Trianglar med givna omskrivna och inskrivna cirklar

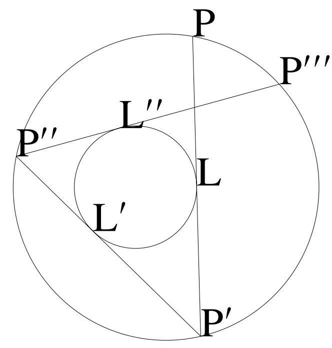
Ulf Persson

Matematiska Institutionen
Chalmers Tekniska Högskola och
Göteborgs Universitet
ulfp@chalmers.se

Inledning

Detta är den andra i en planerad serie av tre artiklar om moduli rum för trianglar. I den första - Modulirum för trianglar (Normat 57:1 10-21) satte vi upp maskineriet och härledde några kända formler. Huvudpoängen var att en triangel upp till kongruens beror på tre parametrar, och således upp till likformighet på två. Naturliga parametrar för det första fallet utgöres av triangelns sidor, medan i det andra av dess vinklar som inte kan vara godtyckliga utan måste addera upp till π. I denna artikel skall vi konstruera trianglar med given omskriven radie (R) och inskriven radie (r), dessa bör utgöra ett 1-dimensionellt system, och vi beskriver denna familj. Resultatet är något slående och bygger på transcendenta metoder. Istället för att begränsa oss till de reella talen betraktar vi de komplexa och beskriver därmed en polynomrelation som kan parametriseras med en elliptisk kurva, d.v.s. en komplex kurva E av formen $\mathbb{C}/\Lambda$. Sådana parametriseringar är klassiska och göres naturligast med så kallade theta-funktioner. I den avslutande artikeln tänker jag presentera en explicit sådan parametrisering i samband med problemet att beskriva alla trianglar med samma omkrets och area, som introducerades i Normat av Bengt Ulin (Normat 55:2) och som utgjorde den ursprungliga inspirationen för denna artikelserie. I denna artikel skall vi ta parametriseringen för given och utnyttja att en elliptisk kurva utgör en grupp, och visa att vårt problem är intimt förknippat med tre-torsions punkterna till denna kurva, vilket vill säga punkter $z \in E$ sådana att $3z = 0$ d.v.s. punkterna $\frac{1}{3}\Lambda/\Lambda$. Slutsatsen är att den 1-dimensionella familjen ovan parametriseras av en oval av reella punkter till en elliptisk kurva, modula translation med en 3-torsionspunkt. Jag tänker avsluta med ett försök att konkretisera den allmänna lösningsstrategin genom att ge explicita formler.

Att inskriva och omskriva en triangel



Givet en cirkel C_O med radie R och en innesluten cirkel C_I med radie r kan dessa placeras på ett 1-dimensionellt antal olika sätt, helt enkelt genom att föreskriva distansen d mellan dess centra. Det naturliga är nu att ta en punkt P på cirkeln C_O och välja en av två tangenter L från P till C_I och låta P' vara den andra skärningspunkten av L med C_O. Kordan P, P' är således tangent till C_I. Från P' kan man dra två tangenter till C_1, en av dem L är redan dragen och låt L' vara den andra. På motsvarande sätt erhåller vi då en ny punkt P'' på C_O. Vi fortsätter konstruktionen och erhåller P'''. Om denna punkt sammanfaller med P säger vi att processen sluter sig efter en triangel, och den uppkomna triangeln P, P', P'' kommer per konstruktion ha C_O som omskriven cirkel och C_I som inskriven. Dock det finns ingen anledning att förvänta sig att vi får en triangel om vi startar med en godtycklig punkt P på C_O, denna måste uppenbarligen väljas med omsorg. Kanske finns det bara en sådan triangel som således är unik given av datat R, r, d?

Situationen är emellertid inte som man kan förvänta sig. Låt oss antaga att $d = 0$ d.v.s. de två cirklarna är koncentriska. Varje till C_I tangerande korda till C_0 kommer ha samma längd. Den sökta triangeln kommer därmed att vara liksidig. Detta betyder att kvoten R/r lätt kan beräknas. Om sidlängden är a kommer vi få att $R = \frac{a^3}{4A}$ och $r = \frac{2A}{3a}$ (se bis sid 19) där A är arean. Vilket ger $R/r = 3a^4 8A^2 = 2$ ty uppenbarligen gäller att $A = \frac{\sqrt{3}}{4}a^2$. Med andra ord om $R/r \neq 2$ och cirklarna är koncentriska kommer vi aldrig att erhålla en sluten triangel, däremot om likhet gäller, får vi en sluten triangel oberoende av vilken punkt P vi startar med på den yttre cirkeln. Det förvånande är att denna situation gäller i allmänhet. D.v.s. givet två cirklar, den ena innesluten i den andra, kommer vi antingen att aldrig erhålla någon sluten triangel, eller alltid erhålla en, oberoende av vilken punkt på den yttre cirkeln vi startar med.

Den elliptiska kurvan

Beviset för detta är elegant om än något transcendent och gäller för en betydligt mera generell situation. Först ersätter vi de två cirklarna med godtyckliga kägelsnitt A, B definierade över de komplexa talen. D.v.s. vi betraktar godtyckliga ickedegenererade tertiära (d.v.s. tre variabler) kvadratiska former över de komplexa talen och därefter dess samtliga nollställen såsom delmängder av det komplexa projektiva planet $\mathbb{C}P^2$. Detta betyder att vi endast intresseross för tre-tuppler (så kallade homogena ko-ordinater) (x_0, x_1, x_2) upp till proportionalitet. Det projektiva planet är en 2-dimensionell kompakt komplex mångfald, och nollställena till en sådan icke-singuljär kvadratisk form utgör en kompakt 1-dimensionell mångfald isomorf med Riemann-sfären $\mathbb{C}P^1$. Detta är elementärt via en projektionsparametrisering och vi skall återkomma till detta i ett senare avsnitt. Vi betraktar sedan par (L,p) där L är en tangent till B och p en punkt på snittet $L \cap A$. Detta kommer att utgöra en kurva E i den komplexa ytan $A \times B$ med projektionerna $\pi_A : E \to A$ givet av $(L,p) \mapsto p \in A$ och $\pi_B : E \to B$ för vilken (L,p) avbildas på tangeringspunkten av L till på B. Eftersom A, B är kägelsnitt skär varje linje dem i två (inte nödvändigtvis distinkta) punkter, och genom varje punkt återfinner man två tangenter (som sammanfaller omm punkten ligger på kägelsnittet). Detta medför att fibrerna till projektionerna alltid består av två punkter (som kan sammanfalla, i själva verket fyra gånger). Detta betyder att eftersom A, B är Riemannsfärer att kurvan E kan beskrivas av en bihomogen form av bigrad $(2,2)$. En bihomogen form $F(x_0, x_1; y_0, y_1)$ är en form som är homogen i varje variabel separat, och en bihomogen form av bigrad $(1,1)$ är helt enkelt vad man kallar en bilinjär form. I vårt fall kommer en bilinjär form att spännas av de fyra monomen $x_0y_0, x_0y_1, x_1y_0, x_1y_1$. Om vi kallar dessa för X, Y, Z, W kan vi betrakta dessa fyra variabler som homogena ko-ordinater för $\mathbb{C}P^3$. Variablerna är inte oberoende utan satisfierar relationen $XW = YZ$. Detta är en kvadrik i $\mathbb{C}P^3$ och vi har således presenterat $\mathbb{C}P^1 \times \mathbb{C}P^1$ som en kvadrik i det komplexa projektiva rummet. (Denna konstruktion är mycket välkänd och kan givetvis generaliseras och är känd som Segre inbäddningen av produkter av projektiva rum.). Den bihomogena $(2,2)$ formen kan nu presenteras som en kvadrik Q i X, Y, Z, W men den kvadriken är inte unikt definerad på grund av relationen $XW = YZ$, vad man erhåller är dock en 1-dimensionell skara av kvadriker spända av den givna $XW - YZ$ och Q (som är bara väldefinerad modulo $XW - YZ$). Den elliptiska kurvan E är nu beskriven som snittet av två kvadriker.

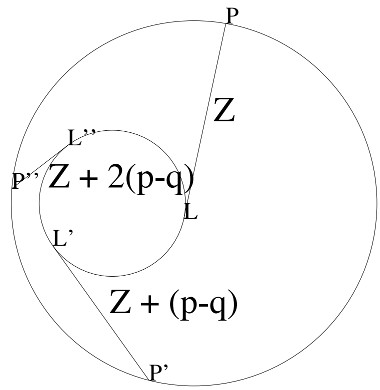
Det stora steget är att parametrisera E som $\mathbb{C}/\Lambda$. Det väsentliga vi skall utnyttja ur detta är att denna kurva bu visar sig vare en grupp vars gruppstruktur är kompatibel med dess komplexa struktur. Vidare gäller att varje avbildning som avbildar nollan på nollan är en homomorfi (i själva verket kan den ges av $z \mapsto \lambda z$ där $\lambda\Lambda \subset \Lambda$). Speciellt involutionerna som fixerar nollan ges av $z \mapsto -z$ och i allmänhet kan en godtycklig involution återföras på en sådan via en translation, ur vilket vi sluter direkt att varje involution är av formen $z \mapsto p - z$, där p är ett fixt element i E.

Det mesta av det ovanstånede bör vara tillgängligt för var och en som har tagit del av en introduktionskurs i komplex analys. Det skulle emellertid ta mig alltför mycket utrymme att bevisa dessa elementära basfakta som dessutom finns lätt tillgängliga i litteraturen och är kanske rentav kända för många läsare. Men oavsett om detta är känt eller inte, har det en poäng, nämligen den att mer avancerad matematik inte bara har tillämpningar på elementär matematik utan även ofta är oundgänglig även om man begränsar sig till elementära frågor.

Trianglar och 3-torsion

Så låt oss tillämpa karaktäriseringen av involutioner. Det följer att $\pi_A(z) = p - z$ och $\pi_B(z) = q - z$. Låt $z = (L, P)$ där vi identifierat tangenten L med dess tangeringspunkt i B. Vi finner då med behållandet av terminologin ovan att $(L, P') = p - z$ och $(L', P' = q - (p - z) = q - p + z$.

Applicerar vi detta en gång till får vi $(L''P'') = 2(q - p) + z$ och gör vi det en tredje gång skall vi återkomma till $(L, P) = z$ d.v.s. $3(q-p)+z = z$, d.v.s. villkoret är att $3(q-p) = 0$ vilket uttryckes att $q-p$ är en 3-torsions punkt, vilket uppenbarligen är oberoende av z. Mera allmänt inser vi att denna process att ta tangerande kordor sluter sig efter ett ändligt antal steg om och endast om $q - p$ är en så kallad torsionspunkt, d.v.s. för något tal n gäller att $n(q - p) = 0$. Torsionspunkter utgör ett nyckelbegrepp inom den aritmetiska teorin för elliptiska kurvor och kan ses som en analogi till enhetsrötterna på enhetscirkeln.

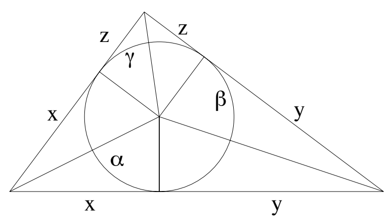


Slutna trianglar

Så låt oss nu explicit beskriva d givet R, r för att vi skall kunna få slutna trianglar. Genom skalning kan vi för enkelhets skull antaga att $r = 1$. De tre hörnen på triangeln ger upphov till avstånden x, y, z. Dessa kan beskrivas som $\tan\alpha, \tan\beta$ och $\tan\gamma$ där $\alpha + \beta + \gamma = \pi$. Detta ger identiteten $x + y + z = xyz$. (Om den inskrivna cirkeln har radien r modifierar vi till $r^2(x + y + z) = xyz$.)

Låt oss betrakta likbenta trianglar. Sätt $x = y$ i den förra identiteten $xyz = x + y + z$ detta leder till $2x + z = x^2 z$ och således

$$z = \frac{2x}{x^2 - 1}$$



Vidare gäller (där $a = y + z, b = x + z, c = x + y$)

$$R = \frac{abc}{4A} = \frac{2x(x+z)^2}{2(4x+2z)}$$

observera att $x + z = x\frac{x^2+1}{x^2-1}$ och vi erhåller

$$R = \frac{(x^2+1)^2}{4(x^2-1)}$$

Således om vi känner $r = 1$ och R återfår vi $t = x^2 - 1 > 0$ genom den kvadratiska ekvationen

$$t^2 + 4(1-R)t + 4 = 0$$

med lösningarna

$$t = t_1 = 2((R-1) + \sqrt{R(R-2)}) \quad t = t_2 = 2((R-1) - \sqrt{R(R-2)})$$

Vi observerar att $R \geq 2$ med likhet precis för liksidiga trianglar $x = y = z = \sqrt{3}$

Givet x kan vi lätt beräkna höjden (se fig nedan)

$$H = 1 + \frac{x+z}{x} = \frac{2x^2}{x^2-1} = \frac{2(t+1)}{t} = 2 + \frac{2}{t}$$

av triangeln. Vi finner från ekvationen att $R-1 = \frac{t}{4} + \frac{1}{t}$ vilket ger oss och avståndet

$$d = H - R - 1 = \frac{1}{t} - \frac{t}{4}$$

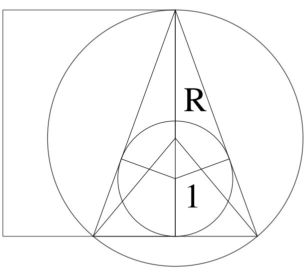
mellan den inskrivna och omskrivna cirkelns medelpunkter. Ur detta följer att

$$d^2 = (R-1)^2 - 1$$

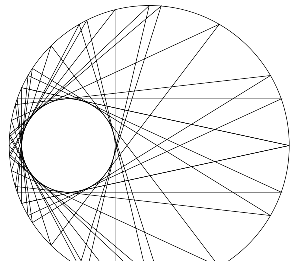
Detta löser vårt problem hur vi skall placera de två cirklarna för att kunna få en sluten triangel. Med andra ord givet R, r skall d väljas lika med $\sqrt{R(R-2r)}$

Vi kan nu nedan rita upp den 1-dimensionella familjen av alla trianglar med given omskriven och inskriven radie.

H



R/r=3



Betrakta nu en godtycklig trippel x, y, z associerad till enhetscirkeln enligt ovan. Givet två x, y kan vi erhålla den tredje $z = \frac{x+y}{xy-1}$. Om vi dessutom fixerar R så bestämmer en variabel, säg y, de övriga. Denna blir då en parameter för den 1-dimensionella familjen. Speciellt har vi ett villkor mellan x, y. Vilket? Introducera de elementära symmetriska funktionerna $\sigma_1 = x + y + z, \sigma_2 = xy + zx + yz, \sigma_3 = xyz$. Vi finner då att $R = \frac{(x+y)(y+z)(z+x)}{4A} = \frac{\sigma_1\sigma_2 - \sigma_3}{4\sigma_1 r}$. Eftersom i vårt fall $r = 1, \sigma_1 = \sigma_3$ kan vi förenkla till $4R = \sigma_2 - 1$. Stoppa in i denna $z = \frac{x+y}{xy-1}$ och vi kan förenkla till

$$4R(xy-1) = (1+x^2)(1+y^2)$$

Detta kan ses som en kvadratisk ekvation av x i termer av y nämligen

$$x^2 - \frac{4Ry}{1+y^2} + \frac{1+y^2+4R}{1+y^2}$$

uppenbarligen med lösningarna x, z. Man kontrollerar även lätt att om x är en lösning är den andra given av $\frac{x+y}{xy-1}$. Genom att betrakta diskriminanten

$$(1 + y^2 + 4R)(1 + y^2) - 4R^2y^2 = 0$$

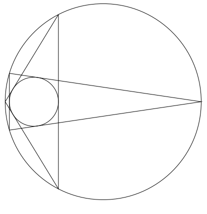
erhåller vi de möjliga värdena för y^2 och därmed även för y. De två nollställena y_i^2 är givna av

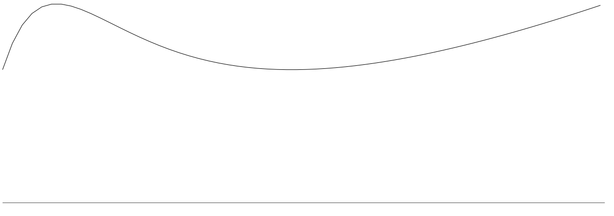
$$2R^2 - 2R - 1 \pm 2R\sqrt{R(R-2)}$$

och motsvaras uppenbarligen av likbenta trianglar $x = z$. Omkretsen p ges som funktion av y via $p(y) = 2(x + y + z) = 2(\frac{4Ry}{1+y^2} + y) = 2y(\frac{4R}{y^2+1} + 1)$. Vi finner att $p'(y) = (y^2 + 1)^2 - 4Ry^2 + 4R$ modulo en postiv faktor. Dess nollställen ζ_i^2 är enkla att finna och man noterar att $\zeta_i^2 - 1 = 2(R - 1 \pm \sqrt{R(R-2)})$ vilka vi känner igen. Dessa korresponderar även till liksidiga trianglar nu med $y = x$ eller $y = z$. Vi sluter därmed att $y_1 \leq \zeta_1 \leq \zeta_2 \leq y_2$ med likhet endast då $R = 2$. Funktionen $p(y)$ är således definerad i intervallet $[y_1, y_2]$ växer fram till ζ_1 avtar sedan fram till ζ_2 för att åter växa fram till y_2. Dess extremvärden antas därmed för de likbenta trianglarna, och genom att sätta in ζ_i finner vi att

$$2\sqrt{2R - 1 + 2\sqrt{R(R-2)}}(R - \sqrt{R(R-2)} + 1) \leq p(y) \leq$$
$$\leq 2\sqrt{2R - 1 - 2\sqrt{R(R-2)}}(R + \sqrt{R(R-2)} + 1)$$

Det finns två olika slags av likbenta trianglar. I ena fallet är de lika sidorna de längsta, i det andra fallet är de de kortaste. I det första fallet är den unika vinkeln mindre än $\pi/3$ i det andra fallet större än $\pi/3$. Vänsterledet (i ekvationen ovan) motsvarar det andra fallet, högerledet det första.





Polärer

Givet ett kägelsnitt kan man från varje punkt P utanför detta finna precis två tangenter genom P. Deras två beröringspunkter bestämmer en linje som kallas kägelsnittets polär med avseende på P. Denna kan skrivas ner enkelt ty till varje kvadratisk form korresponderar en unik symmetrisk bilinjär form, och genom att fixera ett koordinatpar till P bestäms en linjär form.

I det reella fallet behöver inte beröringspunkterna vara reella, men linjen blir automatiskt reell. Man säger att punkten P ligger innanför kägelsnittet om beröringspunkterna är komplext konjugerade, men utanför om de är reella. I det senare fallet kan vi skilja mellan den vänstra och och högra tangenten.

Antag nu att kägelsnittet är enhetscirkeln och $P = (a, b)$ är en godtycklig punkt. Polären ges av linjen $ax + by = 1$

Vi betraktar egentligen den homogena formen $X^2 + Y^2 - Z^2$ (homogeniseringen av $x^2 + y^2 - 1 = 0$) den associerade bilinjära formen ges av $X_0X_1 + Y_0Y_1 - Z_0Z_1$ fixera $(X_0, Y_0, Z_0) = (a, b, 1)$ och dehomogenisera till $aX_1 + bY_1 - Z_1$ och berörings-punkterna ges således av ekvationssystemet

$$\begin{aligned} ax + by &= 1 \\ x^2 + y^2 &= = 1 \end{aligned}$$

Dessa leder till två kvadratiska ekvationer för x, y respektive

$$\begin{aligned} x^2 - \frac{2a}{a^2 + b^2}x + \frac{1 - b^2}{a^2 + b^2} &= 0 \\ y^2 - \frac{2b}{a^2 + b^2}y + \frac{1 - a^2}{a^2 + b^2} &= 0 \end{aligned}$$

Dessa kan givetvis lösas explicit, men innan vi gör detta noterar vi att mittpunkten P' på den korda dessa två punkter bestämmer utgöres av

$$(\frac{a}{a^2 + b^2}, \frac{b}{a^2 + b^2})$$

ur vilket vi inser att om avståndet från P till origo är d är avståndet från P' till origo $1/d$ och de tre punkterna ligger på en rät linje. Avbildningen $P \to P'$ är helt enkelt spegling i enhetscirkeln.

Vidare inser vi att kordans längd är givet av kvadratroten av summan av diskriminanterna vilket lätt beräknas till

$$2\frac{\sqrt{a^2 + b^2 - 1}}{a^2 + b^2}$$

De explicita lösningarna ges av

$$\begin{aligned} x &= \frac{a + b\sqrt{a^2 + b^2 - 1}}{a^2 + b^2} \quad , \quad y = \frac{b - a\sqrt{a^2 + b^2 - 1}}{a^2 + b^2} \\ x &= \frac{a - b\sqrt{a^2 + b^2 - 1}}{a^2 + b^2} \quad , \quad y = \frac{b + a\sqrt{a^2 + b^2 - 1}}{a^2 + b^2} \end{aligned}$$

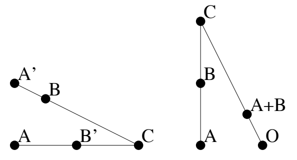
där den översta är den vänstra tangenten (sett från ursprungspunkten) och den nedersta den högra, en distinktion vi endast kan göra i det reella fallet.

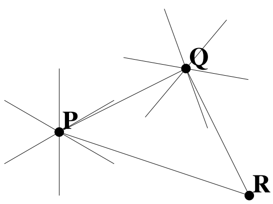
På liknande sätt kan vi till varje punkt på enhetscirkeln beskriva de två skärningspunkterna med tangenten och en omgivande cirkel.

Den geometriska gruppstrukturen

Givet två punkter P, Q på en kubik bör vi kunna geometriskt beskriva hur vi får punkten $P + Q$ på kubiken. Men kubiken är inte en elliptisk kurva i strikt bemärkelse, utan bara ett homogent rum av en sådan. För att kunna identifiera den med en elliptisk kurva måste vi först fixera en punkt som 'nollan'. Däremot mängden av alla translationer på en kubik utgör en elliptisk kurva med en kanonisk enhetselement, nämligen identitetstranslationen. En translation är entydigt bestämt av att vi bestämmer bilden A' av en punkt A. Givet detta hur finner vi bilden B' av B? Vi tar helt enkelt linjen L genom A' och B som skär kubiken i en tredje punkt C. Dra nu linjen L' genom C och A som skär i den tredje punkten B' som är den sökta.

Det hela bygger på att summan av tre punkter på en linje skall vara konstant, således $A+B'+C = A'+B+C$ varur följer $A' - A = B' - B$. Ur detta inser vi lätt hur vi adderar när vi har valt en punkt O som nolla. Vill vi addera A med B låter vi $O \mapsto A$, d.v.s. linjen L genom A och B skär i C och sedan tar vi den residuella intersektionen mellan C och O. Detta är välkänt men oftast inskränker man sig i det kubiska fallet till att ta O som en inflektionspunkt ty då kan man identifiera $P+Q+R = 0$ med att P, Q, R ligger på en linje. Notera att om vi fixerar en nolla O och en fix punkt C kommer linjerna genom C att definera en involution. Summan av punkterna i ett par kommer alltid vara konstant, nämligen det residuella snittet P med linjen genom C och O, vilket visar att denna involution ges av $z \mapsto P - z$.





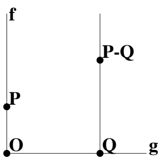
Något snarlikt bör även gälla för en $2,2$ kurva i $\mathbb{C}P^1 \times \mathbb{C}P^1$ men vad? Det råder en intim relation mellan $\mathbb{C}P^1 \times \mathbb{C}P^1$ och $\mathbb{C}P^2$ bägge utgör kompaktifieringar av $\mathbb{C}^2$ i det första fallet med två skärande linjer, i det andra fallet med en enda linje (oändlighetslinjen). Mer explicit betrakta två distinkta punkter P, Q på $\mathbb{C}P^2$. Var och en av dessa ger upphov till en skara av linjer parametriserade av $\mathbb{C}P^1$ nämligen linjerna genom var och en av punkterna. En godtycklig punkt R utanför linjen L genom P, Q bestäms nu som skärningspunkten av två linjer ur vardera skaran, nämligen linjerna PR och QR. Men om R ligger på L har vi problem. Om $R = P$ kan vi välja en godtycklig linje genom P samt L, och på motsvarande sätt om $R = Q$. Vi säger att P, Q blåses upp. Däremot om $L \ni R \neq P, Q$ finns det ingen distinktion paret (L, L) gäller i samtliga fall. Vi blåser därmed ner L. Efter denna process kommer de numera icke snittande linjerna genom P och Q respektive utgöra de två fibreringarna av $\mathbb{C}P^1 \times \mathbb{C}P^1$. Tag nu en kubisk kurva C och välj $P, Q \in C$ och låt O vara den residuella snittet med L. Efter den föregående operationen kommer nu C att bli en $2,2$ kurva och punkterna P, Q kommer att ge upphov till de två involutionerna på denna via de naturliga projektionerna.

Man kan även rent algebraiskt göra transformationen. Antag att P, Q är givna av $(0,0,1)$ och $(0,1,0)$ respektive. En punkt (x,y,z) ger då upphov till de bihomogena ko-ordinaterna $(x,y;x,z)$ ty linjerna genom punkterna är parametriserade av $(x,y,0)$ och $(x,0,z)$ respektive. Om $x \neq 0$ har vi inga problem, vi kan dehomogenisera med x och får avbildningen $(1,y,z) \mapsto (y;z)$. Omvänt erhåller vi en avbildning

$$\mathbb{C}P^1 \times \mathbb{C}P^1 \ni (x_0, x_1; y_0, y_1) \mapsto (x_0 y_0, x_1 y_0, x_0 y_1) \in \mathbb{C}P^2$$

Låt nu $C(x,y,z)$ vara en kubik som går genom punkterna P och Q. Det är lätt att inse att monomen y^3, z^3 därmed inte förekommer. Om vi nu genomför substitutionen $C(x_0y_0, x_1y_0, x_0y_1)$ finner vi att vi kan bryta ut faktorn x_0y_0. Vad som återstår är ett bihomogent polynom av grad två. Ett exempel är den glatta kubiken $x^2y + y^2z + z^2x$ som ger upphov till formen $x_0^2y_1^2 + x_0x_1y_0^2 + x_1^2y_0y_1$

Linjerna i planet kommer nu att korrespondera mot $(1,1)$ kurvor i kvadriken, ty de kommer att snitta varje fiber i de två fibreringarna. Detta motsvaras av snitt med hyperplan i rummet. Det blir nu lätt att inse följande.



Låt O vara nollan. Tangentplanet vid O till kvadriken består av två snittande fibrer f, g, och de residuella snitten utgöres av P och Q. För att addera två punkter A, B på kurvan C tar vi planet genom O, A, B detta snittar C i ytterligare en punkt X ty C är en kvartik. Tag nu planet som innehåller tangentlinjen till C vid O och går genom X, denna skär C i två sammanfallande punkter i O (tangerar) och det finns således en fjärde snittpunkt X' vilken vi identifierar med $A+B$.

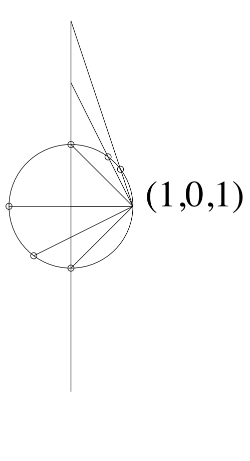
Det är nu lätt att inse att om $f \cap C = \{O, P\}$ kommer involutionen på C given genom att snitta med fibrerna parallella till f ges av $z \mapsto P - z$, och analogt i fallet $g \cap C = \{O, Q\}$. Tar vi en fiber parallel till g och passerar genom Q kommer det residuella snittet att utgöras av $P - Q$.

Den bihomogena ekvationen

En cirkel kan parametriseras av den reella projektiva linjen $\mathbb{R}P^1$. När det gäller enhetscirkeln skulle man kanske tro att $(x,y) \mapsto (\frac{x}{\sqrt{x^2+y^2}}, \frac{y}{\sqrt{y^2+y^2}})$ skulle duga, men den avbildar $(-x,-y)$ på en annan punkt än (x,y). Lösningen är helt enkelt att kvadrera, d.v.s.

$$(x,y) \mapsto (\frac{x^2-y^2}{x^2+y^2}, \frac{2xy}{x^2+y^2})$$

ty om $z = x + iy$ ges $z^2 = x^2 - y^2 + i2xy$



Vi kan parametrisera enhetscirkeln $x^2 + y^2 = z^2$ genom att projicera från punkten $(1,0,1)$ till y-axeln given av $(0,x,y)$. Vi betraktar linjen $s(0,x,y) + t(1,0,1)$ och sätter in den i ekvationen. Efter att vi kortar bort $s = 0$ som motsvarar den fixa punkten $(1,0,1)$ på cirkeln, erhåller vi för den rörliga $s(x^2 - y^2) = t(2y)$ sätt $s = 2y, t = x^2 - y^2$ och vi parametriserar den rörliga punkten på cirkeln med $(x^2 - y^2, 2xy, x^2 + y^2)$ vilket för övrigt är den välkända parametriseringen av den diofantiska ekvationen given av Pythagoras sats.

Låt oss nu välja C_I som enhetscirkeln och C_O given av

$$(x+d)^2 + y^2 = R^2$$

och den (preliminära) parametriseringen av C_0 via

$$(x,y) \mapsto (\frac{R(x^2-y^2)}{x^2+y^2} - d, \frac{2Rxy}{x^2+y^2})$$

Betrakta nu $C_O \times C_I$ och fixera (x_0, y_0) (notera att vi har en liten annan konvention för att bättre ansluta till parametriseringarna ovan). Detta ger upphov till polärlinjen

$$(\frac{R(x_0^2-y_0^2)}{x_0^2+y_0^2} - d)(\frac{x_1^2-y_1^2}{x_1^2+y_1^2}) + (\frac{2Rx_0y_0}{x_0^2+y_0^2})(\frac{2x_1y_1}{x_1^2+y_1^2}) = 1$$

Förenklar vi detta erhåller vi följande bihomogena form

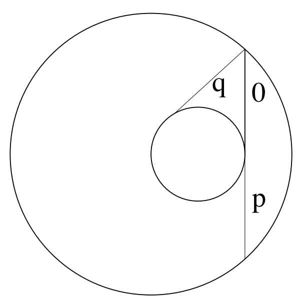
$$x_0^2((R-d-1)x_1^2-(R-d+1)y_1^2)+x_0y_0(4Rx_1y_1)+y_0^2(-(R+d+1)x_1^2+(R+d-1)y_1^2)$$

Vi kan ta dess diskriminant med avseende på (x_0, y_0) och erhåller då ett fjärdegrads polynom som kan skrivas som en kvadrik i x_1^2, y_1^2. Dess fyra nollställen uppvisar då en symmetri som gör att den motsvarande elliptiska kurvan är mycket speciell, nämligen den har komplex multiplikation med i och utgör $\mathbb{C}/\Lambda$ där $\Lambda = \mathbb{Z}[i]$ - de Gaussiska heltalen.

Gruppstrukturen

Vi skall nu tillämpa ovanstående för att ge en explicit gruppstruktur. För att så göra tar vi som nolla tangentstycket givet av vektorn $(0, \sqrt{R^2-(1-d)^2})$ med startpunkt $(1,0)$

Av beräkningstekniska skäl skulle vi vilja att detta motsvarades av punkten$(1,0;1.0)$. Detta tvingar oss till en omparametrisering av C_O. Detta göres genom en rotation med en lämplig vinkel θ att senare bestämmas. Explicit multiplicerar vi med den sedvanliga matrisen och erhåller



$$\begin{aligned}
x_0' &= x_0\cos\theta - y_0\sin\theta \\
y_0' &= x_0\sin\theta + y_0\cos\theta \\
(x_0')^2 &= x_0^2\cos^2\theta - 2x_0y_0\cos\theta\sin\theta + y_0^2\sin^2\theta \\
x_0'y_0' &= x_0^2\cos\theta\sin\theta + x_0y_0(\cos^2\theta - \sin^2\theta) - y_0^2\cos\theta\sin\theta \\
(y_0')^2 &= x_0^2\sin^2\theta + 2x_0y_0\cos\theta\sin\theta + y_0^2\cos^2\theta
\end{aligned}$$

Substiterar vi för $x_0^2\ldots$ motsvarande $(x_0')^2\ldots$ erhåller vi uttrycket,

$$\begin{aligned}
&((R(\cos^2\theta-\sin^2\theta)-(d+1))x_1^2+4R\cos\theta\sin\theta x_1y_1+(-R(\cos^2\theta-\sin^2\theta)+(d-1))y_1^2)x_0^2 \\
&\qquad +(-4R\cos\theta\sin\theta x_1^2+4R(\cos^2\theta-\sin^2\theta)x_1y_1+4R\cos\theta\sin\theta y_1^2)x_0y_0 \\
&+((-R(\cos^2\theta-\sin^2\theta)-(d+1))x_1^2-4R\cos\theta\sin\theta x_1y_1+(R(\cos^2\theta-\sin^2\theta)+(d-1))y_1^2)y_0^2
\end{aligned}$$

Vi väljer nu θ sådant att $R(\cos^2\theta - \sin^2\theta) - (d+1) = 0$ (D.v.s. $\cos 2\theta = (d+1)/R$. I det reella fallet är detta inga problem ty den inskrivna cirkeln är innesluten i den omskrivna, och således $R > (d+1)$)

Låt oss nu dehomogenizera, d.v.s. vi sätter $x_0 = x_1 = 1$ och $y_0 = x, y_1 = y$ och får därmed eftersom $2\cos\theta\sin\theta = \sin 2\theta = \sqrt{1-\cos^2 2\theta} = \sqrt{R^2-(d+1)^2}/R$ uttrycket

$$2\sqrt{R^2-(d+1)^2}(y-x+xy(y-x)) - 2(d+1)x^2 + 4(d+1)xy - 2y^2 + 2dx^2y^2$$

Vi kan nu räkna. Fixerar vi först $x = 0$ finner vi lösningen $y = \sqrt{R^2-(d+1)^2}$, detta motsvarar q, på samma sätt erhåller vi p genom att fixera $y = 0$ med lösningen $x = -\frac{\sqrt{R^2-(d+1)^2}}{d+1}$. För att finna $p - q$ fixerar vi $y = \sqrt{R^2-(d+1)^2}$ och erhåller

$$x = -\frac{(2d+1)\sqrt{R^2-(d+1)^2}}{(d-1)R^2-(d^2+1)(d+1)}$$

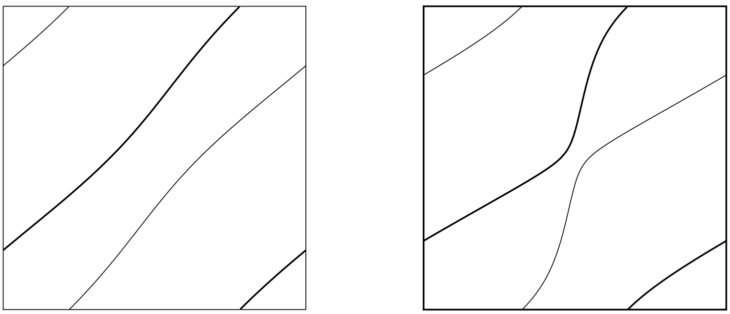
Nu kan vi i princip beräkna summan av två punkter. Först må vi identifiera $1,1$ kurvorna. Dessa kan skrivas i formen $Axy + Bx + Cy + D = 0$ med $D = 0$ varnades de som går genom vårt origo. De kan lätt parametriseras, ty för varje x kan vi lösa ut $y = -\frac{D+Bx}{C+Ax}$ vilket vi igenkänner som Möbiusavbildningar. I själva verket kan vi identifiera $1,1$ kurvorna med graferna till Möbiusavbildningar. Givet två punkter $(x_1, y_1), (x_2, y_2)$ kan vi finna den $1,1$ kurva som går genom dessa, samt origo. Det är lätt att skriva ner koefficienterna $A = (x_1y_2 - x_2y_1), B = y_1y_2(x_2 - x_1), C = x_1x_2(y_1 - y_2), D = 0$. (Ifall punkterna sammanfaller beöver vi också veta tangentriktningen i kurvan). Nu sätts parametriseringen av kurvan in i $2,2$ uttrycket ovan, och vi för samman x^4 och x^3 termer och ignorerar resten. Vi får i själva verket polynomet $\alpha x^4 - \beta x^3 + \dots$ där

$$\begin{aligned}
\alpha &= 2\sqrt{R^2-(d+1)^2}AB + 2d(B^2-A^2) - 2A^2 \\
\beta &= -(2\sqrt{R^2-(d+1)^2}(BC+B^2-A^2) + 4(d+1)A(B+C))
\end{aligned}$$

Vi löser nu ut x_3 för den residuella snittet ur ekvationen $(0)+x_1+x_2+x_3 = \beta/\alpha$ och via Möbiustransformationen ovan får vi ett uttryck för y_3. Nästa steg är att titta på kurvor av typ $Axy + B(x-y) = 0$ ty dessa är tangerade till kurvan vid O. Vi vill att den skall passera genom (x_3, y_3) vilket ger ett enkelt villkor på A, B (t.ex. $A = y_3 - x_3, B = x_3y_3$). Vi sätter in linjen igen och erhåller polynomet som ovan med skillnaden att $C = -B$. Den sökta x_4 ges ur $(2\times 0)+x_3+x_4 = \beta/\alpha$ och y_4 fås ur en Möbiustransformation. Detta ger ko-ordinaterna (x_4, y_4) för summan av punkterna. Att algebraiskt utföra dessa manipulationer vore ogörligt för hand, och det är inte helt säkert att resultatet i slutändan vore speciellt upplysande. Det är dock fullt möjligt att programmera enligt ovanstående. (Att substituera komplicerade symboliska uttryck i andra symboliska uttryck växer snabbt över huvudet, att göra motsvarande substitioner rent numeriskt är någonting helt annat.) Och vi kan även dra den allmänna slutsatsen att (x_4, y_4) kan skrivas såsom ett rationellt uttryck i $(x_1, y_1), (x_2, y_2)$.

Den reella bilden

Vi är framför allt intresserade av den reella situationen. De reella punkterna på den elliptiska kurvan utgör de för oss synliga, och dessa sönderfaller i två disjunkta slingor, varav en utgör en reell delgrupp (ifall vi gjort nollan reell). De motsvarar positivt orienterade tangentstumpar eller ekvivalent vänstertangenter, respektive negativt orienterade (eller högertangenter). Av en tillfällighet sitter de i en torus, nämligen den reella delen av $\mathbb{C}P^1 \times \mathbb{C}P^1$ vilken däremot inte har någon naturlig gruppstruktur. Notera att de två slingorna för sig kan inte skäras ut av polynom, endast dess union. Nedan finner vi illustrationer av dessa för olika värden på R, d. Kvadraten är helt enkelt den uppskurna torusen $\mathbb{R}P^1 \times \mathbb{R}P^1$ där den horisontella axeln ger rotationsvinkeln på C_O och den vertikala på C_I.



R = 2.5, d = 0.5   R = 4, d = 2.82843

Konklusionen är således att alla trianglar med fixa omskrivna och inskrivna radier R, r utgör en 1-dimensionell familj. Denna familj kan naturligt parametriseras av en cirkel med en icke-standard grupp-struktur modulo addition med en 3-torsions punkt som cykliskt permuterar trianglarnas hörn. En illustration av detta återfinnes på Normats omslag, där en punkt av ordning 49 och dess multiplar visas. Läsaren uppmanas tolka mönstret av tal ordnade runt den omskrivna cirkeln.

Not: Den invigde läsaren känner igen detta som ett specialfall av Poncelets teorem. Poncelet bevisade sin sats med rent syntetiska metoder, kopplingen till addition på elliptiska kurvor gjordes av Jacobi. En relativt elementär diskussion av problemet och dess generaliseringar kan återfinnas i nedanstående artiklar av P. Griffiths och J. Harris.

Referenser

[1] P. Griffiths, J. Harris, A Poncelet theorem in space. *Comm.Math.Helvetic* **52** (1977).

[2] P. Griffiths, J. Harris, On Cayley's explicit solution to Poncelet's porism. *Enseign.Math.* **24** (1978).