方程式の解法と群 — 代数学入門

筑波大学数学系　　森田　純

1　はじめの前に

皆さんは代数というと、どういう学問を思い浮かべるでしょうか。高校の教科書にも代数・幾何というものがありますから、ははあ、ああいうものかな、と想像できるかも知れません。大学の学群（筑波大学では学部にあたる組織をこう呼ぶ）では、「線形代数」、「線形代数続論」、「代数入門」、「代数学」といった講義が用意されています。線形代数というのは、行列の高等理論にあたるもので、高校での２次行列の話は、その一部の入門編に相当します。代数学では和や積が定義されている様々な集合を統一的に扱います。１＋２＝３ や ２×３＝６ といった通常の数の計算や、行列の和や積などの様なもの、果ては ２＋３＝０ などという尋常ではない演算体系まで出てきてしまうのです。そして、３年次の最後には、「ガロアの理論」というものを学習します。これは、５次以上の代数方程式には、四則演算と根号だけを用いた解の公式は一般には存在しない、というものです。それを証明する段階で、ここの題名にもある "群" という代数概念が、大活躍してくれるわけです。こういった代数の理論は代数の中だけに留まらず、数学全般、いや広く自然科学全体をしっかりと支えている基礎分野でもあります。

ここでは、なるべく具体的なものを題材にして、代数学の入門的な話ができればと考えています。

2　はじめに

今回は

$$x^2 + y^2 = z^2 \tag{1}$$

という方程式と、

$$x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n = 0 \tag{2}$$

という方程式の二種類を考えてみましょう。(1) については、この方程式を満足する整数の組を考えることにします。例えば、$3^2 + 4^2 = 9 + 16 = 25 = 5^2$ ですから、組 $(3, 4, 5)$ は満たしています。その他にも $(5, 12, 13)$ や $(8, 15, 17)$ など、沢山あります。(2) については、$n = 2$ の場合には高校で二次方程式という単元で、既に学んでいることでしょう。そこでは、実数解だけではなくて、$a + bi$ （a, b は実数、i は虚数単位）という形の数、いわゆる複素数の解も登場してきます。そして、n が一般の場合にも、(2) の解を調べるためには、この複素数の範囲で十分であることが知られています。しかし、その解が、四則演算と根号だけを用いて記述できるかというと、話が別になってくるのです。

まあ、とにかく代数の世界の扉を開けてみましょう。

－－－－－－ パチ パチ パチ －－－－－－

3　ピタゴラス数（はじまり・はじまり）

ピタゴラス (Pythagorus) 数は古代エジプト時代にまで、その歴史を遡（さかのぼ）ることができます。また、それ以来、多くの人々に興味をもたれ、親しまれてきました。現在も中学校で、三平方の定理と関連して、ピタゴラス数の話が出てくる様です。紀元前２０００年頃に作られたという、エジプトの一つのパピルスには、直角三角形の三辺を表す様な数の組が書かれていて、$3^2 + 4^2 = 5^2$ に相当するものだと言われ

ています。一方、壁画には縄張り師たちが描かれていて、彼らは等間隔の結び目のついた縄で、３、４、５の長さにより、直角の測量をしています。この様に、世界各地、文明の栄えた所には三角測量があり、従って、そこでは三つ組 $(3,4,5)$ によって直角が作図できるということは、かなり一般に知られていた様です。しかしながら、$3^2+4^2=5^2$ となることと、$(3,4,5)$ が直角三角形を作ることの関連性については、まだ、はっきりとした認識は無かった様でした。両者を系統だてて論じたのは、紀元前６〜５世紀頃に、ギリシャで活躍したピタゴラス学派の人々です。いわゆる三平方の定理の誕生です。

以下、ここでは、$a^2+b^2=c^2$ を満たす整数の三つ組 (a,b,c) を考え、これをピタゴラス数と呼ぶことにします。ですから、$(3,4,5)$ や $(5,12,13)$、$(8,15,17)$ はピタゴラス数です。ピタゴラス学派はピタゴラス数として、$n=3,5,7,9,\cdots$ (奇数) に対応した三つ組

$$(n,\frac{n^2-1}{2},\frac{n^2+1}{2})$$

を得ていました。これらをピタゴラス学派の解と呼ぶことにしましょう。しかし、ピタゴラス学派の解だけでは全ての自然数解を尽くしてはいなかったのです。例えば、上の $(8,15,17)$ は、実はピタゴラス学派の解としては得られません。（何故でしょうか？）後に、ユークリッド (Euclid)、ディオファントス (Diophantus) らにより、

$$(m^2-n^2,2mn,m^2+n^2)$$

(m,n は整数) の形で、本質的に（すなわち、順序や符合や整数倍を無視すれば）全てのピタゴラス数が得られることが示されたのです。 — ナルホド！ —

4 ピタゴラス数（その解法）

では、実際にピタゴラス数を全て求めてみましょう。空欄を適当に埋めながら進んでみて下さい。a,b,c を整数として、$a^2+b^2=c^2$ が成立しているものとします。$(0,0,0)$ は解ですが、自明なので、以下 $(a,b,c)\neq(0,0,0)$ とします。また、$a=0,\ b=c$ や $b=0,\ a=c$ も自明ですので、以下これ以外の解を探すことにしましょう。ここでさらに、a,b,c は全て正の場合に考えておけば、他の場合も全て導けますから、以下 a,b,c は自然数と仮定しましょう。もし a,b,c に公約数 $\ell>1$ があれば、$a=\ell a',\ b=\ell b',\ c=\ell c'$ として、$a'^2+b'^2=c'^2$ を解けばいいので、結局 a,b,c の最大公約数が 1 の場合を考えれば十分となります。従って、我々は $a^2+b^2=c^2$ を満たす自然数 a,b,c で、最大公約数が 1 となるものを全て探せばよいのです。さて、その様な a,b,c があったとします。仮に a と b 共に偶数だとすれば、c も $\boxed{\quad}$ となり、$\boxed{\qquad}$。従って a,b のどちらか一方は $\boxed{\quad}$ だと仮定してよいことになります。今、a の方を奇数だとしましょう。このとき、b は $\boxed{\quad}$ であり、c は $\boxed{\quad}$ となります。ここで

$$b^2=c^2-a^2=\boxed{\qquad}$$

と因数分解します。すると、$b,\ c+a,\ c-a$ は全て $\boxed{\quad}$ になります。$b=2u,\ c+a=2v,\ c-a=2w$ とおいてみると、$(2u)^2=\boxed{\qquad}$ となり、$u^2=vw$ が得られます。我々の仮定より、a と c の公約数は 1 のみですから、v と w の最大公約数も $\boxed{\quad}$ となります。また、$u^2=vw$ の左辺は平方数ですから、従って、v や w も $\boxed{\qquad}$ でなければなりません。すなわち、$v=m^2,\ w=n^2$ の形をしていることになります。よって、

$$\begin{aligned}a&=v-w=m^2-n^2\\ b&=2u=2\sqrt{vw}=2mn\\ c&=v+w=m^2+n^2\end{aligned}$$

となります。できましたね。 — ヤッタネ! —

正確には、ピタゴラス数 (a,b,c) は

$$\begin{cases} a = \ell(m^2-n^2) \\ b = 2\ell mn \\ c = \ell(m^2+n^2) \end{cases} \qquad \begin{cases} a = 2\ell mn \\ b = \ell(m^2-n^2) \\ c = \ell(m^2+n^2) \end{cases}$$

$(\ell, m, n :$ 整数$)$ で、その全てが与えられることになります。

問題 1　$\ell,\ m,\ n$ に色々な値を入れて、ピタゴラス数をひとり五個程度求めよ。

注意　「$\ell = 1$、$m > n > 0$、$m + n =$ 奇数、m と n の最大公約数が 1」ならば、「$a,\ b,\ c > 0$ の最大公約数が 1 」である。

5　ピタゴラス数（つづき）

さて、以下の議論を進め易くするために、

$$\mathbf{Z} = \{0, \pm1, \pm2, \cdots\} : \text{整数全体}$$
$$P = \{(a,b,c) \mid a,b,c \in \mathbf{Z},\ a^2+b^2=c^2,\ \text{かつ } |a|,|b|,|c| \text{ の最大公約数が } 1\}$$

と記号を定めます。そうすれば、全てのピタゴラス数は

$$(na, nb, nc); \qquad (a,b,c) \in P,\ n = 0,1,2,3,\cdots$$

なる形で表せますから、集合 P を調べればよいわけです。まず、方程式 (1) の形より、P から P 自身への一対一、上への写像が四個見つかります。

$$\begin{aligned} r_1 &: (a,b,c) \mapsto (-a,b,c) \\ r_2 &: (a,b,c) \mapsto (a,-b,c) \\ r_3 &: (a,b,c) \mapsto (a,b,-c) \\ t &: (a,b,c) \mapsto (b,a,c) \end{aligned}$$

これらを、仮に基本変換と呼ぶことにします。また、もう一つ

$$s : (a,b,c) \mapsto (2c-a-2b, 2c-2a-b, 3c-2a-2b)$$

で定義される写像も考えます。これを特殊変換と呼ぶことにしましょう。

問題 2　s は、P から P への写像になっていることを示せ。

さて、(a,b,c) を r_1 で写すと、定義から $(-a,b,c)$ になりますね。では、さらにもう一度 r_1 で写すとどうなるでしょうか？ そうですね、元に戻って (a,b,c) になってしまいますね。他の $r_2,\ r_3,\ t$ もそうです。同じ写像を二度つづけると、元に戻ってしまうという性質がありますね。では、s という写像はどうでしょうか？

問題 3　次の空欄の中を適当に埋めよ。

$$s\ :\ (2c-a-2b, 2c-2a-b, 3c-2a-2b) \mapsto (\boxed{}, \boxed{}, \boxed{})$$

えっ？ どうでしたって？ そうですか、うまくいきましたか。では今度は写像 r_1 と写像 s の合成を考えてみましょう。この合成写像にも f という名前を付けましょう。

$$f\ :\ (a,b,c) \overset{r_1}{\mapsto} (-a,b,c) \overset{s}{\mapsto} (2c+a-2b, 2c+2a-b, 3c+2a-2b)$$

問題 4　写像 f で写した結果 (1) 〜 (5) を計算せよ。

(1)　$f\ :\ (1,0,1) \mapsto (\boxed{}, \boxed{}, \boxed{})$
(2)　$f\ :\ (3,4,5) \mapsto (\boxed{}, \boxed{}, \boxed{})$
(3)　$f\ :\ (5,12,13) \mapsto (\boxed{}, \boxed{}, \boxed{})$
(4)　$f\ :\ (7,24,25) \mapsto (\boxed{}, \boxed{}, \boxed{})$
(5)　$f\ :\ (9,40,41) \mapsto (\boxed{}, \boxed{}, \boxed{})$

いかがでしたか？ 今度もうまくいきましたか？ 自明な基本的な解 $(1,0,1)$ に写像 f を次々に施すと、何とピタゴラス学派の解がどんどん出てきてしまうのですね。これはうまい仕掛けですね。今は、f のみ、従って r_2 や r_3 は使いませんでした。それでは、$r_1,\ r_2,\ r_3,\ t,\ s$ の有限個の組み合わせ全てを用いると、どうなるでしょうか？ そう、実は今度は $(1,0,1)$ から出発して、ピタゴラス数の全体 P が出てきてしまうのです。これを数学的記法で

$$P = \langle r_1, r_2, r_3, t, s\rangle(1,0,1)$$

と書き表したりもします。この $\langle r_1, r_2, r_3, t, s\rangle$ の部分の数学的構造が “群” と呼ばれるものになっています。代数的に詳しく調べてみると、今の場合その構造が ＜**魔法の万華鏡**＞ の様なものになっていて、まん中に $(1,0,1)$ を落すと、それが次々に鏡に映されていって、そしてピタゴラス数の全てが得られてしまう、そんな状況になっているのです。 — スゴーイ! —

6　休憩

最近、フェルマー（Fermat）予想の話題が賑やかです。ワイルズ (Wiles) 氏の前回の論文中にあったギャップを、今回はワイルズ氏自身と、それにテイラー（Taylor）氏の協力も得て乗り越えているそうです。歴史的な大問題も二十一世紀を前にして解決されたと言っても、よさそうな状況になりつつあります。色々な経緯がありますから、より慎重にならざるを得ませんが、近々に完全な評価も定まることでしょう。一つの大きな数学の話題ではあります。おっと、フェルマー予想の内容を言うのを忘れました。

フェルマー予想： n を 3 以上の自然数とするとき、$a^n + b^n = c^n$ を満たす自然数 a, b, c は存在しない。

7　代数方程式（二次方程式の巻）

さて、話を代数方程式に移しましょう。一般に、代数方程式というのは

$$a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_{n-1}x + a_n = 0$$

という形をしている方程式のことです。最高次 x^n の係数 a_0 が零でない時、これを n 次（代数）方程式と呼びます。二次方程式の場合には、既に皆さんは解の公式を学んでいることでしょう。

$$a_0x^2 + a_1x + a_2 = 0$$

を解くと、

$$\boxed{x = \frac{-a_1 \pm \sqrt{a_1^2 - 4a_0a_2}}{2a_0}}$$

となっていた筈ですね。我々は $a_0 \neq 0$ と仮定しているので、始めに a_0 で両辺を割っておいて、$x^2+a_1x+a_2=0$ なる形から始めても理論上はいいわけですね。その時の解の公式は

$$\boxed{x = \frac{-a_1 \pm \sqrt{a_1^2 - 4a_2}}{2}}$$

となります。同じ理由で、n 次方程式も

$$x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_{n-1}x + a_n = 0$$

なる形から出発しても、一般性は失わないわけです。では、三次方程式は実際に解けるのでしょうか？ 次の節に行ってみましょう。 — ワクワク! —

8　代数方程式（三次・四次方程式の巻）

三次方程式

$$x^3 + a_1x^2 + a_2x + a_3 = 0$$

を考えましょう。ここで

$$x = X - \frac{a_1}{3}$$

と置きますと、$X^3 + b_2X + b_3 = 0$ なる形になりますから、初めから解くべき方程式が

$$x^3 + ax = b \tag{3}$$

としても、一般性は失われません。ここで、補助の二次方程式

$$t^2 - bt - \frac{a^3}{27} = 0$$

を考え、その解を

$$\alpha = \frac{b + \sqrt{b^2 + \frac{4}{27}a^3}}{2}, \quad \beta = \frac{b - \sqrt{b^2 + \frac{4}{27}a^3}}{2}$$

とします。このとき、解と係数の関係より、

$$\alpha + \beta = b, \quad \alpha\beta = -\frac{a^3}{27}$$

が成立しています。さて、α の三乗根 $\sqrt[3]{\alpha}$ と β の三乗根 $\sqrt[3]{\beta}$ を

$$\sqrt[3]{\alpha}\sqrt[3]{\beta} = -\frac{a}{3}$$

となる様に選んでおきましょう。このとき、

$$\begin{aligned} & (\sqrt[3]{\alpha} + \sqrt[3]{\beta})^3 + a(\sqrt[3]{\alpha} + \sqrt[3]{\beta}) \\ = \; & \alpha + \beta + 3(\sqrt[3]{\alpha} + \sqrt[3]{\beta})\sqrt[3]{\alpha}\sqrt[3]{\beta} + a(\sqrt[3]{\alpha} + \sqrt[3]{\beta}) \\ = \; & \alpha + \beta = b \end{aligned}$$

となりますから、$x = \sqrt[3]{\alpha} + \sqrt[3]{\beta}$ が解となります。α と β の三乗根の採り方には三通りの自由度がありますから、一般には三つの解が得られるのです。よって、三次方程式 (3) の解の公式は

$$\boxed{x = \sqrt[3]{\frac{b + \sqrt{b^2 + \frac{4}{27}a^3}}{2}} + \sqrt[3]{\frac{b - \sqrt{b^2 + \frac{4}{27}a^3}}{2}}}$$

となります。正確には $\sqrt[3]{\alpha}$ と $\sqrt[3]{\beta}$ を一組み固定したとき、$\sqrt[3]{\alpha}+\sqrt[3]{\beta},\ \omega\sqrt[3]{\alpha}+\omega^2\sqrt[3]{\beta},\ \omega^2\sqrt[3]{\alpha}+\omega\sqrt[3]{\beta}$ の三つが解を与えているのです。ここで、ω は 1 の原始三乗根で、$\omega=(-1+\sqrt{-3})/2$ とします。

問題 5　三次方程式

$$x^3-3x+3=0$$

の解を求めよ。

次に四次方程式

$$x^4+a_1x^3+a_2x^2+a_3x+a_4=0$$

を考えましょう。ここで

$$x=X-\frac{a_1}{4}$$

と置きますと、

$$X^4+b_2X^2+b_3X+b_4=0$$

なる形になりますから、初めから解くべき方程式が

$$x^4+ax^2+bx=c \tag{4}$$

としても、一般性は失われません。ここで、補助の三次方程式

$$t^3+2at^2+(a^2+4c)x-b^2=0$$

を考えましょう。その解を$\alpha,\ \beta,\ \gamma$ とします。先程やりました様に、この$\alpha,\ \beta,\ \gamma$ は四則演算と根号を用いて導くことが出来ました。このとき、解と係数の関係より、

$$\alpha+\beta+\gamma=-2a,\quad \alpha\beta+\beta\gamma+\gamma\alpha=a^2+4c,\quad \alpha\beta\gamma=b^2$$

が成立しています。さて、$\alpha,\ \beta,\ \gamma$ の平方根$\sqrt{\alpha},\ \sqrt{\beta},\ \sqrt{\gamma}$ を

$$\sqrt{\alpha}\sqrt{\beta}\sqrt{\gamma}=-b$$

となる様に選んでおきましょう。計算し易い様に、

$$\begin{aligned}\lambda&=\sqrt{\alpha}\sqrt{\beta}+\sqrt{\beta}\sqrt{\gamma}+\sqrt{\gamma}\sqrt{\alpha}\\ \mu&=\alpha\sqrt{\beta}\sqrt{\gamma}+\beta\sqrt{\gamma}\sqrt{\alpha}+\gamma\sqrt{\alpha}\sqrt{\beta}\end{aligned}$$

と置くと、

$$\begin{aligned}&(\tfrac{\sqrt{\alpha}+\sqrt{\beta}+\sqrt{\gamma}}{2})^4+a(\tfrac{\sqrt{\alpha}+\sqrt{\beta}+\sqrt{\gamma}}{2})^2+b(\tfrac{\sqrt{\alpha}+\sqrt{\beta}+\sqrt{\gamma}}{2})\\
=\ &\tfrac{1}{16}(\alpha+\beta+\gamma+2\lambda)^2+\tfrac{a}{4}(\alpha+\beta+\gamma+2\lambda)+\tfrac{b}{2}(\sqrt{\alpha}+\sqrt{\beta}+\sqrt{\gamma})\\
=\ &\tfrac{1}{16}(-2a+2\lambda)^2+\tfrac{a}{4}(-2a+2\lambda)-\tfrac{1}{2}(\sqrt{\alpha}\sqrt{\beta}\sqrt{\gamma})(\sqrt{\alpha}+\sqrt{\beta}+\sqrt{\gamma})\\
=\ &\tfrac{1}{4}(-a+\lambda)^2+\tfrac{a}{2}(-a+\lambda)-\tfrac{1}{2}\mu\\
=\ &\tfrac{1}{4}(a^2-2a\lambda+\alpha\beta+\beta\gamma+\gamma\alpha+2\mu)+\tfrac{a}{2}(-a+\lambda)-\tfrac{1}{2}\mu\\
=\ &\tfrac{1}{4}(a^2-2a\lambda+a^2+4c+2\mu)+\tfrac{a}{2}(-a+\lambda)-\tfrac{1}{2}\mu\\
=\ &\tfrac{1}{4}(4c+2\mu)-\tfrac{1}{2}\mu\\
=\ &c\end{aligned}$$

が成り立ちますから、四次方程式 (4) に対して、

$$\boxed{x=\frac{\sqrt{\alpha}+\sqrt{\beta}+\sqrt{\gamma}}{2}}$$

が解となります。α、β、γ の平方根の採り方には四通りの自由度がありますから、一般には四つの解が得られるのです。詳しくいうと、$\sqrt{\alpha},\ \sqrt{\beta},\ \sqrt{\gamma}$ を一組み固定したとき、$(\sqrt{\alpha}+\sqrt{\beta}+\sqrt{\gamma})/2,\ (\sqrt{\alpha}-\sqrt{\beta}-\sqrt{\gamma})/2,\ (-\sqrt{\alpha}+\sqrt{\beta}-\sqrt{\gamma})/2,\ (-\sqrt{\alpha}-\sqrt{\beta}+\sqrt{\gamma})/2$ の四つが解を与えているのです。四次方程式も四則演算と根号を用いて解けましたね。 — カンゲキ! —

四次方程式の解の公式は、かなり面倒な表示になりますが、原理的には作ることが出来ますね。三次・四次方程式の解の公式については、昨年の体験学習の際の、木村達雄教授による明解な解説もこの冊子に載るそうですので、そちらも参照してください。 — ハーイ! —

9　代数方程式（五次以上の方程式の巻）

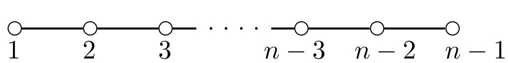
さて、こうして三次、四次ときまして、では五次は？ と当然なる訳ですが、さてさて、これが難物でありまして、多くの研究者の努力も虚しく、なかなか公式が発見できません。そういう中で、十九世紀、アーベル（Abel）やガロア（Galois）は、当時としては “とんでもない” 発見をしたのです。そもそも、解の公式には四則演算と根号のみが許されていたのですが、この意味を徹底的に追求する必要があったのです。四則演算と根号を組み合わせて、新しい数を探していくということを、数の拡大と解釈して、一定の条件をもつ拡大（現在では、アーベル拡大と呼ばれているもの）を、次々に行なっていくことが、解の公式を導くことに対応しているのだ、ということが発見されたのです。その条件を上手に数学的に述べるには、当時はまだ必要な概念が明確には確立されていませんでした。これは、今では “群” と呼ばれている概念のことです。ピタゴラス数の所でも、解すなわちピタゴラス数の間の変換を考えましたが、ここでも n 次方程式の解の変換を考えます。その代数的な構造（現在では、ガロア群と呼ばれているもの）を調べることにより、n が 5 以上ならば、n 次方程式は、四則演算と根号だけを用いたのでは、一般には解に到達できないことが証明されてしまったのです。かくして、解の公式の発見合戦には、一応の終始符が打たれたのです。しかし、それは話の終りではなく、現代代数学の大きな出発点でした。彼らの概念の導入により、代数学が飛躍的に進歩したのです。 — フムフム! —

10　組み紐

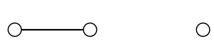
組み紐って聞いたことがありますか？ 単なる紐を組むのです。或は、編むといった方がピンと来るかも知れません。長い髪を頭の後ろで三つ編みにしている姿を想像して下さい。要するに三本の束を、上手に組み合わせて編んでいるわけですね。組み紐とは、n 本の紐を組み合わせて、順々に編んでいくものです。しかし、編んでいるつもりが途中から気づかずに、ほどいていたりすることもあるでしょう。実はこの組み紐、これも重要な数学の研究対象なのです。組み紐群と呼んだりします。また “群” が出て来ましたね。そして、この代数構造において、$n \leq 4$ の場合と $n \geq 5$ の場合とでは、決定的に違う部分があります。えっ、もう何かに気がつきましたか？そう、この事実が五次以上の代数方程式に対する解の公式の非存在と、綺麗に対応しているのですよ。驚きましたか？ — オドロキ・モモノキ! —

さらに、n 本の組み紐に対して、ある代数的解釈として、$n-1$ 個の頂点と辺からなる図形が描けます。実際、それは

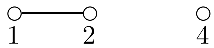
（∗）



となります。部分図形とは、幾つかの頂点と、そこから出る全ての辺を取り除いて出来る図形のことです。この図形（∗）が



という部分図形を含んでいるか否か？ この性質が大切なのです。$n \geq 5$ ならば、確かに



として含んでいますね。$n \leq 4$ なら駄目ですね。こんな簡単な仕掛けが、解の公式の存在・非存在と密接な関わりがあるのです。代数って、すごいでしょ！ またまた、驚きましたか？ — ビックリ! —

11　おわりに

面白かったですね。代数学の小さな旅でしたが、楽しめましたね。大学でもっと数学を学んでみたいたいですね。もっと代数を勉強したいですね。もっと "群" について知りたいですね。僅か二日間ですが、今回の体験学習を大いにエンジョイしていって下さい。ではまたお会いしましょう。そう、この筑波大学でネ！　　: –)

数学を楽しむことは、最高に幸せなことである。 — 作者不詳 —