定義 (根 (こん))．n 次多項式 $f(x)$ の**根** (こん, root) とは，n 次**方程式** $f(x)=0$ の**解**のこと．

• 1 次 (線形) 方程式 $ax+b=0$ の解は $x=-\dfrac{b}{a}$ によって与えられる．

• 2 次方程式 $ax^2+bx+c=0$ を考える．根 x を平行移動して $X:=x+\dfrac{b}{2a}$ とおけば，

$$ax^2+bx+c=a\Big(x+\frac{b}{2a}\Big)^2-\frac{b^2-4ac}{4a}=aX^2-\frac{b^2-4ac}{4a}$$

となって，X の1次の項を消すことができる．これより，

$$X=\pm\frac{\sqrt{b^2-4ac}}{2a},\quad x=X-\frac{b}{2a}=\frac{-b\pm\sqrt{b^2-4ac}}{2a}.$$

• **代数学**は上述のような n **次 (代数) 方程式を解く学問** (のはず) である．しかし，高校では2次方程式の解の公式までしか習わなかった．(← 他の微分方程式などと区別して，代数方程式とも言う)

n 次方程式の解は (第 10 回で説明したように) 四則演算が可能な体 K 上で考える事ができる．例えば，位数 p の有限体 $\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$ 上で，$ax^2+bx+c=0$ なる解 $x\in\mathbb{F}_p$ (つまり，$ax^2+bx+c\equiv 0 \pmod p$ の解) を考えることができる．
しかし，ここでは通常通り，多項式 $f(x)$ の係数は有理数体 $\mathbb{Q}$ 上，根 ($f(x)=0$ の解) は複素数体 $K=\mathbb{C}$ (または実数体 $K=\mathbb{R}$) の中で考えることとする．

• そこで，大学生らしく，n 次方程式 $ax^n+bx^{n-1}+\cdots=0$ の解の公式について考えることにする．2 次方程式のときと同様に，$X:=x+\frac{b}{na}$ とおけば，X の $n-1$ 次の項を消すことができる．また両辺を a で割り，X^n の係数は $a=1$ とできる．これより，

$$X^n+pX^{n-2}+qX^{n-3}+\cdots=0$$

の形の方程式に解の公式を与えれば十分である (← その後に (2 次同様に) X を x に戻せばよい)．

定理 (カルダノの公式, Cardano's formula, 1545)．3 次方程式 $X^3+pX+q=0$ の解は，

$$X=\omega^i\sqrt[3]{-\frac{q}{2}+\sqrt{\Big(\frac{p}{3}\Big)^3+\Big(\frac{q}{2}\Big)^2}}+\omega^{2i}\sqrt[3]{-\frac{q}{2}-\sqrt{\Big(\frac{p}{3}\Big)^3+\Big(\frac{q}{2}\Big)^2}},\quad (i=0,1,2)$$

の 3 つの複素数である．但し，$\omega=\dfrac{-1+\sqrt{-3}}{2}$ は $w^3=1$ なる複素数 (1 の原始 3 乗根という)，2 つの 3 乗根 $\sqrt[3]{\cdot}$ は，それぞれ 3 通りの選び方があるが，その積が $\dfrac{-p}{3}$ となる 3 つを選ぶ．

補題．$x^3+y^3+z^3-3xyz=(x+y+z)(x^2+y^2+z^2-xy-yz-zx)$
$=(x+y+z)(x+\omega y+\omega^2 z)(x+\omega^2 y+\omega z).$

定理の証明 ①．補題で $(x,y,z):=(X,-s,-t)$ とおくと，複素数体 $\mathbb{C}$ の中では
$X^3-3stX-s^3-t^3=(X-s-t)(X-\omega s-\omega^2 t)(X-\omega^2 s-\omega t)$ と因数分解できる．そこで，

$$\begin{cases}3st=-p,\\ s^3+t^3=-q\end{cases}$$

なる s,t を取れば，$X^3-3stX-s^3-t^3=X^3+pX+q$ の根は $X=s+t,\ \omega s+\omega^2 t,\ \omega^2 s+\omega t$.
ここで，$s^3+t^3=-q,\ s^3t^3=-(p/3)^3$ より s^3 と t^3 は $Y^2+qY-(p/3)^3=0$ の根．よって，
$s^3,\ t^3=\dfrac{-q\pm\sqrt{q^2+4(p/3)^3}}{2}$ であり，$s=\sqrt[3]{s^3},\ t=\sqrt[3]{t^3}$ は $st=\dfrac{-p}{3}$ を満たす様にとる．

定理の証明 ②．$X=s+t$ とすれば，$(s+t)^3+p(s+t)+q=s^3+t^3+(s+t)(3st+p)+q=0.$
ここで，$3st=-p$ **を仮定する**．あとは，①と同様に，s,t を求めることができる．

• 3 次方程式の解の公式 (カルダノの公式) が分かったからといって，**安心してはいけない**．高校生でも解ける**可約な** 3 次方程式 $(X-d)(X^2+bX+c) = X^3+(b-d)X^2+(c-bd)X-cd = 0$ の 3 つの解 d, $(-b\pm\sqrt{b^2-4c})/2$ とカルダノの公式による解を比べてみると**一致しない**ことが分かる．(← そもそも 2 次方程式の解の公式で解を求めると，$\sqrt{\cdot}$ は出てくるが，$\sqrt[3]{\cdot}$ は出てこない)

• しかし，(上で示した) 二次方程式の解の公式もカルダノの公式も**どちらも間違ってはいない**．実は，根 (解) の表示 (見た目) が異なるだけであって，その数値が異なっているわけではないのである．これに気付く為には，そもそも，**実数や複素数の** 少数，分数，べき根 (ルート) を用いた**表示は一意的ではない**ことに注意する必要がある．

実数や複素数の異なる表現．

• $\dfrac{1}{3} = 0.3333\cdots$, $1 = 0.9999\cdots$ (← $\neq$ とすれば，実数の稠密性 $1 > \exists x > 0.9999\cdots$ に矛盾する)

• $\sqrt{5\pm2\sqrt{6}} = \sqrt{3}\pm\sqrt{2}$, 2 **重根号を外す公式**: $\sqrt{(a+b)\pm2\sqrt{ab}} = \sqrt{a}\pm\sqrt{b}$. (← 両辺を 2 乗)

• $\omega = \dfrac{-1+\sqrt{-3}}{2}$ (1 の原始 3 乗根) とする．$\omega^3-1 = (\omega-1)(\omega^2+\omega+1) = 0$ と $\omega\neq1$ より，$\omega^2+\omega+1=0$ である．よって，$\omega^2(\omega^2+2\omega+1) = (\omega(\omega+1))^2 = (\omega^2+\omega)^2 = (-1)^2 = 1$.

• 次の等式は Daniel Shanks の “驚くべき等式” (Incredible identities) と呼ばれる (参考文献 [**9**], [**10**]) (← この等式もガロア理論を学ぶと自然に理解できる) ([**10**] はミスプリントが多いので注意)：

$$\sqrt{5}+\sqrt{22+2\sqrt{5}} = \sqrt{11+2\sqrt{29}}+\sqrt{16-2\sqrt{29}+2\sqrt{55-10\sqrt{29}}} \qquad (=7.38117\cdots).$$

カルダノの公式を計算してみる．

例 1． $X^3-12X+16 = (X+4)(X-2)^2 = 0$ の解は $X=-4$, $X=2$ (2 重根) である．カルダノの公式を $p=-12$, $q=16$ に適用すると，

$$\begin{aligned}
X &= \sqrt[3]{-8+\sqrt{(-4)^3+8^2}}+\sqrt[3]{-8-\sqrt{(-4)^3+8^2}} = \sqrt[3]{-8}+\sqrt[3]{-8} = -4,\\
X &= \omega\sqrt[3]{-8}+\omega^2\sqrt[3]{-8} = (\omega+\omega^2)\sqrt[3]{-8} = (-1)\sqrt[3]{-8} = 2,\\
X &= \omega^2\sqrt[3]{-8}+\omega\sqrt[3]{-8} = (\omega^2+\omega)\sqrt[3]{-8} = (-1)\sqrt[3]{-8} = 2.
\end{aligned}$$

例 2． $X^3-15X-4 = (X-4)(X^2+4X+1) = 0$ の解は $X=4$, $X=-2\pm\sqrt{3}$ である．カルダノの公式を $p=-15$, $q=-4$ に適用すると，

$$\begin{aligned}
X &= \sqrt[3]{2+\sqrt{(-5)^3+(-2)^2}}+\sqrt[3]{2-\sqrt{(-5)^3+(-2)^2}} = \sqrt[3]{2+\sqrt{-121}}+\sqrt[3]{2-\sqrt{-121}},\\
X &= \omega\sqrt[3]{2+\sqrt{-121}}+\omega^2\sqrt[3]{2-\sqrt{-121}}, \quad X = \omega^2\sqrt[3]{2+\sqrt{-121}}+\omega\sqrt[3]{2-\sqrt{-121}}.
\end{aligned}$$

しかし，実は $\sqrt[3]{2\pm\sqrt{-121}} = 2\pm\sqrt{-1}$ が成り立つ (← 両辺を 3 乗してみる)．よって，

$$\begin{aligned}
X &= (2+\sqrt{-1})+(2-\sqrt{-1}) = 4,\\
X &= \omega(2+\sqrt{-1})+\omega^2(2-\sqrt{-1}) = \frac{-1+\sqrt{-3}}{2}(2+\sqrt{-1})+\frac{-1-\sqrt{-3}}{2}(2-\sqrt{-1}) = -2-\sqrt{3},\\
X &= \omega^2(2+\sqrt{-1})+\omega(2-\sqrt{-1}) = \frac{-1-\sqrt{-3}}{2}(2+\sqrt{-1})+\frac{-1+\sqrt{-3}}{2}(2-\sqrt{-1}) = -2+\sqrt{3}.
\end{aligned}$$

例 3． $X^3+X-2 = (X-1)(X^2+X+2) = 0$ の解は $X=1$, $X=\dfrac{-1\pm\sqrt{-7}}{2}$ である．カルダノの公式を $p=1$, $q=-2$ に適用すると，唯一の実根は以下の表示になってしまう (!)：

$$1 = \sqrt[3]{1+\sqrt{\left(\frac{1}{3}\right)^3+(-1)^2}}+\sqrt[3]{1-\sqrt{\left(\frac{1}{3}\right)^3+(-1)^2}} = \sqrt[3]{1+\frac{2}{3}\sqrt{\frac{7}{3}}}+\sqrt[3]{1-\frac{2}{3}\sqrt{\frac{7}{3}}}.$$

例 2 をよく見ると，**解は 3 つとも実数解**なのにも関わらず，カルダノの公式では，3 つの解を表示するのに，**複素数が必要**になっている．一般に，解の公式の $\sqrt{\cdot}$ の中身が $\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2 < 0$ の場合には，3 つ解は実数になることが分かる．そこで，複素数を用いない，より良い公式が作れないかと思うのは自然なことである．しかし，次のことが分かる (参考文献 [**4**] 参照)：

(known) Fact. $\mathbb{Q}$ 上既約な 3 次式 $f(X)$ に対して，3 次方程式 $f(X) = 0$ は 3 の実数解をもつとする．このとき，3 つの実数解を実の根号 (ルート) だけで表すことはできない．

3 つの実数解を持つ場合は「不還元」(casus irreducibilis) とも呼ばれる．これは，3 つの実数解を表す解の公式は，実数の中の世界だけで生きていては作れない，それまでは不合理なものと考えられていた「複素数」の世界にまで数の世界を拡張して，初めて解の公式が作れることを表している.「複素数」がいかに自然なものかが明らかになったのである．

4 次方程式の場合. 4 次方程式の解法はカルダノの弟子であるフェラーリ (Ludovico Ferrari, 1522-1565) によって発見され，カルダノの著書「アルス・マグナ (Ars Magna, 大いなる術, 1545)」の中で発表された．ここでは，後のデカルト (René Descartes, 1596-1650) による方法を紹介する．

$$X^4 + pX^2 + qX + r = (X^2 + kX + l)(X^2 - kX + m)$$

と因数分解することを考えると，未定係数法 (p.17 参照) によって

$$(p, q, r) = (l + m - k^2, k(m - l), lm)$$

を得る．最初の 2 つから，$2m = k^2 + p + q/k$, $2l = k^2 + p - q/k$ を得て，3 番目に代入すれば

$$k^6 + 2pk^4 + (p^2 - 4r)k^2 - q^2 = 0$$

を得る．これは，k^2 **に関する 3 次式**であるから，カルダノの公式を使って解くことが出来る．よって，(k, l, m) が得られ，最後に 2 次方程式の解の公式によって，$X^4 + pX^2 + qX + r$ の解を求めることができる．(← 特に，4 次方程式の解法は，3 次方程式及び 2 次方程式の解法に帰着される)

代数学の基本定理 (ガウス, Carl Friedrich Gauss, 1799).
複素数係数の n 次方程式は，複素数の中に重複度を込めて n 個の解を持つ．

• ガウスによる，代数学の基本定理は n 次方程式は解を複素数にまで広げれば，(重複度を込めて) 丁度 n 個存在することを主張している．しかし，解が存在するという事と，解の公式が実際に作れるかということは別問題である．ここで，解の公式とは 2 次，3 次，4 次のときと同様に，四則演算とべき根 (ルート) をとる操作を繰り返して，解を表示する式 を表すことにする．

5 次方程式の場合. 4 次方程式が 3 次, 2 次方程式に帰着されたように，5 次方程式をより低次の場合に帰着させようとする試みが，多くの数学者によってなされた．が，ことごとく失敗に終わった．それどころか，アーベル (Abel, 1802–1829) によって次の定理が示された．(← 3 次と 4 次の解の公式が発表された，カルダノの「アルス・マグナ」から実に 280 年もの歳月を経ている (!))

定理 (アーベル, Niels Henrik Abel, 1826).
5 次以上の代数方程式は，四則演算とべき根 $\sqrt[\nu]{\cdot}$ をとる操作を繰り返して得られる，解の公式は一般には存在しない．

• ここで注意すべきなのは，解の公式は**一般には存在しない**という部分である．第 10 回 (p.24) に注意したように，ある特別な 5 次式については解の公式は存在する．(← 例えば，$X^5 = 2$ の解は $X = \sqrt[5]{2}, \sqrt[5]{2}\zeta, \sqrt[5]{2}\zeta^2, \sqrt[5]{2}\zeta^3, \sqrt[5]{2}\zeta^4$ で与えられる．但し，$\zeta \in \mathbb{C}$ は $\zeta^5 = 1$ なる複素数；原始 5 乗根)

• どのような 5 次以上の方程式に解の公式が存在し，どのような 5 次以上の方程式に公式が存在しないのかを，我々に教えてくれるのが**ガロア理論**である．

定理 (ガロア, Évariste Galois, 1830). n 次方程式 $f(X)=0$ の解が四則演算とべき根 $\sqrt[n]{\cdot}$ を繰り返し使って書ける $\iff$ 多項式 $f(X)$ のガロア群が可解群 (solvable group) である

例 (5 次既約多項式のガロア群). $f(X)$ を $\mathbb{Q}$ 上の 5 次既約多項式とする．このとき，$f(X)$ のガロア群は 5 次対称群 S_5 の部分群であり，次の群 S_5, A_5, F_{20}, D_5, C_5 のいずれか (と同型) となる：

5 次方程式	$f_i(X)$ のガロア群	
$f_1(X)=X^5-X^3-X^2+X+1=0$	$\longrightarrow S_5$ (5 次対称群)	
$f_2(X)=X^5+X^4-2X^2-2X-2=0$	$\longrightarrow A_5$ (5 次交代群)	
$f_3(X)=X^5+X^4+2X^3+4X^2+X+1=0$	$\longrightarrow F_{20}=\langle\sigma,\rho\rangle$	$\rho=(1\,2\,4\,3)$
$f_4(X)=X^5-X^3-2X^2-2X-1=0$	$\longrightarrow D_5=\langle\sigma,\tau\rangle$	$\tau=(1\,4)(2\,3)=\rho^2$
$f_5(X)=X^5+X^4-4X^3-3X^2+3X+1=0$	$\longrightarrow C_5=\langle\sigma\rangle$	$\sigma=(1\,2\,3\,4\,5)$

実は，解の公式が作れるかどうかはガロア群 G がどの位可換群に近いかが密接に関係する．(← 可解群とは可換群または非可換群でも可換群に近い性質を持つ群のことである) つまり，ガロア群が可換群に近い性質をもつのか，可換群とはかけ離れていて，非常に強い非可換性を持つ群なのかといった，より G のことを詳細に知る必要がある．そのためには，第 10 回で述べたように G の部分群を調べる必要がある (p.24 参照)．多項式 $f_5(X)$ のガロア群は位数 5 の巡回群 C_5 であり，可換群であるから $f_5(X)=0$ の解は四則演算とべき根の繰り返しで書ける．一方，$f_1(X)=0$ のガロア群は S_5 であり，可解群でないことが示される．すなわち，$f_1(X)=0$ の解は，四則演算とべき根を繰り返し使って表示することはできないのである．

• n 次方程式に解の公式が存在するかどうかという問題は，S_n の部分群の性質の問題に置き換わる．よって，これから学ぶ，**群の理論 (群論)，環の理論 (環論)，体の理論 (体論)** をしっかりと理解することが，ガロア理論によって代数方程式の解の公式の有無を調べる為には重要になる．

• ガロア理論は，大学における代数学の 1 つの目標であり，是非，自分で納得できるまで学んでほしい．一方で，ガロアによって 1830 年頃に作られた理論であるということも事実である．これまで紹介したように，その先には，代数的整数論，高木貞治による類体論，岩澤健吉による岩澤理論，楕円曲線の理論，保型形式の理論，解析的整数論，代数幾何学，数論幾何学，... と非常に興味深い数学の世界が，まだまだ広がっている．このような現代数学は 4 年生から大学院にかけてじっくりと学ぶことができる．(← **さらに驚く事に，これらの世界は有機的につながっているのである！**)

• 少しでも興味が出てきたら，夏休みに図書館で，これまでに紹介した本を読んでみましょう (!).

参考文献

[1] ガロアの時代 ガロアの数学〈第 1 部〉時代篇, 彌永昌吉 (著), 267 ページ, シュプリンガー・フェアラーク東京 (1999), 2079 円.

[2] ガロアの時代 ガロアの数学〈第 2 部〉数学篇, 彌永昌吉 (著), 289 ページ, シュプリンガー・フェアラーク東京 (2002), 2079 円.

[3] 代数方程式のガロアの理論, J.-P. Tignol(著), 新妻弘 (翻訳), 348 ページ, 共立出版 (2005), 3360 円.

[4] ガロア理論講義, 足立恒雄 (著), 239 ページ, 日本評論社; 増補版 (2003), 3045 円.

---

[5] 解決!フェルマーの最終定理―現代数論の軌跡, 加藤和也 (著), 271 ページ, 日本評論社 (1995), 2625 円.

[6] フェルマーの最終定理―ピュタゴラスに始まり、ワイルズが証明するまで (単行本) サイモン シン (著), 青木薫 (翻訳), 397 ページ, 新潮社 (2000), 2415 円. (文庫本も有り)

[7] 数論入門, 山本芳彦 (著), 372 ページ, 岩波書店 (2003), 3990 円.

[8] 数論への出発, 藤崎源二郎, 山本芳彦, 森田康夫 (著), 194 ページ, 日本評論社; 増補版 (2004), 2730 円.

---

[9] D. Shanks, Incredible identities, Fibonacci Quart. **12** (1974), 271.

[10] C. E. van der Ploeg, Duality in Nonnormal Quartic Fields, Amer. Math. Monthly **94** (1987), 279–284.