DOI:10.11721/cqnuj20140612

拟 Eisenstein 型数域中素数的分解*

周琰博,安 莹,罗 明
(西南大学 数学与统计学院,重庆 400715)

摘要:Eisenstein 型数域在素理想的分解研究中有着十分重要的作用。若将 Eisenstein 型数域进行推广,就会得到在更广泛的数域中素理想分解的信息。如果将代数整数 ω 的不可约多项式的条件减弱,就得到 Eisenstein 型数域的推广。本文尝试推广 Eisenstein 型数域为拟 Eisenstein 型数域 $K=(E,p,k)$,并且探讨在这样推广的条件下素理想分解的相应结果。利用 Newton 折线图,证明了在拟 Eisenstein 型数域(E,p,k)中素数 p 有 $e(P/p)=k$ 的的素理想因子 P,在 $k=n,n-1$ 时,通过计算代数整数的范数证明了 p 在 K 中的分解满足 Dedekind 的引理,从而给出了素理想 P 的具体形式。对于拟 Eisenstein 域(E,p,k)的判别式中 p 的个数利用赋值方法做了估计,证明了 p^{k-1} 整除判别式 $d(K)$。

关键词:代数数论;素理想分解;判别式
中图分类号:O156.2 **文献标志码**:A **文章编号**:1672-6693(2014)06-0058-04

设 $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$,$p$ 为素数并且 $p\mid a_i(0\leqslant i\leqslant n-1)$,$p^2\nmid a_0$。由 Eisenstein 判别法可知 $f(x)$是 $\mathbf{Q}[x]$中不可约多项式,令 ω 是 $f(x)$的一个根,则 n 次数域 $K=\mathbf{Q}(\omega)$叫做对于 p 的 Eisenstein 型数域,简称(E,p)型数域。Eisenstein 型数域在素理想分解的研究中有着十分重要的作用[1-2]。本文尝试对 Eisenstein 型数域进行推广,定义 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in\mathbf{Z}[x]$,$\exists$ 素数 p,$p\nmid a_n,a_{n-1},\cdots,a_k$,$p\mid a_{k-1},\cdots,a_0$,$p^2\nmid a_0(1<k\leqslant n)$,则称 $f(x)$为拟 Eisenstein 多项式。关于 Eisenstein 判别法的推广以及与拟 Eisenstein 多项式的联系,已有很多工作[3-5]。若 $f(x)$为首项系数为 1 的不可约拟 Eisenstein 多项式,ω 为 $f(x)$的一个根,则称 n 次数域 $K=\mathbf{Q}(\omega)$为拟 Eisenstein 型数域,简记为(E,p,k)型数域。$k=n$ 时就是 Eisenstein 型数域。

1 素数 p 在(E,p,k)型数域中的分解

引理 1[2] $g(x)\in\mathbf{Z}[x]$不可约多项式,ω 是 $g(x)$的根,$K=\mathbf{Q}[\omega]$,p 是素数,

$$g(x)\equiv\varphi_1(x)^{e_1}\varphi_2(x)^{e_2}\cdots\varphi_r(x)^{e_r}(\mathrm{mod}\ p),$$

$\varphi_i(x)$是 $g(x)$对于 mod p 分解的不可约因子。若 $p\nmid|O_k/Z[\omega]|$,那么 $pO_K=P_1^{e_1}P^{e_2}\cdots P^{e_r}$,其中 $P_i=(p,\varphi_i(\omega))$,并且 $f(P_i/p)=\deg(\varphi_i(x))$。

引理 2[6] $g(x),\omega,K,p$ 同引理 1。对于 K 中 p 的素理想因子 P,商 $v_P(\omega)/e(P/p)$等于 $g(x)$关于 p 的 Newton 折线的一条边的斜率;反之,若$\lambda\in\mathbf{Q}$是这样的 Newton 折线的一条边的斜率,则存在 K 中 p 的素理想因子 P,使得 $v_P(\omega)/e(P/p)=\lambda$。

这里 $v_P(\omega)=e(P/(\omega))$,设 $g(x)=b_nx^n+\cdots+b_1x+b_0\in\mathbf{Z}[x]$,$b_0b_n\neq0$,$g(x)$关于 p 的 Newton 折线[7-8]是平面点集 $S=\{(i,v_p(b_{n-i}))\mid0\leqslant i\leqslant n\}$的下凸包络线。这里的 $v_p(b_j)$为 $p^s\mid b_j$ 的最大整数 s。

定理 1 设 $K=\mathbf{Q}(\omega)$为(E,p,k)型数域,p 在 K 中有素理想因子 P,$e(P/p)=k$。

证明 ω 的极小多项式 $f(x)$关于 p 的 Newton 折线图如图 1 所示。其中一条边的斜率为 $1/k$,由引理 2 知,存在 L 中 p 的素理想因子 P,使得 $v_P(\omega)/e(P/p)=1/k$,由 $N_{K/Q}(P)^{v_P(\omega)}\mid N_{K/Q}((\omega))$,$N_{K/Q}(P)=p$,$N_{K/Q}((\omega))=$

* **收稿日期**:2013-05-03 **修回日期**:2013-06-04 **网络出版时间**:2014-11-19 21:49
作者简介:周琰博,男,研究方向为代数数论,E-mail:spinoza70@sina.com;**通讯作者**:罗明,E-mail:luoming1958@126.com
网络出版地址:http://www.cnki.net/kcms/detail/50.1165.N.20141119.2149.012.html

$|a_0|$，a_0 中只含一个 p，所以 $v_P(\omega)=1$，$e(P/p)=k$。

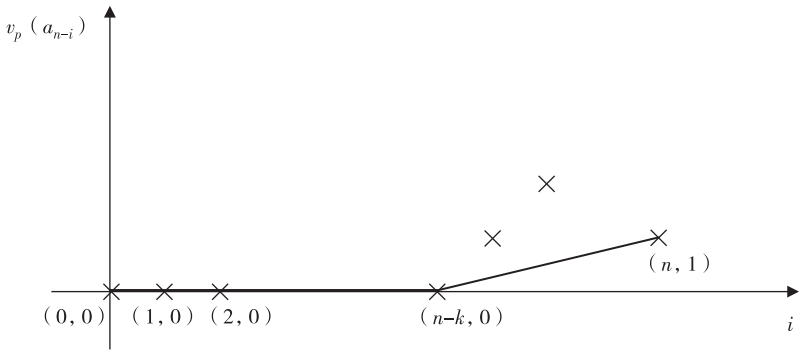

图 1　$f(x)$关于 p 的 Newton 折线图

定理 1 只表明(E,p,k)型数域中 p 有 $e(P/p)=k$ 的素理想因子 P，却没给出 P 的具体形式。下面的定理证明对于(E,p,n)，$(E,p,n-1)$型数域可以得到 P 的具体形式。

引理 3[2,9]　设 L/K 是数域的扩张，对于 $\alpha\in L$，定义映射 $\varphi_\alpha:L\to L$，$\varphi_\alpha(\beta)=\alpha\beta$，则 φ_α 是 K-向量空间 L 中的线性变换。如果 $\boldsymbol{A}_\alpha$ 是线性变换 φ_α 对于向量空间 L 的任意一组 K-基的变换方阵，则 $N_{L/K}(\alpha)=|\boldsymbol{A}_\alpha|$。

引理 4　设 $K=\mathbf{Q}(\omega)$为(E,p,k)型数域，则 $N_{K/Q}(\omega^{n-k}+a_{n-1}\omega^{n-k-1}+\cdots+a_k)=(-1)^{(n-k)(n+2)}a_0^{n-k}$。

证明　用引理 3 的方法计算 $N_{K/Q}(\omega^{n-k}+a_{n-1}\omega^{n-k-1}+\cdots+a_k)$，设 $\alpha=\omega^{n-k}+a_{n-1}\omega^{n-k-1}+\cdots+a_k$，在 K 的一组 $\mathbf{Q}$ 基 $1,\omega,\cdots,\omega^{n-1}$ 下 φ_α 的矩阵为

$$\boldsymbol{A}_\alpha=\left\{\begin{array}{l}n-k\left\{\\k\left\{\end{array}\right.\right.\left(\begin{array}{ccccc:ccccc}a_k & & & & & -a_0 & & & & \\ a_{k+1} & a_k & & & & -a_1 & -a_0 & & & \\ \vdots & a_{k+1} & \ddots & & & \vdots & -a_1 & \ddots & & \\ \vdots & \vdots & & \ddots & & \vdots & \vdots & & \ddots & \\ a_{n-1} & a_{n-2} & \cdots & \cdots & a_k & -a_{k-1} & \vdots & & & -a_0 \\ \hdashline 1 & a_{n-1} & \cdots & \cdots & a_{k+1} & 0 & -a_{k-1} & \cdots & \cdots & -a_1 \\ & 1 & & & \vdots & & 0 & & & \vdots \\ & & \ddots & & \vdots & & & \ddots & & \vdots \\ & & & \ddots & a_{n-1} & & & & \ddots & -a_{k-1} \\ & & & & 1 & & & & & 0\end{array}\right)。$$

$N_{K/Q}(\omega^{n-k}+a_{n-1}\omega^{n-k-1}+\cdots+a_k)=|\boldsymbol{A}_\alpha|$，由 Laplace 定理[10]，取定行列式的前 $n-k$ 行

$$|\boldsymbol{A}_\alpha|=\sum_{1\leqslant j_1<j_2<\cdots<j_{n-k}\leqslant n}\left|\boldsymbol{A}\begin{pmatrix}1 & 2 & \cdots & n-k\\ j_1 & j_2 & \cdots & j_{n-k}\end{pmatrix}\right|\left|\hat{\boldsymbol{A}}_c\begin{pmatrix}1 & 2 & \cdots & n-k\\ j_1 & j_2 & \cdots & j_{n-k}\end{pmatrix}\right|=$$

$$\left|\boldsymbol{A}\begin{pmatrix}1 & 2 & \cdots & n-k\\ k+1 & k+2 & \cdots & n\end{pmatrix}\right|\left|\hat{\boldsymbol{A}}_c\begin{pmatrix}1 & 2 & \cdots & n-k\\ k+1 & k+2 & \cdots & n\end{pmatrix}\right|=(-a_0)^{n-k}(-1)^{(n-k)(n+1)}=(-1)^{(n-k)(n+2)}a_0^{n-k}。$$

即 $N_{K/Q}(\omega^{n-k}+a_{n-1}\omega^{n-k-1}+\cdots+a_k)=(-1)^{(n-k)(n+2)}a_0^{n-k}$，又由 $p|a_0$，并且 $p^2\nmid a_0$，$N_{K/Q}(\omega^{n-k}+a_{n-1}\omega^{n-k-1}+\cdots+a_k)$只含 $n-k$ 个 p。　　证毕

引理 5　设 $K=\mathbf{Q}(\omega)$为(E,p,k)型数域，$k=n,n-1$，$r_0,r_1,\cdots,r_{n-1}\in\mathbf{Z}$，若 $r_0+r_1\omega+\cdots+r_{n-1}\omega^{n-1}\equiv0(\mathrm{mod}\ pO_K)$，则对所有的 i，$r_i\equiv0(\mathrm{mod}\ p\mathbf{Z})$。

证明　当 $k=n-1$ 时，在等式

$$r_0+r_1\omega+\cdots r_{n-1}\omega^{n-1}\equiv0(\mathrm{mod}\ pO_K)\tag{1}$$

两边同乘以 $\omega^{n-1}+a_{n-1}\omega^{n-2}$，左边除第一项外其他各项都是 $\omega^n+a_{n-1}\omega^{n-1}$的倍数，又 $\omega^n+a_{n-1}\omega^{n-1}=-a_{n-2}\omega^{n-2}-\cdots-a_0\equiv0(\mathrm{mod}\ pO_K)$，故 $r_0(\omega^{n-1}+a_{n-1}\omega^{n-2})\equiv0(\mathrm{mod}\ pO_K)$。两边同时取范数，得 $r_0^nN_{K/Q}(\omega^{n-1}+a_{n-1}\omega^{n-2})\equiv$

$0(\mathrm{mod}\ p^n\mathbf{Z})$。

由引理4,$N_{K/Q}(\omega^{n-1}+a_{n-1}\omega^{n-2})$只有$n-1$个$p$,因此由上式得$p|r_0$,因此(1)式成为

$$r_1\omega+\cdots r_{n-1}\omega^{n-1}\equiv 0(\mathrm{mod}\ pO_K)。\tag{2}$$

在(2)式两边同乘以$\omega^{n-2}+a_{n-1}\omega^{n-3}$,得$r_1(\omega^{n-1}+a_{n-1}\omega^{n-2})\equiv 0(\mathrm{mod}\ pO_K)$。取范数得$p|r_1$。类似得依次乘$\omega^{n-3}+a_{n-1}\omega^{n-4},\cdots,\omega+a_{n-1}$,并且取范数得$p|r_2,\cdots,p|r_{n-2}$。最后只剩下$r_{n-1}\omega^{n-1}\equiv 0(\mathrm{mod}\ pO_K)$,两边同时取范数,得$r_{n-1}^n N_{K/Q}(\omega)^{n-1}\equiv 0(\mathrm{mod}\ p^n\mathbf{Z})$。

由$N_{K/Q}(\omega)$只有一个p,因此得$p|r_{n-1}$。

类似地,$k=n$时,在(1)式两边依次乘以$\omega^{n-1},\cdots,\omega$,并且取范数,得$p|r_0,\cdots,p|r_{n-2}$。最后只剩下$r_{n-1}\omega^{n-1}\equiv 0(\mathrm{mod}\ pO_K)$,取范数得$p|r_{n-1}$。 证毕

定理2 设$K=\mathbf{Q}(\omega)$为(E,p,k)型数域,$k=n,n-1$时,$p\nmid|O_K/\mathbf{Z}[\omega]|$。

证明 用反证法。假设$p||O_K/\mathbf{Z}[\omega]|$,则$O_K/\mathbf{Z}[\omega]$看作有限Abel群存在$p$阶元。即存在$\gamma\in O_K,\gamma\notin\mathbf{Z}[\omega]$,但是$p\gamma\in\mathbf{Z}[\omega]$,则$p\gamma=s_0+s_1\omega+\cdots+s_{n-1}\omega^{n-1},s_i\in\mathbf{Z}$。

由引理5知,s_i都能被p整除,所以$\gamma=\dfrac{s_0+s_1\omega+\cdots+s_{n-1}\omega^{n-1}}{p}\in\mathbf{Z}[\omega]$,与$\gamma\notin\mathbf{Z}[\omega]$矛盾。因此$p\nmid|O_k/\mathbf{Z}[\omega]|$。

证毕

由定理2和引理1可以得到以下熟知的结果。

推论1[1-2,11] 若$K=\mathbf{Q}(\omega)$为(E,p,n)型数域,则p在K中完全分歧,即$pO_K=P^n$,其中$P=(p,\omega)$。

此外,对$k=n-1$的情形不难验证有下面结论。

推论2 若$K=\mathbf{Q}(\omega)$为$(E,p,n-1)$型数域,则$pO_K=P_1^{n-1}P_2$,其中$P_1=(p,\omega),P_2=(p,\omega+a_{n-1})$。

2 (E,p,k)型数域判别式中p的个数估计

定理3 若$K=\mathbf{Q}(\omega)$为(E,p,k)型数域,则$p^{k-1}|d(K)$。

证明 由定理1可设P为p的素理想因子,$e=e(P|p)=k$。设$\omega\in P^s-P^{s+1},s\geqslant 1$。以$t_n,t_{n-1}\cdots,t_1,t_0$分别表示主理想$(\omega^n),(a_{n-1}\omega^{n-1}),\cdots,(a_0)$中出现的$P$因子的个数,则$t_n=ns,t_{n-1}=(n-1)s,\cdots,t_k=ks,t_{k-1}=k+(k-1)s>k,\cdots,t_1=k+s>k,t_0=k$,由于$t_n,t_{n-1},\cdots,t_1,t_0$中的最小值至少在两个$t_i$处达到,这只可能是$ks=k,s=1$,即$(\omega)=P\mathbf{Q},P\nmid\mathbf{Q}$。$f'(\omega)=n\omega^{n-1}+(n-1)a_{n-1}\omega^{n-2}+\cdots+2a_2\omega+a_1,P^k|a_i,1\leqslant i<k$。

$f'(\omega)\equiv n\omega^{n-1}+(n-1)a_{n-1}\omega^{n-2}+\cdots+ka_k\omega^k=\omega^{k-1}(n\omega^{n-k}+(n-1)a_{n-1}\omega^{n-k-1}+\cdots+ka_k)(\mathrm{mod}\ P^k)$。

由$P^{k-1}|(\omega)^{k-1}$得$P^{k-1}|(f'(\omega)),N_{K/Q}(P)=p$得$p^{k-1}|N_{K/Q}(f'(\omega))=(-1)^{\frac{n(n-1)}{2}}d(K)$。 证毕

参考文献:

[1] Alaca S,Williams K S. Introductory algebraic number theory[M]. London:Cambridge University Press,2004:259- 260.

[2] 冯克勤. 代数数论[M]. 北京:科学出版社,2000:16,49-51,61-62.
Feng K Q. Algebraic number theory[M]. Beijing: Science Press,2000:16,49-51,61-62.

[3] 罗永超,畅敏,张洪. 关于整系数多项式的不可约性与有理根存在性的新判别法[J]. 西南师范大学学报:自然科学版,2013,38(4):1-4.
Luo Y C,Chang M,Zhang H. On new discriminating method for irreducibility of integer coefficients polynomial and the existence of the rational roots[J]. Journal of Southwest China Normal University:Nature Science Edition,2013,38(4):1-4.

[4] 陈秀梅,滕长春. Eisenstein判别法的几个推广[J]. 潍坊学院学报,2011,11(4):75-76.
Cheng X M,Teng C C. Several generalization of Eisenstein criterion[J]. Journal of Weifang University,2011,11(4):75-76.

[5] 吴捷云. Eisenstein判别法的若干推广[J]. 高师理科学刊,2010,30(1):37-39.
Wu J Y. Some generalization of Eisenstein criterion[J]. Journal of Science of Teacher's Colledge and University,2010,30(1):37-39.

[6] Baurr M. Zur allgemeinen theorie der algebraaischen groessen[J]. J Reine Angew Math,1907,132:21-32.

[7] Llorente P, Nart E. Effective determination of decomposition of the rational primes in a cubic fields[J]. Proc Amer Math Soc, 1983, 87: 579-585.

[8] Weiss E. Algebraic number theory[M]. New York: Dover Publication, 1998: 73-78.

[9] 张贤科. 代数数论导引[M]. 北京: 高等教育出版社, 2006: 26-27.
Zhang X K. Algebraic number theory[M]. Beijing: Higher Education Press, 2006: 26-27.

[10] 屠伯勋. 高等代数[M]. 上海: 上海科技出版社, 1980: 92-98.
Tu B Y. Higher algebra[M]. Shanghai: Shanghai Science Press, 1980: 92-98.

[11] Narkwicz W. Elementary and analytic theory of algebraic numbers[M]. Warsaw: Polish Science Publication, 1974: 54, 166.

On The Decomposition of Rational Prime in the Pseudo-Eisenstein Field

ZHOU Yanbo, AN Ying, LUO Ming

(School of Mathematics and Statistics, Southwest University, Chongqing 400715, China)

Abstract: Eisenstein fields play an important role in the decomposition of rational prime. One of the most important conclusion says that, If ω is an algebraic number and its irreducible polynomial is p-Eisenstein, then p is completely ramifies in $K=Q(\omega)$. On the other hand, algebraic fields such as $Q(\sqrt[n]{p})$ are Eisenstein fields. In the study of pure cubic fields, in many case we will found the problem can be solved in Eisenstein fields. If we generalized the Eisenstein fields, we will get much information of the decomposition of prime ideals. The method is loose the condition of the Eisenstein polynomial, acquire pseudo-Eisenstein fields. In this paper, we generalize the Eisenstein field and discuss the decomposition of rational prime in pseudo-Eisenstein fields. We find the rational prime p has a factor ideal P with $e(P/p)=k$ by Newton polygon. When $k=n, n-1$ we calculate the norm of some algebraic number. We find the prime number p satisfies the condition of a theorem of Dedekind. Thus we can determine form of ideal P. We also determine the number of p in the discriminant of the pseudo-Eisenstein field (E, p, k). We prove p^{k-1} divides the discriminant $d(K)$.

Key words: algebraic number; decomposition of prime ideal; discriminant

(责任编辑 黄 颖)