutativna grupa reda 16 (inače $Gl_2(\mathbf{Z}/3\mathbf{Z})$ ima 48 elemenata, pa tu slika od G nije maksimalna.

Eliptičke krivulje s kompleksnim množenjem.

U nastavku ćemo se poslužiti identifikacijom kompleksnih eliptičkih krivulja s kompleksnim torusima $\mathbf{C}/L$ da bismo opisali eliptičke krivulje s kompleksnim množenjem i njihove endomorfizme.

Sjetimo se da za svaku kompleksnu eliptičku krivulju E postoji dvostruko periodna funkcija $\mathcal{P}$ (s rešetkom perioda $L := \{r\omega_1 + s\omega_2$ gdje su r, s cijeli brojevi, a ω_1, ω_2 dva izabrana nezavisna perioda), tako da preslikavanje kompleksne ravnine

$$z \mapsto (\mathcal{P}(z), \mathcal{P}'(z))$$

postaje analitički izomorfizam izmedju $\mathbf{C}/L$ i $E(\mathbf{C})$ (tu treba pravilno tretirati beskonačno daleke točke, a E napisati u posebnom obliku). Naime, tu pripadnu krivulju E treba predočiti jednadžbom, tradicionalno pisanom kao

$$y^2 = 4x^3 - g_2x - g_3$$

što se uvijek može, a g_2, g_3 jednoznačno su odredjeni s L.
Kako su $\mathcal{P}, \mathcal{P}'$ analitičke kompleksne funkcije osim točkama rešetke L, analitičnost gornjeg preslikavanja, upravo znači da su gornje koordinatne funkcije analitičke. Kako vidimo, to i jest, ali za $\mathbf{C}/L\setminus\{\tilde{0}\}$ i afine točke na $E(\mathbf{C})$, tj na $E(\mathbf{C}) \setminus \{\mathbf{O}\}$ (tu smo s tildom označili klase kompleksnih brojeva modulo L, i napomenimo da ima malo problema s dokazivanjem surjektivnosti gornjeg preslikavanja).
Ostaje vidjeti da se preslikavanje analitički produžuje i na neutralne elemente, tj. na okoline oko nule u torusu odnosno od O u eliptičkoj krivulji. Oko O su, kako smo vidjeli, koordinate (u, v) pri čemu je $O = (0, 0)$, a izvan O vrijedi
$(u, v) = (\frac{x}{y}, \frac{1}{y})$.
Kako je $(x, y) = (\mathcal{P}(z), \mathcal{P}'(z))$ za z oko 0 (ili, što je ekvivalentno za z oko nekog elementa od L), onda je

$$z \mapsto (\frac{\mathcal{P}'(z)}{\mathcal{P}(z)}, \frac{1}{\mathcal{P}'(z)})$$

analitičko preslikavanje iz otvorene okoline 0 (bez nule), u otvorenu okolinu od O (bez O). Medjutim, kako $\mathcal{P}$ ima u 0 pol 2. reda, a $\mathcal{P}'$ pol 3. reda, vidimo da su prekidi u gornjim razlomcima za $z = 0$ uklonjivi, pa se preslikavanje

produljuje po analitičnosti i na 0, s vrijednošću O, kako smo i trebali.
Tome treba dodati da je ova anlitička bijekcija medju točkama kompleksnog torusa i $E(\mathbf{C})$ ujedno i izomorfizam grupa. To proizlazi iz transformacijskih svojstava funkcija $\mathcal{P}, \mathcal{P}'$ s jedne strane i definicije grupnog zakona na na E (odnosno pripadnih formula).

Sad je svakom (netrivijalnom) endomorfizmu

$$\phi : E \to E$$

jednoznačno pridružen analitički endomorfizam

$$f : \mathbf{C}/L \to \mathbf{C}/L$$

(to da je f analitički upravo znači da se lokalno zapisuje analitičkim funkcijama). Razlog tomu ješto se endomorfizam oko svake točke zapisuje racionalnim funkcijama (kojima se nazivnik ne poništava u toj točki), a to onda kod torusa prelazi u analitičke funkcije.
Netrivijalniji je dio da svakom analitičkom endomorfizmu f torusa odgovara racionalno preslikavanje kod eliptičkih krivulja (s grupnom strukturom nema problema). Općenito ova se problematika najbolje opisuje u terminima Riemannovih ploha, ali mi ćemo postapak provesti izravno. Na malim okolinama U, V oko 0 u $\mathbf{C}$ funkcija f odredjuje običnu analitičku funkciju
$F : U \to V$ tako da je $F(0) = 0$ (jer f klasu od nule preslikava u klasu od nule).
Nadalje f je homomorfizam pa je

$$F(z_1 + z_2) - F(z_1) - F(z_2) \in L$$

za sve $z_1, z_2 \in U$ tako da je i $z_1 + z_2 \in U$. Kako u V ima samo konačno mnogo elemenata od L, možemo ga smanjiti (U takodjer - sve to jer je F neprekinuta) tako da tu bude samo 0 i da svaki rezultat $t_3 - t_1 - t_2$ za $t_1, t_2, t_3 \in V$ bude u krugu oko 0 koji od L sadrži samo 0. Tada će biti

$$F(z_1 + z_2) = F(z_1) + F(z_2)$$

za svaka dva $z_1, z_2 \in U$ tako da je i $z_1 + z_2 \in U$. Fiksirajmo sad $z_0 \in U$. Neka je U' mali otvoreni krug oko 0 u U, takav da je za svaki $z \in U'$ ispunjeno da je $z + z_0 \in U$. Tada je

$$F(z + z_0) = F(z) + F(z_0),$$

za svaki $z \in U'$. Sad je
$F'(z_0) := \lim_{h\to 0} \frac{F(z_0+h)-F(z_0)}{h}$,
a kako h možemo uzimati iz U' i kako je $F(0) = 0$, dobijemo $F'(z_0) = F'(0)$ (tu smo koristili da je f analitičko preslikavanje, pa je F analitička funkcija). Kako to možemo uraditi za svaki $z_0 \in U$ vidimo da postoji kompleksan broj $c \neq 0$ tako da bude
$F(z) = cz$, za sve $z \in U$. Zato je (uz dogovor da tildom označavamo klase modulo L i podsjećanje da je $\tilde{(}z + t) = \tilde{z} + \tilde{t}$ i $m\tilde{z} = \tilde{(}mz)$):
$f(\tilde{z}) = \tilde{cz}$ za $\tilde{z}$ oko $\tilde{0}$.
Dalje, neka je sad $z \in \mathbf{C}$ bilo koji. Tada postoji n tako da $\frac{z}{n} \in U$, pa je $f(\tilde{(}\frac{z}{n})) = (\tilde{c\frac{z}{n}})$, odakle se množenjem s n i uzimajući u obzir da su f i tilda homomorfizmi dobije $f(\tilde{z}) = \tilde{cz}$, tj.

$$f(z \text{ modulo } L) = cz \text{ modulo } L.$$

Posebno, za svaki $\omega \in L$ vrijedi $\tilde{0} = f(\tilde{0}) = f(\omega) = \tilde{c\omega}$, što znači da c nije bilo kakav, već da vrijedi

$$cL \subset L.$$

Sad je sve spremno za opisivanje endomorfizama eliptiqv ckih krivulja (nad kompleksnim brojevima).

Kompleksno množenje eliptičkih krivulja. Taj pojam ima smisla u svakoj karakteristici, ali mi se ograničavamo na karakteristiku 0.

Teorem 1. (i) Skup endomorfizama $End(\mathbf{C}/L)$ od $\mathbf{C}/L$ je u bijekciji sa skupom svih kompleksnih brojeva c sa svojstvom $cL \subset L$.
(ii) Skup endomorfizama je komutativni prsten s 1 obzirom na zbrajanje i kompoziciju (koji se kod pripadnih kompleksnih brojeva svode na zbrajanje i množenje).
(iii) $End(\mathbf{C}/L)$ je podprsten prstena cijelih brojeva u nekom kvadratno imaginarnom polju.
Taj podprsten sadrži $\mathbf{Z}$, a ako sadrži nešto više, onda je eliptička krivulja s kompleksnim množenjem.

Napomenimo prije dokaza da (iii) govori da je kompleksno množenje rijetkost.
Dokaz. (i) Prema predhodnom razmatranju, ostaje pokazati samo jedan smjer (jednostavniji), naime da svaki kompleksni broj c sa svojstvom $cL \subset L$

odredjuje endomorfizam. To je upravo endomorfizam f zadan kao $f(\tilde{z}) = \tilde{cz}$. Uvjet $cL \subset L$ omogućuje da je f dobro definiran, tj. da klasa od nule odlazi u klasu od nule. Sad ostaje samo uočiti da različiti takvi c odredjuju različite endomorfizme (a to je lako).
(ii) Za zbrajanje je jasno; takodjer je jasno da je kompozicija dobro definirana operacija. Jedino ostaje komutativnost. Neka endomorfizmima f, g odgovaraju kompleksni brojevi c, d. Tada je
$(g \circ f)(\tilde{z}) := g(f(\tilde{z})) = g(\tilde{(cz)} = \tilde{(dcz)} = \tilde{(cdz)} = (f \circ g)(\tilde{z})$.
(iii) Neka je L generirana s ω_1, ω_2 i neka c odgovara nekom f, tj. neka je $cL \subset L$, tj. vrijedi
$c\omega_1 = A\omega_1 + B\omega_2;\ c\omega_2 = C\omega_1 + D\omega_2$,
za neke cijele A, B, C, D. Stavimo $\tau := \frac{\omega_1}{\omega_2}$ i napomenimo da τ nije realan. Sad dobijemo
$c\tau = A\tau + B;\ c = C\tau + D$, odakle izlazi $C\tau^2 + D\tau = A\tau + B$, tj.

$$(C\tau)^2 + (D - A)(C\tau) - CD = 0,$$

odakle vidimo da $C\tau$ cijeli kvadratno imaginarni broj (jer nije realan). Kako je $c = C\tau + D$ vidimo da je i c cijeli kvadratno imaginaran broj.
Napomenimo da činjenica da je τ kvadratno imaginaran govori da je kompleksno množenje rijetkost (naime, τ je omjer perioda ω_1, ω_2, pa može biti gotovo svaki broj, a kvadratno imaginarnih prema svima ima zanemarivo malo - ta se tvrdnja može još preciznije izreći).
Takodjer, vidi se da $EndE$ uvijek sadrži $\mathbf{Z}$.

Uvod u aritmetiku eliptičkih krivulja

Abelova proširenja od $\mathbf{Q}(i)$ - 19. lekcija

Opisat ćemo na primjeru eliptičke krivulje $E : y^2 = x^3 + x$ Kroneckerov Jugendtraum. Podsjetimo da Kronecker-Weberov teorem tvrdi da je svako Galoisovo proširenje $K/\mathbf{Q}$ (tj. takvo kojemu je Galoisova grupa abelova) sadržano u nekom ciklotomskom, tj. generiranom nekim korijenom iz jedinice (drugim riječima generirano vrijednošću $e^{\frac{2\pi i}{m}}$, za neki cijeli m, periodne analitičke funkcije $z \mapsto e^{2\pi iz}$ - s temeljnim periodom 1).
Naravno da je prirodno tražiti analogan rezultat za abelova proširenja K/k, gdje je k neko (konačno) proširenje od $\mathbf{Q}$, a najjednostavniji su slučajevi kad je k kvadratno proširenje od $\mathbf{Q}$. Poznato je da se kvadratna proširenja dijele na kvadratno realna i kvadratno imaginarna. Pokazuje se da je problem s kvadratno realnim puno tvrdji i do danas je vrlo nejasan, dok je, na osnovi primjera, Kronecker postavio slutnju da za kvadratno imaginarna proširenja funkciju $z \mapsto e^{2\pi iz}$ treba zamijeniti dvostrukoperiodnim Weiestrassovim funkcijama $\mathcal{P}$, $\mathcal{P}'$, za zgodno odabranu rešetku L perioda (vrlo gruba formulacija). Geometrijskim jezikom govoreći točke konačnog reda na jediničnoj kružnici (koje odgovaraju vrijednostima $e^{\frac{2\pi i}{m}}$) treba zamijeniti točkama konačnog reda na korespondirajućim eliptičkim krivuljama nad $\mathbf{Q}$. Da kažemo nešto preciznije, te eliptičke krivulje treba birati medju eliptičkim krivuljama s kompleksnim množenjem i to, ako je k pripadno kvadratno imaginarno polje, onda biramo eliptičke krivulje koje imaju kompleksno množenje s cjelim brojevima tog polja (vidite 18. lekciju).
U našem primjeru bit će $k := \mathbf{Q}(i)$, a pripadna eliptička krivulja

$$E : y^2 = x^3 + x$$

Tu smo eliptičku krivulju izabrali jer ona ima kompleksno množenje s i, tj.

$$\phi : E \to E;\ \phi(x, y) = (-x, iy)$$

je endomorfizam različit od svakog množenja $[m]$ s cijelim brojevima $P \mapsto mP$. Lako se pokaže da je ϕ i automorfizam od E. Naime, za $P = (x, y)$ je $(\phi \circ \phi)(P) = \phi(-x, iy) = (-(-x), i(iy)) = (x, -y) = -P$, pa je $\phi^{-1} = -\phi$.
Treba uočiti da ϕ nije definiran nad $\mathbf{Q}$ već nad $\mathbf{Q}(i)$. Nadalje, za sve cijele brojeve m, n, pripadno preslikavanje $m + n\phi$ definirano kao $(m + n\phi)(P) :=$

$mP + n\phi(P)$ je endomorfizam od E. Može se pokazati da je time prsten endomorfizama $EndE$ izomorfan prstenu cijelih Gaussovih brojeva $\mathbf{Z}[i]$, ali to nam sad nije važno, dovoljno će biti razmatranje s automorfizmom ϕ.
Podsjetimo najprije na primjere (uz oznaku $K_n := \mathbf{Q}(E[n])$). Vidjeli smo u predhodnoj lekciji da je:
(I) $K_2 = \mathbf{Q}(i) = k$, pa je $Gal(K/\mathbf{Q})$ ciklička grupa reda 2 (dakle abelova), a $Gal(K/k)$ je trivijalna (dakle abelova),
(II) $K_4 = \mathbf{Q}(i, \sqrt{2})$, pa je $Gal(K/\mathbf{Q})$ umnožak ciklička grupa reda 2 (dakle abelova), a $Gal(K/k)$ je trivijalna (dakle abelova),
(III) $K_3 = \mathbf{Q}(i, \beta)$, gdje je $\beta = \sqrt[4]{\frac{8\sqrt{3}-12}{9}}$ i pokazuje se da je $GalK/\mathbf{Q}$ **neabelova** grupa reda 16 (vidi [S-T, str.191]), a za $Gal(K/k)$ može se pokazati da je abelova.
Dakle $K_n/\mathbf{Q}$ općenito nije abelovo, a tvrdnja je (odnosno dio tvrdnje) da je K_n/k abelovo za sve n.
Izravno računanje je već za $n = 3$ mukotrpno i netrivijalno. Opći rezultat odakle će slijediti i ovaj posebni dokazat ćemo poslije. Tvrdnju lakše možemo ilustrirati za eliptičku krivulju $y^2 = x^3 - 2$ već za $n = 2$ (vidi predhodnu lekciju, samo što je u tom slučaju $k = \mathbf{Q}(\rho)$).
Prije nastavka komentirajmo dvije činjenice.
Prva je da polje K_n sadrži $\mathbf{Q}(i)$ za svaki $n \geq 2$. Naime, ako je $P = (x, y)$ i $nP = O$, onda je
$O = nP = \phi(np) = n\phi(P)$, pa je $\phi P \in E[n]$, čim je $P \in E[n]$.
Kako je $\phi(P) = (-x, iy)$, zaključujemo da je $y \in K_n$ i $iy \in K_n$, pa je $i \in K_n$ čim je $y \neq 0$. Ako je pak $y = 0$, za sve točke, onda je $n = 2$, pa podsjetimo da je $K_2 = \mathbf{Q}(i)$.
Važna posljedica jest to da je

$$K_n := \mathbf{Q}(E[n]) = \mathbf{Q}(i)(E[n]).$$

Druga ječinjenica dio osnovnog teorema Galoisove teorije, naime ako su k, K dva Galoisova (konačna) proširenja od $\mathbf{Q}$ i ako je $k \subseteq K$, onda je K/k takodjer Galoisovo (to je očito iz definicije), i sljedeći niz Galoisovih grupa je egzaktan (koji je nama važan samo za k kvadratno imaginarno, ili, još uže, za $k = \mathbf{Q}(i)$)

$$\{1\} \to Gal(K/k) \to Gal(K/\mathbf{Q}) \to Gal(k/\mathbf{Q}) \to \{1\}.$$

Tu je $\{1\}$ jedinična grupa generirana identitetom (označavali smo je i kao σ_0). Takodjer, $Gal(K/k) \to Gal(K/\mathbf{Q})$ je prirodno ulaganje grupa (nama

ovaj rezultat iz Galoisove teorije ne treba za razmatranje, već samo za bolje shvaćanje tvrdnje, naime velika grupa $Gal(K/\mathbf{Q})$ općenito ne mora biti abelova, a njena podgrupa $Gal(K/k)$ indeksa 2 mora). Preslikavanje $Gal(K/\mathbf{Q}) \to Gal(k/\mathbf{Q})$ prirodna je surjekcija dobivena restrikcijom automorfizama s K na k, i još nam je manje važno za daljnje razmatranje.

Formulirajmo sad tvrdnje.

Teorem 1. Neka je $E : y^2 = x^3 + x$ i $K_n := \mathbf{Q}(i)(E[n])$ za $n \in \mathbf{N}$ (a vidjeli smo da je $K_n = \mathbf{Q}(E[n])$ za $n \geq 2$). Tada je $K_n/\mathbf{Q}(i)$ Galoisovo abelovo proširenje.

Ta je tvrdnja analogna (gotovo trivijalnoj) tvrdnji da je ciklotomsko proširenje $\mathbf{Q}(e^{\frac{2\pi i}{n}})/\mathbf{Q}$ Galoisovo abelovo, za svaki prirodni n.
Ono što je netrivijalno jest obrat te tvrdnje, a to je Kronecker-Weberov teorem. Formulirajmo njen analogon i u ovoj složenijoj situaciji.

Teorem 2. Neka je $F/\mathbf{Q}(i)$ Galoisovo abelovo proširenje. Tada je $F \subseteq K_n := \mathbf{Q}(i)(E[n])$ za neki $n \in \mathbf{N}$, gdje je $E[n]$ skup rješenja jednadžbe $nP = O$ na eliptičkoj krivulji $E : y^2 = x^3 + x$.

Mi ćemo dokazati samo Teorem 1, a Teorem 2 je pretežak za dokazivanje na ovoj razini. Opet napomenimo da obje tvrdnje vrijede za svako kvadratno imaginarno polje k, a ne samo $\mathbf{Q}(i)$, samo se treba pravilno formulirati, na primjer za $k := \mathbf{Q}(\rho)$ treba gledati eliptičku krivulju $E : y^2 = x^3 + 1$, ili neku njoj srodnu (ima i dodatnih problema, na primjer općenito treba dodati vrijednost j-funkcije, što ovdje ne treba jer je $j(E) = 0$). Analogon teorema 1 relativno je lako dokazati, dok je analogon teorema 2 bitno teži.

Dokaz teorema 1. Možemo gledati samo za $n \geq 2$. To da je $K_n/\mathbf{Q}(i)$ Galoisovo je evidentno (naime $K_n/\mathbf{Q}$ je Galoisovo). Ono što je netrivijalno jest to da je $K_n/\mathbf{Q}(i)$ abelovo.
Sjetimo se injektivne reprezentacije $\rho_n : Gal(\mathbf{Q}(E[n])/\mathbf{Q}) \to Gl_2(\mathbf{Z}/n\mathbf{Z})$.
Kako je $G := Gal(\mathbf{Q}(i)(E[n])/\mathbf{Q}(i)) \subset Gal(\mathbf{Q}(E[n])/\mathbf{Q})$, onda s ρ_n označimo i restrikciju te reprezentacije na tu podgrupu (i ona je takodjer injektivna). Zato, da bismo dokazali da je G abelova, dovoljno je dokazati da je $\rho_n(G)$ abelova grupa.

Redom vrijedi:
(I) Automorfizam ϕ (kompleksno množenje) preslikava $E[n]$ u $E[n]$ i to je preslikavanje aditivno i linearno (s obzirom na množenje s cijelim brojevima modulo n). Naime $\phi(nP) = n\phi(P)$, pa ρ_n možemo proširiti i na ϕ. Zato je automorfizmu ϕ pridružena (invertibilna) matrica

$$\rho_n(\phi) = A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in Gl_2(\mathbf{Z}/n\mathbf{Z}).$$

(II) ϕ komutira sa svakim elementom $\sigma \in G$. Naime, za $(x, y) = P \in E(K_n)$ vrijedi $\phi(\sigma(P)) = \phi(\sigma x, \sigma y) = (-\sigma x, i\sigma y) = (\sigma(-x), \sigma(iy)) = \sigma(\phi(P))$ (tu smo iskoritili da je $\sigma(i) = i$).
Zato matrica A komutira sa svakom matricom $\rho_n(\sigma)$ za $\sigma \in G$. Ta će činjenica biti presudna za konačan zaključak.
(III) Postoji baza od $E[n]$ oblika $\{P, \phi(P)\}$ za neku točku $P \in E[n]$.
Ako bismo znali da je to istina bili bismo gotovi. Naime u toj bazi bi bilo

$$\rho_n(\phi) := A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},$$

jer je $\phi(P) = 0 \cdot P + 1 \cdot \phi(P)$ i $\phi(\phi(P)) = -P = (-1)P + 0 \cdot \phi(P)$.
Sad, ako je $B = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in Gl_2(\mathbf{Z}/n\mathbf{Z})$ bilo koja matrica sa svojstvom $AB = BA$, onda je

$$B = \begin{bmatrix} \alpha & \beta \\ -\beta & \alpha \end{bmatrix}.$$

Zato skup svih invertibilnih matrica B sa svojstvom $AB = BA$ čini abelovu grupu (izravna provjera).
Kako je $\rho_n(G)$ podgrupa te grupe i ona je abelova.
Zato je preostalo pokazati da postoji takva baza. To se izravno vidi iz toga što je $E(\mathbf{C})$ izomorfna kvocijentu $\mathbf{C}/L$ gdje je L najjednostavnija moguća rešetka $L := \{r + si : r, s \in \mathbf{Z}\}$ (tj. L je razapeta s 1 i i). Naravno, pri tom izomorfizmu, endomorfizmi od E prelaze u endomorfizme od $\mathbf{C}/L$, a to su svi cijeli Gaussovi brojevi (kao skup poklapaju se s L). Endomorfizmi koji su automorfizmi prelaze u invertibilne cijele Gaussove brojeve, a to su $-1, 1, -i, i$. Kako je ϕ automorfizam njemu je pridružen broj i ili broj $-i$ (1 nije jer ϕ nije identitet, a -1 nije jer ϕ nije preslikavanje $T \mapsto -T$). Ako u $\mathbf{C}/L$ gledamo jednadžbu $nz = 0$, a upravo ona odgovara jednadžbi $nT = O$

u E, dobijemu bazu rješenja $\{\frac{1}{n}, \frac{i}{n}\}$, takodjer i bazu $\{\frac{1}{n}, \frac{-i}{n}\}$, a jedna od njih u E odgovara bazi oblika $\{P, \phi(P)\}$, gdje točka P odgovara broju $\frac{1}{n}$.
Za preciznu formulaciju izomorfizma izmedju E i torusa $\mathbf{C}/L$ vidi [S-T, zad. 6.21. na str. 219]. Za dokaz podsjetimo da smo u 3. lekciji pokazali da je $\mathbf{C}/L$ izomorfna s eliptičkom krivuljom C zadanom jednadžbom $y^2 = 4x^3 - g_2 x$ gdje je $g_2 > 0$ (to nije previše bitno). Izravnom provjerom (množimo jednadžbu od C s $\frac{16}{(2i\sqrt{g_2})^3}$) vidimo da je preslikavanje

$$(x, y) \mapsto (\frac{4x}{2i\sqrt{g_2}}, \frac{4y}{(\sqrt{2i\sqrt{g_2}})^3})$$

izomorfizam izmedju C i E.

Uvod u aritmetiku eliptičkih krivulja

l-adski brojevi - 20. lekcija

U elementarnoj teoriji brojeva (koja se bavi cijelim i racionalnim brojevima) postoje tri važne konstrukcije.
Prva je razmatranje ostataka modulo m, za neki cijeli broj m (različit od $0, -1, 1$). Taj je skup konačan prsten koji ima djelitelje nule, osim ako je m prost, kada je polje. Postoji prirodni surjektivni homomorfizam s prstena cijelih brojeva na prsten ostataka modulo m.
Druga je smještanje prstena cijelih brojeva u prsten cijelih algebarskih brojeva. Na primjer, izraz $a^2 + b^2$ ne može se rastaviti nad cijelim brojevima, dok na cijelim gaussovim brojevima vrijedi $a^2 + b^2 = (a + bi)(a - bi)$.
Treća je smještanje prstena cijelih brojeva u prsten $\mathbf{Z}_p$ cijelih p-adskih brojeva, za svaki prosti broj p. Pri tom se polje racionalnih brojeva smješta u polje p-adskih brojeva $\mathbf{Q}_p$. Sa stanovišta analize konstrukcija p-adskih brojeva analogna je konstrukciji realnih brojeva iz racionalnih (upotpunjenju), samo što se tu upotpunjenje vrši u tzv. p-adskoj apsolutnoj vrijednosti. S algebarskog stanovišta riječ je o razmatranju "uskladjenih" kongruencija modulo p^n za svaki prirodni broj n. Tu ćemo važnu konstrukciju opisati u sljedeće dvije lekcije, samo što ćemo umjesto oznake p za proste brojeve, koristiti oznaku l. Prije opisa te konstrukcije dat ćemo još jedan, čisto algebarski, dokaz komutativnosti Galoisove grupe $Gal(K_n/\mathbf{Q}(i))$ iz predhodne lekcije, u kojemu će se nazrijeti ta konstrukcija.

Eliptička krivulja $E : y^2 = x^3 + x$ ima kompleksno množenje s i, preciznije

$$\phi : E \to E;\ \phi(x, y) = (-x, iy)$$

je endomorfizam različit od svakog množenja $[m]$ s cijelim brojevima $P \mapsto mP$. Vidjeli smo da je ϕ i automorfizam od E.

Teorem 1. Neka je $E : y^2 = x^3 + x$ i n prirodan broj. Tada postoji baza od $E[n]$ nad $\mathbf{Z}/n\mathbf{Z}$) oblika $(P, \phi P)$.
Dokaz. Neka je (P, Q) bilo koja baza za ϕ i neka je u toj bazi automorfizmu ϕ pridružena (invertibilna) matrica

$$\rho_n(\phi) = A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in Gl_2(\mathbf{Z}/n\mathbf{Z}).$$

To znači da je $\phi(P) = aP + cQ$ i $\phi(Q) = cP + dQ$, taj je prikaz jednoznačan za brojeve a, b, c, d modulo n. Sad dokaz provodimo u nekoliko koraka.
(I) Dovoljno je pokazati da postoji takva baza za koju je c invertibilan modulo n, tj. da je $(c, n) = 1$ (analogno za b). Naime, tada bi $(P, \phi P)$ bila dobra baza. Za to je dovoljno provjeriti da relacija $r\phi(P) = sP$ implicira $r = s = 0$ modulo n. Iz $\phi(P) = aP + cQ$ slijedi $r\phi(P) = arP + crQ$, a kad bi bilo $r\phi(P) = sP$ bilo bi $cr = s - ar = 0$, a kako je c invertibilan, bilo bi $r = 0$, a onda i $s = 0$.
(II) Ako je $n = l$, prost broj, tvrdnja teorema vrijedi. Možemo predpostaviti da je $l \neq 2$, jer za $l = 2$ imamo dobru bazu $((i, 0), (-i, 0))$ koja je oblika $(P, \phi(P))$.
Sad dokaz provodimo tako da predpostavimo da po volji odabrana baza (P, Q) ne zadovoljava (I), tj. da automorfizmu ϕ odgovara matrica

$$\begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix}$$

s koeficijentima iz polja ostataka modulo l. Zato bi u bazi $(P + Q, Q)$ automorfizam ϕ imao matricu

$$\begin{bmatrix} a & 0 \\ d - a & d \end{bmatrix}.$$

Ta matrica zadovoljava (I), što je nama dovoljno. Naime, u suprotnom bi bilo $d = a$, a odatle bi bilo $\phi(T) = T$ za sve T. Posebno bi bilo $\phi(P) = aP$ i $\phi(\bar{P}) = a\bar{P}$, za bazni element $P = (u, v)$. Odatle bismo dobili

$$\overline{\phi(\bar{P})} = aP$$

jer je kompleksno konjugiranje kao preslikavanje na $E[l]$ takodjer linearno prelikavanje (kao i svaki element Galoisove grupe). Sad je:
$aP = \overline{\phi(\bar{u}, \bar{v})} = \overline{(-\bar{u}, i\bar{v})} = (-u, -iv) = -(-u, iv) = -\phi(P)$.
Zaključujemo da je $-a = a$ pa je, zbog neparne karakteristike, $a = 0$, što je kontradikcija.
(III) Ako tvrdnja teorema vrijedi za n, ona vrijedi i za nl. Dokaz dijelimo u dva dijela, ovisno o tome je li n djeljiv s l ili nije.
(i) $l|n$.
Neka je (P, Q) dobra baza za $E[n]$, tj. neka u toj bazi preslikavanje ϕ ima matricu

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \text{ modulo } n.$$

Neka je par (P', Q') bilo koji sa svojstvom $lP' = P$ i $lQ' = Q$ (takvi parovi zaista postoje). Tvrdimo da je (P', Q') baza za $E[nl]$, a za to je dovoljno pokazati da iz $rP' = sQ'$ slijedi $r = s = 0$ modulo nl. Množenjem relacije $rP' = sQ'$ s l dobijemo $rP = sQ$, odakle slijedi $r = s = o$ modulo n. Sad samo treba pokazati da je $r = s = n$ modulo nl nemoguće. Zaista, kad bi tako bilo, bilo bi;
$r = \alpha n$ i $s = \beta n$ za neke $\alpha, \beta = 0, 1, ..., l - 1$.
Sad bismo iz $\alpha n P' = \beta n Q'$ dobili $(\alpha \frac{n}{l})P = (\beta \frac{n}{l})Q$, a odatle $\alpha = \beta = 0$, što je kontradikcija.
Dakle (P', Q') je baza na $E[nl]$ pa neka ϕ u toj bazi ima matricu

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ modulo } nl.$$

Odatle je $\phi(P') = aP' + cQ'$ pa je $\phi(P) = \phi(lP') = laP' + lcQ' = aP + bQ$, a kako je $\phi(P) = Q$, zaključujemo da je $c = 1$ modulo n, posebice c je invertibilan modulo n, pa prema (I) zaključujemo da ima dobra baza za $E[nl]$.
(ii) l ne dijeli n.
Neka je (P, Q) dobra baza za $E[n]$ i neka je (P_l, Q_l) dobra baza za $E[l]$.
Neka su, dalje, P_1, Q_1 jedinstvene točke iz $E[n]$ za koje je $lP_1 = P$ i $lQ_1 = Q$ (one postoje jer l ne dijeli n, a zato su i jedinstvene).
Sad definiramo

$$(P', Q') := (P_1 + P_l, Q_1 + Q_l).$$

Tvrdimo da je (P', Q') baza za $E[nl]$. Za dokaz, kao i prije, predpostavimo da je $rP' = sQ'$ i dokažimo da je $r = s = 0$ smodulo nl.
;Množenjem gornje jednakosti s l dobijemo $rP = sQ$, pa je $r = s = 0$ modulo n.
Množenjem, pak, s n dobijemo $rnP_l = snQ_l$ pa je, jer l ne dijeli n, $rP_l = sQ_l$, odnosno $r = s = 0$ modulo l.
Sve skupa daje $r = s = 0$ modulo nl.
Sad kad znamo da je (P', Q') baza za $E[nl]$, neka preslikavanju ϕ u toj bazi odgovara matrica

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ modulo } nl.$$

Odatle, slično kao u (i) dobijemo

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \text{ modulo } n.$$

Jednako tako dobijemo

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \text{ modulo } l.$$

Te dvije relacije za posljedicu imaju da je c relativno prost s nl, pa prema (I) postoji dobra baza za $E[nl]$.
Dokaz završavamo primjedbom da je (II) baza indukcije, a (III) korak indukcije s obzirom na broj prostih faktora od n.

Pojava l-adskih brojeva. Pri dokazu teorema, dio (III), pojavila se konstrukcija baze za $E[nl]$ iz baze za $E[n]$ tako da ako je preslikavanju ϕ na $E[nl]$ bila pridružena matrica $\begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}$ modulo nl, odnosno matrica $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ modulo n na $E[n]$, onda je vrijedilo

$$\begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ modulo } n.,$$

što znači da je $a' = a$ modulo n, $b' = b$ modulo n, itd. Tu treba uočiti i to da je a' zadan modulo nl, a a modulo n, itd.
Posebno, ako gledamo samo (III) (i), kad $l|n$, onda možemo startati s $n = l$, pa nastaviti s $l^2, l^3, ...$, tj. gledati module točaka konačnog reda
$E[l], E[l^2], E[l^3], ..., E[l^n], E[l^{n+1}], ...,$
onda na njima tako možemo izabrati baze da pripadne matrice za ϕ ali i za bilo koje drugo linearno preslikavanje budu redom
$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$ modulo l, $\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$ modulo l^2, $\begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix}$ modulo $l^3, ...$
i da bude $a_2 = a_1$ modulo l, $a_3 = a_2$ modulo l^2, itd. (a isto i za $b_1, b_2, b_3, ...$ itd.).
Dakle, pojavio se niz brojeva

$$(a_1, a_2, a_3, ...)$$

takav da je n-ta koordinata zadana modulo l^n i da za svaki prirodni n bude $a_{n+1} = a_n$ modulo l^n. Takvi se nizovi zovu l-adski brojevi i o njima govorimo u sljedećoj lekciji.

Uvod u aritmetiku eliptičkih krivulja

Konstrukcija i svojstva l-adskih brojeva - 21. lekcija

Definicija. Neka je l fiksiran prost broj i neka n prolazi skupom prirodnih brojeva. **Cijeli** l-adski broj je, prema definiciji, niz brojeva

$$a = (a_1, a_2, a_3, ...)$$

takav da je n-ta koordinata zadana modulo l^n i da za svaki prirodni n bude $a_{n+1} = a_n$ modulo l^n.

Ovo je jedna od konstrukcija cijelih l-adskih brojeva (inače uobičajeno je govoriti o p-adskim brojevima, ali u ovom kontekstu povijesno se pojavljuje oznaka l). Vrijedi sljedeće:
(i) Definicija jednakost cijelih l-adskih brojeva. Dva su cijela l-adska broja $a = (a_1, a_2, a_3, ...)$ i $b = (b_1, b_2, b_3, ...)$ jednaka ako je $a_n = b_n$ za sve n.

(ii) Skup svih cijelih l-adskih brojeva (oznaka $\mathbf{Z}_l$) je komutativni prsten s jedinicom uz neutralni element $0 := (0, 0, 0, ...)$, suprotni element $-a := (-a_1, -a_2, -a_3, ...)$, $1 := (1, 1, 1, ...)$, te uz pokomponentno zbrajanje i množenje, tj.
$a + b := (a_1 + b_1, a_2 + b_2, a_3 + b_3, ...)$; $ab := (a_1b_1, a_2b_2, a_3b_3, ...)$.
Lako se pokaže da je sve dobro definirano i da svojstva vrijede (tu je bitno da je prirodno preslikavanje s cijelih brojeva modulo l^{n+1} na cijele brojeve modulo l^n homomorfizam prstena - koji je ujedno i surjekcija). Na primjer, ako je $a_{n+1} = a_n$ modulo l^n i $b_{n+1} = b_n$ modulo l^n, onda je i $a_{n+1}b_{n+1} = a_nb_n$ modulo l^n.

(iii) Prsten cijelih brojeva $\mathbf{Z}$ prirodno se ulaže u prsten cijelih l-adskih brojeva preko $m \mapsto (m, m, m, ...)$. Od sad ćemo l-adski broj $(m, m, m, ...)$ jednostavno označavati kao m. Posebice, pisat čemo $m(a_1, a_2, a_3, ...)$ umjesto $(ma_1, ma_2, ma_3, ...)$.

(iv) Svaki se cijeli l-adski broj $(a_1, a_2, a_3, ...)$ različit od nule jednoznačno zapisuje kao $l^r(b_1, b_2, b_3, ...)$ gdje je r prirodan broj ili 0, a $(b_1, b_2, b_3, ...)$ je l-adski broj sa svojstvom $b_1 \neq 0$ modulo l.

za dokaz neka je $r+1$ prvi indeks n za koji je $a_n \neq 0$ modulo l^n. Dakle, $a_r = 0$ modulo l^r, pa je i $a_{r+1} = 0$ modulo l^r. Zato je $a_{r+1} = l^r b_1$ gdje je $b_1 \neq 0$ modulo l. Dalje $a_{r+2} = a_{r+1}$ modulo l^{r+1} pa je i a_{r+2} djeljiv s l^r. Slično je a_{r+2} djeljiv s l^r itd. Zato su dobro definirani brojevi $b_2, b_3, ...$ tako da bude

$$a = l^r(b_1, b_2, b_3, ...).$$

Kako je $l^r b_k = a_{r+k}$, za sve k, vrijedi $l^r b_{k+1} = l^r b_k$ modulo l^{r+k}, pa je $b_{k+1} = b_k$ modulo l^k, što znači da je sve dobro definirano.

(v) $\mathbf{Z}_l$ je prsten bez djelitelja nule. To proizlazi izravno iz (iv), jer ako su a, c različiti od nule, onda je
$a = l^r(b_1, b_2, b_3, ...)$ i $c = l^s(d_1, d_2, d_3, ...)$, gdje su $b_1, d_1 \neq o$ modulo l. Kako je $ad = l^{r+s}(b_1d_1, b_2d_2, b_3d_3, ...)$ i kako je $b_1d_1 \neq 0$ modulo l , zaključujemo da je $ab \neq 0$.

(vi) $a = l^r(b_1, b_2, b_3, ...)$ je invertibilan ako i samo ako je $r = 0$ i $b_1 \neq 0$ modulo l. Drugim riječima $a = (a_1, a_2, a_3, ...)$ je invertibilan ako i samo ako je $a_1 \neq 0$.
Jedan je smjer očit: ako je a invertibilan, mora tako biti. Za obrat, ako je $r = 0$, onda $a = (b_1, b_2, b_3, ...)$, a kako je $b_1 \neq 0$, postoji cijeli c_1 takav da je $b_1c_1 = 1$ modulo l. Posebno $c_1 \neq 0$ modulo l. Kako je $b_2 = b_1$ modulo l, vidimo da je b_2 invertibilan modulo l^2. Zato postoji cijeli broj c_2 sa svojstvom $b_2c_2 = 1$ modulo l^2. Slično konstruiramo brojeve c_3, c_4 itd. tako da vrijedi $b_nc_n = 1$ modulo l^n za sve n. Tada je $c := (c_1, c_2, ...)$ inverz od a. Da to dokažemo dovoljno je vidjeti da je c zaista cijeli l-adski broj. Treba vidjeti da je $c_2 = c_1$ modulo l, zatim da je $c_3 = c_2$ modulo l^2 itd. Zaista:
$c_2 - c_1 = \frac{1}{a_2} - \frac{1}{a_1} = \frac{a_1 - a_2}{a_1 a_2} = 0$ modulo l. Slično:
$c_3 - c_2 = \frac{1}{a_3} - \frac{1}{a_2} = \frac{a_2 - a_3}{a_2 a_3} = 0$ modulo l^2 itd.
Uočite da smo usput dokazali i to da je $a := (a_1, a_2, ...)$ invertibilan ako i samo ako su svi a_n invertibilni.

(vii) Prsten $\mathbf{Z}_l$ ima jedinstveni prosti ideal (koji je onda ujedno i maksimalan). To je glavni ideal generiran s l, tj. $\mathcal{P}_l := l\mathbf{Z}_l = \{a \in \mathbf{Z}_l : a_1 = 0\}$ modulo l.
Lako se dokazuje da $\mathbf{Z}_l/\mathcal{P}_l \equiv \mathbf{Z}/l\mathbf{Z}$.

(viii) Prema (v) dobro je definirano polje razlomaka $\mathbf{Q}_l$ od $\mathbf{Z}_l$. Vidimo

da se svaki element od $\mathbf{Q}_l$ jednoznačno zapisuje kao

$$l^r u$$

gdje je r cijeli broj, a u je invertibilan element od $\mathbf{Z}_l$.

Primjer. Znamo da jednadžba $x^2 = 2$ nema rješenja u polju racionalnih brojeva $\mathbf{Q}$.
(A) Ta jednadžba nema rješenja u $\mathbf{Q}_3$. Dovoljno je pokazati da ona nema rješenja u $\mathbf{Z}_3$. Naime, kad bi $a := (a_1, a_2, ...)$ bilo rješenje te jednadžbe, bilo bi $a_1^2 = 2$ modulo 3, a to je nemoguće.
(B) Ta jednadžba ima rješenja u $\mathbf{Z}_7$. Naime, kako je $2 = 3^2$ modulo 7, možemo staviti $a_1 = 3$. Za a_2 možemo staviti 10 jer je $10 = 3$ modulo 7 i $10^2 = 2$ modulo 7^2 itd.
Da pokažemo da to uvijek možemo sprovesti, predpostavimo da smo konstruirali dobre $a_1, a_2, ..., a_n$. Dakle, vrijedi $a_n^2 = 2 + m7^n$ za neki cijeli m. Tada stavimo

$$a_{n+1} = a_n + k7^n$$

pri čemu ćemo k izabrati tako da bude $a_{n+1}^2 = 2$ modulo 7^{n+1}. Dakle, treba biti
$a_n^2 + 2a_n k7^n + k^2 7^{2n} = 2$ modulo 7^{n+1}, a za to je dovoljno da bude $m + 2a_n k = 0$ modulo 7,
tj. $k = m$ modulo 7.
Napomenimo da smo ovako pokazali da se polje $\mathbf{Q}(\sqrt{2})$ ne može smjestiti u $\mathbf{Q}_3$, ali da se to polje može smjestiti u $\mathbf{Q}_7$. Govoreći malo neprecizno $\sqrt{2} \notin \mathbf{Q}_3$, ali $\sqrt{2} \in \mathbf{Q}_5$.

U sljedečoj lekciji ova če nam konstrukcija poslužiti za opis tzv. l-adske reprezentacije Galoisove grupe u grupu regularnih matrica s koeficijentima u $\mathbf{Z}_l$.

Uvod u aritmetiku eliptičkih krivulja

Konstrukcija l-adske reprezentacije Galoisove grupe pridružene eliptičkoj krivulji - 22. lekcija

Fiksirajmo:
prost broj l
eliptičku krivulju E nad $\mathbf{Q}$.
Podsjetimo na niz abelovih grupa indeksiranih prirodnim brojevima n:
$E[l^n] := \{T \in E(\mathbf{C}) : l^n T = O\} \cong \mathbf{Z}/l^n\mathbf{Z} \oplus \mathbf{Z}/l^n\mathbf{Z}$,
ovo posljednje znači da je $E[l^n]$ slobodni modul ranga 2 nad prstenom ostataka $\mathbf{Z}/l^n\mathbf{Z}$, posebno, ta grupa ima n^2 elemenata.
Za svaki n postoji **prirodan** surjektivni homomorfizam množenja s l:
$[l] : E[l^{n+1}] \to E[l^n]$, $T_{n+1} \mapsto lT$, za $T_{n+1} \in E[l^{n+1}]$.
Definiramo **Tateov modul** $T_l(E)$ kao skup svih nizova točaka konačnog reda na E uskladjenih ovim homomorfizmima. Preciznije

$$T_l(E) := \{T = (T_1, T, 2, T_3, ...) : T_n \in E[l^n],\ i\ lT_{n+1} = T_n,\ \text{za sve } n\}.$$

Uočite sličnost s konstrukcijom cijelih l-adskih brojeva. Opet je riječ o inverznom limesu, tj. $T_l(E)$ je inverzni limes modula $E[l^n]$. Iz te opće konstrukcije slijedi da je $T_l(E)$ slobodan modul ranga 2 nad prstenom cijelih brojeva, medjutim to se vidi i izravno. Naime,
(i) uz zbrajanje po komponentama $T_l(E)$ je očito abelova grupa s neutralnim elementom $\mathcal{O} = (O, O, O, ...)$ i suprotnim elementom $-T := (-T_1, -T, 2, -T_3, ...)$.
(ii) $T_l(E)$ je $\mathbf{Z}_l$-modul uz pokomponentno množenje, tj.

$$aT = (a_1, a_2, a_3, ...)(T_1, T_2, T_3, ...) := (a_1T_1, a_2T_2, a_3T_3, ...).$$

Lako se može dokazati da je taj modul slobodan i ranga 2 (jer svaki od $T_l(E)$ slobodan ranga 2), medjutim dokaz ćemo na kratko izostaviti, a poslije ćemo izravno konstruirati bazu.
Prednost rada s modulom $T_l(E)$ umjesto s beskonačno modula $E[l^n]$ upravo je u tome što je to modul nad komutativnim prstenom s jedinicom bez djelitelja nule pa se može prijeći na vektorske prostore nad poljem. Tu je konstrukciju predložio Tate pedesetih godina 20. st.

Podsjetimo na polja generirana s $E[l^n]$ (uz nešto potpunije oznake):
$K_{E,l,n} = \mathbf{Q}(E[l^n])$:= polje definirano nad $\mathbf{Q}$ koordinatama točaka iz $E[l^n]$.
Vidjeli smo da je to konačno Galoisovo proširenje od $\mathbf{Q}$ jer su koordinate točaka iz $E[l^n]$ algebarski brojevi.
Kako je $E[l] \subset E[l^2] \subset ...$, vrijedi
$\mathbf{Q}(E[l]) \subset \mathbf{Q}(E[l^2]) \subset ...$, tj.
$K_{E,l,1} \subset K_{E,l,2} \subset ....$ Uvedimo oznaku:
$K_{E,l} := \bigcup_{n\geq 1} K_{E,l,n}$. Polje $K_{E,l}$ je algebarsko Galoisovo (beskonačnog stupnja). Naime, neka je $\sigma : K_{E,l} \hookrightarrow \mathbf{C}$ ulaganje polja. Treba pokazati da je $\sigma(K_{E,l}) = K_{E,l}$. Neka je $x \in K_{E,l}$, tada postoji n tako da bude $x \in K_{E,l,n}$, pa je $\sigma(x) = (\sigma|K_{E,l,n})(x) \in K_{E,l,n} \subset K_{E,l}$ (jer je $K_{E,l,n}$ Galoisovo.
Imamo, dakle, Galoisovu grupu $\mathrm{Gal}(K_{E,l}/\mathbf{Q})$, pridruženu krivulji E i prostom broju l.
Kako izgleda ta grupa?. Prije svega, ona je beskonačna. Kako je $K_{E,l,n} \subset K_{E,l}$, za svaki n, imamo prirodni homomorfizam (restrikciju):
$\mathrm{Gal}(K_{E,l}/\mathbf{Q}) \to \mathrm{Gal}(K_{E,l,n}/\mathbf{Q})$, $\sigma \mapsto \sigma|K_{E,l,n} := \sigma_n$,
s veće (beskonačne) grupu na manju, konačnu (dodatno je svojstvo da je ta restrikcija surjektivna,što je opće svojstvo Galoisovih grupa - naime automorfizam se uvijek može proširiti s Galoisova polja na Galoisovo proširenje).
Dakle, svakom σ pridružen je niz $(\sigma_1, \sigma_2, ...)$ gdje je $\sigma_n := \sigma|K_{E,l,n}$.
Taj je niz restrikcija uskladjen, tj. vrijedi $\sigma_{n+1}|K_{E,l,n} = \sigma_n$ za sve n. Automorfizam σ jednoznačno je odredjen tim restrikcijama, što opravdava oznaku

$$\sigma = (\sigma_1, \sigma_2, ...)$$

(to je jednakost u projektivnom limesu, naime $\mathrm{Gal}(K_{E,l}/\mathbf{Q})$ je projektivni limes konačnih grupa $\mathrm{Gal}(K_{E,l,n}/\mathbf{Q})$ - što mi tu nećemo koristiti već sve izravno računati).
Da to dokažemo, uočimo da svaki uskladjeni niz automorfizama $(\sigma_1, \sigma_2, ...)$ jednoznačno odredjuje automorfizam σ polja $K_{E,l}$, prema formuli $\sigma(x) := \sigma_n(x)$ za $x \in K_{E,l}$, gdje je n bilo koji indeks za koji vrijedi $x \in K_{E,l,n}$ (koji postoji jer je $K_{E,l}$ unija konačnih polja $K_{E,l,n}$ - treba uočiti da definicija ne ovisi ozboru indeksa n, što je posljedica uskladjenosti).
Podsjetimo da smo imali niz reprezentacija Galoisovih grupa (uz malo potpunije oznake)

$$\rho_{E,l,n} : \mathrm{Gal}(K_{E,l,n}/\mathbf{Q}) \to \mathrm{Aut}E[l^n]$$

u grupu automorfizama modula $E[l^n]$ (samo što smo prije te automorfizme odmah zapisivali kao 2×2 matrice - nakon izbora baze u $E[l^n]$). Ta je

reprezentacija definirana ovako: neka je $\sigma_n \in \mathrm{Gal}(K_{E,l,n}/\mathbf{Q})$ i neka je $(x_n, y_n) = T_n \in E[l^n]$ afina točka; tada je

$$(\rho_{E,l,n}\sigma_n)(T_n) = \sigma_n(T_n) := (\sigma_n x_n, \sigma_n y_n)$$

(naravno $(\rho_{E,l,n}\sigma_n)(O) := O$, gdje je O neutralni element - beskonačno daleka točka).
Reprezentacije $\rho_{E,l,n}$ su uskladjene u smislu: ako je $lT_{n+1} = T_n$, onda je

$$l(\rho_{E,l,n+1}\sigma_{n+1})(T_{n+1}) = (\rho_{E,l,n}\sigma_n)(T_n).$$

Zato je dobro definirana reprezentacija

$$\rho_{E,l} : \mathrm{Gal}(K_{E,l}/\mathbf{Q}) \to \mathrm{Aut}T_l(E)$$

$(\rho_{E,l}\sigma)(T) := ((\rho_{E,l,1}\sigma_1)(T_1), (\rho_{E,l,2}\sigma_2)(T_2), ...)$,
gdje je $\sigma = (\sigma_1, \sigma_2, ...)$ i $T = (T_1, T_2, ...)$.
Da to sve konkretiziramo, prijedjimo na matrice, a za to je dovoljno odabrati uskladjene baze u modulima $E[l^n]$. To se može napraviti na više načina. Evo jedne takve konstrukcije.
Izaberimo bazu (P_1, Q_1) za $E[l]$, tj. $E[l] = \{rP_1 + sP_2 : r, s \in \mathbf{Z}/l\mathbf{Z}\}$.
Tada možemo (vidjeli smo) izabrati bazu za (P_2, Q_2) za $E[l^2]$ tako da bude $lP_2 = P_1$ i $lQ_2 = Q_1$.
Dalje,, m ožemo izabrati bazu za (P_3, Q_3) za $E[l^3]$ tako da bude $lP_3 = P_2$ i $lQ_3 = Q_2$ itd.
Neka je, sad $\sigma = (\sigma_1, \sigma_2, ...)$. U bazi (P_1, Q_1) automorfizmu $\rho E, l, 1\sigma_1$ pridružena je 2×2 matrica $\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \in Gl_2(\mathbf{Z}/l\mathbf{Z})$. Tu ćemo matricu poistovjećivati s automorfizmom, tj.
$\rho_{E,l,1}\sigma_1 = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$. Napomenimo da to znači da je $\sigma_1(P_1) = a_1P_1 + c_1Q_1$ i $\sigma_2(Q_1) = b_1P_1 + d_1Q_1$.
Slično dobijemo $\rho_{E,l,2}\sigma_2 = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \in Gl_2(\mathbf{Z}/l^2\mathbf{Z})$, što znači da je $\sigma_2(P_2) = a_2P_2 + c_2Q_2$ i $\sigma_2(Q_2) = b_2P_2 + d_2Q_2$ itd.
Matrice $\begin{bmatrix} a_n & b_n \\ c_n & d_n \end{bmatrix} \in Gl_2(\mathbf{Z}/l^n\mathbf{Z})$ medjusobno su uskladjene, što znači da je
$a_{n+1} = a_n$ modulo l^n, $b_{n+1} = b_n$ modulo l^n, $c_{n+1} = c_n$ modulo l^n i $d_{n+1} = d_n$

modulo l^n za sve n.
Na primjer, kako je $\sigma_2|K_{E,l,1} = \sigma_1$ i $lP_2 = P_1$ i $lQ_2 = Q_1$, vrijedi
$a_1P_1 + c_1Q_1 = \sigma_1(P_1) = \sigma_2(P_1) = \sigma_2(lP_2) = l(\sigma_2(P_2)) = l(a_2P_2 + c_2Q_2) = a_2P_1 + c_2Q_1$. Sad iz činjenice da je (P_1, Q_1) baza s koeficijentima modulo l, iz jednoznačnosti prikaza zaključujemo da je $a_2 = a_1$ i $c_2 = c_1$ modulo l.
Tako smo dobili reprezentaciju s matricama nad prstenom cijelih l-adskih brojeva $\rho_{E,l}(\sigma) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in Gl_2(\mathbf{Z}_l)$, gdje je
$a := (a_1, a_2, ...)$, $b := (b_1, b_2, ...)$, $c := (c_1, c_2, ...)$ i $d := (d_1, d_2, ...)$.
Postavlja se pitanje u kojoj bazi u modulu $T_l(E)$ je prikaz te reprezentacije. To je prikaz u bazi (P, Q) gdje je $P = (P_1, P_2, ...)$ i $Q = (Q_1, Q_2, ...)$. P, Q nisu točke eliptičke krivulje E u uobičajenom smislu, posebice, one nisu točke konačnog reda. U svakom slučaju ovako smo eksplicitno pokazali da je $T_l(E)$ slobodan modul ranga 2 nad prstenom cijelih l-adskih brojeva $\mathbf{Z}_l$.
Napomenimo da je reprezentacija $\rho_{E,l} : \mathrm{Gal}(K_{E,l}/\mathbf{Q}) \to \mathrm{Gl}_2(\mathbf{Z}_\mathrm{l}$.
Tako smo dobili familiju injektivnih reprezentacija indeksiranih eliptičkim krivuljama E nad $\mathbf{Q}$ i prostim brojevima l. To su reprezentacije različitih grupa. Da bismo uniformizirali gledište, razmotrima polje $\bar{\mathbf{Q}}$ polje svih algebarskih brojeva (ono je jedinstveno ako ga razmatramo kao podpolje polja kompleksnih brojeva $\mathbf{C}$). Tada je jednoznačno definirana Galoisova grupa $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. Sad se reprezentacija $\rho_{E,l}$ može proširiti do reprezentacije od $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$, tako da najprije djelujemo s restrikcijom na $\mathrm{Gal}(K_{E,l}/\mathbf{Q})$, potom da komponiramo s reprezentacijom $\rho_{E,l}$. Tu kompoziciju označavamo istom oznakom. Dakle, za $\sigma \in \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ definiramo:
$\rho_{E,l}(\sigma) := \rho_{E,l}(\sigma|K_{E,l})$,
gdje je lijevo nova oznaka, a desno ona od prije. Tu reprezentaciju nazivamo l-adskom reprezentacijom Galoisove grupe $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$, pridruženoj eliptičkoj krivulji E.
Uočimo da je jezgra reprezentacije $\rho_{E,l} : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Gl}_2(\mathbf{Z}_\mathrm{l}$ grupa $\mathrm{Gal}(\bar{\mathbf{Q}}/K_{E,l})$.
Uočimo, takodjer, da je prsten cijelih l-adskih brojeva podprsten polja l-adskih brojeva $\mathbf{Q}_l$, pa imamo prirodno ulaganje grupe $\mathrm{Gl}_2(\mathbf{Z}_\mathrm{l}$ u grupu $\mathrm{Gl}_2(\mathbf{Q}_\mathrm{l}$, a time i reprezentaciju Galoisove grupe u invertibilne 2×2 matrice nad $\mathbf{Q}_l$.
Pripadni vektorski prostor je $V_l(E)$ koji se dobije iz $T_l(E)$ proširenjem skalara, tj., pomoću tenzoriranja

$$V_l(E) := T_l(E) \otimes_{\mathbf{Z}_l} \mathbf{Q}_l.$$

Uvod u aritmetiku eliptičkih krivulja

Frobeniusov element (skica) - 23. lekcija

Galoisova grupa $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ za matematiku je još uvijek zagonetna i daleko smo od njena eksplicitnog opisa. Jedan od očitih elemenata te grupe jest kompleksno konjugiranje (koje je restrikcija standardnog kompleksnog konjugiranja na polju kompleksnih brojeva, koje se može karakterizirati i time da ostavlja na miru polje realnih brojeva). Sjetimo se da, uz standardno upotpunjenje polja racionalnih brojeva do polja realnih brojeva, imamo i p-adska upotpunjenja, za svaki prosti broj p. Frobeniusovi elementi bit će p-adski analogoni kompleksnog konjugiranja i imat će važnu ulogu u aritmetici. Mi nećemo sustavno razvijati tu analogiju, već ćemo do tog pojma doći od **Frobeniusova automorfizma** konačnog polja (koji onda definira i Frobeniusov automorfizam eliptičke krivulje nad konačnim poljem), preko **Frobeniusovih automorfizama** konačnog abelovog proširenja od $\mathbf{Q}$ i **Frobeniusovih elemenata** (bilo kakvih) konačnih Galoisovih proširenja od $\mathbf{Q}$.

Frobeniusov automorfizam konačnog polja.
Podsjetimo da je $\mathbf{F}_p$ minimalno polje karakteristike p (prost broj) i da ima p elemenata, a možemo ga realizirati kao skup ostataka modulo p ili kao kvocijentni prsten $\mathbf{Z}/p\mathbf{Z}$. Ako fiksiramo jedno algebarsko zatvorenje $\bar{\mathbf{F}}_p$ od $\mathbf{F}_p$, onda za svaki prirodni broj n postoji točno jedno podpolje od $\bar{\mathbf{F}}_p$ koje ima p^n elemenata. To je polje

$$\mathbf{F}_{p^n} = \{x \in \bar{\mathbf{F}}_p : x^{p^n} = x\}.$$

Sva su ta polja algebarska proširenja od $\mathbf{F}_p$, sva su Galoisova, i nema drugih konačnih proširenja od $\mathbf{F}_p$ koji su u $\bar{\mathbf{F}}_p$ (drugim riječima, za svaki n postoji jedinstveno proširenje stupnja n). Takodjer se vidi:

$$\mathbf{F}_{p^m} \subseteq \mathbf{F}_{p^n} \text{ akko } m|n.$$

Nadalje, Galoisova grupa $\mathrm{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_p$ je **ciklička** i generirana **Frobeniusovim automorfizmom** $Frob_p$ zadanim kao

$$Frob_p(x) := x^p.$$

Podsjetimo da je grupna operacija kompozicija, pa ako, radi jednostavnosti, pišemo σ umjesto $Frob_p$, onda je

$$\mathrm{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_p = \{1, \sigma, \sigma^2, ..., \sigma^{n-1}\}$$

gdje je $\sigma^k := \sigma \circ \sigma \circ ... \circ \sigma$ (k puta), tj. $\sigma^k(x) = x^{p^k}$, za sve x.
Uočite da je fiksno polje Frobeniusova automorfizma upravo minimalno polje $\mathbf{F}_p$.
Uočite takodjer da formula za Frobeniusov automorfizam ne ovisi o n, već samo o p. Zato su $Frob_p$ za različite n uskladjeni pa je tom formulom zadan i automorfizam polja $\bar{\mathbf{F}}_p$ nad $\mathbf{F}_p$.

Frobeniusov automorfizam eliptičke krivulje.
Neka je E eliptička krivulja definirana nad poljem $\mathbf{F}_p$. Tada je formulom

$$\phi_p(x, y) := (x^p, y^p)$$

zadan morfizam $\phi_p : E \to E$ (pri tom točke od E razmatramo s koordinatama iz $\bar{\mathbf{F}}_p$). Dakle, ϕ_p je zadan djelovanjem Frobeniusova automorfizma na koordinatama.
Uočite da vrijedi $\phi_p(P) = P$ akko P je definirana nad $\mathbf{F}_p$.
To znači da je broj $\mathbf{F}_p$-racionalnih točaka na E jednak broju nultočaka morfizma $\phi_p - 1$, gdje 1 označava morfizam identiteta; ta je činjenica polazna za dokaz Hasse-Weilova teorema.

Frobeniusov automorfizam konačnog abelova proširenja od $\mathbf{Q}$.
Neka je $K/\mathbf{Q}$ konačno abelovo proširenje. To znači da je ono konačnog stupnja (posebice, tada je ono i algebarsko), Galoisovo i da je Galoisova grupa G abelova. Pokazat će se da za svaki prosti p (osim njih konačno mnogo - koji se granaju u K) jednoznačno možemo definirati automorfizam σ iz G koji ima jaku vezu s Frobeniusovim automorfizmom odredjenog proširenja od $\mathbf{F}_p$, zato ćemo taj σ takodjer zvati Frobeniusovim automorfizmom i označavati $Frob_p$.
Kako je G konačna grupa, a prostih brojeva ima beskonačno mnogo, to znači da će bar jedan σ biti $Frob_p$ za beskonačno mnogo p. Teorem Čebotareva govori da je svakom σ tako pridruženo "jednako mnogo" prostih brojeva, tj. da za svaki σ skup svih onih prostih brojeva p za koje je $\sigma = Frob_p$ čini $|G|$-ti dio skupa svih prostih brojeva (zanemarujući konačno mnogo onih koji se granaju. To ćemo preciznije formulirati poslije. Započet ćemo s jednim

primjerom.

Primjer 1. Neka je $K = \mathbf{Q}(i) = \{a + bi : a, b \in \mathbf{Q}\}$ polje Gaussovih brojeva. To je proširenje 2. stupnja, s Galoisovom grupom $G = \{1, \sigma\}$ gdje je σ kompleksno konjugiranje, tj. $\sigma(a + bi) = a - bi$.
Uz polje Gaussovih brojeva prirodno ide prsten cijelih Gaussovih brojeva $\mathbf{Z}[i] = \{a + bi : a, b \in \mathbf{Z}\}$, koji treba gledati kao prirodno proširenje prstena cijelih brojeva $\mathbf{Z}$. Prsten $\mathbf{Z}[i]$ ima jednoznačnu faktorizaciju koja se može opisati ovako:
(i) ako je $p = 3$ modulo 4, onda je p prost i u $\mathbf{Z}[i]$. Kažemo da je p inertan.
(ii) (i) ako je $p = 1$ modulo 4, onda je $p = (u + vi)(u - vi)$ umnožak dvaju prostih u $\mathbf{Z}[i]$, medjusobno kompleksno konjugiranih. Kažemo da se p cijepa.
(iii) $2 = i(1-i)^2$ je umnožak od kvadrata od $1-i$ koji je prost u $\mathbf{Z}[i]$ i broja i koji je invertibilan u $\mathbf{Z}[i]$ (još su invertibilni ± 1 i $-i$). Kažemo da se 2 grana.
Na primjer $3, 7, 11, 19, 23, ...$ ostaju prosti u $\mathbf{Z}[i]$, dok je
$5 = (2 + i)(2 - i),\ 13 = (3 + 2i)(3 - 2i),\ 17 = (4 + i)(4 - i)...$
Podsjetimo da je kvocijent $\mathbf{Z}/p\mathbf{Z}$ minimalno konačno polje $\mathbf{F}_p$.
Uočite da je za inertne p analogni kvocijentni prsten $\mathbf{Z}[i]/p\mathbf{Z}[i]$ kvadratno proširenje od $\mathbf{F}_p$.
Naime, taj je prsten izomorfan prstenu $\mathbf{F}_p[\eta]$ uz $\eta^2 + 1 = 0$, koji se ostvaruje tako da se klasi od $a + bi$ pridruži $\bar{a} + \bar{b}\eta$, gdje je $\bar{a} := a$ modulo p itd.
Kako je $p = 3$ modulo 4, -1 nije kvadrat u $\mathbf{F}_p$ pa je $X^2 + 1$ ireducibilan polinom nad $\mathbf{F}_p$, tj. prsten $\mathbf{F}_p[\eta]$ je polje drugog stupnja nad $\mathbf{F}_p$, pa je izomorfan polju $\mathbf{F}_{p^2}$.
Sad imamo Frobeniusov automorfizam $Frob_p : x \mapsto x^p$ proširenja $\mathbf{F}_{p^2}/\mathbf{F}_p$, koje ima Galoisovu grupu $\{1, Frob_p\}$, koja je pak prirodno izomorfna Galoisovoj grupi $\{1, \sigma\}$ proširenja $K/\mathbf{Q}$. Naime, σ preslikava prsten cijelih brojeva u sebe, takodjer ostavlja na miru prosti element p, pa i pripadni ideal $p\mathbf{Z}[i]$, zato se djelovanje od σ može prenijeti na kvocijent $\mathbf{Z}[i]/p\mathbf{Z}[i]$ prema formuli

$$\sigma(\overline{a + bi} = \overline{\sigma(a + bi)}$$

Zato je $\sigma(\bar{a} + \bar{b}\eta) = \overline{a - bi} = \bar{a} - \bar{b}\eta = (\bar{a} + \bar{b}\eta)^p$. Naime, kako je $eta^2 = -1$ i $p = 3$ modulo 4, vrijedi $(\bar{a} + \bar{b}\eta)^p = \bar{a}^p + \bar{b}^p\eta^p = \bar{a} + \bar{b}(-1)$. Dakle, pri tom prirodnom izomorfizmu σ prelazi u $Frob_p$ (kako je jedino i moguće), pa zato definiramo $\sigma = Frob_p$ za sve $p = 3$ modulo 4. Naravno, pri tom izomorfizmu, identitet u G prelazi u identitet za konačno polje.
Ako je pak $p = 1$ modulo 4, tj. $p = (u + vi)(u - vi)$, onda je

$\mathbf{Z}[i]/(u+vi)\mathbf{Z}[i] \cong \mathbf{F}_p \cong \mathbf{Z}[i]/(u-vi)\mathbf{Z}[i]$
jer je sad -1 kvadrat u $\mathbf{F}_p$. Zato je sad pripadni Frobeniusov automorfizam identitet (proširenje je stupnja 1), pa je $Frob_p = 1$ za sve $p = 1$ modulo 4. Ako želimo uspostaviti analogiju s prvim slučajem (kad je p inertan), sad σ prosti element $u+vi$ prebacuje u $u-vi$ (i obratno), dok ih na miru ostavlja samo identitet 1, pa je σ odmah isključen iz razmatranja.

Općenito, neka je K konačno abelovo proširenje stupnja n od $\mathbf{Q}$ i neka je G pripadajuća Galoisova grupa. Neka je O_K pripadni prsten cijelih brojeva. Taj prsten ne mora (i u pravilu nije) biti s jednoznačnom faktorizacijom. Umjesto toga jednoznačna je faktorizacija na proste ideale. Posebno za glavne ideale pO_K u O_K generirane prostim brojevima p vrijedi (za sve osim konačno mnogo njih koji se granaju)
$pO_K = \mathcal{P}_1\mathcal{P}_2...\mathcal{P}_m$, umnožak na **različite** proste ideale. Pri tom je
$O_K/\mathcal{P}_1 \cong O_K/\mathcal{P}_2 \cong ... \cong O_K/\mathcal{P}_m \cong \mathbf{F}_p^f$,
za neki prirodni broj f koji se zove indeks inercije od p i vrijedi $mf = n$.
Ako je $f = 1$ onda kažemo da se p potpuno rastavlja (cijepa), a ako je $f = n$, onda p ostaje prost (inertan). Za svaki od ovih $\mathcal{P}_j$ kažemo da dijeli pO_K i pišemo $\mathcal{P}_j | pO_K$ (odnosno da je iznad p jer je $\mathcal{P}_j \cap \mathbf{Z} = (p)$ - ideal u $\mathbf{Z}$ generiran s p).
Ovi $\mathcal{P}_j$ medjusobno su povezani, kako ćemo ubrzo vidjeti. Ako je $\mathcal{P}$ neki prost ideal u O_K i $\sigma \in G$ automorfizam od K, onda je skup

$$\sigma(\mathcal{P}) := \{\sigma(x) : x \in \mathcal{P}\}$$

opet prost ideal.
Fiksirajmo načas jedan prost broj p i jedan prosti ideal $\mathcal{P}$ iznad p. Neka je $O_K/\mathcal{P} \cong \mathbf{F}_p^f$ (*), tj. f je indeks inercije u p. Definirajmo:
$D_\mathcal{P} = \{\sigma \in G : \sigma(\mathcal{P}) = \mathcal{P}\}$ - grupa rastavljanja u $\mathcal{P}$ (dekompozicijska grupa)
Postoji prirodni surjektivni homomorfizam $D_\mathcal{P} \to \mathrm{Gal}(\mathbf{F}_p^f/\mathbf{F}_p)$. Naime, preko izomorfizma (*), svaki $\sigma \in D_\mathcal{P}$ djeluje na konačno polje preko

$$\sigma(u \ mod \ \mathcal{P}) := \sigma(u) \ mod \ \mathcal{P}$$

za svaki $u \in O_K$.
Taj je homomorfizam izomorfizam ako se p ne grana i tada postoji jedinstveni automorfizam iz G (preciznije iz dekompozicijske grupe) koji se preslikava u $Frob_p$ i njega nazivamo Frobeniusovim automorfizmom u $\mathcal{P}$ - oznaka $Frob_\mathcal{P}$. Lako se vidi da $D_\mathcal{P}$ pa tako niti $Frob_\mathcal{P}$ ne ovise o izboru prostog ideala iznad

p, pa je tako jednoznačno odredjen Frobeniusov automorfizam u p - oznaka $Frob_p$ (kao i za konačna polja).
Iz gornjeg opisa slijedi da je $Frob_p$ jednoznačno odredjeno kao:

$$Frob_p(u) = u^p \text{ modulo } \mathcal{P}$$

za neki (pa onda za svaki) $\mathcal{P}$ iznad p.

Primjer 2. (peti korijeni iz jedinice).
Neka je $K := \mathbf{Q}(\mu_5)$ polje generirano (bilo kojim) primitivnim petim korijenom iz jedinice, na pr. neka je $\mu_5 = e^{\frac{2\pi i}{5}}$. To je polje Galoisovo (jer sadrži i ostale pete korijene iz jedinice, koje su potencije od μ_5). Minimalni polinom je $f(X) := X^4 + X^3 + X^2 + X + 1$ (dobije se dijeljenjem polinoma $X^5 - 1$ s $X - 1$), pa je proširenje stupnja $n = 4$. Galoisova grupa je ciklička reda 4 izomorfna grupi $\{1, 2, 3, 4\}$ uz množenje modulo 5 (uočite da su izvodnice brojevi 2 i 3), tj. $\text{Gal}(K/\mathbf{Q}) = \{1, \sigma, \sigma^2, \sigma^3\}$, gdje je, na primjer, $\sigma(\mu_5) = \mu_5^2$ (drugi je izbor da bude $\sigma(\mu_5) = \mu_5^3$). Sad je $\sigma^2(\mu_5) = \sigma(\mu_5^2) = \mu_5^4$ itd.
Pokazuje se da je tu prsten cijelih brojeva $O_K = \mathbf{Z}[\mu_5]$, grana se jedino broj 5.
(I) Prosti brojevi p za koje je $Frob_p = 1$, tj. $f = 1$ su upravo oni za koje se pO_K rastavlja na umnožak četiri različita prosta (jer mora biti $m = 4$) i ako je $\mathcal{P}$ jedan od tih faktora, onda je

$$pO_K = \mathcal{P}\sigma(\mathcal{P})\sigma^2(\mathcal{P})\sigma^3(\mathcal{P})$$

Prema teoremu Čebotareva ima $\frac{1}{4}$ takvih prostih p. To su inače svi oni p za koje se minimalni piolinom f modulo p rastavlja na različite linearne faktore.
(II) Prosti brojevi p za koje je $Frob_p = \sigma$, tj. $f = 4$, jer σ generira grupu 4-tog reda, imaju svojstvo da je pO_K prost (odnosno da je f ireducibilan modulo p). Analogno je s onim p za koji je $Frob_p = \sigma^3$ (jer je i σ_3 izvodnica. Prema teoremu Čebotareva ima $\frac{2}{4} = \frac{1}{2}$ takvih prostih p.
(III) Ostaju prosti p za koje je $Frob_p = \sigma^2$, tj. $f = 2$, jer σ^2 generira grupu 2-gog reda. Oni imaju svojstvo da je

$$pO_K = \mathcal{Q}\sigma(\mathcal{Q})$$

gdje je $\mathcal{Q}$ jedan od prostih djelitelja (naime 1 i σ^2 čine dekompozicijsku grupu i oni fiksiraju Q, dok ga σ ne fiksira; uočite i to da je $\sigma^3(Q) = \sigma(Q)$). Takvih p ima jedna četvrtina i to su upravo oni za koje se f modulo p rastavlja na

umnožak dvaju različitih ireducibilnih polinoma drugog stupnja.
Napomenimo da je u ovomu slučaju O_K prsten s jednoznačnom faktorizacijom, pa se gornji rastavi mogu napisati pomoću prostih brojeva umjesto ideala (ali to ne činimo).
Dirichletov teorem o prostim projevima u aritmetičkim nizovima vodi do preciznije tvrdnje: u (I) spadaju oni prosti koji su kongruentni 1 modulo 5, u (II) oni kongruentni 2 odnosno 3, a u (III) oni kongruentni 4 modulo 5.
Na primjer, $19 = 4$ modulo 5, a

$$X^4 + X^3 + X^2 + X + 1 = (X^2 + 5X + 1)(X^2 - 4X + 1) \text{ modulo } 5$$

je rastav na ireducibilne faktore, što potvrdjuje da je $f = 2$.

Frobeniusov element konačnog Galoisova proširenja.
Za razliku od abelova proširenja, tu Frobeniusov element u p (za nerazgranati p) nije dobro definiran, već samo njegova klasa konjugiranosti. Podsjetimo, ako je G neka grupa i $h \in G$, onda je klasa konjugiranosti od h, prema definiciji, $\{g^{-1}hg : g \in G\}$. Očito je da su klase konjugiranosti u abelovoj grupi jednočlane (i obratno). Općenito, klase konjugiranosti čine particiju grupe na disjunktne podskupove - biti u istoj klasi konjugiranosti je relacija ekvivalencije).

Primjer 3. Klase konjugiranosti u $\mathbf{S_3}$.
Kako je poznato, simetrična grupa S_3 izomorfna je grupi

$$\{1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$$

gdje je $\sigma^3 = \tau^2 = 1$ i $\tau\sigma = \sigma^2\tau$
(odakle onda slijedi i da je $\tau\sigma^2 = \sigma\tau$; takodjer vrijedi $(\sigma\tau)^2 = (\sigma^2\tau)^2 = 1$).
Ova grupa ima tri klase konjugiranosti.
Klasa konjugiranosti od 1 je $\{1\}$ (to je uvijek tako).
Klasa konjugiranosti od σ je $\{\sigma, \sigma^2\}$ jer je $\tau^{-1}\sigma\tau = \tau\sigma\tau = \sigma^2\tau\tau = \sigma^2$ (a daljnjim se konjugiranjem ništa novo ne dobiva - provjerite).
Klasa konjugiranosti od τ je $\{\tau, \sigma\tau, \sigma^2\tau\}$ jer je, na primjer, $\sigma^{-1}\tau\sigma = \sigma^2\tau\sigma = \sigma^4\tau = \sigma\tau$ (slično se dobije i da je $\sigma^2\tau$ u klasi).

Frobeniusov element za konačna neabelova proširenja.
Neka je $K/\mathbf{Q}$ Galoisovo proširenje stupnja n s Galoisovom grupom G (općenito neabelovom) i prstenom cijelih brojeva O_K. Fiksirajmo neki prost broj p koji

se ne grana u K. Tada je glavni ideal pO_K umnožak različitih prostih ideala i neka je $\mathcal{P}$ jedan od njih.
Kao i u abelovom slučaju definiramo grupu razlaganja $D_{\mathcal{P}}$ u $\mathcal{P}$ (koje se sastoje od onih $g \in G$ za koje je $g(\mathcal{P}) = \mathcal{P}$ i pripadno konačno polje $\mathbf{F}_{p^f} \cong O_K/\mathcal{P}$. Kao i prije, $D_{\mathcal{P}}$ je ciklička reda f i imamo prirodni izomorfizam izmedju $D_{\mathcal{P}}$ i $\mathrm{Gal}(\mathbf{F}_{p^f}/\mathbf{F}_p)$ koja je generirana Frobeniusovim automorfizmom $Frob_p : x \mapsto x^p$, pa postoji jedinstven element u $D_{\mathcal{P}}$ koji pri tom izomorfizmu korespondira $Frob_p$ pa ga označavamo kao $Frob_{\mathcal{P}}$, odredjen je kongruencijom

$$Frob_{\mathcal{P}}(u) = u^p \text{ modulo } \mathcal{P}.$$

Ako je $\mathcal{Q}$ neki drugi prosti ideal iznad p, onda postoji $g \in G$ tako da bude $\mathcal{Q} = g(\mathcal{P})$ i tada je

$$D_{\mathcal{Q}} = gD_{\mathcal{P}}g^{-1}$$

i prema tomu i

$$Frob_{\mathcal{Q}} = gFrob_{\mathcal{P}}g^{-1},$$

tj. Frobeniusovi automorfizmi u različitim prostim idealima iznad p medjusobno su konjugirani. Takodjer, indeks inercije f jednak je za sve proste ideale iznad p, i ako se pO_K rastavlja na umnožak m prostih faktora, onda je

$$mf = n \ (**)$$

Uočite, takodjer, da vrijedi čim je $\mathcal{P}$ iznad p onda je i $g(\mathcal{P})$ iznad p za svaki $g \in G$. Zato su svi elementi iz klase konjugiranosti od $Frob_{\mathcal{P}}$ Frobeniusovi elementi u nekim prostim idealima nad p. To omogućuje definiciju:

Frobeniusovim elementom $Frob_p$ u prostom broju p zovemo klasu konjugiranosti Frobeniusova automorfizma $Frob_{\mathcal{P}}$ za bilo koji prosti ideal $\mathcal{P}$ iznad p (i ona ne ovisi o tom izboru).

Teorem Čebotareva.
Neka je K konačno Galoisovo proširenje od $\mathbf{Q}$ stupnja n s Galoisovom grupom G. Neka je $A \subset G$ podskup zatvoren na konjugiranje (na primjer, klasa konjugiranosti). Tada je

$$\mu(\{p : \ p \text{ prost i } Frob_p \subseteq A\} = \frac{\mathrm{card}A}{n},$$

pri čemu je μ **Dirichletova gustoća**, definirana za podskupove skupa prostih brojeva kao

$$\mu(B) := \lim_{X\to\infty} \frac{\text{card}(\{p : p \le X\} \cap B)}{\text{card}\{p : p \le X\}}$$

(ako limes postoji).

Primjer 4. Frobeniusovi elementi u $\text{Gal}(\mathbf{Q}(\sqrt[3]{2}, \rho)/\mathbf{Q})$.
Poznato je da je polje $K := \mathbf{Q}(\sqrt[3]{2}, \rho)$, gdje je $\rho = e^{\frac{2\pi i}{3}}$, Galoisovo stupnja 6, s Galoisovom grupom izomorfnom S_3 (pa prema tomu nije abelovo). Takodjer u K se granaju 2 i 3, pa njih izključujemo iz razmatranja.
Sjetimo se identifikacije $S_3 = \{1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$ i klasa konjugiranosti $\{1\}$, $\{\sigma, \sigma^2\}$ i $\{\tau, \sigma\tau, \sigma^2\tau\}$. Sad imamo:
(I) $Frob_p = 1$ akko $f = 1$, tj. pO_K se potpuno rastavlja (na 6 prostih faktora), i ako je $\mathcal{P}$ jedan od prostih faktora onda je

$$pO_K = \mathcal{P}(\sigma\mathcal{P})(\sigma^2\mathcal{P})(\tau\mathcal{P})(\sigma\tau\mathcal{P})(\sigma^2\tau\mathcal{P}).$$

Teorem Čebotareva kaže da ima šestina takvih prostih p.
(II) $Frob_p = \{\sigma, \sigma^2\}$ akko je $f = 3$ (jer σ generira cikličku grupu reda 3), pa je $m = 2$ u (**), i ako je $\mathcal{P}$ jedan od faktora od pO_K onda je

$$pO_K = \mathcal{P}(\tau\mathcal{P})$$

(uočite da je $\tau\mathcal{P} = \sigma\tau\mathcal{P} = \sigma^2\tau\mathcal{P}$). Teorem Čebotareva kaže da ima ďvije sestine takvih prostih p.
(III) $Frob_p = \{\tau, \sigma\tau, \sigma^2\tau\}$ akko je $f = 2$ (naime, svaki od tih elemenata je drugog reda) pa, ako je za $\mathcal{P}$ iznad p onda je

$$pO_K = \mathcal{P}(\sigma\mathcal{P})(\sigma^2\mathcal{P}).$$

Teorem Čebotareva kaže da ima tri šestine takvih prostih p.
Uočite da ne postoji ni jedan p za koji je pO_K prost.

Uvod u aritmetiku eliptičkih krivulja

Frobeniusov element beskonačnog proširenja (skica) - 24. lekcija

Neka je sad $L/\mathbf{Q}$ Galoisovo proširenje beskonačnog stupnja (tj. unija svojih Galoisovih podproširenja $K/\mathbf{Q}$ konačnog stupnja). Uskladjena familija $(\mathcal{P}_K)$ prostih ideala iznad prostog broja p, prema definiciji je familija za koju je svaki $\mathcal{P}_K$ prost ideal u prstenu cijelih algebarskih brojeva O_K od K i koji dijeli ideal pO_K, ali takva da ako je $K' \subset K$, onda je $\mathcal{P}_K \cap O_{K'} = \mathcal{P}_{K'}$. Tada je $\mathcal{P}_L := \bigcup \mathcal{P}_K$ prost ideal u O_L i obratno, svaki se prosti ideal u O_L tako dobije.
Ako su sad za neki $\mathcal{P}_L$ svi pripadni $\mathcal{P}_K$ nerazgranati, onda kažemo da je i $\mathcal{P}_K$ nerazgranat. Ako su svi $\mathcal{P}_L$ iznad p nerazgranati, kažemo de je p nerazgranat u L, odnosno da je L nerazgranato u p (inače je razgranato). Jasno je da je, općenito, nerazgranatost kod proširenja beskonačna stupnja rijetkost, ali nije potpuno isključena.

Primjer 1. (i) Neka je $L := \bigcup_n \mathbf{Q}(\mu_{l^n})$ unija proširenja generiranih l^n-tim korijenima iz jedinice, za fiksiran prost broj l, dok n prolazi skupom svih prirodnih brojeva. Može se pokazati da je $\mathcal{P}_L$ razgranat ako i samo ako je $\mathcal{P}_L$ iznad l. Drugim riječima, tu je L nerazgranato osim u l (gdje je razgranato).
(ii) (**vrlo važan primjer**) Neka je $L := K_{E,l}$ polje generirano koordinatama točkama l^n-tog reda fiksirane eliptičke krivulje E nad $\mathbf{Q}$, pri fiksiranom prostom broju l, i prirodnim brojevima n. Prema teoremu Serrea i Tatea, L je nerazgranat upravo u onim prostim brojevima $p \neq l$ u kojima E ima dobru redukciju (posebice, ono je nerazgranato izvan konačnog skupa prostih brojeva).
(iii) Neka je $L := \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ polje svih algebarskih brojeva. Tada je L Galoisovo beskonačnog stupnja u kojemu je svaki $\mathcal{P}_L$ razgranat (pa je L razgranato u svim prostim p). Naime, neka je $\mathcal{P}_L$ iznad p i neka je K kvadratno proširenje u kojemu se p grana (na primjer $K := \mathbf{Q}(\sqrt{p})$). Tada je pripadni $\mathcal{P}_K$ razgranat.

Ako je neki $\mathcal{P}_L$ iznad p nerazgranat onda definiramo Frobeniusov automorfizam $Frob_{\mathcal{P}_L}$ u $\mathcal{P}_L$ kao uskladjenu familiju Frobeniusovih automorfizama $(Frob_{\mathcal{P}_K})$ gdje K ide svim konačnim Galoisovim podproširenjima od L (tu

uskladjenost znači da se Frobeniusov automorfizam manjeg polja dobije restrikcijom Frobeniusova automorfizma s većega, što slijedi iz definicije). Zato je $Frob_{\mathcal{P}_L}$ element Galoisove grupe od L nad $\mathbf{Q}$.
Nije teško vidjeti da ako je neki $\mathcal{P}_L$ iznad p nerazgranat onda je i svaki $\mathcal{P}_L$ iznad p nerazgranat i da su svaka dva pripadna Frobeniusova automorfizma konjigirana, i svaki automorfizam iz klase konjugiranosti jednoga $\mathcal{P}_L$ je Frobeniusov automorfizam nekoga prostoga ideala nad p. Zato je jednoznačno definirana klasa konjugiranosti Frobeniusova automorfizma $Frob_{\mathcal{P}_L}$ koja se zove **Frobeniusov element** prostog broja p i označava se kao $Frob_p$ (da ne dodje do zabune, kadkad se u oznaci stavi i L da se dade do znanja koje je gornje polje).

Trag i determinanta Frobeniusova elementa pri l-adskoj reprezentaciji.
Zaključujemo, prema Primjeru 1(ii), da je za $K_{E,l}$ uvijek jednoznačno definirana klasa konjugiranosti $Frob_p$ uz uvjet da E ima dobru redukciju u p i da je $p \neq l$. Kako je pripadna l-adska reprezentacija

$$\rho_{E,l} : \mathrm{Gal}(K_{E,l}/\mathbf{Q}) \to \mathrm{Gl}_2(\mathbf{Z}_l)$$

injektivna, razumno je definirati tragom, odnosno determinantom svakog automorfizma, kao tragom odnosno determinantom pripadne 2×2 matrice. Kako konjugirani automorfizmi pri reprezentaciji prelaze u konjugirane matrice, i kako konjugirane matrice imaju jednake tragove i determinante, jednoznačno su definirani
$tr(Frob_p)$ i $det(Frob_p)$ kao $tr(\rho_{E,l}Frob_{\mathcal{P}})$ i $det(\rho_{E,l}Frob_{\mathcal{P}})$
gdje je $\mathcal{P}$ **bilo koji** prosti ideal u prstenu cijelih od $O_{K_{E,l}}$ iznad p.

Općenito, trag automorfizma grupe $\mathrm{Gal}(K_{E,l}/\mathbf{Q})$ je cijeli l-adski broj, a determinanta invertibilni cijeli algebarski broj (jer pripadna matrica ima koeficijente u $\mathbf{Z}_l$). Vrlo važno svojstvo Froneniusovih elemenata (odnosno klase konjugiranosti pripadnih Frobeniusovih automorfizama) jest da su njihovi trag i determinanta obični cijeli brojevi (iako pripadne matrice u pravilu nemaju cijele koeficijente). To se dobije pažljivom analizom koju sad ne možemo prezentirati. Vrijedi naime, puno preciznija tvrdnja.

Teorem. Neka je E fiksirana eliptička krivulja nad $\mathbf{Q}$ i neka je l fiksiran prost broj. Tada za svaki prosti $p \neq l$ u kojemu E ima dobru redukciju vrijedi:

$$trFrob_p = a_p \text{ i } detFrob_p = p$$

gdje je $a_p = p + 1 - N_p$, a N_p je broj $\mathbf{F}_p$-racionalnih točaka na redeciranoj eliptičkoj krivulji modulo p. Prema Hasseovu teoremu vrijedi $|a_p| < 2\sqrt{p}$.

Frobeniusovi elementi u razgranatim prostim brojevima i idealima.
Prema dosadašnjem razmatranju, definirali smo Frobeniusove automorfizme i elemente samo u nerazgranatom slučaju. Kao posljedicu imali smo, na primjer, da tako ne možemo definirati Frobeniuosove elemente u $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ niti za jedan prosti p. Zato ćemo sad naše definicije proširiti i na razgranati slučaj. Startat ćemo, kao i obično, s konačnim Galoisovim proširenjima. Kao što je poznato, eksplicitno se može definirati diskriminanta D svakog takvog proširenja, koja je cijeli broj različit od $0, -1, 1$ i vrijedi:
p se grana u proširenju ako i samo ako $p|D$.
Podsjetimo, ako je $K/\mathbf{Q}$ konačno Galoisovo proširenje s Galoisovom grupom G, p prost broj i $\mathcal{P}$ neki prost ideal u K koji je iznad p. Tada smo definirali grupu razlaganja u $\mathcal{P}$:
$D_{\mathcal{P}} = \{\sigma \in G : \sigma(\mathcal{P}) = \mathcal{P}\}$,
i grupu inercije $I_{\mathcal{P}}$ u $\mathcal{P}$ kao jezgru prirodnog surjektivnog homomorfizma
$D_{\mathcal{P}} \to \mathrm{Gal}(\mathbf{F}_{p^f}/\mathbf{F}_p)$, gdje je f indeks inercije u p. Napomenimo da je ta jezgra trivijalna ako i samo ako je p nerazgranat. Dakle imamo prirodni izomorfizam

$$D_{\mathcal{P}}/I_{\mathcal{P}} \cong \mathrm{Gal}(\mathbf{F}_{p^f}/\mathbf{F}_p).$$

Zato je jednoznačno definiran automorfizam $Frob_{\mathcal{P}}$ iz $D_{\mathcal{P}}/I_{\mathcal{P}}$ koji pri tom izomorfizmu prelazi u Frobeniusov automorfizam konačnog polja.
Napomenimo da za razgranati p svi $\mathcal{P}$ koji sudjeluju u rastavu od pO_K dolaze s fiksnim eksponentom $e \geq 2$ (indeks grananja) i da vrijedi

$$efm = n \ (***)$$

gdje je m broj različitih prostih faktora u rastavu.
Ako je proširenje Abelovo onda $D_{\mathcal{P}}, I_{\mathcal{P}}, D_{\mathcal{P}}/I_{\mathcal{P}}$ i $Frob_{\mathcal{P}}$ ne ovise o $\mathcal{P}$ već samo o p pa je, prema definiciji, $Frob_p := Frob_{\mathcal{P}}$, za bilo koji $\mathcal{P}$ iznad p.
Uočite da $Frob_p$ nije više element od G (ako je u p grananje), već klasa elemenata iz G koja ima bar dva elementa, pa nije klasa konjugiranosti (u abelovom slučaju).

Primjer 2. (i) U $K = \mathbf{Q}(i)$ je $G = \{1, \sigma\}$, gdje je σ kompleksno konjugiranje; grana se samo 2 i jer je $2O_K = (1-i)^2$ vidimo da je $\mathcal{P} = (1-i)$

(glavni ideal), s indeksom grananja $e = 2$. Izravno se dobije:
$D_{\mathcal{P}} = G$ (jer je $\sigma(1-i) = 1+i = -i(1-i)$). Kako je $O_K = \mathbf{Z}[i]$ vidi se da je $O_K/\mathcal{P} \cong \mathbf{F}_2$ pa je $f = 1$, tj. $I_{\mathcal{P}} = G$ i $Frob_2$ je 1 kao jedini element od G/G.
(ii) U $K = \mathbf{Q}(\mu_5)$ je $G = \{1, \sigma, \sigma^2, \sigma^3\}$, gdje je σ jednoznačno zadano kao $\sigma(\mu_5) := \mu_5^2$. Grana se jedino 5. Naime $X^4+X^3+X^2+X+1 = (X-1)^4$ modulo 5, pa je $5O_K = \mathcal{P}^4$ za prosti ideal $\mathcal{P}$ (koji se može eksplicitno napisati, štoviše tu ideali nisu ni potrebni).
Zato je tu opet $Frob_5 = 1 \in G/G$.
(iii) Neka je $K := \mathbf{Q}(\sqrt{3}, i)$. To je proširenje 4-tog stupnja s abelovom Galoisovom grupom G koja je direktni produkt dviju cikličkih grupa 2-gog reda $\{1, \sigma\}$ i $\{1, \tau\}$, gdje je $\sigma(i) = -i$ i $\sigma(\sqrt{3}) = \sqrt{3}$, dok je $\tau(i) = i$ i $\tau(\sqrt{3}) = -\sqrt{3}$. Lako se vidi da se samo 2 i 3 granaju, a može se pokazati da su ostali prosti brojevi nerazgranati. Nije teško vidjeti da je

$$2O_K = \mathcal{P}^2$$

za neki prosti ideal $\mathcal{P}$. Zato je $e = f = 2$, i takodjer $D_{\mathcal{P}} = G$. Zaključujemo da je $I_{\mathcal{P}} = \{1, \sigma\}$ (jer je restrikcija te grupe na $\mathbf{Q}(i)$ netrivijalna - naime 2 se grana i u tom polju). Zato je $Frob_2$ klasa od τ u $G/\{1, \sigma\}$.
Potpuno analogno $Frob_3$ je klasa od σ u $G/\{1, \sigma\tau\}$. Naime, restrikcija grupe inercije na $\mathbf{Q}(\sqrt{-3})$ (koje je takodjer podpolje od K) mora biti netrivijalna, kako se 3 grana i u tom polju. Kako su σ i τ trivijalni na tom polju, ostaje nam $\sigma\tau$.

Ako je G nekomutativna grupa, onda se sve malo usložnjuje. Opet je za svaki fiksirani prosti broj p i svaki prosti ideal $\mathcal{P}$ u O_K koji je iznad p jednoznačno definiran automorfizam $Frob_{\mathcal{P}}$ iz $D_{\mathcal{P}}/I_{\mathcal{P}}$. Ako je $\mathcal{Q}$ neki drugi prosti ideal iznad p, onda postoji $g \in G$ tako da bude $g\mathcal{P} = \mathcal{Q}$; tada je $D_{\mathcal{Q}} = gD_{\mathcal{P}}g^{-1}$ i $I_{\mathcal{Q}} = gI_{\mathcal{P}}I^{-1}$. Takodjer,
za $Frob_{\mathcal{P}} \in D_{\mathcal{P}}/I_{\mathcal{P}}$ i $Frob_{\mathcal{Q}} \in D_{\mathcal{Q}}/I_{\mathcal{Q}}$, vrijedi $Frob_{\mathcal{Q}} = gFrob_{\mathcal{P}}g^{-1}$,
gdje definiramo prirodno djelovanje od G na klase kao $h(\sigma I_{\mathcal{P}}) := (h\sigma)(hI_{\mathcal{P}})$, za $h \in G$ i $\sigma \in D_{\mathcal{P}}$, i slično za djelovanje zdesna.
Sad definiramo $Frob_p$ kao familiju $Frob_{\mathcal{P}}$ za sve $\mathcal{P}$ iznad p. Vidimo, ako je klasa od $Frob_{\mathcal{P}}$ oblika $\sigma I_{\mathcal{P}}$, onda je $g\sigma I_{\mathcal{P}}g^{-1} = g\sigma g^{-1}gI_{\mathcal{P}}g^{-1} = g\sigma g^{-1}I_{\mathcal{Q}}$, a to je klasa od $Frob_{\mathcal{Q}}$.
Uočite da $Frob_p$, za razgranati p (shvaćen kao skup svih automorfizama koji u njemu sudjeluju) nije nužno klasa konjugiranosti u G (iako može biti, za razliku od abelova slučaja). To čemo vidjeti u sljedećem primjeru.

Primjer 3. Neka je $K := \mathbf{Q}(\sqrt[3]{2}, \sqrt{-3})$. Kako smo vidjeli, ono je Galoisovo i neabelovo stupnja 6, s Galoisovom grupom $\{1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$ uz $\sigma^3 = \tau^2 = 1$ i $\tau\sigma = \sigma^2\tau$. Može se uzeti da je $\sigma(\sqrt[3]{2}) = \rho\sqrt[3]{2}$ i $\sigma(\rho) = \rho$. Lako se vidi da se 2 i 3 granaju u K, a može se pokazati da su ostali prosti brojevi nerazgranati.
Opišimo $Frob_2$. Kako je 2 inertan u $\mathbf{Q}(\rho)$, zaključujemo da mora biti $2O_K = \mathcal{P}^3$ za neki prosti ideal $\mathcal{P}$. Zato je $f = 2$, a restrikcija od $I_\mathcal{P}$ na $\mathbf{Q}(\rho)$ treba biti trivijalna pa je $I_\mathcal{P} =< \sigma >$, i konačno $Frob_2$ klasa τ modulo $< \sigma >$.
Vidimo da $Frob_2$ shvaćen kao skup elemenata od G čini jednu klasu konjugiranosti.
Opiv simo sad $Frob_3$. Kako se 3 grana u $\mathbf{Q}(\rho)$ i u $\mathbf{Q}(\sqrt[3]{2}$, vrijedi $3O_K = Q^6$ za neki prosti ideal Q. Sad je $e = 6$ pa je $f = 1$, $D_\mathcal{P} = I\mathcal{P} = G$, tj. $Frob_3 = 1$ kao element od G/G, a kao skup elemenata od G to je cijeli G, što nije klasa onjugiranosti.

Definicija $Frob_p$ za bilo koji p i proširenje.
Neka je L bilo koje Galoisovo proširenje od $\mathbf{Q}$, neka je p fiksirani prost broj i neka je $\mathcal{P}$ fiksirani prosti ideal u L iznad p. To znači da imamo uskladjenu familiju prostih ideala $\mathcal{P}_K$ za konačna Galoisova proširenja K. Za svaki $\mathcal{P}_K$ imamo $Frob_{\mathcal{P}_K} \in D_{\mathcal{P}_K}/I_{\mathcal{P}_K}$ koji su uskladjeni u smislu da su i svi $D_{\mathcal{P}_K}$ i svi $I_{\mathcal{P}_K}$ uskladjeni, pa su dobro definirani $D_\mathcal{P}$, $I_\mathcal{P}$ i $Frob_\mathcal{P} \in D_\mathcal{P}/I_\mathcal{P}$.
Ako je $\mathcal{Q}$ neki drugi prosti ideal iznad p, onda je $g\mathcal{P} = \mathcal{Q}$ za neki $g \in G$, pa su pripadni Frobeniusovi (odnosno klase) konjugirani itd., pa je dobro definirana klasa $Frob_p$ koju zovemo Frobeniusov element u p.

Uvod u aritmetiku eliptičkih krivulja

L-funkcija eliptičke krivulje (skica) - 25. lekcija

Prototip L-funkcije je (kompleksna) Riemannova zeta funkcija

$$\zeta(s) := \sum_{n\geq 1} \frac{1}{n^s} = \prod_p \frac{1}{1-p^{-s}}$$

za $Res > 1$, a produkt ide po svim prostim brojevima (Eulerov produkt). Riemannova zeta funkcija važna je jer u sebi nosi informaciju o dobrom dijelu tajne o prostim brojevima.
Prva generalizacija Riemannove zeta funkcije (i njoj srodnih) jest takva funkcija kojoj Eulerov produkt u nazivnicima ima kvadratne izraze (u p^{-s}). Takva je L-funkcija eliptičke krivulje E nad $\mathbf{Q}$ (uz izuzetak konačno mnogo faktora za proste p u kojima E ima lošu redukciju). Ona ima važnu ulogu u aritmetici eliptičkih krivulja.
Neka je E eliptička krivulja nad $\mathbf{Q}$ s globalnim minimalnim modelom (tada ona u pravilu ima općenitiju jednadžbu od one $y^2 = x^3 + ax^2 + bx + c$).
Neka je Δ diskriminanta od E i neka je E_p pripadna krivulja dobivena iz E redukcijom njene jednadžbe modulo p. Znamo da vrijedi:
(I) Ako je p ne dijeli Δ onda je E_p opet eliptička krivulja; tada definiramo $a_p := p + 1 - N_p$ gdje je N_p broj točaka na reduciranoj krivulji, s koordinatama iz $\mathbf{F}_p$;
vrijedi $|a_p| < 2\sqrt{p}$ (Hasse-Weilova ocjena - analogon Riemannove slutnje): tada definiramo pripadni Eulerov p-faktor L- funkcije kao

$$L_p(E,s) := \frac{1}{1 - a_p p^{-s} + p \cdot p^{-2s}}$$

(vidimo da je u nazivniku kvadratan faktor - on ima i aritmetičko značenje koje sad ne obradjujemo).
(II) Ako $p|\Delta$ (znači za konačno mnogo p) onda je redukcija loša, reducirana krivulja je singularna kubika (ima genus 0) i imamo dva slučaja.
(i) redukcija je multiplikativna (ili polustabilna) - tipični je primjer $y^2 = x^3 + ax^2$ sa singularnom točkom $(0,0)$ (dvostruka točka ili node) i opet imamo dva podslučaja:

(A) Rascjepivi slučaj (kad su tangente na grane u singularnoj točki definirane nad $\mathbf{F}_p$, tj. kad je a kvadrat); tada definiramo

$$L_p(E,s) := \frac{1}{1-p^{-s}}$$

(B) Nerascjepivi slučaj (kad tangente na grane u singularnoj točki nisu definirane nad $\mathbf{F}_p$, tj. kad a nije kvadrat); tada definiramo

$$L_p(E,s) := \frac{1}{1+p^{-s}}.$$

(ii) redukcija je aditivna (nestabilna) - tipični je primjer $y^2 = x^3$ sa singularnom točkom $(0,0)$ (šiljak ili kasp); tada definiramo

$$L_p(E,s) = 1$$

Konačno definiramo L- funkciju od eliptičke krivulje E kao

$$L(E,s) := \prod_p L_p(E,s) = \sum_{n\geq 1} \frac{a_n}{n^s}.$$

Ako dodatno definiramo da je $a_p = 1$ za multiplikativni rascjepivi slučaj, $a_p = -1$ za multiplikativni nerascjepivi slučaj i $a_p = 0$ za aditivni, vrijedi

$$L(E,s) = \prod_{p \text{ ne dijeli } \Delta} \frac{1}{1-a_p p^{-s} + p\cdot p^{-2s}} \prod_{p|\Delta} \frac{1}{1-a_p p^{-s}}$$

.

Konstrukcija L-funkcije eliptičke krivulje (nad Q) iz l-adske reprezentacije Galoisove grupe.

Pokazuje se da informacije o L-funkciji eliptičke krivulje nosi pripadna l-adska reprezentacija Galoisove grupe $G := \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. Time će se dobiti uniformna definicija L-funkcije, što je osnova njenog suvremenog proučavanja.
Podsjetimo da smo u Teoremu u 24. lekciji naveli da za prosti broj p koji je različit od l i u kojemu je redukcija dobra, vrijedi

$$a_p = tr\rho_{E,l}Frob_p \ i \ det\rho_{E,l}Frob_p = p$$

Podsjetimo, takodjer da tu l-adska reprezentacija $\rho_{E,l}$ nije išla s cijele Galoisove grupe G, već njene podgrupe $\mathrm{Gal}(K_{E,l}/\mathbf{Q})$, gdje je $K_{E,l}$ polje generirano koordinatama točaka reda l^n za $n \geq 1$.

Kako se ta polja mijenjaju za različite E i l, dobro je to izbjeći proširenjem reprezentacija na G (a i inače, G je središnji objekt suvremene aritmetike, pa ovo gledamo tako da variranjem E ili, općenito, abelovih mnogostrukosti i sličnih geometrijskih objekata, dobivamo familije reprezentacija od G za sve proste l). Kako smo vidjeli, to se prirodno provodi tako da najprije napravimo restrikciju s G na $\mathrm{Gal}(K_{E,l}/\mathbf{Q})$, potom komponira s $\rho_{E,l}$; kompoziciju opet označimo kao $\rho_{E,l}$ (što ne bi trebalo stvarati zabunu). Naravno, uz ovaj dobitak, dolazi i do gubitaka; prvi je što l-adska reprezentacija s G nije više vjerna (injektivna), a drugi je što sad ni jedan p nije nerazgranat. Zato nastaje problem s tragom i determinantom Frobeniusovih elemenata. Posljednja se poteškoća tu može razriješiti.
(I) Neka je u p redukcija dobra i $p \neq l$. Tada je, prema teoremu Serrea i Tatea, $\rho_{E,l}$ djeluje trivijalno na sve elemente od I_p - to je inače definicija nerazgranatosti reprezentacije u p (jer je restrikcija te grupe na $\mathrm{Gal}(K_{E,l}/\mathbf{Q})$ trivijalna grupa); zato ni trag ni determinanta matrica koje pripadaju elementima koje čine $Frob_p$ ne ovise o reprezentantima, pa su oni jednoznačno definirani i vrijedi

$$a_p = tr\rho_{E,l}Frob_p \; i \; det\rho_{E,l}Frob_p = p$$

(gdje, za razliku od prijašnjih idfentičnih formula po izgledu, $Frob_p$ se odnosi na cijelu grupu G). Uočite da se sad p faktor L-funkcije može zapisati kao

$$L_p(E,s) = \frac{1}{\det(I - (\rho_{E,l}Frob_p)p^{-s})}$$

(II) Neka je u p redukcija loša i neka je $p \neq l$.
Tada $\rho_{E,l}$ djeluje trivijalno na sve elemente od I_p, tj. matrice koje su pridružene elementima inercijske grupe u p nisu sve jedinične matrice. Podsjetimo da su matrice $\rho_{E,l}(\sigma)$ za $\sigma \in G$ kvadratne drugog reda jer prirodno djeluju na slobodni $\mathbf{Z}_l$ modul $T_l(E)$ ranga 2, što se prirodno proširuje na djelovanje na $\mathbf{Q}_l$ vektorski prostor $V_l(E)$ dimenzije 2.
Sad činjenica da je $\rho_{E,l}(I_p)$ grupa matrica koja sadrži bar jednu nejediničnu matricu povlači da je fiksni podprostor od I_p

$$V_l(E)^{I_p} := \{v \in V_l(E) : \rho_{E,l}(\sigma)(v) = v, \text{ za sve } \sigma \in I_p\}$$

vektorski podprostor od $V_l(E)$ različit od $V_l(E)$, pa je jednodimenzionalan ili nul-dimenzionalan.

Pokazuje se da je $V_l(E)^{I_p}$ jednodimenzionalan ako i samo ako je redukcija u p multiplikativna. Nadalje, $Frob_p$ djeluje na $V_l(E)^{I_p}$ kao množenje s 1 u rascjepivom slučaju, a kao množenje s -1 u nerascjepivom. Zato dobijemo:
$\frac{1}{\det(I-(\rho_{E,l}Frob_p|V_l(E)^{I_p})p^{-s})} = \frac{1}{1-p^{-s}}$ u rascjepivom, a
$\frac{1}{\det(I-(\rho_{E,l}Frob_p|V_l(E)^{I_p})p^{-s})} = \frac{1}{1+p^{-s}}$ u nerascjepivom slučaju.
Naravno, $V_l(E)^{I_p}$ je nul-dimenzionalan akko je redukcija aditivna. Uočite da je tada trivijalno $\frac{1}{\det(I-(\rho_{E,l}Frob_p|V_l(E)^{I_p})p^{-s})} = 1$
Uočimo još da je $V_l(E)^{I_p} = V_l(E)$ akko je u p redukcija dobra.
Zaključujemo da za sve $p \neq l$ imamo uniformnu formulu

$$L_p(E,s) = \frac{1}{\det(I - (\rho_{E,l}Frob_p|V_l(E)^{I_p})p^{-s})}$$

(ovdje | znači restrikciju djelovanja operatora).
Uočite, posebno, da ovo vrijedi za sve proste l i rezultati ne ovise o izboru prostog broja l (osim što za svaki l treba izključiti jedan p, naime $p = l$). Takvu familiju l-adskih reprezentacija zovemo uskladjenom.