Informal Notes on
Mathematics
2022.10.02

有限域上的因式分解

1 域论基础

本节我们先从最基础的概念——域的定义开始讨论。

1.1 域的定义与基本性质

设 F 是一个集合，并在 F 上定义了两个运算：加法“+”和乘法“·”。如果满足下列条件，则称 F 构成一个域：

1. $(F,+)$ 是一个阿贝尔群，即存在加法单位元 0，且每个元素 $x \in F$ 都有唯一的加法逆元 $-x$；
2. $F \setminus \{0\}$ 在乘法下构成一个阿贝尔群，即存在乘法单位元 1（且 $1 \neq 0$），每个非零元素 $x \in F$ 都有唯一的乘法逆元 x^{-1}；
3. 乘法对加法满足分配律：对任意 $a, b, c \in F$，有

$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

举个大家都比较熟悉的例子，我们常见的有理数域 $\mathbb{Q}$、实数域 $\mathbb{R}$ 和复数域 $\mathbb{C}$。在这里，我们不难发现，域不仅要求加法和乘法都能良好进行，而且还要满足“每个非零元素都有逆元”这一条件，这一点使得域比一般的环具有更强的结构性。

（摘自 MathStackExchange 的讨论）：
问：为什么在定义域时必须排除 *0*？

答：因为如果允许 0 参与乘法逆元的讨论，就会违反乘法逆元的唯一性和存在性；0 没有乘法逆元，这是数学上一个基本的共识。（参见 MathStackExchange 讨论[1]）

现在，我们突然发现，这里涉及的“群”的概念其实还没有被系统地讲解过，所以我们先简单温习一下：群是满足封闭性、结合性、有单位元、每个元素有逆元的集合。如果读者对群的概念已经耳熟能详，这里就不赘述。

在这里，我想特别指出，域的存在性与其扩张构造问题紧密相关。比如，从整数环 $\mathbb{Z}$ 构造出有理数域 $\mathbb{Q}$，这个过程可以看作是一种“局部化”过程。

1.2 域的扩张及其性质

对于一个给定的域 F，我们往往希望能构造出一个更大的域 K，使得 F 嵌入于 K 中，并且在 K 中某些原来在 F 中没有“解”的多项式能够分解。这个过程称为域的扩张。常见的扩张方式包括简单扩张、多重扩张等。

举例说明： 设 $F = \mathbb{R}$，考虑多项式 $x^2 + 1 \in \mathbb{R}[x]$。由于该多项式在 $\mathbb{R}$ 上无实根，我们构造复数域 $\mathbb{C}$ 作为 $\mathbb{R}$ 的一个扩张，使得 $x^2 + 1$ 在 $\mathbb{C}$ 中可以分解为 $(x + i)(x - i)$。

在研究域的扩张时，一个重要的概念是**扩张次数**。若 K 作为 F 上

[1]MathStackExchange 讨论中提到：“零除问题使得 0 无法拥有乘法逆元”，此处仅作参考说明，不求全引。

的向量空间具有有限维，则称扩张 K/F 为有限扩张，其维数称为扩张次数。

（摘自 MathOverflow 的讨论）：
问：有限扩张和无限扩张在具体问题中有什么不同的应用？
答：有限扩张通常容易处理，因为其代数结构较为简单，可以用基、维数等概念进行刻画；而无限扩张则需要引入更复杂的工具，如超限数等。

由于我们主要讨论有限域上的因式分解问题，后续的讨论中将主要用到有限域的相关性质。需要注意的是，有限域本身必然是有限扩张的一个典型例子，这里我们就不再赘述无限扩张的复杂性了。

2 有限域的构造与性质

有限域，又称伽罗华域，是指仅含有有限个元素的域。一个基本事实是：有限域的阶数一定是素数的幂，即若 F 为有限域，则 $|F| = p^n$，其中 p 为素数，n 为正整数。接下来我们从构造和性质两方面详细讨论有限域。

2.1 有限域的构造

首先我们以最简单的有限域——素域为例。设 p 为素数，则模 p 的整数集合 $\mathbb{F}_p = \{0, 1, 2, \ldots, p-1\}$ 在加法和乘法模 p 运算下构成一个有限域。

例 1： 取 $p = 5$，则 $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$。在此域中，$2+4 \equiv 1 \pmod 5$，而 $3 \cdot 4 \equiv 2 \pmod 5$。这样的运算规则虽然简单，但却体现了有限域内严谨而紧凑的代数结构。

接下来讨论更一般的有限域构造方法。设 p 为素数，考虑多项式环

$\mathbb{F}_p[x]$。若存在一个不可约多项式 $f(x)$，其次数为 n，则理想 $\langle f(x)\rangle$ 是 $\mathbb{F}_p[x]$ 的极大理想，从而商环 $\mathbb{F}_p[x]/\langle f(x)\rangle$ 构成一个有限域，其元素个数为 p^n。

例 2： 取 $p=2$，考虑多项式 $f(x)=x^3+x+1\in\mathbb{F}_2[x]$。经过检验可知，$f(x)$ 在 $\mathbb{F}_2$ 上不可约，因此构造出的有限域记作 $\mathbb{F}_{2^3}$，其元素个数为 8。

在具体构造中，我们需要对不可约多项式的判定方法进行详细了解。对于低次多项式，可直接检验；而对于高次多项式，我们可能需要借助一些判别准则。

现在我们突然发现这里的不可约性判定方法我们还没有系统地学过，所以我们先简单探讨一下。对于一个多项式 $f(x)\in\mathbb{F}_p[x]$，若 $f(x)$ 在 $\mathbb{F}_p$ 中无非平凡因子，则称 $f(x)$ 不可约。一般来说，对于次数较低的多项式，可以通过枚举 $\mathbb{F}_p$ 中的元素来检验是否存在根，但对于高次多项式，情况则复杂很多。我猜可以借鉴 Eisenstein 判别法的一些思想，但具体细节在有限域上会有所不同。由于时间原因，我们先打住。回到刚刚构造有限域的主题。

此外，还可以采用更一般的构造方法，比如利用伽罗华理论中的分裂域等概念。这里不再做深入展开，只简单给出构造思路：选取某个不可约多项式 $f(x)$ 后，考虑其所有根构成的最小域即为 $f(x)$ 的分裂域，该分裂域在有限域情形下必定有限，而且其阶数恰为 p^m，其中 m 是 $f(x)$ 的分裂域的次数。

2.2 有限域的重要性质

有限域具有许多优良的性质，以下列举几个常用且关键的性质：

1. **唯一性：** 对于每个形如 p^n 的正整数，都存在唯一（同构意义下）的有限域，其记作 $\mathbb{F}_{p^n}$。

2. **乘法群的循环性：**有限域 $\mathbb{F}_{p^n}$ 中，非零元构成的乘法群是循环群，即存在一个生成元 α 使得所有非零元可表示为 α^k 的形式。

3. **自同构群：**有限域的自同构群具有明确的结构，特别是由 Frobenius 自同构给出：$\sigma(a) = a^p$，这种自同构在有限域中起到了核心作用。

这些性质在后续讨论有限域上多项式的因式分解时会反复出现。

问：为什么有限域中的乘法群一定是循环的？
答：这一结论来源于有限交换群理论中的一个基本定理。因为有限域中非零元构成的阿贝尔群必定分解为循环群的直积，而由于域的乘法结构的特殊性，该群实际上只能是单一的循环群。

3 有限域上的多项式因式分解

在本节中，我们将重点探讨有限域上多项式的因式分解问题。这一问题不仅在理论上有着重要意义，而且在计算代数和密码学中也有广泛应用。讨论将从多项式的基本性质开始，然后逐步引入因式分解的基本定理及具体算法。

3.1 多项式的定义与性质

考虑有限域 $\mathbb{F}_q$，其中 $q = p^n$。在该域上，我们定义多项式环 $\mathbb{F}_q[x]$。多项式的加法和乘法均满足通常的运算规则。

定义：设 $f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_0 \in \mathbb{F}_q[x]$，其中 $a_i \in \mathbb{F}_q$，若 $a_m \neq 0$，则称 m 为 $f(x)$ 的次数。

对于多项式的因式分解问题,我们关心的问题是:给定 $f(x) \in \mathbb{F}_q[x]$,是否存在非平凡多项式 $g(x), h(x) \in \mathbb{F}_q[x]$ 使得 $f(x) = g(x)h(x)$。

这里有一点需要注意，多项式在有限域上虽然和在实数域或复数域上类似，但其因式分解的唯一性可能与我们直观的认识有所不同。实际上，在有限域上，不可约多项式的分解是唯一的（模单位元的乘积），这与整数分解的唯一性有着类似的‘素数分解定理’。也许可以用这一点来类比整数的素因数分解，从而加深对因式分解唯一性的理解。

3.2 因式分解基本定理在有限域中的讨论

在实数域或复数域中，存在著名的代数学基本定理：每个非零单变量多项式可以分解为线性因子。然而在有限域中，由于有限性，情形就显得更为复杂。事实上，有限域上多项式的因式分解定理指出：任何非零多项式都可以分解为不可约多项式的乘积，而且这一分解是唯一的(模顺序和单位元)。

证明这一结论的思路基本沿用了整环中的归纳法思想。考虑一个非零多项式 $f(x)$，若 $f(x)$ 不可约，则分解终止；否则，可以写成 $f(x) = g(x)h(x)$，其中 $\deg g(x), \deg h(x) < \deg f(x)$，然后对 $g(x)$ 和 $h(x)$ 继续进行分解。由于域 $\mathbb{F}_q$ 是有限的，因此归纳法可以顺利进行。

问：在有限域上，多项式分解是否一定可以分解为完全线性因子？
答：不一定。只有在扩域中，多项式才能分解为线性因子。例如，多项式 $x^2 + 1 \in \mathbb{F}_p[x]$（对于某些 p）在 $\mathbb{F}_p$ 上可能不可分解，但在某个合适的扩域中可以写成 $(x - \alpha)(x - \beta)$ 的形式。这一点与复数域上每个多项式都有根的情况类似，但在有限域中需要借助扩域构造。

3.3 因式分解算法与实例分析

在理论讨论之外，因式分解的实际算法也是数学研究和计算机实现的重要内容。这里我们简单介绍几种常见算法：

1. **试除法：**对多项式进行枚举检验，适用于低次数多项式。
2. **Berlekamp 算法：**一种经典的有限域多项式因式分解算法，基于有限域上线性代数的思想。
3. **Cantor-Zassenhaus 算法：**随机化算法，通常在计算机代数系统中实现效率较高。

例 3：考虑有限域 $\mathbb{F}_3$ 上的多项式 $f(x) = x^4 + x^2 + 2$。首先，我们尝试在 $\mathbb{F}_3$ 中寻找根。将 $x = 0, 1, 2$ 依次代入：

$$\begin{aligned} x = 0: &\quad f(0) = 2 \neq 0, \\ x = 1: &\quad f(1) = 1 + 1 + 2 = 4 \equiv 1 \pmod 3, \\ x = 2: &\quad f(2) = 16 + 4 + 2 = 22 \equiv 1 \pmod 3. \end{aligned}$$

显然 $f(x)$ 在 $\mathbb{F}_3$ 中没有线性因子。于是我们考虑是否存在不可约的二次多项式因子。假设

$$f(x) = (x^2 + ax + b)(x^2 + cx + d),$$

展开后比对系数，我们可以得到一组关于 a, b, c, d 的方程组。经过一番计算（这里略去繁琐的过程，读者可自行验证），我们发现 $f(x)$ 可以分解为

$$f(x) = (x^2 + x + 2)^2,$$

其中 $x^2 + x + 2 \in \mathbb{F}_3[x]$ 不可约。这一结果说明，在有限域中，多项式不仅可以有不可约因子，而且有时因子会出现重根的情况。

（此外，我们可以通过编程工具 Matlab 来实现有限域多项式因式分解。虽然这里不展开具体代码，但我可以告诉大家，Matlab 中有专门的工具箱可以处理有限域运算，例如利用 GF 函数构造有限域，并使用相应的函数进行因式分解。这样的数值实验不仅能加深对理论的理解，还能验证我们手算所得的结论。）

4 其他相关问题探讨

在完成了有限域上多项式因式分解的讨论后，我们还可以顺便探讨一些与之密切相关的问题。这些问题包括不可约多项式的判定、有限域上多项式根的分布以及与其他数学领域的联系等。下面我们逐一展开讨论。

4.1 多项式不可约性判定

多项式不可约性的判定是有限域上因式分解问题的前提。通常来说，对于一个多项式 $f(x) \in \mathbb{F}_q[x]$，若不存在次数小于 $\deg f(x)$ 的非平凡因子，则称 $f(x)$ 不可约。

判定方法：

1. **枚举法：**对于低次数多项式，可以直接枚举所有可能的因子进行验证。

2. **利用 Frobenius 映射：**设 $f(x)$ 为 $\mathbb{F}_q[x]$ 中的多项式，则 $f(x)$ 不可约当且仅当其在扩域中的分裂情况满足一定条件。具体来说，可以考察 $\gcd(f(x), x^{q^m} - x)$ 是否为 1，其中 m 是 $f(x)$ 的次数。

3. **其他判别准则：**比如利用一些特定的判别式或利用模 p 的特性。

问：是否所有不可约多项式都满足 $f(x) \mid (x^{q^m} - x)$？
答：是的，这是有限域中一个非常基本的事实。实际上，有限域 $\mathbb{F}_q$ 中所有元素都是 $x^q - x = 0$ 的根，而在扩域中类似的结论也成立。因此，不可约多项式必定整除某个形如 $x^{q^m} - x$ 的多项式。不过，这一结论的证明涉及到域的扩张和元素的循环结构，读者可参考高等代数教材。

4.2 有限域上多项式的根的分布问题

在有限域上，多项式根的分布呈现出与实数域和复数域截然不同的特点。由于有限域本身是有限的，多项式的根必定在有限的集合中取值。

讨论： 设 $f(x) \in \mathbb{F}_q[x]$，若 $f(x)$ 的分解式为

$$f(x) = a(x - \alpha_1)^{e_1}(x - \alpha_2)^{e_2} \cdots (x - \alpha_k)^{e_k},$$

其中 $\alpha_i \in \overline{\mathbb{F}}_q$（扩域中的元素），则可以证明 α_i 实际上都来自某个有限扩域 $\mathbb{F}_{q^m}$。这种现象提示我们，在研究有限域上多项式根时，必须考虑扩域的影响。

也许可以利用这种根的分布规律来设计一种快速检验多项式是否在某个给定有限域中有根的算法。毕竟，有限域中的元素有限，如果我们能有效枚举扩域中可能的根，就可能降低计算复杂度。不过，我猜这种方法在高次多项式上仍然会遇到瓶颈，需要借助更高级的算法，比如 Berlekamp 算法。

4.3 与其他领域的联系

有限域的因式分解问题并非孤立存在，它与数学的其他分支有着千丝万缕的联系。下面简单列举几种典型联系：

1. **密码学：**有限域上的多项式因式分解在构造公钥密码体制（如RSA、椭圆曲线密码等）中起到了重要作用。虽然这些应用更多涉及数论和椭圆曲线理论，但有限域的理论基础不可或缺。

2. **编码理论：**在纠错码的构造中，如 Reed-Solomon 码，就需要大量使用有限域上的多项式运算和因式分解。对于这些编码算法，我猜测进一步的优化可能与因式分解算法的改进有关。

3. **组合数学：**有限域上的多项式方法在组合设计、有限几何等领域也有应用。例如，通过多项式方法可以证明某些组合数的不可解性，这与有限域的性质有直接联系。

问：在编码理论中，有限域因式分解算法是否可以直接用于构造纠错码？

答：答案不尽然。实际上，编码理论中更多用到的是有限域上的插值问题和多项式求逆等运算，而因式分解算法主要用于解码过程中的错误定位问题。这两者虽然密切相关，但应用场景有所不同。

补充：

另外，在抽象代数中，有限域上的因式分解问题也与伽罗瓦理论密切相关。通过研究多项式的分裂域和伽罗华群，我们可以进一步理解有限域中多项式分解的内在机制。虽然伽罗华理论的内容较为抽象，但对于我们理解有限域上因式分解问题提供了深刻的理论解释。

一些联想：

我们在有限域上的讨论是否能推广到其他更一般的环结构上？答案可能是肯定的，但这需要引入更高层次的范畴论思想。我猜某种意义上，有限域的因式分解问题与自然变换之间也存在着微妙的联系。不过这些内容超出了当前笔记的讨论范围，留待以后有空时再探讨。