وزارت علوم، تحقیقات و فناوری
دانشگاه تربیت معلم آذربایجان
دانشکده علوم پایه
گروه ریاضی

پایان نامه
جهت اخذ درجه کارشناسی ارشد
رشته ریاضی محض

عنوان:

خم‌های بیضوی رتبه بالا با گروه تاب $\mathbb{Z}/(۲\mathbb{Z})$

استاد راهنما:
دکتر فرضعلی ایزدی

استاد مشاور:
دکتر اسمعیل عابدی

پژوهشگر:
فاطمه مالکی

اسفند ماه / ۱۳۹۰
تبریز / ایران

بسم الله الرّحمن الرّحيم

تقدیم به

پدر و مادر بزرگوارم

و برادر عزیزم

سپاس گزاری...

سپاس خداوندی را که به من آموخت در لحظه‌های شادی شکرگزار باشم و فراموش نکنم، تمام داشته‌ها و دانسته‌هایم از لطف بی‌منت اوست و آموخت که در لحظه‌های اندوهم صبور باشم که همه‌ی غم‌ها رفتنی است و سربلند کسی است که مطیع تقدیر و حکمت الهی باشد.
اینک به پاس لطف الهی که پایان‌نامه‌ی حاضر، آماده شده است برخود واجب می‌دانم از حمایتهای بی‌دریغ، بذل توجه و مساعدت‌های استاد راهنمایم جناب آقای دکتر فرضعلی ایزدی سپاس‌گزاری نمایم.
از جناب آقای دکتر اسمعیل عابدی، که مشاوره و مطالعه این پایان‌نامه را به عهده گرفتند، کمال تشکر را دارم. و از آقای دکتر قربانعلی حقیقت دوست نیز سپاسگزارم که قبول زحمت فرموده و داوری این تحقیق را برعهده گرفتند.
از آقایان فواد خوشنام ، کامران نبردی و سایر دوستان به پاس کمک‌های بی دریغ‌شان تشکر ویژه دارم.
از مقدس‌ترین واژه‌های زندگیم، مادرم به پاس مهربانی اش، پدرم به پاس بردباری اش، آنانکه راستی قامتم در شکستگی قامتشان تجلی یافت، در برابر وجودشان زانوی ادب بر زمین می‌نهم و با دلی مملو از عشق و محبت و خضوع بر قلبشان بوسه می‌زنم.

فاطمه مالکی
اسفند ماه ۱۳۹۰

فهرست مطالب

چکیده

خم‌های بیضوی و رتبه آن‌ها نقش مهمی در سیستم‌های رمزنگاری ایفا می‌کنند. تعیین رتبه جزء مسائل پیچیده بوده و تاکنون هیچ الگوریتم کلی برای حل آن ارائه نشده است.
در این رساله ابتدا الگوریتم ساده‌ای برای محاسبه رتبه‌ی یک خم بیضوی ارائه می‌کنیم. سپس به توسعه الگوریتم برای محاسبه رتبه‌ی خم‌هایی به‌فرم $y^2 = x^3 - Bx$ می‌پردازیم. تمام این دسته از خم‌ها دارای گروه تاب $\mathbb{Z}/(2\mathbb{Z})$ و پایای مدولار $j = 1728$ می‌باشند. روش ارائه شده را برای جستجوی خم‌های رتبه بالا، از این خانواده از خم‌ها بکار می‌بریم و ۴ خم از رتبه ۱۳ و۲۲ خم با رتبه ۱۲ پیدا می‌کنیم.

کلمات کلیدی: خم بیضوی، رتبه، گروه تاب.

پیشگفتار

خم‌های بیضوی جزء شاخه بسیار مهم ریاضیات مدرن ویابطور دقیق تر نظریه اعداد و هندسه جبری بوده، در عین حال دارای تاریخچه بسیار طولانی هستند. بحث در مورد خم‌های بیضوی اولین بار توسط دیوفانتوس [۱] در قرن سوم میلادی به‌طور کاملا ابتدایی مطرح شد. او معادلاتی به‌صورت چند جمله‌ای با ضرایب صحیح معرفی کرد که بعدها به معادلات دیوفانتی معروف شدند. نخستین مثال ارائه شده توسط او این بود که آیا عدد ۷ را می‌توان به‌صورت مجموع دو عدد گویای توان سوم نوشت یعنی $a^۳ + b^۳ = ۷$. دیوفانتوس از طریق آزمون و خطا توانست جواب سوالات خود را پیدا کند، اما بعدها توسط نیوتن [۲] ، لوکاس [۳] و سیلوستر [۴] نشان داده شد که تعبیر کاملا هندسی برای این مسائل وجود دارد.

گاو س [۵] به ارائه شاخه جدید نظریه اعداد با استفاده از معادلات دیوفانتی پرداخت. توسعه‌ی معادلات به توان‌های بزرگ‌تر به ارائه قضایای مهم نظریه اعداد تا سال ۱۹۲۰ منجر شد. در تمام این سال‌ها خم‌های بیضوی توسط نظریه اعداد پردازان ناشناخته مورد مطالعه قرار می‌گرفت.

اولین قانون کلی که در مورد خم‌های بیضوی مطرح شد این بود که نقاط گویای خم بیضوی یک گروه آبلی با مولدهای متناهی می‌باشد، که این قانون توسط پوانکاره [۶] در یکی از مقالاتش ارائه شد و توسط مردل [۷] اثبات شد. اندرو ویل [۸] یکی از بزرگ‌ترین ریاضی‌دانان قرن بیستم اثبات جدید و واضح‌تری برای قضیه مردل ارائه کرد.

---

[۱] Diophantus
[۲] Newton
[۳] Lucas
[۴] Sylvester
[۵] Gauss
[۶] Ppincare
[۷] Mordell
[۸] Andre Weil

در طول سال‌ها مسائل زیادی در این شاخه مطرح شد و از شاخه های مهم به‌حساب می‌آمد، اما به مرور زمان کمتر مورد توجه ریاضی دانان قرار گرفت. اما با توجه به کاربردهایی که برای آن پیدا شد دوباره در کانون توجهات قرار گرفت، چرا که این خم‌ها در تجزیه اعداد صحیح تعیین اعداد اول بکار برده می‌شوند و در اثبات آخرین قضیه فرما [۹] بسیار راه گشا بودند. در سال‌های اخیر در رمز گذاری سیستم‌های امنیتی و مخابراتی اهمیت فوق العاده‌ای یافتند. هرچه از خم‌هایی با رتبه بالاتر برای رمز گذاری استفاده شود، سیستم دارای امنیت بهتری است. بنابراین محاسبه رتبه حایز اهمیت می‌باشد. تلاش‌های زیادی از طرف متخصصین این رشته برای ارائه الگوریتم یا پیدا کردن خم با رتبه‌های بالا انجام پذیرفته اما متاسفانه تاکنون الگوریتم کلی برای محاسبه رتبه ارائه نشده و فقط روش‌هایی برای دسته‌ای از خم‌ها ارائه شده است و بزرگترین رتبه محاسبه شده عدد ۲۸ بوده که در سال ۲۰۰۶ میلادی توسط الکیز [۱۰] پیدا شده است. در این پایان نامه سعی شده به برخی از این روش‌ها اشاره شود.

این پایان نامه مشتمل بر سه فصل است. در فصل اول به تعاریف اولیه خم بیضوی و ارتباط آن با هندسه تصویری و جبر اشاره می‌شود و چند قضیه مهم مورد بررسی قرار می‌گیرد. در فصل دوم با ارائه یک هومومرفیسم به محاسبه رتبه با استفاده از آن می‌پردازیم و در طول این کار قضیه مردل ـ ویل ضعیف را نیز اثبات می‌کنیم. در فصل سوم با استفاده از قضیه تیت [۱۱] و محاسبه گروه ۲ ـ سلمر یک کران بالا و پایین برای رتبه خم های به فرم $y^۲ = x^۳ - Bx$ ارائه می‌کنیم، هم‌چنین الگوریتمی برای یافتن رتبه خم‌های مورد نظر ارائه می‌شود.

[۹] Fermat
[۱۰] Elkies
[۱۱] Tate

فصل ۱

تعاریف و مفاهیم اولیه

۱.۱ هندسه تصویری

تعریف ۱.۱.۱. فرض کنید $f \in \mathbb{Q}[X,Y]$ یک چند جمله ای از درجه سوم به‌فرم

$$f(x,y) = aX^3 + bX^2Y + cXY^2 + dY^3 + eX^2 + fXY + gY^2 + hX + iY + J,$$

باشد. زیر مجموعه C از $\mathbb{Q}^2$ را به‌عنوان مجموعه صفرهای f تعریف کرده و آن‌را یک خم درجه سوم گویای آفین می نامیم.

روی فضای آفین $\mathbb{A}_{\mathbb{R}}{}^3 \setminus \{(0,0,0)\}$ رابطه $\sim$را به این صورت تعریف می کنیم که $(a,b,c) \sim (a_1,b_1,c_1)$ اگر و تنها اگر $t \neq 0$ موجود باشد به‌طوری‌که

$$(a,b,c) = (ta_1, tb_1, tc_1).$$

به‌وضوح این رابطه یک رابطه هم ارزی است و کلاس‌های هم ارزی آن‌را با $[a : b : c]$ نمایش می‌دهیم.

تعریف ۲.۱.۱. مجموعه $\mathbb{P}^2_R = \mathbb{A}^3_R/\{(0,0,0)\}$ را صفحه تصویر ۲ـ بعدی می نامیم.
توجه کنیم که که می‌توانیم $\mathbb{R}$را با هر میدان دیگری جایگزین کنیم. بنابراین به همین طریق می‌توانیم صفحه تصویر مختلط یا گویا را تعریف کنیم.

تعریف ۳.۱.۱. مشابها برای هر میدان K ، $\mathbb{P}^n_K = \mathbb{A}^{n+1}_K/\{(0,0,0,...)\}$ را یک فضای تصویری n بعدی روی K می نامیم.
ملاحظه: فرض کنید L توسیعی از میدان K باشد. آن‌گاه نگاشت کانونی $\mathbb{P}^n_K \longrightarrow \mathbb{P}^n_L$ که $[x_0 : ... : x_n] \in \mathbb{P}^n_K$ را به $[x_0 : ... : x_n] \in \mathbb{P}^n_L$ می برد خوش تعریف و یک به یک است.

۱.۱.۱ تعاریف هم ارزی

$\mathbb{P}^n_R$ را می توان به‌عنوان مجموعه خطوط گذرنده از مبداء $\mathbb{A}^{n+1}_R$ در نظر گرفت. توجه کنید که $\mathbb{P}^0$ مجموعه خط های $\mathbb{A}^1$ است. اما $\mathbb{A}^1$ یک خط است و بنابراین $\mathbb{P}^0$ شامل یک نقطه تنها می‌باشد که آن‌را نقطه در بی‌نهایت $\mathbb{A}^0$ می‌گویند.
می‌توانیم $\mathbb{P}^{n+1}$ را به‌عنوان $\mathbb{A}^{n+1} \sqcup \mathbb{P}^n$ در نظر بگیریم.
تعریف می‌کنیم $U_0 = \{[x_0 : ... : x_{n+1}] : x_0 \neq 0\}$. چون $x_0 \neq 0$ پس می‌توانیم نگاشت

$$\phi : U_0 \longrightarrow \mathbb{A}^{n+1}$$

$$[x_0 : ... : x_{n+1}] \longrightarrow (\frac{x_1}{x_0}, ..., \frac{x_{n+1}}{x_0}),$$

را تعریف کنیم. هم‌چنین می‌توانیم نگاشت

$$\psi : \mathbb{A}^{n+1} \longrightarrow U_0$$

$$(x_1, ..., x_{n+1}) \longrightarrow [1 : x_1 : ... : x_{n+1}],$$

را بسازیم. به سادگی می‌توان دید که ϕ و ψ خوش تعریف و وارون همدیگرند.
اگر $V_0 = \mathbb{P}^{n+1} \setminus U_0$ با یک بررسی ساده می‌بینیم که تناظر

$$V_0 \longleftrightarrow \mathbb{P}^n$$

$$[0 : x_1 : ... : x_{n+1}] \longleftrightarrow [x_1 : ... : x_{n+1}].$$

خوش تعریف و یک به‌یک است.
برای $\mathbb{P}^0$ این ساختار به‌وضوح غیر ممکن است. پس $\mathbb{P}^0$ را با استفاده از مطالب قسمت اول می‌سازیم.

۲.۱.۱ هندسه صفحه تصویری

فرض کنید K یک میدان دلخواه باشد. در این بخش $\mathbb{A}^n = \mathbb{A}^n_K$ و $\mathbb{P}^n = \mathbb{P}^n_K$ را تعریف می‌کنیم.

تعریف ۴.۱.۱. فرض کنید $\Pi \subset \mathbb{A}^{n+1}$ یک ابر صفحه گذرنده از مبداء $\mathbb{A}^{n+1}$ باشد. تصویر$[\Pi]$ از $\Pi \setminus \{(0,...,0)\}$ در $\mathbb{P}^n$ را یک ابر صفحه از فضای تصویری می‌نامیم. اگر $n = 3$ باشد، $[\Pi]$ را یک خط در صفحه تصویری می‌گویند.
ملاحظه: فرض کنید $F \in K[X_0,...,X_n]$ یک چند جمله‌ای همگن از درجه m باشد. آن‌گاه به‌ازای هر $t \in K$ و $(x_0,...,x_n) \in \mathbb{A}^{n+1}_K$ داریم

$$F(t.x_0,...,t.x_n) = t^m F(x_0,...,x_n).$$

حال فرض کنید $[a_0 : .. : a_n] \in P^n_K$. پس به‌ازای هر $t \neq 0$:

$$F(a_0,...,a_n) = 0 \iff F(ta_0,...,ta_n) = 0.$$

تعریف ۵.۱.۱. تحت مفروضات ملاحظه قبلی،$[a_0 : ... : a_n] \in \mathbb{P}^n_k$ را صفرهای F می‌گویند، اگر $F(a_0,...,a_n) = 0$.

گزاره: فرض کنید H زیر مجموعه‌ای از $\mathbb{P}^n$ باشد. آن‌گاه H یک ابر صفحه است اگر وتنها اگر H مجموعه صفر چند جمله‌ای همگون از درجه ۱ در $K[X_0,...X_n]$ باشد.

برهان. اگر H یک ابر صفحه باشد پس یک ابر صفحه مانند Π از فضای $\mathbb{A}^{n+1}$ وجود دارد که H تصویر Π در $\mathbb{P}^n$ است. پس Π مجموعه صفر از چند جمله‌ای همگن از درجه ۱، F در $K[X_0,...,X_n]$ است. به‌وضوح می‌بینیم که H مجموعه صفر F در $\mathbb{P}^n$ است.
برعکس. اگر H مجموعه صفر در $\mathbb{P}^n$ از یک چند جمله‌ای همگن از درجه ۱ در $K[X_0,...,X_n]$ باشد وفرض کنید Π ابر صفحه ای در $\mathbb{A}^{n+1}$ تولید شده توسط F باشد. به آسانی می‌توان دید که تصویر Π در $\mathbb{P}^n$ همان H است. پس H یک ابر صفحه است. □

۲.۱ قانون گروه یک خم درجه سه

تعریف ۱.۲.۱. مجموعه صفرهای واقع در $\mathbb{P}^2_{\mathbb{Q}}$ از یک چند جمله‌ای همگن درجه ۳ در $\mathbb{Q}[X,Y,Z]$ را یک خم گویای درجه ۳ گویند.
مشابها می‌توان یک خم درجه سوم حقیقی یا مختلط را تعریف کرد.

یادآوری: فرض کنید $F \in \mathbb{Q}[X,Y,Z]$ چند جمله‌ای همگن از درجه ۳ باشد. فرض کنید $\mathbb{Q} \subset K \subset \mathbb{C}$ یک میدان توسیعی از $\mathbb{Q}$ باشد. ضرایب F گویا اند اما مختلط نیز می‌باشند. پس این سبب می‌شود که خم درجه سوم مختلط تعریف شده توسط F را در نظر بگیریم. هم‌چنین سبب می‌شود که خم درجه سوم $C(K)$ که مجموعه صفر F در $\mathbb{P}^2_K$ است را نیز در نظر بگیریم.

تعریف ۲.۲.۱. فرض کنید C خم درجه سوم

$$f(X,Y) = aX^3 + bX^2Y + cXY^2 + dY^3 + eX^2 + fXY + gY^2 + hX + iY + j,$$

را در نظر بگیریم و $f^*(X,Y,Z)$ را به صورت زیر تعریف کنیم:

$$aX^3 + bX^2Y + cXY^2 + dY^3 + eX^2Z + fXYZ + gY^2Z + hXZ^2 + iYZ^2 + jZ^3,$$

آن گاه f^* را چند جمله‌ای همگن شده f می‌نامیم. $\overline{C}$ را خم درجه سوم تصویری تعریف شده توسط f^* می‌نامیم. در هندسه جبری $\overline{C}$ را بستار تصویری C می‌گویند.

تعریف ۳.۲.۱. فرض کنید K یک میدان و $F \in K[X,Y,Z]$ یک چند جمله‌ای همگن از درجه ۳ و C خم درجه سوم منصوب به آن باشد.
اگر $P = [a:b:c]$ یک نقطه روی C ، یعنی $F(a,b,c) = 0$ که $(a,b,c) \in \mathbb{A}^3_K$ و $(a,b,c) \neq (0,0,0)$. خم C را در نقطه P نامنفرد گویند اگر

$$(\frac{\partial F}{\partial X}(P), \frac{\partial F}{\partial Y}(P), \frac{\partial F}{\partial Z}(P)) \neq (0,0,0).$$

اگر P نقطه‌ای نامنفرد برای C باشد آن‌گاه

$$\frac{\partial F}{\partial X}(P)X + \frac{\partial F}{\partial Y}(P)Y + \frac{\partial F}{\partial Z}(P)Z = 0,$$

خطی از $\mathbb{P}^{۲}_{K}$ است که آن‌را خط مماس بر C در نقطه P می‌نامیم و با نماد T_PC نمایش می‌دهیم. C را نا منفرد یا هموار می‌گوییم اگر در هر نقطه نامنفرد باشد.

قضیه ۱.۲.۱. (بزو)[۱] *فرض کنید $F_۱, F_۲ \in \mathbb{C}[X,Y,Z]$ متناظر با چند جمله‌ای های همگن از درجه m و n باشند. مجموعه صفرهای $F_۱, F_۲$ با خم‌های تصویری از درجه m و n متناظر هستند. اگر $F_۱$ و $F_۲$ عامل مشترک نداشته باشند، آن‌گاه $C_۱$ و $C_۲$ مولفه مشترک ندارند، پس $C_۱ \cap C_۲$ یک مجموعه با mn نقطه با احتساب مرتبه تکرار است.*

نتیجه: *دو خم درجه سوم مختلط با هیچ مولفه مشترک، هم‌دیگر را در ۹ نقطه (با احتساب مرتبه تکرار) قطع می‌کنند.*

قضیه ۲.۲.۱. (۹ نقطه) *فرض کنید $C_۱, C_۲$ دو خم درجه سوم باشند که مولفه مشترک ندارند. ۹ نقطه در اشتراک $C_۱, C_۲$ به‌نام‌های $A_۱ ... A_۹$ را در نظر بگیرید. فرض کنید C یک خم درجه سوم باشد که شامل $A_۱ ... A_۸$ می‌باشد. در این صورت $A_۹ \in C$.*
سه مطلب اخیر نتایج مهمی در هندسه جبری می‌باشند که اثباتشان فراتر از سطح این رساله می‌باشد.

تعریف ۴.۲.۱. فرض کنید C یک خم مختلط از درجه سه و نامنفرد باشد و P, Q دو نقطه از خم C باشند. اگر $P \neq Q$ آن‌گاه بنابر قضیه بزو، خط گذرنده از Q, P خم C را در سه نقطه (با احتساب مرتبه تکرار) قطع می‌کند. فرض کنید $P * Q$ نقطه سوم اشتراک خط PQ با خم C باشد. ممکن است این نقطه یکی از نقاط P یا Q باشد. اگر $P = Q$ آن‌گاه T_PC دوبار خم C را در P قطع می کند.
ملاحظه: " $*$ " یک عمل‌گر گروه روی C نیست. برای دیدن این مطلب ثابت می‌کنیم که این عمل‌گر عضو خنثی ندارد.
فرض کنید به‌ازای هر $P \in C$ داشته باشیم $P * \mathcal{O} = P$. پس خط $P\mathcal{O}$ خم C را دوبار در نقطه P به‌ازای همه‌ی Pهای متعلق به C قطع می‌کند. این بدین معنی است که $P\mathcal{O}$ مماس برC در

[۱] Bezaut

نقطه P به‌ازای هر $P \in C$ است. فرض کنید F چند جمله‌ای همگن از درجه سه باشد که C را تعریف می‌کند و فرض کنید $\mathcal{O} = [a : b : c]$.
ما داریم که $\mathcal{O} \in T_P C$ اگر و تنها اگر

$$\frac{\partial F}{\partial X}(P)a + \frac{\partial F}{\partial Y}(P)b + \frac{\partial F}{\partial Z}(P)c = ۰.$$

فرض کنید

$$G(X,Y,Z) = \frac{\partial F}{\partial X}(X,Y,Z)a + \frac{\partial F}{\partial Y}(X,Y,Z)b + \frac{\partial F}{\partial Z}(X,Y,Z)c = ۰.$$

G یک چند جمله‌ای از درجه ۲ است که یک مقطع مخروطی را در $\mathbb{P}^۲$ تعریف می‌کند. از قضیه بزو داریم که $gcd(G,F) \neq ۱$ یا ، اشتراک مجموعه صفرهای G و C یک مجموعه متناهی است، این مطلب متناقض با این است که به‌ازای هر $P \in C$ ، $\mathcal{O} \in T_P C$. و $gcd(G,F) \neq ۱$ متناقض با تحویل پذیری F است.

تعریف ۵.۲.۱. فرض کنید که C یک خم مختلط از درجه سه و نامنفرد باشد. یک نقطه ثابت مانند $\mathcal{O} \in C$ را در نظر بگیرید. برای هر $P, Q \in C$ دلخواه تعریف می‌کنیم

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

قضیه ۳.۲.۱. *تحت شرایط تعریف بالا ،* $(C, +)$ *یک گروه آبلی است.*

برهان. جابه‌جایی " $+$ " به‌سادگی از جابه‌جایی " $*$ " نتیجه می‌گردد.
فرض کنید $P \in C$ ، پس $P + \mathcal{O} = \mathcal{O} * (P * \mathcal{O})$. خط $P\mathcal{O}$ ، C را در نقاط $P, \mathcal{O}$ و $P * \mathcal{O}$ قطع می‌کند. این خط بدیهیا همان خط $\mathcal{O}(\mathcal{O} * P)$ است که خم C را در نقاط $P, \mathcal{O}, \mathcal{O} * P$ قطع می‌کند. بنابراین $\mathcal{O} * (\mathcal{O} * P) = P$. این ثابت می‌کند که $\mathcal{O}$ یک عضو خنثی برای " $+$ " روی C است.
حال فرض کنید $Q \in C, S = \mathcal{O} * \mathcal{O}$ و $Q' = Q * S$. پس

$$Q * Q' = S \quad , \quad Q + Q' = \mathcal{O} * S = \mathcal{O},$$

بنابراین Q' وارون Q است.
جذاب‌ترین بخش برهان، اثبات شرکت پذیری است. فرض کنید $P,Q,R \in C$. به‌منظور اثبات $P+(Q+R)=(P+Q)+R$ کافی است که ثابت کنیم

$$P*(Q+R)=(P+Q)*R.$$

فرض کنید S اشتراک خط‌های $(P,Q+R)$ و $(R,P+Q)$ باشد. باید ثابت کنیم $S \in C$.
C_1 را به‌عنوان اجتماع خط‌های $(P,Q,P*Q)$ ، $(Q*R,\mathcal{O},Q+R)$ و $(P+Q,S,R)$ و C_2 را به‌عنوان اجتماع خط‌های $(P,S,Q+R)$, $(\mathcal{O},P*Q,P+Q)$, $(Q,R,Q*R)$ تعریف کنید . پس C_1 و C_2 خم‌های درجه سوم‌اند و اشتراکشان ۹ نقطه‌ی ، $Q+R,P+Q,Q*R,\mathcal{O},P,Q,R,S$ و$P*Q$ است. خم درجه سوم C از نقاط $P*Q,Q*R,P+Q,Q+R,\mathcal{O},P,Q,R$ عبور می‌کند. پس از S نیز بنابه قضیه ۹ نقطه ، عبور می‌کند. □

لم ۱.۲.۱. *اگر C خم تعریف شده توسط چند جمله‌ای $F \in \mathbb{Q}[X,Y,Z]$ ، و دارای نقطه‌ای گویا مانند $\mathcal{O}$ باشد (به‌عبارت دیگر a,b,c در $\mathbb{Q}$ موجود باشد به‌طوری‌که $[a:b:c]=\mathcal{O}$) ، آن‌گاه "+" روی $C(\mathbb{Q})$ خوش تعریف است و $(C(\mathbb{Q}),+)$ یک گروه آبلی است.*

برهان. برای اثبات خوش تعریفی "+" کافی است ثابت کنیم که اگر $P,Q \in C(\mathbb{Q})$ آن‌گاه $P+Q \in C(\mathbb{Q})$. یا به‌عبارتی اگر $P,Q \in C(\mathbb{Q})$ آن‌گاه $P*Q \in C(\mathbb{Q})$.
اصولا این یک نتیجه از این حقیقت است که یک چند جمله‌ای درجه سوم یک متغیر با ضرایب گویا و دو ریشه گویا دارای ریشه‌ی سوم گویا است. □

۳.۱ فرم نرمال وایراشتراس

فرض کنید $F(X,Y)=Y^2-f(X)$ که

$$f(X)=X^3+aX^2+bX+c \ , \ a,b,c \in \mathbb{Q} \, ,$$

و C خم درجه سوم آفین مختلط مشخص شده توسط F باشد.

تعریف ۱.۳.۱. خم آفین گویای $C(\mathbb{Q})$ تعریف شده توسط $F(X,Y)$ را یک خم بیضوی به‌فرم وایراشتراس می‌نامیم.

نکته: فرم همگن (بستار تصویری $\overline{C}(\mathbb{Q})$) خم $C(\mathbb{Q})$ توسط چند جمله‌ای زیر به‌دست می‌آید:

$$F^*(X,Y,Z) = Y^۲Z - X^۳ - aX^۲Z - bXZ^۲ - cZ^۳.$$

قبلا ابر صفحه در بی‌نهایت $\mathbb{P}^n_K$ را برای هر میدان K با کار کردن روی اولین متغیر $X_۰$ تعریف کردیم. بنابراین واضح است که، وقتی با دیگر متغیرها کار می‌کنیم، تغییری حاصل نمی‌شود. به‌ویژه وقتی که در $\mathbb{P}^۲$ کار می‌کنیم، در واقع ما داریم با نقاط در بی‌نهایت کار می‌کنیم نسبت به آخرین متغیر Z .

نقاط در بی‌نهایت خم $\overline{C}$ از $F^*(X,Y,Z) = ۰$ حاصل می‌گردد. پس

$$F^*(X,Y,Z) = ۰ \iff Z = ۰ \iff X^۳ = ۰ \iff X = ۰.$$

این بدان معناست که تنها نقطه در بی‌نهایت از خم $\overline{C}$ برابر است با $\mathcal{O} = [۰ : ۱ : ۰]$ ، زیرا $[۰ : ۱ : ۰] = [۰ : Y : ۰]$ به‌ازای هر $Y \neq ۰$.
توجه کنیم که $\mathcal{O}$ هم‌چنین یک نقطه از $\overline{C}(\mathbb{Q})$ است.
$\mathcal{O}$ یک نقطه نامنفرد برای $\overline{C}$ است. این بدان خاطر است که $\frac{\partial F^*}{\partial Y}((۰,۱,۰)) = ۲ \neq ۰$.

تعریف ۱.۳.۲. نقطه $P(x,y)$ از خم C را نامنفرد می‌گوییم اگر

$$(\frac{\partial F}{\partial X}(P), \frac{\partial F}{\partial Y}(P)) \neq (۰,۰).$$

یک نقطه که نامنفرد نباشد، منفرد می‌گوییم. اگر $P(x,y)$ یک نقطه نامنفرد برای C باشد، آن‌گاه خط مماس بر C در P ، یعنی خط T_PC توسط معادله‌ی زیر به‌دست می‌آید:

$$\frac{\partial F}{\partial X}(P)(X-x) + \frac{\partial F}{\partial Y}(P)(Y-y) = ۰.$$

تعریف ۱.۳.۳. خم C را نامنفرد (هموار) گویند هرگاه هر $P \in C(\mathbb{Q})$ نامنفرد باشد.

۱.۳.۱ فرمول‌های صریح برای قانون گروه

فرض کنید

$$y^۲ = x^۳ + ax^۲ + bx + c$$

خم بیضوی به‌فرم وایراشترای باشد. با جای‌گذاری $x = \frac{X}{Z}$ ، $y = \frac{Y}{Z}$ فرم همگن آن به صورت زیر به‌دست می‌آید:

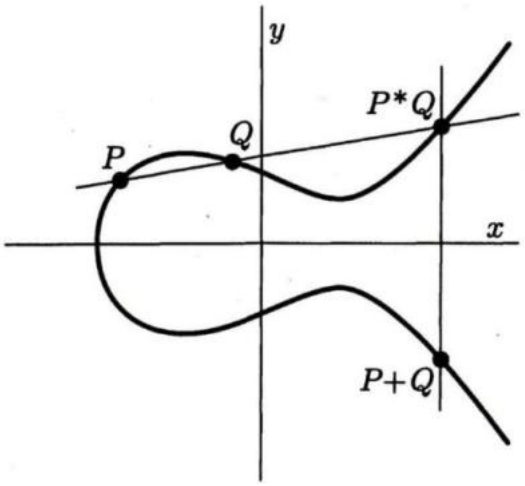
$$Y^۲Z = X^۳ + aX^۲Z + bXZ^۲ + cZ^۳.$$

توجه کنیم که در ادامه منظور از $x(P)$ و $y(P)$ مولفه‌های x و y از نقطه $P(x, y)$ اند.

حال نگاهی عمیق‌تر به ساختار گروه می‌اندازیم. چگونه دو نقطه P و Q روی خم درجه سوم به‌فرم وایراشتراس را جمع می‌کنیم؟

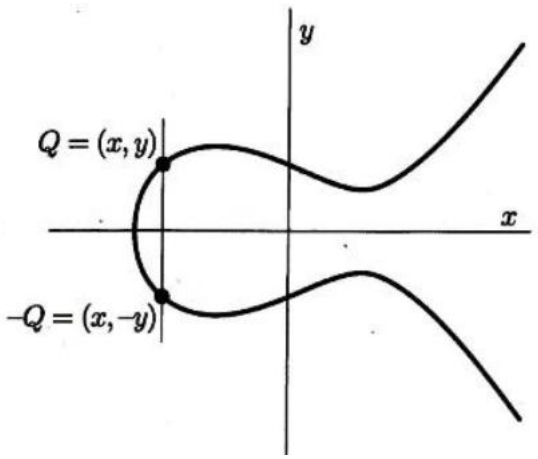
ابتدا خط گذرا از P و Q را رسم کرده و سومین نقطه تقاطع، $P * Q$ را پیدا می‌کنیم. سپس خط گذرا از $\mathcal{O}$ و $P * Q$ را رسم می‌کنیم که در واقع خط عمودی عبوری از $P * Q$ می‌باشد.
خم به‌فرم وایراشتراس نسبت به محور x ها متقارن می‌باشد. بنابراین برای محاسبه $P + Q$ کافی است $P * Q$ را پیدا کرده و سپس آن‌را نسبت به محور x ها قرینه کنیم. (شکل (۱.۱))

اگر $Q = (x, y)$ آن‌گاه $-Q = (x, -y)$. (شکل (۲.۱))
برای نشان دادن علت آن به روش ذیل عمل می‌کنیم:
فرض کنید که نقطه Q را با نقطه مورد ادعای $-Q$ جمع کنیم. در این صورت خط عبوری از Q و $-Q$ عمود خواهد بود، بنابراین سومین نقطه مشترک در روی خم $\mathcal{O}$ خواهد بود. حال $\mathcal{O}$ را



شکل (۱.۱): جمع نقاط روی فرم وایراشتراس

به $\mathcal{O}$ وصل کرده و سومین نقطه تقاطع را می‌یابیم. از وصل کردن $\mathcal{O}$ به $\mathcal{O}$ خطی در بی‌نهایت حاصل می‌شود که سومین نقطه نیز $\mathcal{O}$ است، چرا که خط در بی‌نهایت، خم را در $\mathcal{O}*\mathcal{O}*\mathcal{O}$ قطع می‌کند. این نشان می‌دهد که $Q+(-Q)=\mathcal{O}$. بنابراین $-Q$ همان قرینه Q است. واضح است که $-\mathcal{O}=\mathcal{O}$.



شکل (۲.۱): قرینه یک نقطه روی خم

حال به ارائه فرمول‌هایی برای محاسبه $P+Q$ می‌پردازیم.

$$P=(x_۱,y_۱) \quad , \quad Q=(x_۲,y_۲) \quad , \quad P*Q=(x_۳,y_۳) \quad , \quad P+Q=(x_۳,-y_۳).$$

• فرض کنید $x_۱ \neq x_۲$. آن‌گاه خط PQ خطی با معادله $y=\lambda x+\nu$ است که $\lambda=\dfrac{y_۱-y_۲}{x_۱-x_۲}$ و $\nu=y_۱-\lambda x_۱=y_۲-\lambda x_۲$. اشتراک PQ وخم C از قطع دادن دو معادله زیر به‌دست می‌آید:

$$\begin{cases} y^۲=x^۳+ax^۲+bx+c \\ \\ y=\lambda x+\nu \end{cases}$$

پس داریم:

$$۰=x^۳+(a-\lambda^۲)x^۲+(b-۲\lambda\nu)x+(c-\nu^۲).$$

می‌دانیم که P و Q جواب‌هایی برای معادله فوق می‌باشند، جواب سوم همان $P*Q$ است. از این‌که مجموع سه ریشه یک معادله درجه سوم برابر منفی ضریب جمله $x^۲$ از آن معادله می‌باشد، پس داریم:

$$x(P*Q)=\lambda^۲-a-x_۱-x_۲.$$

بنابراین با جایگذاری در معادله $y=\lambda x+\nu$ داریم

$$y(P*Q)=\lambda^۳-\lambda a-\lambda x_۱-\lambda x_۲+\nu.$$

در نتیجه برای جمع فرمول‌های ذیل را داریم:

$$\begin{cases} x_۳=x(P+Q)=\lambda^۲-a-x_۱-x_۲, \\ \\ -y_۳=y(P+Q)=-\lambda^۳+\lambda a+\lambda x_۱+\lambda x_۲-\nu=-\lambda x_۳-\nu. \end{cases}$$

• اگر $P=Q$. آن‌گاه معادله خط T_PC برابر است با

$$-f'(x_۱)(x-x_۱)+۲y_۱(y-y_۱)=۰.$$

◦ اگر $y_۱=۰$. آن‌گاه چون C هموار است پس $f'(x_۱)\neq ۰$ و T_PC موازی با $x=۰$ است. بنابراین

$$P*P=\mathcal{O} \implies P+P=\mathcal{O}.$$