گشت و گذاری در ریاضیات معاصر

● غلامرضا یاسی‌پور

قانون تقابل. بررسی این پرسش که به ازای کدام یک از پیمانه‌های p ، عدد مفروض a ماندهٔ درجهٔ دوم است، به کشف قانون مشهور تقابل درجهٔ دوم انجامید، که توسط اویلر بر مبنای اطلاعات عددی گسترده‌ای تنظیم شد.

فرض می‌کنیم p و q اعداد اوّل و فرد باشند. در صورتی که دست کم یکی از آنها به صورت $4k+1$ باشد، آن‌گاه هم‌نهشتیهای $x^2 \equiv p \pmod q$ و $y^2 \equiv q \pmod p$ هردو حل‌پذیر یا هردو حل‌ناپذیرند (به عبارت دیگر، p ماندهٔ به پیمانهٔ q است، اگر و تنها اگر q ماندهٔ به پیمانهٔ p باشد).

اما در صورتی که هم p و هم q به صورت $4k+3$ باشند، آن‌گاه تنها یکی از دو هم‌نهشتی حل‌پذیر است و دیگری حل‌ناپذیر.

اوّلین اثبات کامل این قانون، توسط گاوس، زمانی که هجده ساله بود، یافت شد. بعدها وی، شش اثبات دیگر از آنچه که *قضیهٔ اصلی* «Theorema fundamentale» نامید، به دست داد، و از آن زمان تاکنون، روی هم رفته، بیش از پنجاه اثبات مختلف برای این قضیه به دست آمده است.

اصول گوناگونی که برای یافتن قوانین تقابل مانده‌های توانی بالاتر به کار رفته و زحماتی که برای این کار کشیده شده، وسیله‌ای قدرتمند به نظریهٔ اعداد داده‌اند.

در حدود ده سال پیش از اثبات گاوس، اثباتی در مورد قانون تقابل درجهٔ دوم توسط **لژاندر** «LEGENDRE» (۱۷۵۲-۱۸۳۳) انتشار یافت ؛ اما این اثبات دارای رخنه بود. لژاندر نماد سودمند $(\frac{a}{p})$ (*نماد لژاندر* «Legendre symbol») را معرفی کرد، که بسته به این که a ماندهٔ به پیمانهٔ p یا ماندهٔ به پیمانهٔ p و یا بخشپذیر بر p باشد، دارای مقدار $+1$ ، -1 ، یا ۰ است. این نماد، بیان قانون مورد بحث را در یک فرمول ممکن می‌کند :

$$(\frac{p}{q}).(\frac{q}{p}) = (-1)^{\frac{p-1}{2}.\frac{q-1}{2}}$$

قضیه‌های زیر مکملهای قانون تقابل‌اند :

$$(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} \quad , \quad (\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$$

قضیهٔ اوّل مقرر می‌کند که هم‌نهشتی $x^2 \equiv -1 \pmod p$ زمانی حل‌پذیر است که p به صورت $4k+1$ باشد. در نتیجه، $\frac{(p-1)}{2}$ زوج است و زمانی حل‌ناپذیر است که p به صورت $4k+3$ باشد ؛ در نتیجه $\frac{(p-1)}{2}$ فرد است.

معادله‌های دیوفانتی. فرض می‌کنیم $f(x_1, x_2, \ldots, x_n)$ چندجمله‌ای با ضرایب صحیحی بر حسب x_1 ، x_2 ، ... ، x_n باشد.

معادلهٔ $f(x_1, x_2, \ldots, x_n) = b$ را در صورتی *دیوفانتی* «Diophantine» می‌نامیم که جواب صحیح آن را خواسته باشیم. این نوع معادله را به نام ریاضیدان یونانی **دیوفانت** اسکندرانی «DIOPHANTOS of Alexandria» نامگذاری کرده‌اند.

دستگاه معادله‌های دیوفانتی «Diophantine equations»

$$f_1 = b_1 \ , \ f_2 = b_2 \ , \ \ldots \ , \ f_k = b_k$$

هم‌ارز معادلهٔ منفرد

$$(f_1 - b_1)^2 + (f_2 - b_2)^2 + \ldots + (f_k - b_k)^2 = 0$$

است ؛ یعنی مجموعه‌های جواب واقع در $\mathbf{Z}$ دستگاه و معادلهٔ منفرد فوق یکسان‌اند.

معادلهٔ دیوفانتی

$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$ (a_1 ، a_2 ، ...، a_n ، b صحیح)

حل‌پذیر است ؛ اگر و تنها اگر b بر $(a_1, a_2, \ldots, a_n)$ ب.م.م. بخشپذیر باشد.

معادلهٔ مورد بحث اگر حل‌پذیر باشد، در این صورت، بی‌نهایت جواب nتایی دارد. در این مورد، بررسی حالت $n = 2$ آسان است.

اگر a_1 و a_2 متباین (نسبت به هم اوّل) و x'_1 ، x'_2 یکی از جوابهای $a_1x_1 + a_2x_2 = b$ باشد، آن‌گاه کل جوابها را می‌توان به صورت $x_1 = x'_1 + a_2t$ ، $x_2 = x'_2 - a_1t$ نمایش داد، که در آن t عددی صحیح است.

یک جفت جواب خصوصی را می‌توان از کسر تقریبی یکی مانده به آخر عبارت کسر مسلسل $\frac{a_1}{a_2}$ به دست آورد.

مثال: $43x_1 + 19x_2 = b$. کسرهای تقریبی ۴۳/۱۹ عبارت‌اند از ۷/۳، ۹/۴ و ۴۳/۱۹. کسر ۹/۴،

$x'_1 = 4b \quad , \quad x'_2 = -9b$

را به دست می‌دهد ؛ بنابراین جواب عمومی معادله را می‌توان به صورت زیر نوشت :

$x_1 = 4b + 19t \quad , \quad x_2 = -9b - 43t$

به‌ازای $n \geq 3$ روشهای کسر مسلسلی عمومی تری "general continued fraction methods" مطرح شده‌اند.

اگر دستگاهی خطی از m معادلهٔ مستقل

$$\sum_{j=1}^{n} a_{ij}x_j = b_i \quad , \quad i = 1, 2, \ldots, m$$

مفروض باشد و اگر $m > n$ ، در این صورت دستگاه مزبور، *فرامعین* «overdetermined» است و عموماً جواب ندارد.

اما اگر $m < n$ ، دستگاه *فرومعین* «underdetermined» است و عموماً بی‌نهایت جواب دارد. به طور دقیقتر، در حالت اخیر، دستگاه برحسب اعداد صحیح x_1 ، x_2 ، ...، x_n حل‌پذیر است ؛ اگر و تنها اگر بزرگترین مقسوم‌علیه مشترک دترمینانهای m ـ سطری «m ـ rowed determinants» ماتریس ضرایب (a_{ij}) برابر ب.م.م. دترمینانهای m ـ سطری ماتریس ضرایب فزوده‌ای باشد، که از (a_{ij}) با افزودن ستون b_i ایجاد می‌شود.

مسألهٔ حل عمومیترین معادلهٔ دیوفانتی درجهٔ دوم برحسب دو مجهول x_1 ، x_2 ،

$c_{11}x_1^2 + c_{12}x_1x_2 + c_{22}x_2^2 + c_{13}x_1 + c_{23}x_2 + c_{33} = 0$

با اعداد صحیح c_{ij} را می‌توان با تبدیل متغیرها به مسألهٔ همسان معادله‌ای به صورت خاص

$y_1^2 - Dy_2^2 = b$

با اعداد صحیح D و b تحویل کرد. در این مورد، دو حالت متمایز وجود دارند.

اگر $D < 0$ ، در این صورت یا جوابی موجود نیست یا بی‌نهایت جواب y_1 ، y_2 موجود می‌شوند.

اگر $D > 0$ ، آن‌گاه معادلهٔ موسوم به معادلهٔ پِل Pell's equation

$y_1^2 - Dy_2^2 = 1$

بجز جوابهای بدیهی $y_1 = \pm 1$ ، $y_2 = 0$ بی‌نهایت جواب دارد، که می‌توانند از جوابی مینیمال به دست آیند.

بسادگی ملاحظه می‌شود که معادلهٔ عمومی

$y_1^2 - Dy_2^2 = b$

در صورتی که b نامانده درجهٔ دوم به پیمانهٔ D باشد، اصلاً جواب ندارد.

مثالها:

۱. معادلهٔ $x_1^2 + x_1x_2 + x_2^2 = 19$ دقیقاً دارای ۱۲ جفت جواب زیر است :

$2,3;-2,-3;3,2;-3,-2;2,-5;$

$-2,5;5,-2;-5,2;3,-5;-3,5;5,-3;-5,3$

۲. $y_1^2 - 5y_2^2 = 1$. از جواب مینیمال $y'_1 = 9$ ، $y'_2 = 4$ و به‌ازای $n = 0, 1, 2, \ldots$ کل جوابها، یعنی :

$$y_1 = \pm\left[(9 + 4\sqrt{5})^n + (9 - 4\sqrt{5})^n\right]/2$$

$$y_2 = \pm\left[(9 + 4\sqrt{5})^n - (9 - 4\sqrt{5})^n\right]/(2\sqrt{5})$$

را به دست می‌آوریم.

مسألهٔ یافتن جمیع مثلثهای قائم‌الزاویه‌ای که در مورد آنها x و y، اضلاع زاویهٔ قائمه و وتر z مضارب صحیحی از طول واحد باشند، به معادلهٔ دیوفانتی $x^2 + y^2 = z^2$ منجر می‌شود. جوابهای



آن، یعنی *اعداد فیثاغورسی* «*Pythagorean numbers*» را می‌توان با فرمولهای

$$x = u^2 - v^2 \ , \ y = 2uv \ , \ z = u^2 + v^2$$

نمایش داد، که در آنها u و v اعداد صحیح دلخواه‌اند. کوچکترین این جوابها عبارت‌اند از :

$$3^2 + 4^2 = 5^2 \ , \ 5^2 + 12^2 = 13^2$$

در این موارد، تفاوت شگفت‌آوری بین حالتهای $n = 2$ و $n \geq 3$ موجود است. قضیهٔ تو «theorem of Thue» بر این است که معادلهٔ

$$a_1x^n + a_2x^{n-1}y + \ldots + a_ny^n = b \quad (n \geq 3 \ , \ a_1 \neq 0)$$

با اعداد صحیح a_1 ، a_2 ، ...، a_n تنها به تعداد متناهی جواب دارد ؛ مگر آن که بتوان سمت چپ آن را به عاملهای همگن از درجات پایین‌تری با ضرایب صحیح تجزیه کرد.

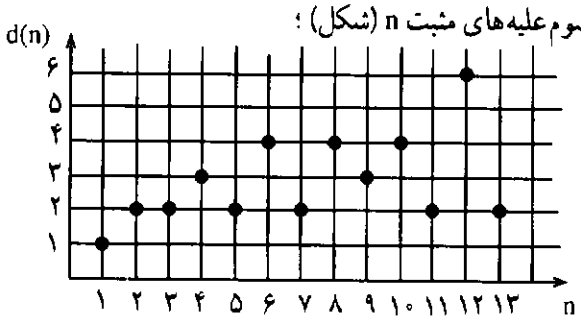
معادله‌های دیوفانتی از درجهٔ بالاتر، به مسائل عمیقی می‌انجامند که حلشان به معلوماتی از نظریهٔ میدانهای اعداد جبری نیازمند است.

در میان این معادله‌ها، *حدس فرما* «Fermat's conjecture» (نیز موسوم به آخرین قضیهٔ فرما) از توجه خاصی برخوردار بوده است : به ازای هر نمای صحیح $n > 2$ ، هیچ سه عدد صحیح ناصفر x ، y و z صادق در معادلهٔ $x^n + y^n = z^n$ وجود ندارد.

در مورد این قضیه، فرما (در حدود ۱۶۳۷) در حاشیهٔ کپی خودش از آثار دیوفانت نوشته است : «من در این مورد، اثباتی به واقع شگفت‌آور یافته‌ام ؛ اما این حاشیه، کوچکتر از آن است که دربرگیرندهٔ آن باشد.» اثبات فرما هیچ‌گاه به دست نیامد و به رغم کوششهای ریاضیدانهای مشهور، هیچ کس تاکنون موفق به اثبات یا عدم اثبات این حدس نشده است[1] ؛ اما نتایج جزئی جالبی دربارهٔ آن به دست آمده که از آن جمله است مورد زیر : معلوم شده که حدس مزبور به ازای جمیع نماهای تا ۱۲۵۰۰۰ صحیح است.

نظریهٔ اعداد تحلیلی. بجز تابع اویلر، یعنی $\varphi(n)$ توابع عدد ـ نظریه‌ای بسیار دیگری با مجموعهٔ اعداد طبیعی به عنوان حوزهٔ تعریف، مورد بررسی قرار گرفته‌اند.

مثالها عبارت‌اند از : $\pi(x)$، تعداد اولهای $\leq x$ ؛ $d(n)$، تعداد مقسوم‌علیه‌های مثبت n (شکل) ؛



تابع عدد نظریه‌ای $d(n)$: تعداد کل مقسوم علیه‌های مثبت n

$d(n)$ ، مجموع مقسوم‌علیه‌های مثبت n ؛ $r(n)$ ، تعداد جفتهای جواب صحیح x ، y معادلهٔ $x^2 + y^2 = n$.

بعضی از این توابع، رفتاری بسیار غیرعادی از خود نشان می‌دهند ؛ به عنوان مثال :

$$d(1) = 1 \ , \ d(2) = 2 \ , \ d(3) = 2 \ , \ d(4) = 3,$$

$$d(5) = 2 \ , \ d(6) = 4 \ , \ d(7) = 2 \ , \ d(8) = 4 \ , \ \ldots$$

با وجود این، اغلب می‌توان در مورد متوسط «average»، n مقدار اولیهٔ تابع f ، نظمی به دست آورد.

تابع

$$[f(1) + f(2) + \ldots + f(n)]/n$$

در بسیاری از حالتها، به ازای n صعودی، مانند یک تابع تحلیلی n، به‌طور مجانبی رفتار می‌کند. به عنوان مثال، $(1/n) \sum_{k \leq n} d(k)$ مانند لگاریتم طبیعی n نمو می‌کند. با قرار دادن :

$$[d(1) + d(2) + \ldots + d(n)]/n = \ln n + R(n)$$

درمی‌یابیم که اندازهٔ $R(n)$ نسبت به n از مرتبه‌ای کوچکتر از مورد $\ln n$ است.

بررسی متوسطهای توابع عدد ـ نظری و بالاتر از آن، باقیمانده‌های $R(n)$ آنها، به ظریفترین ابزارهای آنالیز نیازمند است. این شاخه از ریاضیات، یعنی نظریهٔ *اعداد تحلیلی* «*analytic* number theory» ذهن ریاضیدانان مشهوری را اشغال کرده که

۱ـ این حدس در دههٔ ۱۹۹۰ به اثبات رسیده است. توضیح مترجم

با اویلر در قرن هجدهم میلادی آغاز می‌شود و به‌طور مستقیم تا امروزه ادامه دارد. در این مورد، به تابع $\pi(x)$، یعنی تعداد اولهای تا (با) x، توجه خاصی معطوف شده است.

گاوس قانون مجانبی «asymptotic law» $\pi(x) \sim x/\mathrm{Ln}x$ را حدس زد، که درستی آن تا حدود ۱۹۰۰ که توسط **آدامار** «HADAMARD و **دولاواله ـ پواسن** «de la VALLEE - POUSSIN» به اثبات رسید، ثابت نشده بود.

بررسیهای اینان نشان داد که بهترین تقریب به $\pi(x)$ *انتگرال لگاریتمی* «*integral logarithm*» $\mathrm{li}(x) = \int_0^x \frac{dt}{\ln t}$ است و برآورد باقیماندهٔ $R(x) = \pi(x) - \mathrm{li}(x)$ به گونه‌ای تنگاتنگ با موضع صفرهای مختلط *تابع زتای ریمان* «Riemann zeta - function»، یعنی، $\zeta(s) = \sum(1/n^s)$ با $s = \sigma + it$ و $\sigma > 1$ مرتبط است.

در میان مسائل توزیعی «distribution problems» بسیار دیگر، قضیهٔ مشهور زیر است، که ابتدا توسط **لژیون دیریکله** «Lejeune DIRICHLET» (۱۸۰۵ ـ ۱۸۵۹) به اثبات رسیده است: هر تصاعد حسابی که در آن جملهٔ اوّل و قدر نسبت، نسبت به هم اوّل باشند، شامل بی‌نهایت عدد اوّل است.

نظریهٔ اعداد جمعی. سؤالهای مربوط به نظریهٔ اعداد جمعی را با استفاده از چند قضیه و مسألهٔ خاص توضیح می‌دهیم.

قضیهٔ فرما: هر عدد اوّل p با $p \equiv 1 \pmod 4$ مجموع مربعات دو عدد طبیعی است. نمایش مزبور، غیر از ترتیب جمعوندها، یکتاست.

مثال: $۲۳۳ = ۸^۲ + ۱۳^۲$

قضیهٔ لاگرانژ: هر عدد طبیعی را می‌توان به صورت مجموع مربعات حداکثر چهار عدد طبیعی نمایش داد.

مثال: ۱۱ را می‌توان به صورت مجموع سه مربع نوشت:

$$۱۱ = ۳^۲ + ۱^۲ + ۱^۲$$

۷ به چهار مربع نیاز دارد:

$$۷ = ۲^۲ + ۱^۲ + ۱^۲ + ۱^۲$$

مسألهٔ وارینگ «Waring's problem» (در سال ۱۷۷۰ توسط **وارینگ** مطرح، و ابتدا در سال ۱۹۰۹ توسط هیلبرت حل شد). تابع عدد ـ نظریه‌ای $g(k)$ای چنان موجود است که هر عدد طبیعی را می‌توان به صورت مجموع حداکثر $g(k)$ توان kام اعداد طبیعی نمایش داد.

به عنوان مثال، بنابه قضیهٔ لاگرانژ، $g(۲) = ۴$ و $g(۳) = ۹$.

جالب است که به ازای $k \geq ۳$، هر عدد به قدر کافی بزرگ n، به جمعوندهایی کمتر از $g(k)$ نیاز دارد و معلوم شده است که

$$۲۳۹ = ۴^۳ + ۴^۳ + ۳^۳ + ۳^۳ + ۳^۳ + ۱^۳ + ۱^۳ + ۱^۳ + ۱^۳$$

بزرگترین عددی است که به ۹ مکعب نیاز دارد؛ جمیع اعداد بزرگتر، حداکثر ۸ مکعب لازم دارند و اثبات شده که از عدد طبیعی معینی به بعد، جمیع اعداد بعدی، تجزیه‌ای به حداکثر ۷ مکعب را پذیرا می‌شوند.

حدس گلدباخ «Goldbach's conjecture». به سال ۱۷۴۲، گلدباخ در نامه‌ای به اویلر حدس زد که هر عدد زوج $n > ۶$ مجموع دو عدد اوّل فرد است. این حدس، تاکنون نه به اثبات رسیده و نه رد شده است. بهترین نتیجه در این زمینه، از **وینوگرادوف** «VINOGRADOV» (متولد ۱۸۹۱)، قضیهٔ سه اوّل «three primes theorem» است: هر عدد صحیح به قدر کافی بزرگ و فردی مجموع سه اوّل فرد است. اثبات قضیه از روشهای تحلیلی بسیار ظریفی، استفاده کرده است.

افرازها. منظور از افراز «partition» عدد طبیعی n، نمایش آن به صورت مجموعی از اعداد طبیعی است.

تعداد کل افرازهای عدد n را با $p(n)$ نمایش می‌دهیم، که در آن تعداد جمله‌ها محدود نیست؛ جمعوندهای برابر پذیرفته می‌شود و از ترتیب جمعوندها صرف‌نظر می‌شود.

به این ترتیب

$$۵ = ۴+۱ = ۳+۲ = ۳+۱+۱ = ۲+۲+۱$$

$$= ۲+۱+۱+۱ = ۱+۱+۱+۱+۱$$

هفت افراز ۵اند، و بنابراین $p(۵) = ۷$.

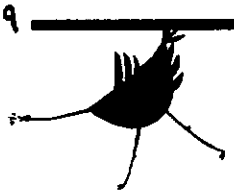
تابع $p(n)$ دارای ویژگیهای بسیار جالبی است؛ به عنوان مثال:

$$p(۵n+۴) \equiv ۰ \pmod ۵$$

و به ازای nهای بزرگ:

$$p(n) \sim \left[۱/(۴n\sqrt{۳})\right] \exp\left[\pi\sqrt{۲n/۳}\right]$$

به‌طور عمومیتر، یکی از مسائل اصلی نظریهٔ اعداد جمعی را می‌توان به صورت زیر بیان کرد. فرض می‌کنیم A مجموعه‌ای از اعداد طبیعی و $S > ۲$ عدد طبیعی مفروضی باشد؛ آیا می‌توان هر عدد طبیعی را به صورت مجموع حداکثر S عنصر A نمایش داد؟



از سال ۱۹۳۰ به بعد و با استفاده از روشها و مفاهیم جدید (چگالی «density» و مرتبهٔ ۱) به چنین مسائلی پرداخته شده است.

اعداد جبری

میدانهای اعداد جبری، عدد جبری «algebraic number» α عددی مختلط است که ریشهٔ معادلهٔ جبری «algebraic equation» $f(x)=0$ است. در این‌جا :

$$f(x)=a_0x^m+\ldots+a_m$$

یک چند جمله‌ای روی Q، میدان اعداد گویا، با $a_0\neq 0$ ، $m\geq 1$ است ؛ به عبارت دیگر، ضرایب a_0 ، a_1 ، ... ، a_m گویا هستند.

عدد α ریشهٔ بی‌نهایت معادله از درجه‌های گوناگون است ؛ به‌عنوان مثال $\alpha=\sqrt{3}$ در معادله‌های

$$x^2-3=0\ ,\quad x^3-x^2-3x+3=0\ ,\quad x^4-9=0$$

و غیره صدق می‌کند. اما چندجمله‌ایهای دو معادلهٔ اخیر را می‌توان به چندجمله‌ایهایی از درجهٔ پایین‌تر تجزیه کرد :

$$x^3-x^2-3x+3=(x^2-3)(x-1)$$

و

$$x^4-9=(x^2-3)(x^2+3)$$

چندجمله‌ایهایی از این دست را تجزیه‌پذیر «reducible» می‌نامیم و در صورتی که تجزیهٔ چندجمله‌ای f روی Q به عوامل ناثابت «non - constant factors» از درجهٔ پایین‌تر، البته باز هم با ضرایب در Q ، ممکن نباشد، f را روی Q *تحویل‌ناپذیر* «*irreducible*» می‌نامیم ؛ به عنوان مثال، $f(x)=x^2-3$ تحویل‌ناپذیر است.

به ازای عدد جبری α دقیقاً یک چندجمله‌ای گویا ـ تحویل‌ناپذیر «rationally irreduciblePolynomial» $\phi(x)$ با ضریب پیشرو[1]، چنان وجود دارد که $\phi(\alpha)=0$. درجهٔ عدد جبری α را به صورت درجهٔ $\phi(x)$ تعریف می‌کنیم. به عنوان مثال، هر عدد گویای r جبری از درجهٔ ۱ است ؛ زیرا ریشهٔ $x-r=0$ است، $(1+i\sqrt{3})/2$ از درجهٔ ۲ است ؛ زیرا ریشهٔ $x^2-x+1=0$ به حساب می‌آید، و $\sqrt[n]{2}$ ، به عنوان ریشهٔ $x^n-2=0$ ، از درجهٔ n است.

$\alpha^{(1)}$ ، $\alpha^{(2)}$ ، ... ، $\alpha^{(n)}$ ریشه‌های $\phi(x)=0$ (که یکی از آنها α است) به مزدوجها «conjugates»ی α موسوم و جمیعاً متمایزند. اگر در $\phi(x)=0$ جمیع ضرایب عدد صحیح باشند، آن‌گاه α را عدد صحیح جبری «algebraic integer» می‌نامیم.

فرض می‌کنیم V عدد جبری باشد. کوچکترین میدان $k=Q(V)$ را که شامل Q نیز V است، *میدان اعداد جبری* algebraic number « field می‌نامیم. به عنوان مثال، $Q(\sqrt{3})$ شامل جمیع اعداد به صورت $a+b\sqrt{3}$ ای‌است، که در آنها a و b اعدادی گویا هستند.

به سادگی می‌توان بررسی کرد که این اعداد، در واقع، تشکیل یک میدان می‌دهند ؛ به عنوان مثال :

$$1/(a+b\sqrt{3})=(a-b\sqrt{3})/(a^2-3b^2)=A+B\sqrt{3}$$

درجهٔ k را به صورت درجهٔ n(به گونه‌ای یکتا معین شدهٔ) هر عدد Vای تعریف می‌کنیم که به ازای آن $k=Q(V)$.

میدانهای عددی درجهٔ دوم. در میان میدانهای از نوع خاص، *میدانها (هیئتها)ی عددی درجهٔ دوم* «quadratic number fields» به گونه‌ای کاملتر مورد بررسی قرار گرفته‌اند. با درنظر گرفتن $V=\sqrt{d}$ ، می‌توان فرض کرد که d عدد صحیحی نابخش‌پذیر بر یک مربع است. تحت این شرط، بین میدانهای عددی درجهٔ دوم $Q(\sqrt{d})$ با $d\equiv 1 \pmod 4$ و با $d\equiv 2$ یا $3 \pmod 4$ تمیز قائل می‌شویم.

در حالت اوّل پایهٔ صحیح «integralbasis» میدان با

$$\omega_1=1\ ,\quad \omega_2=(-1+\sqrt{2})/2$$

و در حالت اخیر با $\omega_1=1$ ، $\omega_2=\sqrt{d}$ داده شده است. مقصود از این موضوع، آن است که هر عدد صحیح جبری $Q(\sqrt{d})$ را می‌توان به گونه‌ای یکتا به صورت $c_1\omega_1+c_2\omega_2$ با اعداد صحیح گویای c_1 و c_2 نمایش داد.