مسألهٔ اعداد دوقلو همنهشت

رباب بایرامی

دانشکدهٔ علوم
گروه ریاضی

مهر ۱۳۹۱

پایان‌نامهٔ کارشناسی ارشد

استاد راهنما:

دکتر علی سرباز جانفدا

تقدیم به دستان پدرم و قلب مادرم

سپاسگزاری

خداوندا، مرا ذهنی ببخش که بی‌گناه، پاک و رها از بدیها باشد، ذهنی که توکل کند، تردید نورزد، داوری نکند، ذهنی که تو را در همه ببیند و همه را در تو.

مراتب سپاس صمیمانه خود را از استاد راهنمای بزرگوارم جناب آقای دکتر علی سرباز جانفدا دارم که در تمام مراحل این پایان‌نامه همواره مشوق و پشتیبان برایم بوده وبا رهنمودهای ارزنده خود راهنمای اینجانب بوده‌اند.

از جناب آقای دکتر بهروش و جناب آقای دکتر قاسمی که زحمت خواندن و داوری این پایان‌نامه را بر عهده گرفتند تشکر می‌کنم.

در پایان از پدر و مادر مهربانم که اسوه‌ای از صبر و شکیبایی و تجسمی از لطف ومهربانی هستند، کمال تشکر را دارم.

چکیده

در این پایان‌نامه چهار ویژگی هم‌ارزی از اعداد همنهشت را مورد بررسی قرار داده‌ایم ویژگی چهارم که توسط کوبلیتز مطرح شده بود، با یک مثال نقض رد شده و اشکال آن برطرف می‌گردد. این چهار ویژگی نقش اساسی در مسأله‌ی اعداد دوقلو همنهشت دارند. اعداد دوقلو همنهشت را به طور هندسی و با یک نگاه جبری مورد مطالعه قرار داده‌ایم. ابتدا، تناظر بین اعداد همنهشت و خم‌های بیضوی را مورد بررسی قرار داده و سپس، به شمارش و تولید اعداد دوقلو همنهشت از نقطه نظر گروهی پرداخته‌ایم.

پیش‌گفتار

در میان مسأله‌های متعدد دیوفانتی فیثاغورث، مشهورترین مسأله‌ای که هنوز حل نشده مسأله‌ی اعداد همنهشت می‌باشد. اعداد همنهشت تاریخچه‌ای بسیار طولانی دارند، به‌طوری که ده‌ها قرن پیش اولین بار توسط دانشمندان مسلمان کشف شده‌اند. فرض کنیم n یک عدد صحیح مثبت باشد. در این صورت n را یک عدد همنهشت گوییم هرگاه n مساحت یک مثلث قائم‌الزاویه با اضلاع گویا باشد. یک خانواده از خم‌های بیضوی که معادلات آن به فرم $y^2 = x^3 - n^2x$ است را در نظر می‌گیریم. در این صورت ارتباط خاصی بین این خم‌های بیضوی و اعداد همنهشت n وجود دارد.

این پایان نامه بر اساس مقاله‌ی[٦] نوشته شده است. در فصل اول، تعاریف و مفاهیم اولیه مربوط به خم‌های بیضوی که در طول پایان‌نامه مورد استفاده قرار می‌گیرند، آورده شده‌اند. در فصل دوم ابتدا، قضایای مهم موردل—ویل و لاتز—ناقل را بیان می‌کنیم. سپس، اعداد همنهشت را تعریف کرده و ارتباط این اعداد و خم‌های بیضوی $E_n : y^2 = x^3 - n^2x$ را مطرح می‌کنیم. همچنین در این فصل چهار ویژگی مقدماتی از اعداد همنهشت را بررسی می‌کنیم که ویژگی‌های سوم و چهارم نقش اساسی درمسأله‌ی اعداد دوقلو همنهشت دارند.

در فصل سوم، که اصلی‌ترین قسمت این پایان‌نامه است، ابتدا یک تعریف از اعداد دوقلو همنهشت ارائه می‌دهیم. چون اعداد دوقلو همنهشت در فصل مشترک دو خم بیضوی خوش تعریف قرار می‌گیرند ضروری است که یک شرایط جبری برای وجود یک ریشه‌ی گویای مشترک از این دو خم بیضوی برقرار باشند، که در گزاره‌ی ۱.۲.۳ این شرایط آورده شده‌اند. سرانجام ارتباط بین اعداد همنهشت و سه‌تایی‌های فیثاغورث اولیه را مورد بررسی قرار داده و به شمارش و تولید اعداد دوقلو همنهشت از نقطه نظر گروهی پرداخته‌ایم.

فهرست مندرجات

فصل ۱

مفاهیم اولیه

در این فصل مقدماتی از مباحث جبری و نظریه‌ی خم‌های بیضوی را ارائه می‌کنیم. سعی کرده‌ایم که مطالب مختصر بوده و برای درک بهتر مطالب فصل‌های بعدی مفید باشند. بنابراین، تا حد امکان از ارائه‌ی اثبات‌ها خودداری کرده‌ایم.

۱.۱ مباحثی از جبر

تعریف ۱.۱.۱ فرض کنیم K یک میدان باشد. میدان L را توسیع[۱] میدان K می‌گوییم هرگاه $K \subseteq L$. به راحتی می‌توان دید که L یک K–فضای برداری است. بعد این فضای برداری را درجه‌ی توسیع[۲] نامیده و با نماد $[L : K]$ نشان می‌دهیم. توسیع L را یک توسیع متناهی روی K می‌گوییم هرگاه $[L : K] < \infty$.

تعریف ۲.۱.۱ فرض کنیم L یک توسیع از K بوده و $A = \{a_1, \cdots, a_n\} \subseteq L$. کوچک‌ترین میدان شامل K و A را توسیع تولید شده توسط A[۳] گفته و به صورت $K(A) = K(a_1, \cdots, a_n)$ نشان می‌دهیم.

---

[۱] extention
[۲] degree of extention
[۳] extention generated by A

تعریف ۳.۱.۱ فرض کنیم L یک توسیع از K بوده و $K[x]$ حلقه‌ی چندجمله‌ای‌ها با ضرایبی در K باشد. عنصر $a \in L$ را یک عنصر جبری[۴] روی K می‌گوییم هرگاه ریشه‌ی یک چندجمله‌ای ناصفری در $K[x]$ باشد.

تعریف ۴.۱.۱ فرض کنیم L یک توسیع میدان K باشد. L را بستار جبری K می‌نامیم اگر در شرایط زیر صدق کند:

(۱) میدان L روی K جبری باشد؛

(۲) میدان L بسته‌ی جبری[۵] باشد، یعنی هر چندجمله‌ای $f(x) \in L[x]$ روی L به عوامل خطی تجزیه شود.

تعریف ۵.۱.۱ میدان K را بسته‌ی جبری گوییم هرگاه تمامی چندجمله‌ای‌های غیر ثابت در $K[x]$ دارای ریشه‌هایی در $K[x]$ باشد. کوچکترین توسیع جبری میدان K را بستار جبری K می‌گوییم.

۲.۱ مباحثی از نظریه‌ی خم‌های بیضوی

فرم‌های نرمال خم‌بیضوی

در این فصل مقدمه‌ای از نظریه‌ی خم‌های بیضوی را بیان می‌کنیم. K را میدانی دلخواه با بستار جبری $\bar{K}$ در نظر می‌گیریم.

تعریف ۱.۲.۱ مجموعه‌ی تمامی n—تایی‌های واقع در $\bar{K}$ یعنی مجموعه‌ی

$$\mathbb{A}^n = \mathbb{A}^n(\bar{K}) = \{(x_1, \cdots, x_n) : x_i \in \bar{K}\},$$

را n—فضای آفین[۶] روی K می‌گوییم. همچنین مجموعه‌ی

$$\mathbb{A}^n(K) = \{(x_1, \cdots, x_n) : x_i \in K\},$$

[۴] algebraic element
[۵] algebraically closed
[۶] affine n-space

را نقاط K–گویای $\mathbb{A}^n$ می نامیم.

تعریف ۲.۲.۱ رابطه‌ی هم‌ارزی $\sim$ را روی $\mathbb{A}^{n+1}$[۱] به صورت زیر تعریف می‌کنیم:

$(x_0,\cdots,x_n) \sim (y_0,\cdots,y_n)$ اگر و تنها اگر یک $\lambda \in \bar{K}^*$ وجود داشته باشد به‌طوری که برای هر $0 \leq i \leq n$، $y_i = \lambda x_i$.

مجموعه‌ی $\{(\lambda x_0,\cdots,\lambda x_n) : \lambda \in \bar{K}^*\}$ را کلاس هم‌ارزی $(x_0,\cdots,x_n)$ نامیده و با $[x_0 : \cdots : x_n]$ نمایش می‌دهیم. حال n–فضای تصویری[۲] (روی K) را به صورت زیر تعریف می‌کنیم:

$$\mathbb{P}^n = \mathbb{P}^n(\bar{K}) = \{[x_0 : \cdots : x_n] \mid x_i \in \bar{K},\ \exists i : x_i \neq 0\}.$$

هرگاه $[x_0 : \cdots : x_n] \in \mathbb{P}^n$، آن‌گاه x_0، $\cdots$، x_n را مختصات همگن[۳] متناظر با $[x_0 : \cdots : x_n]$ می‌گوییم. همچنین مجموعه‌ی $\mathbb{P}^n(K) = \{[x_0 : \cdots : x_n] \mid \forall i\ ;\ \ x_i \in K\}$ را مجموعه نقاط K–گویای $\mathbb{P}^n$ می‌گوییم.

تعریف ۳.۲.۱ چندجمله‌ای $F \in \bar{K}[X] = [X_0,\cdots,X_n]$ را همگن از درجه‌ی d می‌گوییم هرگاه به ازای هر $\lambda \in \bar{K}$ داشته باشیم:

$$F(\lambda X_0,\cdots,\lambda X_n) = \lambda^d F(X_0,\cdots,X_n).$$

مثال ۴.۲.۱ چندجمله‌ای‌های $X^2Y + XY^2$، $X^3 + Y^3$، $2X^3 - 7XYZ + Y^3 \in \bar{Q}[X,Y,Z]$ همگن از درجه‌ی ۳ هستند.

تبصره ۵.۲.۱ چندجمله‌ای $f(X,Y) \in K[X,Y]$ از درجه‌ی d در صفحه‌ی آفین را می‌توان به صورت

$$F(X,Y,Z) = Z^d f(\frac{X}{Z},\frac{Y}{Z}) \in K[X,Y,Z]$$

[۷] projective n-space
[۸] homogenous coordinates

همگن کرد. این عمل را همگن‌سازی می نامیم. یک چندجمله‌ای همگن $F(X,Y,Z)$ را می‌توان با تعریف

$$f(X,Y) = F(X,Y,1) \in K[X,Y]$$

به یک چندجمله‌ای (نه لزوماً همگن) در صفحه‌ی آفین تبدیل کرد.

تعریف ۶.۲.۱ یک خم مسطح جبری تصویری[۹] روی K، مجموعه‌ی ریشه‌های چندجمله‌ای همگن غیر ثابت $F(X,Y,Z) \in K[X,Y,Z]$ در $\bar{K}$ است:

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

مجموعه نقاط $K-$گویای C را به صورت زیر تعریف می‌کنیم:

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

نقطه در بی‌نهایت این خم، نقطه‌ی $P = [x:y:z] \in C$ است که در آن $z = 0$.

تعریف ۷.۲.۱ یک خم مسطح جبری آفین[۱۰] روی K، مجموعه‌ی ریشه‌های چندجمله‌ای همگن غیر ثابت $f(X,Y) \in K[X,Y]$ در $\bar{K}$ است:

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

مجموعه‌ی نقاط $K-$گویای C را به صورت زیر تعریف می‌کنیم:

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

نقطه در بی‌نهایت این خم، $\mathcal{O} = (\infty, \infty)$ می‌باشد.

[۹] plane projective algebraic
[۱۰] plane affin algebraic

تعریف ۸.۲.۱ گونه‌ی[۱۱] یک خم مسطح هموار از درجه‌ی d (به بیان دقیق‌تر یک خم هموار که با یک معادله‌ی همگن از درجه‌ی d، $F(X,Y,Z) \in \bar{K}[X,Y,Z]$ داده شده باشد.) به صورت زیر تعریف می‌شود:

$$g = \frac{۱}{۲}(d-۲)(d-۱).$$

تعریف ۹.۲.۱ یک خم بیضوی[۱۲] زوج مرتب $(E,\mathcal{O})$ است که E یک منحنی هموار با گونه‌ی یک است و $\mathcal{O} \in E$. (اغلب فقط E را می‌نویسیم و از نوشتن $\mathcal{O}$ صرف‌نظر می‌کنیم.) می‌گوییم خم بیضوی E روی K تعریف شده است و می‌نویسیم E/K، هرگاه E به‌عنوان یک منحنی روی K تعریف شده باشد و $\mathcal{O} \in E(K)$.

تعریف ۱۰.۲.۱ فرض می‌کنیم K یک میدان بوده، $a_۱, a_۲, a_۳, a_۴, a_۶ \in \bar{K}$ و خم E توسط معادله‌ی درجه سوم

$$E : y^۲ + a_۱xy + a_۳y = x^۳ + a_۲x^۲ + a_۴x + a_۶, \qquad (۱)$$

تعریف شده باشد. خم E را به همراه نقطه در بینهایت $\mathcal{O} = (\infty,\infty)$ در نظر می‌گیریم. تغییر متغیرهای $x = X/Z$ و $y = Y/Z$ خم E را به فرم تصویری و همگن

$$C : Y^۲Z + a_۱XYZ + a_۳YZ^۲ = X^۳ + a_۲X^۲Z + a_۴XZ^۲ + a_۶Z^۳ \qquad (۲)$$

تبدیل می‌کند. نقطه‌ی $\mathcal{O} = (\infty,\infty)$ روی E با نقطه‌ی $[X : Y : ۰]$ روی رابطه‌ی همگن به‌دست آمده متناظر است. بنابراین با قرار دادن $Z = ۰$ در رابطه‌ی همگن نتیجه می‌شود $X^۳ = ۰$، پس $X = ۰$. چون $[۰ : ۰ : ۰] \notin \mathbb{P}^۲(\bar{K})$، در نتیجه $\mathcal{O} = [۰ : ۱ : ۰]$ تنها نقطه‌ی متناظر با نقطه‌ی $\mathcal{O} = (\infty,\infty)$ است. یعنی تنها نقطه در بی‌نهایت روی E نقطه‌ی $[۰ : ۱ : ۰] = \mathcal{O}$ می‌باشد. معمولاً

[۱۱] genuse
[۱۲] elliptic curve

به معادله‌ی خم جبری (تصویری) C و یا به طور معادل خم جبری (آفین) E، معادله‌ی تعمیم یافته‌ی وایرشتراس[۱۳] گفته می‌شود. اگر $a_i \in K$، می‌گوییم E روی K تعریف شده است. و با نماد E/K نشان می‌دهیم.

تعریف ۱۱.۲.۱ معادله‌ی به فرم نرمال وایرشتراس طولانی (وایرشتراس تعمیم یافته) با ضرایب $a_1, a_2, a_3, a_4, a_6 \in K$ را در نظر می‌گیریم. پروفسور جان تِیْت[۱۴] کمّیت‌های b_2، b_4، b_6، b_8، c_4، c_6، Δ، j و ω را برای خم E به صورت زیر محاسبه کرده است. (این کمّیت‌ها به مقادیر تِیْت معروف هستند. برای جزئیات بیشتر به[۱۵] مراجعه کنید.)

$$b_2 = a_1^2 + 4a_2 \qquad c_4 = b_2^2 - 24b_4$$

$$b_4 = a_1a_3 + 2a_4 \qquad c_6 = -b_2^3 + 36b_2b_4 - 216b_6$$

$$b_6 = a_3^2 + 4a_6 \qquad \Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

$$b_8 = b_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \qquad j = \frac{c_4^3}{\Delta}$$

$$\omega = \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y},$$

که در آن Δ، j و ω به ترتیب مبین میدان[۱۵]، $-j$ پایا[۱۶] و دیفرانسیل نرون[۱۷] خم جبری E نامیده می‌شوند. به راحتی می‌توان دید که این مقادیر در روابط زیر صدق می‌کنند:

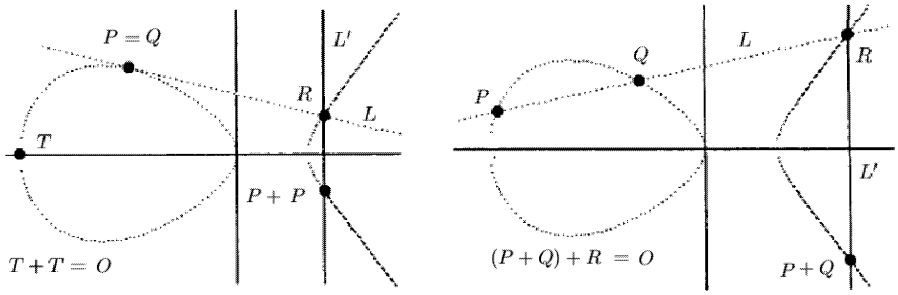
$$4b_8 = b_2b_6 - b_4^2,\ 1728\Delta = c_4^3 - c_6^2.$$

تعریف ۱۲.۲.۱ یک خم بیضوی روی K، زوج مرتب $(E, \mathcal{O})$ است که E یک خم با فرم نرمال وایرشتراس طولانی (وایرشتراس تعمیم یافته) با $\Delta \neq 0$ و $\mathcal{O}$ نقطه در بی‌نهایت می‌باشد.

[۱۳] generalized Weierstrass equation
[۱۴] John T.Tate
[۱۵] discriminant
[۱۶] j-invariant
[۱۷] neron differential

از ویژگی‌های خم‌های بیضوی این است که بر مجموعه‌ی نقاط این خم‌ها، عملی می‌توانیم تعریف کنیم که آن را تبدیل به یک گروه آبلی جمعی می‌کند. اساس تعریف این عمل بر خصوصیات هندسی خم استوار است.

تعریف **۱۳.۲.۱** (**قانون جمع هندسی**) فرض می‌کنیم E/K یک خم بیضوی روی K بوده و $P, Q \in E(K)$ دو نقطه (نه لزوماً متمایز) باشند. خط گذرا از P و Q را L می‌نامیم. $\mathcal{O}$ را نقطه در بی‌نهایت خم می‌گیریم به‌طوری که خطوط موازی با محور y ها همدیگر را در $\mathcal{O}$ قطع می‌کنند. به عبارت دیگر، هر خط گذرا از $\mathcal{O}$ موازی محور y ها است. این خط، خم بیضوی را در نقطه‌ی R قطع می‌کند. (ثابت می‌شود که این قطع کردن همواره اتفاق می‌افتد.) حال اگر خط گذرا از R و $\mathcal{O}$ را L' در نظر بگیریم، در این صورت $P + Q$ را نقطه‌ی تقاطع دیگر خط L' و خم بیضوی E تعریف می‌کنیم. (اگر $P = Q$، باید خط مماس در E در نقطه‌ی P رادر نظر بگیریم.)



شکل ۱.۱: قانون جمع هندسی

گزاره **۱۴.۲.۱** قانون جمع تعریف شده توسط تعریف قبل در خواص زیر صدق می‌کند:

(آ) اگر P، Q و R نقاط تقاطع (نه لزوماً متمایز) خط L و خم جبری E باشند آن‌گاه

$$(P + Q) + R = \mathcal{O}.$$

(ب) برای هر $P \in E$، $P + \mathcal{O} = P$؛

(پ) برای هر $P,Q \in E$، $P+Q=Q+P$؛

(ت) برای هر $P \in E$، یک نقطه‌ی $P' \in E$ وجود دارد که $P+P'=\mathcal{O}$. این نقطه را به صورت $-P$ نشان می‌دهیم؛

(ث) برای هر $P,Q,R \in E$، $(P+Q)+R=P+(Q+R)$؛

(ج) به ازای هر خم بیضوی E/K مجموعه‌ی

$$E(K)=\left\{(x,y)\in K\times K \mid y^{۲}+a_{۱}xy+a_{۳}y=x^{۳}+a_{۲}x^{۲}+a_{۴}x+a_{۶}\right\}\cup\{\mathcal{O}\}$$

یک زیرگروه از E می‌باشد. در نتیجه می توان گفت که این قانون جمع، مجموعه‌ی نقاط روی خم جبری E را به یک گروه آبلی تبدیل می کند و عنصر همانی این گروه، نقطه‌ی $\mathcal{O}$ می‌باشد.

اثبات: به [[۱۱]، فصل III، گزاره‌ی ۲.۲] مراجعه کنید. □

قضیه ۱۵.۲.۱ فرض کنیم E/K یک خم جبری تعریف شده توسط رابطه‌ی تعمیم یافته‌ی وایرشتراس بوده و نقاط $P_i=(x_i,y_i)$، $i=۰,۱,۲,۳$، روی E باشد.

(آ) $-P_۰=(x_۰,-y_۰-a_{۱}x_۰-a_{۳})$؛

(ب) اگر $x_۱=x_۲$ و $y_۱+y_۲+a_{۱}x_۲+a_{۳}=۰$ آن‌گاه $P_۱+P_۲=\mathcal{O}$؛

(پ) هرگاه $x_۱=x_۲$ ولی $y_۱+y_۲+a_{۱}x_۲+a_{۳}\neq ۰$، λ و ν را به صورت

$$\lambda=\frac{۳x_{۱}^{۲}+۲a_{۲}x_{۱}+a_{۴}-a_{۱}y_{۱}}{۲y_{۱}+a_{۱}x_{۱}+a_{۳}},\ \nu=\frac{-x_{۱}^{۳}+a_{۴}x_{۱}+۲a_{۶}-a_{۳}y_{۱}}{۲y_{۱}+a_{۱}x_{۱}+a_{۳}},$$

و هرگاه $x_۱\neq x_۲$ و $y_۱+y_۲+a_{۱}x_۲+a_{۳}\neq ۰$، λ و ν را به صورت زیر در نظر می گیریم:

$$\lambda=\frac{y_۲-y_۱}{x_۲-x_۱},\ \nu=\frac{y_۱x_۲-y_۲x_۱}{x_۲-x_۱}.$$

بنابر این، با فرض $P_۱ + P_۲ = P_۳ = (x_۳, y_۳)$ داریم:

$$x_۳ = \lambda^۲ + a_۱\lambda - a_۲ - x_۱ - x_۲,\ y_۳ = -(\lambda + a_۱)x_۳ - \nu - a_۳;$$

(ت) هرگاه $P = (x, y)$ روی E بوده و $۲P = (u, u')$ (که $۲P = P + P$) باشد آن‌گاه

$$u = \frac{x^۴ - b_۴x^۲ - ۲b_۶x - b_۸}{۴x_۳ + b_۲x^۲ + ۲b_۴x + b_۶}, u' = -(\lambda + a_۱)u - \nu - a_۳.$$

که λ و ν همانند قسمت (پ) معین می‌شوند.

اثبات: فرض می کنیم L خط گذرا از $P_۰$ و $\mathcal{O}$ باشد. در این صورت معادله‌ی L به صورت زیر خواهد بود:

$$x - x_۰ = ۰.$$

تابع $F(x, y)$ را به صورت زیر در نظر می‌گیریم:

$$F(x, y) = y^۲ + a_۱xy + a_۳y - x^۳ - a_۲x^۲ - a_۴x - a_۶.$$

با جایگذاری $x = x_۰$ و دسته‌بندی جملات نتیجه می‌شود:

$$F(x_۰, y) = y^۲ + (a_۱x_۰ + a_۳)y - ({x_۰}^۳ + a_۲{x_۰}^۲ + a_۴x_۰ + a_۶).$$

بنابراین $F(x_۰, y)$ یک چند جمله‌ای درجه دوم با متغیر y است. چون $F(x_۰, y_۰) = ۰$ پس $F(x_۰, y) = c(y - y_۰)(y - y'_۰)$. با مقایسه‌ی این دو رابطه نتیجه می‌شود $c = ۱$ و $y_۰ + y'_۰ = -(a_۱x_۰ + a_۳)$، در نتیجه $y'_۰ = -y_۰ - a_۱x_۰ - a_۳$. بنابراین قسمت (آ) اثبات می‌شود.

حال فرض می‌کنیم $P_۱ + P_۲ = P_۳ = (x_۳, y_۳)$ هرگاه $x_۱ = x_۲$ و $y_۱ + y_۲ + a_۱x_۰ + a_۳ = ۰$ آن‌گاه بنابر قسمت (آ)، $P_۱ + P_۲ = \mathcal{O}$، بنابراین قسمت (ب) نتیجه می‌شود. در غیر این صورت

$$L : y = \lambda x + \nu,$$

را خط گذرا از P_1 و P_2 (در صورتی که $P_1 = P_2$، خط مماس بر P_1) در نظر می‌گیریم. با قرار دادن $y = \lambda x + \nu$ و محاسبات ساده‌ای خواهیم داشت:

$$F(x, \lambda x + \nu) = -x^3 + (\lambda^2 + a_1\lambda - a_2)x^2 + (2\lambda\nu + a_1\nu + a_3\lambda - a_4)x + (a_3\nu - a_6).$$

حال چون P_1 و P_2 روی L قرار داشته و $F(P_1) = F(P_2) = 0$، بنابراین x_1 و x_2 ریشه‌های چندجمله‌ای درجه سوم زیر هستند:

$$x^3 - (\lambda^2 + a_1\lambda - a_2)x^2 - (2\lambda\nu + a_1\nu + a_3\lambda - a_4)x - (a_3\nu - a_6) = 0.$$

در نتیجه این چندجمله‌ای را می‌توان به صورت زیر تجزیه کرد:

$$0 = (x-x_1)(x-x_2)(x-x_3') = x^3 - (x_1+x_2+x_3')x^2 + (x_1x_2 + x_1x_3' + x_2x_3')x - x_1x_2x_3'$$

با مقایسه‌ی دو رابطه‌ی اخیر نتیجه می شود $x_1 + x_2 + x_3' = \lambda^2 + a_1\lambda - a_2$، بنابراین

$$x_3' = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2.$$

حال با جایگذاری این مقدار در معادله‌ی خط L نتیجه می‌شود $y_3' = \lambda x_3' + \nu$. با استفاده از قسمت (آ) و تعریف عمل جمع، قسمت (پ) قضیه نتیجه می‌شود یعنی

$$P_3 = (x_3', -(\lambda + a_1)x_3' - \nu - a_3).$$

اکنون باید نشان دهیم λ و ν موجود در معادله‌ی خط L برابر مقادیر ذکر شده در قضیه هستند. ابتدا فرض می‌کنیم $x_1 \neq x_2$ یعنی $P_1 \neq P_2$. در این صورت شیب خط L برابر با $m = (y_2 - y_1)/(x_2 - x_1)$ بوده و در نتیجه معادله‌ی آن به این ترتیب به‌دست می آید:

$$y = m(x - x_1) + y_1 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)x - \frac{y_2x_1 - y_1x_1}{x_2 - x_1} + y_1$$

$$= \left(\frac{y_2 - y_1}{x_2 - x_1}\right)x + \frac{y_1x_2 - y_2x_1}{x_2 - x_1}$$

بنابراین λ و ν مطلوب در این حالت به‌دست می‌آید. حال فرض می‌کنیم $x_۱ = x_۲$ ولی $y_۱ + y_۲ + a_۱x_۲ + a_۳ \neq ۰$، یعنی $P_۱ = P_۲ = (x_۱, y_۱)$. در این حالت خط L بر خم E در نقطه‌ی $(x_۱, y_۱)$ مماس شده و شیب آن با استفاده از مشتق‌های ضمنی تابع $F(x, y)$ در این نقطه به‌دست می‌آید:

$$m = \frac{۳x_۱^۲ + ۲a_۲x_۱ + a_۴ - a_۱y_۱}{۲y_۱ + a_۱x_۱ + a_۳}.$$

در نتیجه می‌توان معادله‌ی خط L را به صورت زیر نوشت:

$$y = \left(\frac{۳x_۱^۲ + ۲a_۲x_۱ + a_۴ - a_۱y_۱}{۲y_۱ + a_۱x_۱ + a_۳}\right)(x - x_۱) + y_۱$$

$$= \left(\frac{۳x_۱^۲ + ۲a_۲x_۱ + a_۴ - a_۱y_۱}{۲y_۱ + a_۱x_۱ + a_۳}\right)x - \frac{۳x_۱^۳ + ۲a_۲x_۱^۲ + a_۴x_۱ - a_۱y_۱x_۱}{۲y_۱ + a_۱x_۱ + a_۳} + y_۱$$

$$= \left(\frac{۳x_۱^۲ + ۲a_۲x_۱ + a_۴ - a_۱y_۱}{۲y_۱ + a_۱x_۱ + a_۳}\right)x + \frac{۲y_۱^۲ + a_۱x_۱y_۱ - ۳x_۱^۳ - ۲a_۲x_۱^۲ - a_۴x_۱}{۲y_۱ + a_۱x_۱ + a_۳}$$

$$= \left(\frac{۳x_۱^۲ + ۲a_۲x_۱ + a_۴ - a_۱y_۱}{۲y_۱ + a_۱x_۱ + a_۳}\right)x + \frac{-x_۱^۳ + a_۴x_۱ + ۲a_۶ - a_۳y_۱}{۲y_۱ + a_۱x_۱ + a_۳}.$$

در تساوی اخیر از رابطه‌ی زیر استفاده کردیم:

$$۰ = F(x_۱, y_۲) = y_۱^۲ + a_۱x_۱y_۱ + a_۳y_۱ - x_۱^۳ - a_۲x_۱^۲ - a_۴x_۱ - a_۶.$$

بنابراین، در این حالت نیز λ و ν مطلوب به‌دست می‌آید.

اثبات قسمت (ت) دقیقاً مشابه حالت اخیر می‌باشد، بنابراین از آن صرف‌نظر می‌کنیم. □

فصل ۲

اعداد همنهشت

۱.۲ خم‌های بیضوی روی $\mathbb{Q}$

در این بخش بعضی از قضایای اساسی نظریه‌ی خم‌های بیضوی تعریف شده روی میدان اعداد گویا از جمله قضیه‌ی موردل—ویل[۱] را بیان می‌کنیم.

قضیه ۱.۱.۲ **(موردل—ویل)** فرض کنیم E یک خم بیضوی روی میدان اعداد گویا باشد. در این صورت گروه $E(\mathbb{Q})$ یک گروه آبلی متناهی مولد است.

اثبات: به [[۱۷]، قضیه ۱۷.۸] مراجعه کنید. □

تبصره ۲.۱.۲ اگر از دید هندسی، به این قضیه نگاه کنیم می‌بینیم که یک مجموعه متناهی از نقاط روی خم موجودند به‌طوری که هر نقطه در روی خم با تعداد متناهی مرحله، از روی این نقاط با ترسیم خطوط مماس بر خم و خطوط گذرا از دو نقطه روی خم به‌دست می‌آیند.

تعریف ۳.۱.۲ بنابر قضیه‌ی موردل—ویل و قضیه‌ی اساسی گروه‌های آبلی متناهی مولد، به ازای یک عدد صحیح نامنفی r،

$$E(\mathbb{Q}) = T \oplus \mathbb{Z}^r.$$

[۱] Mordell-wiell

که گروه $T = E(\mathbb{Q})_{\text{tors}}$ یک زیرگروه متناهی از گروه $E(\mathbb{Q})$ بوده و شامل تمامی نقاط با مرتبه‌ی متناهی روی خم E است. این زیرگروه را زیرگروه تابی[۲] خم E (یا گروه $E(\mathbb{Q})$) می‌نامیم. عدد صحیح نا منفی r را رتبه‌ی $E(\mathbb{Q})$ نامیده و با rank_{E} نشان می‌دهیم.

تعیین رتبه‌ی $E(\mathbb{Q})$ برای یک خم بیضوی E روی میدان اعداد گویا مسئله‌ی مشکلی است. ولی روش‌های متنوعی برای پیدا کردن زیرگروه تابی وجود دارد. یکی از روش‌های محاسبه‌ی زیرگروه $T = E(\mathbb{Q})_{\text{tors}}$، استفاده از قضیه‌ی لوتز—ناقل[۳] می‌باشد.

۲.۲ محاسبه‌ی زیرگروه $E(\mathbb{Q})_{\text{tors}}$

در این قسمت ابتدا گزاره‌ای آورده و سپس قضیه‌ی لاتز- ناقل را به کمک آن بیان می‌کنیم. ابتدا ذکر این مطلب لازم است که این قضیه و قضیه مازور[۴] برای خم بیضوی تعریف شده روی $\mathbb{Q}$ مطرح شده و می‌توان به طور مشابه آن‌ها را برای میدان عددی K هم مطرح کرد. برای اطلاعات بیشتر در مورد این مطلب به فصل ٦ مرجع [۱۴] مراجعه شود.

تعریف ۱.۲.۲ فرض کنیم $\frac{a}{b}$ یک عدد گویای مخالف صفر باشد، به‌طوری که $(a, b) = ۱$. می‌نویسیم:

$$\frac{a}{b} = p^r \frac{a_۱}{b_۱} \quad (r \in \mathbb{Z}),$$

که $p \nmid a_۱ b_۱$. در این صورت ارزش p ای[۵] را به صورت $\nu_p(\frac{a}{b}) = r$ تعریف می‌کنیم.

به عنوان مثال،

$$\nu_۲\left(\frac{۷}{۴۰}\right) = -۳, \nu_۵\left(\frac{۵۰}{۳}\right) = ۲, \nu_۷\left(\frac{۱}{۲}\right) = ۰.$$

[۲] subgroup tortion
[۳] Lutz-Nugell
[۴] Mazur
[۵] P-adic valuation