KJHM Vol. 16, No. 3, 2003, 89-94

유일인수분해에 대하여*

건국대학교 수학교육과 **최상기**

Abstract

Though the concept of unique factorization was formulated in the 19th century, Euclid already had considered the prime factorization of natural numbers, so called the fundamental theorem of arithmetic. The unique factorization of algebraic integers was a crucial problem in solving elliptic equations and the Fermat Last Problem in the 19th century. On the other hand the unique factorization of the formal power series ring were a critical problem in the past century. Unique factorization is one of the idealistic condition in computation and prime elements and prime ideals are vital ingredients in thinking and solving problems.

0. 유클리드와 유일인수분해

누가 처음으로 유일인수분해를 생각하였는가? 또 수학사에서 유일인수분해는 문제 해결에 어떤 역할을 하였으며, 어떤 문제를 제시하고 있는가? 우리는 왜 유일인수분해를 하며, 유일인수분해는 우리의 사고에 어떤 역할을 하고 있는가?

이 논문에서는 위와 같은 물음을 생각하면서, 수학사에 나타난 유일인수분해의 문제와 그의 응용을 살펴보고자 한다. 유일인수분해는 인수분해가 유일하게 되는 것을 말한다. 더 정확히 서술하면 0도 아니고 기약원도 아닌 원소가 유한 개의 기약원의 곱으로 유일하게 나타나는 것을 말한다.

정의 1. 정역 R에서 0도 아니고 단원도 아닌 모든 원소 a에 대하여 다음이 성립할 때, R을 유일인수분해정역(UFD; unique factorization domain)이라 한다.

(i) $a = p_1 p_2 \cdots p_n$, p_i는 기약원, $n \geq 1$.

* 이 논문은 2002년도 건국대학교 학술진흥연구비 지원에 의한 논문임.

(ii) $a=p_1p_2\cdots p_n=q_1q_2\cdots q_m$, p_i와 q_j는 기약원이면, $n=m$이고, 순서를 적절히 바꾸면 $p_i=u_iq_i$, u_i는 단원.

부르바키(Bourbaki)는 R이 유일인수분해정역일 때, R을 factorial이라고 불렀다. 정역 R이 정의 1의 조건 (i)을 만족시킬 때, 인수분해정역(factorization domain)이라 한다.

$Z[\sqrt{-5}]$에서 $6=2\cdot 3=(1+\sqrt{-5})(1-\sqrt{-5})$이고, 2, 3, $1+\sqrt{-5}$, $1-\sqrt{-5}$는 모두 기약원이다. 따라서 $Z[\sqrt{-5}]$는 인수분해정역이나, 유일인수분해정역은 아니다. 이와 같이 기약원 중 소원이 아닌 것이 있을 때, 인수분해가 유일하게 되지 않으며, 반대로 인수분해정역에서 모든 기약원이 소원이라는 것은 인수분해가 유일하다는 것과 동치이다.

누가 유일인수분해를 처음으로 생각하였는가? 하는 물음에 답하는 것은 간단하지 않다. 그러나 자연수가 유일인수분해의 대상으로 가장 먼저 고려되었음은 당연하다.

정리 2.(산술의 기본 정리; The Fundamental Theorem of Arithmetic) 정수환 $(Z, +, \cdot)$은 유일인수분해정역이다.

산술의 기본 정리는 가우스(C.F. Gauss, 1777-1855)가 1801년 발표한 **수론 연구**(Disquisitiones Arithmeticae)에 공식적으로 나타난다. 그러나 산술의 기본 정리는 '1보다 큰 자연수는 소수의 곱으로 나타난다.'는 것이며, 이는 유클리드에게서 찾을 수 있다.

정리 3.(Euclid, *Elements* IX, Proposition 14) If the number is the least that is measured by prime numbers, it will not be measured by any other prime number except those originally measuring it(cf. [4, p. 184], [6]).

유클리드가 정의 1에 있는 조건과 같은 소수의 곱이나 소인수의 개수에 대하여 명확히 알지 못했다고 주장하는 이도 있다. 그러나 논리적인 수식화를 너무 과신하여서는 안 된다. 유클리드에서 가우스까지는 2000년이 넘는 시간이며, 그 사이에도 사람들은 자연수의 소인수분해를 활발하게 썼으며, 그를 이용하여 많은 계산을 해냈다.

유클리드는 자연수의 소인수분해를 이용하여 $\sqrt{2}$가 무리수라는 것을 보였으며, 또한 **원론** 제9권에서 소수가 무한하다는 증명을 하였다. 이와 같은 사실들은 자연수의 소인수분해, 즉 산술의 기본 정리에 대한 유클리드의 인식을 보여준다. 뿐만 아니라, 최대공약수의 계산에서도 유클리드가 자연수의 소인수분해를 잘 이해하고 있음을 볼 수 있다.

정리 4.(Euclid, *Elements* VII, Proposition 24, Euclid Lemma) 세 자연수 a, b, c에서 a가 bc의 약수이고 a와 b가 서로 소이면, a는 c의 약수이다.

유클리드는 나눗셈을 의하여 최대공약수가 두 수의 일차결합으로 나타난다는 것을 이용하여 증명하였다. 즉, a와 b가 서로 소이므로 $1=ax+by$이고, 다음은 a의 배수이다.

$$c=c\cdot 1=c(ax+by)=cax+cby$$

즉, 정수환은 유클리드 정역이므로 단항이데알정역이고, 따라서 기약원은 소원이고 인수분해는 유일하다. 다음의 정리를 고려하면 유클리드의 정수환의 유일인수분해에 대한 인식을 이해할 수 있다.

정리 5. 인수분해정역 R에서 다음은 서로 동치이다.

(i) R은 유일인수분해정역이다.
(ii) R에서 모든 기약원이 소원이다.
(iii) R에서 임의 두 원소의 최대공약수가 존재한다.

1. 부정방정식과 페르마의 마지막 정리의 풀이에서 유일인수분해

가우스는 1832년 발표한 논문에서 가우스 정수환 $Z[i]$은 유일인수분해정역으로 단원은 1, -1, i, $-i$ 네 개이고, 소원은 다음의 3 가지 종류의 α임을 보인다.

(i) $N(\alpha)=2$인 원소. 즉, $\alpha=\pm(1\pm i)$.
(ii) $N(\alpha)=4n+1$ 꼴의 소수. 즉, $\alpha=\pm(1\pm 2i)$, $\pm(2\pm 3i)$, ….
(iii) $\alpha=4n+1$ 꼴의 소수. 즉, $\alpha=3$, 7, 11, ….

가우스의 결과와 더불어 대수적 정수환 $Z[\sqrt{m}]$의 유일인수분해성은 부정방정식의 풀이의 길잡이가 된다. 예를 들면, 펠 방정식 $x^2-dy^2=1$은 대수적 정수환 $Z[\sqrt{d}]$에서 다음과 같이 인수분해 된다.

$$x^2-dy^2=(x+y\sqrt{d})(x-y\sqrt{d})=1$$

1738년 오일러(L. Euler, 1707-1783)는 방정식 $y^2+2=x^3$을 풀었는데, 다음과 같이 시작했다.

$$(y-\sqrt{-2})(y+\sqrt{-2})=x^3$$

여기서 $y-\sqrt{-2}$과 $y+\sqrt{-2}$이 서로 소이므로 자연수에서와 같이 유일인수분해성에 의하여

$(y-\sqrt{-2})$과 $(y+\sqrt{-2})$이 삼제곱 수이다. 즉, 다음과 같다.

$$y-\sqrt{-2}=(a-b\sqrt{-2})^3,\quad y+\sqrt{-2}=(a+b\sqrt{-2})^3$$

위의 식을 풀면 $a=\pm 1$, $b=1$이며, 따라서 방정식 $y^2+2=x^3$의 자연수해는 $x=3$, $y=\pm 5$임을 밝혔다. 그러나 100년도 더 지나서야 $Z[\sqrt{-2}]$가 유일인수분해정역이라는 사실이 밝혀졌으며, 더구나 $y-\sqrt{-2}$과 $y+\sqrt{-2}$는 일반적으로 서로 소가 아니다. $2-\sqrt{-2}$과 $2+\sqrt{-2}$의 최대공약수는 $\sqrt{-2}$이다.

정리 6.(완첼, 1848년) $m=\pm 2.\ \pm 3,\ 5$일 때, $Z[\sqrt{m}]$은 유일인수분해정역이다.

그러나 $Z[\sqrt{-5}]$과 같이, 일반적으로 $Z[\sqrt{m}]$은 유일인수분해정역이 아니다. 1869년 르베그(V. A. Lesbeque)은 방정식 $y^2=x^3+7$의 자연수해가 없음을 증명하였는데 그의 증명도 가우스 정수환이 유일인수분해정역이라는 사실을 이용하였다. 르베그는 먼저 다음과 인수분해하였다.

$$y^2+1=x^3+8=(x+2)(x^2-2x+4)$$

그리고 가우스 정수환 $Z[i]$에서 $y^2+1=(y+i)(y-i)$로 인수분해하고 $4n+3$ 꼴의 자연수 소수는 $Z[i]$에서도 소원이라는 사실을 이용하여 증명하였다([1], [8]).

페르마의 마지막 정리를 풀기 위한 시도에서도 유일인수분해는 이용되었다. 1847년 3월 1일 파리 과학원의 학술회의에서 라메(G. Lame ; 1795-1870)는 언제 인수분해정역이 유일인수분해정역이 되는가? 하는 질문을 던지면서, 페르마의 마지막 정리에 대하여 다음과 같은 풀이 방법을 제시하였다.

페르마 방정식 $x^n+y^n=z^n$, $n\geq 3$은 n이 홀수 소수인 경우에만 풀면 된다. ρ를 1의 n차 원시근이라 하면, 다음과 같이 인수분해할 수 있다.

$$x^n+y^n=(x+y)(x+\rho y)(x+\rho^2 y)\cdots(x+\rho^{n-1}y)$$

만일 $Z[\rho]$가 유일인수분해정역이면, $Z[\rho][x, y]$가 유일인수분해정역이다. 이 경우 각각의 인수가 서로 소이면 그 곱이 완전 n승 꼴이므로, 각각의 인수는 완전 n승 꼴이 된다. 이 때, 더 작은 세 수 x', y', z'을 구할 수 있고, 따라서 $z'=1$이 되어 모순이다.

라메의 발표 후 리우빌(J. Lioville, 1809-1882)은 라메의 방법에 의문을 제기하였다. 즉, 일반적으로 $Z[\rho]$가 유일인수분해정역인가 하는 사실을 묻게 되었다. 곧 이어 리우빌은 쿠머(E. Kummer, 1810-1893)에게서 다음의 사실을 알리는 편지를 받게 된다[5, p. 356].

정리 7.(쿠머, 1844년) ρ가 1의 23차 원시근일 때, $Z[\rho]$가 유일인수분해정역이 아니다.

오일러는 $Z[\sqrt{-2}]$가 유일인수분해정역임에도 서로 소에 대한 인식을 잘못하여 그릇된 풀이를 착각하였고, 라메의 경우는 $Z[\rho]$가 유일인수분해정역이 아닌 것을 알지 못하여 틀린 풀이 제시하였다.

2. 멱급수환의 유일인수분해성

가우스가 유일인수분해정역 R을 계수로 하는 다항식환 $R[x]$가 유일인수분해정역임을 증명한지 100년 가까이 멱급수환 $R[[x]]$가 유일인수분해정역인가 하는 문제는 미해결의 상태였다.

정리 8. R이 유일인수분해정역이면, 다항식환 $R[x]$도 유일인수분해정역이다.

가우스의 아이디어는 R의 분수체를 F라 할 때 $F[x]$는 유클리드정역이어서 유일인수분해정역이고, $R[x]$와 $F[x]$에서의 인수분해의 차이는 $R[x]$에서 다항식의 계수들의 최대공약수인 내용(content)을 R에서의 유일인수분해로 처리하는 것이다. 그러나 가우스의 이와 같은 방법은 $R[x]$와 $R[[x]]$의 단원이 다르기 때문에 $R[[x]]$에서는 쓸 수가 없다. $R[[x]]$에서는 상수항이 단원인 모든 멱급수가 단원이다.

문제 9. R이 유일인수분해정역일 때, 멱급수환환 $R[[x]]$도 유일인수분해정역인가?

이 문제는 완비화(completion)와 코헨의 완비 국소환의 구조정리(Cohen structure theorem for complete local rings)를 기본적으로 쓰는 현대 수학의 기법으로 볼 때 더욱 중요하다. 이 문제는 1900년 초에 제기되어 1960년대에 이르러 완성되었으며, 첫 결과는 수학자이며 세계 체스 챔피언인 래스커(E. Lasker, 1868-1941)에 의하여 주어진다.

정리 10.(래스커, 1905년) R이 무한체일 때, 멱급수환환 $R[[x]]$도 유일인수분해정역이다.

1961년 사무엘(P. Samuel)과 부스바움(D. Buchsbaum)은 각각 R이 locally regular UFD 이면, $R[[x]]$가 유일인수분해정역임을 증명하였는데([3], [11]), 더구나 사무엘은 이 문제가 R이 2차원인 경우에만 문제가 되며 R이 2차원이 아닌 경우에는 성립한다는 것을 보였다 [11]. 쉐자(G. Scheja), 리프만(J. Lipman)은 이차원 국소환 중에서 문제 9가 성립하는 것을

찾아내었으며([12], [7]), 살몬(P. Salmon)은 성립하지 않는 보기를 찾았는데 다음과 같다 [10].

보기 11.([11]) k가 체일 때 $R=k(u)[[x,y,z]]/(x^2+y^3+uz^6)$은 유일인수분해정역이나, 멱급수환환 $R[[T]]$는 유일인수분해정역이 아니다.

문제 9를 해결한 위의 결과들과 더불어 1957년 오스랜더(M. Auslander)와 부스바움(D. Buchsbaum)이 증명한 regular local ring은 유일인수분해정역이라는 결과[2]도 60년 가까운 미해결의 문제를 푼 것이다. 이와 같이 오스랜더와 부스바움에 의하여 대수적인 문제의 해결에 호몰로지의 방법이 도입되었는데, Cohen-Maucaulay 유일인수분해정역은 Gorenstein이라는 무티(M. P. Murthy)의 결과[9]도 호몰로지 방법의 위력을 보여준다.

참고 문헌

1. 최상기, "부정방정식에 대하여," **한국수학사학회지** 제 16 권 제 1 호(2003), 17-24.
2. Auslander, M., Buchsbaum, D., "Homological dimensions in local rings," *Trans. Amer. Math.* 85 (1957), 390-405.
3. Buchsbaum, D., "Some Remarks on Factorization in Power Series Rings," *J. Math. Mech.* 10 (1961), 749-753.
4. Burton, D.M., *Burton's History of Mathematics*, 3rd ed. WCB 1995.
5. Fraleigh, J., *A First Course in Abstract Algebra*, 6th ed. Addison-Wesley 2000.
6. Hartshorne, R., "Teaching Geometry according to Euclid," *Notices of AMS* Vol. 47, No. 4(2000), 460-465.
7. Lipman, J., "Unique Factorization in Complete Local Rings," *Proceedings Symposia in Pure Math. AMS* vol. 29, 1975.
8. Mordell, L.J., *A Chapter in the Theory of Numbers*, Cambridge University Press, 1947.
9. Murthy, M.P. "A Note on Factorial Rings," *Arch. Math.* 15(1964), 418-420.
10. Salmon, P., "Su un Problem Posto da P. Samuel," *Atti. Accad. NAz. Lincei Rend. Cl. Sci. Fis. MAt. Natur. (8)* 40(1966), 801-803.
11. Samuel, P., "On Unique Factorization Domains," *Illinois J. Math.* 5(1961), 1-17.
12. Scheja, G., "Einige Beispiele Faktorieller lokaler Ringe," *Math. Annalen* 172(1967), 124-134.