بسم الله الرحمن الرحیم

دانشگاه ارومیه

دانشکده علوم

گروه ریاضی

پایان‌نامه دوره کارشناسی ارشد در رشته ریاضی محض گرایش جبر

تاب خم‌های بیضوی روی میدان‌های دایره‌بر مربعی

استاد راهنما:

دکتر علی سرباز جانفدا

نام دانشجو:

لیلا افشاری

بهمن ۱۳۹۲

تقدیم به

پدرم: چراغ راه و امید زندگیم،

مادرم: مهربان ترین فرشته زندگی ام که اکنون در بین

ما نیست،

برادرانم: یاوران همیشگی من در زندگی،

خواهرم: همدل و همراه همیشگی من،

و

تقدیم به تمام عزیزانی که دوستشان دارم.

سپاس گزاری...

خدایم سپاس، سپاس تو را برای همه چیز، سپاس بر آن چه به من دادی و هر آن چه که از من گرفتی. تو خود دانی که تنها پناهم تو بودی و هستی. در آن شب‌ها و روزهای سخت که خستگی طاقتم می‌برد و ناامیدی رمقم می‌گرفت تو بودی، تو بودی توانم دادی و آن تلاش‌های بی‌وقفه و مداوم را ثمر دادی. در آن تنهایی‌ها تو بودی تنها پناهم، در آن نامهربانی‌ها تو بودی همراه و هم‌نوایم. در آن بیچارگی‌ها تو بودی کارساز مشکلاتم، خدایا مباد رهایم کنی که به الطافت ایمان دارم.

اینک که به لطف پروردگار با کوله‌باری از تجربه که از راهنمایی و تلاشهای اساتید فرزانه‌ام اندوخته‌ام به پایان تلاش چند ساله نزدیک می‌شوم، به حکم ادب و وظیفه بر خود لازم می‌دانم مراتب قدردانی و تشکر خود را نسبت به تمام عزیزانی که به نحوی مرا در به انجام رساندن این مسئولیت یاری نمودند، هر چند کوتاه ابراز دارم.

از استاد راهنمای گرامی جناب آقای دکتر علی سرباز جانفدا که خالصانه مرا از گنجینه گهربار علم و تجربیات خود بهره‌مند ساخته و درنهایت صبر و شکیبایی مرا تشویق و راهنمایی نموده و در تمام مراحل مورد لطف و محبت خویش قرار دادند، تشکر می‌کنم. همچنین از اساتید گرامی آقایان دکتر رضا سزیده و دکتر محسن قاسمی که زحمت داوری این پایان‌نامه را بر عهده داشتند کمال تشکر و قدردانی را دارم. از تمامی اساتید محترم گروه ریاضی دانشگاه ارومیه که در رشد علمی بنده سهیم بوده‌اند، نیز کمال تشکر را دارم.

از پدر عزیزم که در تمام این مدت با صبر و شکیبایی و رهنمودهای ارزشمند خود در این راه یاریم کرد، از مادرم که دعای خیر خود را حتی در نبودش بدرقه راهم در همه مراحل زندگی‌ام کرده، از برادرعزیزم غلامرضا که درتنظیم این پایان‌نامه کمک‌های شایانی انجام داده و همچنین از همه اعضای خانواده‌ام که در این راه با من همراه و همدل بودند، تشکر و قدردانی می‌کنم.

لیلا افشاری

بهمن ۹۲

چکیده

در این پایان‌نامه، تاب‌های احتمالی از خم‌های بیضوی را روی میدان‌های $\mathbb{Q}(i)$ و $\mathbb{Q}(\sqrt{-۳})$ بررسی خواهیم کرد.

فهرست مطالب

پیشگفتار

در این پایان‌نامه در مورد دو میدان مربعی $\mathbb{Q}(i)$ و $\mathbb{Q}(\sqrt{-۳})$ بحث خواهیم کرد. حلقه اعداد صحیح میدان $\mathbb{Q}(i)$ عبارت است از:

$$\partial = \mathbb{Z}[i] = \Big\{a + bi | a, b \in \mathbb{Z}\Big\}$$

که به حلقه گاوسی معروف است. حلقه اعداد صحیح $\mathbb{Q}(\sqrt{-۳})$ نیز بصورت:

$$\partial = \mathbb{Z}[\sqrt{-۳}] = \Big\{a + b\sqrt{-۳} | a, b \in \mathbb{Z}\Big\}$$

است. این میدان‌ها تا حدودی استثنایی هستند، زیرا تنها میدان‌هایی هستند که ریشه‌های واحدی غیر از ۱ و ۱− دارند؛ یعنی آنها تنها میدان‌های دایره‌بر مربعی هستند. همچنین روی هر یک از این میدان‌ها، زیرگروه‌های تابی ظاهر می‌شود که روی میدان‌های دیگر ظاهر نمی‌شود. به عنوان مثال تنها میدان مربعی روی تاب $\mathbb{Z}_۴ \oplus \mathbb{Z}_۴$ در $\mathbb{Q}(i)$ ظاهر می‌شود وتنها میدان مربعی روی تاب‌های $\mathbb{Z}_۳ \oplus \mathbb{Z}_۳$ و$\mathbb{Z}_۳ \oplus \mathbb{Z}_۶$ در $\mathbb{Q}(\sqrt{-۳})$ بنا به [۶] ظاهر می‌شود. لازم به ذکر است که حلقه اعداد صحیح از هر دو این میدان‌ها حوزه تجزیه یکتا هستند. در این پایان‌نامه ما یک خط مشیء متفاوت خواهیم گرفت، بطوریکه میدان مربعی را ثابت نگه داشته و تاب‌های احتمالی را بررسی خواهیم کرد.[۸] این پایان‌نامه شامل سی فصل می‌باشد. فصل اول تعاریف و قضایای مقدماتی، که در فهم و درک بهتر مطالب ارائه شده در فصل‌های بعدی، کمک شایانی خواهد کرد، را گنجاندهیم. در فصل دوم اثبات تعمیم قضیه لوتز – ناقل [۱] در میدان $\mathbb{Q}(i)$ را آورده‌ایم؛ و نیز تاب‌های احتمالی روی این میدان را بررسی خواهیم کرد. در نهایت در فصل سوم نیز تاب‌های احتمالی روی میدان $\mathbb{Q}(\sqrt{-۳})$ را بررسی خواهیم کرد.

این پایان نامه بر اساس مقاله زیر تدوین گردیده است:

[۱] Lutz - Nagell

- Filip Najman .Torsion of elliptic corves over quadratic cyclotomic fields. *Math. J. Okayama Univ*. 53, pp. 75-82, 2011.

فصل ۱

تعاریف و قضایای مقدماتی

۱.۱ اعداد گاوسی

تعریف ۱.۱.۱. یک عدد صحیح گاوسی، یک عدد مختلط بفرم $a+bi$ است که $a,b \in \mathbb{Z}$. مجموعه همه اعداد صحیح گاوسی را با $\mathbb{Z}(i)$ نمایش می‌دهیم. ثابت می‌شود که $\mathbb{Z}(i)$ یک حلقه، به نام حلقه گاوسی، است.

تعریف ۲.۱.۱. فرض کنید $\alpha, \beta \in \mathbb{Z}(i)$. گوییم α بر β بخش‌پذیر است هر گاه $\beta \neq ۰$. و $\gamma \in \mathbb{Z}(i)$ وجود داشته باشد بطوریکه $\alpha = \beta\gamma$. این عمل را با نماد $\beta \mid \alpha$ نمایش می‌دهیم. در غیر این صورت گوییم α بر β بخش‌پذیر نیست و با $\beta \nmid \alpha$ نمایش می‌دهیم.

هر $x \in \mathbb{Q}(i)$ را می‌توان بصورت $\frac{g}{h}$ که $g,h \in \mathbb{Z}(i)$ یعنی بصورت یک خارج قسمت از اعداد گاوسی نوشت. فرض کنید که $\frac{g}{h}$ در ساده‌ترین فرم باشد یعنی g و h هیچ اشتراکی از عامل‌های اصلی گاوسی ۱ و ۱− و i و $-i$ نداشته باشد.

اگر $x \notin \mathbb{Z}(i)$ در اینصورت h نمی‌تواند یک یکه باشد، در این صورت یک عدد اول گاوسی p بخش‌پذیر بر h است. (یک عدد اول گاوسی p یک عدد صحیح گاوسی غیر یکه است، به طوری که هیچ عدد صحیح گاوسی دیگر، به جز یکه‌ها، نتواند p را عاد کند.)

رفتار اعداد گاوسی در بسیاری از روابط مشابه اعداد صحیح است. این روابط شامل موارد زیر می‌باشد:

۱) برای هر $\alpha = a+bi \in \mathbb{Z}(i)$، نرم گاوسی از α بوسیله $\mathbf{N}(\alpha) = |\alpha|^۲ = a^۲ + b^۲$ تعریف می‌شود که همیشه عددصحیح غیر منفی است.

۲) همه یکه‌ها از $\mathbb{Z}(i)$ عبارتند از ۱± و $\pm i$.

۳) یک عدد $\pi \in \mathbb{Z}(i)$ یک عدد گاوسی است اگر و فقط اگر بخش‌پذیر از $\pm ۱, \pm i, \pm\pi, \pm i\pi$ باشد.

۴) عدد اول $p \in \mathbb{Z}$ اول گاوسی است اگر و فقط اگر $p \equiv ۳ \pmod{۴}$.

۵) عدد $\pi \in \mathbb{Z}(i)$ یک اول گاوسی است اگر و فقط اگر

الف) $\mathbf{N}(\pi)$ یک عدد صحیح باشد یا،

ب) یک یکه ε و یک اول گاوسی p وجود داشته باشد بطوری که $\pi = \varepsilon P$.

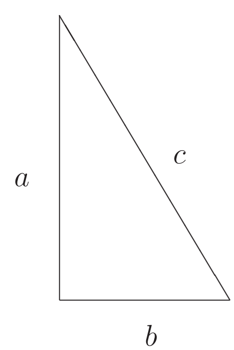
۲.۱ خم‌های بیضوی

خم بیضوی [1] چیست؟

آیا مثلث قائمه‌ای با اضلاع گویا و با مساحت ۵ وجود دارد؟

کوچکترین سه تایی فیثاغورس $(۳,۴,۵)$ مثلثی با مساحت ۶ را بدست می‌دهد. بنابراین می‌بینیم که ما نمی‌توانیم توجه‌مان را فقط به اعداد صحیح محدود کنیم. حال مثلثی با اضلاع $(۸,۱۵,۱۷)$ را در نظر می‌گیریم، این مثلث دارای مساحت ۶۰ می‌باشد. اگر این اضلاع بر ۲ تقسیم کنیم مثلثی با اضلاع $(\frac{۱۷}{۲},\frac{۱۵}{۲},۴)$، و مساحت ۱۵ را خواهیم داشت. بنابراین ممکن است که اضلاع غیرصحیح اما مساحت صحیح داشته باشیم.

فرض کنیم مثلثی که به دنبال آن هستیم با اضلاع a,b,c باشد.



چون مساحت $\frac{ab}{۲}=۵$ است، از این رو به دنبال اعداد صحیح a,b,c هستیم بطوری که

$$ab = ۱۰$$

و

$$a^۲ + b^۲ = c^۲$$

با دستکاری کوچک بدست می‌آوریم:

$$(\frac{a+b}{۲})^۲ = \frac{a^۲ + ۲ab + b^۲}{۴} = \frac{c^۲ + ۲۰}{۴} = (\frac{c}{۲})^۲ + ۵$$
$$(\frac{a-b}{۲})^۲ = \frac{a^۲ - ۲ab + b^۲}{۴} = \frac{c^۲ - ۲۰}{۴} = (\frac{c}{۲})^۲ - ۵$$

[1] elliptic curve

فرض کنیم $x = (\frac{c}{2})$ پس داریم:

$$x - 5 = (\frac{a-b}{2})^2$$

و

$$x + 5 = (\frac{a+b}{2})^2$$

از این رو به دنبال یک عدد گویای x هستیم. به طوری که مربع اعداد گویا تشکیل یک تصاعد حسابی با تفاضل ۵ باشد. فرض کنیم عدد x را داریم پس

$$(x-5)x(x+5) = x^3 - 25x$$

بایستی مربع کامل باشد. بنابراین نیاز به جواب گویا برای

$$y^2 = x^3 - 25x$$

داریم. این معادله یک خم بیضوی است.

۱.۲.۱ معادلات وایرشتراس

خم بیضوی E دارای معادله‌ای بفرم $y^2 = x^3 + Ax + B$ می‌باشد، بطوریکه A, B ثابت هستند. این معادله، معادله وایرشتراس برای خم بیضوی است. اگر $\mathbf{K}$ یک میدان با $A, B \in \mathbf{K}$ باشد آنگاه گوئیم که E روی $\mathbf{K}$ تعریف می‌شود. اگر بخواهیم نقاطی را با مختصاتشان در میدان‌های $L \supset \mathbf{K}$ بررسی کنیم، به صورت زیر تعریف می‌کنیم:

$$E(L) = \{\infty\} \cup \{(x,y) \in L \times L | y^2 = x^3 + Ax + B\}$$

اگر خم‌های بیضوی $y^2 = x^3 - x$ و $y^2 = x^3 + x$ را بررسی کنیم. ملاحظه می‌کنیم، معادله $y^2 = x^3 - x$ دارای سه ریشه حقیقی و معادله $y^2 = x^3 + x$ فقط دارای یک ریشه حقیقی است. از طرفی کمیت $4A^3 + 27B^2$ که مبین خم است، مخالف صفر در نظر می‌گیریم که ریشه مضاعف نداشته باشیم. اگر ریشه‌های معادله درجه سوم، را r_1, r_2 و r_3 در نظر بگیریم. از این رو معادله زیر، مشخص کننده معادله

درجه سه می‌باشد:

$$((r_1-r_2)(r_1-r_3)(r_2-r_3))^2=-(4A^3+27B^2)$$

لذا باید ریشه‌های معادله درجه سه مجزا باشد. در حالتی که ریشه‌ها متمایز نباشند، خم ناهموار خواهد بود که در بحث ما نمی‌گنجد. زیرا بحث ما در مورد خم‌های هموار است.

معادله وایرشتراس تعمیم یافته

$$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$$

به طوری که $a_1,a_2,\ldots,a_6$ ثابت باشند؛ زمانی که با میدان‌هایی با مشخصه ۲و۳ کار می‌کنیم، مفید است.

اگر مشخصه ۲ نباشد می‌توانیم با تقسیم بر ۲ به مربع کامل تبدیل کنیم:

$$(y+\frac{a_1x}{2}+\frac{a_3}{2})^2=x^3+(a_2+\frac{a_1^2}{4})x^2+(a_4+\frac{a_1a_3}{2})x+(\frac{a_3^2}{4}+a_6)$$

که می‌تواند بصورت زیر نوشته شود:

$$y_1^2=x^3+a_2'x^2+a_4'x+a_6'$$

با $y_1=y+\frac{a_1x}{2}+\frac{a_3}{2}$ و ثابت‌های a_2',a_4' و a_6'.

اگر مشخصه ۳ نباشد آنگاه با فرض $x_1=x+\frac{a_2'}{3}$، بدست می‌آوریم:

$$y_1^2=x_1^3+A_1x+B$$

بطوری که A,B ثابت هستند. اما خم‌هایی وجود دارند که به فرم $y^2=x^3+Ax+B$ نیستند. از این رو فرم کلی برای مشخصه ۳ می‌تواند بصورت زیر باشد:

$$y^2=x^3+Cx^2+Ax+B$$

۲.۲.۱ نقاط K-گویا

به ازای هر خم بیضوی E روی میدان عددی **K** مجموعه

$$E(\mathbf{K}) = \{(x, y) \in \mathbf{K} \times \mathbf{K} | y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6\} \cup \{\infty\}$$

یک زیرگروه از E بوده که نقاط **K**-گویا روی E گفته می‌شوند. قضیه‌ای که در ادامه بحث ارائه خواهیم داد دارای ساختار یک گروه آبلی می‌باشد، به طوری که نقطه ∞ عضو همانی آن است.

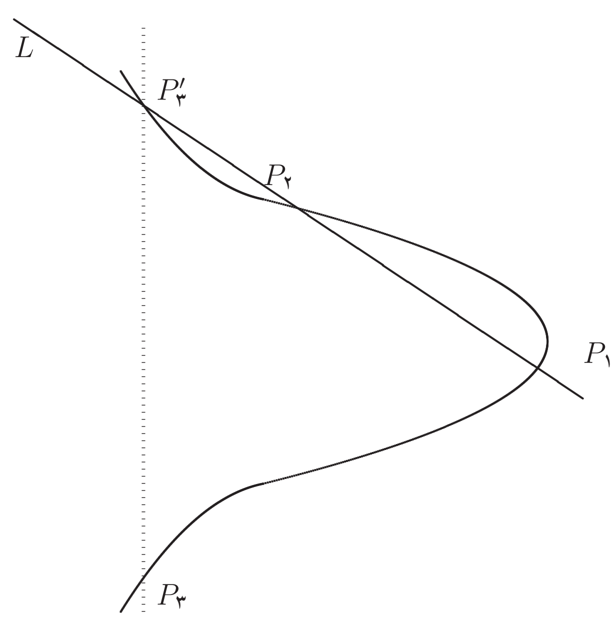
در زیر در مورد قانون گروهی روی $E(\mathbf{K})$، که در فصل مشترک خط گذرنده از نقاط در $E(\mathbf{K})$ است، بحث خواهیم کرد.

۳.۲.۱ قانون گروهی

جمع نقاط روی خم بیضوی:

فرض کنید E یک خم بیضوی تعریف شده روی میدان عددی **K** به فرم $y^2 = x^3 + Ax + B$ باشد. فرض کنید $P_1 = (x_1, y_1)$ و $P_2 = (x_2, y_2)$ نقاطی روی E باشد. خط گذرنده از نقاط P_1 و P_2 که L می‌نامیم، خم E را در نقطه P'_3 قطع می‌کند. از بازتاب این نقطه نسبت به محور xها نقطه P_3 بدست می‌آید. که تعریف می‌کنیم:

$$P_1 +_E P_2 = P_3$$



با توجه به شکل موجود حالت‌هایی از نقاط را در نظر گرفته، و به مطالعه آنها می‌پردازیم.

۱) فرض کنید $P_1=(x_1,y_1)$ و $P_2=(x_2,y_2)$ نقاطی روی E با $P_1\neq P_2$ و $P_1,P_2\neq\infty$ باشد. شیب خط گذرنده از نقاط P_1,P_2 برابر است با:

$$m=\frac{y_2-y_1}{x_2-x_1}$$

الف) اگر $x_1\neq x_2$، در این حالت معادله خط L به صورت:

$$y=m(x-x_1)+y_1.$$

می‌باشد. با قطع دادن این معادله با معادله خم E بدست می‌آوریم:

$$(m(x-x_1)+y_1)^2=x^3+Ax+B$$

که با دوباره‌نویسی داریم:

$$0=x^3-m^2x^2+\dots$$

سه ریشه از این معادله درجه سوم متناظر با سه نقطه از قطع دادن خط L با خم E است. چون دو ریشه x_1,x_2 را داریم، لذا ریشه سوم را به روش زیر پیدا می‌کنیم:

با فرض چندجمله‌ای x^3+ax^2+bx+c با ریشه‌های r,s و t داریم:

$$\begin{aligned}x^3+ax^2+bx+c&=(x-r)(x-s)(x-t)\\&=x^3-(r+s+t)x^2+\dots\end{aligned}$$

بنابراین:

$$r+s+t=-a$$

با معلوم بودن دو ریشه r,s سومین ریشه بصورت زیر بدست می‌آید:

$$t=-a-r-s$$

پس داریم:

$$x = m^{2} - x_{1} - x_{2}$$
$$y = m(x - x_{1}) + y_{1}$$

بازتاب این نقاط نسبت به محور xها نقطه $P_{3} = (x_{3}, y_{3})$ را بصورت زیر بدست می‌آوریم:

$$x_{3} = m^{2} - x_{1} - x_{2}$$
$$y_{3} = m(x_{1} - x_{3}) + y_{1}$$

ب) اگر $x_{1} = x_{2}$ ولی $y_{1} \neq y_{2}$، در این حالت خط L یک خط عمودی است که E را در ∞ قطع می‌کند. بازتاب ∞ نسبت به محور xها همان نقطه ∞ می‌باشد. (چون می‌توانیم ∞ را در بالا و پایین محور yها قرار دهیم.) بنابراین در این حالت

$$P_{1} + P_{2} = \infty.$$

۲) فرض کنید $P_{1} = P_{2} = (x_{1}, y_{1})$، در این حالت خط L یک خط مماس است. با مشتق‌گیری ضمنی شیب خط L برابر است با:

$$2y\frac{dy}{dx} = 3x^{2} + A \Longrightarrow m = \frac{dy}{dx}|_{P_{1}} = \frac{3x_{1}^{2} + A}{2y_{1}}$$

الف) اگر $y_{1} = 0$، در این صورت خط L یک خط عمود است و داریم:

$$2P_{1} = P_{1} + P_{1} = \infty.$$

ب) اگر $y_{1} \neq 0$، معادله خط L بصورت زیر است:

$$y = m(x - x_{1}) + y_{1}$$

معادله درجه سوم زیر را بدست می‌آوریم:

$$0 = x^3 - m^2x^2 + \ldots$$

در این حالت x_1 ریشه مضاعف می‌باشد. از طرفی چون خط L بر خم E در نقطه P_1 مماس است، بنابراین داریم:

$$x_3 = m^2 - 2x_2 \quad , \quad y_3 = m(x_1 - x_3) - y_1.$$

۳) فرض کنید $P_2 = \infty$، در این حالت خط گذرنده از نقطه P_1 و ∞ خط عمودی است که خم E را در نقطه P_1' قطع می‌کند و بازتاب آن نسبت به محور xها نقطه P_1 است. بنابراین برای همه نقاط P_1 روی خم E داریم:

$$P_1 + \infty = P_1.$$

آنچه که در بالا بحث شد می‌توان بصورت زیر خلاصه کرد.

قانون گروهی

فرض کنید E یک خم بیضوی تعریف شده به فرم $y^2 = x^3 + Ax + B$ باشد. فرض کنید $P_1 = (x_1, y_1)$ و $P_2 = (x_2, y_2)$ نقاطی روی E با $P_1, P_2 \neq \infty$ باشد. در این صورت مقادیر $P_1 +_E P_2 = P_3 = (x_3, y_3)$ از تعریف زیر محاسبه می‌شود:

۱) اگر $x_1 \neq x_2$ باشد، آنگاه :

$$x_3 = m^2 - x_1 - x_2 \quad , \quad y_3 = m(x_1 - x_3) - y_1 \quad , \quad m = \frac{y_2 - y_1}{x_2 - x_1}.$$

۲) اگر $x_1 = x_2$ و $y_1 \neq y_2$، آنگاه :

$$P_1 + P_2 = \infty.$$

۳) اگر $P_1 = P_2$ و $y_1 \neq 0$، آنگاه :

$$x_3 = m^2 - 2x_1 \quad , \quad y_3 = m(x_1 - x_3) - y_1 \quad , \quad m = \frac{3x_1^2 + A}{2y_1}.$$

۴) اگر $P_۱ = P_۲$ و $y_۱ = ۰$، آنگاه :

$$P_۱ + P_۲ = \infty.$$

بعلاوه برای همه نقاط P روی E تعریف می‌کنیم:

$$P + \infty = P.$$

در حالتی که نقاط $P_۱, P_۲$ دارای مختصاتی در میدان $\mathbf{K}$، باشند که شامل A, B هست. آنگاه $P_۱ + P_۲$ نیز دارای مختصاتی در $\mathbf{K}$ است، از این رو $E(\mathbf{K})$ تحت جمع نقاطی ارائه شده بسته است.

قضیه ۱.۲.۱. *عمل جمع گروهی روی خم E در خاصیت های زیر صدق می‌کند:*

۱) *(جابجایی) برای همه نقاط $P_۱$ و $P_۲$ روی خم E داریم:*

$$P_۱ + P_۲ = P_۲ + P_۱$$

۲) *(وجود عضو همانی) برای همه نقاط P روی خم E داریم:*

$$P + \infty = P$$

۳) *(وجود عضو وارون) با در نظر گرفتن نقطه P روی خم E، نقطه P' روی خم E وجود دارد بطوری که:*

$$P + P' = \infty$$

معمولا نقطه P' مشخص کننده $-P$ می‌باشد.

۴) *(شرکت پذیری) برای همه نقاط $P_۱$ و $P_۲$ و $P_۳$ روی خم E داریم:*

$$(P_۱ + P_۲) + P_۳ = P_۱ + (P_۲ + P_۳)$$

به بیان دیگر نقاط خم E روی میدان عددی $\mathbf{K}$ تشکیل یک گروه آبلی می‌دهند که ∞ عضو همانی آن است.

اثبات. به [[۱۴]،قضیه ۱.۲] رجوع شود. □

تعریف ۲.۲.۱. خمی را نامنفرد گوئیم هر گاه هیچ نقطه‌ای از آن دارای مشتقات جزئی صفر نباشد. و خمی را منفرد(ناهموار) گوئیم که حداقل یک نقطه از آن دارای مشتقات جزئی صفر باشد.

قضیه ۳.۲.۱. *فرض کنید E یک خم بیضوی تعریف شده روی یک میدان $\mathbf{K}$ با مشخصه مخالف ۲، ۳ مفروض به وسیله*

$$y^{۲} = (x-\alpha)(x-\beta)(x-\gamma)$$

به طوری که α ، β و γ در $\mathbf{K}$ باشد. برای این که (x,y) در $E(\mathbf{K})$ یک نقطه $\mathbf{K}$ ـگویا باشد (x',y') در $E(\mathbf{K})$ وجود دارد به طوری که $۲(x',y') = (x,y)$ اگر و فقط اگر $x-\alpha$ ، $x-\beta$ و $x-\gamma$ همه در $\mathbf{K}$ مربع باشند.

اثبات. به [[۷]، قضیه ۲.۴] رجوع شود. □

به هر حال اگر ما هر یکی از $\sqrt{x-\alpha}$ ، $\sqrt{x-\beta}$ و $\sqrt{x-\gamma}$ را ثابت نگه داریم، x' با یکی از حالات زیر برابر است:

$$\sqrt{x-\alpha}\sqrt{x-\beta} \pm \sqrt{x-\alpha}\sqrt{x-\gamma} \pm \sqrt{x-\beta}\sqrt{x-\gamma} + x$$

یا

$$-\sqrt{x-\alpha}\sqrt{x-\beta} \pm \sqrt{x-\alpha}\sqrt{x-\gamma} \mp \sqrt{x-\beta}\sqrt{x-\gamma} + x$$

که علامت‌ها بطور همزمان برداشته می‌شود.

۴.۲.۱ نقاط از مرتبه متناهی

فرض کنیم خم $E : y^{۲} = x^{۳} + Ax + B$ روی میدان $\mathbf{K}$ باشد؛ یعنی $A, B \in \mathbf{K}$. در مطالعات خود مشخصه میدان $\mathbf{K}$ را مخالف ۲ و ۳ در نظر می‌گیریم. ثابت می‌شود که E نامنفرد است اگر و فقط اگر $۴A^{۳} + ۲۷B^{۲} \neq ۰$. کمیت $-(۴A^{۳} + ۲۷B^{۲})$ را مبین خم E می‌نامیم.

تعریف ۴.۲.۱. فرض کنیم E خم بیضوی روی میدان $\mathbf{K}$ و p یک نقطه روی E باشد. مرتبه p را با $ord(p)$ نشان می‌دهیم. اگر n متناهی باشد، آنگاه p یک نقطه تاب روی خم E است و چنین تعریف می‌کنیم:

$$E[n] = \Big\{p \in E | np = \infty\Big\}$$

لازم به ذکر است که نقاط از مرتبه n زیرمجموعه‌ای از $E[n]$ است ولی عکس آن برقرار نیست.

قضیه ۵.۲.۱. *فرض کنیم E یک خم بیضوی روی میدان $\mathbf{K}$ و n یک عدد صحیح مثبت باشد. اگر مشخصه $\mathbf{K}$، n را عاد نکند یا صفر باشد آنگاه:*

$$E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n$$

ولی اگر مشخصه $\mathbf{K}$، $p > 0$ باشد و $p \mid n$، در این صورت $n = p^r n'$ با $p \nmid n'$. آنگاه:

$$E[n] \simeq \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'} \quad \text{یا} \quad \mathbb{Z}_n \oplus \mathbb{Z}_{n'}$$

اثبات. به [[۱۴]، قضیه ۲.۳] رجوع شود. □

۵.۲.۱ خم‌های بیضوی روی میدان‌های متناهی

در این قسمت قضایای اساسی که به ما در محاسبه مرتبه گروه کمک خواهد کرد، را بیان می‌کنیم:

قضیه ۶.۲.۱. (قضیه هس[۱]) *فرض کنید E یک خم بیضوی روی میدان متناهی $\mathbb{F}_q$ باشد (q یا عدد اول یا توانی از عدد اول است.)، دراینصورت مرتبه گروه $E(\mathbb{F}_q)$ در نامساوی زیر صدق می‌کند:*

$$|q + 1 - \sharp E(\mathbb{F}_q)| \leq 2\sqrt{q}$$

اثبات. به [[۱۴]، قضیه ۲.۴] رجوع شود. □

قضیه ۷.۲.۱. *فرض کنید $\sharp E(\mathbb{F}_q) = q + 1 - a$، و چندجمله‌ای مشخصه $X^2 - aX + q$ را بتوانیم بصورت زیر تجزیه کنیم:*

$$X^2 - aX + q = (X - \alpha)(X - \beta) \qquad , \qquad \alpha\beta = q \quad , \quad \alpha + \beta = a$$

در این صورت به ازای هر $n \geq 1$ داریم:

$$\sharp E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n)$$

[۱] Hasse