Matematicko-fyzikálny časopis

Václav Medek

O jednej interpretácii afinnej roviny nad telesom tried zvyškov modulo p

Matematicko-fyzikálny časopis, Vol. 16 (1966), No. 1, 41--44

Persistent URL: `http://dml.cz/dmlcz/126711`

Terms of use:

© Mathematical Institute of the Slovak Academy of Sciences, 1966

Institute of Mathematics of the Academy of Sciences of the Czech Republic provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.

This paper has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* `http://project.dml.cz`

MATEMATICKO-FYZIKÁLNY ČASOPIS SAV, 16, 1, 1966

O JEDNEJ INTERPRETÁCII AFINNEJ ROVINY NAD TELESOM TRIED ZVYŠKOV MODULO p

VÁCLAV MEDEK, Bratislava

Budeme uvažovať o konečnej desarguesovskej afinnej rovine zostrojenej nad telesom zvyškov mod p, kde p je prvočíslo.

Pripomeňme, že afinná rovina je množina bodov s množinou význačných podmnožín (priamok), pričom sa požaduje splnenie týchto axióm:

1. Každými dvoma rôznymi bodmi prechádza práve jedna priamka.
2. Existujú tri body neležiace na jednej priamke.
3. Každým bodom A neležiacim na priamke a prechádza aspoň jedna priamka b, ktorá nemá s priamkou a žiaden spoločný bod.
4. Každým bodom A prechádza najviac jedna priamka, ktorá nemá s priamkou a žiaden spoločný bod.

1. Jednoduchú interpretáciu afinnej roviny nad telesom zvyškov mod p (p prvočíslo) nájdeme pomocou rotačnej valcovej plochy Φ, ktorú rozrežeme rôznymi rovinami ${}^i\alpha$ ($i = 0, \ldots, p-1$) kolmými na os o plochy Φ v kružniciach ${}^ik$, pričom nech susedné roviny ${}^{i-1}\alpha$, ${}^i\alpha$ ($i = 1, \ldots, p-1$) majú od seba rovnaké vzdialenosti. Vpíšme teraz do kružnice ${}^0k$ pravidelný p-uholník ${}^00, \ldots, {}^0(p-1)$ a každým vrcholom tohto p-uholníka zostrojme tvoriacu priamku plochy Φ. Tieto tvoriace priamky pretínajú kružnice ${}^ik$ v bodoch ${}^ij$ ($i, j = 0, \ldots, p-1$). Tým dostávame p^2 bodov ${}^ij$, kde index i reprezentuje kružnicu ${}^ik$ a číslo j tvoriacu priamku prechádzajúcu bodom ${}^0j$; priesečníkom kružnice ${}^ik$ s priamkou ${}^0j$ je potom bod ${}^ij$.

Množina bodov ${}^ij$ tvorí afinnú rovinu, ak priamkami budú tieto jej podmnožiny:

a) Podmnožiny všetkých bodov ${}^ij$ vždy s pevným indexom i (tieto body ležia na kružnici ${}^ik$).

b) Podmnožiny všetkých bodov ${}^ij$ vždy s pevným číslom j (tieto body ležia na jednej tvoriacej priamke).

c) Podmnožiny všetkých bodov ${}^ij$ ležiacich vždy na kladne orientovanej skrutkovici plochy Φ takej, že pretína každú kružnicu ${}^ik$ v niektorom bode ${}^ij$.

Preveríme platnosť axióm 1.—4. pre takúto afinnú rovinu.

1. Axióma je zrejme správna pre každé dva rôzne body ${}^ij$ s rovnakým indexom i, resp. s rovnakým číslom j. Tieto dva prípady teda v ďalšom vylúčime.

Zostrojme teraz všetky priamky typu c) prechádzajúce bodom ^{00}. Budú to podmnožiny bodov ${}^ij$ ležiacich na skrutkoviciach kladnej orientácie prechádzajúcich bodmi ${}^1j$ ($j = 1, \ldots, p - 1$). Z vlastností skrutkovíc ihneď vyplýva, že každá z takto zostrojených skrutkovíc pretína každú kružnicu ${}^ik$ v niektorom bode ${}^ij$. Treba ukázať, že pre dva ľubovoľné body ${}^ij$, ${}^{i'}j'$ takejto podmnožiny platí $i \neq i'$, $j \neq j'$. Správnosť $i \neq i'$ vyplýva z toho, že žiadna skrutkovica nemôže prechádzať dvoma bodmi tej istej kružnice ${}^ik$. Aby sme ukázali, že platí aj $j \neq j'$, uvažujme o skrutkovici prechádzajúcej bodmi ^{00} a ${}^1j$ ($j \neq 0$). Táto skrutkovica pretína kružnicu ${}^ik$ v bode ${}^i(ij)$ ($i = 0, \ldots, p - 1$). Predpokladajme, že pre $i \neq i'$ platí $ij = i'j$. Z rovnice $ij = i'j$ vyplýva $i = i'$ (pretože $j \neq 0$), čo však je spor. Tým sme ukázali, že skrutkovica prechádzajúca bodmi ^{00}, ${}^1j$ neobsahuje žiadne dva body ležiace na tej istej tvoriacej priamke plochy Φ. Ukážeme ešte, že pre $j \neq j'$ ($j \neq 0$, $j' \neq 0$) skrutkovice prechádzajúce bodmi ^{00}, ${}^1j$ a ^{00}, ${}^1j'$ nemajú okrem bodu ^{00} žiaden iný spoločný bod afinnej roviny. Skutočne, taký bod by mohol ležať iba na niektorej z kružníc ${}^ik$ ($i = 2, \ldots, p - 1$) a muselo by o ňom platiť $ij = ij'$. Z rovnice $ij = ij'$ vyplýva $j = j'$ (pretože $i \neq 0$), čo je spor. Bodmi ^{00} a ${}^ij$ ($i \neq 0, j \neq 0$) prechádza teda jediná priamka typu c).

Všetky priamky typu c) dostaneme z priamok typu c) prechádzajúcich bodom ^{00} otočením plochy Φ okolo jej osi o o niektorý z uhlov $2k\pi/p$ ($k = 1, \ldots, p - 1$).

Majme teraz dva rôzne body ${}^ij$, ${}^{i'}j'$, kde $i \neq i'$, $j \neq j'$. Nech $i < i'$ a $j < j'$; body ^{00}, ${}^{(i'-i)}(j' - j)$ majú tú istú vzájomnú polohu, pokiaľ ide o konštrukciu priamok typu c), ako body ${}^ij$, ${}^{i'}j'$. Pretože ale bodmi ^{00}, ${}^{(i'-i)}(j' - j)$ prechádza práve jedna priamka typu c), prechádza práve jedna priamka typu c) aj bodmi ${}^ij$, ${}^{i'}j'$. Dôkaz tohto tvrdenia by prebiehal tak isto aj pre $i < i'$, $j > j'$; $i > i'$, $j < j'$; $i > i'$, $j > j'$.

2. Tri body, ktoré neležia na jednej priamke sú napr. ^{00}, ^{01}, ^{11}.

3. Správnosť tejto axiómy je zrejmá pre priamky typu a) a b). Nech teda priamka a je typu c) a nech bod $A = {}^ij$ na nej neleží. Skrutkovica ${}^as$ reprezentujúca priamku a pretína kružnicu ${}^ik$ v bode ${}^ij'$, kde $j \neq j'$. Ak otočíme plochu Φ okolo osi o tak, aby bod ${}^ij'$ sa otočil do bodu ${}^ij$, otočí sa skrutkovica ${}^as$ do skrutkovice ${}^{a'}s$, ktorá reprezentuje hľadanú priamku a' bodom A.

4. Správnosť tejto axiómy je zrejmá pre priamky typu a) a b).

Uvažujme najprv o takýchto dvoch priamkach typu c): Priamka a nech je reprezentovaná skrutkovicou bodmi ^{00}, ${}^1j$ (tvoria ju body ${}^i(ij)$) a priamka b nech je reprezentovaná skrutkovicou bodmi ${}^0m$, ${}^1j'$ (tvoria ju body ${}^i[i(j' - m) + m]$). Pýtajme sa, za akých podmienok sa priamky a, b pretnú. To nastane vtedy, ak existuje také i, že $ij = i(j' - m) + m$, čiže $i(j' - j - m) =$

$-m$. Ak $m = 0$, potom rovnica $i(j' - j) = 0$ má alebo jediné riešenie $i = 0$ pre $j' \neq j$, alebo jej vyhovuje každé i pre $j' = j$. Z toho vyplýva známy fakt, že dve skrutkovice prechádzajúce bodom ${}^{0}0$ alebo splývajú, alebo majú jediný spoločný bod ${}^{0}0$. Ak $m \neq 0$, má rovnica $i(j' - j - m) = -m$ riešenie len v tom prípade, ak $j' - j - m \neq 0$ a to jediné: $i = -m(j' - j - m)^{-1}$; ak $j' = j + m$, rovnica nemá riešenie. Z toho vyplýva, že bodom ${}^{0}m$ prechádza jediná priamka a', ktorá nemá s priamkou a žiaden spoločný bod. Pritom skrutkovice reprezentujúce priamky a, a' vzniknú jedna z druhej otočením o uhol $2m\pi/p$ okolo osi o. V každom inom prípade majú obidve priamky spoločný jediný bod ${}^{-m(j'-j-m)^{-1}}[-mj(j' - j - m)^{-1}]$.

Predpokladajme teraz, že bodom A prechádzajú dve priamky b, c, ktoré nemajú žiaden spoločný bod s priamkou a. Otočme plochu Φ okolo osi o tak, aby priamka a sa otočila do priamky a' prechádzajúcej bodom ${}^{0}0$; bod A nech sa pritom otočí do bodu A'. Nech teda existujú dve priamky b', c' bodom A', ktoré nemajú s priamkou a' žiaden spoločný bod. Potom ale skrutkovice reprezentujúce priamky b', c' musia vzniknúť zo skrutkovice reprezentujúcej priamku a' otočením okolo osi o. Takéto dve skrutkovice môžu mať ovšem spoločný bod afinnej roviny len vtedy, ak splynú, čiže musia splynúť aj priamky b', c' a teda aj priamky b, c.

2. Túto interpretáciu možno dostať aj iným spôsobom: V každej desarguesovskej konečnej afinnej rovine je možné zaviesť súradnice ako usporiadané dvojice prvkov z príslušného telesa. Potom priamky sú podmnožiny obsahujúce všetky body, ktoré spĺňajú rovnicu $ax + by + c = 0$, kde aspoň jedno z čísel a, b je rôzne od nuly. Nech $\mathfrak{Q}$ je množina všetkých bodov reálnej euklidovskej roviny s celočíselnými súradnicami. Model afinnej roviny nad telesom tried zvyškov mod p, kde p je prvočíslo, zostrojíme takto: Na množine $\mathfrak{Q}$ zavedieme reláciu ekvivalencie ε podľa predpisu $(x_1, y_1) \equiv (x_2, y_2) \Leftrightarrow x_1 \equiv x_2 \pmod{p}$, $y_1 \equiv y_2 \pmod{p}$. Nech $\mathfrak{P}$ je množina všetkých bodov s celočíselnými súradnicami na tých priamkach reálnej euklidovskej roviny, ktoré alebo spájajú dva body s tou istou y-ovou súradnicou, alebo dva body s y-ovými súradnicami líšiacimi sa o jednotku. Potom triedy ekvivalencie $\mathfrak{Q}/\varepsilon$, $\mathfrak{P}/\varepsilon$ možno interpretovať ako body a priamky afinnej roviny izomorfnej s afinnou rovinou nad telesom tried zvyškov modulo p. Ak teraz navinieme reálnu euklidovskú rovnicu na rotačnú valcovú plochu vhodného polomeru, dostaneme interpretáciu popísanú v **1**.

Došlo 19. 1. 1965.

*Katedra matematiky a deskriptívnej geometrie
Stavebnej fakulty
Slovenskej vysokej školy technickej,
Bratislava*

ON AN INTERPRETATION OF THE FINITE AFFINE PLANE OVER THE FIELD OF RESIDUE CLASSES MODULO p

Václav Medek

Summary

The model of the finite affine plane is a set of points on a cylindrical surface of revolution; the lines are subsets on the geodesics of this surface.