代数学中的“化整为零”

宁中

【我们假设读者具有一定的代数学基础知识，包括环和域的概念、环上（至少是交换环上）整除、环的理想和商、环上的多项式及其整除等等。】

我们知道“化整为零”，或者说是从整体到局部，是微分学的出发点（当然具体而言是局部线性化，也就是在局部用切线的一部分代替曲线）。但是你是否知道，在代数学里面也有类似的做法？我们通过下面的例子来说明这个做法。

模*p*简约：多项式的不可约性

这里*p* 表示一个素数。我们知道整数环**Z**模*p* 的同余类构成一个域*p*（一般模的同余类构成一个环）。用环论的语言说，*p*的所有倍数的集合*p*构成**Z**的一个理想，也记作,称为由*p*生成的理想。一般而言，非零整数的所有倍数的集合构成**Z**的一个理想，称为由生成的理想。但是只有当是素数的时候，商*p*才是一个域。特别是生成零理想，而生成的理想是整个环**Z**。

整数环上的多项式，也就是整系数多项式全体的集合构成一个环**。从Z到***p*的典范映射*p*（即把整数 映到它所在的同余类 的映射）诱导出多项式环的映射 把整系数多项式

映到*p*中的多项式

注意到这个映射是一个环的同态，也就是它跟环的所有运算都可以交换，特别是其中能够被*p* 整除的系数都被映成了零，也就是*p*中的零元素。于是系数全部能够被*p* 整除的多项式就被映成了中的零多项式。注意

所谓的“模*p*简约”，就是把整数环上的问题利用这个典范映射 转移到*p*上来考虑。比如我们想要知道一个整系数多项式是否可约，就可以对某些素数*p*考虑在*p* 上是否可约。虽然这个条件只是必要而非充分，但是对于确认某些多项式不可约还是很有用的。而这样做的好处也是显而易见的：因为*p*是一个有限域，想要知道一个多项式是否可约，只需要有限步的验证。从某种意义上这就是一个“化整为零”，或者说从整体到局部的过程。换言之，把原来相对困难的问题转化为某个“局部”相对不那么困难的问题，看看是否能够得出我们需要的信息。在条件（或者运气）足够好的情形，有可能因此就解决了原来的问题。当然，这个“局部-整体”来回“倒腾”的philosophy是否能够奏效很大程度上依赖于具体情况。我们看看下面的例子。

设*p* 为素数，考虑如下多项式的可约性

两边乘以就得到.如果，其中和的次数都大于1，我们考虑它们在下的像

因为在当中有，我们有

于是只能有。但是的因子一定是形如，所以在中有 。也就是说和都是的倍数，从而是的倍数。另一方面，只是的倍数而不是的倍数。所以原来的多项式不可约。

从这个做法可以得出一个一般的不可约性判别法

**定理**(Eisenstein判别法) 如果整系数多项式

的系数中，不能整除，整除、、……，，不能整除，那么不可约。

证明的方法跟上面几乎一模一样。能够读到这里的朋友，是否可以自己试试？

高斯引理：素数和素理想

 上面的办法还可以用来证明本原多项式的高斯引理：整数环上(一个变元)的两个本原多项式的乘积仍然是本原多项式。

 这里的本原多项式是指系数互素的多项式，也就是所有系数的最大公因子为1的多项式。古典的证明是这样的：把两个本原多项式写成

如果乘积不是本原的，那么它的系数的最大公因子一定有一个素因子。这样就能够整除所有的，但是不能整除所有的和。我们不妨假设能够整除和，但是不能整除和。那么 当中，等式右边除了第一项，所有的项都能够被整除，而左边也能够被整除，这样就迫使右边第一项也被整除。但是是素数，所以必须整除和当中至少一个。这就跟我们的假设矛盾。因此也是本原的。

接下来我们用模简约的方法来证明。同样假设是乘积所有系数的最大公因子的一个素因子。因为*p*是域，多项式环是整环，也就是非零元的乘积一定非零。既然和都是本原的，它们的系数不能全部被整除，则它们在下的像和的非零，于是他们的乘积同样也非零。另一方面，是乘积所有系数的最大公因子的一个素因子，所以在*p*上。这个矛盾说明乘积也是本原的。

这里需要说明的是，高斯引理在更为一般的情形下也是正确的。假设是有乘法单位元的交换环。上的多项式（即系数在中的多项式）称为是本原的，如果其系数生成的理想就是自己。换言之，的单位元（为简单起见记作1）也在这个理想当中。注意这里我们已经不能再用最大公因子来定义本原多项式，这是因为在一般的交换环当中最大公因子未必存在。自然，我们也不能再用“最大公因子的素因子”来证明这个一般的高斯引理了。会不会有人开始怀疑，这个结果到底对不对啊？看起来条件似乎太一般了！

确实，没有了最大公因子，原来的那些办法似乎都没有用了。怎么办呢？

我们需要一个观念上的转换。从整除的定义看，我们说环的两个元素整除，如果存在着当中的元素使得。但是如果从理想的观点来看，这等价于理想的包含关系。既然整除关系可以用理想的包含关系代替，一些元素的最大公因子其实就可以用它们生成的理想代替。特别是素数的概念，就拓展为所谓的“素理想”的概念。的理想𝔭称为是一个素理想，如果当两个理想 和 的乘积的时候，至少有一个 或者 包含在𝔭里面。问题在于，对于一个一般的交换环，素理想一定存在吗？

这个问题跟集合论有关。我们现在通常使用（或者默认）的集合论是所谓的Zermelo-Fraenkel体系，简称为Z-F体系。其中包含一条重要的公理，叫做“选择公理”，它的一个等价形式是所谓的Zorn引理。在这里我们不准备涉及到细节，只是笼统地说，利用Zorn引理，我们可以证明任何非零交换环当中素理想的存在性。特别是对于任何一个非平凡理想（平凡理想是(0)和整个环）一定存在包含这个理想的素理想。

解决了这个素理想的存在问题以后，我们几乎可以照搬上面高斯引理的证明，只不过需要把素数换成素理想𝔭。相应的做法可以叫做模𝔭简约。这里需要用到素理想的一个刻画：的理想𝔭是素理想当且仅当商环是一个整环。

同样假设两个本原多项式和的乘积不是本原的，那么它的系数生成的理想一定包含在一个素理想𝔭中。同样地，典范映射诱导出多项式环的同态]。注意到我们有]。既然的系数生成的理想包含在素理想𝔭中，那么。但是和但是本原的，它们的系数不全在𝔭中，所以和都在当中非零。因为整环上的多项式环仍然是整环，非零多项式和的乘积也是非零的。这个矛盾表明也是本原的。

这里的例子对于“局部-整体”原理的说明其实连冰山的尖儿都算不上。真正触及到哪怕是稍微不那么初等的内容也需要做很多背景知识的准备，比如首先需要建立所谓局部域的理论。在最简单的情形，是考虑整数环和有理数域对于各种度量的完备化。如果使用的是普通的绝对值导出的度量，就得到平常的实数域；如果使用所谓的进度量（来自素数定义的非阿基米德赋值），得到的完备化称为进数域。这方面一个成功的范例是所谓的Hasse-Minkowski定理；两个二次型在有理数域是等价当且仅当它们在实数域和对所有素数的进数域上等价。对于这方面知识的介绍远非这篇短文能够企及，也超出了作者的能力。所以就此打住应该是比较合适的做法。

【后记】

1. 多项式 不可约性的传统证明是先做一个变量替换，然后用Eisenstein判别法去证明不可约。这里所给证明的最初想法来自一位不愿公开身份的朋友。

2. 一般交换环上的高斯引理载于Atiyah-MacDonald《交换代数导引》(Introduction to Commutative Algebra)。