整数論の基本定理 って知ってますか？

小川 裕之　(大阪大学大学院 理学研究科)†

§0　整数論の基本定理って知ってますか？

整数論の基本定理とは「1 より大きいすべての自然数は、ただ一通りの仕方で素因数分解できる」と言う定理で、知らない人はいないでしょう。証明もほとんどの人が知っているでしょう。でもまぁ、しばらく、話に付き合ってみてください。

§1　整数論の基本定理の証明

証明を思い出してみましょう。いや、元い（もとい）。学習指導要領によると、証明はしていない（しなくていい）ことになってました。たくさん計算して、なんとなくわかったことにせよ、って書いてあるのでした。でも、証明習ったような気がしませんか？

先生　素因数分解の話をします。え〜、n を 1 より大きい自然数とします。
生徒　え？ え〜えぬ。n って 何で 1 より大きいの？
先生　自然数やから、1 以上やん。ええか？
生徒　1 は？ 1 ってどうなったん？
先生　ええねん、1 個ぐらい、放っとけ
生徒　え〜〜
先生　n が素数やったら、もうお終いやから、素数でないとしましょう。
生徒　うんうん。
先生　素数やないから、2 つの自然数の積で表したとき、どっちも 1 やないようにできるよね。
生徒　何でやったっけ？
先生　素数の定義やん。もう忘れたんか。
生徒　2 つの自然数の積で表したとき、どっちかが 1 になるんやったっけ？
先生　やったっけって、それぐらい覚えとけ。
生徒　でも何で素数の定義が関係すんの？ 素数やなかったらって話やったやん。
先生　頭ん中、なに入ってんねん？ 豆腐か？
生徒　豆腐ちゃう。みそ、やなくて、脳みそ。脳みそちゃんと入っとる。
先生　素数やないから、素数の定義が満たされへんってこと。
生徒　ええわもう。わかったことにしといたる。
先生　さっきから思っててんけど、なんや知らんえらい偉そうやな。
生徒　偉いもん。
先生　ななななな。ほんならこの先続けてみぃ。
生徒　ところで、n ってどうなったん？
先生　知らんわい！

1.1　仕方ないので続けましょう。n は素数でないので、1 より大きい自然数 n_1, n_2 で $n = n_1 \times n_2$ と表すことができます。n_1 と n_2 のどちらも素数なら、$n = n_1 \times n_2$ が素因数分解になります。どちらか一方、あるいは両方ともが素数でないなら、同じように 1 より大きい自然数の積で表して、素数になったかどうか調べます。これをどんどん繰り返すのですが、1 より大きい自然数は 2 以上ですから、$n = n_1 \times n_2$ において、$n_1 \geqq 2$ だから、 $n_2 = n/n_1 \leqq n/2$ です。

† 〒 560-0043 大阪府豊中市待兼山町 1-1　　ogawa@math.sci.osaka-u.ac.jp
2022 年 10 月　於 奈良高等学校

同様に $n_1 \leqq n/2$ です。つまり、素数でない自然数を１でない２つの自然数の積に分ける度に、その２つの自然数の大きさが半分以下になります。n 以下の自然数の個数は有限個 (n 個) なので、こうやって分ける操作を無限回続けることはできません。１より大きい自然数の積に分けることができなくなったということは、その数が素数になったということです。

1.2　背理法で証明してみます。帰納法をちょっと変形したような方法です。素因数分解できない１より大きい自然数があったとして、そういう自然数の中で最小のものを n とします。n が素数なら、素因数分解できているので、n は素数ではありません。そこで $n = n_1 \times n_2$ (n_1, n_2 は１より大きい自然数) と積に分けることができます。$n_1 \geqq 2, n_2 \geqq 2$ なので $n_2 = n/n_1 \leqq n/2 < n$, $n_1 = n/n_2 \leqq n/2 < n$ なので、n_1, n_2 は素因数分解できます。n_1, n_2 の素因数分解を使って n を素数の積であわらすことができるので、n も素因数分解できることになります。これは矛盾なので、１より大きいどの自然数も素因数分解できることになります。

§２　一意性（ただ一通りの ••• ）は？

素因数分解できることは証明しましたが、それがただ一通りであることはまだ示していません。

2.1　一通りであることを見る前に、なぜ１を省いたのでしょう。素数の定義にもさりげなく１が入っています。ある１より大きい自然数を２つの自然数の積で表したとき、２つの自然数のうち一方が必ず１であるとき、その自然数を素数と定義します。あるいは、同じ定義ですが、約数が１と自分自身に限る１より大きい自然数を素数と言います。１と言うのは特別な自然数です。どの自然数の約数でもあるし、どの自然数を何回でも割り切ります。逆数もまた自然数だからです。逆数が自然数の１に対して、割り切るかどうかと言う問いは無意味なのです。約数、倍数や素数、素因数分解などで、特別な自然数として１を区別する必要があるのです。

2.2　さて、素因数分解の一意性、素因数分解の仕方が掛け算の順序を除いてただ一通りであることの証明を考えましょう。••• その前に素因数分解できたことと、素数の定義の必然的な関係を押さえておきましょう。最初に与えられた自然数よりも小さい自然数の個数が有限なので、小さいものの積に分けていく操作は、有限回で終わり、あるところから続けることができなくなります。その止まったところ、それ以上分けることのできなくなった自然数が素数です。素数の定義は因数分解を続けていく過程で自然に現れます。積に関して自然数の構成要素の最小単位が素数で、素数とはこれ以上分割できない自然数です。この意味で素数が定義されていますが、後述するように**既約**な数と呼ぶ方が適しています。積が定義された数の集合の世界で、素因数分解と素数（既約元）にあたるものを考えることは、本質的かつ根源的な問題です。

2.3　自然数には**積**が定義されています。**和**と**差**も定義されています。和と差は、自然数だけで考えるより、零や負の整数も含めた整数全体の集合の中で見た方が合理的です。整数全体の集合は、和差積の３つの演算が定義された世界です。和差積の定義された数の集合を**環**と言います。和差積が定義されていることを込めて、整数全体の集合を**整数環**と呼び、記号 $\mathbb{Z}$ で表します。同様に多項式全体の集合も、和差積が定義され、**多項式環**と呼ばれます。多項式環の場合は、変数の個数、係数に許される数の集合（整数、有理数、実数など）によって、さまざまなものがあり、扱い方が異なります。ついでに、有理数全体や実数全体の集合のように、和差積商の四則演算が定義された世界を**体**と言います。有理数全体の集合を**有理数体**、実数全体の

集合を**実数体**と呼びます。環には素因数分解に関係なさそうな和差が定義されていますが、和差があるが故に素因数分解と一意性は個々の環の特徴を知るための最初の一歩になります。

2.4　§1 で素因数分解が可能であることを証明しましたが、最も重要だったのは、**有限性**です。因数分解（ある数を 2 数の積で表すこと）を繰り返す過程で、数がどんどん小さくなるけど、とりうる数が有限個に限られることから、因数分解が有限回で止まってしまい、素因数分解できることが示されたのでした。2 つ目の証明では「最小の … 」を選ぶことのできる根拠に有限性が使われています。整数環 $\mathbb{Z}$、有理数を係数とする多項式環 $\mathbb{Q}[x]$、実数を係数とする 1 変数多項式環 $\mathbb{R}[x]$、少しややこしい環 $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}$ や $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ などでは、素因数分解が可能です。ところで、**既約多項式**と言いますが、素多項式とは言いません。§3 で話しますが、**素**と言わないことに意味があります。

§3　素因数分解の一意性の証明

前節で、素因数分解が定義される環（和差積の定義された数の集合）の話しをしました。整数論の基本定理は、整数環において、素因数分解できて、それが一意的であると言う定理でした。一意性の証明がまだ残っています。

3.1　1 より大きい自然数、例えば 12 で、素因数分解の一意性について考えましょう。素因数分解可能であることの証明に従うと、12 を 2 つの数の積で表すことから始めます。$12 = 2 \times 6$ で、2 は素数だけど、6 は素数でなくて $6 = 2 \times 3$ となって、2 と 3 はどちらも素数だから、ここでお終い。12 の素因数分解は $12 = 2 \times 2 \times 3$ となります。でも、$12 = 3 \times 4$ で、3 は素数だけど、4 は素数でなくて $4 = 2 \times 2$ となって、2 は素数だから、ここでお終い。12 の素因数分解は $12 = 3 \times 2 \times 2$ となります。因数分解での分け方によって、さまざまな形になりそうです。上の 12 では 2 通りの分け方で 2 種の素因数分解が得られました。積の順序を気にしなければ、それらは同じ形と言えます。素因数分解の一意性とは、積の順序を気にせず、うまく並べ替えれば一通りの形になると言うことです。

3.2　上の計算で 12 の場合が証明できたように見えますが、上の計算だけでは不十分です。素因数分解が存在することを示した手続きに従って 2 通りの計算をしただけで、2 つの点で不十分です。ひとつ目の問題点は、手続きに従ったとしても全ての場合を尽くしていることが述べられていません。たまたま見つけた 2 通りを計算しただけのことです。ふたつ目の問題点は、素因数分解の存在することを示した手続き以外に素因数分解を与えることができるかどうか検討されていません。手続きに従って調べた場合は、そもそもその手続き以外に方法があるのかどうかなどを検討する必要があります。たまたま出会った手続きに従って見つかったものが全てであるとは限らないことをいつも心に留めておいてください。

3.3　一意性（ある性質を満たすものがひとつだけであること）を示す方法は、ふたつあったとして結局同じ … 、とか、異なるのがふたつあったら矛盾が生じる … 、とか。

（証明） $n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ (p_1,p_2,$\cdots$,p_r, q_1,q_2,$\cdots$,q_s は素数) とふた通りの素因数分解が見つかったとします (①)。n は p_1 で割り切れるので、$q_1 q_2 \cdots q_s$ も p_1 で割り切れます (②)。p_1 は素数なので、$q_s \neq p_1$ ならば、$q_1 q_2 \cdots q_{s-1}$ は p_1 で割り切れます (③)。続けて、$q_{s-1} \neq p_1$ ならば、$q_1 q_2 \cdots q_{s-2}$ は p_1 で割り切れます (④)。これを繰り返すと、q_1,q_2,$\cdots$,q_s の中に p_1 と同じ素数が

現れます (⑤)。$q_1, q_2, \cdots, q_s$ を適当に並べ替えて $q_1 = p_1$ とします (⑥)。$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ の両辺を $p_1 = q_1$ で割って、$p_2 \cdots p_r = q_2 \cdots q_s$ となります (⑦)。$p_2 \cdots p_r = q_2 \cdots q_s$ の素因子 p_2 について同じことをすると、$q_2 = p_2$ とできます (⑧)。これを繰り返せば、$r > s$ では $p_{s+1} \cdots p_r = 1$ となり、$r < s$ では $1 = q_{r+1} \cdots q_s$ となるので、$r = s$ かつ $p_1 = q_1, \cdots, p_r = q_r$ でなければならない (⑨)。素因数分解の一意性が示されました (⑩)。

3.4　ここからが本題。上の証明の中にギャップがあります。前提条件である、和差積の定義された整数環、素因数分解できることの証明、素数の定義から演繹できないところです。それは ③ と ⑦ です。ちなみに、① は証明の方針、② は自明、④ は ③ と同じ、⑤ は ③ の繰り返し、⑥ は有限個のものの並べ替え、⑧ は ③〜⑦ の繰り返し、⑨ も自明、⑩ はまとめ。

⑦ は「整数 a, b について、$ab = 0$ ならば $a = 0$ または $b = 0$」と言う性質を必要とします。この性質を満たす環は **整域** と呼ばれます。整域でない環もたくさんあります。⑦ には、「整数環は整域である」を証明する必要があるのです。

3.5　③ は厄介です。整数 p が素数であることの定義は、命題 (I)「$p = ab$（a, b は整数）ならば $a = \pm 1$ または $b = \pm 1$」です。③ に必要なことは、命題 (P)「整数 a, b において、p が ab を割り切るならば、p は a か b の少なくとも一方を割り切る」です。比較しやすいように少し書き直すと、命題 (I)「$p = ab$（a, b は整数）ならば、$a = \pm p$ または $b = \pm p$」で、命題 (P)「$pc = ab$（a, b, c は整数）ならば、$a = px$（x は整数）または $b = py$（y は整数）」です。命題 (I) は命題 (P) の $c = 1$ の場合だけを取り出したものなので、命題 (P) を満たす数 p は、命題 (I) を満たす素数よりも強い条件を満たす数になります。代数（環論）では、命題 (I) で定義される数を **既約元** と呼び、命題 (P) で定義される数を **素元** と呼び、区別しています。「整域において、素元ならば既約元」ですが、この逆は一般に成り立ちません。③ におけるギャップは、既約元として定義した素数に、素元の性質を使っていることにあります。

§4　最後に

整数環では、命題 (I) を満たす既約元（素数）は命題 (P) を満たす素元であることが証明されます。③ のギャップを乗り越え、整数論の基本定理の証明が完結するのです。

「整数環において、既約元は素元である」

これこそが整数論の基本定理の本質です。

4.1　整数環 $\mathbb{Z}$ で既約元が素元であることの証明に使われる原理は、**余りのある割り算**とそれを基盤とした**ユークリッド互除法**です。ユークリッド互除法はもう学ばれたでしょうか？その応用として、整数論の基本定理の証明してみてください。「整数環は整域である」ことと⑦を導くところも残されてました。いろいろな証明がありますが、有理数を使わない証明を考えてみてください。多項式環 $\mathbb{Q}[x]$ や $\mathbb{R}[x]$ でも、環 $\mathbb{Z}[\sqrt{2}]$ でも、余りのある割り算が定義され、ユークリッド互除法が働き、既約元が素元であることが示され、整数論の基本定理が成り立ちます

4.2　有名な例ですが、$\mathbb{Z}[\sqrt{-5}]$ には素元でない既約元が存在し、既約元の積に分解することはできるけれど、一意的ではありません。ちょっと難しい例ですが、$\mathbb{Z}[\frac{1+\sqrt{-7}}{2}] = \{a + b\frac{1+\sqrt{-7}}{2} \mid a, b \in \mathbb{Z}\}$ は複素数の和差積で環になります。余りのある割り算が定義できず、ユークリッド互除法も使えません。でも、この環では、素因数分解可能で一意性が成り立つのです。なかなか難しい。。。