ریاضی و جامعه
شاپا (چاپی): ۶۴۹۳-۲۳۴۵، شاپا(الکترونیکی): ۶۵۰۷-۲۳۴۵
جلد ۳، شماره ۲ (۱۳۹۷)، صص. ۳۵-۲۱

http://www.ui.ac.ir
http://math-sci.iranjournals.ir

سیری تاریخی در حوزه‌های اقلیدسی

امیر مافی* و سید شهاب ارکیان

چکیده. در این نوشتار تلاش شده است با بررسی تاریخچهٔ کارهای انجام شده در زمینهٔ حوزه‌های اقلیدسی و میدان‌های عددی اقلیدسی، ضمینهٔ آشنایی علاقه‌مندان با این مباحث ریاضی فراهم شود.

۱. مقدمه

اقلیدس (۳۰۰ ق.م)، ریاضیدان یونانی بود که به دلیل کارهایش در ریاضی و به‌ویژه هندسه، شهرت داشت. امروزه وی را پدر هندسهٔ اقلیدسی می‌نامند. کتاب اصول اقلیدس یکی از موفق‌ترین و پرکاربردترین مراجع و کتاب‌های درسی در زمینهٔ ریاضی، تا اوایل قرن بیستم بود. البته یکی دیگر از دلایل شهرت اقلیدس، لم او در تجزیهٔ یکتای یک عدد صحیح مثبت به عامل‌های اول و ارائهٔ الگوریتمی برای محاسبهٔ بزرگترین مقسوم‌علیه مشترک دو عدد است. مفهوم تقسیم اقلیدسی و الگوریتم اقلیدس یکی از قدیمی‌ترین الگوریتم‌های غیر بدیهی است که تا کنون مورد توجه و استفاده قرار گرفته است. البته مشخص نیست که آیا این الگوریتم قبل از او نیز وجود داشته، یا وی آن را کشف کرده است. در قرن نوزدهم، استفاده از این الگوریتم منجر به توسعهٔ دستگاه اعداد به اعداد صحیح گاوسی و اعداد صحیح آیزنشتاین شد. در سال ۱۸۱۵، کارل گاوس [۱] از الگوریتم اقلیدسی برای نشان دادن یکتایی تجزیهٔ اعداد گاوسی، استفاده کرد. پیتر دیریکله [۲] الگوریتم اقلیدس را به عنوان پایه‌ای برای نظریهٔ اعداد توصیف کرد. از نظر وی بسیاری از نتایج نظریهٔ اعداد را علاوه بر مجموعهٔ اعداد صحیح معمولی، می‌توان در مورد هر مجموعه‌ای از اعداد که الگوریتم اقلیدسی درست باشد، به‌کار برد. ددکیند [۳] از الگوریتم اقلیدس برای مطالعهٔ ماهیت اعداد صحیح جبری، استفاده کرد. او مفهوم دامنهٔ اقلیدسی را مطرح کرد. نه تنها در ریاضی، بلکه در سایر موضوعات و رشته‌های دیگر مرتبط با آن، الگوریتم اقلیدسی دارای کاربردهای عملی و نظری گسترده‌ای است.

در سراسر این نوشتار، منظور از حلقه، حلقهٔ جابجایی و یکدار است. یادآوری می‌کنیم هر حلقهٔ جابجایی غیر صفر که در آن حاصل‌ضرب هر دو عنصر غیر صفر، صفر نباشد، حوزهٔ صحیح است. مثلاً حلقهٔ اعدادصحیح $\mathbb{Z}$ یک حوزهٔ

عبارات و کلمات کلیدی. حوزهٔ اقلیدسی، میدان عددی اقلیدسی، توسیع جبری میدان.
*نویسنده مسئول: امیر مافی
دبیرتخصصی رابط: جواد اسدالهی
تاریخ دریافت: ۱۳۹۶/۰۶/۲۶ تاریخ پذیرش: ۱۳۹۷/۰۳/۰۱
http://dx.doi.org/10.22108/msci.2018.106491.1248

[1]Carl Friedrich Gauss [2]Johann Peter Gustav Lejeune Dirichlet [3]Richard Dedekind

صحیح است. یک *میدان* از یک مجموعهٔ عناصر با دو عمل تعریف شده بر روی آن، که آنها را جمع و ضرب می‌نامیم، و برخی خواص مشخص، تشکیل شده است. کوچکترین و مهم‌ترین میدان اعداد، $\mathbb{Q}$ میدان اعداد گویا است. بسیاری از خواص میدان‌های اعداد در حالت کلی، از روی خواص $\mathbb{Q}$ مدل‌سازی شده است. به عنوان مثال دیگر، می‌توان به $\mathbb{Q}(i) = \{a + bi | a, b \in \mathbb{Q}\}$، *میدان گاوسی اعداد گویا* اشاره کرد که در آن $i^2 = -1$. میدان گاوسی اعداد گویا، یک فضای برداری دو بعدی روی $\mathbb{Q}$ است. در حالت کلی، برای هر عدد خالی از مربع مانند d (d دارای یک مقسوم علیه مربع کامل نیست)، میدان درجهٔ دوم [۴] $\mathbb{Q}[\sqrt{d}]$ میدانی است که از الحاق ریشهٔ دوم d به مجموعهٔ اعداد گویا به دست می‌آید. اعمال حسابی در این میدان چنان تعریف می شود که در حالت خاص $d = -1$ میدان گاوسی اعداد گویا به‌دست آید.

پس از یک مقدمهٔ نه‌چندان کوتاه، در بخش دوم به معرفی حوزه‌های اقلیدسی پرداخته‌ایم. در آن قسمت، ضمن معرفی الگوریتم اقلیدسی، محکی برای وجود الگوریتم اقلیدسی در یک حوزهٔ صحیح دلخواه ارائه می‌کنیم. بخش سوم این نوشتار به یادآوری نکاتی از توسیع میدان می‌پردازد. یکی از مهم‌ترین قسمت‌های این نوشتار، میدان‌های عددی اقلیدسی است که در بخش چهارم مورد بحث قرار گرفته است. نهایتاً بخش آخر را به میدان‌های عددی از درجه‌های مختلف اختصاص داده‌ایم.

قضیهٔ آخر فرما. بعد از مرگ پی‌یر دو فرما [۵] ، ریاضیدان فرانسوی قرن ۱۷ میلادی، در حاشیهٔ یکی از کتاب‌ها مطلبی کشف شد، که در آینده به‌عنوان «قضیهٔ آخر فرما» مشهور شد. قضیهٔ آخر فرما یکی از مشهورترین قضایای تاریخ ریاضیات است. این قضیه می‌گوید: «معادلهٔ $x^n + y^n = z^n$ برای $n > 2$ جواب صحیح و غیر صفر ندارد». یعنی اعداد صحیح و غیر صفر x، y و z را نمی‌توان یافت که جواب‌های معادله فوق باشند. وی در حاشیهٔ آن کتاب نوشته بود که من یک برهان درست و قابل توجه برای این قضیه پیدا کرده‌ام که حاشیهٔ این صفحه برای جای گرفتن آن بسیار کوچک است. فرما در نوشته‌هایش ادعاهای گوناگونی در مورد مسائل متعددی کرده بود، که همهٔ حدس‌ها و نظریه‌های مطرح شدهٔ وی، غیر از این مسئله، تا سال ۱۸۴۷ حل شدند. در ۴ آگوست ۱۷۵۳ اویلر در نامه‌ای به گلدباخ، ادعا کرد که قضیهٔ فرما را در حالت $n = 3$ ثابت کرده‌است. البته اثبات وی اشتباه داشت. فرد دیگری که قدمی به جلو برداشت، یک ریاضیدان فرانسوی به نام ماری‌ـ‌سوفی ژرمن [۶] بود. او نشان داد که اگر n و $2n + 1$ اعداد اولی باشند، آنگاه ایجاب می‌کند که یکی از x، y یا z بر n بخشپذیر باشد. بنابراین قضیه آخر فرما به دو حالت زیر تفکیک می‌شود:

(۱) n هیچیک از اعداد x، y و z را نمی‌شمارد.

(۲) n یکی از اعداد x و y و z را می‌شمارد.

ژرمن حالت (۱) را برای هر $n < 100$ ثابت کرد و ریاضیدان فرانسوی دیگر، لژاندر [۷]، روش وی را به همهٔ اعداد کوچک‌تر از ۱۹۷ گسترش داد. حالت (۲) برای $n = 5$ به دو بخش تقسیم شد و بخشی را دیریکله در جولای ۱۸۲۵ و حالت دیگر را لژاندر در سپتامبر ۱۸۲۵ ثابت کرد. در سال ۱۸۳۲ دیریکله اثباتی از قضیه فرما را برای $n = 14$ منتشر کرد. حالت $n = 7$ در ۱۸۳۹ توسط گابریل لَمه [۸] ثابت شد. با وجود جوایزی که برای حل مسئلهٔ فرما تعیین شده بود، این قضیه، همچنان حل نشده باقی ماند و رکورددار بیشترین اثبات‌های غلط شد. به عنوان مثال بیش از ۱۰۰۰ اثبات غلط در بین سالهای ۱۹۰۸ تا ۱۹۱۲ منتشر گردید. سال‌ها گذشت و ریاضیدان‌ها، یکی پس از دیگری، یا اثباتی غلط ارائه می‌دادند، و یا قسمتی از مسئله را حل می‌کردند و کار را به نسل‌های بعدی می‌سپردند. یکی از این تلاش‌های ناموفق توسط لَمه انجام گرفت. همانگونه که در بخش ۱.۴ اشاره شده، اشکال کار وی این بود که قضیهٔ یکتایی تجزیه را در بارهٔ حلقه‌هایی به‌کار برده بود که این حکم در مورد آنها صحیح نیست. در ادامه، حلقه‌هایی به نام حوزه‌های اقلیدسی

[4]Quadratic Field [5]Pierre de Fermat [6]Marie-Sophie Germain [7]Adrien-Marie Legendre [8]Gabriel Lame

را معرفی خواهیم کرد که دارای ویژگی تجزیهٔ یکتا هستند. اندرو وایلز [۹] استاد دانشگاه پرینستون و دارای لقب سلطنتی سر بود. علت عمده شهرت وی اثبات قضیهٔ آخر فرما است که به خاطر آن برندهٔ جایزهٔ آبل سال ۲۰۱۶ شد. وی در سال ۱۹۹۳ با استفاده از نظریهٔ اعداد پیشرفته، اثباتی برای این قضیه ارائه کرد که این اثبات نیز دارای مشکلی بود ولی در سپتامبر ۱۹۹۴ اشکال این راه‌حل توسط خود وایلز و با همکاری یکی از دانشجویانش به نام «تیلر» برطرف شد. وایلز برای اثبات این قضیه جایزه ولف (۱۹۹۶-۱۹۹۵) را نیز دریافت کرد. همچنین، در سال ۱۹۹۸، اتحادیه بین المللی ریاضیات در کنگره بین المللی ریاضیدانان برلین، علی‌رغم این‌که سن اندرو از چهل سال بیشتر بود و نمی‌توانست مدال فیلدز را دریافت نماید، با تقدیم یک مدال نقره‌ای از وی تقدیرکرد.

۲. حوزهٔ اقلیدسی

تعریف ۱.۲. *تابع f از $R\setminus\{0\}$ به مجموعهٔ خوش‌ترتیبی چون W (که غالباً $\mathbb{N}_0$، مجموعهٔ اعداد صحیح نامنفی است)، که در دو شرط زیر صدق کند، یک قدرمطلق (الگوریتم) اقلیدسی گوییم.*

(۱) *برای هر دو عنصر a,b از R که $b\neq 0$، عناصر q,r از R چنان موجود باشند که $a=bq+r$ و $r=0$ یا $f(r)<f(b)$.*

(۲) *برای هر دو عنصر a,b از R، که $b\neq 0$، $f(a)\leq f(ab)$.*

هر حوزهٔ صحیح که بتوان حداقل یک قدرمطلق اقلیدسی بر روی آن تعریف کرد، حوزهٔ اقلیدسی گوییم.

مثال ۲.۲. (۱) *در حلقهٔ گوسی $\mathbb{Z}[i]$ تابع نرم $f(a+bi)=|a+bi|^2=a^2+b^2$ یک قدرمطلق اقلیدسی است.*

(۲) *فرض کنید $F[x]$ حلقهٔ چندجمله‌ای روی میدان F باشد. تابع ϕ را که به هر چندجمله‌ای غیر صفر مانند $p(x)$، $deg p(x)+1$ و به چندجمله‌ای صفر، صفر را نسبت می‌دهد، یک قدرمطلق اقلیدسی است ($deg p(x)$، درجهٔ $p(x)$ است).*

وایردن در ([۳۲]، صفحهٔ ۵۶) و ساموئل و زاریسکی در ([۳۱]، صفحهٔ ۲۳) اصولی اساسی و معادل شرایط موجود در تعریف ۱.۲ ارائه کرده‌اند. جاکوبسون در ([۲۰]، صفحهٔ ۱۲۲) پیشنهاد می‌کند در تعریف ۱.۲ فرض کنیم $f\geq 1$، زیرا تابع $f'(=f-f(1_R)+1)$ ویژگی لازم را دارد. همچنین، وی شرط قوی‌تر « برای هر $b\in R\setminus\{0\}$، $f(ab)=f(a)f(b)$»، را جایگزین شرط « برای هر $b\in R\setminus\{0\}$، $f(a)\leq f(a)f(b)$» نموده است. البته در حالت $W=\mathbb{N}_0$، می‌توان شرط اخیر را با شرط « برد f زیر مجموعه‌ای کراندار (از پایین) است» جایگزین نمود. این امر دور از انتظار نبود، زیرا در برهان استاندارد (مانند ([۲۰]، صفحهٔ ۱۲۳-۱۲۱)) که اقلیدسی بودن، اصلی بودن و اصلی بودن تجزیهٔ یکتا را ایجاب می‌کند، فقط از الگوریتم تقسیم و گزارهٔ اخیر، استفاده شده است. بنابراین شرط $f(a)\leq f(a)f(b)$ نه تضمینی برای اقلیدسی بودن R است و نه در برهان مدرنِ تجزیهٔ یکتا مورد استفاده قرار گرفته است. این نکته را، راجرز در [۲۸] به صورت زیر بیان کرده است.

قضیه ۳.۲. *فرض کنید R یک حوزهٔ صحیح دارای الگوریتم تقسیم متناظر با تابع تعریف شده f با مقادیر صحیح روی $R\setminus\{0\}$ چنان باشد که برد f از پایین کراندار است. در اینصورت R یک حوزهٔ اقلیدسی است.*

ملاحظه ۴.۲. *توجه داشته باشید که قدرمطلق اقلیدسی f بخشی از ساختار حوزهٔ اقلیدسی R نیست. در حالت کلی هر حوزهٔ اقلیدسی، تعداد زیادی قدرمطلق اقلیدسی می‌پذیرد. مثلاً می‌توان با تعریف توابع $f(a)=|a|$ و $f(a)=[\log_2|a|]$،*

[9] Sir Andrew John Wiles

http://dx.doi.org/10.22108/msci.2018.106491.1248

($[x]$ جزء صحیح x است) روی $\mathbb{Z}$، نشان داد که $\mathbb{Z}$ یک حوزهٔ اقلیدسی است. پرسش دربارهٔ چگونگی ارتباط بین قدرمطلق‌های اقلیدسی مختلف روی یک حوزهٔ صحیح اولین بار توسط زاریسکی طرح شد.

۱.۲. سری مشتق و محک موتزکین. موتزکین در مقالهٔ اصلی خود [۲۷]، محکی به صورت زیر برای وجود قدرمطلق اقلیدسی در یک حوزهٔ صحیح بر حسب سری مشتق بیان کرده است. این محک یکی از مهم‌ترین احکام این موضوع است. فرض کنید R یک حوزهٔ صحیح باشد. زیرمجموعهٔ P از $R \setminus \{0\}$ یک ایده‌ال ضرب نامیده می‌شود هرگاه $P(R \setminus \{0\}) \subseteq P$. برای هر زیرمجموعهٔ S از R، مجموعهٔ B شامل همهٔ عناصر $b \in R$ که $a \in R$ چنان وجود داشته باشد که $a + bR \subseteq S$، یک مجموعهٔ مشتق کلی S و $B \cap S$ مجموعهٔ مشتق S نامیده، آن را با S' نشان می‌دهیم. توجه داریم که اگر S ایده‌ال ضرب باشد، S' نیز چنین است. همچنین اگر $S_1 \subseteq S$، آنگاه $S'_1 \subseteq S'$.

فرض کنید R یک حوزهٔ صحیح و f از $R\setminus\{0\}$ به مجموعهٔ اعداد صحیح نامنفی چنان تعریف شده باشد که برای هر $b \in R\setminus\{0\}$ ، اگر a، a را بشمارد آنگاه $f(b) \leq f(a)$ و اگر a، b را نشمارد $q, r \in R$ چنان موجود باشد که $a = bq + r$ و $f(r) \leq f(b)$. در اینصورت f یک قدرمطلق اقلیدسی است. برای $i = 0, 1, 2, \ldots$، قرار دهید $P_i = \{b | f(b) \geq i\}$. واضح است که برای هر i، P_i یک ایده‌ال ضرب است. فرض کنید $b \in P'$. دراینصورت برای $a \in R$، $a + bR \subseteq P_i$. از آنجا که $r = a - bq \neq 0$ و $f(r) < f(b)$، $f(r) \geq i$ و $f(b) \geq i + 1$. بنابراین $P'_i \subseteq P_{i+1}$. برعکس فرض کنید $R - \{0\} = P_0 \supseteq P_1 \supseteq \cdots$ دنباله‌ای ایده‌ال‌های ضرب باشد که $P_i \cap$ تهی بوده، $P'_i \subseteq P_{i+1}$. برای هر $b \in R\setminus\{0\}$، عدد صحیح نامنفی i چنان موجود است که $b \in P_i - P_{i+1}$. در اینصورت تابع f را در b به‌صورت $f(b) = i$ تعریف می‌کنیم. واضح است که f یک قدرمطلق اقلیدسی است. بنابراین یک تناظر یک‌به‌یک بین دنباله‌هایی به این صورت و قدرمطلق‌های اقلیدسی وجود دارد.

فرض کنید g یک قدرمطلق اقلیدسی دیگر با دنبالهٔ $\{\bar{P}_i\}_{i\geq 0}$ چنان باشد که برای هر $i \geq 0$، $P_i \subseteq \bar{P}_i$. در اینصورت قدرمطلق اقلیدسی f را سریعتر از g گوییم. اگر لااقل یک قدرمطلق اقلیدسی حاصل از دنبالهٔ $\{P_i\}_{i\geq 0}$ در R وجود داشته باشد، می‌توان یک قدرمطلق اقلیدسی سریعتر، توسط دنبالهٔ $P_0, P'_0, P''_0, \ldots$ تعریف نمود. لذا تهی بودن $\cap P_0^{(i)}$ محکی برای وجود قدرمطلق اقلیدسی در R است.

ملاحظه ۵.۲. *فرض کنید R یک حلقه و قدرمطلق اقلیدسی f روی آن تعریف شده باشد. در اینصورت $f(0)$ کوچکترین عنصر $f(R)$ است، یعنی برای هر $0 \neq r \in R$، $f(0) < f(r)$. همچنین عنصر $r \in R$ به این شرط که $f(r) - f(0)$ کوچکترین عنصر $f(R) - f(0)$ باشد، یکتاست.*

تعریف ۶.۲. *فرض کنید F یک میدان و W یک مجموعهٔ خوش‌ترتیب باشد. فرض کنید $\nu : F \to W$ یک تابع باشد. مجموعهٔ $R = \{a \in F | \nu(a) \geq 0\}$ یک زیر حلقهٔ موضعی از F با ایده‌ال ماکسیمال $\mathfrak{m} = \{a \in F | \nu(a) > 0\}$ است. در این صورت حلقهٔ R را یک حلقهٔ مقادیر ν روی F گوییم. همچنین اگر W و $\mathbb{Z}$ یکریخت باشند، ν را مقدار مجزا گوییم.*

نتیجه ۷.۲. *هر حلقهٔ یک مقدار مجزا مانند ν یک حلقهٔ اقلیدسی با قدرمطلق اقلیدسی $\varphi(x) = 1 + \nu(x)$، $(x \neq 0)$ است.*

ساموئل در [۳۰]، یک‌سری از ویژگی‌های حوزه‌های اقلیدسی را بررسی کرده است، که از آن جمله، می‌توان به احکام زیر اشاره کرد.

(۱) حاصل‌ضرب هر تعداد متناهی از حوزه‌های اقلیدسی، یک حوزهٔ اقلیدسی است. در حالت خاص، اگر R یک حوزهٔ اقلیدسی و n یک عدد صحیح مثبت باشد، R^n نیز حوزهٔ اقلیدسی است. به‌ویژه $\mathbb{Z}^n$ حوزهٔ اقلیدسی است.

(۲) اگر R یک حوزهٔ اقلیدسی و S یک زیرمجموعهٔ بستهٔ ضربی از R باشد، آنگاه $S^{-1}R$ یک حوزهٔ اقلیدسی است.

(۳) فرض کنید R یک حلقهٔ اقلیدسی و R' حلقهٔ سری‌های توانی به شکل $\Sigma_{n\geq n_0} a_n x^n$، $(a_n \in R)$ باشد. در اینصورت R' نیز اقلیدسی است.

(۴) فرض کنید R یک حوزهٔ ایده‌ال اصلی (PID) باشد (حوزهٔ صحیحی که هر ایده‌ال آن، توسط یک عنصر تولید شود). فرض کنید $M = \{(m_1), (m_2), \ldots, (m_n)\}$ مجموعهٔ ایده‌ال‌های ماکسیمال R باشد (R تعداد متناهی ایده‌ال ماکسیمال دارد). دراینصورت R یک حوزهٔ اقلیدسی با قدرمطلق اقلیدسی

$$f(x) = \begin{cases} 0 & x = 0 \\ 1 + \sum_{i=1}^{n} v_i(x) & 0 \neq x = m_1^{v_1(x)} m_2^{v_2(x)} \cdots m_n^{v_n(x)} \end{cases}$$

است.

(۵) هر حوزهٔ اقلیدسی، یک حوزهٔ ایده‌ال اصلی است. توجه داشته باشید که فرض حوزهٔ صحیح بودن حلقه در این گزاره، اساسی نیست. به‌عبارت دیگر، هر ایده‌ال از یک حلقهٔ اقلیدسی، اصلی است. چون بحث اصلی این نوشتار دربارهٔ حوزه‌های اقلیدسی است، آن را با این فرض بیان کرده‌ایم.

یکی از مهم‌ترین عوامل جلب توجه حوزه‌های اقلیدسی را می‌توان این ویژگی آنها دانست که در هر حوزهٔ اقلیدسی تعمیم قضیهٔ اساسی حساب درست است. یعنی، هر حوزهٔ اقلیدسی، یک حوزه تجزیهٔ یکتا (UFD) است. به‌ویژه، $\mathbb{Z}[i]$ یک حوزهٔ تجزیهٔ یکتا است. حلقه‌های چند جمله‌ای $\mathbb{Z}[x_1, \ldots, x_n]$ و $F[x_1, \ldots, x_n]$ نیز برای $n \geq 1$، حوزهٔ تجزیهٔ یکتا هستند. اما حلقه‌های $\mathbb{Z}[x_1, \ldots, x_n]$، برای $n \geq 1$، و $F[x_1, \ldots, x_n]$، برای $n \geq 2$ PID نیستند. بنابراین مثال‌هایی از حوزهٔ تجزیهٔ یکتا در دست است که PID نیستند.

ملاحظه ۸.۲. *توجه داشته باشید که مثال‌هایی از حلقه‌های PID وجود دارند که اقلیدسی نیستند. در بسیاری از مقالات و منابع علمی از حلقهٔ $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ به عنوان حلقهٔ PID و غیر اقلیدسی نام برده می‌شود. البته برهان PID بودن این حلقه، به مراتب دشوارتر از اثبات غیر اقلیدسی بودنش است. در برخی از این منابع، برهان آن را حذف کرده، یا به خواننده واگذار کرده‌اند. در [۳۴]، [۳۵] و اخیراً [۶] و [۳۶] تلاش‌هایی برای ساده‌سازی برهان آن صورت گرفته است. به‌ویژه، کامپولی در [۶]، یک بررسی مقایسه‌ای بین برهان‌های مختلف آن انجام داده است.*

۲.۲. حلقه‌های اقلیدسی با یکای یکتا. یک حلقه را با تولید متناهی گوییم هرگاه روی زیرحلقهٔ اولش، با تولید متناهی باشد. هینزر و رویتمن در [۱۹، قضیهٔ ۳–۵] نشان داده‌اند که هر حوزهٔ اقلیدسیِ با تولید متناهی که تنها یکای آن 1_R باشد، با میدان دو عضوی F_2، یا $F_2[x]$ یکریخت است. همچنین آنها مثال ۹.۲ به‌عنوان نمونه‌هایی از حوزهٔ ایده‌ال اصلیِ نااقلیدسی ارائه کرده‌اند که این حلقه‌ها با تولید متناهی بوده، تنها عنصر یکال آن، 1_R می‌باشد. به ویژه، هیچ یک از این مثال‌ها با F_2 یا $F_2[x]$ یکریخت نیستند.

مثال ۹.۲. *فرض کنید R حلقهٔ مختصات یک منحنی آفین از ردهٔ یک یا دو روی میدان F_2 باشد. دراینصورت R یک حوزهٔ ایده‌ال اصلیِ نااقلیدسی است که 1_R تنها یکای آن است* ([۱۹، مثال‌های ۳–۲ و ۲–۴] *را ببینید*).

در هر حوزه صحیح مانند R که 1_R تنها یکال آن باشد، $1_R = -1_R$. بنابراین R دارای مشخصه دو است و شامل میدانی با دو عنصر، F_2 ، به عنوان یک زیر حلقه خود است.

http://dx.doi.org/10.22108/msci.2018.106491.1248

۳.۲. حوزه‌های اقلیدسی که در آنها قدرمطلق تقسیم دارای خارج‌قسمت و باقیماندهٔ یکتاست. همانطور که پیشتر اشاره شد، حلقهٔ اعداد صحیح $\mathbb{Z}$ و حلقهٔ $F[x]$، چندجمله‌ای روی میدان F، دو مثال مشهور از حوزهٔ صحیح هستند که البته دارای خواص متفاوتی نیز می‌باشند. به‌عنوان مثال در $\mathbb{Z}$ خارج قسمت و باقیمانده الگوریتم تقسیم یکتا نیست (وقتی که آن را به مجموعهٔ اعداد صحیح مثبت محدود کنیم، یکتا می‌شود)، درحالیکه در $F[x]$ خارج قسمت و باقیماندهٔ الگوریتم تقسیم، یکتاست. جودیت در [۲۱] نشان داده است که هر حوزهٔ اقلیدسی که در آن خارج قسمت و باقیماندهٔ الگوریتم تقسیم یکتا باشد، با یک میدان یا حلقهٔ چندجمله‌ای روی یک میدان، یکریخت است. به عبارت دقیق‌تر،

قضیه ۱۰.۲. *فرض کنید R یک حوزهٔ اقلیدسی چنان باشد که در آن $1 \neq 0$. قرار دهید $F = U(R) \cup \{0\}$. در اینصورت $R = F$ یا $R \cong F[x]$.*

۳. توسیع میدان

فرض کنید E یک میدان باشد. زیرمیدان F از E تحت اعمال E بسته است. به‌عبارت دیگر F یک میدان با اعمالی است که از E به ارث می برد. E، میدان بزرگتر، را یک *توسیع میدان* F می‌گوییم. برای سهولت در این حالت می‌نویسیم E/F و می‌خوانیم E روی F. اگر E/F، می‌توان E را به‌عنوان یک فضای برداری روی میدان F درنظر گرفت. در این حالت چنانچه بعد فضای برداری E روی میدان F متناهی باشد، E را یک توسیع میدان از درجهٔ متناهی برای F می‌گوییم. در این حالت برای سهولت بعد فضای برداری E روی میدان F را درجهٔ آن گوییم. میدان عددی جبری (یا به‌اختصار *میدان عددی*) یک توسیع میدان از درجهٔ متناهیِ میدان اعداد گویا است. میدان اعداد حقیقی، $\mathbb{R}$، و میدان اعداد مختلط، $\mathbb{C}$، میدان‌های عددی نیستند. میدان‌های *دایره‌بر*، میدان‌های عددی حاصل از الحاق ریشهٔ اول یکال مختلط به $\mathbb{Q}$ هستند (تعریف ۴.۴ را ببینید).

فرض کنید E توسیع میدان F باشد. هر خودریختی E که روی F ثابت باشد، یک خود ریختی E/F گوییم. به‌عبارت دیگر هر خودریختی E/F، یک یکریختی مانند σ از E به E است که $\sigma(a) = a$، برای هر $a \in F$. مجموعهٔ همهٔ خودریختی‌های E/F با عمل ترکیب توابع تشکیل یک گروه می‌دهد که ما آن را با $\mathrm{Aut}(E/F)$ نشان می‌دهیم.

تعریف ۱.۳. *فرض کنید E توسیع میدان F باشد. دراینصورت اگر $|\mathrm{Aut}(E/F)| = [E : F]$، یعنی تعداد خودریختی‌های E/F، برابر با درجهٔ توسیع باشد، E را یک توسیع گالوا F گوییم. اگر E/F یک توسیع گالوا باشد، $\mathrm{Aut}(E/F)$ را گروه گالوا توسیع E روی F گفته، آن را با $\mathrm{Gal}(E/F)$ نشان می‌دهیم.*

۱.۳. توسیع جبری میدان. یک توسیع میدان E/F جبری است هرگاه هر عنصر α از میدان بزرگتر، E، ریشهٔ یک چندجمله‌ای مانند p با ضرایب $e_m, \ldots, e_0$ در F باشد، یعنی:

$$p(\alpha) = e_m\alpha^m + e_{m-1}\alpha^{m-1} + \cdots + e_1\alpha + e_0 = 0.$$

می‌دانیم که هر توسیع میدان از درجهٔ متناهی، جبری است. به‌ویژه هر عنصر از یک میدان عددی مانند F، ریشهٔ یک چندجمله‌ای با ضرایب گویا است. لذا عناصر F را *اعدادجبری* می‌نامیم. چندجمله‌ای p را که $p(\alpha) = 0, e_m \neq 0$ در نظر بگیرید. در صورت لزوم با تقسیم همهٔ ضرایب بر e_m، ضریب جملهٔ پیشرو آن، یک شود. این چندجمله‌ای را تکین گوییم. لذا در حالت کلی $p(\alpha) = 0$ دارای ضرایب گویا است. در صورتی‌که ضرایب آن صحیح باشد، α را یک *عدد صحیح جبری* گوییم. جمع و ضرب هر دو عدد صحیح جبری، یک عدد صحیح جبری است. درنتیجه، مجموعه همهٔ اعداد صحیح جبری در میدان F یک حلقهٔ مشمول در F است که آن را با $\mathcal{O}_F$ نشان می‌دهیم. هر عدد صحیح z ریشهٔ

معادلهٔ $p(t) = t - z$ است و بنابراین z یک عدد صحیح جبری است. همچنین نشان داده می‌شود که هر عدد گویای جبری، عددی صحیح است. بنابراین $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.

مثال ۲.۳. *فرض کنید d یک عدد صحیح خالی از مربع و $F = \mathbb{Q}(\sqrt{d})$ باشد. در اینصورت*

$$\mathcal{O}_F = \begin{cases} \mathbb{Z} \oplus \frac{۱+\sqrt{d}}{۲}\mathbb{Z} & d \equiv ۱ \pmod{۴} \\ \mathbb{Z} \oplus \sqrt{d}\mathbb{Z} & d \equiv ۲, ۳ \pmod{۴} \end{cases}$$

به‌عبارت دیگر، اگر

$$\alpha = \begin{cases} \frac{۱+\sqrt{d}}{۲} & d \equiv ۱ \pmod{۴} \\ \sqrt{d} & d \equiv ۲, ۳ \pmod{۴} \end{cases}$$

آنگاه

$$\mathcal{O}_F = \{n + m\alpha | \quad m, n \in \mathbb{Z}\}.$$

۴. میدان‌های عددی اقلیدسی

هر میدان را که حلقهٔ اعداد صحیح جبری آن اقلیدسی باشد، میدان اقلیدسی نامیده می‌شود. در ادامه، میدان‌های عددی را که اقلیدسی هستند، بررسی می‌کنیم. ۱۴ کوچکترین عددی مانند d است که اقلیدسی بودن $\mathbb{Q}(\sqrt{d})$ معلوم نبود. فرض کنید F یک توسیع متناهی $\mathbb{Q}$ باشد. $\mathrm{Hom}(F, \mathbb{C})$ را به‌صورت زیر تعریف می‌کنیم

$$\mathrm{Hom}(F, \mathbb{C}) = \{\sigma : F \to \mathbb{C} | \ \sigma \text{ همریختی میدان‌ها است}\}$$

فرض کنید $x \in F$. توابع رد [۱۰] و نرم [۱۱] را به ترتیب به صورت

$$\mathrm{Tr}_{F/\mathbb{Q}}(x) = \Sigma_{\sigma \in \mathrm{Hom}(F,\mathbb{C})}\sigma(x) \quad \text{و} \quad \mathrm{N}_{F/\mathbb{Q}}(x) = \Pi_{\sigma \in \mathrm{Hom}(F,\mathbb{C})}\sigma(x)$$

تعریف می‌کنیم. توجه داریم که برای توسیع گالوای $K/\mathbb{Q}$، $\mathrm{Hom}(F, \mathbb{C}) = \mathrm{Gal}(F/\mathbb{Q})$.

فرض کنید $n = [F : \mathbb{Q}]$ درجهٔ F، تعداد خودریختی‌های F مانند σ است که در گروه گالوا $\mathrm{Gal}(F/\mathbb{Q})$ اعداد گویا را ثابتی نگه می‌دارد. به‌ویژه، برای هر $q \in \mathbb{Q}$ را در نظر بگیریم، چون همهٔ خودریختی‌ها اعداد گویا را ثابت نگه می‌دارند، داریم $\mathrm{N}_{F/\mathbb{Q}}(\alpha) = q^n$.

تعمیم اویلر از قضیه کوچک فرما بیان می‌کند که اگر $n \in \mathbb{N}$ و $a \in \mathbb{Z}$ چنان باشند که $\gcd(a, n) = ۱$، آنگاه $a^{\varphi(n)} \equiv ۱ \pmod{n}$ که در آن $\varphi(n)$ تابع فیِ اویلر است که تعداد اعداد صحیح بین ۱ و n را که نسبت n اولند، می‌شمارد.

تعریف ۱.۴. *فرض کنید $n \in \mathbb{N}$ و $a \in \mathbb{Z}$ نسبت به‌هم اول باشند. مرتبهٔ a به هنگ n را با $e = \mathrm{ord}(a)$ نشان داده، آن را کوچکترین توان e که $a^e \equiv ۱ \pmod{n}$ تعریف می‌کنیم. همچنین اگر $\mathrm{ord}(a) = \varphi(n)$، a را یک ریشهٔ اولیه به هنگ n گوییم. اگر برای یک ریشهٔ اولیه به هنگ n مانند a و $b \in \mathbb{Z}$ داشته باشیم $b \equiv a^{\beta} \pmod{n}$، عدد صحیح β را شاخص b به هنگ n در پایهٔ a گوییم.*

[10] Trace [11] Norm

http://dx.doi.org/10.22108/msci.2018.106491.1248

میدان F را اقلیدسی گوییم هرگاه $\mathcal{O}_F$ حوزهٔ اقلیدسی باشد. سؤال اساسی این است که برای کدام میدان‌های F، تابع قدر مطلق نرم $\varphi(\alpha) = |N_{F/\mathbb{Q}}(\alpha)|$ یک قدرمطلق اقلیدسی برای $\mathcal{O}_F$ است؟ چنین میدان‌هایی را *نرم‌ـاقلیدسی* می‌نامیم. ساموئل نشان داد که برای $\mathcal{O}_F$ یک قدرمطلق اقلیدسی به مجموعهٔ خوش‌ترتیب W وجود دارد اگر و تنها اگر یک قدرمطلق اقلیدسی به $\mathbb{N}_\circ$ وجود داشته باشد [۳۰]. لذا ما تنها توابع اقلیدسی به $\mathbb{N}_\circ(=\mathbb{N}\cup\{\circ\})$ را بررسی می‌کنیم. به کمک تعریف و با استفاده از ضرب نرم، به‌سادگی می‌توان دید که هر حلقهٔ نرم‌ـاقلیدسی، یک حوزهٔ اقلیدسی است. اکنون سؤالی که ممکن است مطرح شود آن‌است آیا عکس این گزاره نیز درست است؟ پاسخ غیر واضح آن، منفی است. کلارک در [۹] نشان داده است که حلقهٔ صحیح‌های میدان عددی درجهٔ دوم $\mathbb{Q}(\sqrt{۶۹})$ اقلیدسی است، اما نرم‌ـاقلیدسی نیست. قضیهٔ ۲.۴ یک محک هندسی، برای نرم اقلیدسی بودن، در اختیار ما قرار می‌دهد.

قضیه ۲.۴. *فرض کنید F یک میدان و تابع N، قدر مطلق نرم باشد. در اینصورت $\mathcal{O}_F$ نرم اقلیدسی است اگر و تنها اگر برای هر $y\in F$ عنصری مانند $x\in\mathcal{O}_F$ چنان موجود باشد که $N(y-x)<۱$.*

ملاحظه ۳.۴. *برخلاف $\mathbb{Z}$ به‌عنوان حلقهٔ صحیح‌های $\mathbb{Q}$، الزاماً در حلقهٔ صحیح‌های هر توسیع سرهٔ $\mathbb{Q}$، نمی‌توان هر ایده‌ال را به حاصل‌ضرب ایده‌ال‌های اولش تجزیه کرد. به‌عنوان مثال، ایده‌ال (۶) از حلقهٔ $\mathcal{O}_{\mathbb{Q}(\sqrt{-۵})}$ را به دو صورت زیر به حاصل‌ضرب ایده‌ال‌های اول تجزیه کرد*

$$(۶)=(۲)(۳)=(۱+\sqrt{-۵})(۱-\sqrt{۵}).$$

۱.۴. ریشهٔ nـام اولیهٔ واحد و میدان دایره‌بُر. اولین‌بار، لَمه هنگامی که در تلاش برای اثبات قضیهٔ آخر فرما بود، ریشه‌های nـام اولیهٔ واحد را معرفی کرد.

تعریف ۴.۴. *فرض کنید $n\in\mathbb{N}$ و $\zeta_n=e^{۲\pi i/n}$. در اینصورت $\zeta_n^n=۱$ و $\zeta_n^k\neq ۱$ برای هر $۰<k<n$. یعنی $\zeta_n=\sqrt[n]{۱}$ ریشهٔ nـام اولیهٔ واحد است. حلقهٔ دایره‌بر $\mathbb{Z}[\zeta_n]$ را به‌صورت*

$$\mathbb{Z}[\zeta_n]=\{z|\quad z=a_\circ+a_۱\zeta_n+a_۲\zeta_n^۲+\cdots+a_{n-۱}\zeta_n^{n-۱}, a_i\in\mathbb{Z}\quad \forall i\}$$

تعریف کرده، $\mathbb{Q}(\zeta_n)$ را nـامین میدان دایره‌بُر می‌نامیم.

در اول مارس ۱۸۴۷، در نشست آکادمی علوم پاریس، گابریل لَمه ادعا کرد موفق به اثبات قضیهٔ آخر فرما شده است. وی در اثبات خود، تجزیهٔ یکتا را در مورد حلقه‌هایی که در آنها یکتایی تجزیه برقرار نیست، به‌کار برده بود. پس از این ادعا، لیویل [۱۲] که وی نیز در آن نشست حضور داشت، در درستی اثبات لَمه ابراز تردید کرد. لیویل پرسش خود را به این صورت مطرح کرد که «آیا برای هر n در $\mathbb{Z}[e^{۲\pi i/n}]$ یکتایی تجزیه برقرار است؟». لَمه تردید لیویل را با کسی مطرح نکرد اما چندین ماه وقت خود را صرف ارائهٔ پاسخ مثبت به پرسش لیویل نمودند. تنها دو هفته پس از سخنرانی لَمه، وانتزل [۱۳] به‌درستی مشاهده کرد برای آنکه نشان دهیم $\mathbb{Z}[e^{۲\pi i/n}]$ حوزهٔ تجزیهٔ یکتا است، کافی است ثابت کنیم نرم‌ـاقلیدسی است (زیرا هر حوزهٔ نرم‌ـاقلیدسی، یک حوزهٔ اقلیدسی است و همانگونه که پیشتر گفته شد، هر حوزهٔ اقلیدسی، یک حوزهٔ ایده‌ال اصلی و درنتیجه حوزهٔ تجزیهٔ یکتا است). حتی او تصور می‌کرد می‌تواند نشان دهد همهٔ این حلقه‌ها نرم‌ـاقلیدسی هستند. اما متأسفانه در اثبات او یک خطای آشکار وجود داشت. در همین حال، کوشی [۱۴] نیز مشغول به اثبات این گزاره برای موارد خاص بود و توانست آن را برای مقادیر $n=۳,۴,۵,۶,۷,۸,۹,۱۰,۱۲,۱۴,۱۵$ ثابت کند. اما در حقیقت، ریاضیدانی فرانسوی به نام کومر [۱۵]، قبل از سخنرانی لَمه، اثبات کرده بود که $\mathbb{Z}[e^{۲\pi i/۲۳}]$ حوزهٔ تجزیهٔ یکتا

[12] Liouville [13] Wantzel [14] Cauchy [15] Kummer

نیست. مشکل اساسی در این میان، فقدان اطلاعات کافی آنان از کار هم بود. لذا این تلاش لَمه نیز بی‌ثمر ماند. از آن پس سؤال‌هایی مانند « به‌ازای کدام یک از مقادیر n، $\mathbb{Z}[e^{۲\pi i/n}]$ حوزهٔ تجزیهٔ یکتا، حوزهٔ اقلیدسی یا نرم‌ـاقلیدسی است» مطرح و مورد توجه قرار گرفت. می‌دانیم براساس قضیه‌ای در [۲۶]، دقیقاً به‌ازای سی مقدار مختلف n ، که (به هنگ ۴) $n \not\equiv ۲$، $\mathbb{Z}[\zeta_n]$ حوزهٔ ایده‌ال اصلی است. این مقادیر عبارتند از ۱ ، ۳ ، ۵ ، ۷ ، ۸ ، ۹ ، ۱۱ ، ۱۲ ، ۱۳ ، ۱۵ ، ۱۶ ، ۱۷ ، ۱۹ ، ۲۰ ، ۲۱ ، ۲۴ ، ۲۵ ، ۲۷ ، ۲۸ ، ۳۲ ، ۳۳ ، ۳۵ ، ۳۶ ، ۴۰ ، ۴۴ ، ۴۵ ، ۴۸ ، ۶۰ ، ۸۴.

موتزکین در [۲۷] ثابت کرده است، حلقهٔ صحیح‌های $\mathbb{Q}(\sqrt{-d})$ یک حوزهٔ اقلیدسی است اگر و تنها اگر $d = ۱, ۲, ۳, ۷, ۱۱$. البته بی‌کر و استارک نیز ثابت کرده‌اند که این حلقه، حوزهٔ ایده‌ال اصلی است اگر و تنها اگر $d = ۱, ۲, ۳, ۷, ۱۱, ۱۹, ۴۳, ۶۷, ۱۶۳$، [۳]. یعنی مثال‌هایی از حوزهٔ اقلیدسی دردست است که حوزهٔ ایده‌ال اصلی نیستند.

یکی دیگر از گزاره‌های مهم در ارتباط با ساختار جبری میدان‌های دایره‌بر، گزاره‌ای است که براساس آن $\mathbb{Z}[\zeta_n]$، حلقه صحیح‌های جبری $\mathbb{Q}(\zeta_n)$ است [۲۹]. به‌بیان دیگر، اگر $F = \mathbb{Q}(\zeta_n)$، آنگاه $\mathcal{O}_F = \mathbb{Z}[\zeta_n]$.

۱.۱.۴. مینیمای اقلیدسی. فرض کنید R یک حوزهٔ اقلیدسی و f تابعی با مقادیر صحیح، تعریف شده روی R چنان باشد که $f(\alpha) = ۰$ اگر و تنها اگر $\alpha = ۰$. کمینه اقلیدسیِ [۱۶] R نسبت به f را با [۱۷] $M(R, f)$، نشان داده، به صورت زیر تعریف می‌کنیم

$$M(R, f) = \inf\{\kappa > ۰ | \forall \alpha, \beta \in R \setminus \{۰\} \exists \gamma \in R \text{ s.t. } f(\alpha - \beta\gamma) < \kappa . f(\beta)\}.$$

در حالتیکه F یک میدانِ نرم‌ـاقلیدسی باشد، کمینه اقلیدسیِ F نسبت به نرم را کمینه نرم‌ـاقلیدسی گفته آن را با $M(F)$ نشان می‌دهند. به‌وضوح می‌توان دید R به‌ترتیب، اقلیدسی (نااقلیدسی) است هرگاه $M(R, f) < ۱$ ($M(R, f) > ۱$). اگر $M(R, f) = ۱$، هر یک از دو حالت اقلیدسی یا نااقلیدسی ممکن است.

فرض کنید R یک حوزهٔ اقلیدسی باشد. تابع *حداقل اقلیدسی* [۱۸] روی R با $f_{\min}$ نشان داده، به صورت زیر تعریف می‌شود

$$f_{\min}(\alpha) = \min\{f(\alpha) | \quad f \text{یک تابع اقلیدسی روی } R \text{ است}\}$$

به‌سادگی می‌توان دید $f_{\min}$ یک تابع اقلیدسی روی R است.

عنصر u از حلقهٔ R را یکا گوییم هرگاه وارون ضربی داشته باشد. همچنین مجموعه عناصر یکای R را با $U(R)$ نشان می‌دهیم. برای یک حوزهٔ صحیح مانند R ، *مجموعه‌های موتزکین* [۱۹] E_k، $k < ۰$، به‌صورت $E_۰ = \{۰\}, E_۱ = U(R) \cup \{۰\}$ تعریف می‌شوند. درحالت کلی

$E_k = \{۰\} \cup \{\alpha \in R | \quad \alpha$ هر کلاس خارج‌قسمتی به هنگ $\beta \in E_{k-۱}$ شامل یک است $\}$ و $E_\infty = \bigcup_{k \geq ۰} E_k$.

به‌عنوان مثال مجموعه‌های موتزکینِ $R = \mathbb{Z}$، عبارتند از: $E_۰ = \{۰\}$، $E_۱ = \{۰, \pm ۱\}$، $E_۲ = \{۰, \pm ۱, \pm ۲, \pm ۳\}$، ...، $E_k = \{۰, \pm ۱, \ldots, \pm(۲^k - ۱)\}$. موتزکین در [۲۷] محکی را برای بررسی اقلیدسی بودن R از روی مجموعه‌های موتزکین بیان کرده‌است. براساس آن حوزهٔ صحیح R اقلیدسی است اگر و تنها اگر $E_\infty = R$. به‌علاوه اگر $E_\infty = R$، آنگاه $f_{\min}(\alpha) = \min\{k \in \mathbb{N} | \quad \alpha \in E_k\}$. در این حالت تابع $f_{\min}$ را با f_M نشان می‌دهند. گزارهٔ ۵.۴ ما را با نمونه‌هایی از توابع اقلیدسی مانند f آشنا می‌کند که $M(R, f) = ۱$:

گزاره ۵.۴. [۲۲]. *فرض کنید R یک حوزهٔ صحیح باشد. دراینصورت*

۱) $R = E_۱$ *اگر و تنها اگر R یک میدان باشد.*

[16] Euclidean Minimum [17] Euclidean Minimum [18] Minimal Euclidean [19] Motzkin Sets

http://dx.doi.org/10.22108/msci.2018.106491.1248

۲) *اگر R یک میدان نباشد، آنگاه برای هر $k \in \mathbb{N}$، $R \neq E_k$. همچنین اگر R اقلیدسی باشد، آنگاه $M(R, f_{\min}) = ۱$.*

فرض کنید F یک میدان عددی جبری با حلقهٔ صحیح‌های $\mathcal{O}_F$ باشد. برای هر $\xi \in F$، کمینهٔ اقلیدسی در ξ، $M(\xi)$ را به‌صورت $M(\xi) = \inf\{|N_{F/\mathbb{Q}}(\xi - \eta)| \quad | \quad \eta \in \mathcal{O}_F\}$ تعریف می‌کنیم. همچنین $M(F)$ را نیز به صورت $M(F) = \sup\{M(\xi)|\xi \in F\}$ تعریف می‌کنیم. واضح است که برای هر $\eta \in \mathcal{O}_F$، $M(\xi) = M(\xi - \eta)$، یعنی $M(\xi)$ فقط به ردهٔ ξ در $F/\mathcal{O}_F$ بستگی دارد. به‌علاوه قرار می‌دهیم $C_۱ = \{\xi \in F/\mathcal{O}_F | M(\xi) = M(F)\}$. دومین کمینهٔ اقلیدسی F را به‌صورت $M_۲(F) = \sup\{M(\xi)|\xi \in (F/\mathcal{O}_F)\backslash C_۱\}$. واضح است که $M_۲(F) \leq M(F) = M_۱(F)$. درصورتیکه این نامساوی اکید باشد، $M_۱(F)$ را تنها [۲۰] گوییم. مینیمای اقلیدسی [۲۱] $M_k(F)$، $k \geq ۲$ را می‌توان به طریق مشابه تعریف کرد. میدان‌های عددی با دنباله‌های نامتناهی و نزولی از مینیمای اقلیدسی، و همچنین میدان‌هایی که کمینهٔ اقلیدسی دوم آنها تنها نیست، شناسایی شده‌اند ([۵] را ببینید).

۲.۴. حوزهٔ ددکیند. هر میدان شامل مقسوم علیه صفر نیست، پس $\mathcal{O}_F$ یک حوزهٔ صحیح است. F، میدان کسرهای $\mathcal{O}_F$ است. علاوه بر این ویژگی $\mathcal{O}_F$ دو ویژگی مهم دیگر دارند: نخست، $\mathcal{O}_F$ یک حلقهٔ نوتری است (هر زنجیر صعودی از ایده‌ال‌های آن، ایستاست). دوم آنکه، هر ایده‌ال اول غیر صفر از $\mathcal{O}_F$ ماکسیمال است. هرحلقهٔ جابجایی با این سه

ویژگی، را به‌خاطر کارهای ریچارد ددکیند در این زمینه و به‌افتخار او *حلقهٔ ددکیند* (یا حوزهٔ ددکیند) می‌نامند. هر ایده‌ال از یک حلقهٔ ددکیند، و در حالت خاص هر ایده‌ال از حلقهٔ صحیح، را می‌توان به‌صورت یکتا به حاصل‌ضرب ایده‌ال‌های اول تجزیه کرد. به‌عنوان مثال ایده‌ال (۶) از حلقهٔ $\mathbb{Z}[\sqrt{-۵}]$ را می‌توان به صورت زیر به حاصل‌ضرب ایده‌ال‌های اول تجزیه کرد.

$$(۶) = (۲, ۱ + \sqrt{-۵})(۲, ۱ - \sqrt{-۵})(۳, ۱ + \sqrt{-۵})(۳, ۱ - \sqrt{-۵}).$$

۳.۴. حدس آرتین و میدان‌های نرم‌ـاقلیدسی. امیل آرتین [۲۲] (۱۹۶۲-۱۸۹۸) ریاضیدان ارمنی‌تبارِ اهل اتریش بود که در زمینهٔ جبر کار می‌کرد. وی حدس مشهور خود را دربارهٔ ریشه‌های اولیه در سال ۱۹۲۷ مطرح کرد. فرض کنید a عدد صحیح مخالف ± ۱ باشد که مربع کامل نیست. این حدس بیان می‌کند که a ریشهٔ اولیهٔ تعداد نامتناهی اول است

([۲] ببینید).

درسال ۱۹۸۴ گوپتا و مورتی اولین نتیجه‌ای را که اعتبار حدس آرتین را برای حداقل یک مقدار a بررسی می‌کرد، منتشر کردند [۱۴]. وینبرگر، تکنیک‌های ریشهٔ اولیهٔ هولی را روی مسئلهٔ قدرمطلق اقلیدس به‌کار برد و گزارهٔ ۶.۴ را ثابت کرد [۳۳].

گزاره ۶.۴. *فرض کنید F یک میدان عددی از ردهٔ عددی یک باشد. فرض کنید $\mathcal{O}_F$ دارای گروه یکاهای نامتناهی باشد. با فرضیات تعمیم ریمان (GRH)، $\mathcal{O}_F$ اقلیدسی است.*

[20] Isolated [21] Euclidean Minima [22] E. Artin

در سال ۱۹۸۰ لنسترا پیشنهاد کرد که تکنیک‌های ریشهٔ اولیهٔ گوپتا و مورتی مطرح شده در [۱۴]، مستقل از فرض (GRH)، روی مسئلهٔ اقلیدس بررسی شود [۲۵]. گوپتا، ر. مورتی و ک. مورتی توانستند اولین مثال از حلقه‌های $\mathcal{O}_S$ که اقلیدسی هستند، اما نرم‌ـاقلیدسی نیستند، بیابند. برای به‌دست آوردن نتایجی برای $\mathcal{O}_F$ باید چند سال دیگر صبر می‌کردیم.

دیوید کلارک، در رسالهٔ دکتری خود تحت راهنمایی رام مورتی، قدرمطلق اقلیدسی را برای توسیع‌های گالوا اعداد گویا مطالعه کرد [۱۰]. وی در این کار یک محک بسیار مهم ، برای بررسی اقلیدسی بودن یک میدان گالوای درجهٔ دوم کاملاً حقیقی داده شده، ارائه کرد. بر پایه تحقیق انجام شده توسط گوپتا، ر. مورتی و ک. مورتی در [۱۵]، کلارک و مورتی روشی برای نشان دادن تعداد میدان‌هایی که نسبت به توابع متمایز با نرم، اقلیدسی هستند، ابداع کردند [۱۱]. این روش بر روی توسیع‌های گالوای سراسر حقیقی از درجهٔ بیشتر از دو، با یک ویژگی اضافی اعمال می‌شود.

کلارک و مورتی اشاره می‌کنند که $\mathbb{Z}[\sqrt{۱۴}, \frac{۱}{p}]$ اقلیدسی است هرگاه $p = ۱۲۹۸۸۵۲۲۳۷$. درواقع با یک استدلال سرراست و ترکیب دو گزارهٔ آنها، می‌توان نشان داد برای هر p، $\mathbb{Z}[\sqrt{۱۴}, \frac{۱}{p}]$ اقلیدسی است [۱۶].

در سال ۲۰۰۰، هارپر در رساله دکترای خود ادعا کرد $\mathbb{Z}[\sqrt{۱۴}]$ اقلیدسی است، اما نرم‌ـاقلیدسی نیست [۱۷]. وی

با استفاده از آثار مهم محققان فوق‌الذکر دربارهٔ مسائل اقلیدسی، به‌ویژه نتایج کلارک و مورتی، و با روش غربال بزرگ در میدان عددی، نتیجه خود را اثبات کرد. روش غربال بزرگ، تکنیکی است که توسط آن، تعداد نسبتاً زیادی از رده‌های باقیماندهٔ مدول‌ها، به‌دلیل عدم اهمیت در موضوع مورد مطالعه، حذف می‌شوند. یک مثال ساده و خوب از این دست، غربال اراتستن است. حدود سه سال بعد از تنظیم پایان‌نامهٔ هارپر، دستنویس کار مشترکش با مورتی آماده نشر شد [۱۸]. درواقع این کار یک تعمیم کار قبلی هارپر به یک چارچوب بزرگتر که شامل توسیع‌های آبلی است. از این‌رو آنها تا حد زیادی از [۱۵] استفاده کردند. قضیهٔ ۷.۴ نتیجه اصلی آنها است:

قضیه ۷.۴. *فرض کنید F یک توسیع گالوا $\mathbb{Q}$ با رتبهٔ واحد بزرگتر از ۳ باشد. دراینصورت حلقهٔ صحیح‌های آن، $\mathcal{O}_F$ اقلیدسی است اگر و تنها اگر حوزهٔ ایده‌ال اصلی باشد.*

یکی دیگر از نتایج جالب هارپر در [۱۷] محک مناسبی برای بررسی حوزهٔ اقلیدسی بودن $\mathbb{Z}[\zeta(d)]$ است ($\zeta(d)$ تابع زِتا ریمان، یک تابع با مقادیر مختلط است و به صورت $\zeta(d) := \sum_{n=۱}^{\infty} \frac{۱}{n^d}$ تعریف می‌شود). براساس این گزاره، $\mathbb{Z}[\zeta(d)]$ حوزهٔ اقلیدسی است اگر و تنها اگر حوزه ایده‌ال اصلی باشد.

۴.۴. اقلیدسی $k-$مرحله‌ای. زنجیر تقسیم $k-$مرحله‌ای کوکی [۲۳] برای دو عنصر α, β از حوزهٔ صحیح R، توسط $۲k$ عنصر r_i, q_i از R، که i از ۱ تا k تغییر می‌کند، به صورت زیر تعریف می‌شود

$$\begin{aligned} \alpha &= \beta q_۱ + r_۱ & \alpha &= q_۱ + \frac{۱}{\beta/r_۱} \\ \beta &= r_۱ q_۲ + r_۲ & \beta/r_۱ &= q_۲ + \frac{۱}{r_۱/r_۲} \\ &\cdots & &\cdots \\ &\cdots & \Rightarrow &\cdots \\ &\cdots & &\cdots \\ r_{k-۲} &= r_{k-۱} r_k + q_k & r_{k-۲}/r_{k-۱} &= q_k + \frac{۱}{r_{k-۱}/r_k} \end{aligned}$$

[23] Cooki

http://dx.doi.org/10.22108/msci.2018.106491.1248

با ترکیب آنها با هم، می‌توان β/α را با کسر مسلسل زیر نشان داد

$$\frac{\beta}{\alpha} = q_1 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + \cdots + \cfrac{1}{q_k}}}}}.$$

برای سادگی در نوشتار، کسر مسلسل فوق را با $[q_1, q_2, \ldots, q_k]$ نشان می‌دهیم.

تعریف ۸.۴. *حوزهٔ صحیح R را نسبت به نرم داده شدهٔ N، اقلیدسی $k-$مرحله‌ای گوییم هرگاه برای هر $\alpha, \beta \in R$ که $\beta \neq 0$، برای یک عدد طبیعی n که $n < k$، یک زنجیر تقسیم $n-$مرحله‌ای با شروع از این دو عنصر داده شده، چنان موجود باشد که r_k، آخرین باقیماندهٔ آن، در نامساوی $N(r_k) < N(\beta)$ صدق کند.*

تعریف ۹.۴. *R را یک حوزهٔ اقلیدسی $\omega-$مرحله‌ای می‌نامیم هرگاه برای هر جفت عنصر $\alpha, \beta \in R$ که $\beta \neq 0$، عدد صحیح و مثبت k و یک زنجیر تقسیم $k-$مرحله‌ای با شروع از این دو عنصر داده شده، چنان موجود باشد که r_k، آخرین باقیماندهٔ آن، در نامساوی $N(r_k) < N(\beta)$ صدق کند.*

ملاحظه ۱۰.۴. (۱) *فرض کنید $m > k$. در اینصورت هر حوزهٔ اقلیدسی $k-$مرحله‌ای، $m-$مرحله‌ای است.*

(۲) *فرض کنید k یک عدد صحیح مثبت باشد. دراینصورت هر حوزهٔ اقلیدسی $k-$مرحله‌ای، حوزهٔ اقلیدسی $\omega-$مرحله‌ای است.*

(۳) *هر حوزهٔ اقلیدسی $1-$مرحله‌ای، یک حوزهٔ اقلیدسی در معنای معمول آن است.*

ملاحظه ۱۱.۴. *با نمادگذاری فوق، هر زنجیر تقسیم $k-$مرحله‌ای را به‌وسیلهٔ دنبالهٔ q_k ; $q_1; q_2; \ldots$ از خارج قسمت‌هایش تعیین کرد و برعکس هر دنباله مانند q_k ; $q_1; q_2; \ldots$ از عناصر R یک زنجیر تقسیم $k-$مرحله‌ای با شروع از دو عنصر α, β تعریف می‌کند. بنابراین*

$$[q_1] = q_1 = a_1/b_1 \quad \text{که در آن} \quad a_1 = q_1, b_1 = 1،$$
$$[q_1, q_2] = q_1 + \frac{1}{q_2} \quad \text{که در آن} \quad a_2 = q_1 q_2 + 1, b_2 = q_2 \text{ و}$$
$$[q_1; q_2; \ldots; q_k] = \frac{a_k}{b_k} \quad \text{که در آن} \quad a_k = q_k a_{k-1} + a_{k-2}; b_k = q_k b_{k-1} + b_{k-2}.$$

گزاره ۱۲.۴. *فرض کنید R یک حوزهٔ صحیح و $\alpha, \beta \in R$. دراینصورت یک زنجیر تقسیم $k-$مرحله‌ای با شروع از این دو عنصر، و آخرین باقیمانده r_k موجود است که $N(r_k) < N(\beta)$، اگر و تنها اگر یک کسر مسلسل مانند $\frac{a_k}{b_k}$ چنان موجود باشد که $N(\frac{\alpha}{\beta} - \frac{a_k}{b_k}) < N(\frac{1}{b_k})$.*

گزاره ۱۳.۴. *فرض می‌کنیم $F = \mathbb{Q}(\sqrt{n})$ یک میدان عددی و $\mathcal{O}_F$ حلقهٔ صحیح های آن باشد. دراینصورت $\mathcal{O}_F$ اقلیدسی $\omega-$مرحله‌ای است اگر و تنها اگر عدد صحیح و مثبت k چنان موجود باشد که $\mathcal{O}_F$ اقلیدسی $k-$مرحله‌ای باشد.*

۵. اقلیدسی از درجه‌های مختلف

۱.۵. میدان‌های عددی درجه دوم. فرض کنید m عددی صحیح و خالی از مربع باشد. بسته به این‌که m مثبت یا منفی باشد، میدان‌های عددی به فرم $F = \mathbb{Q}(\sqrt{m})$ را میدان‌های عددی درجه دوم حقیقی یا مختلط می‌نامیم.

الف) میدان‌های عددی درجه دوم مختلط. میدان F را یک میدان عددی درجهٔ دوم موهومی گوییم هرگاه عدد صحیح، مثبت و خالی از مربعِ m چنان موجود باشد که $F = \mathbb{Q}(\sqrt{-m})$. در این قسمت مقادیری را که میدان عددی درجهٔ دوم

موهومی نظیر آنها نرم‌ـ اقلیدسی است معرفی می‌کنیم. برای کسب اطلاعات بیشتر در این زمینه، خواننده را به [۷]و [۱۲] ارجاع می‌دهیم.

قضیه ۱.۵. *فرض کنید $F = \mathbb{Q}(\sqrt{-m})$ یک میدان عددی درجهٔ دوم موهومی باشد. دراینصورت $\mathcal{O}_F$ اقلیدسی است اگر و تنها اگر $m = ۱, ۲, ۳, ۷, ۱۱$، و حتی قوی‌تر، در این حالت‌ها $\mathcal{O}_F$ نسبت به نرم، اقلیدسی هستند.*

ب) میدان‌های عددی درجه دوم حقیقی. در قضیهٔ ۲.۵، مقادیری را که میدان عددی درجهٔ دوم حقیقی نظیر آنها نرم‌ـ اقلیدسی است، معرفی می‌کنیم.

قضیه ۲.۵. *فرض کنید m عددی صحیح، مثبت و خالی از مربع باشد که $m \leq ۲$. فرض کنید F میدان عددی درجهٔ دوم حقیقیِ $\mathbb{Q}(\sqrt{m})$ باشد. دراینصورت $\mathcal{O}_F$ نرم‌ـ اقلیدسی است اگر و تنهااگر m یکی از شانزده عدد*

$$۲, ۳, ۵, ۶, ۷, ۱۱, ۱۳, ۱۷, ۱۹, ۲۱, ۲۹, ۳۳, ۳۷, ۴۱, ۵۷, ۷۳$$

باشد.

۲.۵. میدان‌های عددی درجه سوم. میدان‌های عددی به فرم $\mathbb{Q}(\sqrt[۳]{m})$ را میدان‌های عددی درجهٔ سه می‌نامیم. داونپورت ثابت کرد که تعداد متناهی میدان عددی مختلط وجود دارد که نرم‌ـ اقلیدسی هستند [۱۲]. گزارهٔ ۳.۵ به بررسی میدان‌های عددی درجه سوم سره‌ای که نرم‌ـ اقلیدسی هستند می‌پردازد.

قضیه ۳.۵. *همهٔ میدان‌های عددی درجه سوم سره‌ای که نرم‌ـ اقلیدسی هستند عبارتند از $\mathbb{Q}(\sqrt[۳]{۲}), \mathbb{Q}(\sqrt[۳]{۳})$ و $\mathbb{Q}(\sqrt[۳]{۱۰})$،* [۸].

۳.۵. میدان‌های عددی مختلط کلی. در این قسمت میدان‌هایی به فرم

$$\mathbb{Q}(\sqrt{m}, \sqrt{n}) = \{\alpha | \alpha = r_۱ + r_۲\sqrt{m} + r_۳\sqrt{n} + r_۴\sqrt{mn}\}$$

را که نرم اقلیدسی هستند، معرفی می‌کنیم [۲۳].

قضیه ۴.۵. *فرض کنید m یک عدد صحیح منفی و n عددی صحیح و دلخواه باشد فرض کنید قدرمطلق m, n خالی از مربع باشد. دراینصورت دقیقاً ۱۳ میدان عددی نرم‌ـ اقلیدسی به فرم $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ وجود دارد. این میدان‌ها عبارتند از*

$$\begin{array}{llll} \mathbb{Q}(\sqrt{-۱}, \sqrt{۲}), & \mathbb{Q}(\sqrt{-۱}, \sqrt{۳}), & \mathbb{Q}(\sqrt{-۱}, \sqrt{۵}), & \mathbb{Q}(\sqrt{-۱}, \sqrt{۷}), \\ \mathbb{Q}(\sqrt{-۲}, \sqrt{-۳}), & \mathbb{Q}(\sqrt{-۲}, \sqrt{۵}), & \mathbb{Q}(\sqrt{-۳}, \sqrt{۲}), & \mathbb{Q}(\sqrt{-۳}, \sqrt{۵}), \\ \mathbb{Q}(\sqrt{-۳}, \sqrt{-۷}), & \mathbb{Q}(\sqrt{-۳}, \sqrt{-۱۱}), & \mathbb{Q}(\sqrt{-۳}, \sqrt{۱۷}), & \mathbb{Q}(\sqrt{-۳}, \sqrt{-۱۹}), \\ \mathbb{Q}(\sqrt{-۷}, \sqrt{۵}). & & & \end{array}$$

۴.۵. میدان‌های عددی درجه چهارم. فرض کنید عدد صحیح مثبت m چنان باشد که $\sqrt[۴]{m}$ عدد صحیح نیست. بحث را با بررسی میدان‌های عددی به فرم $\mathbb{Q}(\sqrt[۴]{m})$ به پایان می‌رسانیم.

قضیه ۵.۵. *دقیقاً ۴ میدان درجه دوم مختلط به فرم $\mathbb{Q}(\sqrt[۴]{m})$ وجود دارد که نرم‌ـ اقلیدسی هستند. این میدان‌ها عبارتند از $\mathbb{Q}(\sqrt[۴]{۳}), \mathbb{Q}(\sqrt[۴]{۷}), \mathbb{Q}(\sqrt[۴]{۱۲})$ و $\mathbb{Q}(\sqrt[۴]{۲})$.*

http://dx.doi.org/10.22108/msci.2018.106491.1248

مراجع

[1] R. Akhtar, *Cyclotomic Euclidean number fields*, Senior thesis, Harvard Univ., 1995.

[2] E. Artin, *Collected Papers*, Reading, MA: Addison-Wesley, 1965.

[3] M. Artin, *Algebra*, Prentice-Hall, 1991.

[4] M. F. Atiyah and I. G. MacDonald, *Introduction to Commutative Algebra*, Addison-Wesley, 1969.

[5] E. S. Barnes and H. P. F. Swinnerton-Dyer, The inhomogeneous minima of binary quadratic forms I, *Acta Math.*, **87** (1952) 259–323.

[6] O. A. Campoli, A principal ideal domain that is not a Euclidean domain, *American Mathematical Monthly*, **95** (1988) 868–871.

[7] J. P. Cerri, Inhomogeneous and Euclidean spectra of number fields with unit rank strictly greater than 1, *J. Reine Angew. Math.*, **592** (2006) 49–62.

[8] V. Cioffari, The Euclidean condition in pure cubic and complex quartic fields, *Math. Comp.*, **33** (1979) 389–398.

[9] D. CLARK, A Quadratic Field that is Euclidean but not Norm-euclidean, *Manuscripta Mathematica*, **83** (1994) 327–330.

[10] D. A. Clark, *The Euclidean algorithm for Galois extensions of the rational numbers*, Ph. D. thesis, McGill University, Montreal, 1992.

[11] D. A. Clark and M. R. Murty, The Euclidean algorithm in Galois extensions of $\mathbb{Q}$, *J. Reine Angew. Math.*, **459** (1995) 151–162.

[12] H. Davenport, Euclid's algorithm in cubic elds of negative discriminant, *Acta Math.*, **84** (1950) 159–179.

[13] M. A. Jodeit, Uniqueness in the division algorithm, *The American Mathematical Monthly*, **74** (1967) 835–836.

[14] R. Gupta and M. Murty, A remark on Artin's conjecture, *Invent.Math.*, **78** (1984) 127–130.

[15] R. Gupta, M. R. Murty and V. K. Murty, The Euclidean algorithm for S-integers, *Canad. Math. Soc. Conference Proc.*, **7** (1987) 189–201.

[16] M. Harper, A family of Euclidean rings containing $\mathbb{Z}[\sqrt{۱۴}]$, CMS talk, 1998.

[17] M. Harper, $\mathbb{Z}[\sqrt{۱۴}]$ is Euclidean, *Canad. J. Math.*, **56** (2004) 55–70.

[18] M. Harper and M. R. Murty, Euclidean rings of algebraic integers, *Canad. J. Math.*, **56** (2004) 71–76.

[19] W. Heinzer and M. Roitman, Principal ideal domains and Euclidean domains having 1 as the only unit, *Comm. Algebra*, **29** (2001) 5197–5208.

[20] N. Jacobson, *Lectures in Abstract Algebra I*, Van Nostrand, Princeton, N. J., 1951.

[21] M. A. Jodeit, Uniqueness in the Division Algorithm, *The American Mathematical Monthly*, **74** (1967) 835–836.

[22] F. Lemmermayer, The Euclidean algorithm in algebraic number fields, *Expo. Math.*, **13** (1995) 385–416.

[23] F. Lemmermayer, Euclids algorithm in quartic CM-fields, *ArXiv e-prints*, (2011).

[24] H.W. Lenstra, Euclidean number fields of large degree, *Inventiones math.*, **38**(1977) 237–254.

[25] H.W. Lenstra, Euclidean number fields 1, 2 and 3, *The Mathematical Intelligencer*, Springer-Verlag (1979), 1980, 1980 resp.) 6-15; 73–77; 99–103 resp.

[26] J. M. Masley and H. L. Montgomery, Cyclotomic fields with unique factorization, *J. Reine Angew. Math.*, **286/287**, (1976), 248–256.

[27] Th. Motzkin, The Euclidean algorithm, *Bull. Amer. Math. Soc.*, **55** (1949), 1142–1146.

[28] K. Rogers, The Axioms for Euclidean Domains, *The American Mathematical Monthly*, **78** (1971) no. 10, 1127–1128.

[29] P. Ribenboim, *Algebraic Numbers*, John Wiley and Sons, 1972.

[30] P. Samuel, About Euclidean rings, *J. Algebra* **19** (1971) 282–301.

[31] P. Samuel and 0. Zariski, *Commutative Algebra I*, Van Nostrand, Princeton, N. J., 1958.

[32] B. L. van and der Waerden, *Modern Algebra I*, Ungar, New York, 1949.

[33] P. J. Weinberger, On Euclidean rings of algebraic integers, *Proc. Symp. Pure Math.*, **24** (1973) 321–332.

[34] K.S. Williams, Note on non-Euclidean principal ideal domains, *Mathematics Magazine*,**48** (1975) no. 3, 176–177.

http://dx.doi.org/10.22108/msci.2018.106491.1248

[35] J.C. Wilson, A principal ideal ring that is not a Euclidean ring, *Mathematics Magazine*, **46** (1973) no. 1, 34–38.

[36] C. Wong, On a principal ideal domain that is not a Euclidean domain, *International Mathematical Forum*, **8**, 2013, no. 29, 1405–1412.

امیر مافی

سنندج، خیابان پاسداران، دانشگاه کردستان، گروه ریاضی

A_Mafi@ipm.ir

امیر مافی متولد دی‌ماه ۱۳۵۳ در شهر سردشت آذربایجان غربی است. وی در سال ۱۳۸۴ دکتری خود را در رشتهٔ ریاضی محض از دانشگاه خوارزمی تحت راهنمایی پروفسور ذاکری اخذ نمود. مافی در سال ۱۳۸۴ به‌عنوان استادیار گروه ریاضی دانشگاه اراک استخدام شد و تا سال ۱۳۸۷ در آن دانشگاه به‌کار خود ادامه داد و از آن پس به استخدام گروه ریاضی دانشگاه کردستان درآمد. اکنون وی دانشیار گروه ریاضی دانشگاه کردستان می‌باشد.

سید شهاب ارکیان

سنندج، میدان سهروردی، دانشگاه فرهنگیان استان کردستان، پردیس شهید مدرس)

Shahab_Arkian@yahoo.com

سید شهاب ارکیان متولد دی‌ماه ۱۳۵۴ در شهر بیجار است. وی کارشناسی خود رادر سال ۱۳۷۸ در دانشگاه کردستان، کارشناسی ارشد خود را در رشتهٔ ریاضی محض در سال ۱۳۸۰ تحت راهنمایی پروفسور ذاکری در دانشگاه خوارزمی و دکتری خود را در سال ۱۳۹۶ در دانشگاه کردستان تحت راهنمایی دکتر امیر مافی در رشته ریاضی محض، گرایش جبر جابجایی به پایان رساند. ارکیان در حال حاضر عضو هیئت علمی دانشگاه فرهنگیان استان کردستان است.

http://dx.doi.org/10.22108/msci.2018.106491.1248