Časopis pro pěstování matematiky, roč. 106 (1981), Praha

O MODELECH KONEČNÝCH AFINNÍCH ROVIN

JAROMÍR KRYS, Hradec Králové
(Došlo dne 25. září 1978)

V tomto článku sestrojíme model afinních rovin řádu p, kde p je prvočíslo a dále jeden zajímavý model roviny řádu 4. Mějme množinu prvních p přirozených čísel, kde p je prvočíslo. Vzhledem k násobení definovaným následující tabulkou:

(1)

	1	2	3	...	p
1	1	2	3	...	p
2	2	3	4	...	1
3	3	4	5	...	2
...	...	...	...	...	...
p	p	1	2	...	$p-1$

tvoří tato množina cyklickou grupu. Definujme na množině $G = \{1, 2, \ldots, p, p + 1, \ldots, p^2\}$ operaci tabulkou:

(2)

	$1, \ldots, p$	$p+1, \ldots, 2p$	$2p+1, \ldots, 3p$	...	$(p-1)p+1, \ldots, p^2$
$1, \ldots, p$	$\bar{1}$	$\bar{2}$	$\bar{3}$	...	$\bar{p}$
$p+1, \ldots, 2p$	$\bar{2}$	$\bar{3}$	$\bar{4}$	...	$\bar{1}$
$2p+1, \ldots, 3p$	$\bar{3}$	$\bar{4}$	$\bar{5}$	...	$\bar{2}$
$\vdots$	...	...	...	...	...
$p(p-1)+1, \ldots, p^2$	$\bar{p}$	$\bar{1}$	$\bar{2}$	...	$\overline{p-1}$

kde:

$$\bar{1} = \begin{array}{ccccc} 1 & 2 & 3 & \dots & p \\ 2 & 3 & 4 & \dots & 1 \\ 3 & 4 & 5 & \dots & 2 \\ \dots & \dots & \dots & \dots & \dots \\ p & 1 & 2 & \dots & p-1 \end{array}, \quad \bar{2} = \begin{array}{cccc} p+1 & p+2 & \dots & 2p \\ p+2 & p+3 & \dots & p+1 \\ p+3 & p+4 & \dots & p+2 \\ \dots & \dots & \dots & \dots \\ 2p & p+1 & \dots & 2p-1 \end{array}$$

$$\dots, \quad \bar{p} = \begin{array}{cccc} (p-1)p+1 & (p-1)p+2 & \dots & p^2 \\ (p-1)p+2 & (p-1)p+3 & \dots & (p-1)p+1 \\ (p-1)p+3 & (p-1)p+4 & \dots & (p-1)p+2 \\ \dots & \dots & \dots & \dots \\ p^2 & (p-1)p+1 & \dots & p^2-1 \end{array}$$

Věta 1. *Množina G je vzhledem k uvažované operaci dané tabulkou* (2) *komutativní grupa řádu* p^2 *a má* $p + 1$ *podgrup řádu* p.

Důkaz. Jak vypadá násobení v G, sledujme na příkladě: $(2p + 2)(p + 4)$. První číslo patří do čísel tabulky $\bar{3}$ a druhé do tabulky $\bar{2}$. V tabulce (1) násobíme 3 a 2, dostáváme 4 a tedy výsledek našeho násobení patří do čísel tabulky $\bar{4}$. Které číslo tabulky $\bar{4}$ to bude, poznáme opět z tabulky (1), kde násobíme 2 a 4, což je 5. Platí tedy: $(2p + 2)(p + 4) = 3p + 5$. Množina G je grupou, neboť všechny její prvky jsou tvaru $\alpha p + \beta$, kde α, β určujeme podle tabulky (1). Dále, grupa G je komutativní, protože tabulka (2) je symetrická. Z předcházejícího také plyne, že každý prvek grupy $G(\neq 1)$ je generátorem cyklické podgrupy řádu p: Kupříkladu $p + 2, 2p + 3, \dots$ $\dots$ (mod $p^2 + 1$). Prvků této podgrupy různých od jednotky je $p - 1$ a tedy $(p^2 - 1)/(p - 1) = p + 1$ je počet podgrup řádu p. Označme získané podgrupy G_i, kde $i = 1, \dots, p + 1$.

Definice 1. *Přímkou* množiny G nazveme každou třídu faktorové grupy G/G_i, kde $i = 1, \dots, p + 1$.

Definice 2. *Afinní rovinou* rozumíme každou neprázdnou množinu bodů, v níž jsou takovým způsobem vyznačeny určité podmnožiny zvané přímky, že pro tyto body a přímky jsou splněny požadavky:

1) Každé dva různé body určují právě jednu přímku, přičemž oba tyto body jsou prvky této přímky.
2) Každým bodem, který není prvkem dané přímky prochází právě jedna přímka, která nemá s danou přímkou žádný společný bod.
3) Existují alespoň tři body, které nejsou prvky jediné přímky.

Poznámka 1. Každá přímka konečné afinní roviny obsahuje vždy týž počet bodů dané roviny. Toto číslo nazýváme řádem dané roviny. Dále zavádíme incidenci a rovnost na množině, množinovou inkluzí a rovností.

Věta 2. *Množina G spolu s přímkami definovanými v definici* 1 *je konečná afinní rovina řádu p.*

Důkaz. 1) Dva různé prvky grupy G náleží jediné třídě faktorové grupy G/G_i pro jediné i, neboť je známo, že platí: Dvě různé třídy téže faktorové grupy nemají žádný společný prvek a (v našem případě) dvě různé třídy dvou různých faktorových grup mají právě jeden společný prvek. Dále platí, že každým bodem je určena jediná třída každé G/G_i.

2) Z předchozího plyne i tato druhá podmínka.

3) Jestliže je $p > 1$, potom zřejmě prvků dané třídy je méně než počet prvků grupy G a tedy existuje aspoň jeden prvek, který nepatří dané třídě.

Poznámka 2. Za grupu G můžeme pokládat:

1) Podgrupy grupy bodů rovinné kubiky rodu 1. Zvolíme-li $p = 3$ jedná se o známý model afinní roviny řádu tři, jež tvoří inflexní body této kubiky.

2) Grupy všech uspořádaných dvojic komplexních jednotek pro dané p (viz závěr [2]).

3) Grupy uspořádaných dvojic vrcholů pravidelných p-úhelníků (plyne z geometrického významu předchozího).

Na množině $M = \{1, 2, \ldots, 16\}$ definujme operaci tabulkou:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	2	1	4	3	6	5	8	7	10	9	12	11	14	13	16	15
3	3	4	1	2	7	8	5	6	11	12	9	10	15	16	13	14
4	4	3	2	1	8	7	6	5	12	11	10	9	16	15	14	13
5	5	6	7	8	1	2	3	4	13	14	15	16	9	10	11	12
6	6	5	8	7	2	1	4	3	14	13	16	15	10	9	12	11
7	7	8	5	6	3	4	1	2	15	16	13	14	11	12	9	10
8	8	7	6	5	4	3	2	1	16	15	14	13	12	11	10	9
9	9	10	11	12	13	14	15	16	1	2	3	4	5	6	7	8
10	10	9	12	11	14	13	16	15	2	1	4	3	6	5	8	7
11	11	12	9	10	15	16	13	14	3	4	1	2	7	8	5	6
12	12	11	10	9	16	15	14	13	4	3	2	1	8	7	6	5
13	13	14	15	16	9	10	11	12	5	6	7	8	1	2	3	4
14	14	13	16	15	10	9	12	11	6	5	8	7	2	1	4	3
15	15	16	13	14	11	12	9	10	7	8	5	6	3	4	1	2
16	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

Množina M spolu s příslušnou operací je grupou (ověření přenecháme čtenáři, právě tak jako i další výsledky). Uvažujme její podgrupy: $G_1 = \{1, 2, 5, 6\}$, $G_2 = \{1, 3, 9, 11\}$, $G_3 = \{1, 4, 13, 16\}$, $G_4 = \{1, 7, 12, 14\}$ a $G_5 = \{1, 8, 10, 15\}$.

Nyní sestrojíme všechny třídy faktorových grup M/G_i, $i = 1, 2, 3, 4, 5$. Dostáváme:

$$\begin{aligned}
p_1 &= \{1, 2, 5, 6\}, & q_1 &= \{1, 3, 9, 11\}, & r_1 &= \{1, 4, 13, 16\}, \\
p_2 &= \{3, 4, 7, 8\}, & q_2 &= \{2, 4, 10, 12\}, & r_2 &= \{2, 3, 14, 15\}, \\
p_3 &= \{9, 10, 13, 14\}, & q_3 &= \{5, 7, 13, 15\}, & r_3 &= \{5, 8, 9, 12\}, \\
p_4 &= \{11, 12, 15, 16\}, & q_4 &= \{6, 8, 14, 16\}, & r_4 &= \{6, 7, 10, 11\},
\end{aligned}$$

$$\begin{aligned}
s_1 &= \{1, 7, 12, 14\}, & t_1 &= \{1, 8, 10, 15\}, \\
s_2 &= \{2, 8, 11, 13\}, & t_2 &= \{2, 7, 9, 16\}, \\
s_3 &= \{3, 5, 10, 16\}, & t_3 &= \{3, 6, 12, 13\}, \\
s_4 &= \{4, 6, 9, 15\}, & t_4 &= \{4, 5, 11, 14\}.
\end{aligned}$$

Z předchozího a při sledování postupu důkazu věty 2, plyne:

Věta 3. *Množina M spolu s přímkami p_i, q_i, r_i, s_i, t_i pro $i = 1, 2, 3, 4$ tvoří model afinní roviny řádu 4.*

Poznámka 3. Uvažovaná grupa není izomorfní s grupou příslušných bodů kubiky tj.: Inflexní bod J, body J_i jejichž tečnovým bodem je bod J a body J_{ij}, $i = 1, 2, 3$, $j = 1, 2, 3, 4$, přičemž tečnový bod bodu J_{ij} je bod J_i.

Afinní rovinu řádu 4 můžeme pomocí těchto bodů rovinné kubiky, která má aspoň 3 inflexní body, konstruovat také a to takto:

1) Jejími body rozumíme shora vyznačené body kubiky.

2) Čtyři přímky volíme: $\{J, J_1, J_2, J_3\}$, $\{J_{11}, J_{12}, J_{13}, J_{14}\}$, $\{J_{21}, J_{22}, J_{23}, J_{24}\}$, $\{J_{31}, J_{32}, J_{33}, J_{34}\}$. Zbývajících 16 přímek dostaneme takto. Z polohy uvažovaných bodů na kubice víme, že existuje 16 přímek dané roviny na kterých leží právě jeden bod J_{1j}, jediný bod J_{2j} a jediný bod J_{3j}. Těchto 16 přímek uvažujeme jako přímky našeho hledaného modelu konečné afinní roviny tak, že ke každé trojici bodů přiřadíme právě jeden z bodů J, J_1, J_2, J_3. Konkrétní přiřazení snadno najdeme užitím grupových vlastností. Tabulka uvažované grupy je:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	2	3	4	1	6	7	8	5	10	11	12	9	14	15	16	13
3	3	4	1	2	7	8	5	6	11	12	9	10	15	16	13	14
4	4	1	2	3	8	5	6	7	12	9	10	11	16	13	14	15
5	5	6	7	8	9	10	11	12	13	14	15	16	1	2	3	4
6	6	7	8	5	10	11	12	9	14	15	16	13	2	3	4	1
7	7	8	5	6	11	12	9	10	15	16	13	14	3	4	1	2
8	8	5	6	7	12	9	10	11	16	13	14	15	4	1	2	3
9	9	10	11	12	13	14	15	16	1	2	3	4	5	6	7	8
10	10	11	12	9	14	15	16	13	2	3	4	1	6	7	8	5
11	11	12	9	10	15	16	13	14	3	4	1	2	7	8	5	6
12	12	9	10	11	16	13	14	15	4	1	2	3	8	5	6	7
13	13	14	15	16	1	2	3	4	5	6	7	8	9	10	11	12
14	14	15	16	13	2	3	4	1	6	7	8	5	10	11	12	9
15	15	16	13	14	3	4	1	2	7	8	5	6	11	12	9	10
16	16	13	14	15	4	1	2	3	8	5	6	7	12	9	10	11

přičemž např.: $1 = J$, $3 = J_1$, $9 = J_2$, $11 = J_3$, $2 = J_{11}$, $4 = J_{12}$, $10 = J_{13}$, $12 = J_{14}$, $7 = J_{21}$, $5 = J_{22}$, $13 = J_{23}$, $15 = J_{24}$, $6 = J_{31}$, $8 = J_{32}$, $14 = J_{33}$ a $16 = J_{34}$.

Vlastnosti polohy bodů kubiky dosáhneme tím, že zavedeme: tři body leží v přímce, je-li jejich součin roven jednotkovému prvku a výpočet provádíme podle tabulky, jež je specializací (2) pro $p = 4$. Odtud je například vidět, že bodu J_1 mohou být přiřazeny jedině prvky 3, 9, 11, neboť $3 . 3 . X = 1 \Rightarrow X = 1$ a prvek 3 má tečnovým bodem bod 1 (Tato rovnice je splněna i pro prvky 9, 11 – dále může být nejen $3 = J_1$, ale i J_2 nebo J_3; v předchozím byla jedna možná interpretace zvolena).

Ověření zbývajících výsledků přenecháme čtenáři s tím, že hledaných dalších 16 přímek je (první tři body každé přímky najdeme pomocí tabulky a zbývající bod určíme tak, aby uvažované přímky měly požadované vlastnosti konečné afinní roviny):

$$
\begin{array}{llll}
\{2, 7, 14, 1\}, & \{2, 5, 16, 3\}, & \{2, 8, 13, 9\}, & \{2, 15, 6, 11\}, \\
\{4, 7, 16, 9\}, & \{4, 5, 14, 11\}, & \{4, 13, 6, 1\}, & \{4, 15, 8, 3\}, \\
\{10, 7, 6, 3\}, & \{10, 5, 8, 1\}, & \{10, 13, 16, 11\}, & \{10, 15, 14, 9\}, \\
\{12, 7, 8, 11\}, & \{12, 5, 6, 9\}, & \{12, 13, 14, 3\}, & \{12, 15, 16, 1\}.
\end{array}
$$

Literatura

[1] *Jaromír Krys:* Konfigurace bodů rovinné kubiky III. Čas. pěst. mat. *102* (1972), 186–188.
[2] *Jaromír Krys:* Rovinné konfigurace typu $(3n_n\ n_3^2)$. Čas. pěst. mat. *95* (1970), 66–70.
[3] *Karel Havlíček a kol.:* Cesty moderní matematiky. Praha 1976.

Adresa autora: 501 91 Hradec Králové, Orlické nábř. č. 1 (katedra matematiky PF Hradec Králové).

Zusammenfassung

ÜBER DIE MODELLE ENDLICHER AFFINER EBENEN

JAROMÍR KRYS, Hradec Králové

Das Hauptergebnis dieses Artikels ist eine Konstruktion der Modelle endlicher affiner Ebenen der Ordnung p, wo p eine Primzahl ist. Die Punkte dieses Modells sind die Elemente einer komutativen Gruppe G der Ordnung p^2, welche $p + 1$ verschiedene Untergruppen G_{p_i}, $i = 1, 2, \ldots, p + 1$ hat. Die Geraden dieses Modells sind alle Klassen der Faktorgruppen G/G_{p_i}. Weiter wird in diesem Artikel eine Kubik in Zusammenhang mit den vorhergehenden und weiteren Modellen affiner Ebenen betrachtet.