

Povzetek vsebine:

Diplomsko delo je razdeljeno na vsebinsko povezana poglavja:

1. V uvodu spoznamo definiciji projektivnega prostora in projektivne krivulje.
2. V drugem poglavju definiramo seštevanje na poljubni projektivni nesingularni kubični krivulji. Dokažemo, da ima krivulja za to operacijo strukturo Abelove grupe. Kot zanimivost z uporabo kubičnih krivulj dokažemo Pascalov izrek o magičnem šestkotniku.
3. V tretjem poglavju izpeljemo eksplisitne formule za seštevanje in računanje inverza na Weierstrassovi krivulji. V tem poglavju izvemo tudi, kako lahko definiramo strukturo grupe na singularni kubični krivulji.
4. V četrtem poglavju obravnavamo točke končnega reda s celoštevilskimi koordinatami na Weierstrassovi krivulji nad obsegom $O \subset C$. Natančneje spoznamo točke drugega in tretjega reda. Dokažemo Nagell - Lutzov izrek o točkah končnega reda s celoštevilskimi koordinatami.

Math. Subj. Class. (1991): 11G05, 11D25, 14H52

Meničelna elementa v in v' vektorskoga prostora \mathbb{P}^{n+1} sta predstavnika iste točke v projektivnem prostoru \mathbb{P}^n natančno tedaj, ko obstaja tak neničelen $\lambda \in \mathbb{K}$, da je $\lambda v = v'$.
Neničelen vektor $(x_0, \dots, x_n) \in \mathbb{P}^{n+1}$ je predstavnik nekega elementa $x \in \mathbb{P}^n$. Homogeni koordinati elementa x imenujemo n-terico $[x_0 : \dots : x_n]$. Pri tem za vsak neničelen $\lambda \in \mathbb{K}$ velja: $[x_0 : \dots : x_n] = [\lambda x_0 : \dots : \lambda x_n]$.

Definicija:

Če bo $F(x,y,z)$ homogen polinom stopnje d in naj nima večkratnih korenov. Projektivna krivulja $C \subset \mathbb{P}^2$ podana s polinomom F je množica

$$C = \{(x,y,z) \in \mathbb{P}^2 \mid F(x,y,z) = 0\}.$$

Homogenja krivulje C je enaka stopnji polinoma F , ki jo določa.

Definicija:

Točka $[a,b,c]$ na projektivni krivulji C je singularna, če za polinom F , ki določa krivuljo velja:

$$\frac{\partial F}{\partial x}(a,b,c) = \frac{\partial F}{\partial y}(a,b,c) = \frac{\partial F}{\partial z}(a,b,c) = 0.$$

Krivulja C je nesingularna, če ne vsebuje nobene singularne točke.

Definicija:

(Krač ravnino A^2 v \mathbb{P}^2 nad obsegom O lahko predstavimo z enačbo $z = 1$:

$$A^2 = \{(x,y,z) \in \mathbb{P}^2 \mid z = 1\} \cap \{(x,y,1) \in \mathbb{P}^2\}.$$

Tj. na krivulja, ki jo določa polinom $F(x,y,1) = f(x,y)$ je množica

$$C_f = \{(x,y) \in A^2 \mid f(x,y) = 0\}.$$

LITERATURA:

- [1] M. Ried, *Undergraduate Algebraic Geometry*, Cambridge University Press, Cambridge, 1988
- [2] J. H. Silverman, J. Tate, *Rational Points on Elliptic Curves*, Springer - Verlag, New York, Berlin, Heidelberg, 1992
- [3] D. Husemöller, *Elliptic Curves*, Springer - Verlag, New York, Berlin, Heidelberg, 1987
- [4] I. Vidav, *Eliptične krivulje in eliptične funkcije*. Društvo matematikov, fizikov in astronomov Slovenije, Ljubljana 1991
- [5] A. W. Knapp, *Elliptic Curves*, Princeton University Press, Princeton, New Jersey, 1992