Historia Mathematica Vol. 13, No. 2, 2000, 33-40

初期 群論의 歷史

숙명여자대학교 수학과 **홍영희**

Abstract

This paper deals with the development of early group theory. We first investigate how the concept of abstract groups has emerged as a generalization of groups of substitution(=permutation groups) which strongly relate the theory of equations.

0. 서론

수 체계의 대수적 구조는 항상 덧셈과 곱셈을 동시에 생각하고 있는 방정식의 이론을 통하여 대수학으로 발전되어 왔다. 19세기에 방정식의 이론이 치환군을 통하여 정리되는 과정에서 한 개의 연산만을 갖는 대수적 체계가 군의 개념으로 추상화가 이루어짐으로써 현대 대수학의 발전의 기원을 이루었다고 할 수 있다.

우리는 덧셈과 곱셈의 추상화로 연산이 도입되어 유니버설 대수학으로 발전되는 과정을 [23]에서 다루었다. 이 논문은 전작의 계속으로 추상군의 개념이 정립되는 과정을 살펴보고자 한다.

수의 대수적인 구조의 기본은 이항연산이다. 수학의 기록으로는 가장 오래된 고대 이집트인과 바빌로니아 사람들의 기록에도 자연수와 양의 유리수의 계산법과 길이와 넓이 계산에 대한 법칙이 나와 있으나 지금과 같은 연산으로 정확한 정의를 한 것은 아니다. 또 유클리드는 곱에 대해서 공식적인 정의는 하지 않았어도 그의 **기하학 원본**(제 6 권 정의 5)에 후에 수정 삽입한 것을 보면 그는 분명히 연산(operation)의 개념과 그 성질을 알고 있어서, 합성의 법칙의 공리적 개념은 이미 유클리드에 의하여 시작되었다고 본다.

그러나 기하의 압도적인 우세로 대수적인 기호의 독자적인 발전은 마비되었고, 계산되는 모든 원소는 기하학적으로 이해하였을 뿐 아니라 사용되는 두 개의 연산의 법칙도 같은 집

---

* 2000 Mathematics Subject Classification - 01A55, 20-03

합 위에 정의되지 않았다.

이집트인과 바빌로니아인들의 자연수의 계산을 이어 받은 디오판토스(Diophantus)는 부호의 법칙(rule of sign)을 말하고 음수의 계산을 처음 시작하였으며, 방정식에서 미지수를 문자로 처음 사용하였다. 그는 수의 기하학적 표현에 더 이상 얽매이지 않고 자연스럽게 추상대수적 계산의 법칙의 발전을 이끌었으나 연산의 법칙의 공리적인 시도의 흔적은 없다. 이후로 대수학자들이 방정식을 통해서 수의 개념을 넓혀 갔는데 이 논문의 범주 밖으로 한다.

16세기 초에 이탈리아의 수학자 페로(Scipione del Ferro)와 타르탈리아(Nicolo Tartaglia)의 방법의 영향으로 카르다노(Girolamo Cardano, 1501-1576)와 그의 제자 페라리(Lodovico Ferrari)가 3차 방정식과 4차 방정식의 해를 구하는 공식을 찾았으나, 그들 역시 허수의 도입에 대하여 불편한 느낌이었고, 두 세기 이상을 허수는 불가능한 수로 생각되어져 왔다. 다항방정식에서 x를 미지수로 표현하는 것은 데카르트(Decartes, 1596-1650)에 기원한다[6]. 그보다 전에 비에트(Viète, 1540-1630)가 처음으로 대수적인 문제에서 모든 원소를 문자로 사용하여 일반적인 법칙을 설명하는 방법으로 사용했다[17]. 또 일찍부터 추상대수적인 구조(체의 구조)는 원소들의 연산법칙들에 의하여 따로 정의되었다. 예를 들면, 1560년 봄벨리(Bombelli)의 **대수학**(Algebra)에는 이미 복소수들의 덧셈과 곱셈에 대한 법칙이 설명되어 있다[19].

체의 추상적인 개념이 일찍 발견된 데 비하여 군론은 다른 길을 통하여 만들어졌다. 추상군론의 발전의 역사적 뿌리는 19세기의 다항방정식론, 정수론과 기하학에 있다. 다항방정식으로부터 치환군을, 기하학으로부터 변환군의 개념을 인지하여 추상군의 개념이 정립되는 과정을 살펴보는 것이 이 논문의 목적이다.

1. 치환군과 변환군

대수방정식론에서 가장 확실한 군의 개념이 정립되기 시작하였다. 라그랑주(Lagrange, 1736-1813), 로피니(Ruffini, 1765-1822), 코시(Cauchy, 1789-1857)가 초기의 치환군에 대한 연구 결과를 많이 남겼다[19]. 이미 13세기에 아랍과 유대 문화권에서 치환에 대한 개념이 도입은 되었으나-모로코의 Abu-l-'Abbas ibnal-Banna(1256-1321)와 프랑스의 Levi ben Gerson(1288-1344) 등이 연구결과를 남겨 놓았다[8]-, 그 때는 유한집합의 단순한 배열로서의 치환(=순열)으로 생각되었다.

18세기 말에 라그랑주 등에 의하여 다항방적식의 해법을 찾는 과정에서 치환은 주어진 방정식의 해집합인 유한집합 위의 함수로 생각되었다. 치환론의 기본정리를 자세히 정리한 사람이 코시이다. 라그랑주, 루피니, 코시 등은 그들의 주된 목적인 n차 다항방정식의 해를 찾기 위해서 차수가 낮은 보조방정식을 찾아서 풀려고 하였다. 이를 위해 유리함수

$f(x_1, x_2, \ldots, x_n)$을 생각할 때 $\{x_1, x_2, \ldots, x_n\}$의 치환으로 생길 수 있는 서로 다른 f의 값을 $f_1, f_2, \ldots, f_s$ 라 하면 이들이 차수가 s인 보조방정식 $(t-f_1)(t-f_2)\cdots(t-f_s)=0$의 해가 되므로 라그랑주 등은 이 s가 될 수 있는 수에 관심을 쏟았다. 위의 유리함수 $f(x_1, x_2, \ldots, x_n)$에서 $H=\{\sigma \in S_n \mid f(x_1, x_2, \ldots, x_n)=f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})\}$라 하면 H는 S_n의 부분군이고 $s=[S_n : H]$, 즉 S_n에서 H의 지표(index)이다.

많은 수학자들이 카르다노와 페라리의 3차·4차 방정식의 해법과 비슷한 방법으로 5차 방정식의 거듭제곱근을 이용한(by radicals) 해법을 찾으려고 노력하였다. 1770년에 라그랑주가 3차·4차 방정식의 경우에만 보조방정식의 차수(즉 위의 S_n의 부분군 H의 지표 s)가 2차, 3차가 되는 유리함수 $f(x_1, x_2, \ldots, x_n)$이 존재하기 때문인 것을 알아내었다. 5차 방정식의 공식을 찾을 수 없다는 것은 라그랑주의 제안에 따라 루피니가 증명하여 1799년 그의 책에 발표하였다. 그러나 불행히도 그의 증명은 불완전하였고, 후에 1824년과 1826년에 아벨(Abel, 1802-1829)이 증명을 완성하여, 두 세기에 걸친 문제가 해결되었다.

아벨은 다항방정식의 거듭제곱근을 이용한 가해성의 필요충분조건은 이 방정식의 갈루아군이 가해(solvable)인 것을 1829년에 발표했는데[1], 같은 해에 갈루아(Galois, 1811-1832)가 갈루아 이론의 증명을 Academy of Paris에 제출하였다. 그러나 제출한 논문은 코시가 잃어버리고, 1830년 4월에 Bulletin des Sciences mathématiques of Férussac에 갈루아는 증명 없이 그의 결과를 short note 형식으로 발표하였다. 이 논문에서 그는 소수차 다항방정식의 거듭제곱근을 이용한 가해성의 필요충분조건은 만일 두 개의 해를 안다면 나머지 해들은 이들의 유리식으로 나타나는 것이라고 주장하였다. 이 정리는 5차 방정식의 거듭제곱근을 이용한 불가해성을 함의한다. 같은 해 6월 그는 같은 잡지에 유한체의 구조를 확정하는 논문[10]을 발표하였다. 1831년 갈루아는 그의 결과를 "Mémoire sur les conditions de résolubilité des équations par radicaux"로 개정하여 Academy of Paris에 제출하였다. 한편 Academy of Paris에서 푸아송(Poisson)과 라크루아(Lacroix)에게 심사 의뢰하였으나 푸아송은 매우 자세히 읽었으나 이해할 수 없다고 보고하였다. 그가 죽은 뒤 1846년에 리우빌(Liouville, 1809-1882)에 의하여 그의 *Journal de Mathématiques pures et appliquées*에 갈루아의 논문[11]을 발표한 후에야 갈루아 이론이 알려졌고, 이후로 대수학의 연구가 대수적인 구조의 연구로 방향을 잡아서 추상화의 길을 걷게 되었다. 실제로 위의 아벨의 결과는 갈루아의 결과의 특별한 경우이고, 오늘날 우리가 알고 있는 갈루아 이론은 1926년에 아르틴(Artin, 1898-1962)이 데데킨트(Dedekind)가 도입한 체의 자기동형사상을 이용하여 정리하여 발표하고 이는 반 데르 베르덴(van der Waerden)이 1930년에 출판한 대수학 책[18]에 그 결과가 정리되었다.

한편 오일러(Euler, 1707-1783)와 로드리게스(Olinde Rodrigues)는 3차 공간에서 강체운동(rigid motion)의 군의 구조에 대한 연구를 하였고, 이어서 조르당(Jordan, 1838-1922)은 이 군의 폐부분군의 조직적인 연구를 하여 변환군의 개념을 발표하였다. 군이라는 용어는 조르

당이 "group of geometrical transformations"의 개념으로 처음 사용된 것으로 추정된다[19].

케일리(Cayley, 1821-1895)는 치환군에 대한 많은 업적을 남겼지만 변환군에 대한 연구도 많이 하였다. 그는 사영기하학을 정의하고, 사영변환의 군을 도입하였다[3]. 한편 클라인(Klein, 1849-1925)은 분수선형변환(fractional linear transformations)의 유한군을[13], 또 리(Lie, 1842-1899)와 함께 선형변환군에 대한 연구를 하였다[14].

치환군과 변환군 이외에도 군론의 발전에 영향을 준 결과로는 오일러가 1761년에 발표한 "Theorems on the residues left by the division of powers"와 가우스(Gauss, 1777-1855)가 1800년에 발표한 "Disquisitione Arithmeticae"을 빼놓을 수 없다. 이 들은 각각 군의 성질을 갖는 대상을 다루었다.

대수방정식의 풀이에 대한 아벨과 갈루아의 연구의 중요성을 그 당시 제대로 인식한 독일 수학자는 크로네커(Kronecker, 1823-1891)와 데데킨트(Dedekind, 1831-1916)이었다. 1870년에 크로네커는 교환법칙과 결합법칙에 대해서 분명히 설명하여 가환군을 다루었다[15]. 또 데데킨트는 1871년에 디리클레(Dirichlet, 1805-1859)의 정수론에 관한 책에 부록으로 체(field)를 두 개의 이항연산 +와 ×를 갖는 실수나 복소수의 집합으로 정의하였다. 실제로 크로네커나 데데킨트 두 사람 모두 이보다 먼저 1850년대에 이런 개념에 대하여 강의는 하였다고 한다. 체에 대한 추상적인 정의는 1893년 베버(Weber, 1842-1913)가 처음으로 도입하였다.

2. 추상군의 도입

이 절에서는 추상군이 도입되는 과정을 알아본다.

추상군의 정의에 가까운 것은 케일리가 1854년에 발표한 논문[4]에서 다음과 같은 정의를 한 것이다. "서로 다른 기호(symbol) 1, α, β, …의 집합과, 그리고 원소의 곱이 다시 그 집합에 속하는 것을 군이라 한다." 즉 이항연산이 정의된 집합을 군으로 본 셈이고, 또 그가 쓴 기호 1, α, β, …는 여전히 치환을 나타내고 있어서 추상군의 정의로 보기는 어렵다. 1878년에 *American Journal of Mathematics*(vol. 1)에 발표한 논문 "The Theory of groups"에서 케일리는 좀더 발전된 군의 정의를 다음과 같이 발표하였다[5].

"A set of symbols α, β, γ, … such that the product $\alpha\beta$ of each two of them (in each order, $\alpha\beta$ or $\beta\alpha$) is a symbol of the set, is a group …. A group is defined by the laws of combination of its symbols."

또 이 논문에서 현재 우리가 케일리의 정리라고 부르는 "위수(order)가 *n*인 유한군은 대

칭군 S_n의 부분군과 동형"임을 곱셈표(multiplication table)를 사용하여 증명하였다. 이 논문에 보이는 군의 정의에서는 결합법칙을 따로 설명하지 않고 당연한 가정으로 사용하였다. 그의 마음속에는 유한군의 추상적인 개념이 있었을지도 모르지만 곱이 갖는 조건을 분명히 나타내지는 못하여서, 1870년에 크로네커가 사용한 가환군의 정의보다도 표현이 분명하지 못했다[15].

1882년에 폰 디크(von Dyck, 1856-1934)와 베버(Weber, 1842-1913)에 의하여 군의 추상 개념이 정확히 정의되었다. 두 사람은 거의 동시에 추상군의 공리적인 정의를 하여 같은 논문집 *Mathematische Annalen*(vol. 20)에 발표하였는데, 디크는 1881년 12월, 베버는 1882년 5월에 논문을 완성하였다. 그들의 정의는 전혀 다른 말로 표현이 되어 있었는데, 특히 베버의 정의는 유한군으로 제한되어 있었다.

디크는 그의 논문 [7]의 첫머리에 케일리[5]로부터 “A group is defined by means of the laws of combination of its symbols.”를 인용하고, 바로 이어서 다음과 같은 그의 주된 관점을 쓰고 나서 군을 정의했다.

> “To define a group of discrete operations, which are applied to a certain object, while abstracting from any special form of representation of the single objects and supposing the operations to be given only by those properties that are essential for the formation of the group.”

유한 개의 생성원(generating elements)과 항등원 1, 그리고 역원의 존재성을 가정하여 그가 정의한 이산군(discrete group)은 바로 오늘의 유한생성군(finitely generated group)이다. 실제로 그는 오늘날 우리가 쓰고 있는 유한 개의 원소로 생성되는 자유군 (free group)을 만들고, 유한생성군은 이 자유군의 상군(quotient group)이 됨을 보였다. 그의 유한생성군은 생성원 $A_1, A_2, \cdots, A_n$과 그 역원 $A_1^{-1}, A_2^{-1}, \cdots, A_n^{-1}$들의 word로 군을 얻어내었다. 물론 이는 오늘날의 유한생성군과 같지만, 그는 군의 정의를 하지는 않고, 군을 연산의 법칙으로 정의될 수 있음을 인지하였다.

베버는 [20]에서 다음과 같이 군을 정의하였다.

> “A system G of elements of any kind, $\Theta_1, \Theta_2, \cdots, \Theta_n$ is called a group of order n, if it satisfies the following conditions:
>
> 1. From any two elements of the system one derives a new element of the same system by a prescription, which is called composition or multiplication. In signs
>
> $$\Theta_r \Theta_s = \Theta_t.$$

2. One always has $(\Theta_r\Theta_s)\Theta_t = \Theta_r(\Theta_s\Theta_t) = \Theta_r\Theta_s\Theta_t$.

3. From $\Theta\Theta_r = \Theta\Theta_s$ or from $\Theta_r\Theta = \Theta_s\Theta$ it follows that $\Theta_r = \Theta_s$."

위의 공리로부터 베버는 항등원과 역원의 존재성을 유도하고 유한군의 정의를 확정하였다.

한편 노르웨이의 수학자 실로우(Sylow, 1832-1918)가 1872년에 지금 우리가 실로우의 정리라고 부르는 정리들을 발표했는데[16], 이 때도 추상군의 정의가 완성되기 이전이므로 그의 정리는 치환군에 관한 것이었다. 프로베니우스(Frobenius, 1849-1917)는 1887년에 4개의 공리로 추상 유한군을 정의하였다[9]. 그는 케일리의 정리에 의하여 유한군이 치환군으로 표현되는 것을 알고 있었지만, 유한군에 대한 실로우의 정리를 다시 증명하여 *Crelle's Journal für Math.*(vol. 100)에 발표하였다.

그 후 1893년 베버는 [21]에서 유한군을 벗어나 임의의 군을 다음과 같이 정의하였다.

"A system S of things (elements) of any kind in finite or infinite number becomes a group, if the following assumptions are fulfilled:

1) A prescription is given, according to which from any first and second element of the system a definite third element of the same system is derived."

이 때 두 원소 A와 B의 곱을 AB로 나타내고, 그는 교환법칙을 가정하지 않는다고 하였다.

"2) The associative law is assumed ….

3) It is supposed that, if $AB=AB'$ or $AB=A'B$, then necessarily $B=B'$ or $A=A'$ must hold.

4) If two of the three elements A, B, C are taken arbitrarily in S, the third can always be determined in such a way that $AB=C$ holds."

베버는 유한군에 대하여 4)가 1)~3)에 의하여 유도됨을 보이고, 그는 다음과 같이 말하였다.

"For infinite groups this proof is not conclusive. For infinite groups we will include the property 4) as a postulate in the definition of the notion group."

실제로 그의 정의는 1886년에 출판한 그의 책 *Lehrbuch der Algebra* Vol. II에 이미 나타나 있다.

그 후, 1897년에 번사이드(Burnside)가 *Theory of Groups*를 출판한 후에 군론은 최초로 발달한 추상대수학의 부문이 되었다.

3. 결론

추상대수의 구조가 일찍부터 연산의 법칙에 따라 정의되고 설명되었음에도 불구하고, 수의 사칙연산에서 벗어나서 한 개의 이항연산의 공리로 구조를 정의하는데는 많은 시간과 연산구조의 경험을 거쳤다.

19세기에 수학의 전 분야에 걸쳐서 이론의 재정립이 이루어지는 과정과, 방정식의 이론이 치환군으로, 기하학이 변환군을 통하여 정리되는 과정을 따라서 군의 개념이 서서히 정립되었다. 그 중에 크로네커, 케일리, 폰 디크, 베버, 프로베니우스 등에 의하여 추상군이 정의되었다. 그러나, 그들은 여전히 공리적인 접근과는 상당한 거리를 두고 있고, 치환군의 부분군을 항상 머리 속에 두고 있어서, 결합법칙이나 역원의 존재성을 정의에 넣지 않고 당연한 것으로 받아들이고 군의 성질을 규명하고 있었다. 그러나 폰 디크는 오늘날의 자유군과 그의 상군으로 군을 정의하고, 자유군을 분수선형변환군의 부분군으로 표현할 수 있음을 보일 정도로 군의 정확한 정의 없이 군의 구조에 대한 훌륭한 결과를 얻어내었다. 또 베버는 역원의 존재성 대신에 유한군은 모든 원소가 소거법칙을 만족한다는 것으로 정의하고, 이는 "모든 원소 a와 b에 대하여 $ax=b$의 해가 존재하는 것"을 함의하고, 무한군에서는 소거법칙 대신에 위의 방정식의 해의 존재성으로 군을 정의하였다. 이는 가장 단순한 명제를 정의로 택하지 않고 방정식에 관심을 가지고 있었음을 알 수 있다. 20세기에 들어와서 군론은 급속한 발전을 이루고, 추상대수학의 가장 중요한 부분으로 자리를 차지하게 된다.

참고 문헌

1. Abel, N.H., "Mémoire sur une classe particulière d'équations résoluble algébriquement," *Crelle's J. für Math.*, 4(1829), 478-514.
2. Bourbaki, N., *Algebra I*, Addison-Wesley, Paris, 1973.
3. Cayley, A., "Sixth Memoir upon Quantics," *Philos. Transactions of the Royal Society*, Vol. 149, 1859.
4. Cayley, A., "On the theory of groups, as depending on the symbolic equation $\theta^n = 1$," *Philos. Magazine of the Royal Society London*, 7(1854).

5. Cayley, A., "The theory of groups," *Amer. J. Math.* 1(1878), 50-52.
6. Descartes, R., *Discours de la Méthode* (La géométrie), 1637.
7. Dyck, W. von, "Gruppentheoretische Studien," *Math. Annalen,* 20(1882), 1-44.
8. Fraleigh, J.B., *A First Course in Abstract Algebra* (with historical notes by Victor Katz), 5th. ed., Addison-Wesley, 1993.
9. Frobenius, G., "Neuer Beweis des Sylowschen Satzes," *Crelle's J. für Math.,* 100 (1887), 179-181.
10. Galois, E., "Sur la théorie des nombres," *Férussac's Bulletin,* (1830), 15-23.
11. Galois, E., "Mémoire sur les conditions de résolubilité des équations par radicaux," *J. Math. pures et appl.,* 11(1846), 381-444.
12. Jordan, C., *Traité des substitutions et des équations algébriques,* Gauthier-Villars, Paris, 1870.
13. Klein, F., "Über biräre Formen mit linearen Transformationen in sich selbst," *Math. Annalen,* 9(1875), 209-217.
14. Klein F. and S. Lie, "Über die jenigen ebenen Kurven, welche durch ein geschlossenes System von einfach unendlich vielen vertauschbaren linearen Transformationen in sich übergehen," *Math. Annalen,* 4(1871), 424-429.
15. Kronecker, L., "Auseinandersetzung einiger Eigenschaften der Klassenzahl idealer Komplexer Zahlen," *Monat. Berliner Akad.,* (1870), 881-889.
16. Sylow, M.L., "Théorèmes sur les groupes de substitutions," *Math. Annalen,* 5(1872), 584-594.
17. Viète, F., *In artem analyticem Isagoge,* Tours, 1591.
18. Waerden, B.L. van der, *Modern Algebra,* Springer, Berlin, 1940.
19. Waerden, B.L. van der, *A History of Algebra,* Springer, Berlin, 1980.
20. Weber, H., "Beweis des Satzes, dass jede eigentlich primitive quadratische Form unendlich viele Primzahlen darzustellen fähig ist," *Math. Annalen,* 20(1882), 301-329.
21. Weber, H., "Die allgemeinen Grundlagen der Galois'schen Gleichungstheorie," *Math. Annalen,* 43(1893), 521-549.
22. Wussing, H., *Die Genesis des abstrakten Gruppenbegriffs,* Verlag der Wissenschaften Berlin, 1969.
23. 홍영희, "유니버설 대수학의 발전," 한국수학사학회지 제 12 권 제 1 호(1999), 21-31.