Časopis pro pěstování mathematiky a fysiky

Karel Petr

Poznámka o Legendre-Jacobiově symbolu $\left(\frac{P}{Q}\right)$

Časopis pro pěstování mathematiky a fysiky, Vol. 40 (1911), No. 2, 162--165

Persistent URL: `http://dml.cz/dmlcz/122395`

sestrojíme-li tedy k přímce A harmonickou přímku B vzhledem k tečně T kružnice K v bodě a a površce $\overline{c'a}$ uvažovaného kužele, jest B řídící přímkou hyperboloidu zborceného, oskulujícího danou plochu podél přímky A. Druhé dvě řídící přímky našli bychom tímtéž způsobem pomocí kuželů s ostatních bodů zmíněných ploše opsaných. Jak by se oskulačních hyperboloidů dané plochy užilo, je známo a netřeba se o tom šířiti.

Poznámka: Předpokládejme, že z veškerých bodů přímky $\overline{cs}$ (obr. 1[a]) vycházejí světelné paprsky. Pak tvoří ony paprsky, které se od rotačního válce **V** o ose O jen jedenkráte odrazily a to pouze v bodech kružnice K paprskovou kongruenci 6. stupně. Kongruence ta obsahuje ∞^1 ploch affinních k uvažované ploše a veškery tyto plochy obsahují kružnici K a dotýkají se kardioidického válce **C** původně uvažované ploše směrem O opsaného. Z toho patrno, že kongruenčních paprsků spadajících do určité roviny ϱ je šestero, jest to totiž oněch šest tečen, jež lze k průsečné křivce roviny ϱ s válcem **C** průsečnými body kružnice K a roviny ϱ vésti. Libovolným bodem p lze vésti tři tečné roviny válci **C** a v každé z nich leží dva paprsky jdoucí bodem p a protínající kružnici K. I jde libovolným bodem v prostoru rovněž šest paprsků uvažované kongruence, čímž dovozeno, že táž jest 6. stupně.

Konečně, svítí-li celá přímka $\overline{sc}$, a odrážejí-li se paprsky ve všech bodech válce **V**, vytvářejí jednou odražené paprsky velmi specielní komplex, sestávající z veškerých tečen kardioidického válce **C**. Jakého druhu jsou komplexní křivky a kužely, jest patrno z věci samé.

Poznámka o Legendre-Jacobiově symbolu $\left(\frac{P}{Q}\right)$.

Napsal **K. Petr.**

V pojednání „Über eine Darstellung des Legendre'schen Zeichens“ (Sitzungsb. der k. Akad. der W. in Wien, Bd. CXIII. Abt. II*a*, 1904) podal *F. Mertens* vyjádření Legendrova symbolu $\left(\frac{q}{p}\right)$ pomocí polynomu o dvou proměnných

$$\prod_{a,b} (x^a - y^b)(x^a y^b - 1) \tag{1}$$

$$a = 1, 2, \ldots \frac{p-1}{2}; \qquad b = 1, 2, \ldots \frac{q-1}{2}.$$

Výsledek Mertensův lze jednak bez potíže rozšířiti na symbol Legendre-Jacobiův, jednak lze pomocí Mertensovy funkce (1) podati přímý a zcela jednoduchý důkaz zákona reciprocity pro tento symbol. Obojí — i vyjádření Legendre-Jacobiova symbolu i důkaz zákona reciprocity — se pak ještě zjednoduší, užíváme-li místo polynomu (1) polynom

$$f(x, y) = \Pi (x^a y^{Q-b} - x^{P-a} y^b)(x^a y^b - x^{P-a} y^{Q-b}); \tag{2}$$

$$a = 1, 2, \ldots \frac{P-1}{2}; \qquad b = 1, 2, \ldots \frac{Q-1}{2},$$

kde o P a Q budeme toliko předpokládati, že to jsou čísla celá lichá bez společné míry.

Symbol $\left(\frac{Q}{P}\right)$ lze, jak známo, definovati pomocí počtu zbytků záporných, které dostáváme, dělíme-li po řadě všecka čísla

$$1 \,.\, Q, \quad 2 \,.\, Q, \quad 3 \,.\, Q, \ldots \frac{P-1}{2} \, Q$$

číslem P tak, aby zbytek byl co do absolutní hodnoty nejmenší $\left(\text{menší než } \frac{P}{2}\right)$. Je-li počet ten μ, jest dle definice

$$\left(\frac{Q}{P}\right) = (-1)^\mu.$$

Abychom dokázali zákon reciprocity pro symbol $\left(\frac{Q}{P}\right)$, vypočteme $f(\alpha, \beta)$, kde α jest primitivní P-tý kořen z jednotky a β jest primitivní Q-tý kořen z jednotky.

Nejprve jest

$$f(x, \beta) = \prod_{a,b} (x^a \beta^{-b} - x^{P-a} \beta^b)(x^a \beta^b - x^{P-a} \beta^{-b})$$

$$= \prod_{a,b} (x^a - x^{P-a} \beta^{2b})(x^a - x^{P-a} \beta^{-2b}).$$

Avšak čísla

$$\beta^{2b}, \beta^{-2b}; \qquad b = 1, 2, \ldots \frac{Q-1}{2}$$

jsou všecky Q-té kořeny z jedné různé od jedné, t. j. jsou to všecky kořeny rovnice

$$\frac{x^Q - 1}{x - 1} = 0;$$

i můžeme tudíž psáti

$$f(x, \beta) = \prod_a \frac{x^{Qa} - x^{Q(P-a)}}{x^a - x^{P-a}}, \quad a = 1, 2, \ldots \frac{P-1}{2}. \tag{3}$$

Dosadíme-li do této rovnice α za x, máme

$$f(\alpha, \beta) = \prod_a \frac{\alpha^{Qa} - \alpha^{-Qa}}{\alpha^a - \alpha^{-a}}, \quad a = 1, 2, \ldots \frac{P-1}{2}.$$

V exponentech čísla α můžeme však libovolný celistvý násobek čísla P odčítati; shodují se tudíž faktory čitatele až na pořádek a na znaménko s faktory jmenovatele a jest jich celkem μ, které se znaménkem od sebe liší, takže máme konečně

$$f(\alpha, \beta) = (-1)^\mu = \left(\frac{Q}{P}\right). \tag{4}$$

Polynom (2) můžeme však také psáti ve tvaru

$$f(x, y) = (-1)^{\frac{P-1}{2} \cdot \frac{Q-1}{2}} \prod_{a,b} (x^{P-a} y^b - x^a y^{Q-b})(x^a y^b - x^{P-a} y^{Q-b})$$

a počet právě provedený opakovati s tím pouze rozdílem, že napřed dosadíme za x číslo α a potom β za y. Dostaneme

$$f(\alpha, \beta) = (-1)^{\frac{P-1}{2} \cdot \frac{Q-1}{2}} \left(\frac{P}{Q}\right).$$

Srovnání obou výsledků dává vztah

$$\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2} \cdot \frac{Q-1}{2}} \left(\frac{P}{Q}\right),$$

což jest právě zákon reciprocity pro Legendre-Jacobiův symbol.

Označme, abychom podali vyjádření symbolu $\left(\frac{Q}{P}\right)$ obdobné vyjádření Mertensově, polynom dělitelný polynomem g krátce $[g)$;

značme dále X polynom v x, který položen rovný nulle, dává rovnici pro primitivní P-té kořeny z jedné; podobně budiž Y polynom v y, který položen rovný nulle dává rovnici pro primitivní Q-té kořeny z jedné. Pak jest nejprve dle (3) a (4) polynom

$$f(x, \beta) - \left(\frac{Q}{P}\right)$$

rovný nulle, když x jest rovno primitivnímu P-tému kořenu z jedné a tedy

$$f(x, \beta) - \left(\frac{Q}{P}\right) = [X). \tag{5}$$

Zcela podobně jest

$$f(x, y) - f(x, \beta) = [Y); \tag{6}$$

neboť koefficienty polynomu $f(x, \beta)$ jsou čísla racionálná celistvá dle (3) nezávislá na β. Jsou tedy i koefficienty polynomů $[X)$, $[Y)$ čísla racionálná celistvá.

Z (5) a (6) vyplývá

$$f(x, y) = \left(\frac{Q}{P}\right) + [X) + [Y),$$

což jest identita dávající vyjádření symbolu $\left(\frac{Q}{P}\right)$ polynomem $f(x,y)$.

Mertens odvodil v cit. pojednání tento vztah

$$\left(\frac{q}{p}\right) = U^{pq} + [X) + [Y),$$

kde p, q jsou dvě různá lichá prvočísla, U polynom (1) a

$$X = \frac{x^p - 1}{x - 1}, \qquad Y = \frac{y^q - 1}{y - 1}.$$