发光的玉雕——那些不朽的数学小品

贾朝华

“发光的玉雕”是美国天才的国际象棋棋手费舍尔（Bobby Fischer）的一局自战评述的标题，这局棋短小精悍却又光彩夺目。1972 年，费舍尔获得世界冠军，打破了当时前苏联棋手在国际象棋上的垄断地位。费舍尔的棋风华美、飘逸，算路极其精深，他的经典著作《我难忘的 60 局》一直被无数职业棋手和爱好者所推崇。

作为国际象棋的爱好者，只要知道基本规则和一些常见战术，就可以欣赏美妙的棋局。但这在数学中却往往行不通，因为要能欣赏一个深刻的数学定理，通常需要经过长时间的专业学习，读者只能通过专家的解说来得到间接的体验。

然而，在数学中也有一些定理，其证明经过不断地简化变得比较容易读懂。在本系列文章中，我们将借用“发光的玉雕”这个词，不定期地来介绍一些精彩而有深远意义的数学短论文。我们将提供与论文相关的背景知识和基本概念，使得读者能够读懂这些精彩而深刻的定理，从而直接地领略数学的美妙。

本文涉及的知识是大学“抽象代数”和“初等数论”课程中的一些基础知识。

1. 各种代数系统

求解多项式的根或解代数方程，一直是数学史上的重要问题。早在四千多年之前的巴比伦时代，人们就会解一元二次方程了，如今这已是中学数学里的常识。而解三次方程需要巧妙的方法，现在称为“卡尔达诺公式”。卡尔达诺（Girolamo Cardano, 1501-1576）是意大利文艺复兴时期的学者，他的学生费拉里（Lodovico Ferrari, 1522-1565）给出了四次方程的解法。

由高斯的代数学基本定理知，任何系数为复数的代数方程都有复数解。对于不超过四次的代数方程，它的解可以通过对系数进行加、减、乘、除或开方来得到，就是有所谓的“根式解”。1824 年，挪威数学家阿贝尔证明了，五次或五次以上的代数方程一般没有根式解。

法国天才数学家伽罗瓦给出了代数方程有根式解的一个充分必要条件，从而彻底解决了长期困扰数学家的难题。伽罗瓦死于 1832 年一场为爱而进行的决斗，在决斗的前夜他才最后完成他的理论。他的思想是超前而且深邃的，以至于当时的一些大数学家，如柯西、傅里叶和泊松等人都不能完全理解和接受他的思想。

1846 年，伽罗瓦的手稿得以公开发表。1870 年，若尔当（Camille Jordan）在他的书中首次全面地介绍了伽罗瓦理论。至此，人们才逐步地理解了伽罗瓦理论的精髓。这个理论不但能解决代数方程的根式解问题，还能判断

几何图形能否用圆规和直尺作图的问题，从而圆满地解决了不能三等分任意角等几何难题。更重要的是，伽罗瓦的思想为数学的发展提供了一条全新的思路，它把人们从偏重于计算的思维方式引向了用结构来研究的思维方式，从而产生了广泛而深远的影响。

为了解代数方程，要引入复数；为了研究线性方程组，要引入矩阵；为了处理解析几何中的曲线，要引入变换，等等。数学发展到了 19 世纪，需要研究处理的对象日益增多。因此，数学家要将其中共性的东西提炼出来，形成一些统一的理论。

人们将伽罗瓦的研究加以提炼和抽象，形成了群论，并公认伽罗瓦为群论的创始人之一。群论为很多数学现象提供了统一的处理和更深入的理解，在群论的基础上，又发展出了环论、体论和域论等等，形成了抽象代数的辉煌大厦。经过将近 200 年的发展，抽象代数已经成为现代数学最重要的部分之一。

现在，我们来给出群的定义。设 G 是一个非空集合，在 G 上定义了一个运算，记作“$\cdot$”，称为乘法。这种运算是一种结合方式，并不局限于算术中的乘法。对于 G 中任意两个元 a, b, 都有 G 中的元 c, 使得 $a\cdot b = c$，或简记为 $ab = c$. 如果 G 满足以下条件：

1. 乘法适合结合律，即对于 G 中任意三个元 a,b,c, 都有

$$(ab)c = a(bc);$$

2.G 中有一个单位元 e, 使得对于 G 中的任意元 a, 总有

$$ea = ae = a;$$

3. 对于 G 中的任意元 a, 在 G 中总有一个逆元 a^{-1}, 满足

$$a^{-1}a = aa^{-1} = e,$$

则我们称 G 为一个群。

如果乘法还满足交换律，即对于 G 中任意两个元 a, b, 都有

$$ab = ba,$$

则称 G 为一个交换群。

例如，所有正有理数之集，对于通常的乘法形成一个群，其单位元为 1。全体整数之集，对于通常的加法形成一个群，其单位元为 0。而所有 $n\times n$ 阶的非奇异的实数矩阵之集，对于矩阵乘法形成一个群，其单位元是对角线上的元全为 1，其余的元全为 0 的单位矩阵。当 $n \geq 2$ 时，这个矩阵群不是交换群。

进一步地，我们要研究有两种运算的代数系统。在这类代数系统中，环与体是最基本的。

环的构造最初出现在 19 世纪时戴德金（Richard Dedekind）和克罗内克（Leopold Kronecker）的著作里，直到 20 世纪希尔伯特才引入“环”这个术语，环的抽象理论是在 20 世纪发展起来的。

下面给出环的定义。设 R 是一个非空集合。在 R 上有两种运算。一种叫做加法，用“+”表示。另一种叫做乘法，用“·”表示。如果 R 满足以下条件：

1. R 对于加法成为交换群；
2. 乘法适合结合律；
3. 加法和乘法适合分配律，即对于 R 中任意三个元 a, b, c，有

$$a(b+c) = ab + ac, \qquad (a+b)c = ac + bc,$$

则我们称 R 为一个环。

例如，全体整数之集，对于普通的加法和乘法形成一个环。所有实系数多项式之集，对于多项式的加法和乘法形成一个环。所有 $n\times n$ 阶的元素为整数的矩阵之集，对于矩阵的加法和乘法形成一个环。

在环的基础上，我们可以得到体的概念。设 F 为一个环，它包含非零元，并且所有非零元对于乘法形成一个群，则我们称 F 为一个体。如果乘法还满足交换律，则我们称 F 为一个域。

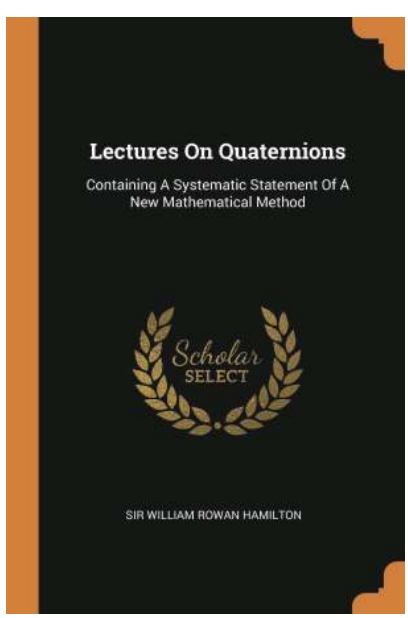
域比较常见，例如，有理数域、实数域和复数域等。对于元素个数为有限的域，伽罗瓦做过深入的研究，因此，有限域也称为伽罗瓦域。

1843 年，哈密尔顿提出了四元数。这是一种比复数更广泛的数，它形如

$$a\boldsymbol{e} + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k},$$

其中 a, b, c, d 均为实数，而

$$\boldsymbol{ij} = \boldsymbol{k}, \quad \boldsymbol{ji} = -\boldsymbol{k}, \quad \boldsymbol{ik} = -\boldsymbol{j}, \quad \boldsymbol{ki} = \boldsymbol{j},$$
$$\boldsymbol{jk} = \boldsymbol{i}, \quad \boldsymbol{kj} = -\boldsymbol{i}, \quad \boldsymbol{ii} = \boldsymbol{jj} = \boldsymbol{kk} = -\boldsymbol{e}.$$



哈密尔顿和他的专著