有理数域的单代数扩张

原生生物

2025 年 8 月 31 日

1 $\mathbb{Q}[\sqrt[a]{b}]$ 的含义

在这篇文章中，我们试着解决这样一个问题：对一般的正整数 a,b，$\mathbb{Q}[\sqrt[a]{b}]$ 何时是一个域。为此，我们需要先明确一些定义。

在一个集合上，定义加法 $(+)$ 与乘法 $(\times)$ 两种运算，如果集合满足在加法上构成一个阿贝尔群，在乘法上构成半群，且乘法对加法有左右分配律，则称为一个环；进一步地，如果在乘法上构成群，则称为一个域。

由于此处只考虑复数所构成的域，而复数的加法、乘法即为通常意义上的加法、乘法，定义可以简化为：如果某个复数集的非空子集对加减与乘法**封闭** (所谓对某种二元运算封闭是指，集合中任意两个元素 (可以相同) 在运算后仍在集合中)，则这个集合成为一个环；若含 1，且被除数不为 0 时对除法也封闭，则成为一个域，称为**数域**。

在此定义下，由于 1 出发通过加减乘除可得到所有有理数，因此有理数集 $\mathbb{Q}$ 是任何数域的子集。

对于 $\mathbb{Q}[\sqrt[a]{b}]$，一个标准的定义是：域 $\mathbb{Q}$ 在添加元素 $\sqrt[a]{b}$ 后形成的**最小**环 (此处的最小指任何包含 $\mathbb{Q}$ 与 $\sqrt[a]{b}$ 的环均包含这个环)。为了更明确地表达这句话的含义，我们对一般的元素 t 形成的 $\mathbb{Q}[t]$ 进行观察：由于环对乘法封闭，$a\in\mathbb{Q}$ 时，a 乘 t 的任意次方 at^n 均在 $\mathbb{Q}[t]$ 中，再由对加法封闭可知，任何 $\sum_{k=0}^{n}a_kt^k, a_0,\dots,a_n\in\mathbb{Q}$ 均在环中。这个形式与 $\mathbb{Q}[x]$ 完全一致 ($\mathbb{Q}[x]$ 为一切有理系数多项式 $\sum_{k=0}^{n}a_kx^k, a_0,\dots,a_n\in\mathbb{Q}$ 构成的集合)，事实上，由于 $\mathbb{Q}[t]$ 必然包含 $\sum_{k=0}^{n}a_kt^k, a_0,\dots,a_n\in\mathbb{Q}$，且两个关于 t 多项式乘积依然为关于 t 的多项式，$\mathbb{Q}[t]$ 即为把 t 代入所有有理系数多项式所能得到的可能值的集合。

举几个例子：当 $t\in\mathbb{Q}$ 时，由于代入有理系数多项式的结果仍为有理数，$\mathbb{Q}[t]$ 即为 $\mathbb{Q}$。若 $t=\sqrt{2}$，可以发现，由于 $at^2=2a, a\in\mathbb{Q}$，次数大于等于两次的有理系数多项式代入 $\sqrt{2}$ 后都可以化为两次以下，因此 $\mathbb{Q}[\sqrt{2}]=\{a+b\sqrt{2}, a,b\in\mathbb{Q}\}$。

由于 $\mathbb{Q}[t]$ 已经为环，且其中含 1，由定义知其为域当且仅当被除数不为 0 时除法的结果也在其中，又由于除法可以看作与倒数相乘，$\mathbb{Q}[t]$ 为域当且仅当非零元素的倒数在其中。

2 $\mathbb{Q}[\sqrt{b}]$ 的情况

由上方讨论可以发现，的 $\mathbb{Q}[\sqrt{b}], b\in\mathbb{N}^*$ 即为 $\{c+d\sqrt{b}, c,d\in\mathbb{Q}\}$。由于 $\sqrt{b}\in\mathbb{Q}$ 时，$\mathbb{Q}[\sqrt{b}]=\mathbb{Q}$，已经为域，不妨设 $\sqrt{b}\notin\mathbb{Q}$。当 $c-d\sqrt{b}=0$ 时，若 d 不为 0，则 $\sqrt{b}=\dfrac{c}{d}$，与其为无理数矛盾，于是 $d=0$，从而 $c=0, c+d\sqrt{b}=0$。因此，只要 $c+d\sqrt{b}\neq 0$，就有 $c-d\sqrt{b}\neq 0$。

由此可以计算 $\dfrac{1}{c+d\sqrt{b}}=\dfrac{c-d\sqrt{b}}{(c+d\sqrt{b})(c-d\sqrt{b})}=\dfrac{c-d\sqrt{b}}{c^2+d^2b}=\dfrac{c}{c^2-d^2b}-\dfrac{d}{c^2-d^2b}\sqrt{b}$，且 $c,d\in\mathbb{Q}, b\in\mathbb{N}^*\Rightarrow\dfrac{c}{c^2-d^2b},\dfrac{d}{c^2-d^2b}\in\mathbb{Q}$，因此 $\dfrac{1}{c+d\sqrt{b}}\in\mathbb{Q}[t]$，即证明了 $\mathbb{Q}[\sqrt{b}]$ 一定为域。

证明的实质是，试图通过分子分母同乘一些式子将分母化为有理数。但是，虽然这样看起来很简单对一般情况，这样操作会陷入对每个式子是否为 0 的讨论，而且不容易构造，因此无法如此做。

3 最小多项式

当我们考虑 $\mathbb{Q}[\sqrt[a]{b}]$ 时，类似之前的讨论可发现，$\mathbb{Q}[\sqrt[a]{b}]=f(\sqrt[a]{b})$，$f$ 为某个有理系数多项式。记 $t=\sqrt[a]{b}$ 倒数的实质是，我们希望对某个 $f(t)$，存在 $g(t)$ 使得 $f(t)g(t)=1$。如果对一般的 x 能找到 $f(x)g(x)=1$，代入 t 则问题已经解决，遗憾的是，讨论次数可得，只要 $f(x)$ 不是零次多项式，$f(x)g(x)$ 次数至少为 $f(x)$ 的次数，因此不可能为 1。

然而，事情未必没有转机。t 与一般的 x 不同的是，$t^a=b$，也即 $t^a-b=0$。如果能找到有理系数多项式 $g(x),h(x)$ 使得 $f(x)g(x)+h(x)(x^a-b)=1$，则代入 t 后即会变成 $f(x)g(x)=1$。为此，需要了解 x^a-b 的性质。下面引入一些背景知识 (为简化表达，如无特殊说明，**3,4 两部分中所有多项式均指非零有理系数多项式**)：

一个多项式**可约**是指，它可以写为两个次数至少为 1 的多项式的乘积。如 $x^2-\frac{1}{4}=(x+\frac{1}{2})(x-\frac{1}{2})$ 可约，而任何一次多项式不满足可约要求，因此不可约。

如果多项式 f 可写为多项式 g 与另一多项式 h 的乘积 (此处不要求次数)，则称 g **整除** f(由定义 h 也整除 f)，记为 $g|f$。对两个多项式，能同时整除它们的次数最大的多项式 (由于可以同乘有理数，不妨设最高次项系数为 1) 称为它们的**最大公约式**，记为 $\gcd(f,g)$。若两多项式最大公因式为 1，则称它们**互素**。

引理 1 *两多项式最大公因式存在且唯一。*

由于整除定义，可发现 f,g 的最大公约式与 $f,g-af(a$ 为多项式$)$ 相同，采取类似整数的辗转相除法，这里直接给两个操作范例：

对 x^4-2 与 x^3+x-1，先取 $-x$ 使得 $x^4-2-x(x^3+x-1)=-x^2+x-2$(注意其次数小于原来两多项式次数的最小值)，再取 $x+1$ 使 $x^3-x-1+(x+1)(-x^2+x-2)=-2x-3$，最后取 $-\frac{1}{2}x+\frac{5}{4}$ 使 $-x^2+x-2-(\frac{1}{2}x-\frac{5}{4})(-2x-3)=\frac{7}{4}$，因此 $\gcd(x^4-2,x^3+x-1)=\gcd(-x^2+x-2,x^3+x-1)=\gcd(-x^2+x-2,-2x-3)=\gcd(\frac{7}{4},-2x-3)=1$，两多项式互素。

对 x^3-1 与 x^2-1 先取 $-x$ 使得 $x^3-1-x(x^2-1)=x-1$，再取 $x+1$ 发现 $x^2-1-(x-1)(x+1)=0$，因此类似上方写出序列可得最大公因式为 $x-1$。

由于每次可使次数小于原来两多项式次数的最小值，这个操作一定可以进行下去，直到某个多项式 f' 整除另一个多项式 g'(由定义非零有理数整除任何多项式)，这时容易发现最小多项式即为 f' 将最高次项化为 1 的结果。

引理 2 *裴蜀定理：若两多项式 f,g 互素，则存在 (可能为 0 的) 多项式 a,b，使得 $af+bg=1$。*

事实上，我们利用操作的过程即可构建。由于使 $-x^2+x-2-(\frac{1}{2}x-\frac{5}{4})(-2x-3)=\frac{7}{4}$，可将 $-2x-3$ 用 $-2x-3=x^3-x-1+(x+1)(-x^2+x-2)$ 代入，再将 $-x^2+x-2$ 用 $x^2+x-2=x^4-2-x(x^3+x-1)$ 代入，展开、整理，即可得到 a,b 使 $a(x)(x^3+x-1)+b(x)(x^4-2)=\frac{7}{4}$，再将 a,b 同乘 $\frac{4}{7}$ 即可。

引理 3 *若多项式 $f(x)$ 不可约，则其与任何多项式的最大公因式为 $f(x)$ 最高次项化为 1 的结果或 1。*

直接利用不可约定义可知，整除 f 的多项式只有 0 次多项式与 f 的有理数倍，因此成立。

对任何复数，如果它是某个多项式的根 (例如此处的 $\sqrt[a]{b}$ 即为 x^a-b) 的根，则称其为**代数数**，将所有以它为根的多项式 (称为它的**化零多项式**) 中次数最小的那个 (由于可以同乘有理数，不妨设最高次项系数为 1) 称为它在 $\mathbb{Q}$ 上的**最小多项式**。例如，任何有理数 q 的最小多项式为 $x-q$，而 $\sqrt{2}$ 的最小多项式为 x^2-2。

引理 4 对任何代数数，存在唯一的最小多项式，且此多项式不可约。

对代数数 t，若不唯一，不妨设为 f,g，则有 $f(t)=g(t)=0$，由于任意多项式 $a(t)$，$f(t)-a(t)g(t)=0$，$\gcd(f,g)$ 亦为 t 的化零多项式，又由于最小性，其次数不可能更小，因此其次数必然等于 f,g 的次数，因此 f,g 均为其有理数倍，但 f,g 最高次项次数都为 1，因此 $f=g$，矛盾。

引理 5 对某个代数数，其任何化零多项式被最小多项式整除。

若否，类似上个引理证明中考虑最大公因式可构造次数小于最小多项式的化零多项式，由此矛盾。

4 证明与拓展

对于 $\mathbb{Q}[\sqrt[a]{b}]$，由之前可知使 $\sqrt[a]{b}$ 为 0 的多项式包括 x^a-b。若其不为最小多项式，则一定可以用更小的 a 替换 (如 $\sqrt[6]{9}$ 的最小多项式为 x^3-3，$\sqrt[6]{9}=\sqrt[3]{3}$)，因此不妨设其即为 $\sqrt[a]{b}$ 的最小多项式，记为 f_{ab}。

对 $\mathbb{Q}[\sqrt[a]{b}]$ 中某个不为 0 的元素，设其对应的多项式为 $g(\sqrt[a]{b})$，由引理 5，$g(x)$ 不被 f_{ab} 整除；由引理 4，f_{ab} 不可约。若 $\gcd(g,f_{ab})=f_{ab}$，则 f_{ab} 为 g 因式，矛盾，因此由引理 3，g 与 f_{ab} 互素，由引理 2 知存在多项式 s,t 使 $sg+tf_{ab}=1$。由于此处 f_{ab} 次数大于 1，s 不可能为 f_{ab} 的倍数，否则 f_{ab} 整除左侧，但不整除右侧，矛盾。代入 $\sqrt[a]{b}$ 可知 $s(\sqrt[a]{b})$ 即为 $g(\sqrt[a]{b})$ 的倒数。

由此可知，对任何 $\sqrt[a]{b}$，$\mathbb{Q}[\sqrt[a]{b}]$ 都能构成一个域。

不仅如此，可以发现，对任何代数数 t(注意代数数未必是实数)，设其最小多项式为 f，都可以类似上述证明操作，因此，对任何代数数 t，$\mathbb{Q}[t]$ 都构成一个域。记 $\mathbb{Q}(t)$ 为包含 $\mathbb{Q}$ 与 t 的最小域，由刚才的证明知此时 $\mathbb{Q}(t)=\mathbb{Q}[t]$。事实上，这种在 $\mathbb{Q}$ 中增添代数数之后封闭成的域称为 $\mathbb{Q}$ 的**代数扩张**，而这里只增添了一个 t(假设 t 不为有理数)，因此称为 $\mathbb{Q}$ 的**单代数扩张**。例如，$\mathbb{Q}(\sqrt[3]{2},\sqrt[3]{4}-1)$ 由于可以写成 $\mathbb{Q}(\sqrt[3]{2})$，因此也是 $\mathbb{Q}$ 的单代数扩张。

反过来，若 t 为**超越数**，即 t 不为代数数，即 $\mathbb{Q}[t]$ 不为域。若否，设 $t^{-1}=f(t)$，f 为某个多项式，则 $tf(t)-1=0$，由于 $xf(x)-1$ 亦为多项式，与超越数定义矛盾，由此得证。此时，为了使 $\mathbb{Q}(t)$ 为域，需要在其中增添所有形如 $\dfrac{f(t)}{g(t)}$ 元素，其中 f,g 为多项式。限于文章长度，此处的证明省略。此时，$\mathbb{Q}(t)$ 称为 $\mathbb{Q}$ 的**超越扩张**。

由此，我们得到最终结论：

$\mathbb{Q}[t]$ 为域 $\Leftrightarrow \mathbb{Q}[t]=\mathbb{Q}(t) \Leftrightarrow t$ 为代数数 $\Leftrightarrow$ 存在非零有理系数多项式 f 使得 t 为其根。