

Hlavným cieľom tejto práce je dôkaz Cayleovho kritéria, ktoré popisuje nutnú a postačujúcu podmienku na to, aby rád bodu $(0, a_0)$ na danej eliptickej krivke delil dané prirodzené číslo n . V práci popisujeme potrebnú teóriu k diskretným valuačným okruhom, algebraickým množinám a polynomiálnym a racionálnym funkciám na ireducibilných algebraických množinách. Zaoberáme sa tiež vlastnosťami rovinných kriviek a eliptických kriviek, ktoré sú špeciálnym prípadom afinných rovinných kriviek. Na množine bodov projektívneho uzáveru eliptickej krivky definujeme grupovú štruktúru dvomi spôsobmi - geometricky a pomocou divizorov - a ukazujeme, že tieto dve grupové štruktúry si odpovedajú. Nakoniec sa venujeme samotnému dôkazu Cayleyovho kritéria.