代数教学中渗透符号计算的理念

张圣贵

福建师范大学数计学院

March 20, 2008

内容提要

内容提要

内容提要

内容提要

内容提要

内容提要

内容提要

一. 引言

我们的《高等代数》、《线性代数》和《近世代数》的教学内容改革的主要特点: 将代数计算的理念贯彻到平时的代数教学过程中.

代数中的运算都是符号运算, 因此, 我们需要一种能进行符号计算的软件. 我选择了代数计算软件: CoCoA.

CoCoA是意大利Genova大学(University of Genova)的一个研究小组为《交换代数》的计算而设计的一个代数系统软件. 它的核心是计算域上的多项式环的理想的Geobner基的Buchberger算法. 要很好地使用这个软件, 必须对域上多项式环的理想的Geobner基理论有一定的了解. 这个软件主要进行符号计算.

一. 引言(续)

在工程应用等领域有大量的数值计算, 而数值计算已有很多优秀的软件, 比如, Matlab等. 这些软件已被广泛使用. 数值计算都是近似计算, 而代数计算常常要求精确计算. 在编码理论中编码和解码以及密码学中的加密和解密都要求精确计算. 如何在代数结构中用计算机进行精确计算是许多代数学家和计算机专家广泛关注的问题. 在国内, 本科的《高等代数》和《线性代数》以及《近世代数》的教学中引进计算机精确计算的尝试较少. 因此, 我在这个方面做了一些尝试, 学生普遍欢迎. 有一些做法已经分别在前几次会上做了交流. 现分几个方面, 通过典型例子给出说明.

二. 对称多项式

用初等对称多项式表示对称多项式:

例1 在3元多项式环$R[x,y,z]$中, 初等对称多项式为

$$\begin{aligned}\sigma_1 &= x+y+z\\ \sigma_2 &= xy+xz+yz\\ \sigma_3 &= xyz\end{aligned}$$

将对称多项式$(x-y)^4(y-z)^4(z-x)^4$表示为$\sigma_1,\sigma_2,\sigma_3$的多项式.

二. 对称多项式

用初等对称多项式表示对称多项式:

例1 在3元多项式环$R[x,y,z]$中, 初等对称多项式为

$$\begin{aligned}\sigma_1 &= x+y+z\\ \sigma_2 &= xy+xz+yz\\ \sigma_3 &= xyz\end{aligned}$$

将对称多项式$(x-y)^4(y-z)^4(z-x)^4$表示为$\sigma_1,\sigma_2,\sigma_3$的多项式.

$$\begin{aligned}&(x-y)^4(y-z)^4(z-x)^4\\ =\ & x^8y^4-4x^7y^5+6x^6y^6-4x^5y^7+x^4y^8-4x^8y^3z+12x^7y^4z-8x^6y^5z-8x^5y^6z\\ &+12x^4y^7z-4x^3y^8z+6x^8y^2z^2-8x^7y^3z^2-22x^6y^4z^2+48x^5y^5z^2-22x^4y^6z^2\\ &-8x^3y^7z^2+6x^2y^8z^2-4x^8yz^3-8x^7y^2z^3+48x^6y^3z^3-36x^5y^4z^3-36x^4y^5z^3\\ &+48x^3y^6z^3-8x^2y^7z^3-4xy^8z^3+x^8z^4+12x^7yz^4-22x^6y^2z^4-36x^5y^3z^4\\ &+90x^4y^4z^4-36x^3y^5z^4-22x^2y^6z^4+12xy^7z^4+y^8z^4-4x^7z^5-8x^6yz^5+48x^5y^2z^5\\ &-36x^4y^3z^5-36x^3y^4z^5+48x^2y^5z^5-8xy^6z^5-4y^7z^5+6x^6z^6-8x^5yz^6-22x^4y^2z^6\\ &+48x^3y^3z^6-22x^2y^4z^6-8xy^5z^6+6y^6z^6-4x^5z^7+12x^4yz^7-8x^3y^2z^7-8x^2y^3z^7\\ &+12xy^4z^7-4y^5z^7+x^4z^8-4x^3yz^8+6x^2y^2z^8-4xy^3z^8+y^4z^8\end{aligned}$$

二. 对称多项式(续)

$$
\begin{aligned}
& (x-y)^4(y-z)^4(z-x)^4 \\
= \; & (x+y+z)^4(xy+xz+yz)^4 - 8(x+y+z)^5(xy+xz+yz)^2(xyz) + 16(x+y+z)^6(xyz)^2 \\
& -8(x+y+z)^2(xy+xz+yz)^5 + 68(x+y+z)^3(xy+xz+yz)^3(xyz) \\
& -144(x+y+z)^4(xy+xz+yz)(xyz)^2 + 16(xy+xz+yz)^6 \\
& -144(x+y+z)(xy+xz+yz)^4(xyz) + 270(x+y+z)^2(xy+xz+yz)^2(xyz)^2 \\
& +216(x+y+z)^3(xyz)^3 + 216(xy+xz+yz)^3(xyz)^2 \\
& -972(x+y+z)(xy+xz+yz)(xyz)^3 + 729(xyz)^4
\end{aligned}
$$

二. 对称多项式(续)

$$
\begin{aligned}
& (x-y)^4(y-z)^4(z-x)^4 \\
= \; & (x+y+z)^4(xy+xz+yz)^4 - 8(x+y+z)^5(xy+xz+yz)^2(xyz) + 16(x+y+z)^6(xyz)^2 \\
& -8(x+y+z)^2(xy+xz+yz)^5 + 68(x+y+z)^3(xy+xz+yz)^3(xyz) \\
& -144(x+y+z)^4(xy+xz+yz)(xyz)^2 + 16(xy+xz+yz)^6 \\
& -144(x+y+z)(xy+xz+yz)^4(xyz) + 270(x+y+z)^2(xy+xz+yz)^2(xyz)^2 \\
& +216(x+y+z)^3(xyz)^3 + 216(xy+xz+yz)^3(xyz)^2 \\
& -972(x+y+z)(xy+xz+yz)(xyz)^3 + 729(xyz)^4 \\
= \; & \sigma_1^4\sigma_2^4 - 8\sigma_1^5\sigma_2^2\sigma_3 + 16\sigma_1^6\sigma_3^2 - 8\sigma_1^2\sigma_2^5 + 68\sigma_1^3\sigma_2^3\sigma_3 - 144\sigma_1^4\sigma_2\sigma_3^2 + 16\sigma_2^6 \\
& -144\sigma_1\sigma_2^4\sigma_3 + 270\sigma_1^2\sigma_2^2\sigma_3^2 + 216\sigma_1^3\sigma_3^3 + 216\sigma_2^3\sigma_3^2 - 972\sigma_1\sigma_2\sigma_3^3 + 729\sigma_3^4
\end{aligned}
$$

三. 标准正交基

例2 令

$$\epsilon_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \ \epsilon_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \ \epsilon_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \ \epsilon_4 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \ \alpha = \begin{pmatrix} \frac{1}{7}\sqrt{7} \\ \frac{2}{7}\sqrt{7} \\ \frac{1}{7}\sqrt{7} \\ \frac{1}{7}\sqrt{7} \end{pmatrix}.$$

求正交矩阵M使得$M\alpha = \epsilon_4$.

三. 标准正交基(续)

令$\alpha_1 = \alpha$,

$$M_1 = \begin{pmatrix} \frac{<\alpha_1,\epsilon_2>}{\sqrt{<\alpha_1,\epsilon_1>^2+<\alpha_1,\epsilon_2>^2}} & -\frac{<\alpha_1,\epsilon_1>}{\sqrt{<\alpha_1,\epsilon_1>^2+<\alpha_1,\epsilon_2>^2}} & 0 & 0 \\ \frac{<\alpha_1,\epsilon_1>}{\sqrt{<\alpha_1,\epsilon_1>^2+<\alpha_1,\epsilon_2>^2}} & \frac{<\alpha_1,\epsilon_2>}{\sqrt{<\alpha_1,\epsilon_1>^2+<\alpha_1,\epsilon_2>^2}} & 0 & 0 \\ 0 & & 0 & 1 & 0 \\ 0 & & 0 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} \frac{2}{5}\sqrt{5} & -\frac{1}{5}\sqrt{5} & 0 & 0 \\ \frac{1}{5}\sqrt{5} & \frac{2}{5}\sqrt{5} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

则

$$\alpha_2 = M_1\alpha_1 = \begin{pmatrix} 0 \\ \frac{1}{7}\sqrt{35} \\ \frac{1}{7}\sqrt{7} \\ \frac{1}{7}\sqrt{7} \end{pmatrix}.$$

三. 标准正交基(续)

令

$$M_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{<\alpha_2,\epsilon_3>}{\sqrt{<\alpha_2,\epsilon_2>^2+<\alpha_2,\epsilon_3>^2}} & -\frac{<\alpha_2,\epsilon_2>}{\sqrt{<\alpha_2,\epsilon_2>^2+<\alpha_2,\epsilon_3>^2}} & 0 \\ 0 & \frac{<\alpha_2,\epsilon_2>}{\sqrt{<\alpha_2,\epsilon_2>^2+<\alpha_2,\epsilon_3>^2}} & \frac{<\alpha_2,\epsilon_3>}{\sqrt{<\alpha_2,\epsilon_2>^2+<\alpha_2,\epsilon_3>^2}} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{6}\sqrt{6} & -\frac{1}{6}\sqrt{30} & 0 \\ 0 & \frac{1}{6}\sqrt{30} & \frac{1}{6}\sqrt{6} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

则

$$\alpha_3 = M_2\alpha_2 = \begin{pmatrix} 0 \\ 0 \\ \frac{1}{7}\sqrt{42} \\ \frac{1}{7}\sqrt{7} \end{pmatrix}.$$

三. 标准正交基(续)

令

$$M_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{<\alpha_3,\epsilon_4>}{\sqrt{<\alpha_3,\epsilon_3>^2+<\alpha_3,\epsilon_4>^2}} & -\frac{<\alpha_3,\epsilon_3>}{\sqrt{<\alpha_3,\epsilon_3>^2+<\alpha_3,\epsilon_4>^2}} \\ 0 & 0 & \frac{<\alpha_3,\epsilon_3>}{\sqrt{<\alpha_3,\epsilon_3>^2+<\alpha_3,\epsilon_4>^2}} & \frac{<\alpha_3,\epsilon_4>}{\sqrt{<\alpha_3,\epsilon_3>^2+<\alpha_3,\epsilon_4>^2}} \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1}{7}\sqrt{7} & -\frac{1}{7}\sqrt{42} \\ 0 & 0 & \frac{1}{7}\sqrt{42} & \frac{1}{7}\sqrt{7} \end{pmatrix}.$$

则

$$M = M_3M_2M_1 = \begin{pmatrix} \frac{2}{5}\sqrt{5} & -\frac{1}{5}\sqrt{5} & 0 & 0 \\ \frac{1}{30}\sqrt{30} & \frac{1}{15}\sqrt{30} & -\frac{1}{6}\sqrt{30} & 0 \\ \frac{1}{42}\sqrt{42} & \frac{1}{21}\sqrt{42} & \frac{1}{42}\sqrt{42} & -\frac{1}{7}\sqrt{42} \\ \frac{1}{7}\sqrt{7} & \frac{2}{7}\sqrt{7} & \frac{1}{7}\sqrt{7} & \frac{1}{7}\sqrt{7} \end{pmatrix}.$$

故有$M\alpha = \epsilon$.

三. 标准正交基(续)

例3 令

$$\alpha_1 = \begin{pmatrix} \frac{1}{2}\sqrt{2} \\ 0 \\ -\frac{1}{2} \\ \frac{1}{2} \end{pmatrix}, \alpha_2 = \begin{pmatrix} 0 \\ -\frac{1}{2}\sqrt{2} \\ -\frac{1}{2} \\ -\frac{1}{2} \end{pmatrix}, \alpha_3 = \begin{pmatrix} 0 \\ \frac{1}{2}\sqrt{2} \\ -\frac{1}{2} \\ -\frac{1}{2} \end{pmatrix}.$$

求正交矩阵A使得$A\alpha_1 = \epsilon_4, A\alpha_2 = \epsilon_3, A\alpha_3 = \epsilon_2$.

三. 标准正交基(续)

例3 令

$$\alpha_1 = \begin{pmatrix} \frac{1}{2}\sqrt{2} \\ 0 \\ -\frac{1}{2} \\ \frac{1}{2} \end{pmatrix}, \alpha_2 = \begin{pmatrix} 0 \\ -\frac{1}{2}\sqrt{2} \\ -\frac{1}{2} \\ -\frac{1}{2} \end{pmatrix}, \alpha_3 = \begin{pmatrix} 0 \\ \frac{1}{2}\sqrt{2} \\ -\frac{1}{2} \\ -\frac{1}{2} \end{pmatrix}.$$

求正交矩阵A使得$A\alpha_1 = \epsilon_4, A\alpha_2 = \epsilon_3, A\alpha_3 = \epsilon_2$.

求得

$$M_1 = \begin{pmatrix} 0 & -1 & 0 & 0 \\ -\frac{1}{3}\sqrt{3} & 0 & -\frac{1}{3}\sqrt{6} & 0 \\ \frac{1}{6}\sqrt{6} & 0 & -\frac{1}{6}\sqrt{3} & -\frac{1}{2}\sqrt{3} \\ \frac{1}{2}\sqrt{2} & 0 & -\frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

使得$M_1\alpha_1 = \epsilon_4$.

三. 标准正交基(续)

例3 令

$$\alpha_1 = \begin{pmatrix} \frac{1}{2}\sqrt{2} \\ 0 \\ -\frac{1}{2} \\ \frac{1}{2} \end{pmatrix}, \alpha_2 = \begin{pmatrix} 0 \\ -\frac{1}{2}\sqrt{2} \\ -\frac{1}{2} \\ -\frac{1}{2} \end{pmatrix}, \alpha_3 = \begin{pmatrix} 0 \\ \frac{1}{2}\sqrt{2} \\ -\frac{1}{2} \\ -\frac{1}{2} \end{pmatrix}.$$

求正交矩阵A使得$A\alpha_1 = \epsilon_4, A\alpha_2 = \epsilon_3, A\alpha_3 = \epsilon_2$.

求得

$$M_1 = \begin{pmatrix} 0 & -1 & 0 & 0 \\ -\frac{1}{3}\sqrt{3} & 0 & -\frac{1}{3}\sqrt{6} & 0 \\ \frac{1}{6}\sqrt{6} & 0 & -\frac{1}{6}\sqrt{3} & -\frac{1}{2}\sqrt{3} \\ \frac{1}{2}\sqrt{2} & 0 & -\frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

使得$M_1\alpha_1 = \epsilon_4$.

令$N_1 = M_1$. 则有

$$\alpha_{12} = N_1\alpha_2 = \begin{pmatrix} \frac{1}{2}\sqrt{2} \\ \frac{1}{6}\sqrt{6} \\ \frac{1}{3}\sqrt{3} \\ 0 \end{pmatrix}.$$

三. 标准正交基(续)

求得

$$M_2 = \begin{pmatrix} \frac{1}{2} & -\frac{1}{2}\sqrt{3} & 0 & 0 \\ \frac{1}{2} & \frac{1}{6}\sqrt{3} & -\frac{1}{3}\sqrt{6} & 0 \\ \frac{1}{2}\sqrt{2} & \frac{1}{6}\sqrt{6} & \frac{1}{3}\sqrt{3} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

使得$M_2\alpha_{12} = \epsilon_3$.

三. 标准正交基(续)

求得

$$M_2 = \begin{pmatrix} \frac{1}{2} & -\frac{1}{2}\sqrt{3} & 0 & 0 \\ \frac{1}{2} & \frac{1}{6}\sqrt{3} & -\frac{1}{3}\sqrt{6} & 0 \\ \frac{1}{2}\sqrt{2} & \frac{1}{6}\sqrt{6} & \frac{1}{3}\sqrt{3} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

使得$M_2\alpha_{12} = \epsilon_3$.

计算M_2N_1 和$N_2\alpha_3$, 有

$$N_2 = M_2N_1 = \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} & \frac{1}{2}\sqrt{2} & 0 \\ -\frac{1}{2} & -\frac{1}{2} & 0 & \frac{1}{2}\sqrt{2} \\ 0 & -\frac{1}{2}\sqrt{2} & -\frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2}\sqrt{2} & 0 & -\frac{1}{2} & \frac{1}{2} \end{pmatrix}, \quad \alpha_{23} = N_2\alpha_3 = \begin{pmatrix} -\frac{1}{2}\sqrt{2} \\ -\frac{1}{2}\sqrt{2} \\ 0 \\ 0 \end{pmatrix}$$

三. 标准正交基(续)

求得

$$M_3 = \begin{pmatrix} -\frac{1}{2}\sqrt{2} & \frac{1}{2}\sqrt{2} & 0 & 0 \\ -\frac{1}{2}\sqrt{2} & -\frac{1}{2}\sqrt{2} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

使得$M_3\alpha_{23} = \epsilon_2$.

三. 标准正交基(续)

求得

$$M_3 = \begin{pmatrix} -\frac{1}{2}\sqrt{2} & \frac{1}{2}\sqrt{2} & 0 & 0 \\ -\frac{1}{2}\sqrt{2} & -\frac{1}{2}\sqrt{2} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

使得$M_3\alpha_{23} = \epsilon_2$.

计算M_3N_2, 有

$$N_3 = M_3N_2 = \begin{pmatrix} -\frac{1}{2}\sqrt{2} & 0 & -\frac{1}{2} & \frac{1}{2} \\ 0 & \frac{1}{2}\sqrt{2} & -\frac{1}{2} & -\frac{1}{2} \\ 0 & -\frac{1}{2}\sqrt{2} & -\frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2}\sqrt{2} & 0 & -\frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

三. 标准正交基(续)

求得

$$M_3 = \begin{pmatrix} -\frac{1}{2}\sqrt{2} & \frac{1}{2}\sqrt{2} & 0 & 0 \\ -\frac{1}{2}\sqrt{2} & -\frac{1}{2}\sqrt{2} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

使得$M_3\alpha_{23} = \epsilon_2$.

计算M_3N_2, 有

$$N_3 = M_3N_2 = \begin{pmatrix} -\frac{1}{2}\sqrt{2} & 0 & -\frac{1}{2} & \frac{1}{2} \\ 0 & \frac{1}{2}\sqrt{2} & -\frac{1}{2} & -\frac{1}{2} \\ 0 & -\frac{1}{2}\sqrt{2} & -\frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2}\sqrt{2} & 0 & -\frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

令$A = N_3$, 则A是正交矩阵, 且$A\alpha_1 = \epsilon_4, A\alpha_2 = \epsilon_3, A\alpha_3 = \epsilon_2$.

四. 矩阵

在《高等代数》教学过程中, 常常要构造一些特征值为有理数的3阶有理对称矩阵, 作为作业或考题. 手工构造既枯燥又花时间. 用符号计算方法和代数计算软件CoCoA, 给出批量满足要求的有理对称矩阵的程序.

四. 矩阵(续)

构造出了下列有理对称矩阵:

$$\begin{pmatrix} \frac{2}{3} & -\frac{1}{3} & -\frac{1}{3} \\ -\frac{1}{3} & \frac{2}{3} & -\frac{1}{3} \\ -\frac{1}{3} & -\frac{1}{3} & \frac{2}{3} \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{4}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{4}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{4}{3} \end{pmatrix} \begin{pmatrix} \frac{5}{3} & \frac{2}{3} & \frac{2}{3} \\ \frac{2}{3} & \frac{5}{3} & \frac{2}{3} \\ \frac{2}{3} & \frac{2}{3} & \frac{5}{3} \end{pmatrix} \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}$$

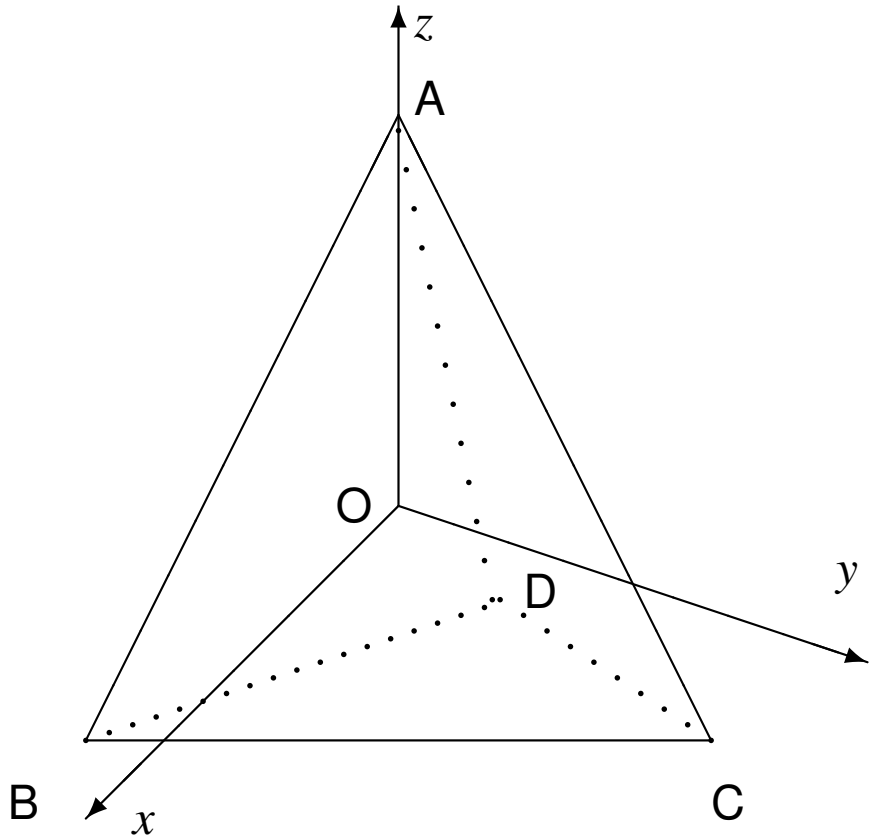
$$\begin{pmatrix} \frac{7}{3} & \frac{4}{3} & \frac{4}{3} \\ \frac{4}{3} & \frac{7}{3} & \frac{4}{3} \\ \frac{4}{3} & \frac{4}{3} & \frac{7}{3} \end{pmatrix} \begin{pmatrix} \frac{8}{3} & \frac{5}{3} & \frac{5}{3} \\ \frac{5}{3} & \frac{8}{3} & \frac{5}{3} \\ \frac{5}{3} & \frac{5}{3} & \frac{8}{3} \end{pmatrix} \begin{pmatrix} 3 & 2 & 2 \\ 2 & 3 & 2 \\ 2 & 2 & 3 \end{pmatrix} \begin{pmatrix} \frac{10}{3} & \frac{7}{3} & \frac{7}{3} \\ \frac{7}{3} & \frac{10}{3} & \frac{7}{3} \\ \frac{7}{3} & \frac{7}{3} & \frac{10}{3} \end{pmatrix} \begin{pmatrix} \frac{11}{3} & \frac{8}{3} & \frac{8}{3} \\ \frac{8}{3} & \frac{11}{3} & \frac{8}{3} \\ \frac{8}{3} & \frac{8}{3} & \frac{11}{3} \end{pmatrix}$$

它们的特征值依次分别为

$$(1,1,0),\ (1,1,1),\ (1,1,2),\ (1,1,3),\ (1,1,4),$$

$$(1,1,5),\ (1,1,6),\ (1,1,7),\ (1,1,8),\ (1,1,9).$$

五. 群论



五. 群论(续)

例4 在上图正四面体中, 设$\overline{AB} = \overline{AC} = \overline{AD} = \overline{BC} = \overline{BD} = \overline{CD} = 1$, 选正四面体的重心$O$为原点, 在$\Delta OAC$, 过$O$作一直线$\overline{OC'}$使得$\overline{OC'} \perp \overline{OA}$, 以$\overrightarrow{OA}$为$z-$轴, $\overrightarrow{OC'}$为$y-$轴, 向量积$\overrightarrow{OC'} \times \overrightarrow{OA}$为$x-$轴. 设$K, I, J$分别为$\overline{AB}, \overline{AC}, \overline{AD}$的中点.

五. 群论(续)

例4 在上图正四面体中, 设$\overline{AB}=\overline{AC}=\overline{AD}=\overline{BC}=\overline{BD}=\overline{CD}=1$, 选正四面体的重心$O$为原点, 在$\Delta OAC$, 过$O$作一直线$\overline{OC'}$使得$\overline{OC'}\perp\overline{OA}$, 以$\overrightarrow{OA}$为$z-$轴, $\overrightarrow{OC'}$为$y-$轴, 向量积$\overrightarrow{OC'}\times\overrightarrow{OA}$为$x-$轴. 设$K, I, J$分别为$\overline{AB}, \overline{AC}, \overline{AD}$的中点.

计算得,

$$
\begin{aligned}
\alpha_1 &= \overrightarrow{OA} = (0,0,\tfrac{\sqrt{6}}{4})^T,\\
\alpha_2 &= \overrightarrow{OB} = (\tfrac{1}{2},-\tfrac{\sqrt{3}}{6},-\tfrac{\sqrt{6}}{12})^T,\\
\alpha_3 &= \overrightarrow{OC} = (0,\tfrac{\sqrt{3}}{3},-\tfrac{\sqrt{6}}{12})^T,\\
\alpha_4 &= \overrightarrow{OD} = (-\tfrac{1}{2},-\tfrac{\sqrt{3}}{6},-\tfrac{\sqrt{6}}{12})^T,\\
\alpha_5 &= \overrightarrow{OI} = (0,\tfrac{1}{6}\sqrt{3},\tfrac{1}{12}\sqrt{6})^T,\\
\alpha_6 &= \overrightarrow{OJ} = (-\tfrac{1}{4},-\tfrac{1}{12}\sqrt{3},\tfrac{1}{12}\sqrt{6})^T,\\
\alpha_7 &= \overrightarrow{OK} = (\tfrac{1}{4},-\tfrac{1}{12}\sqrt{3},\tfrac{1}{12}\sqrt{6})^T,\\
\overline{\alpha}_5 &= -\alpha_5,\\
\overline{\alpha}_6 &= -\alpha_6,\\
\overline{\alpha}_7 &= -\alpha_7.
\end{aligned}
$$

五. 群论(续)

正四面体的旋转群$H=\{I,A_1,A_1^2,A_2,A_2^2,A_3,A_3^2,A_4,A_4^2,B_1,B_2,B_3\}$, 其中

$$I=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix},\quad A_1=\begin{pmatrix}-\frac{1}{2}&-\frac{1}{2}\sqrt{3}&0\\\frac{1}{2}\sqrt{3}&-\frac{1}{2}&0\\0&0&1\end{pmatrix},$$

$$A_1^2=\begin{pmatrix}-\frac{1}{2}&\frac{1}{2}\sqrt{3}&0\\-\frac{1}{2}\sqrt{3}&-\frac{1}{2}&0\\0&0&1\end{pmatrix},\quad A_2=\begin{pmatrix}\frac{1}{2}&-\frac{1}{6}\sqrt{3}&-\frac{1}{3}\sqrt{6}\\-\frac{1}{2}\sqrt{3}&-\frac{1}{6}&-\frac{1}{3}\sqrt{2}\\0&\frac{2}{3}\sqrt{2}&-\frac{1}{3}\end{pmatrix},$$

$$A_2^2=\begin{pmatrix}\frac{1}{2}&-\frac{1}{2}\sqrt{3}&0\\-\frac{1}{6}\sqrt{3}&-\frac{1}{6}&\frac{2}{3}\sqrt{2}\\-\frac{1}{3}\sqrt{6}&-\frac{1}{3}\sqrt{2}&-\frac{1}{3}\end{pmatrix},\quad A_3=\begin{pmatrix}-\frac{1}{2}&\frac{1}{6}\sqrt{3}&\frac{1}{3}\sqrt{6}\\-\frac{1}{6}\sqrt{3}&\frac{5}{6}&-\frac{1}{3}\sqrt{2}\\-\frac{1}{3}\sqrt{6}&-\frac{1}{3}\sqrt{2}&-\frac{1}{3}\end{pmatrix},$$

$$A_3^2=\begin{pmatrix}-\frac{1}{2}&-\frac{1}{6}\sqrt{3}&-\frac{1}{3}\sqrt{6}\\\frac{1}{6}\sqrt{3}&\frac{5}{6}&-\frac{1}{3}\sqrt{2}\\\frac{1}{3}\sqrt{6}&-\frac{1}{3}\sqrt{2}&-\frac{1}{3}\end{pmatrix},\quad A_4=\begin{pmatrix}\frac{1}{2}&\frac{1}{2}\sqrt{3}&0\\\frac{1}{6}\sqrt{3}&-\frac{1}{6}&\frac{2}{3}\sqrt{2}\\\frac{1}{3}\sqrt{6}&-\frac{1}{3}\sqrt{2}&-\frac{1}{3}\end{pmatrix},$$

$$A_4^2=\begin{pmatrix}\frac{1}{2}&\frac{1}{6}\sqrt{3}&\frac{1}{3}\sqrt{6}\\\frac{1}{2}\sqrt{3}&-\frac{1}{6}&-\frac{1}{3}\sqrt{2}\\0&\frac{2}{3}\sqrt{2}&-\frac{1}{3}\end{pmatrix},\quad B_1=\begin{pmatrix}-1&0&0\\0&\frac{1}{3}&\frac{2}{3}\sqrt{2}\\0&\frac{2}{3}\sqrt{2}&-\frac{1}{3}\end{pmatrix},$$

$$B_2=\begin{pmatrix}0&\frac{1}{3}\sqrt{3}&-\frac{1}{3}\sqrt{6}\\\frac{1}{3}\sqrt{3}&-\frac{2}{3}&-\frac{1}{3}\sqrt{2}\\-\frac{1}{3}\sqrt{6}&-\frac{1}{3}\sqrt{2}&-\frac{1}{3}\end{pmatrix},\quad B_3=\begin{pmatrix}0&-\frac{1}{3}\sqrt{3}&\frac{1}{3}\sqrt{6}\\-\frac{1}{3}\sqrt{3}&-\frac{2}{3}&-\frac{1}{3}\sqrt{2}\\\frac{1}{3}\sqrt{6}&-\frac{1}{3}\sqrt{2}&-\frac{1}{3}\end{pmatrix}.$$

五. 群论(续)

它的乘法表:

$\cdot$	I	A_1	A_1^2	A_2	A_2^2	A_3	A_3^2	A_4	A_4^2	B_1	B_2	B_3
I	I	A_1	A_1^2	A_2	A_2^2	A_3	A_3^2	A_4	A_4^2	B_1	B_2	B_3
A_1	A_1	A_1^2	I	A_4^2	B_2	A_2^2	B_3	A_3^2	B_1	A_2	A_3	A_4
A_1^2	A_1^2	I	A_1	B_1	A_3	B_2	A_4	B_3	A_2	A_4^2	A_2^2	A_3^2
A_2	A_2	A_3^2	B_2	A_2^2	I	A_4^2	B_1	A_1^2	B_3	A_1	A_4	A_3
A_2^2	A_2^2	B_1	A_4	I	A_2	B_3	A_1	B_2	A_3	A_3^2	A_1^2	A_4^2
A_3	A_3	A_4^2	B_3	A_1^2	B_1	A_3^2	I	A_2^2	B_2	A_4	A_1	A_2
A_3^2	A_3^2	B_2	A_2	B_3	A_4	I	A_3	B_1	A_1	A_2^2	A_4^2	A_1^2
A_4	A_4	A_2^2	B_1	A_3^2	B_3	A_1^2	B_2	A_4^2	I	A_3	A_2	A_1
A_4^2	A_4^2	B_3	A_3	B_2	A_1	B_1	A_2	I	A_4	A_1^2	A_3^2	A_2^2
B_1	B_1	A_4	A_2^2	A_3	A_1^2	A_2	A_4^2	A_1	A_3^2	I	B_3	B_2
B_2	B_2	A_2	A_3^2	A_1	A_4^2	A_4	A_1^2	A_3	A_2^2	B_3	I	B_1
B_3	B_3	A_3	A_4^2	A_4	A_3^2	A_1	A_2^2	A_2	A_1^2	B_2	B_1	I

五. 群论(续)

设$\Omega = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \alpha_7, \overline{\alpha}_5, \overline{\alpha}_6, \overline{\alpha}_7\}$, 则

$$\{M\alpha_i, M\overline{\alpha}_j | M \in H, i = 1, 2, 3, 4, 5, 6, 7, j = 5, 6, 7\} = \Omega,$$

$$\{M\alpha_i, M\overline{\alpha}_j | M \in G, i = 1, 2, 3, 4, 5, 6, 7, j = 5, 6, 7\} = \Omega.$$

$$H \times \Omega \to \Omega, \ (M, \alpha) \mapsto M\alpha, \forall M \in H$$

满足

(1) $I\alpha = \alpha$,

(2) $M_1(M_2\alpha) = (M_1M_2)\alpha$.

由此导出群作用的定义.

五. 群论(续)

若$\Omega = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \alpha_7, \overline{\alpha}_5, \overline{\alpha}_6, \overline{\alpha}_7\}$, 则

$$H(\alpha_1) = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\},\ H(\alpha_5) = \{\alpha_5, \alpha_6, \alpha_7, \overline{\alpha}_5, \overline{\alpha}_6, \overline{\alpha}_7\},$$

且

$$\Omega = H(\alpha_1) \cup H(\alpha_5),\ H(\alpha_1) \cap H(\alpha_5) = \emptyset.$$

五. 群论(续)

令$\Omega = \{\beta_{1,2}^n, \beta_{2,1}^n, \beta_{1,3}^n, \beta_{3,1}^n, \beta_{1,4}^n, \beta_{4,1}^n, \beta_{2,3}^n, \beta_{3,2}^n, \beta_{2,4}^n, \beta_{4,2}^n, \beta_{3,4}^n, \beta_{4,3}^n | n = 1, 2, \cdots\}$, 其中

$$
\begin{aligned}
\beta_{1,2}^n &= \tfrac{1}{n}\alpha_1 + (1-\tfrac{1}{n})\alpha_2,\ \beta_{2,1}^n = \tfrac{1}{n}\alpha_2 + (1-\tfrac{1}{n})\alpha_1,\\
\beta_{1,3}^n &= \tfrac{1}{n}\alpha_1 + (1-\tfrac{1}{n})\alpha_3,\ \beta_{3,1}^n = \tfrac{1}{n}\alpha_3 + (1-\tfrac{1}{n})\alpha_1,\\
\beta_{1,4}^n &= \tfrac{1}{n}\alpha_1 + (1-\tfrac{1}{n})\alpha_4,\ \beta_{4,1}^n = \tfrac{1}{n}\alpha_4 + (1-\tfrac{1}{n})\alpha_1,\\
\beta_{2,3}^n &= \tfrac{1}{n}\alpha_2 + (1-\tfrac{1}{n})\alpha_3,\ \beta_{3,2}^n = \tfrac{1}{n}\alpha_3 + (1-\tfrac{1}{n})\alpha_2,\\
\beta_{2,4}^n &= \tfrac{1}{n}\alpha_2 + (1-\tfrac{1}{n})\alpha_4,\ \beta_{4,2}^n = \tfrac{1}{n}\alpha_4 + (1-\tfrac{1}{n})\alpha_2,\\
\beta_{3,4}^n &= \tfrac{1}{n}\alpha_3 + (1-\tfrac{1}{n})\alpha_4,\ \beta_{4,3}^n = \tfrac{1}{n}\alpha_4 + (1-\tfrac{1}{n})\alpha_3.
\end{aligned}
$$

则

$$H(\beta_{1,2}^n) = \{\beta_{1,2}^n, \beta_{2,1}^n, \beta_{1,3}^n, \beta_{3,1}^n, \beta_{1,4}^n, \beta_{4,1}^n, \beta_{2,3}^n, \beta_{3,2}^n, \beta_{2,4}^n, \beta_{4,2}^n, \beta_{3,4}^n, \beta_{4,3}^n\},$$

$n = 1, 2, \cdots$, 且$\Omega = \bigcup_{n=1}^{\infty} H(\beta_{1,2}^n),\ H(\beta_{1,2}^n) \cap H(\beta_{1,2}^m) = \emptyset,\ n \neq m.$

六. 环论

1. 商环的结构

例5 令$u = \frac{-1+\sqrt{-3}}{2}$, 则$u \in \mathbb{C}$在$\mathbb{Z}$上的极小多项式为$x^2 + x + 1$.

故$\mathbb{Z}[u] = \{a + bu | a, b \in \mathbb{Z}\}$. 令$f(u) = 2 + 3u$. 给定$a + bu \in \mathbb{Z}[u]$, 有

$$(a + bu)(2 + 3u) = (2a - 3b) + (3a - b)u.$$

令$r_0(a, b) = 2a - 3b,\ r_1(a, b) = 3a - b$. 则$D = \begin{vmatrix} 2 & -3 \\ 3 & -1 \end{vmatrix} = 7$. 因此, 可计算得:

$$\mathbb{Z}[u]/(3u + 2) = \left\{ \begin{array}{cccc} 0 + (2 + 3u), & -1 + (2 + 3u), & -2 + (2 + 3u), & u + (2 + 3u), \\ u - 1 + (2 + 3u), & 2u + 1 + (2 + 3u), & 2u + (2 + 3u) & \end{array} \right\}$$

和一个集合$\mathcal{A} = \{(0, 0), (1, 3), (2, 6), (3, 2), (4, 5), (5, 1), (6, 4)\}$ 以及双

射$\eta : \mathcal{A} \to \mathbb{Z}[u]/(3u + 2)$,

$$\begin{array}{llll} (0,0) \leftrightarrow & 0 + (2 + 3u) & (4,5) \leftrightarrow & u - 1 + (2 + 3u) \\ (1,3) \leftrightarrow & -1 + (2 + 3u) & (5,1) \leftrightarrow & 2u + 1 + (2 + 3u) \\ (2,6) \leftrightarrow & -2 + (2 + 3u) & (6,4) \leftrightarrow & 2u + (2 + 3u) \\ (3,2) \leftrightarrow & u + (2 + 3u) & & \end{array}$$

六. 环论(续)

可得到双射$\psi : \mathcal{P} \to \mathcal{A}$,

$$
\begin{array}{lll}
 & & (5,5) \to (1,3) \\
(1,1) \to (0,0) & (3,3) \to (4,5) & (5,6) \to (2,6) \\
(1,2) \to (1,3) & (3,4) \to (5,1) & (5,7) \to (3,2) \\
(1,3) \to (2,6) & (3,5) \to (6,4) & (6,1) \to (5,1) \\
(1,4) \to (3,2) & (3,6) \to (0,0) & (6,2) \to (6,4) \\
(1,5) \to (4,5) & (3,7) \to (1,3) & (6,3) \to (0,0) \\
(1,6) \to (5,1) & (4,1) \to (3,2) & (6,4) \to (1,3) \\
(1,7) \to (6,4) & (4,2) \to (4,5) & (6,5) \to (2,6) \\
(2,1) \to (1,3) & (4,3) \to (5,1) & (6,6) \to (3,2) \\
(2,2) \to (2,6) & (4,4) \to (6,4) & (6,7) \to (4,5) \\
(2,3) \to (3,2) & (4,5) \to (0,0) & (7,1) \to (6,4) \\
(2,4) \to (4,5) & (4,6) \to (1,3) & (7,2) \to (0,0) \\
(2,5) \to (5,1) & (4,7) \to (2,6) & (7,3) \to (1,3) \\
(2,6) \to (6,4) & (5,1) \to (4,5) & (7,4) \to (2,6) \\
(2,7) \to (0,0) & (5,2) \to (5,1) & (7,5) \to (3,2) \\
(3,1) \to (2,6) & (5,3) \to (6,4) & (7,6) \to (4,5) \\
(3,2) \to (3,2) & (5,4) \to (0,0) & (7,7) \to (5,1)
\end{array}
$$

六. 环论(续)

由双射$\eta\psi : \mathcal{P} \to \mathbb{Z}[u]/(2+3u)$, 得到加法表:

$+$	0	-1	-2	u	$u-1$	$2u+1$	$2u$
0	0	-1	-2	u	$u-1$	$2u+1$	$2u$
-1	-1	-2	u	$u-1$	$2u+1$	$2u$	0
-2	-2	u	$u-1$	$2u+1$	$2u$	0	-1
u	u	$u-1$	$2u+1$	$2u$	0	-1	-2
$u-1$	$u-1$	$2u+1$	$2u$	0	-1	-2	u
$2u+1$	$2u+1$	$2u$	0	-1	-2	u	$u-1$
$2u$	$2u$	0	-1	-2	u	$u-1$	$2u+1$

六. 环论(续)

由双射$\eta\psi : \mathcal{P} \to \mathbb{Z}[u]/(2+3u)$, 得到加法表:

$+$	0	-1	-2	u	$u-1$	$2u+1$	$2u$
0	0	-1	-2	u	$u-1$	$2u+1$	$2u$
-1	-1	-2	u	$u-1$	$2u+1$	$2u$	0
-2	-2	u	$u-1$	$2u+1$	$2u$	0	-1
u	u	$u-1$	$2u+1$	$2u$	0	-1	-2
$u-1$	$u-1$	$2u+1$	$2u$	0	-1	-2	u
$2u+1$	$2u+1$	$2u$	0	-1	-2	u	$u-1$
$2u$	$2u$	0	-1	-2	u	$u-1$	$2u+1$

同样方法可得到乘法表:

$\times$	0	-1	-2	u	$u-1$	$2u+1$	$2u$
0	0	0	0	0	0	0	0
-1	0	$2u$	$2u+1$	$u-1$	u	-2	-1
-2	0	$2u+1$	u	-1	$2u$	$u-1$	-2
u	0	$u-1$	-1	$2u+1$	-2	$2u$	u
$u-1$	0	u	$2u$	-2	$2u+1$	-1	$u-1$
$2u+1$	0	-2	$u-1$	$2u$	-1	u	$2u+1$
$2u$	0	-1	-2	u	$u-1$	$2u+1$	$2u$

六. 环论(续)

2. 欧氏环

欧氏环的定义:

设R是一个整环, 令$R^* = R \setminus \{0\}$, $\mathbb{N}$为全体非负整数的集合, $\varphi : R^* \to \mathbb{N}$是映射. 若对于任意$a \in R^*$, $b \in R$, 存在$q, r \in R$使得$b = aq + r$, 其中$r = 0$或$\varphi(r) < \varphi(a)$, 则称R是欧氏环.

六. 环论(续)

2. 欧氏环

欧氏环的定义:

设R是一个整环, 令$R^* = R \setminus \{0\}$, $\mathbb{N}$为全体非负整数的集合, $\varphi : R^* \to \mathbb{N}$是映射. 若对于任意$a \in R^*$, $b \in R$, 存在$q, r \in R$使得$b = aq + r$, 其中$r = 0$或$\varphi(r) < \varphi(a)$, 则称R是欧氏环.

通常欧氏环的例子有整数环$\mathbb{Z}$, 域F上的多项式环$F[x]$, 整数环的扩环$\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{-2}]$和$\mathbb{Z}[\sqrt{3}]$.

六. 环论(续)

2. 欧氏环

欧氏环的定义:

设R是一个整环, 令$R^* = R \setminus \{0\}$, $\mathbb{N}$为全体非负整数的集合, $\varphi : R^* \to \mathbb{N}$是映射. 若对于任意$a \in R^*$, $b \in R$, 存在$q, r \in R$使得$b = aq + r$, 其中$r = 0$或$\varphi(r) < \varphi(a)$, 则称R是欧氏环.

通常欧氏环的例子有整数环$\mathbb{Z}$, 域F上的多项式环$F[x]$, 整数环的扩环$\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{-2}]$和$\mathbb{Z}[\sqrt{3}]$.

问题: 是否有其他欧氏环的例子?

六. 环论(续)

2. 欧氏环

欧氏环的定义:

设R是一个整环, 令$R^* = R \setminus \{0\}$, $\mathbb{N}$为全体非负整数的集合, $\varphi : R^* \to \mathbb{N}$是映射. 若对于任意$a \in R^*$, $b \in R$, 存在$q, r \in R$使得$b = aq + r$, 其中$r = 0$或$\varphi(r) < \varphi(a)$, 则称R是欧氏环.

通常欧氏环的例子有整数环$\mathbb{Z}$, 域F上的多项式环$F[x]$, 整数环的扩环$\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{-2}]$和$\mathbb{Z}[\sqrt{3}]$.

问题: 是否有其他欧氏环的例子?

为了构造新的欧氏环的例子, 我们先看下面例子的证明过程.

六. 环论(续)

例6 证明: 整环$\mathbb{Z}[\sqrt{3}] = \{m + n\sqrt{3} | m, n \in \mathbb{Z}\}$关于映射

$$\begin{aligned} \varphi : \mathbb{Z}[\sqrt{3}]^* &\to \mathbb{N} \\ m + n\sqrt{3} &\mapsto |m^2 - 3n^2|, \ \forall m + n\sqrt{3} \in \mathbb{Z}[\sqrt{3}] \end{aligned}$$

是一个欧氏环, 其中$\mathbb{N}$是非负整数集合, $\mathbb{Z}[\sqrt{3}]^* = \mathbb{Z}[\sqrt{3}] \backslash \{0\}$.

六. 环论(续)

例6 证明: 整环$\mathbb{Z}[\sqrt{3}] = \{m + n\sqrt{3} | m, n \in \mathbb{Z}\}$关于映射

$$\begin{aligned} \varphi : \mathbb{Z}[\sqrt{3}]^* &\to \mathbb{N} \\ m + n\sqrt{3} &\mapsto |m^2 - 3n^2|, \ \forall m + n\sqrt{3} \in \mathbb{Z}[\sqrt{3}] \end{aligned}$$

是一个欧氏环, 其中$\mathbb{N}$是非负整数集合, $\mathbb{Z}[\sqrt{3}]^* = \mathbb{Z}[\sqrt{3}] \backslash \{0\}$.

证明: $\forall a = m + n\sqrt{3} \in \mathbb{Z}[\sqrt{3}]^*$, $\forall b = p + q\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$, 有

$$\frac{b}{a} = \frac{p + q\sqrt{3}}{m + n\sqrt{3}} = \frac{pm - 3qn}{m^2 - 3n^2} + \frac{qm - pn}{m^2 - 3n^2}\sqrt{3}.$$

六. 环论(续)

例6 证明: 整环$\mathbb{Z}[\sqrt{3}] = \{m + n\sqrt{3} | m, n \in \mathbb{Z}\}$关于映射

$$\begin{aligned} \varphi : \mathbb{Z}[\sqrt{3}]^* &\to \mathbb{N} \\ m + n\sqrt{3} &\mapsto |m^2 - 3n^2|, \ \forall m + n\sqrt{3} \in \mathbb{Z}[\sqrt{3}] \end{aligned}$$

是一个欧氏环, 其中$\mathbb{N}$是非负整数集合, $\mathbb{Z}[\sqrt{3}]^* = \mathbb{Z}[\sqrt{3}] \backslash \{0\}$.

证明: $\forall a = m + n\sqrt{3} \in \mathbb{Z}[\sqrt{3}]^*$, $\forall b = p + q\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$, 有

$$\frac{b}{a} = \frac{p + q\sqrt{3}}{m + n\sqrt{3}} = \frac{pm - 3qn}{m^2 - 3n^2} + \frac{qm - pn}{m^2 - 3n^2}\sqrt{3}.$$

令

$$u = \frac{pm - 3qn}{m^2 - 3n^2}, \ v = \frac{qm - pn}{m^2 - 3n^2},$$

则$\frac{b}{a} = u + v\sqrt{3}$.

六. 环论(续)

取u', v'分别是与u, v最接近的整数, 则$|u - u'| \leq \frac{1}{2}, |v - v'| \leq \frac{1}{2}$.

六. 环论(续)

取u', v'分别是与u, v最接近的整数, 则$|u-u'| \leq \frac{1}{2}, |v-v'| \leq \frac{1}{2}$. 令$k = u-u'$, $l = v-v'$, 则$|k| \leq \frac{1}{2}, |l| \leq \frac{1}{2}$.

六. 环论(续)

取u', v'分别是与u, v最接近的整数, 则$|u-u'| \leq \frac{1}{2}, |v-v'| \leq \frac{1}{2}$. 令$k = u-u'$, $l = v-v'$, 则$|k| \leq \frac{1}{2}, |l| \leq \frac{1}{2}$. 从而

$$\begin{aligned} b &= a(u + v\sqrt{3}) \\ &= a[(u' + k) + (v' + l)\sqrt{3}] \\ &= a(u' + v'\sqrt{3}) + a(k + l\sqrt{3}) \\ &= aq + r \end{aligned}$$

六. 环论(续)

取u', v'分别是与u, v最接近的整数, 则$|u-u'| \leq \frac{1}{2}, |v-v'| \leq \frac{1}{2}$. 令$k = u-u'$, $l = v-v'$, 则$|k| \leq \frac{1}{2}, |l| \leq \frac{1}{2}$. 从而

$$\begin{aligned} b &= a(u + v\sqrt{3}) \\ &= a[(u' + k) + (v' + l)\sqrt{3}] \\ &= a(u' + v'\sqrt{3}) + a(k + l\sqrt{3}) \\ &= aq + r \end{aligned}$$

其中$q = u' + v'\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$, $r = a(k + l\sqrt{3}) = b - aq \in \mathbb{Z}[\sqrt{3}]$.

六. 环论(续)

若$r \neq 0$, 则

$$\begin{aligned}
\varphi(r) &= \varphi(a(k + l\sqrt{3})) \\
&= \varphi(mk + 3nl + (kn + lm)\sqrt{3}) \\
&= |(m^2 - 3n^2)(k^2 - 3l^2)| \\
&\leq \varphi(a)|k^2 - 3l^2| \\
&\leq \tfrac{3}{4}\varphi(a) \quad (\because \max_{-\frac{1}{2}\leq k\leq \frac{1}{2}, -\frac{1}{2}\leq l\leq \frac{1}{2}} |k^2 - 3l^2| = \tfrac{3}{4}) \\
&< \varphi(a)
\end{aligned}$$

六. 环论(续)

若$r \neq 0$, 则

$$\begin{aligned}
\varphi(r) &= \varphi(a(k+l\sqrt{3})) \\
&= \varphi(mk+3nl+(kn+lm)\sqrt{3}) \\
&= |(m^2-3n^2)(k^2-3l^2)| \\
&\leq \varphi(a)|k^2-3l^2| \\
&\leq \tfrac{3}{4}\varphi(a) \quad (\because \max_{-\frac{1}{2}\leq k\leq\frac{1}{2},-\frac{1}{2}\leq l\leq\frac{1}{2}} |k^2-3l^2| = \tfrac{3}{4}) \\
&< \varphi(a)
\end{aligned}$$

因此整环$\mathbb{Z}[\sqrt{3}] = \{m+n\sqrt{3}|m,n\in\mathbb{Z}\}$关于映射

$$\begin{aligned}
\varphi : \mathbb{Z}[\sqrt{3}]^* &\to \mathbb{N} \\
m+n\sqrt{3} &\mapsto |m^2-3n^2|, \ \forall m+n\sqrt{3}\in\mathbb{Z}[\sqrt{3}]
\end{aligned}$$

是一个欧氏环.

六. 环论(续)

例7 设$u=-\frac{1}{2}+\frac{1}{2}\sqrt{3}i$, 则$u$在$\mathbb{Z}$上的极小多项式为$x^2+x+1$.

令$\mathbb{Z}[u]=\{a+bu|a,b\in\mathbb{Z}\}$, 定义映射

$$\begin{aligned}\varphi:\ \mathbb{Z}[u]^* &\to \mathbb{N},\\ a+bu &\mapsto a^2-ab+b^2\end{aligned}$$

则$\mathbb{Z}[u]$关于映射φ构成欧式环.

六. 环论(续)

例7 设$u=-\frac{1}{2}+\frac{1}{2}\sqrt{3}i$, 则$u$在$\mathbb{Z}$上的极小多项式为$x^2+x+1$.

令$\mathbb{Z}[u]=\{a+bu|a,b\in\mathbb{Z}\}$, 定义映射

$$\begin{aligned}\varphi:\ \mathbb{Z}[u]^* &\to \mathbb{N},\\ a+bu &\mapsto a^2-ab+b^2\end{aligned}$$

则$\mathbb{Z}[u]$关于映射φ构成欧式环.

证明: $\forall m=a+bu\in\mathbb{Z}[u]^*$, $\forall n=c+du\in\mathbb{Z}[u]$, 有

$$\frac{n}{m}=\frac{c+du}{a+bu}=\frac{(c+du)((a-b-bu))}{(a+bu)((a-b-bu))}=\frac{ac-bc+bd}{a^2-ab+b^2}+\frac{-bc+ad}{a^2-ab+b^2}u.$$

六. 环论(续)

例7 设$u=-\frac{1}{2}+\frac{1}{2}\sqrt{3}i$, 则$u$在$\mathbb{Z}$上的极小多项式为$x^2+x+1$.

令$\mathbb{Z}[u]=\{a+bu|a,b\in\mathbb{Z}\}$, 定义映射

$$\begin{aligned}\varphi:\ \mathbb{Z}[u]^* &\to \mathbb{N},\\ a+bu &\mapsto a^2-ab+b^2\end{aligned}$$

则$\mathbb{Z}[u]$关于映射φ构成欧式环.

证明: $\forall m=a+bu\in\mathbb{Z}[u]^*$, $\forall n=c+du\in\mathbb{Z}[u]$, 有

$$\frac{n}{m}=\frac{c+du}{a+bu}=\frac{(c+du)((a-b-bu))}{(a+bu)((a-b-bu))}=\frac{ac-bc+bd}{a^2-ab+b^2}+\frac{-bc+ad}{a^2-ab+b^2}u.$$

令

$$w=\frac{ac-bc+bd}{a^2-ab+b^2},\ v=\frac{-bc+ad}{a^2-ab+b^2},$$

则

$$\frac{n}{m}=w+vu$$

六. 环论(续)

取w', v'分别是与w, v最接近的整数, 则$|w - w'| \leq \frac{1}{2}, |v - v'| \leq \frac{1}{2}$.

六. 环论(续)

取w', v'分别是与w, v最接近的整数, 则$|w - w'| \leq \frac{1}{2}, |v - v'| \leq \frac{1}{2}$. 令$k = u - u'$, $l = v - v'$, 则$|k| \leq \frac{1}{2}, |l| \leq \frac{1}{2}$.

六. 环论(续)

取w', v'分别是与w, v最接近的整数, 则$|w - w'| \leq \frac{1}{2}, |v - v'| \leq \frac{1}{2}$. 令$k = u - u'$, $l = v - v'$, 则$|k| \leq \frac{1}{2}, |l| \leq \frac{1}{2}$. 从而

$$\begin{aligned} n &= m(w + vu) \\ &= m[(w' + k) + (v' + l)u] \\ &= m(w' + v'u) + a(k + lu) \\ &= mq + r \end{aligned}$$

六. 环论(续)

取w', v'分别是与w, v最接近的整数, 则$|w - w'| \leq \frac{1}{2}, |v - v'| \leq \frac{1}{2}$. 令$k = u - u'$, $l = v - v'$, 则$|k| \leq \frac{1}{2}, |l| \leq \frac{1}{2}$. 从而

$$\begin{aligned} n &= m(w + vu) \\ &= m[(w' + k) + (v' + l)u] \\ &= m(w' + v'u) + a(k + lu) \\ &= mq + r \end{aligned}$$

其中$q = w' + v'u \in \mathbb{Z}[u]$, $r = m(k + lu) = n - mq \in \mathbb{Z}[u]$.

六. 环论(续)

若$r \neq 0$, 则

$$\begin{aligned}
\varphi(r) &= \varphi(m(k+lu)) \\
&= \varphi(ak - bl + (bk + al - bl)u) \\
&= (a^2 - ab + b^2)(k^2 - kl + l^2) \\
&\leq \varphi(m)(k^2 - kl + l^2) \\
&\leq \tfrac{3}{4}\varphi(m) \quad (\because \max_{-\frac{1}{2}\leq k\leq \frac{1}{2}, -\frac{1}{2}\leq l\leq \frac{1}{2}} k^2 - kl + l^2 = \tfrac{3}{4}) \\
&< \varphi(m)
\end{aligned}$$

六. 环论(续)

若$r \neq 0$, 则

$$\begin{aligned}
\varphi(r) &= \varphi(m(k+lu)) \\
&= \varphi(ak - bl + (bk + al - bl)u) \\
&= (a^2 - ab + b^2)(k^2 - kl + l^2) \\
&\leq \varphi(m)(k^2 - kl + l^2) \\
&\leq \tfrac{3}{4}\varphi(m) \quad (\because \max_{-\frac{1}{2}\leq k\leq \frac{1}{2}, -\frac{1}{2}\leq l\leq \frac{1}{2}} k^2 - kl + l^2 = \tfrac{3}{4}) \\
&< \varphi(m)
\end{aligned}$$

因此整环$\mathbb{Z}[u] = \{a + bu | a, b \in \mathbb{Z}\}$关于映射

$$\begin{aligned}
\varphi : \mathbb{Z}[u]\backslash\{0\} &\to \mathbb{N}, \\
a + bu &\mapsto a^2 - ab + b^2
\end{aligned}$$

是一个欧氏环.

六. 环论(续)

例8 设$u = \frac{1}{2} + \frac{1}{2}\sqrt{11}i$, 则$u$在$\mathbb{Z}$上的极小多项式为$x^2 - x + 3$.

令$\mathbb{Z}[u] = \{a + bu | a, b \in \mathbb{Z}\}$, 定义映射

$$\begin{aligned} \varphi : \mathbb{Z}[u]\backslash\{0\} &\to \mathbb{N}, \\ a + bu &\mapsto a^2 + ab + 3b^2 \end{aligned}$$

则$\mathbb{Z}[u]$关于映射φ构成欧式环.

六. 环论(续)

例8 设$u = \frac{1}{2} + \frac{1}{2}\sqrt{11}i$, 则$u$在$\mathbb{Z}$上的极小多项式为$x^2 - x + 3$.

令$\mathbb{Z}[u] = \{a + bu | a, b \in \mathbb{Z}\}$, 定义映射

$$\begin{aligned} \varphi : \mathbb{Z}[u]\backslash\{0\} &\to \mathbb{N}, \\ a + bu &\mapsto a^2 + ab + 3b^2 \end{aligned}$$

则$\mathbb{Z}[u]$关于映射φ构成欧式环.

先证明下列引理:

引理: 令$f(a, b) = a^2 + ab + 3b^2$. 则

六. 环论(续)

例8 设$u = \frac{1}{2} + \frac{1}{2}\sqrt{11}i$, 则$u$在$\mathbb{Z}$上的极小多项式为$x^2 - x + 3$.

令$\mathbb{Z}[u] = \{a + bu | a, b \in \mathbb{Z}\}$, 定义映射

$$\begin{aligned} \varphi : \mathbb{Z}[u]\backslash\{0\} &\to \mathbb{N}, \\ a + bu &\mapsto a^2 + ab + 3b^2 \end{aligned}$$

则$\mathbb{Z}[u]$关于映射φ构成欧式环.

先证明下列引理:

引理: 令$f(a, b) = a^2 + ab + 3b^2$. 则

(1) 当$\frac{1}{4} \le a \le \frac{1}{2}, \frac{1}{4} \le b \le \frac{1}{2}$时, $f(a - 1, b) \le \frac{15}{16}$.

六. 环论(续)

例8 设$u = \frac{1}{2} + \frac{1}{2}\sqrt{11}i$, 则$u$在$\mathbb{Z}$上的极小多项式为$x^2 - x + 3$.

令$\mathbb{Z}[u] = \{a + bu | a, b \in \mathbb{Z}\}$, 定义映射

$$\begin{aligned} \varphi : \mathbb{Z}[u]\backslash\{0\} &\to \mathbb{N}, \\ a + bu &\mapsto a^2 + ab + 3b^2 \end{aligned}$$

则$\mathbb{Z}[u]$关于映射φ构成欧式环.

先证明下列引理:

引理: 令$f(a, b) = a^2 + ab + 3b^2$. 则

(1) 当$\frac{1}{4} \le a \le \frac{1}{2}, \frac{1}{4} \le b \le \frac{1}{2}$时, $f(a - 1, b) \le \frac{15}{16}$.

(2) 当$-\frac{1}{2} \le a \le -\frac{1}{4}, -\frac{1}{2} \le b \le -\frac{1}{4}$时, $f(a + 1, b) \le \frac{15}{16}$.

六. 环论(续)

例8 设$u = \frac{1}{2} + \frac{1}{2}\sqrt{11}i$, 则$u$在$\mathbb{Z}$上的极小多项式为$x^2 - x + 3$.

令$\mathbb{Z}[u] = \{a + bu | a, b \in \mathbb{Z}\}$, 定义映射

$$\begin{aligned} \varphi : \mathbb{Z}[u]\backslash\{0\} &\to \mathbb{N}, \\ a + bu &\mapsto a^2 + ab + 3b^2 \end{aligned}$$

则$\mathbb{Z}[u]$关于映射φ构成欧式环.

先证明下列引理:

引理: 令$f(a, b) = a^2 + ab + 3b^2$. 则

(1) 当$\frac{1}{4} \le a \le \frac{1}{2}, \frac{1}{4} \le b \le \frac{1}{2}$时, $f(a - 1, b) \le \frac{15}{16}$.

(2) 当$-\frac{1}{2} \le a \le -\frac{1}{4}, -\frac{1}{2} \le b \le -\frac{1}{4}$时, $f(a + 1, b) \le \frac{15}{16}$.

(3) 其他情况, $f(a, b) \le \frac{15}{16}$.

六. 环论(续)

证明: 因$f(a,b)$是凸函数, 则其最大值在可行域的边界上达到.

六. 环论(续)

证明: 因$f(a,b)$是凸函数, 则其最大值在可行域的边界上达到.

(1) $f(a-1,b) = a^2 + ab - 2a + 3b^2 - b + 1,$

$$\begin{aligned} f(\tfrac{1}{4}-1,\tfrac{1}{2}) &= \tfrac{15}{16}, \\ f(\tfrac{1}{2}-1,\tfrac{1}{2}) &= \tfrac{3}{4}, \\ f(\tfrac{1}{4}-1,\tfrac{1}{4}) &= \tfrac{9}{16}, \\ f(\tfrac{1}{2}-1,\tfrac{1}{4}) &= \tfrac{5}{16}, \end{aligned}$$

则$f(a-1,b) \le \frac{15}{16}$.

六. 环论(续)

证明: 因$f(a,b)$是凸函数, 则其最大值在可行域的边界上达到.

(1) $f(a-1,b) = a^2 + ab - 2a + 3b^2 - b + 1,$

$$\begin{aligned} f(\tfrac{1}{4}-1,\tfrac{1}{2}) &= \tfrac{15}{16}, \\ f(\tfrac{1}{2}-1,\tfrac{1}{2}) &= \tfrac{3}{4}, \\ f(\tfrac{1}{4}-1,\tfrac{1}{4}) &= \tfrac{9}{16}, \\ f(\tfrac{1}{2}-1,\tfrac{1}{4}) &= \tfrac{5}{16}, \end{aligned}$$

则$f(a-1,b) \le \frac{15}{16}$.

(2) $f(a+1,b) = a^2 + ab + 3b^2 + 2a + b + 1,$

$$\begin{aligned} f(-\tfrac{1}{4}+1,-\tfrac{1}{2}) &= \tfrac{15}{16}, \\ f(-\tfrac{1}{2}+1,-\tfrac{1}{2}) &= \tfrac{3}{4}, \\ f(-\tfrac{1}{4}+1,-\tfrac{1}{4}) &= \tfrac{9}{16}, \\ f(-\tfrac{1}{2}+1,-\tfrac{1}{4}) &= \tfrac{5}{16}, \end{aligned}$$

则$f(a+1,b) \le \frac{15}{16}$.

六. 环论(续)

(3)

$$\begin{aligned} f(\tfrac{1}{2},-\tfrac{1}{2}) &= f(-\tfrac{1}{2},\tfrac{1}{2}) = \tfrac{3}{4}, \\ f(\tfrac{1}{2},\tfrac{1}{4}) &= f(-\tfrac{1}{2},-\tfrac{1}{4}) = \tfrac{9}{16}, \\ f(\tfrac{1}{4},\tfrac{1}{2}) &= f(-\tfrac{1}{4},-\tfrac{1}{2}) = \tfrac{15}{16}, \\ f(\tfrac{1}{4},\tfrac{1}{4}) &= f(-\tfrac{1}{4},-\tfrac{1}{4}) = \tfrac{5}{16}, \end{aligned}$$

则$f(a,b) \leq \frac{15}{16}$.

六. 环论(续)

(3)

$$\begin{aligned} f(\tfrac{1}{2},-\tfrac{1}{2}) &= f(-\tfrac{1}{2},\tfrac{1}{2}) = \tfrac{3}{4}, \\ f(\tfrac{1}{2},\tfrac{1}{4}) &= f(-\tfrac{1}{2},-\tfrac{1}{4}) = \tfrac{9}{16}, \\ f(\tfrac{1}{4},\tfrac{1}{2}) &= f(-\tfrac{1}{4},-\tfrac{1}{2}) = \tfrac{15}{16}, \\ f(\tfrac{1}{4},\tfrac{1}{4}) &= f(-\tfrac{1}{4},-\tfrac{1}{4}) = \tfrac{5}{16}, \end{aligned}$$

则$f(a,b) \leq \frac{15}{16}$.

利用此引理证明例8如下:

六. 环论(续)

(3)

$$\begin{aligned} f(\tfrac{1}{2},-\tfrac{1}{2}) &= f(-\tfrac{1}{2},\tfrac{1}{2}) = \tfrac{3}{4}, \\ f(\tfrac{1}{2},\tfrac{1}{4}) &= f(-\tfrac{1}{2},-\tfrac{1}{4}) = \tfrac{9}{16}, \\ f(\tfrac{1}{4},\tfrac{1}{2}) &= f(-\tfrac{1}{4},-\tfrac{1}{2}) = \tfrac{15}{16}, \\ f(\tfrac{1}{4},\tfrac{1}{4}) &= f(-\tfrac{1}{4},-\tfrac{1}{4}) = \tfrac{5}{16}, \end{aligned}$$

则$f(a,b) \leq \frac{15}{16}$.

利用此引理证明例8如下:

对于$a+bu \in \mathbb{Z}[u]*$, $c+du \in \mathbb{Z}[u]$, 有

$$\frac{c+du}{a+bu} = \frac{(c+du)([(a+b)-bu])}{(a+bu)[(a+b)-bu]} = \frac{(-bc+ad)u+ac+bc+3bd}{a^2+ab+3b^2}.$$

六. 环论(续)

(3)

$$\begin{aligned} f(\tfrac{1}{2},-\tfrac{1}{2}) &= f(-\tfrac{1}{2},\tfrac{1}{2}) = \tfrac{3}{4}, \\ f(\tfrac{1}{2},\tfrac{1}{4}) &= f(-\tfrac{1}{2},-\tfrac{1}{4}) = \tfrac{9}{16}, \\ f(\tfrac{1}{4},\tfrac{1}{2}) &= f(-\tfrac{1}{4},-\tfrac{1}{2}) = \tfrac{15}{16}, \\ f(\tfrac{1}{4},\tfrac{1}{4}) &= f(-\tfrac{1}{4},-\tfrac{1}{4}) = \tfrac{5}{16}, \end{aligned}$$

则$f(a,b) \le \frac{15}{16}$.

利用此引理证明例8如下:

对于$a+bu \in \mathbb{Z}[u]*$, $c+du \in \mathbb{Z}[u]$, 有

$$\frac{c+du}{a+bu} = \frac{(c+du)([(a+b)-bu])}{(a+bu)[(a+b)-bu]} = \frac{(-bc+ad)u+ac+bc+3bd}{a^2+ab+3b^2}.$$

令$p_1 = \frac{ac+bc+3bd}{a^2+ab+3b^2}$, $q_1 = \frac{-bc+ad}{a^2+ab+3b^2}$, 分别取最靠近$p_1$和$q_1$的整数$p_0$和$q_0$,

六. 环论(续)

(3)

$$\begin{aligned} f(\tfrac{1}{2},-\tfrac{1}{2}) &= f(-\tfrac{1}{2},\tfrac{1}{2}) = \tfrac{3}{4}, \\ f(\tfrac{1}{2},\tfrac{1}{4}) &= f(-\tfrac{1}{2},-\tfrac{1}{4}) = \tfrac{9}{16}, \\ f(\tfrac{1}{4},\tfrac{1}{2}) &= f(-\tfrac{1}{4},-\tfrac{1}{2}) = \tfrac{15}{16}, \\ f(\tfrac{1}{4},\tfrac{1}{4}) &= f(-\tfrac{1}{4},-\tfrac{1}{4}) = \tfrac{5}{16}, \end{aligned}$$

则$f(a,b) \le \frac{15}{16}$.

利用此引理证明例8如下:

对于$a+bu \in \mathbb{Z}[u]*$, $c+du \in \mathbb{Z}[u]$, 有

$$\frac{c+du}{a+bu} = \frac{(c+du)([(a+b)-bu])}{(a+bu)[(a+b)-bu]} = \frac{(-bc+ad)u+ac+bc+3bd}{a^2+ab+3b^2}.$$

令$p_1 = \frac{ac+bc+3bd}{a^2+ab+3b^2}$, $q_1 = \frac{-bc+ad}{a^2+ab+3b^2}$, 分别取最靠近$p_1$和$q_1$的整数$p_0$和$q_0$,

令$p = p_1 - p_0$, $q = q_1 - q_0$, 则$|p| \le \frac{1}{2}$, $|q| \le \frac{1}{2}$.

六. 环论(续)

对p, p_0作如下修正:

六. 环论(续)

对p, p_0作如下修正:

(1) 当$\frac{1}{4} \leq a \leq \frac{1}{2}, \frac{1}{4} \leq b \leq \frac{1}{2}$时, 令$\overline{p} = p - 1, \overline{p_0} = p_0 + 1.$

六. 环论(续)

对p, p_0作如下修正:

(1) 当$\frac{1}{4} \leq a \leq \frac{1}{2}, \frac{1}{4} \leq b \leq \frac{1}{2}$时, 令$\overline{p} = p - 1, \overline{p_0} = p_0 + 1$.

(2) 当$-\frac{1}{2} \leq a \leq -\frac{1}{4}, -\frac{1}{2} \leq b \leq -\frac{1}{4}$时, 令$\overline{p} = p + 1, \overline{p_0} = p_0 - 1$.

六. 环论(续)

对p, p_0作如下修正:

(1) 当$\frac{1}{4} \leq a \leq \frac{1}{2}, \frac{1}{4} \leq b \leq \frac{1}{2}$时, 令$\overline{p} = p - 1, \overline{p_0} = p_0 + 1$.

(2) 当$-\frac{1}{2} \leq a \leq -\frac{1}{4}, -\frac{1}{2} \leq b \leq -\frac{1}{4}$时, 令$\overline{p} = p + 1, \overline{p_0} = p_0 - 1$.

(3) 其他情况, 令$\overline{p} = p, \overline{p_0} = p_0$.

六. 环论(续)

对p, p_0作如下修正:

(1) 当$\frac{1}{4} \le a \le \frac{1}{2}, \frac{1}{4} \le b \le \frac{1}{2}$时, 令$\overline{p} = p - 1, \overline{p_0} = p_0 + 1$.

(2) 当$-\frac{1}{2} \le a \le -\frac{1}{4}, -\frac{1}{2} \le b \le -\frac{1}{4}$时, 令$\overline{p} = p + 1, \overline{p_0} = p_0 - 1$.

(3) 其他情况, 令$\overline{p} = p, \overline{p_0} = p_0$.

则

$$\begin{aligned} c + du &= (a + bu)(p_1 + q_1 u) \\ &= (a + bu)(p_0 + p + (q_0 + q)u) \\ &= (a + bu)(\overline{p_0} + \overline{p} + (q_0 + q)u) \\ &= (a + bu)(\overline{p_0} + q_0 u) + (a + bu)(\overline{p} + qu) \end{aligned}$$

六. 环论(续)

对p, p_0作如下修正:

(1) 当$\frac{1}{4} \le a \le \frac{1}{2}, \frac{1}{4} \le b \le \frac{1}{2}$时, 令$\overline{p} = p - 1, \overline{p_0} = p_0 + 1$.

(2) 当$-\frac{1}{2} \le a \le -\frac{1}{4}, -\frac{1}{2} \le b \le -\frac{1}{4}$时, 令$\overline{p} = p + 1, \overline{p_0} = p_0 - 1$.

(3) 其他情况, 令$\overline{p} = p, \overline{p_0} = p_0$.

则

$$\begin{aligned} c + du &= (a + bu)(p_1 + q_1 u) \\ &= (a + bu)(p_0 + p + (q_0 + q)u) \\ &= (a + bu)(\overline{p_0} + \overline{p} + (q_0 + q)u) \\ &= (a + bu)(\overline{p_0} + q_0 u) + (a + bu)(\overline{p} + qu) \end{aligned}$$

令$r = (a + bu)(\overline{p} + qu)$, 则$r = c + du - (a + bu)(\overline{p_0} + q_0 u) \in \mathbb{Z}[u]$.

六. 环论(续)

对p, p_0作如下修正:

(1) 当$\frac{1}{4} \le a \le \frac{1}{2}, \frac{1}{4} \le b \le \frac{1}{2}$时, 令$\overline{p} = p - 1, \overline{p_0} = p_0 + 1$.

(2) 当$-\frac{1}{2} \le a \le -\frac{1}{4}, -\frac{1}{2} \le b \le -\frac{1}{4}$时, 令$\overline{p} = p + 1, \overline{p_0} = p_0 - 1$.

(3) 其他情况, 令$\overline{p} = p, \overline{p_0} = p_0$.

则

$$\begin{aligned} c + du &= (a + bu)(p_1 + q_1 u) \\ &= (a + bu)(p_0 + p + (q_0 + q)u) \\ &= (a + bu)(\overline{p_0} + \overline{p} + (q_0 + q)u) \\ &= (a + bu)(\overline{p_0} + q_0 u) + (a + bu)(\overline{p} + qu) \end{aligned}$$

令$r = (a + bu)(\overline{p} + qu)$, 则$r = c + du - (a + bu)(\overline{p_0} + q_0 u) \in \mathbb{Z}[u]$. 若$r \neq 0$,

则$\varphi(r) = \varphi(a + bu)|\overline{p}^2 + \overline{p}q + 3q^2|$.

六. 环论(续)

对p, p_0作如下修正:

(1) 当$\frac{1}{4} \le a \le \frac{1}{2}, \frac{1}{4} \le b \le \frac{1}{2}$时, 令$\overline{p} = p - 1, \overline{p_0} = p_0 + 1$.

(2) 当$-\frac{1}{2} \le a \le -\frac{1}{4}, -\frac{1}{2} \le b \le -\frac{1}{4}$时, 令$\overline{p} = p + 1, \overline{p_0} = p_0 - 1$.

(3) 其他情况, 令$\overline{p} = p, \overline{p_0} = p_0$.

则

$$\begin{aligned} c + du &= (a + bu)(p_1 + q_1 u) \\ &= (a + bu)(p_0 + p + (q_0 + q)u) \\ &= (a + bu)(\overline{p_0} + \overline{p} + (q_0 + q)u) \\ &= (a + bu)(\overline{p_0} + q_0 u) + (a + bu)(\overline{p} + qu) \end{aligned}$$

令$r = (a + bu)(\overline{p} + qu)$, 则$r = c + du - (a + bu)(\overline{p_0} + q_0 u) \in \mathbb{Z}[u]$. 若$r \neq 0$,

则$\varphi(r) = \varphi(a + bu)|\overline{p}^2 + \overline{p}q + 3q^2|$. 由引理知, $|\overline{p}^2 + \overline{p}q + 3q^2| \le \frac{15}{16} < 1$,

则$\varphi(r) < \varphi(a + bu)$.

六. 环论(续)

对p, p_0作如下修正:

(1) 当$\frac{1}{4} \le a \le \frac{1}{2}, \frac{1}{4} \le b \le \frac{1}{2}$时, 令$\overline{p} = p - 1, \overline{p_0} = p_0 + 1$.

(2) 当$-\frac{1}{2} \le a \le -\frac{1}{4}, -\frac{1}{2} \le b \le -\frac{1}{4}$时, 令$\overline{p} = p + 1, \overline{p_0} = p_0 - 1$.

(3) 其他情况, 令$\overline{p} = p, \overline{p_0} = p_0$.

则

$$\begin{aligned} c + du &= (a + bu)(p_1 + q_1 u) \\ &= (a + bu)(p_0 + p + (q_0 + q)u) \\ &= (a + bu)(\overline{p_0} + \overline{p} + (q_0 + q)u) \\ &= (a + bu)(\overline{p_0} + q_0 u) + (a + bu)(\overline{p} + qu) \end{aligned}$$

令$r = (a + bu)(\overline{p} + qu)$, 则$r = c + du - (a + bu)(\overline{p_0} + q_0 u) \in \mathbb{Z}[u]$. 若$r \neq 0$,

则$\varphi(r) = \varphi(a + bu)|\overline{p}^2 + \overline{p}q + 3q^2|$. 由引理知, $|\overline{p}^2 + \overline{p}q + 3q^2| \le \frac{15}{16} < 1$,

则$\varphi(r) < \varphi(a + bu)$. 则$\mathbb{Z}[u]$关于映射$\varphi$构成欧式环.

六. 环论(续)

3. 商环中方根的计算

例9在$\mathbb{Z}[i]/(13)$上, 计算$1+(13)$的平方根.

六. 环论(续)

3. 商环中方根的计算

例9在$\mathbb{Z}[i]/(13)$上, 计算$1+(13)$的平方根.

解: $13=(2+3i)(2-3i)$, 则由中国剩余定理,

$$\mathbb{Z}[i]/(13)\cong\mathbb{Z}[i]/(2+3i)\times\mathbb{Z}[i]/(2-3i).$$

六. 环论(续)

3. 商环中方根的计算

例9在$\mathbb{Z}[i]/(13)$上, 计算$1+(13)$的平方根.

解: $13=(2+3i)(2-3i)$, 则由中国剩余定理,

$$\mathbb{Z}[i]/(13)\cong\mathbb{Z}[i]/(2+3i)\times\mathbb{Z}[i]/(2-3i).$$

若有$a+bi, c+di\in\mathbb{Z}[i]$使得$2+3i=(a+bi)(c+di)$, 则$13=(a^2+b^2)(c^2+d^2)$, 故

$$\begin{cases} a^2+b^2 = 1 \\ c^2+d^2 = 13 \end{cases}, \begin{cases} a^2+b^2 = 13 \\ c^2+d^2 = 1 \end{cases}.$$

六. 环论(续)

3. 商环中方根的计算

例9在$\mathbb{Z}[i]/(13)$上, 计算$1+(13)$的平方根.

解: $13=(2+3i)(2-3i)$, 则由中国剩余定理,

$$\mathbb{Z}[i]/(13)\cong\mathbb{Z}[i]/(2+3i)\times\mathbb{Z}[i]/(2-3i).$$

若有$a+bi, c+di\in\mathbb{Z}[i]$使得$2+3i=(a+bi)(c+di)$, 则$13=(a^2+b^2)(c^2+d^2)$, 故

$$\begin{cases} a^2+b^2 = 1 \\ c^2+d^2 = 13 \end{cases}, \begin{cases} a^2+b^2 = 13 \\ c^2+d^2 = 1 \end{cases}.$$

若

$$\begin{cases} a^2+b^2 = 1 \\ c^2+d^2 = 13 \end{cases},$$

则$a+bi$为$\mathbb{Z}[i]$的单位.

六. 环论(续)

若

$$\begin{cases} a^2 + b^2 = 13 \\ c^2 + d^2 = 1 \end{cases},$$

则$a + bi$为$2 + 3i$的相伴元. 因此$2 + 3i$是$\mathbb{Z}[i]$的不可约元. 同理, $2 - 3i$是$\mathbb{Z}[i]$的不可约元. 从而$\mathbb{Z}[i]/(2 + 3i)$和$\mathbb{Z}[i]/(2 - 3i)$都是域.

六. 环论(续)

若

$$\begin{cases} a^2+b^2 &= 13 \\ c^2+d^2 &= 1 \end{cases},$$

则$a+bi$为$2+3i$的相伴元. 因此$2+3i$是$\mathbb{Z}[i]$的不可约元. 同理, $2-3i$是$\mathbb{Z}[i]$的不可约元. 从而$\mathbb{Z}[i]/(2+3i)$和$\mathbb{Z}[i]/(2-3i)$都是域.

若$a+bi+(13) \in \mathbb{Z}[i]/(13)$使得$[a+bi+(13)]^2 = 1+(13)$, 即

$$\begin{cases} [a+bi+(2+3i)]^2 &= 1+(2+3i) \\ [a+bi+(2-3i)]^2 &= 1+(2-3i) \end{cases}.$$

在域$\mathbb{Z}[i]/(2+3i)$和$\mathbb{Z}[i]/(2-3i)$中, 平方根最多只有两个, 则

$$\begin{cases} a+bi+(2+3i) &= 1+(2+3i) \\ a+bi+(2-3i) &= 1+(2-3i) \end{cases}, \quad \begin{cases} a+bi+(2+3i) &= -1+(2+3i) \\ a+bi+(2-3i) &= 1+(2-3i) \end{cases},$$
$$\begin{cases} a+bi+(2+3i) &= 1+(2+3i) \\ a+bi+(2-3i) &= -1+(2-3i) \end{cases}, \quad \begin{cases} a+bi+(2+3i) &= -1+(2+3i) \\ a+bi+(2-3i) &= -1+(2-3i) \end{cases}.$$

六. 环论(续)

1. 若

$$\begin{cases} a+bi+(2+3i) = 1+(2+3i) \\ a+bi+(2-3i) = 1+(2-3i) \end{cases},$$

则

$$\begin{cases} a+bi-1 \in (2+3i) \\ a+bi-1 \in (2-3i) \end{cases},$$

即存在$c+di, e+fi \in \mathbb{Z}[i]$使得

$$\begin{cases} a+bi-1 = (2+3i)(c+di) = (3c+2d)i+2c-3d \\ a+bi-1 = (2-3i)(e+fi) = (-3e+2f)i+2e+3f \end{cases},$$

六. 环论(续)

1. 若

$$\begin{cases} a+bi+(2+3i) = 1+(2+3i) \\ a+bi+(2-3i) = 1+(2-3i) \end{cases},$$

则

$$\begin{cases} a+bi-1 \in (2+3i) \\ a+bi-1 \in (2-3i) \end{cases},$$

即存在$c+di, e+fi \in \mathbb{Z}[i]$使得

$$\begin{cases} a+bi-1 = (2+3i)(c+di) = (3c+2d)i+2c-3d \\ a+bi-1 = (2-3i)(e+fi) = (-3e+2f)i+2e+3f \end{cases},$$

因此

$$\begin{cases} 3c+2d = a-1 \\ 2c-3d = b \\ -3e+2f = a-1 \\ 2e+3f = b \end{cases} \tag{1}$$

六. 环论(续)

解方程组(1)得,

$$\begin{cases} c = \frac{1}{13}(3a+2b-3) \\ d = \frac{1}{13}(2a-3b-2) \\ e = \frac{1}{13}(-3a+2b+3) \\ f = \frac{1}{13}(2a+3b-2) \end{cases} \tag{2}$$

六. 环论(续)

解方程组(1)得,

$$\begin{cases} c &= \frac{1}{13}(3a+2b-3) \\ d &= \frac{1}{13}(2a-3b-2) \\ e &= \frac{1}{13}(-3a+2b+3) \\ f &= \frac{1}{13}(2a+3b-2) \end{cases} \tag{2}$$

因为$c,d,e,f \in \mathbb{Z}$, 且$a+bi+(13) \in \mathbb{Z}[i]/(13)$, 所以有$0 \le a \le 12$, $0 \le b \le 12$, 且

$$\begin{cases} 3a+2b-3 \equiv 0 \pmod{13} \\ 2a-3b-2 \equiv 0 \pmod{13} \\ -3a+2b+3 \equiv 0 \pmod{13} \\ 2a+3b-2 \equiv 0 \pmod{13} \end{cases} \tag{3}$$

解同余方程组(3)得,

$$\begin{cases} a = 1 \\ b = 0 \end{cases}$$

六. 环论(续)

2. 若

$$\begin{cases} a+bi+(2+3i) &= -1+(2+3i) \\ a+bi+(2-3i) &= \quad 1+(2-3i) \end{cases},$$

则

$$\begin{cases} a+bi+1 \in (2+3i) \\ a+bi-1 \in (2-3i) \end{cases},$$

即存在$c+di, e+fi \in \mathbb{Z}[i]$使得

$$\begin{cases} a+bi+1 &= (2+3i)(c+di) &= \quad (3c+2d)i+2c-3d \\ a+bi-1 &= \quad (2-3i)(e+fi) &= (-3e+2f)i+2e+3f \end{cases},$$

因此

$$\begin{cases} \quad 3c+2d &= a+1 \\ \quad 2c-3d &= b \\ -3e+2f &= a-1 \\ \quad 2e+3f &= b \end{cases} \tag{4}$$

六. 环论(续)

解方程组(4)得,

$$\begin{cases} c &= \frac{1}{13}(3a+2b+3) \\ d &= \frac{1}{13}(2a-3b+2) \\ e &= \frac{1}{13}(-3a+2b+3) \\ f &= \frac{1}{13}(2a+3b-2) \end{cases} \tag{5}$$

因为$c,d,e,f \in \mathbb{Z}$, 且$a+bi+(13) \in \mathbb{Z}[i]/(13)$, 所以有$0 \le a \le 12$, $0 \le b \le 12$, 且

$$\begin{cases} 3a+2b+3 \equiv 0 \pmod{13} \\ 2a-3b+2 \equiv 0 \pmod{13} \\ -3a+2b+3 \equiv 0 \pmod{13} \\ 2a+3b-2 \equiv 0 \pmod{13} \end{cases} \tag{6}$$

解同余方程组(6)得,

$$\begin{cases} a &= 0 \\ b &= 5 \end{cases}$$

六. 环论(续)

3. 若

$$\begin{cases} a+bi+(2+3i) &= 1+(2+3i) \\ a+bi+(2-3i) &= -1+(2-3i) \end{cases},$$

则

$$\begin{cases} a+bi-1 &\in (2+3i) \\ a+bi+1 &\in (2-3i) \end{cases},$$

即存在$c+di, e+fi \in \mathbb{Z}[i]$使得

$$\begin{cases} a+bi-1 &= (2+3i)(c+di) &= (3c+2d)i+2c-3d \\ a+bi+1 &= (2-3i)(e+fi) &= (-3e+2f)i+2e+3f \end{cases},$$

因此

$$\begin{cases} 3c+2d &= a-1 \\ 2c-3d &= b \\ -3e+2f &= a+1 \\ 2e+3f &= b \end{cases} \tag{7}$$

六. 环论(续)

解方程组(7)得,

$$\begin{cases} c &= \frac{1}{13}(3a+2b-3) \\ d &= \frac{1}{13}(2a-3b-2) \\ e &= \frac{1}{13}(-3a+2b-3) \\ f &= \frac{1}{13}(2a+3b+2) \end{cases} \tag{8}$$

因为$c,d,e,f \in \mathbb{Z}$, 且$a+bi+(13) \in \mathbb{Z}[i]/(13)$, 所以有$0 \le a \le 12$, $0 \le b \le 12$, 且

$$\begin{cases} 3a+2b-3 \equiv 0 \pmod{13} \\ 2a-3b-2 \equiv 0 \pmod{13} \\ -3a+2b-3 \equiv 0 \pmod{13} \\ 2a+3b+2 \equiv 0 \pmod{13} \end{cases} \tag{9}$$

解同余方程组(9)得,

$$\begin{cases} a &= 0 \\ b &= 8 \end{cases}$$

六. 环论(续)

4. 若

$$\begin{cases} a+bi+(2+3i) &= -1+(2+3i) \\ a+bi+(2-3i) &= -1+(2-3i) \end{cases},$$

则

$$\begin{cases} a+bi+1 &\in (2+3i) \\ a+bi+1 &\in (2-3i) \end{cases},$$

即存在$c+di, e+fi \in \mathbb{Z}[i]$使得

$$\begin{cases} a+bi+1 &= (2+3i)(c+di) &= (3c+2d)i+2c-3d \\ a+bi+1 &= (2-3i)(e+fi) &= (-3e+2f)i+2e+3f \end{cases},$$

因此

$$\begin{cases} 3c+2d &= a+1 \\ 2c-3d &= b \\ -3e+2f &= a+1 \\ 2e+3f &= b \end{cases} \tag{10}$$

六. 环论(续)

解方程组(10)得,

$$\begin{cases} c = \frac{1}{13}(3a+2b+3) \\ d = \frac{1}{13}(2a-3b+2) \\ e = \frac{1}{13}(-3a+2b-3) \\ f = \frac{1}{13}(2a+3b+2) \end{cases} \tag{11}$$

因为$c,d,e,f \in \mathbb{Z}$, 且$a+bi+(13) \in \mathbb{Z}[i]/(13)$, 所以有$0 \le a \le 12$, $0 \le b \le 12$, 且

$$\begin{cases} 3a+2b+3 \equiv 0 \pmod{13} \\ 2a-3b+2 \equiv 0 \pmod{13} \\ -3a+2b-3 \equiv 0 \pmod{13} \\ 2a+3b+2 \equiv 0 \pmod{13} \end{cases} \tag{12}$$

解同余方程组(12)得,

$$\begin{cases} a = 12 \\ b = 0 \end{cases}$$

因此$1+(13)$在$\mathbb{Z}[i]$的平方根为$1+(13), 12+(13), 5i+(13), 8i+(13)$.

七. 域论

1. 中学分母有理化

对于形如

$$\frac{a+b\sqrt[n]{2}}{c+d\sqrt[n]{3}}$$

(其中$c,d\in\mathbb{Q}$且$cd\neq 0$)的分式的分母有理化问题, 主要利用公式

$$a^n-b^n=(a-b)(a^{n-1}+a^{n-2}b+\cdots+ab^{n-2}+b^{n-1}),$$

将其分母有理化,

七. 域论

1. 中学分母有理化

对于形如

$$\frac{a+b\sqrt[n]{2}}{c+d\sqrt[n]{3}}$$

(其中$c,d\in\mathbb{Q}$且$cd\neq 0$)的分式的分母有理化问题, 主要利用公式

$$a^n-b^n=(a-b)(a^{n-1}+a^{n-2}b+\cdots+ab^{n-2}+b^{n-1}),$$

将其分母有理化, 即

$$\begin{aligned}\frac{a+b\sqrt[n]{2}}{c+d\sqrt[n]{3}} &= \frac{(a+b\sqrt[n]{2})[c^{n-1}+c^{n-2}(-d\sqrt[n]{3})+\cdots+c(-d\sqrt[n]{3})^{n-2}+(-d\sqrt[n]{3})^{n-1}]}{(c+d\sqrt[n]{3})[c^{n-1}+c^{n-2}(-d\sqrt[n]{3})+\cdots+c(-d\sqrt[n]{3})^{n-2}+(-d\sqrt[n]{3})^{n-1}]}\\ &= \frac{(a+b\sqrt[n]{2})[c^{n-1}+c^{n-2}(-d\sqrt[n]{3})+\cdots+c(-d\sqrt[n]{3})^{n-2}+(-d\sqrt[n]{3})^{n-1}]}{(c^n+3d^n)}\end{aligned}$$

七. 域论(续)

问题1: 在域$\mathbb{Q}(\sqrt{2},\sqrt{3})=\{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}|a,b,c,d\in\mathbb{Q}\}$中, 对于形如

$$\frac{e+f\sqrt{2}+g\sqrt{3}+h\sqrt{6}}{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}}$$

的分式, 如何将其分母有理化?

七. 域论(续)

问题1: 在域$\mathbb{Q}(\sqrt{2},\sqrt{3})=\{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}|a,b,c,d\in\mathbb{Q}\}$中, 对于形如

$$\frac{e+f\sqrt{2}+g\sqrt{3}+h\sqrt{6}}{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}}$$

的分式, 如何将其分母有理化?

问题1等价于找$e+f\sqrt{2}+g\sqrt{3}+h\sqrt{6}\in\mathbb{Q}(\sqrt{2},\sqrt{3})$ 使得

$$(e+f\sqrt{2}+g\sqrt{3}+h\sqrt{6})(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6})\in\mathbb{Q}.$$

七. 域论(续)

我们采用待定系数法:

$$\begin{aligned}&(e+f\sqrt{2}+g\sqrt{3}+h\sqrt{6})(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6})\\=\ &(ae+2bf+3cg+6dh)+(be+af+3dg+3ch)\sqrt{2}\\&+(ce+2df+ag+2bh)\sqrt{3}+(de+cf+bg+ah)\sqrt{6}\end{aligned}$$

七. 域论(续)

我们采用待定系数法:

$$\begin{aligned}&(e+f\sqrt{2}+g\sqrt{3}+h\sqrt{6})(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6})\\=\ &(ae+2bf+3cg+6dh)+(be+af+3dg+3ch)\sqrt{2}\\&+(ce+2df+ag+2bh)\sqrt{3}+(de+cf+bg+ah)\sqrt{6}\end{aligned}$$

令

$$\begin{cases} ae+2bf+3cg+6dh = D \\ be+af+3dg+3ch = 0 \\ ce+2df+ag+2bh = 0 \\ de+cf+bg+ah = 0 \end{cases} \tag{13}$$

七. 域论(续)

我们采用待定系数法:

$$\begin{aligned}&(e+f\sqrt{2}+g\sqrt{3}+h\sqrt{6})(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6})\\=\ &(ae+2bf+3cg+6dh)+(be+af+3dg+3ch)\sqrt{2}\\&+(ce+2df+ag+2bh)\sqrt{3}+(de+cf+bg+ah)\sqrt{6}\end{aligned}$$

令

$$\begin{cases} ae+2bf+3cg+6dh = D\\ be+af+3dg+3ch = 0\\ ce+2df+ag+2bh = 0\\ de+cf+bg+ah = 0\end{cases} \tag{13}$$

其中

$$\begin{aligned}D &= \begin{vmatrix} a & 2b & 3c & 6d\\ b & a & 3d & 3c\\ c & 2d & a & 2b\\ d & c & b & a\end{vmatrix}\\ &= a^4-4a^2b^2+4b^4-6a^2c^2-12b^2c^2+9c^4\\ &\quad +48abcd-12a^2d^2-24b^2d^2-36c^2d^2+36d^4\end{aligned}$$

七. 域论(续)

用克莱姆法则解关于变量e,f,g,h的线性方程组(13)得,

$$\begin{aligned} e &= a^3 - 2ab^2 - 3ac^2 + 12bcd - 6ad^2 \\ f &= -a^2b + 2b^3 - 3bc^2 + 6acd - 6bd^2 \\ g &= -a^2c - 2b^2c + 3c^3 + 4abd - 6cd^2 \\ h &= 2abc - a^2d - 2b^2d - 3c^2d + 6d^3 \end{aligned}$$

七. 域论(续)

用克莱姆法则解关于变量e,f,g,h的线性方程组(13)得,

$$\begin{aligned} e &= a^3 - 2ab^2 - 3ac^2 + 12bcd - 6ad^2 \\ f &= -a^2b + 2b^3 - 3bc^2 + 6acd - 6bd^2 \\ g &= -a^2c - 2b^2c + 3c^3 + 4abd - 6cd^2 \\ h &= 2abc - a^2d - 2b^2d - 3c^2d + 6d^3 \end{aligned}$$

例如,

$$(2 - \sqrt{2} + 3\sqrt{3} - 4\sqrt{6})(-98 - 19\sqrt{2} - 193\sqrt{3} - 264\sqrt{6}) = 4441$$

七. 域论(续)

问题2: 更一般地, 若$p(x)$和$q(x)$都是有理数域$\mathbb{Q}$上的次数大于1的两个不同的不可约多项式,

七. 域论(续)

问题2: 更一般地, 若$p(x)$和$q(x)$都是有理数域$\mathbb{Q}$上的次数大于1的两个不同的不可约多项式, u和v分别是$p(x)$和$q(x)$在复数域$\mathbb{C}$上的根,

七. 域论(续)

问题2: 更一般地, 若$p(x)$和$q(x)$都是有理数域$\mathbb{Q}$上的次数大于1的两个不同的不可约多项式, u和v分别是$p(x)$和$q(x)$在复数域$\mathbb{C}$上的根, 设$p(x)$的次数$\partial p(x) = m$, $q(x)$的次数$\partial q(x) = n$,

七. 域论(续)

问题2: 更一般地, 若$p(x)$和$q(x)$都是有理数域$\mathbb{Q}$上的次数大于1的两个不同的不可约多项式, u和v分别是$p(x)$和$q(x)$在复数域$\mathbb{C}$上的根, 设$p(x)$的次数$\partial p(x) = m$, $q(x)$的次数$\partial q(x) = n$, 则在$\mathbb{Q}$上的代数扩张

$$\mathbb{Q}(u,v) = \left\{ \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} a_{ij} u^i v^j \middle| a_{ij} \in \mathbb{Q}, i = 0,1,2,\cdots,m-1, j = 0,1,2,\cdots,n-1 \right\}$$

中,

七. 域论(续)

问题2: 更一般地, 若$p(x)$和$q(x)$都是有理数域$\mathbb{Q}$上的次数大于1的两个不同的不可约多项式, u和v分别是$p(x)$和$q(x)$在复数域$\mathbb{C}$上的根, 设$p(x)$的次数$\partial p(x) = m$, $q(x)$的次数$\partial q(x) = n$, 则在$\mathbb{Q}$上的代数扩张

$$\mathbb{Q}(u,v) = \left\{ \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} a_{ij} u^i v^j \middle| a_{ij} \in \mathbb{Q}, i = 0,1,2,\cdots,m-1, j = 0,1,2,\cdots,n-1 \right\}$$

中, 对于分式

$$\frac{\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} b_{ij} u^i v^j}{\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} a_{ij} u^i v^j},$$

如何将其分母有理化?

七. 域论(续)

2. 有理化方法

问题2等价于给定

$$\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} a_{ij}u^i v^j \in \mathbb{Q}(u,v),$$

找出

$$\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} b_{ij}u^i v^j \in \mathbb{Q}(u,v)$$

使得

$$(\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} a_{ij}u^i v^j)(\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} b_{ij}u^i v^j) \in \mathbb{Q}.$$

七. 域论(续)

给定$\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} a_{ij}u^i v^j \in \mathbb{Q}(u,v)$, 我们有下列有理化步骤:

Step 1. 求多项式环$\mathbb{Q}[a_{00},\cdots,a_{0n-1},\cdots,a_{m-11},\cdots,a_{m-1n-1},x,y]$的理想

$$< \sum_{j=0}^{n-1} a_{ij}x^i y^j, p(x), q(y) >$$

在$x > y > a_{00} > \cdots > a_{0n-1} > \cdots > a_{m-11} > \cdots > a_{m-1n-1}$的字典序下的简化Gröbner基, 并找出简化Gröbner基中不含x,y的多项式$f(a_{00},\cdots,a_{0n-1},\cdots,a_{m-11},\cdots,a_{m-1n-1})$.

七. 域论(续)

Step 2. 计算$(\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} a_{ij}x^iy^j)(\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} b_{ij}x^iy^j)$除以$p(x)$和$q(y)$所得的余式

$$\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} f_{ij}(b_{00},\cdots,b_{0n-1},\cdots,b_{m-11},\cdots,b_{m-1n-1})x^iy^j,$$

其中$f_{ij}(b_{00},\cdots,b_{0n-1},\cdots,b_{m-11},\cdots,b_{m-1n-1})$都

是$b_{00},\cdots,b_{0n-1},\cdots,b_{m-11},\cdots,b_{m-1n-1}$的线性函数,

$i=0,1,2,\cdots,m-1, j=0,1,2,\cdots,n-1.$

七. 域论(续)

Step 2. 计算$(\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} a_{ij}x^iy^j)(\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} b_{ij}x^iy^j)$除以$p(x)$和$q(y)$所得的余式

$$\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} f_{ij}(b_{00},\cdots,b_{0n-1},\cdots,b_{m-11},\cdots,b_{m-1n-1})x^iy^j,$$

其中$f_{ij}(b_{00},\cdots,b_{0n-1},\cdots,b_{m-11},\cdots,b_{m-1n-1})$都

是$b_{00},\cdots,b_{0n-1},\cdots,b_{m-11},\cdots,b_{m-1n-1}$的线性函数,

$i=0,1,2,\cdots,m-1, j=0,1,2,\cdots,n-1.$

Step 3. 解关于变量$b_{00},\cdots,b_{0n-1},\cdots,b_{m-11},\cdots,b_{m-1n-1}$的线性方程组

$$\begin{cases} f_{00}(b_{00},\cdots,b_{0n-1},\cdots,b_{m-11},\cdots,b_{m-1n-1}) = f(a_{00},\cdots,a_{0n-1},\cdots,a_{m-11},\cdots,a_{m-1n-1}) \\ f_{ij}(b_{00},\cdots,b_{0n-1},\cdots,b_{m-11},\cdots,b_{m-1n-1}) = 0, i=1,2,\cdots,m-1, j=1,2,\cdots,n-1 \end{cases}$$

可求得$b_{00},\cdots,b_{0n-1},\cdots,b_{m-11},\cdots,b_{m-1n-1}$使得

$$(\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} a_{ij}u^iv^j)(\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} b_{ij}u^iv^j)\in\mathbb{Q}.$$

七. 域论(续)

3. 算例

下面我们以一个例子说明上节有理化方法的可行性.

七. 域论(续)

3. 算例

下面我们以一个例子说明上节有理化方法的可行性.

例10 设u是多项式$x^3 - 4x + 2$的一个根, 给定元素$a + bu + cu^2 \in \mathbb{Q}(u)$, 求一个元素$d + eu + fu^2 \in \mathbb{Q}(u)$使得$(a + bu + cu^2)(d + eu + fu^2) \in \mathbb{Q}$.

七. 域论(续)

3. 算例

下面我们以一个例子说明上节有理化方法的可行性.

例10 设u是多项式$x^3 - 4x + 2$的一个根, 给定元素$a + bu + cu^2 \in \mathbb{Q}(u)$, 求一个元素$d + eu + fu^2 \in \mathbb{Q}(u)$使得$(a + bu + cu^2)(d + eu + fu^2) \in \mathbb{Q}$.

解: 用上述有理化方法, 求解如下:

七. 域论(续)

3. 算例

下面我们以一个例子说明上节有理化方法的可行性.

例10 设u是多项式x^3-4x+2的一个根, 给定元素$a+bu+cu^2\in\mathbb{Q}(u)$, 求一个元素$d+eu+fu^2\in\mathbb{Q}(u)$使得$(a+bu+cu^2)(d+eu+fu^2)\in\mathbb{Q}$.

解: 用上述有理化方法, 求解如下:

- Step 1. 求多项式环$\mathbb{Q}[a,b,c,x]$的理想$< a+bx+cx^2, x^3-4x+2 >$

  在$x>a>b>c$的字典序下的简化Gröbner基

$$\left\{\begin{array}{l} x^3-4x+2,\\ cx^2+bx+a,\\ bx^2+ax+4cx-2c, ax^2-2cx-4a-2b,\\ b^2x-acx-4c^2x+ab+2c^2,\\ abx+2c^2x+a^2+4ac+2bc,\\ a^2x+4acx+2bcx+4ab+2b^2-2ac,\\ a^3-4ab^2-2b^3+8a^2c+6abc+16ac^2+8bc^2+4c^3 \end{array}\right\}$$

七. 域论(续)

3. 算例

下面我们以一个例子说明上节有理化方法的可行性.

例10 设u是多项式x^3-4x+2的一个根, 给定元素$a+bu+cu^2\in\mathbb{Q}(u)$, 求一个元素$d+eu+fu^2\in\mathbb{Q}(u)$使得$(a+bu+cu^2)(d+eu+fu^2)\in\mathbb{Q}$.

解: 用上述有理化方法, 求解如下:

- Step 1. 求多项式环$\mathbb{Q}[a,b,c,x]$的理想$<a+bx+cx^2, x^3-4x+2>$

  在$x>a>b>c$的字典序下的简化Gröbner基

$$\left\{\begin{array}{l} x^3-4x+2,\\ cx^2+bx+a,\\ bx^2+ax+4cx-2c, ax^2-2cx-4a-2b,\\ b^2x-acx-4c^2x+ab+2c^2,\\ abx+2c^2x+a^2+4ac+2bc,\\ a^2x+4acx+2bcx+4ab+2b^2-2ac,\\ a^3-4ab^2-2b^3+8a^2c+6abc+16ac^2+8bc^2+4c^3 \end{array}\right\}$$

其中不含x,y的多项式为$a^3-4ab^2-2b^3+8a^2c+6abc+16ac^2+8bc^2+4c^3$.

七. 域论(续)

- Step 2. 计算$(a+bx+cx^2)(d+ex+fx^2)$除以x^3-4x+2所得的余式

$$(cd+be+af+4cf)x^2+(bd+ae+4ce+4bf-2cf)x+ad-2ce-2bf.$$

七. 域论(续)

- Step 2. 计算$(a+bx+cx^2)(d+ex+fx^2)$除以x^3-4x+2所得的余式

$$(cd+be+af+4cf)x^2+(bd+ae+4ce+4bf-2cf)x+ad-2ce-2bf.$$

- Step 3. 解关于变量d,e,f的线性方程组

$$\begin{cases} cd+be+(a+4c)f & = 0 \\ bd+(a+4c)e+(4b-2c)f & = 0 \\ ad-2ce-2bf & = D \end{cases}$$

七. 域论(续)

- Step 2. 计算$(a+bx+cx^2)(d+ex+fx^2)$除以x^3-4x+2所得的余式

$$(cd+be+af+4cf)x^2+(bd+ae+4ce+4bf-2cf)x+ad-2ce-2bf.$$

- Step 3. 解关于变量d,e,f的线性方程组

$$\begin{cases} cd+be+(a+4c)f & = 0 \\ bd+(a+4c)e+(4b-2c)f & = 0 \\ ad-2ce-2bf & = D \end{cases}$$

可求得

$$\begin{cases} d & = a^2-4b^2+8ac+2bc+16c^2 \\ e & = -ab-2c^2 \\ f & = b^2-ac-4c^2 \end{cases}$$

七. 域论(续)

其中

$$D = \begin{vmatrix} c & b & a+4c \\ b & a+4c & 4b-2c \\ a & -2c & -2b \end{vmatrix} = a^3 - 4ab^2 - 2b^3 + 8a^2c + 6abc + 16ac^2 + 8bc^2 + 4c^3$$

七. 域论(续)

其中

$$D = \begin{vmatrix} c & b & a+4c \\ b & a+4c & 4b-2c \\ a & -2c & -2b \end{vmatrix} = a^3 - 4ab^2 - 2b^3 + 8a^2c + 6abc + 16ac^2 + 8bc^2 + 4c^3$$

例如, 在$\mathbb{Q}(u)$中, 有

$$(2+3u-5u^2)(258-56u-81u^2) = 442,$$

$$(-3+2u-7u^2)(917-92u-213u^2) = -3187.$$

七. 域论(续)

4. 应用

作为有理化方法的应用, 我们证明下列例子.

七. 域论(续)

4. 应用

作为有理化方法的应用, 我们证明下列例子.

例11 设$u \in \mathbb{C}$在$\mathbb{Z}$上的极小多项式为$x^2 - x + 2$, v在$\mathbb{Z}$上的极小多项式为$x^2 - x + 3$, 令$\mathbb{Z}[u, v] = \{a + bu + cv + duv | a, b, c, d \in \mathbb{Z}\}$, 则$\mathbb{Z}[u, v]$是一个整环. 证明$\mathbb{Z}[u, v]$的分式域是$\mathbb{Q}(u, v)$.

七. 域论(续)

4. 应用

作为有理化方法的应用, 我们证明下列例子.

例11 设$u \in \mathbb{C}$在$\mathbb{Z}$上的极小多项式为$x^2 - x + 2$, v在$\mathbb{Z}$上的极小多项式为$x^2 - x + 3$, 令$\mathbb{Z}[u, v] = \{a + bu + cv + duv | a, b, c, d \in \mathbb{Z}\}$, 则$\mathbb{Z}[u, v]$是一个整环. 证明$\mathbb{Z}[u, v]$的分式域是$\mathbb{Q}(u, v)$.

证明: 设$\mathbb{Z}[u, v]$的分式域为

$$S = \left\{ \frac{e + fu + gv + huv}{a + bu + cv + duv} \middle| a, b, c, d, e, f, g, h \in \mathbb{Z}, a + bu + cv + duv \neq 0 \right\}.$$

七. 域论(续)

4. 应用

作为有理化方法的应用, 我们证明下列例子.

例11 设$u \in \mathbb{C}$在$\mathbb{Z}$上的极小多项式为$x^2 - x + 2$, v在$\mathbb{Z}$上的极小多项式为$x^2 - x + 3$, 令$\mathbb{Z}[u, v] = \{a + bu + cv + duv | a, b, c, d \in \mathbb{Z}\}$, 则$\mathbb{Z}[u, v]$是一个整环. 证明$\mathbb{Z}[u, v]$的分式域是$\mathbb{Q}(u, v)$.

证明: 设$\mathbb{Z}[u, v]$的分式域为

$$S = \left\{ \frac{e + fu + gv + huv}{a + bu + cv + duv} \middle| a, b, c, d, e, f, g, h \in \mathbb{Z}, a + bu + cv + duv \neq 0 \right\}.$$

要证明$S = \mathbb{Q}(u, v)$,

七. 域论(续)

4. 应用

作为有理化方法的应用, 我们证明下列例子.

例11 设$u \in \mathbb{C}$在$\mathbb{Z}$上的极小多项式为$x^2 - x + 2$, v在$\mathbb{Z}$上的极小多项式为$x^2 - x + 3$, 令$\mathbb{Z}[u, v] = \{a + bu + cv + duv | a, b, c, d \in \mathbb{Z}\}$, 则$\mathbb{Z}[u, v]$是一个整环. 证明$\mathbb{Z}[u, v]$的分式域是$\mathbb{Q}(u, v)$.

证明: 设$\mathbb{Z}[u, v]$的分式域为

$$S = \left\{ \frac{e + fu + gv + huv}{a + bu + cv + duv} \middle| a, b, c, d, e, f, g, h \in \mathbb{Z}, a + bu + cv + duv \neq 0 \right\}.$$

要证明$S = \mathbb{Q}(u, v)$, 只要证明分式

$$\frac{e + fu + gv + huv}{a + bu + cv + duv}$$

的分母可有理化,

七. 域论(续)

4. 应用

作为有理化方法的应用, 我们证明下列例子.

例11 设$u \in \mathbb{C}$在$\mathbb{Z}$上的极小多项式为$x^2 - x + 2$, v在$\mathbb{Z}$上的极小多项式为$x^2 - x + 3$, 令$\mathbb{Z}[u, v] = \{a + bu + cv + duv | a, b, c, d \in \mathbb{Z}\}$, 则$\mathbb{Z}[u, v]$是一个整环. 证明$\mathbb{Z}[u, v]$的分式域是$\mathbb{Q}(u, v)$.

证明: 设$\mathbb{Z}[u, v]$的分式域为

$$S = \left\{ \frac{e + fu + gv + huv}{a + bu + cv + duv} \middle| a, b, c, d, e, f, g, h \in \mathbb{Z}, a + bu + cv + duv \neq 0 \right\}.$$

要证明$S = \mathbb{Q}(u, v)$, 只要证明分式

$$\frac{e + fu + gv + huv}{a + bu + cv + duv}$$

的分母可有理化, 即要找出一个元素$e + fu + gv + huv \in \mathbb{Z}[u, v]$使得

$$(a + bu + cv + duv)(e + fu + gv + huv) \in \mathbb{Z}.$$

七. 域论(续)

计算$(a+bu+cv+duv)(e+fu+gv+huv)$得下式:

$$
\begin{aligned}
& (a+bu+cv+duv)(e+fu+gv+huv) \\
= \; & deuv+cfuv+dfuv+bguv+dguv+ahuv+bhuv+chuv+dhuv \\
& +beu+afu+bfu-3dgu-3chu-3dhu+cev-2dfv+agv \\
& +cgv-2bhv-2dhv+ae-2bf-3cg+6dh \\
= \; & (de+cf+df+bg+dg+ah+bh+ch+dh)uv \\
& +(be+af+bf-3dg-3ch-3dh)u \\
& +(ce-2df+ag+cg-2bh-2dh)v \\
& +(ae-2bf-3cg+6dh)
\end{aligned}
$$

七. 域论(续)

要使$(a+bu+cv+duv)(e+fu+gv+huv)\in\mathbb{Z}$,

七. 域论(续)

要使$(a+bu+cv+duv)(e+fu+gv+huv)\in\mathbb{Z}$, 必须令

$$\begin{cases} de+(c+d)f+(b+d)g+(a+b+c+d)h &= 0\\ be+(a+b)f-3dg-(3c+3d)h &= 0\\ ce-2df+(a+c)g-(2b+2d)h &= 0\\ ae-2bf-3cg+6dh &= l \end{cases} \tag{14}$$

七. 域论(续)

要使$(a+bu+cv+duv)(e+fu+gv+huv)\in\mathbb{Z}$, 必须令

$$\begin{cases} de+(c+d)f+(b+d)g+(a+b+c+d)h &= 0\\ be+(a+b)f-3dg-(3c+3d)h &= 0\\ ce-2df+(a+c)g-(2b+2d)h &= 0\\ ae-2bf-3cg+6dh &= l \end{cases} \tag{14}$$

其中

$$\begin{aligned} l &= \begin{vmatrix} d & c+d & b+d & a+b+c+d\\ b & a+b & -3d & -3c-3d\\ c & -2d & a+c & -2b-2d\\ a & -2b & -3c & 6d \end{vmatrix}\\ &= a^4+2a^3b+5a^2b^2+4ab^3+4b^4+2a^3c+3a^2bc+5ab^2c+2b^3c+7a^2c^2\\ &\quad +7abc^2-7b^2c^2+6ac^3+3bc^3+9c^4+a^3d+5a^2bd+6ab^2d+8b^3d+7a^2cd\\ &\quad +49abcd+14b^2cd+9ac^2d+15bc^2d+18c^3d-7a^2d^2+14abd^2+28b^2d^2\\ &\quad +15acd^2+18bcd^2+45c^2d^2+6ad^3+24bd^3+36cd^3+36d^4 \end{aligned}$$

七. 域论(续)

解关于变量e,f,g,h的线性方程组(14)得:

$$\begin{aligned}
e &= a^3+2a^2b+3ab^2+2b^3+2a^2c+3abc+b^2c+4ac^2+bc^2+3c^3+a^2d\\
&\quad +5abd+4b^2d+7acd+13bcd+6c^2d-ad^2+8bd^2+9cd^2+6d^3\\
f &= -a^2b-ab^2-2b^3-2abc-b^2c+2bc^2-abd-4b^2d-6acd-bcd\\
&\quad -3c^2d-3ad^2-8bd^2-3cd^2-6d^3\\
g &= -a^2c-2abc+b^2c-ac^2-bc^2-3c^3-4abd-2b^2d-acd-bcd\\
&\quad -6c^2d-2ad^2-2bd^2-9cd^2-6d^3\\
h &= 2abc+b^2c+bc^2-a^2d+2b^2d+bcd+3c^2d+2bd^2+3cd^2+6d^3
\end{aligned}$$

七. 域论(续)

解关于变量e,f,g,h的线性方程组(14)得:

$$\begin{aligned}
e &= a^3+2a^2b+3ab^2+2b^3+2a^2c+3abc+b^2c+4ac^2+bc^2+3c^3+a^2d\\
&\quad +5abd+4b^2d+7acd+13bcd+6c^2d-ad^2+8bd^2+9cd^2+6d^3\\
f &= -a^2b-ab^2-2b^3-2abc-b^2c+2bc^2-abd-4b^2d-6acd-bcd\\
&\quad -3c^2d-3ad^2-8bd^2-3cd^2-6d^3\\
g &= -a^2c-2abc+b^2c-ac^2-bc^2-3c^3-4abd-2b^2d-acd-bcd\\
&\quad -6c^2d-2ad^2-2bd^2-9cd^2-6d^3\\
h &= 2abc+b^2c+bc^2-a^2d+2b^2d+bcd+3c^2d+2bd^2+3cd^2+6d^3
\end{aligned}$$

例如, 在$\mathbb{Z}[u,v]$中, 有

$$(2-u+3v+2uv)(383-205u-353v+102uv)=4757,$$

$$(1-u-2v+5uv)(243-508u-390v+623uv)=15577.$$

谢谢!