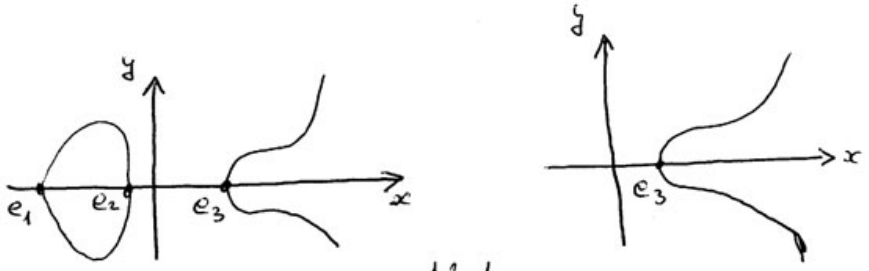
Uvod u aritmetiku eliptičkih krivulja

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).

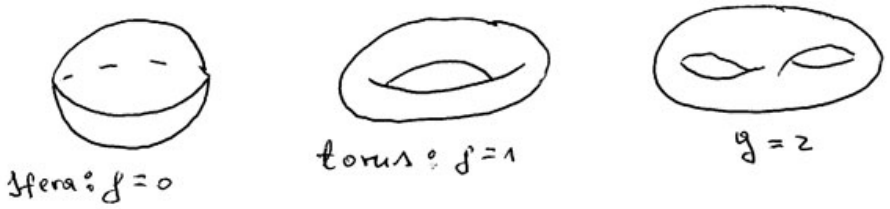


Sl. 1.

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 ćemo 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

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

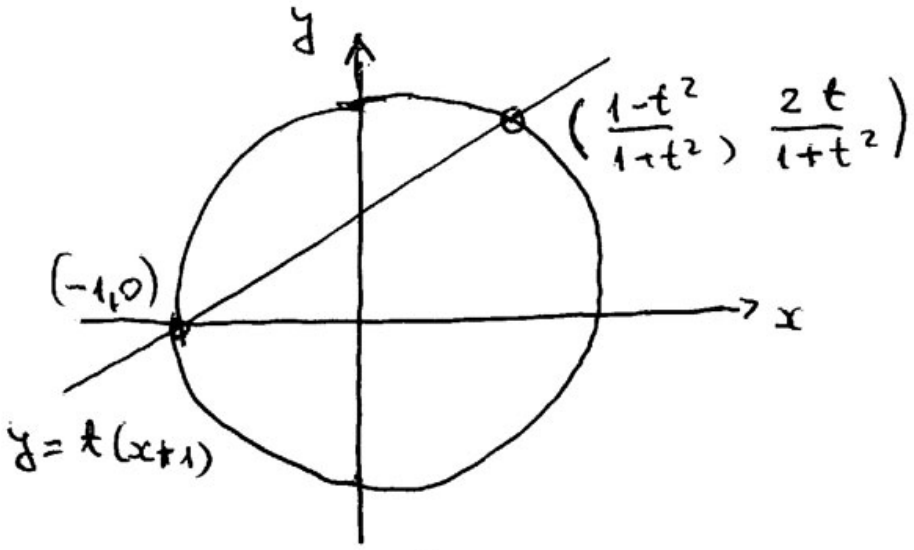
gdje su ϕ i ψ racionalne funkcije od t. Za zaključak o nemogućnosti potrebne su nam sljedeće činjenice:
(i) ta se parametrizacija prosiruje, po istoj formuli, na kompleksne brojeve t i kompleksne točke na eliptičkoj krivulji
(ii) ova nova parametrizacija proširuje se do neprekinute bijekcije (čak i više) 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

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

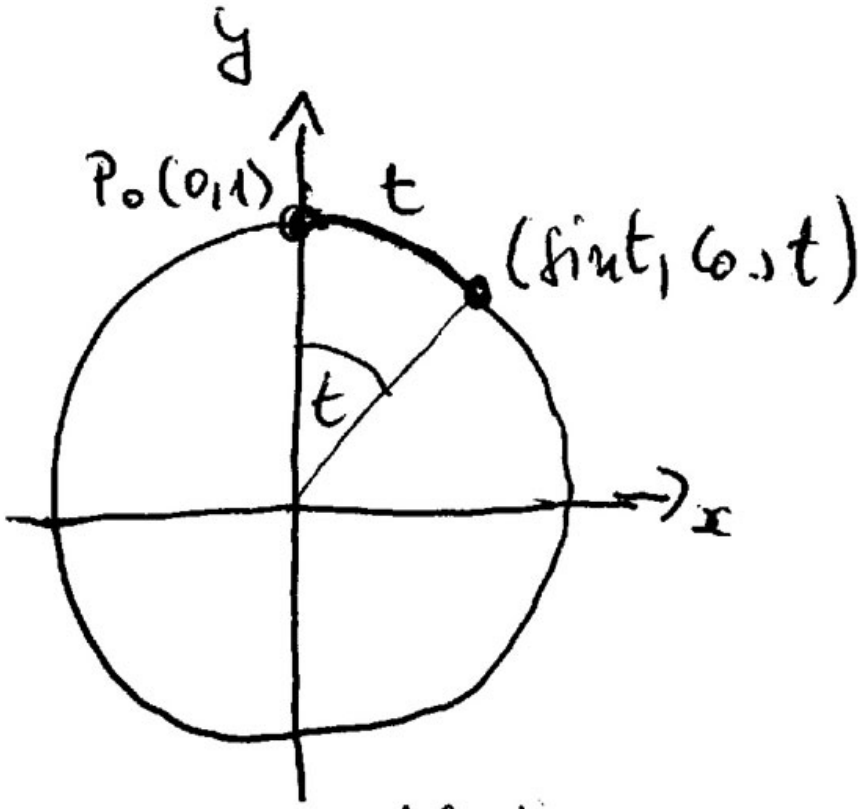
za neki zgodno odabrani fiksirani α i varijabilni u. Abel je uveo novinu da gornja granica bude funkcija od rezultata, tj.

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

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

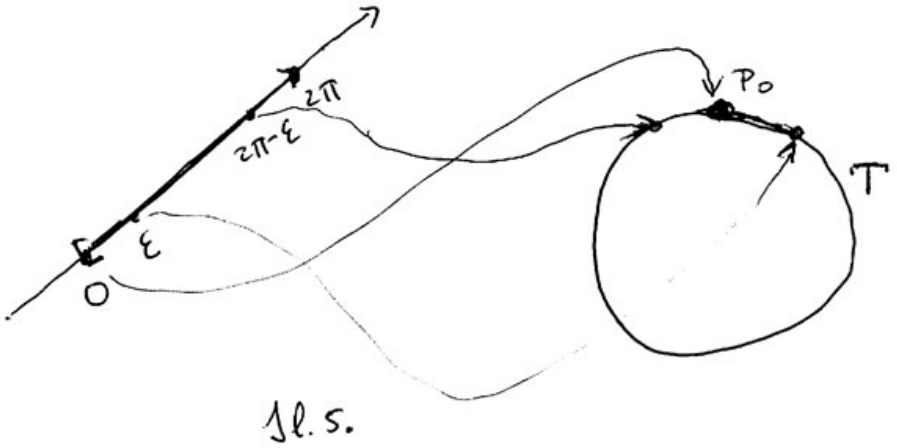
$$\mathbf{R} \mapsto \mathbf{T},\ t \mapsto (\sin t, \cos t).$$

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 točakama 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.).

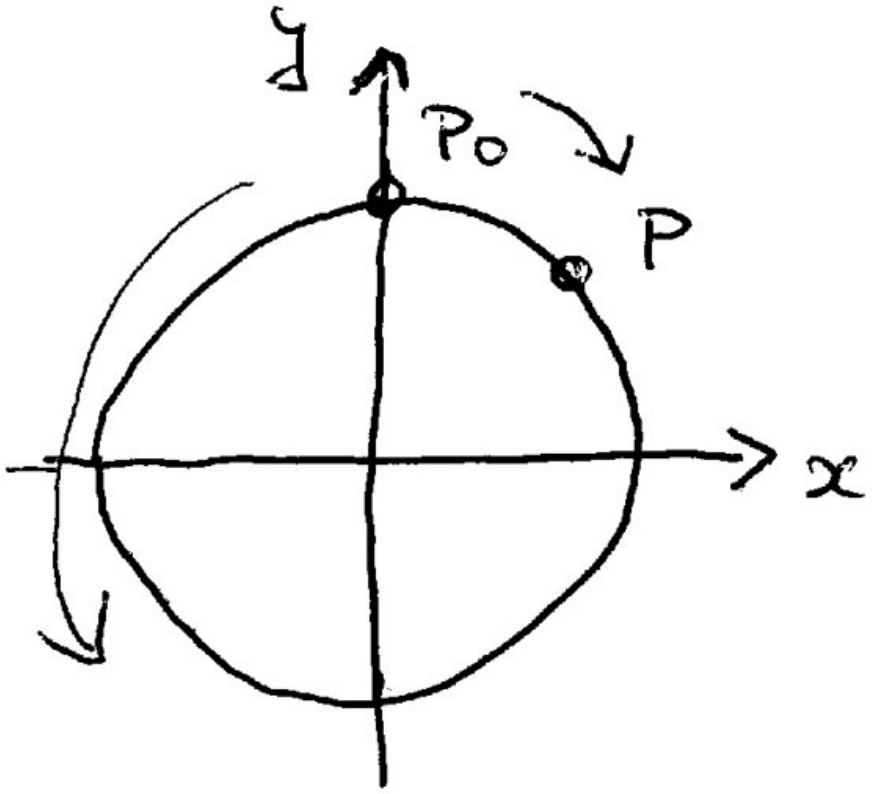


Sl. 5.

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:

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

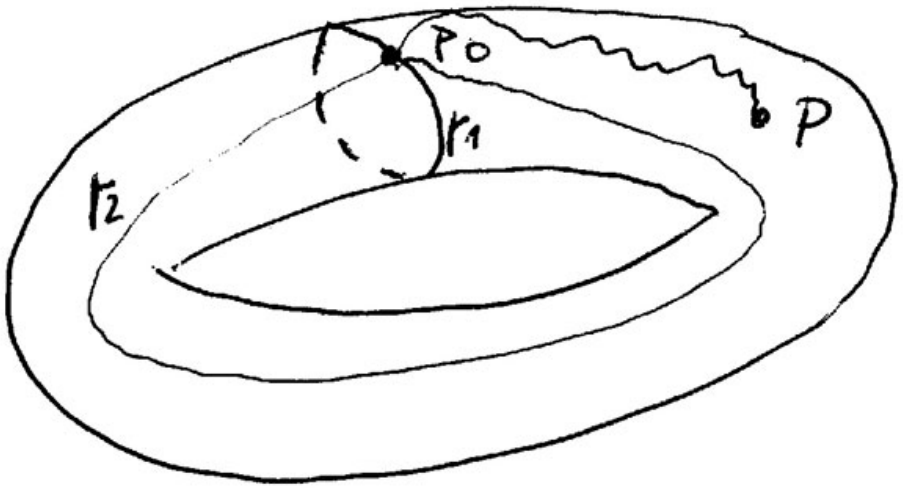
s jedinstvenim rješenjem $h = \sin$, a odavde $r = \cos$, kako smo i tvrdili.

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

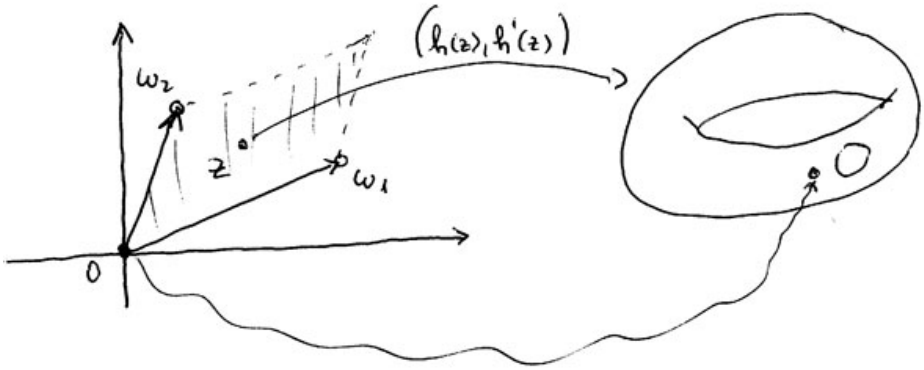
$$P \mapsto \int_O^P \frac{dx}{y} \tag{6}$$

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.