交换环论和 Emmy Noether

扶磊

清华大学丘成桐数学中心

Emmy Noether1882 年 3 月 23 日出生于德国 Erlangen, 父亲 Max Noether 也是数学家。

尽管有重要的数学贡献，Noether 在职业上、性别上、种族受到歧视。她一直到 1923 年才找到一份薪水很低的教职，在此之前，她虽然教过课，但都是用别的教授（如 Gordan, Hilbert...) 的名义，没有工资。到 1932 年，虽然已经是有国际声望、并建立了自己学派的数学家，没有任何机构考虑给 Noether 教授职位。1933 年，因为是犹太人，Noether 被剥夺教书的权利。后来美国的 Bryn Mawr College 给 Noether 一个访问教授的教职。1935 年 4 月 14 日，Noether 因为手术并发症去世。

Emmy Noether 将数学中的抽象的概念和它们之间的关系作为数学研究的对象，抽象概念的引进不仅仅是为了澄清具体的数学问题的本质，而是为了建立一般理论框架，这种风格超越了她的时代。当时图形、公式是创建数学理论的重要工具，但 Noether 不是靠这种方法，她借助概念推理，而不是直觉和计算。同时代数学家对 Noether 的公理化方式存疑，觉得它太抽象、缺乏具体内容。但 Noether 自己取得了巨大成功。Noether 的方法不仅仅是用来建立一套套理论，它更是作研究的方法和思维模式，现在这种方法深深地根植在现代数学中。

定义： **交换环**$(R,+,\times)$ **是个集合** R，**上面有运算** $+,\times: R\times R\to R$，**使得下面性质成立**：

(1) **结合率**：**对任何** $a,b,c\in R$, **有**

$$(a+b)+c=a+(b+c),\quad (ab)c=a(bc).$$

.

(2) **交换率**：**对任何** $a,b\in R$, **有**

$$a+b=b+a,\quad ab=ba.$$

(3) **存在** $0,1\in R$ **使得对任何** $a\in R$，**有**

$$a+0=a,\quad 1\cdot a=a.$$

(4) **对任何** $a\in R$，**存在** $-a\in R$ **使得**

$$a+(-a)=0.$$

例子： $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}[x]$, $\mathbb{C}[x]$.

设 n 是正整数。定义

$$\mathbb{Z}/n = \{\bar{a} : \ a \in \mathbb{Z}\}.$$

给定 $a, b \in \mathbb{Z}$，我们规定

$$\bar{a} = \bar{b} \Leftrightarrow a - b \in \{0, \pm n, \pm 2n, \pm 3n, \ldots\}.$$

定义

$$\bar{a} + \bar{b} = \overline{a + b}, \quad \bar{a} \cdot \bar{b} = \overline{ab}.$$

那么 $(\mathbb{Z}/n, +)$ 是交换环。

设 n 是正整数。定义

$$\mathbb{Z}/n = \{\bar{a} : \ a \in \mathbb{Z}\}.$$

给定 $a, b \in \mathbb{Z}$，我们规定

$$\bar{a} = \bar{b} \Leftrightarrow a - b \in \{0, \pm n, \pm 2n, \pm 3n, \ldots\}.$$

定义

$$\bar{a} + \bar{b} = \overline{a + b}, \quad \bar{a} \cdot \bar{b} = \overline{ab}.$$

那么 $(\mathbb{Z}/n, +)$ 是交换环。

例子：

$$\begin{aligned} \mathbb{Z}/7 &= \{\bar{0}, \bar{1}, \ldots, \bar{6}\}, \\ &= \{\text{周日}, \ \text{周一}, \ \ldots, \ \text{周六}\}. \end{aligned}$$

今天是周六，7 天后是周几？10 天后是周几？

$$\begin{aligned} \bar{6} + \bar{7} &= \overline{13} = \bar{6}, \\ \bar{6} + \overline{10} &= \overline{16} = \bar{2}. \end{aligned}$$

定义 (Dedekind): 环 R 的**理想** I 是 R 的子集，使得对任何 $a, b \in I$, $r \in R$，都有 $a + b$, $ra \in I$。

定义 (Dedekind): 环 R 的**理想** I 是 R 的子集，使得对任何 $a, b \in I$, $r \in R$，都有 $a + b$, $ra \in I$。

$\{0, \pm n, \pm 2n, \ldots\}$ 是 $\mathbb{Z}$ 的理想。

定义 (Dedekind): 环 R 的**理想** I 是 R 的子集，使得对任何 $a, b \in I$, $r \in R$，都有 $a + b$, $ra \in I$。

$\{0, \pm n, \pm 2n, \ldots\}$ 是 $\mathbb{Z}$ 的理想。

设 I 是 R 的理想，定义

$$R/I = \{\bar{a} : \ a \in R\}.$$

给定 $a, b \in R$，我们规定

$$\bar{a} = \bar{b} \Leftrightarrow a - b \in I.$$

定义

$$\bar{a} + \bar{b} = \overline{a + b}, \quad \bar{a} \cdot \bar{b} = \overline{ab}.$$

那么 $(R/I, +, \cdot)$ 是交换环。

定义 (Dedekind): 环 R 的**理想** I 是 R 的子集，使得对任何 $a, b \in I$, $r \in R$，都有 $a+b$, $ra \in I$。

$\{0, \pm n, \pm 2n, \ldots\}$ 是 $\mathbb{Z}$ 的理想。

设 I 是 R 的理想，定义

$$R/I = \{\bar{a} : \ a \in R\}.$$

给定 $a, b \in R$，我们规定

$$\bar{a} = \bar{b} \Leftrightarrow a - b \in I.$$

定义

$$\bar{a} + \bar{b} = \overline{a+b}, \quad \bar{a} \cdot \bar{b} = \overline{ab}.$$

那么 $(R/I, +, \cdot)$ 是交换环。

上面的运算是有意义的：如果 $\bar{a} = \bar{\alpha}$, $\bar{b} = \bar{\beta}$，那么

$$\overline{a+b} = \overline{\alpha+\beta}, \quad \overline{ab} = \overline{\alpha\beta}.$$

我们有 $a - \alpha, b - \beta \in I$。

$$(a+b) - (\alpha+\beta) = (a-\alpha) + (b-\beta) \in I,$$
$$ab - \alpha\beta = ab - a\beta + a\beta - \alpha\beta = a(b-\beta) + (a-\alpha)\beta \in I.$$

$\mathbb{C}^n$ 中形如

$$Z(f_1,\ldots,f_m)=\{(a_1,\ldots,a_m)\in\mathbb{C}^n : f_1(a_1,\ldots,a_n)=\cdots=f_m(a_1,\ldots,a_n)=0\}$$
$$(f_1,\ldots,f_m\in\mathbb{C}[x_1,\ldots,x_n])$$

的集合称为Zariski 闭集。

$\mathbb{C}^n$ 中形如

$$Z(f_1,\ldots,f_m)=\{(a_1,\ldots,a_m)\in\mathbb{C}^n : f_1(a_1,\ldots,a_n)=\cdots=f_m(a_1,\ldots,a_n)=0\}$$
$$(f_1,\ldots,f_m\in\mathbb{C}[x_1,\ldots,x_n])$$

的集合称为Zariski 闭集。

对任何 Zariski 闭集 F，定义

$$I(F)=\{f\in\mathbb{C}[x_1,\ldots,x_n] : f(a_1,\ldots,a_n)=0\ \forall(a_1,\ldots,a_n)\in F\}.$$

那么 $I(F)$ 是多项式环 $\mathbb{C}[x_1,\ldots,x_n]$ 的理想.

$\mathbb{C}^n$ 中形如

$$Z(f_1,\ldots,f_m)=\{(a_1,\ldots,a_m)\in\mathbb{C}^n : f_1(a_1,\ldots,a_n)=\cdots=f_m(a_1,\ldots,a_n)=0\}$$
$$(f_1,\ldots,f_m\in\mathbb{C}[x_1,\ldots,x_n])$$

的集合称为Zariski 闭集。

对任何 Zariski 闭集 F，定义

$$I(F)=\{f\in\mathbb{C}[x_1,\ldots,x_n] : f(a_1,\ldots,a_n)=0\ \forall(a_1,\ldots,a_n)\in F\}.$$

那么 $I(F)$ 是多项式环 $\mathbb{C}[x_1,\ldots,x_n]$ 的理想.

对任何理想 I, 定义 Zariski 闭集

$$Z(I)=\{(a_1,\ldots,a_m)\in\mathbb{C}^n : f(a_1,\ldots,a_n)=0\ \forall f\in I\}.$$

$\mathbb{C}^n$ 中形如

$$Z(f_1,\ldots,f_m)=\{(a_1,\ldots,a_m)\in\mathbb{C}^n : f_1(a_1,\ldots,a_n)=\cdots=f_m(a_1,\ldots,a_n)=0\}$$
$$(f_1,\ldots,f_m\in\mathbb{C}[x_1,\ldots,x_n])$$

的集合称为Zariski 闭集。

对任何 Zariski 闭集 F，定义

$$I(F)=\{f\in\mathbb{C}[x_1,\ldots,x_n] : f(a_1,\ldots,a_n)=0\ \forall(a_1,\ldots,a_n)\in F\}.$$

那么 $I(F)$ 是多项式环 $\mathbb{C}[x_1,\ldots,x_n]$ 的理想.

对任何理想 I, 定义 Zariski 闭集

$$Z(I)=\{(a_1,\ldots,a_m)\in\mathbb{C}^n : f(a_1,\ldots,a_n)=0\ \forall f\in I\}.$$
$$Z(I_1)\cup Z(I_2)=Z(I_1\cap I_2),\quad I(F_1\cup F_2)=I(F_1)\cap I(F_2).$$

$\mathbb{C}^n$ 中形如

$$Z(f_1,\ldots,f_m)=\{(a_1,\ldots,a_m)\in\mathbb{C}^n : f_1(a_1,\ldots,a_n)=\cdots=f_m(a_1,\ldots,a_n)=0\}$$
$$(f_1,\ldots,f_m\in\mathbb{C}[x_1,\ldots,x_n])$$

的集合称为Zariski 闭集。

对任何 Zariski 闭集 F，定义

$$I(F)=\{f\in\mathbb{C}[x_1,\ldots,x_n] : f(a_1,\ldots,a_n)=0\ \forall(a_1,\ldots,a_n)\in F\}.$$

那么 $I(F)$ 是多项式环 $\mathbb{C}[x_1,\ldots,x_n]$ 的理想.

对任何理想 I, 定义 Zariski 闭集

$$Z(I)=\{(a_1,\ldots,a_m)\in\mathbb{C}^n : f(a_1,\ldots,a_n)=0\ \forall f\in I\}.$$
$$Z(I_1)\cup Z(I_2)=Z(I_1\cap I_2),\quad I(F_1\cup F_2)=I(F_1)\cap I(F_2).$$

Zariski 闭集合 F 称为不可约的如果对任何分解 $F=F_1\cup F_2$，这里 F_1,F_2 是闭集，那么 $F=F_1$ 或 $F=F_2$。任何 Zariski 闭集 F 都可以唯一地分解成 $F=F_1\cup\cdots\cup F_m$ 使得每个 F_i 都是不可约闭集。

$\mathbb{C}^n$ 中形如

$$Z(f_1,\ldots,f_m)=\{(a_1,\ldots,a_m)\in\mathbb{C}^n : f_1(a_1,\ldots,a_n)=\cdots=f_m(a_1,\ldots,a_n)=0\}$$
$$(f_1,\ldots,f_m\in\mathbb{C}[x_1,\ldots,x_n])$$

的集合称为Zariski 闭集。

对任何 Zariski 闭集 F，定义

$$I(F)=\{f\in\mathbb{C}[x_1,\ldots,x_n] : f(a_1,\ldots,a_n)=0\ \forall(a_1,\ldots,a_n)\in F\}.$$

那么 $I(F)$ 是多项式环 $\mathbb{C}[x_1,\ldots,x_n]$ 的理想.

对任何理想 I, 定义 Zariski 闭集

$$Z(I)=\{(a_1,\ldots,a_m)\in\mathbb{C}^n : f(a_1,\ldots,a_n)=0\ \forall f\in I\}.$$
$$Z(I_1)\cup Z(I_2)=Z(I_1\cap I_2),\quad I(F_1\cup F_2)=I(F_1)\cap I(F_2).$$

Zariski 闭集合 F 称为不可约的如果对任何分解 $F=F_1\cup F_2$，这里 F_1,F_2 是闭集，那么 $F=F_1$ 或 $F=F_2$。任何 Zariski 闭集 F 都可以唯一地分解成 $F=F_1\cup\cdots\cup F_m$ 使得每个 F_i 都是不可约闭集。

理想 I 称为不可约如果对任何分解 $I=I_1\cap I_2$，我们有 $I=I_1$ 或 $I=I_2$.

$\mathbb{C}^n$ 中形如

$$Z(f_1,\dots,f_m)=\{(a_1,\dots,a_m)\in\mathbb{C}^n : f_1(a_1,\dots,a_n)=\cdots=f_m(a_1,\dots,a_n)=0\}$$
$$(f_1,\dots,f_m\in\mathbb{C}[x_1,\dots,x_n])$$

的集合称为Zariski 闭集。

对任何 Zariski 闭集 F，定义

$$I(F)=\{f\in\mathbb{C}[x_1,\dots,x_n] : f(a_1,\dots,a_n)=0\ \forall(a_1,\dots,a_n)\in F\}.$$

那么 $I(F)$ 是多项式环 $\mathbb{C}[x_1,\dots,x_n]$ 的理想.

对任何理想 I, 定义 Zariski 闭集

$$Z(I)=\{(a_1,\dots,a_m)\in\mathbb{C}^n : f(a_1,\dots,a_n)=0\ \forall f\in I\}.$$
$$Z(I_1)\cup Z(I_2)=Z(I_1\cap I_2),\quad I(F_1\cup F_2)=I(F_1)\cap I(F_2).$$

Zariski 闭集合 F 称为不可约的如果对任何分解 $F=F_1\cup F_2$，这里 F_1,F_2 是闭集，那么 $F=F_1$ 或 $F=F_2$。任何 Zariski 闭集 F 都可以唯一地分解成 $F=F_1\cup\cdots\cup F_m$ 使得每个 F_i 都是不可约闭集。

理想 I 称为不可约如果对任何分解 $I=I_1\cap I_2$，我们有 $I=I_1$ 或 $I=I_2$.

定理 (Lasker-Macauley). 多项式环 $\mathbb{C}[x_1,\dots,x_n]$ 中任何理想 I 都有唯一的分解 $I=I_1\cap\cdots\cap I_m$ 使得每个 I_i 都是准素理想。

在 1921 年的文章"Ideal theory in rings" 中，Noether 考虑满足升链性质的环：环 R 称为满足升链性质 acc (ascending chain condition) 如果对任何 R 中理想的升链

$$I_1 \subset I_2 \subset \cdots,$$

存在足够大的整数 n 使得

$$I_n = I_{n+1} = \cdots.$$

今天我们称满足这种性质的环为noetherian 环。

在 1921 年的文章"Ideal theory in rings" 中，Noether 考虑满足升链性质的环：环 R 称为满足升链性质 acc (ascending chain condition) 如果对任何 R 中理想的升链

$$I_1 \subset I_2 \subset \cdots,$$

存在足够大的整数 n 使得

$$I_n = I_{n+1} = \cdots.$$

今天我们称满足这种性质的环为noetherian 环。

Noether 证明在 noetherian 环 R 中，不可约理想 I 都是准素理想，即对任何 $a, b \in R$ 使得 $ab \in I$, 要么 $a \in I$ 要么存在正整数 n 使得 $b^n \in I$.

在 1921 年的文章"Ideal theory in rings" 中，Noether 考虑满足升链性质的环：环 R 称为满足升链性质 acc (ascending chain condition) 如果对任何 R 中理想的升链

$$I_1 \subset I_2 \subset \cdots,$$

存在足够大的整数 n 使得

$$I_n = I_{n+1} = \cdots.$$

今天我们称满足这种性质的环为noetherian 环。

Noether 证明在 noetherian 环 R 中，不可约理想 I 都是准素理想，即对任何 $a, b \in R$ 使得 $ab \in I$, 要么 $a \in I$ 要么存在正整数 n 使得 $b^n \in I$.

定理 (Noether). Noether 环 R 中的任何理想 I 都可以唯一的写成

$$I = I_1 \cap \cdots \cap I_m$$

使得每个 I_i 都是准素的。

Noether 的定理比 Lasker-Macauley 的定理更一般，证明更简单、更抓住问题的本质。

$\mathbb{Z}$ 具有唯一分解性质，即任何非零整数都可以唯一地分解成素数的乘积。

$\mathbb{Z}$ 具有唯一分解性质，即任何非零整数都可以唯一地分解成素数的乘积。

环 $\mathbb{Z}[\sqrt{-5}]$ 没有唯一分解性质，

$$6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}),$$

但 $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ 都在 $\mathbb{Z}[\sqrt{-5}]$ 中不可约。

$\mathbb{Z}$ 具有唯一分解性质，即任何非零整数都可以唯一地分解成素数的乘积。

环 $\mathbb{Z}[\sqrt{-5}]$ 没有唯一分解性质，

$$6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}),$$

但 $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ 都在 $\mathbb{Z}[\sqrt{-5}]$ 中不可约。

环 R 的理想 $\mathfrak{p}$ 称为素理想如果对任何 $a, b \in R$ 使得 $ab \in \mathfrak{p}$，则 $a \in \mathfrak{p}$ 或 $b \in \mathfrak{p}$。

$\mathbb{Z}$ 具有唯一分解性质，即任何非零整数都可以唯一地分解成素数的乘积。

环 $\mathbb{Z}[\sqrt{-5}]$ 没有唯一分解性质，

$$6 = 2 \times 3 = (1+\sqrt{-5})(1-\sqrt{-5}),$$

但 $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ 都在 $\mathbb{Z}[\sqrt{-5}]$ 中不可约。

环 R 的理想 $\mathfrak{p}$ 称为素理想如果对任何 $a, b \in R$ 使得 $ab \in \mathfrak{p}$，则 $a \in \mathfrak{p}$ 或 $b \in \mathfrak{p}$。

Dedekind 证明了代数数域的代数整数环中的任何非零理想可以唯一的写成素理想的乘积。例如在代数整数环 $\mathbb{Z}[\sqrt{-5}]$ 中，

$$\mathfrak{p} = (2, 1+\sqrt{-5}), \quad \mathfrak{q} = (3, 1+\sqrt{-5}), \quad \mathfrak{r} = (3, 1-\sqrt{-5})$$

都是素理想，我们有理想的素分解

$$(2) = \mathfrak{p}^2, \quad (3) = \mathfrak{q}\mathfrak{r}, \quad (1+\sqrt{-5}) = \mathfrak{p}\mathfrak{q}, \quad (1-\sqrt{-5}) = \mathfrak{p}\mathfrak{r}.$$

这可以给出

$$6 = 2 \times 3 = (1+\sqrt{-5})(1-\sqrt{-5})$$

作为理想的分解：

$$(6) = \mathfrak{p}^2\mathfrak{q}\mathfrak{r}.$$

在 1927 的文章"Abstract development of ideal theory in algebraic number fields and function fields" 中，Noether 刻画了Dedekind 整环，即每个非零理想都是素理想的乘积的整环。

定理 (Noether) 整环 R 是 Dedekind 整环当且仅当下面性质成立：

(1) R 满足 acc，即 R 是 Noetherian 环。

(2) 对 R 中任何非零理想 I, R/I 满足降链性质 dcc，即 R/I 是 Artinian 环。

(3) R 是整闭的，即对任何分式 a/b $(a, b \in R, b \neq 0)$, 如果 $x = a/b$ 满足方程

$$x^n + c_1 x^{n-1} + \cdots + c_n = 0 \quad (c_1, \ldots, c_n \in R),$$

那么 $b|a$，即 $a/b \in R$.

在 1927 的文章"Abstract development of ideal theory in algebraic number fields and function fields" 中，Noether 刻画了Dedekind 整环，即每个非零理想都是素理想的乘积的整环。

定理 (Noether) 整环 R 是 Dedekind 整环当且仅当下面性质成立：

(1) R 满足 acc，即 R 是 Noetherian 环。

(2) 对 R 中任何非零理想 I, R/I 满足降链性质 dcc，即 R/I 是 Artinian 环。

(3) R 是整闭的，即对任何分式 a/b $(a, b \in R, b \neq 0)$, 如果 $x = a/b$ 满足方程

$$x^n + c_1 x^{n-1} + \cdots + c_n = 0 \quad (c_1, \ldots, c_n \in R),$$

那么 $b|a$，即 $a/b \in R$.

对 Dedekind 整环 R，若 $I = I_1 \cap \cdots \cap I_m$ 是非零理想 I 的准素分解，那么 $I_1, \ldots, I_m$ 是素理想的方幂，而且 $I_1 \cap \cdots \cap I_m = I_1 \cdots I_m$，这样 $I = I_1 \cdots I_m$ 就是 I 的素分解。

Noether、Artin、Krull 在 1920 年代的工作建立了环论。在 Noetherian 环上，可以研究维数、完备化、正则性、相交理论、上同调.....