대수기하학

이해의 즐거움 & 중요성과 전망

Understanding Algebraic Geometry with Joy : Its Importance and Future.

글 _ **곽시종**
KAIST 자연과학대학 수리과학과 교수

In this article, we introduce the basics of algebraic geometry to the readers with the modest background knowledge. We also explain its recent developments, current research trends and perspectives with applications.

대수기하학 전반을 간략하게 기술하기란 그리 쉬운 일은 아니다. 그러나 대다수의 대수기하학자들은 전통적으로 대수기하학을 다항식들의 공통근 연구를 목적으로 가환대수를 비롯한 여러 가지 대수학적 방법론과 기하의 언어를 결합한 학문이라는 데는 의견을 일치한다. 그래서 대수기하학은 수학 전 분야를 크게 대수학, 해석학, 기하위상수학, 응용수학 등으로 나눌 때 대수학과 기하위상수학이 만나는 분야라 할 수 있겠다. 어떻게 만난다는 말인가? 저명한 수학자 G. Kempf는 그의 한 저서 서두에서 대수기하학의 특성에 대하여 다음과 같이 적고 있는데 아주 적절한 말이라 여겨진다.

"Algebraic geometry studies the delicate balance

between the geometrically plausible and the algebraically possible."

뒤이어서 다시금 대수학과 기하학의 깐깐한 긴장관계를 유지하는 것의 중요성을 다음과 같이 표현하고 있다.

"Whenever one side of this mathematical teeter-totter outweighs the other, one immediately loses interest and runs off in search of a more exciting amusement."

그렇다. 그 어려운 수학을 평생 직업적으로 연구하면서 살아가려면 흥미진진한 이해의 즐거움과 학문적 열정을 간직해야 하는데 적어도 대수기하학 분야에서는 위에서 언급한 밸런스가 중요하다는 데에 전적으로 공감하는 바이다.

대수기하학은 개략적으로 말하면 다항식들의 공통해집합을 연구하는 분야이다. 공통근을 구하는 데 있어서도 익숙한 유클리드 공간(Euclidean Space)에 원점으로부터 각각의 방향들을 무한대에 있는 하나의 점들로 간주하여 새롭게 확장된 사영공간(Projective Space)에서 방정식들의 해를 구한다. 특히 다양체들이 정의되는 체(Field)를 유리수, 실수, 복소수, 유한체, 수체, 함수체들로 바꾸어 가면서 얻어지는 해집합들을 연구하는데 필요한 대수기하학적 연구방법들과 이론을 개발한다. 그 밖의 중요한 특징으로는 특이점(Singular Point)이 있는 다양체들을 체계적으로 다루고 있다는 점과 모든 부분다양체들을 닫힌집합(Closed Set)으로 정의하는 Zariski 토폴로지를 주로 사용하고 있다는 점이다.

좀 더 수학적으로 자연스러운 질문들을 열거해 보기로 하자. 첫째, 유한개의 대수방정식들의 해집합, 즉 좀 더 쉽게 표현하면 고차 연립방정식의 해들을 연구할 때 과연 해집합이 있는지 없는지를 우선적으로 생각해보는 것은 당연하다. 이러한 해가 존재한다면, 정수해가 있는지 유리해가 있는지, 실수해(Real Algebraic Variety)가 있는지, 복소수해(Complex Algebraic Variety)가 있는지 우리는 주어진 다항식들의 해집합을 어떤 범주에서 찾고자 하는가가 우선 관심사이다. 이와 관련하여 가장 중요한 두 가지 사실들이 있는데 하나는 복소계수 일변수 다항식은 복소수 범위에서 일차식들의 곱으로 표현된다는 정리, 즉 가우스의 대수학에 관한 기본 정리(Fundamental Theorem of Algebra)가 그것이고 또 다른 하나는 힐버트의 영점정리(Hilbert's Nullstellensatz)인데 이는 주어진 복소계수 다항식들이 다항환(Polynomial Ring) 전체를 생성하지 않을 때에는 공통근이 항상 존재한다는 것을 말한다. 특히 정수계수 방정식의 정수해의 존재성은 대수다양체들의 Hodge 구조연구를 통해서도 중요한 정보를 알 수 있다.

둘째, 해가 무수히 많을 때는 이러한 해집합들은 기하학적 연구대상이 되므로 좀 더 흥미롭게 상상력을 동원하여 느끼고 만져볼 수 있다. 그런데 우리는 중 · 고등학교 시

절 어떤 연립방정식들의 해가 무수히 많을 때에는 '부정(不定)' 이라는 말로 다소 어색하게 표현했다. 이러한 용어는 수학적 상상력을 아주 가로막는 최악의 용어가 아닐 수 없다. 요즈음에는 Maple실습이 고등학교에서도 가능하지만, 대수다양체를 대략적으로 그려보려는 노력과 상상력을 훈련해서 기하학적 사고의 영역을 넓혀 줄 수 있었더라면 하는 아쉬움이 남아있다.

셋째, 대수다양체들의 기하구조 연구에서는 중요한 여러 가지 불변량들을 정의할 수 있는데 이러한 불변량들에 따라서 다양체들을 분류하고 각각의 주어진 불변량이 일정한 조건을 갖는 모든 다양체들의 집합들을 다시 대수다양체(Moduli)로 이해해서 재미있는 기하학적 성질과 대수적 구조를 연구한다. 대수기하학의 큰 특징 중의 하나는 기하학적으로 재미있는 성질을 갖는 대수다양체들을 다 모아놓으면 이러한 집합은 다시 대수다양체(Moduli)가 된다는 점이다.

왜 요즈음 대수기하학자들이 모듈라이를 좋아하는가? 다음과 같은 재미있는 말로 대신하고자 한다. "It is just like with people, if you want to get to know someone, go to their family reunion." 가장 간단한 예를 들어 설명해보자. 대학교 미적분학 시간에 3차원 공간에 있는 직선의 방정식을 표현하면서 도대체 얼마나 많은 직선들이 존재하는지를 물어보면 답을 내는 학생들이 한두 명도 되지 않는다. 위의 질문에 대해서 4차원을 이룬다고 답하기란 그리 어렵지도 않다. 그러나 4차원의 어떤 도형인가를 자세히 살펴보면 5차원 사영공간에서 2차초곡면(Quadric Hypersurface)을 이루며 가장 쉬운 Grassmann 다양체임을 아는 것도 사실은 고등학교 수학의 영역이 될 수 있다.

넷째, '이러한 다양체들을 사영공간에 자연스럽게 잘 놓일 수 있도록 주어진 다양체에서 사영공간으로 보내는 동형사상(Isomorphism)을 정의하고 사영공간에 들어있는 대수다양체들에 대해서 어떠한 방정식들이 대수다양체들을 결정하는가?' 하는 문제를 제기할 수 있다. 이러한 문제는 19세기 말-20세기 초 이탈리안 학파에 의해 시작된 고전적 대수기하학에서부터 유행하던 초보적인 Riemann-Roch 문제이며 초기에는 사영다양체들을 결정하는 방정식들이 이차식(Quadric)으로만 이루어질 조건들을 연구하다가 1984년 M. Green 교수에 의해 결정방정식들 사이의 관계(Syzygy)가 주어진 다양체의 기하구조와 밀접한 관계가 있다는 사실이 밝혀지면서 방정식들 간의 관계연구가 현재까지도 활발하게 진행되고 있다.

한편, 대수기하학의 많은 이론들이 20세기 중반 이후로는 점점 더 추상적이고 일반화하면서 혁명적인 발전을 이루었지만 일반인들은 물론 수학자들에게조차도 마치 괴물처럼 비춰지기도 하면서 한 때는 이러한 연구경향에 회의론이 대두되기도 하였다. 그러나 이러한 추상화되고 일반화된 연구방법론들은 광범위하게 수학의 다른 여러 분야 및 다른 학문영역에도 큰 영향을 주면서 현재에는 학제간 공동연구의 가교역할도 톡톡히 해내고 있다.

대수기하학의 가장 기본적인 대상인 n차원 복소사영공간은 다음과 같이 정의된다. 우선 $n+1$차원 유클리드 공간에 다음과 같은 $(x_0, x_1, \cdots, x_n) \sim (\lambda x_0, \lambda x_1, \cdots, \lambda x_n)$ 동치관계를 주어서 Quotient 공간 $\mathbb{C}^{n+1}/\sim$을 만들면 이러한 공간이 n차원 복소사영공간 $\mathbb{CP}^n$이며 유클리드공간을 완전하게 만들어 주는 컴팩트화(Compactification)된 공간이다. 물론 이러한 공간에서 방정식들의 해를 구한다는 것은 위의 동치관계 때문에 반드시 동차방정식(Homogeneous Equation)들의 해를 구해야 한다. 기하구조적으로는 $\mathbb{CP}^n = \mathbb{C}^n \cup \mathbb{CP}^{n-1}$으로 이해할 수 있는데 이때 $\mathbb{CP}^{n-1}$은 n차원 유클리드 공간의 원점에서 각각의 방향들과 일대일 대응된다. 이러한 사영공간에서는 당연하게 평행한 두 직선들은 같은 방향을 가지고 있으므로 사영공간 안에서 특히, ∞ 부분공간인 $\mathbb{CP}^{n-1}$에서 만나게 되는 것이다. 참고로 아래의 그림에서는 직육면체의 3쌍의 평행한 모서리들 또는 3쌍의 평행한 평면들이 무한대 평면 $\mathbb{RP}^2$에서 만나는 모습을 보여준다. 이때, 무한대 평면 $\mathbb{RP}^2$에 있는 세 점들은 일직선상에 있지 않다.

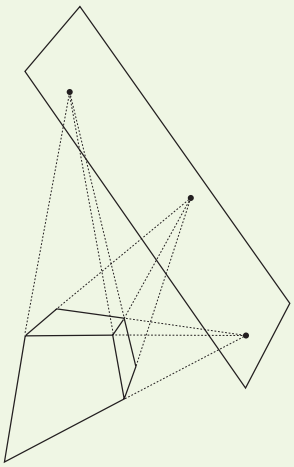
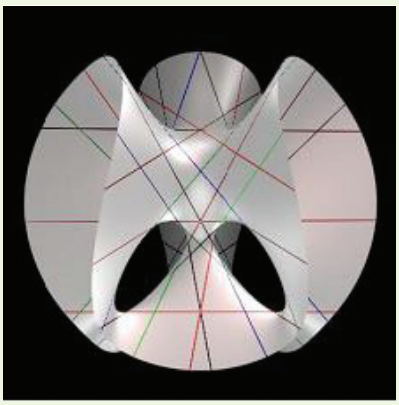


Figure 1: 직육면체의 3쌍의 평행인 면들이 무한대 평면에서 만나는 모습

이밖에도, 사영공간이 하나의 큰 운동장이라면 그 안에 살고 있는 다양한 대수다양체들에 대해서 우리는 무궁무진한 상상력과 재미있는 질문들을 쏟아낼 수 있다. 가장 간단한 사영다양체 중의 하나인 3차원 사영공간 $\mathbb{P}^3$안에 차수가 d인 대수곡면을 생각해보자. 이러한 곡면은 차수가 d인 동차방정식 $f(x, y, z, w)=0$을 만족하는 매우 간단한 집합인데 이러한 대상에 대해서도 아직 풀리지 않은 무궁무진한 문제들이 많은 연구자들을 불러들이고 있다. 물론 대수곡선은 신(God)이 만들었고 대수곡면은 악마(Devil)가 만들었다는 어느 수학자의 말도 있지만, 역시 흥미진진한 호기심 발동은 어쩔 수 없을 것이다.

일반적으로 3차원 사영공간 $\mathbb{P}^3$안에서 매끄러운 2차 곡면은 무한히 많은 직선들을 가지고 있고 매끄러운 3차 곡면은 항상 27개의 직선만을 가지고 있다. 또한 차수가 4이상 일 경우에는 일반적인 곡면이 직선을 포함하고 있지 않다. 이러한 사실들은 그리 어렵지 않게 증명이 가능하다. 그러나 차수가 4이상인 모든 매끄러운 곡면에 대해



(이태리 대수기하학자들에 의하여 연구된 27개의 직선을 포함하고 있는 3차 곡면)
Figure 2: O. Labs, www.AlgebraicSurface.net

Figure 3: 99개의 노드(node) 특이점을 갖고 있는 7차 곡면 (자료: Oliver Labs)

서 이들이 실제로 포함할 수 있는 직선들의 개수의 상한(上限, Upper Bound)을 N_d라고 할 때, B. Segre(1943)에 의해서 $N_4=64$임이 밝혀졌고 일반적으로 다음과 같은 부등식 $3d^2 \le N_d \le (d-2)(11d-6)$이 B. Segre와 Caporaso-Harris-Mazur(1994)에 의해서 알려져 있다. 실제로 가급적 많은 직선들을 갖는 대수곡면을 찾아내기란 그리 쉬운 일이 아니다. 특히, $\mathbb{P}^3$안에서 매끄러운 4차 곡면은 Calabi-Yau다양체의 한 예로써 이러한 곡면위에 존재하는 특정한 조건을 갖는 직선뿐만이 아니라 유리곡선(Rational Curve)들을 개수에 관한 문제는 일반적으로 고차원 Calabi-Yau 다양체에 존재하는 유리곡선들의 개수에 관한 문제로 확장될 수 있으며, 거울대칭(Mirror Symmetry), Quantum 코호모로지, 그리고 Gromov-Witten 이론 등을 이용해서 많은 경우 문제를 해결할 수 있게 되었으며 고전적인 Enumerative Geometry 분야의 급속한 발전을 가져왔다.

마찬가지로 3차원 사영공간 $\mathbb{P}^3$안에 놓여있는 차수가 d인 대수곡면에 대해서 고립된 (Isolated) 특이점들의 개수에 대한 최대상한(上限, Maximal Upper Bound)을 $\mu(d)$라고 하자. 예를 들어 특이점이 있는 3차 곡면(Cubic Surface)에 대해서는 이러한 특이점들이 기껏해야 4개 이하이고, 즉 $\mu(3)=4$ 그리고 특이점이 k개인 일반적인 Singular Cubic Surface들은 오직 ${}_{8-k}C_2$개의 직선들을 포함한다는 것을 초보적인 사영기하학으로도 증명할 수 있다. 일반적으로는 $\mu(d)$에 대해서 다음과 같은 사실들이 알려져 있으며 대수기하학적 알고리듬을 이용하는 컴퓨터그래픽으로 대수곡면들을 구현해 볼 수 있다 (Figure 2 참조).

$\mu(4)=16$ (Kummer, 1864)	$\mu(5)=31$ (Beauville, 1979)
$\mu(6)=65$ (Barth, 1996)	$99 \le \mu(7) \le 104$ (Labs, Givental)
In general, $\frac{4}{9}d^3 \le \mu(d) \le \frac{5}{12}d^3$ (Miyaoka, Chmutov)	

사실, 여러 대수기하학 관련분야들에 대해 소개할 때 아는 것보다는 모르는 것이 훨씬 많아서 최근에 세계 유수한 수학연구소들이 대수기하학 관련 연구들을 어떻게 활발하게 진행시켜왔는지를 알아보는 것이 큰 도움이 될 것 같다. 최근 2-3년간에 열렸던, 또는 앞으로 열릴 많은 학회나 프로그램들의 두드러진 특징은 지금까지 대수기하학에서 사용하였던 다양한 방법들 -고전적인 사영기하학, 복소기하학, 선형체계(Linear Series)방법, Moduli Spaces, 산술기하학(Enumerative Geometry), Group Actions을 갖는 대수다양체, Birational Geometry, 다양체위 유리곡선들

연구, 그리고 Minimal Model Program - 을 통합적으로 연구하려는 시도를 하고 있다는 점이다. 1990년을 전후해서 Birational Geometry에 대한 연구가 매우 활발했고, 2000년을 전후해서 Mirror Symmetry 또는 Quantum Cohomology를 주제로 한 산술기하학이 활발하게 진행되었다면, 지금은 다양하게 발전된 대수기하학의 여러 가지 방법들을 하나로 묶으려는 노력이 활발하게 진행되고 있다.

수학의 각 분야마다 연구와 창의적 사고를 주도하는 독특한 수학적 난제들이 있기 마련이다. 필자는 주로 대수다양체를 결정하는 대수방정식들 사이의 관계들이 이루는 대수적 구조가 기하학적 구조에 미치는 영향에 대해서 연구하고 있는데 사영대수기하학과 고전적 대수기하학분야에서 특히 'Syzygy and Geometry' 라고 일컬어지는 분야이다. 'Syzygy' 라는 용어는 아주 생소하고 사전에도 잘 나와 있지 않지만 천문학에서는 3개 이상의 행성들이 일직선 위에 놓여 있는 상태를 의미한다고 한다. 그러나 수학에서는 모듈(Module)의 생성자(Generator)들과 그들 사이의 관계(Relation)를 뜻하며 Sylvester가 1853년 그의 논문에서 처음 사용하였다. 대수다양체들은 사실 여러 개의 어렵고 복잡한 다항방정식들의 공통근으로 표현되므로 이들의 결정방정식들 상호간의 관계들을 따져보는 것이 자연스럽고 당연하다. $I_x=\{f\in S=\mathbb{C}[x_0, x_1, \cdots, x_n] \mid f(p)=0, \forall p\in X\}$를 주어진 다양체 X의 결정아이디얼(Defining Ideal)이라 부르는데, 이러한 아이디얼을 결정하는 방정식들을 옆으로 길게 늘어뜨려서 얻은 정보를 통해 사영대수다양체들의 구조를 들여다보려는 것이다.

이때, Hilbert Syzygy정리(1890)는 I_x의 최소자유분해(Minimal Free Resolution)는 다음과 같은 기껏해야 n번째에서 끝나게 된다는 것을 말해준다:

$0\rightarrow E_n\rightarrow\cdots\rightarrow E_2\rightarrow E_1\rightarrow Ix\rightarrow 0$, $E_i=\oplus S(-i-j)^{\beta_{i,j}}$ 이때 $\beta_{i,j}$는 i번째 단계에서 차수가 i+j인 최소생성자들의 개수를 나타내며 i번째의 차수가 i+j인 Graded Betti Number라고 부른다. 우리는 이러한 Betti Number들로 이루어진 Betti Table 통해서 주어진 다양체의 기하학적인 성질들을 밝혀내고, 특별한 성질들을 갖는 마땅히 존재해야 할 대수다양체들을 찾아내며, 여러 가지 다양체들을 분류할 수가 있다. 예를 들면, Betti Table이 가장 간단하다는 것은 $\beta_{i,j}=0$, $\forall j\geq 2$, $\forall i\geq 2$를 뜻하는데, 이것은 결정방정식들이 모두 2차식들뿐이고 모든 방정식들 간의 관계식들도 일차식들의 결합으로 생성된다는 의미이다. 이러한 가장 간단한 Betti Table을 갖는 다양체들은 최소차수다양체(Varieties of Minimal Degree)뿐이다.

20세기 초 이탈리안 학파들에 의해서 시작된 현대적인 대수기하학에서는 주로 대수곡선이나 고차 대수다양체들에 대해서 결정방정식들이 모두 이차식으로 정해지는 경우에 관심이 많았지만(Castelnuovo, M. Noether, Mumford, Fujita, Kempf, Saint-Donat etc.) 1984년 M. Green교수는 주어진 다양체들이 이차식들만을

결정방정식으로 갖고 이들의 최소자유분해에서 (p-1)번째 과정까지의 관계식이 Linear Relation들로만 이루어질 때, N_p 성질을 갖는다고 정의하였다. 보통 대수곡선의 차수(Degree)를 크게 해서 곡선을 매립(Embedding)하면 N_p 성질을 갖는다는 사실이 알려져 있으며 현재 이를 고차원으로 확장한 Mukai 예상이 중요한 미해결문제로 남아 있다. 이외에도, 대수곡선 C의 표준매립(Canonical Embedding)이 N_p 성질을 만족할 필요충분조건이 $P<Gon(C)$이 될 것이라는 Green-Lazarsfeld의 Gonality 예상이 있는데 최근에 C. Voisin을 비롯한 여러 학자들에 의해서 많은 진전이 이루어졌다. 뿐만 아니라, N_p 성질을 갖는 사영대수다양체들의 여러 기하학적 성질들이 Eisenbud-Green-Hulek-Popescu, 그리고 필자를 포함한 국내 연구진들에 의해 연구가 진행되고 있다.

한편, 임의의 사영다양체에 대해서, $\beta_{i,j}=0$, $\forall j \geq \deg(X)-\mathrm{codim}(X)+1$, $\forall i \geq 1$가 성립한다는 수학적 예상은 1900년대 초반부터 지금까지 발전해 온 고전적인 대수기하학의 가장 오래된 미해결 문제 중의 하나인 Castelnuovo문제로서 현재에는 Castelnuovo-Mumford-Eisenbud의 정칙성 예상으로 잘 알려져 있다. 예를 들어, 매끄러운 3차원 복소다양체에 대해서는 이 다양체와 4번 이상 만나는 직선들의 Family들의 크기가 주어진 사영공간에서 기껏해야 4차원 다양체를 이룬다는 사실과 R. Lazarsfeld가 개발한 Vector Bundle Technique에 의해서 증명이 가능할 수도 있지만 아직까지 증명이 완전하지 않으며 고차원 사영다양체의 경우에는 기하학적 정칙성 예상(Geometric Regularity Conjecture)로 알려져 있는 미해결 문제로서 새로운 아이디어와 통찰력이 요구된다. 그렇지만 임의의 아이디얼에 대해서는 Castelnuovo-Mumford 정칙성이 아주 복잡하기 때문에 아래에서 설명하고 있는 다항식 기반 암호의 원리를 제공한다.

이제 간략하게 대수기하학의 응용으로서 다항식기반 암호, 부호 정정 코드 구성 등에 대해서 설명하고자 한다. 1965년 오스트리아의 수학자 Buchberger는 "Gröbner Basis"라는 개념을 도입하여 Buchberger 알고리듬을 개발하였고 계산대수기하학의 분야를 새롭게 개척하였다. 다항환 $k[x_0 \cdots x_n]$의 단항식(Monomial)들은 잘 정의된 규칙에 의해서 순서를 정할 수가 있으며 그 순서에 의해 임의의 다항식 f의 Initial Term(초항) $\mathrm{in}(f)$을 정할 수가 있다. 마찬가지로 아이디얼 I에 대해서도 초이데알 $\mathrm{in}(I)=\langle \mathrm{in}(f) \mid f \in I \rangle$을 정의 할 수가 있다. 이때 I의 Gröbner기저라 불리우는 생성자들$\{g_1, \cdots, g_s\}$을 잘 찾으면 $\mathrm{in}(I)=\langle \mathrm{in}(g_1), \cdots, \mathrm{in}(g_s) \rangle$가 성립하고 가우스 소거법으로 Reduced Gröbner기저도 유일하게 구할 수 있다. 특히, 이 Gröbner기저를 가지고 다항식에 대해서도 다음과 같이 나눗셈 $m=\sum_{i=1}^{s} a_i g_i + r$을 할 수 있고(이때 나머지 r은 유일하다), 예전에는 생각할 수 없었던 많은 문제들에 대한 실질적인 계산을 할 수 있게 되어서 여러 분야에 응용이 가능해졌다.

이제 Gröbner기저의 암호로의 적용원리를 간단히 설명해보면 아이디얼 I 의 최소 생성자들의 집합 $F=\{f_1\cdots f_t\}$를 공개키, I 의 Gröbner Basis $G=\{g_1\cdots g_s\}$를 비밀키, 그리고 다항식 $0\neq\overline{m}\in k[x_0\cdots x_n]/I$를 메시지라고 하자. 송신자 A가 수신자 B에게 메시지 $\overline{m}$를 보내려고 할 때 공개키 $F=\{f_1\cdots f_t\}$를 이용해서 메시지 $\overline{m}$에 아이디얼 I에 포함된 임의의 다항식 h를 더한 값 m(i.e $m=\overline{m}+h$, $h\in I$) 을 보낸다. 수신자 B는 미리 알고 있던 비밀키 $G=\{g_1\cdots g_s\}$를 이용해서 m을 나누면 유일한 나머지 $\overline{m}$, 즉 처음에 송신자 A가 보내려 했던 메시지 $\overline{m}$를 얻을 수 있게 된다. 만약 중간자 C가 혼합문 m을 얻더라도 비밀키, 즉 Gröbner기저 $G=\{g_1\cdots g_s\}$를 모르기 때문에 유일한 나머지 $\overline{m}$를 구할 수 가 없다. 이 암호원리가 성립하는 이유는 계산적 관점에서 볼 때 $F=\{f_1\cdots f_t\}$를 이용해 Gröbner기저 $G=\{g_1\cdots g_s\}$를 구하기 어렵기 때문이다. 그러면 여기서 몇 가지 질문들을 던질 수가 있다. 첫째, Gröbner기저를 구하는 것은 얼마나 어려운가? 이것은 암호시스템의 안전성에 관한 문제이고 Projective Scheme을 정의하는 주어진 다항식들의 Gröbner기저를 계산하는 문제가 NP-hard 문제이기에 어렵다는 것은 알고 있다. 이 안전성은 아이디얼의 복잡도와 관련이 있는데 이 복잡도를 재는 척도가 바로 앞에서 소개한 Castelnuovo-Mumford 정칙성이다. 둘째, 임의의 아이디얼 I의 정칙성(Regularity)은 얼마나 커질 수 있는가? $d(I)$를 $F=\{f_1\cdots f_t\}$의 최대차수라고 하고 $reg(I)$를 아이디얼 I의 Castelnuovo-Mumford 정칙성라고 할 때, 1982년 E. Mayr와 A. Meyer는 다음과 같은 부등식 $reg(I)\leq 2d(I))^{2n-1}$이 성립함을 보이고 이 부등식의 최대치를 갖는 중요한 예제를 만들었다. 이 결과로부터 변수의 개수가 증가할수록 Regularity는 Doubly Exponentially 증가한다는 사실을 알 수 있으며 이러한 복잡도(Complexity) 개념과 Gröbner기저를 이용하여 지금까지 사용되고 있는 암호체계를 대체할 수 있는 새로운 암호체계 가능성을 제시할 수 있다. 이를 실현하기 위한 노력들은 현재 고등과학원(KIAS) 계산과학부 박형주 교수 중심의 연구그룹과 카이스트 대수구조 및 응용연구센터(ASARC)의 연구그룹이 연구를 진행 중이다. 위와 같은 응용을 통해 알 수 있듯이 계산대수기하학은 그 자체만으로도 큰 의미가 있지만 이론적인 대수기하 연구에서도 중요한 의미를 갖는다. 즉 사고의 심각한 오류나 잘못된 연구의 방향을 계산적 관점에서 바로잡아 주는 내비게이션 같은 역할도 하면서 그 자체가 하나의 이론연구 분야로 발전해오고 있는 것이다.

한편, 유한체 위에서 대수기하학을 이용한 오류 정정 코드(Error Correcting Code)구성은 1970년대에 러시아 수학자인 Goppa가 대수곡선(Algebraic Curve)에 기초한 특별한 종류의 코드를 처음으로 개발하면서부터이다. 대수기하코드의 핵심적인 원리는 직선위의 점들에 대해서 유리함수들의 Evaluation을 통해 코드를 구성하던 이전의 방법에 반해 대수곡선의 유리점(Rational Point)에서의 유리함수(Rational Function)의 Evaluation을 통해서 코드의 길이를 충분히 크게 할 수 있다는 점이다. 그 이유는 대수곡선위에서의 유리함수의 근이 되는 점들의 Bound는

Bezout 정리와 Riemann-Roch 정리를 통해 해결할 수 있었기 때문이다. 마지막으로 우리가 지금까지 살펴본 대수기하학은 주로 순수수학의 한 분야로서 수학의 다른 여러 분야와 긴밀한 관계를 가지고 발전해 왔으며 자연과학, 공학, 사회과학 등에도 널리 응용되고 있다. 이러한 현상을 가장 적절하게 나타내는 증거가 2006년 9월부터 2007년 6월에 걸쳐서 미국 미네소타 대학 수학연구소 IMA에서 개최된 대수기하학의 응용에 대한 집중세미나 주제 및 IMA 연구소 소장의 결과보고서에 잘 나와 있다.

IMA가 2006-2007년 동안 지원한 대수기하학 관련 응용 프로그램 중에는 CAGD(Computer Aided Geometric Design)에서 대수곡선 및 대수곡면의 이용, 기계적인 결합(Mechanical Linkage)을 기술하기 위한 다변수다항식계의 이용과 해법, Compact Disc나 핸드폰의 사용을 가능하도록 한 오류교정 부호(Error-Correcting Code)의 기본을 이루는 유한체 위에서의 대수곡선의 응용, Control 이론에의 응용, Software in Algebraic Geometry 등등 오래 전부터 연구되고 있는 분야가 있었다. 그리고 이 프로그램에서 논의된 새롭게 대두된 분야로는 유전자 정보(Genomic Data)로부터 계통수(Phylogenetic Tree)를 복구하는데 이용되는 대수통계학(Algebraic Statistics), 공학에서 많이 나타나는 다항식계의 해를 수치적으로 구하고자 하는 Numerical Algebraic Geometry 등이 있었다.

한국에서도 대수기하학에 대한 열기가 아주 높으며 젊은 연구자들의 연구능력도 아주 뛰어나다. 고등과학원에서도 지난 10년간 황준묵 교수와 금종해 교수가 주관하는 대수기하학 관련 국제학회와 집중강연이 매년 2번 이상 열리고 있으며 연구수준도 세계적인 수준에 이미 올라와 있다. 한편, 지난 2007년 9월, 카이스트(KAIST) 수리과학과에 대수구조 및 응용연구센터(ASARC)가 새롭게 설립되어서 많은 역할을 할 수 있을 것으로 기대된다.

지금처럼 대수기하학의 이론연구와 응용가능성을 개괄적으로 살펴보는 것은 매우 즐거운 일이다. 왜냐하면 순수한 이론연구든지 세상을 이롭게 하는 응용연구든지 간에 수학에 매력을 느끼며 삶을 투자하는 모든 연구자들에게는 수학의 진보를 이해하는 즐거움과 수학적 생명력을 지키기 위한 끊임없는 노력을 지속할 수 있는 계기가 되기 때문이다. 뿐만 아니라 일반인들에게는 세상에 자주 등장하는 슬로건 'Globally Think, Locally Act' 도 사실 대수기하학의 오랜 전통과 밀접한 연관이 있음을 알 수 있게 해주며 빠른 결과, 빠른 효과만을 강조하는 풍토에 진리가 우리를 자유케 한다는 정신으로 꾸준히 전진하는 수학의 아름다운 문화를 보여주는 의미가 있다. KIAS

Profile

곽시종 교수 현재 KAIST 수리과학과 교수이다. 미국 컬럼비아대에서 수학 박사학위를 취득했으며, 고등과학원 설립과 함께 수학부 연구원으로 4년간 연구했다. 전공분야는 고전적 대수기하학 및 계산대수기하학이며 '대수다양체의 Castelnuovo-Mumford 예상 및 Syzygy' 와 관련된 다수의 연구업적을 발표했다.