Grupe, krivulje i b(r)ojanja

Uvod

Grupa je uređen par $(G, *)$ nepraznog skupa G i binarne operacije $* : G \times G \to G$ koja je asocijativna, za koju postoji *neutralni element* e (takav da je $a * e = e * a = a$) te za svaki element a postoji *inverzni element* a^{-1} (takav da je $a * a^{-1} = a^{-1} * a = e$). Ako uz to vrijedi da je operacija komutativna ($a * b = b * a$), onda kažemo da je G *Abelova (komutativna)* grupa.

Npr. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Q}\backslash\{0\}, \cdot)$, $(\mathbb{F}_p, +)$ i $(\mathbb{F}_p\backslash\{0\}, \cdot)$ su komutativne grupe ($\mathbb{F}_p$ je skup ostataka modulo prost broj p). S druge strane, $(\mathbb{N}, +)$ nije grupa jer ne postoji neutralni element, a $(\mathbb{N}_0, +)$ nije grupa jer ne postoje inverzni elementi.

Podgrupa grupe $(G, *)$ je podskup $(H, *) \leq (G, *)$ zatvoren na $*$ koji je i sam grupa. Npr. $2\mathbb{Z}$ je aditivna podgrupa cijelih bojeva, a $\{2, 4, 1\}$ je multiplikativna podgrupa od $\mathbb{F}_7\backslash\{0\}$. Obje ove pogrupe generirane su jednim elementom (2) koji zovemo *generatorom*, a dobivenu podgrupu *cikličkom*. *Red* elementa je veličina cikličke podgrupe generirane tim elementom (npr. red od 2 u multiplikativnoj $\mathbb{F}_7\backslash\{0\}$ je tri). Podgrupe možemo generirati i s više elemenata, ali ako ih je konačno, kažemo da je podgrupa *konačno generirana*.

Prsten

Prsten je uređena trojka $(R, +, \times)$ nepraznog skupa R i dvije binarne operacije $+, \times$ (*zbrajanje i množenje*) takve da je $(R, +)$ Abelova grupa, da je $\times$ asocijativno, te vrijede *pravila distribucije*

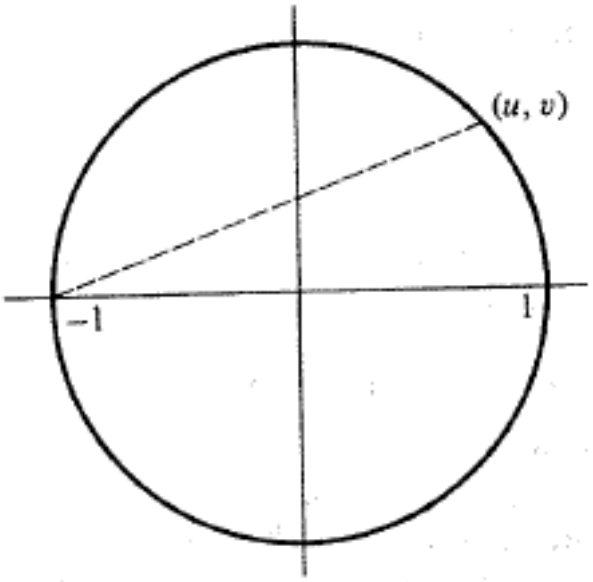
$$(a + b) \times c = a \times c + b \times c, \quad \text{i} \quad a \times (b + c) = (a \times b) + (a \times c).$$

Svi naši prsteni bit će komutativni ($\times$) s jedinicom $1 \in R$ (tako da je $1 \times a = a \times 1 = a$). Npr. $\mathbb{Z}$ je prsten s uobičajenim zbrajanjem i množenjem. Za prost p, ostaci pri dijeljenju s p, $\mathbb{F}_p$, čine komutativan prsten s jedinicom.

Prsten cijelih brojeva može se proširiti na brojne načine a da zadrži mnoga bitna svojstva, poput jedinstvene faktorizacije. Računanjem u prstenu $\mathbb{Z}[\sqrt{3}]$, može se pokazati da jednadžba $x^3 + 48 = y^4$ nema cjelobrojnih rješenja .

Krivulje

Promotrimo jediničnu kružnicu $x^2 + y^2 = 1$ i odredimo sve racionalne točke na njoj. Uzmimo jednu racionalnu točku koju napamet znamo, npr. $(-1, 0)$. Ako imamo neku drugu racionalnu točku (u, v), znamo da pravac kroz te dvije točke ima jednadžbu $y - 0 = \dfrac{v}{u+1}(x+1)$. Dakle, taj pravac ima **racionalni koeficijent smjera** (nagib).



To nam sugerira da sve racionalne točke na kružnici možemo naći na sljedeći način: odaberimo racionalan broj t, odnosno cijeli broj m i prirodan n, provucimo pravac kroz $(-1, 0)$ s nagibom $t = m/n$ i označimo s (u, v) drugu točku presjeka tog pravca s jediničnom kružnicom. Nije teško izračunati da je

$$u = \frac{1-t^2}{1+t^2} = \frac{m^2-n^2}{m^2+n^2}, \quad v = \frac{2t}{1+t^2} = \frac{2mn}{m^2+n^2}.$$

Za $m > n$, brojevi $X = m^2 - n^2$, $Y = 2mn$ i $Z = m^2 + n^2$ su stranice pravokutnog trokuta ($X^2 + Y^2 = Z^2$ slijedi zbog $u^2 + v^2 = 1$). Puštanjem m i n kroz sve prirodne brojeve takve da je $m > n$, dobivamo sve moguće Pitagorine trojke!

Na sličan način moguće ja odrediti sve racionalne točke na bilo kojoj konici.

Riješimo sljedeći

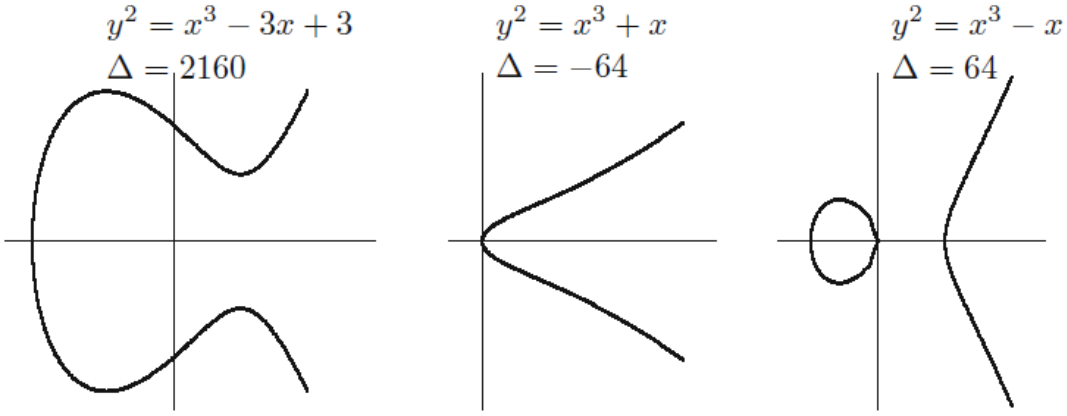
Zadatak 1. Postoji li kružnica i beskonačan skup točaka na njoj takav da je udaljenost svakih dviju od njih racionalna?

(Mediteransko matematičko natjecanje 1999.)

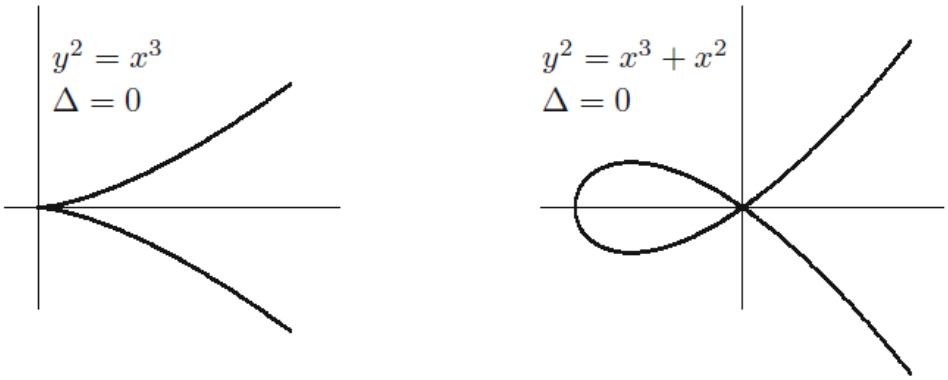
Eliptičke krivulje

Za potrebe ovog predavanja, *eliptička krivulja* je glatka krivulja dana jednadžbom $E : y^2z = x^3+axz^2+bz^3$. Češće radimo s verzijom krivulje bez z, $y^2 = x^3+ax+b$. Ako (x, y) zadovoljava drugu jednadžbu, onda $(x, y, 1)$ zadovoljava prvu, a ako (x, y, z) zadovoljava prvu, onda $(x/z, y/z)$ zadovoljava drugu jednadžbu. Razlika između te dvije jednadžbe je zapravo samo u jednoj točki, kada je $z = 0$, dobivamo točke $(0, y, 0)$ (koje se razlikuju za faktor y od točke $(0, 1, 0)$).

Glatkoća se može opisati algebarskim uvjetom, da je $\Delta = -16(4a^3 + 27b^2) \neq 0$, ali u osnovi znači da se u svakoj točki krivulje može povući točno jedna tangenta. Npr. krivulja dana jednadžbom $y^2 = x^3$ nije eliptička, kao ni krivulja $y^2 = x^3+x^2$.



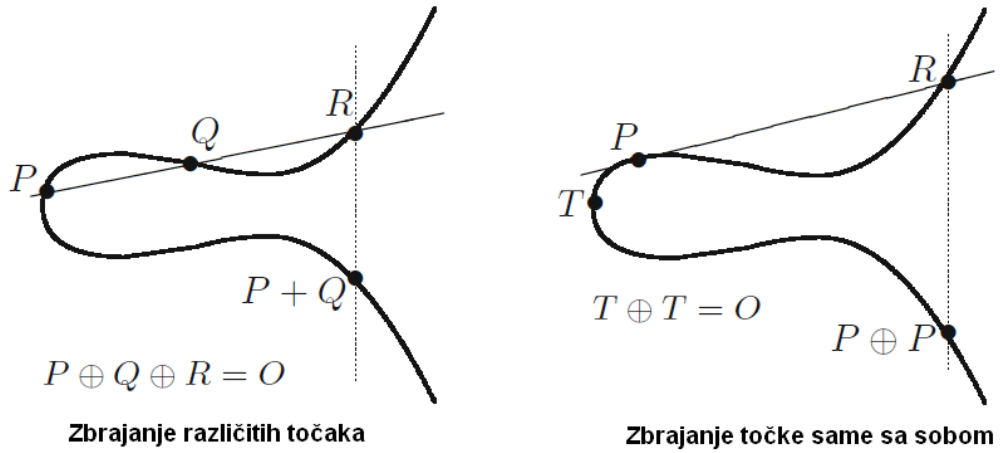
Tri eliptičke krivulje



Dvije kubične krivulje koje nisu glatke (pa ni eliptičke)

Ako uzmemo dvije točke na eliptičkoj krivulji, P i Q, te povučemo pravac kroz njih, vidimo da ćemo dobiti još jednu točku presjeka pravca s krivuljom (sječemo jednadžbu trećeg s jednadžbom prvog stupnja pa očekujemo tri rješenja). To nam omogućava da "zbrojimo" dvije različite točke na eliptičkoj krivulji. No, kako zbrojiti točku samu sa sobom? Ako povučemo tangentu na krivulju u toj točki, moguće je da to bude jedina točka presjeka tangente i krivulje (npr. ako povučemo tangentu na krivulju u točki na x-osi). Nadalje, što bi nam mogao biti neutralni element za takvu operaciju? Pa, prisjetimo se one jedne točke "viška"

koju dobivamo s jednadžbom $y^2z = x^3+axz^2+bz^3$, točke $(0,1,0)$ koju zamišljamo kao točku u beskonačnosti. Ona će nam biti neutralni element O.



Zbrajanje različitih točaka

Zbrajanje točke same sa sobom

Zbrajanje na eliptičkoj krivulji

Na eliptičkoj krivulji točke P, Q i R su kolinearne ako i samo ako je $P+Q+R = O$.

Jedan od najpoznatijih teorema (Mordell-Weilov) kaže da je sve racionalne točke na eliptičkoj krivulji moguće dobiti ovom operacijom zbrajanja počevši od konačno mnogo točaka, *generatora*, u konačno (ali proizvoljno) mnogo koraka.

Zadaci

2. Za prirodan $n > 1$, neka je P_n produkt svih prirodnih $x < n$ takvih da $n|x^2 - 1$. Za svaki $n > 1$, odredi ostatak koji P_n daje pri dijeljenju s n. (IMO Shortlist 2004)

3. Dokaži da postoji beskonačan skup točaka $\ldots, P_{-3}, P_{-2}, P_{-1}, P_0, P_1, P_2, P_3, \ldots$ u ravnini sa sljedećim svojstvom: Za tri različita cijela broja a, b i c, točke P_a, P_b i P_c su kolinearne ako i samo ako je $a+b+c = 2014$. (USAMO 2014.)

4. Za prirodan $n > 1$ neka je $V_n = \{1 + kn : k \in \mathbb{N}\}$. Broj $m \in V_n$ je *nerastavljiv u* V_n ako ne postoje $p, q \in V_n$ takvi da je $pq = m$. Dokaži da u V_n postoji elementi koji se može prikazati kao produkt nerastavljivih u V_n na više od jednog načina (permutirane načine smatramo istima).

5. Odredite postoje li dva beskonačna skupa točaka $A_1, A_2, \ldots$ i $B_1, B_2, \ldots$ u ravnini, takva da za sve i, j, k $(1 \leq i < j < k)$, vrijedi

   (a) B_k je na pravcu koji prolazi kroz A_i i A_j ako i samo ako je $k = i + j$.

   (b) A_k je na pravcu koji prolazi kroz B_i and B_j ako i samo ako je $k = i+j$.

   (Mediteransko matematičko natjecanje 2008.)

DZ Neka je A skup od N ostataka modulo N^2. Dokaži da postoji skup B od N ostataka modulo N^2 takav da $A + B = \{a + b : a \in A, b \in B\}$ sadrži bar pola svih ostataka modulo N^2.

Djelovanje grupa

Kažemo da grupa G *djeluje* na skup S ako je dano preslikavanje s $G \times A$ u A (koje zapisujemo kao $g \cdot a, \forall g \in G, \forall a \in A$) sa sljedećim svojstvima:

(1) $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$, $\forall g_1, g_2 \in G, \forall a \in A$

(2) $1 \cdot a = a$, $\forall a \in A$

Djelovanje grupa definira relaciju ekvivalencije na skupu A, a klasu $\{g \cdot a : g \in G\}$ zovemo *orbitom* koja sadrži a.

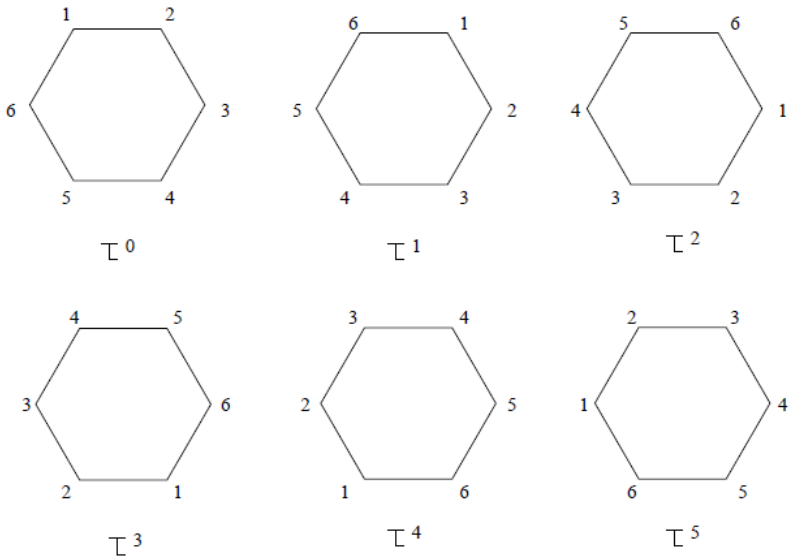
Apstraktna algebra u kombinatorici – Burnsideova lema

Burnside: Neka konačna grupa G djeluje na skup S, te označimo s N broj orbita tog djelovanja. Za pojedini element $g \in G$ označimo sa $S_g = \{x \in S : gx = x\}$, podskup od S koji g fiksira. Tada je

$$N = \frac{1}{|G|} \sum_{g \in G} |S_g|.$$

Nađimo broj bojanja vrhova pravilnog šesterokuta u dvije boje, pri čemu bojanja koja se mogu dobiti rotacijom smatramo istima. Označimo s τ rotaciju za $60°$. Tada ciklička grupa od šest elemenata generirana s τ, djeluje na skup bojanja.

Elementi grupe mogu se zapisati kao permutacije: $\tau = (1,2,3,4,5,6), \tau^2 = (1,3,5)(2,4,6), \tau^3 = (1,4)(2,5)(3,6), \tau^4 = (1,5,3)(2,6,4), \tau^5 = (1,6,5,4,3,2)$, dok je $\tau^6 = e$, identiteta.



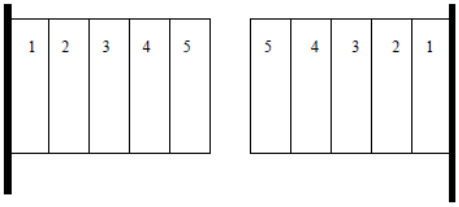
Rotacije pravilnog šesterokuta s vrhovima 1, 2, 3, 4, 5, 6

Tada je broj traženih bojanja $N = \frac{1}{6}\left(2^6 + 2^1 + 2^2 + 2^3 + 2^2 + 2^1\right) = \frac{84}{6} = 14$.

Zadaci

Rješenja svih zadataka ovdje mogu se naći u [Walcott 2004].

7. Koliko zastava s 5 vertikalnih pruga jednake širine postoji, ako se svaka pruga može obojati jednom od q boja? Pri tome zastave smatramo istima ako se takvima mogu činiti zbog rotacije na jarbolu za zastavu.



Preokretanje zastave s pet pruga oko jarbola

8. Koristeći Burnsideovu lemu, odredi broj bojanja vrhova kvadrata u 3 boje pri čemu istima smatramo bojanja koja se mogu dobiti rotacijama i refleksijama.

DZ Dokaži da je broj bojanja $n \times n$ ploče u dvije boje, pri čemu rotirana bojanja smatramo istima, jednak

$$\frac{1}{2}\left(2^{n^2} + 2^{\lfloor \frac{n^2+1}{2} \rfloor} + 2 \cdot 2^{\lfloor \frac{n^2+3}{4} \rfloor}\right).$$

DZ Pokušajte dokazati Cauchyjev teorem: Neka je G konačna grupa. Ako prost broj p dijeli $|G|$, tada u G postoji element reda p. *Ako vam ne ide, pokušajte uz dodatnu pretpostavku da je grupa komutativna.*

Lagrangeov teorem: Ako je H podgrupa konačne grupe G, onda $|H|$ dijeli $|G|$.

Cauchyjev teorem: Ako prost broj p dijeli red konačne grupe G, onda u G postoji element reda p.

Literatura

- D. S. Dummit and R. M. Foote (2004) *Abstract Algebra*. 3rd edition, John Wiley & Sons, Inc.
- J. H. Silverman, J. Tate (2015) *Rational Points on Elliptic Curves*. 2nd edition, Springer-Verlag – Undergraduate Texts in Mathematics
- N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*. 2nd edition, Springer-Verlag – Graduate Texts in Mathematics
- J. H. Silverman (2009), *The Arithmetic of Elliptic Curves*, 2nd edition, Springer-Verlag – Graduate Texts in Mathematics
- K. Walcott (2004), *Application and Analysis of Burnside's Theorem*, A Senior Comprehensive Project, Meadville, PA