DOI:10.11721/cqnuj20140515

Eisenstein 判别法及(E,p)型数域的推广*

陶新恩，宋欣欣，庄媛媛，罗　明
(重庆师范大学 数学学院，重庆 401331)

摘要:Eisenstein 判别法是高等代数中判定整系数多项式在有理数域中的可约性的重要方法,其推广形式很多,而最原始的形式应用代数数论中来定义(E,p)型数域。本文在原来 Eisenstein 判别法的基础上进行适当地推广,并将已知的(E,p)型数域也随其判别法的推广而推广,成为广(E,p)型数域,在此基础上研究此数域的性质:给出素数 p 在广(E,p)型数域中的素理想分解形式,并且给出了这个素数 p 的一个重要性质。其次,得到广(E,p)型数域中素数 p 及相关理想的一些性质,并给出相应的证明。这样,就推广了原本只讨论最原始定义的 Eisenstein 判别法及(E,p)型数域的相关性质,使此理论更加完善。

关键词:Eisenstein 判别法;(E,p)型数域;素理想
中图分类号:O156.4　　**文献标志码**:A　　**文章编号**:1672-6693(2014)05-0085-04

(E,p)型数域在代数数论研究中具有重要的作用[1-9],其定义是由 Eisenstein 判别法得出的。本文将 Eisenstein 判别法稍加推广,即可将(E,p)型数域推广。对推广后的(E,p)型数域进行讨论,得到一些相应的结果。

首先介绍 Eisenstein 判别法和(E,p)型数域概念。

引理 1[1]　(Eisenstein 判别法)设本原整系数多项 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in Z[x]$,且 $\deg f\geqslant 1$。如果存在素数 p,使得 $p\nmid a_n$,$p\mid a_i(0\leqslant i\leqslant n-1)$,$p^2\nmid a_0$,则 $f(x)$为 $Z[x]$中不可约多项式。

定义 1[2]　((E,p)型数域)设 $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in Z[x]$,且 $\deg f\geqslant 1$。p 为素数并且 $p\mid a_i(0\leqslant i\leqslant n-1)$,$p^2\nmid a_0$。由引理 1 知 $f(x)$是 $Q(x)$中的不可约多项式。令 ω 是 $f(x)$的一个根,则 n 次数域 $K=Q(\omega)$叫做是对于 p 的 Eisenstein 型数域,简称作(E,p)型数域。

注 1　若 $K=Q(\omega)$是(E,p)型数域,则 ω 的极小多项式的不可约性 Eisenstein 判别法由素数 p 判别而得出。

1　Eisenstein 判别法的推广

下面将 Eisenstein 判别法加以推广。

引理 2[3]　设本原整系数多项 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in Z[x]$,且 $\deg f=n\geqslant 2$。如果存在素数 p,使得 $p\nmid a_n$, $p\nmid a_{n-1}$,$p\mid a_i(0\leqslant i\leqslant n-2)$,$p^2\nmid a_0$,则 $f(x)$在 $Z[x]$中有次数$\geqslant n-1$ 的不可约多项式因子。

推论 1[3-4]　设本原整系数多项 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in Z[x]$,且 $\deg f=n$。如果存在素数 p 和整数 $k(1\leqslant k\leqslant n)$,使得 $p\nmid a_k$,$p\mid a_i(0\leqslant i\leqslant k-1)$,$p^2\nmid a_0$,则 $f(x)$在 $Z[x]$中必有次数$\geqslant k$ 的不可约多项式因子。

推论 1 可用数学归纳法证明,这里就不再给出其证明。

2　(E,p)型数域的推广及其性质

设 K 为数域,A 为 O_k 的非零理想,P 为 O_k 的素理想。用 $V_P(A)$表示 A 的素理想分解式中 P 的指数(若 P 在 A 中的分解式中不出现,则令 $V_P(A)=0$)。

* **收稿日期**:2013-05-22　　**修回日期**:2013-11-04　　**网络出版时间**:2014-9-17　22:37
作者简介:陶新恩,男,研究方向为数论,E-mail:790033978@qq.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.20140917.2237.016.html

引理 3 对每个元素 $0\neq\alpha\in O_k$,令 $V_P(\alpha)=V_P(\alpha O_k)$。并且规定 $V_P(0)=\infty$,同时规定:对每个 $n\in\mathbf{Z}$($\mathbf{Z}$ 是整数集),$n<\infty$,$n+\infty=\infty+n=\infty+\infty=n\infty=\infty n=\infty\infty=\infty$。当 $\alpha,\beta\in O_k$ 时,则有:1) $V_P(\alpha\beta)=V_P(\alpha)+V_P(\beta)$,$V_P(\alpha+\beta)\geqslant\min(V_P(\alpha),V_P(\beta))$;2)若 $V_P(\alpha)\neq V_P(\beta)$,则 $V_P(\alpha+\beta)=\min(V_P(\alpha),V_P(\beta))$;3) 设 $\alpha_1,\cdots,\alpha_n\in O_k$,$n\geqslant 2$,$\alpha_1+\alpha_2+\cdots+\alpha_n=0$,记 $m=\min\{V_P(\alpha_i)\mid 1\leqslant i\leqslant n\}$。则至少有两个不同的下标 i 和 j,使得 $V_P(\alpha_i)=V_P(\alpha_j)=m$。

证明 1) 由于 $(\alpha\beta)=(\alpha)(\beta)$,所以就可得到 $V_P(\alpha\beta)=V_P(\alpha)+V_P(\beta)$ 成立。

又因为 $(\alpha+\beta)\subseteq(\alpha)+(\beta)$,故 $V_P(\alpha+\beta)\geqslant V_P((\alpha)+(\beta))$,而又因为有结论 $V_P((\alpha)+(\beta))=\min V_P((\alpha),(\beta))$,所以就有 $V_P(\alpha+\beta)\geqslant\min(V_P(\alpha),V_P(\beta))$ 成立。

2)由于 $V_P(\alpha)\neq V_P(\beta)$,故不妨设 $V_P(\alpha)<V_P(\beta)$。则由结论 1)知 $V_P(\alpha+\beta)\geqslant\min(V_P(\alpha),V_P(\beta))=V_P(\alpha)$。

另一方面,$(\alpha)\subseteq(\alpha)+(\beta)=(\alpha+\beta)+(\beta)$,故 $V_P(\alpha)\geqslant\min(V_P(\alpha+\beta),V_P(\beta))$,由于 $V_P(\alpha)<V_P(\beta)$,所以 $V_P(\alpha)\geqslant V_P(\alpha+\beta)$。综上可得 $V_P(\alpha+\beta)=\min(V_P(\alpha)+V_P(\beta))$ 成立。

3)反证法。假设结论不成立,故不妨设只有一个 $V_P(\alpha_1)=m$,其余 $V_P(\alpha_i)>m$ $(2\leqslant i\leqslant n)$,故可知 $\infty=V_P(0)=V_P(\alpha_1+\cdots+\alpha_n)$,但是由结论 1)易知 $m=V_P(\alpha_1)<V_P(\alpha_2+\cdots+\alpha_n)$,所以由结论 2)可得

$$\infty=V_P(\alpha_1+\cdots+\alpha_n)=\min(V_P(\alpha_1),V_P(\alpha_2)+\cdots+V_P(\alpha_n))=\min(m,V_P(\alpha_2)+\cdots+V_P(\alpha_n))=m,$$

得到 $m=\infty$,矛盾。所以至少有两个不同的下标 i 和 j,使得 $V_P(\alpha_i)=V_P(\alpha_j)=m$。 证毕

下面给出广(E,p)型数域的定义。

定义 2 (广(E,p)型数域)设 $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in Z[x]$,且 $\deg f=n\geqslant 2$。p 为素数并且 $p\nmid a_{n-1}$,$p\mid a_i(0\leqslant i\leqslant n-2)$,$p^2\nmid a_0$。则由引理 2 可知 $f(x)$ 在 $Z[x]$ 中有次数$\geqslant n-1$ 的不可约多项式因子。当 $f(x)$ 为 $Z[x]$ 上的不可约多项式时,令 ω 是 $f(x)$ 的一个根,则 n 次数域 $K=Q(\omega)$ 叫做是对于 p 的广 Eisenstein 型数域,简称广(E,p)型数域。

定理 1 设 $K=Q(\omega)$ 为上述的广(E,p)型数域,则 p 在 K 中的分解为 $pO_k=\beta_1^{n-1}\beta_2$,其中 β_1,β_2 是 O_k 中的素理想,并且有 $p\nmid|O_k/Z[\omega]|$。

证明 设 ω 是 $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_0\in Z[x]$ 的根。故 $[K:Q]=n$,并设 $n>2$(这是由于二次域有完善的素理想分解的结论,所以不用纳入(E,p)型数域上来考虑)。令 β 是 K 的素理想且 $\beta\mid p$,令 $e=V_\beta(p)$。由于 $p\mid f(\omega)=\omega^n+a_{n-1}\omega^{n-1}+\cdots+a_1\omega+a_0=0$,故由 $p\mid a_i(0\leqslant i\leqslant n-2)$ 得 $p\mid\omega^n+a_{n-1}\omega^{n-1}$,于是就有 $\beta\mid\omega^{n-1}(\omega+a_{n-1})$。而 β 是 K 中的素理想,故 $\beta\mid\omega^{n-1}$ 或 $\beta\mid\omega+a_{n-1}$。

1)若 $\beta\mid\omega^{n-1}$,则有 $n>2$,并且 $\omega\in\beta$。故设 $\omega\in\beta^s-\beta^{s+1}$,则 $s\geqslant 1$。以 $t_n,t_{n-1},\cdots,t_0$ 分别表示主理想 (ω^n),$(a_{n-1}\omega^{n-1})$,$\cdots$,$(a_1\omega)$,(a_0) 中出现的 β 因子的指数,即

$$t_n=V_\beta(\omega^n),t_{n-1}=V_\beta(a_{n-1}\omega^{n-1}),\cdots,t_1=V_\beta(a_1\omega),t_0=V_\beta(a_0)。$$

故可得 $t_n=ns$,$t_{n-1}=(n-1)s$,$t_{n-2}\geqslant(n-2)s+e>e$,$\cdots$,$t_1\geqslant s+e>e$,$t_0=e$。由引理 3 的结论 3)知,$t_n,t_{n-1},\cdots,t_0$ 中的最小值至少在两个 t_i 处达到,这只可能是 $(n-1)s=e$,故 $n-1\mid e$。由于 $e\leqslant n$,且 $(n,n-1)=1$,所以只能是 $e=n-1$,$s=1$。又由 $n=\sum_{i=1}^{g}e_if_i$ 可知 $g=2$,其中 e_i 是分歧指数,f_i 是剩余类域次数,g 是分裂次数。令 $\beta_1=\beta$,$e_1=e=n-1$,$f_1=1$,则必有 $\beta_2\mid p$,$e_2=V_{\beta_2}(p)$,得到 $e_2=1$,$f_2=1$。所以可得 $pO_k=\beta_1^{n-1}\beta_2$ 成立。

2)若 $\beta\mid\omega+a_{n-1}$,可以得到结论 $\beta\nmid\omega$。这是因为若 $\beta\mid\omega$,则由 $\beta\mid\omega+a_{n-1}$ 可知 $\beta\mid a_{n-1}$,故 $a_{n-1}\in\beta\cap Z=pZ$,于是可得到 $p\mid a_{n-1}$,这与 $p\nmid a_{n-1}$ 矛盾。

下面讨论 K 中理想 $(p)+(\omega)$。可直接验证 $(p)+(\omega)$ 是 K 中的一个理想,并且有 $p\in(p)+(\omega)$,$\omega\in(p)+(\omega)$,故由 $\beta\nmid\omega$ 可得到 $(\beta,(p)+(\omega))=(\beta,(\omega))=1$。令 $\overline{\beta}$ 是 K 中的素理想,并且 $\overline{\beta}\mid(p)+(\omega)$,则有 $\overline{\beta}\mid p$ 和 $\overline{\beta}\mid\omega$,所以 $\omega\in\overline{\beta}$。故 β 和 $\overline{\beta}$ 均为 pO_k 的两个不同的素理想因子。令 $\beta_1=\overline{\beta}$,$\beta_2=\beta$,类似 1)的证明方法可得到 $e_1=n-1$,$e_2=1$,$g=2$,所以仍然有 $pO_k=\beta_1^{n-1}\beta_2$ 成立。

下面证明 $p\nmid|O_k/Z[\omega]|$。由于 $n>2$,用反证法。假设 $p\mid|O_k/Z[\omega]|$,则加法群 $O_k/Z[\omega]$ 中有 p 阶元素,即存在 $\mu\in O_k-Z[\omega]$,使得 $p\mu=x_0+x_1\omega+\cdots+x_{n-1}\omega^{n-1}\in Z[\omega]$,$x_i\in Z$。由于 $pO_k=\beta_1^{n-1}\beta_2$,并且由上述的证明

可知 $s=1,\omega\in\beta_1-\beta_1^2$，并且在 1)的情况下有 $\omega\notin\beta_2$。若不然，则 $\omega\in\beta_2$，可用 1)中同样的证明方法得到 $e_2=n-1$，故 $n=2$，这与 $n>2$ 矛盾。从而有

$$x_0+x_1\omega+\cdots+x_{n-1}\omega^{n-1}=p\mu\in\beta_1^{n-1}\beta_2\Rightarrow x_0+x_1\omega+\cdots+x_{n-1}\omega^{n-1}=p\mu\in\beta_1^{n-1}\Rightarrow\beta_1\mid x_0\Rightarrow x_0\in\beta_1\cap Z=pZ\Rightarrow$$

$$p\mid x_0\Rightarrow x_0\in\beta_1^{n-1}\Rightarrow x_1\omega\in\beta_1^2\Rightarrow x_1\in\beta_1\Rightarrow p\mid x_1\Rightarrow\cdots\Rightarrow p\mid x_{n-2}\Rightarrow x_{n-1}\omega^{n-1}\in\beta_1^{n-1}\beta_2\Rightarrow x_{n-1}\in\beta_2。$$

这是由 $\omega\notin\beta_2$ 而得到的)$\Rightarrow p\mid x_{n-1}$。于是就有 $\mu\in Z[\omega]$，这与假设 $\mu\notin Z[\omega]$ 相矛盾，从而得到 $p\nmid|O_k/Z[\omega]|$。

证毕

注 2　当 $n=2$ 时，定理 1 的结论仍然成立。根据以上证明可知，只要对 $n=2$ 时 $p\nmid|O_k/Z[\omega]|$ 成立即可。这是因为当 $n=2$ 时，$f(x)=x^2+a_1x+a_0$，$K=Q(\omega)$，令 $\overline{\omega}$ 是 $f(x)$ 的另一个根。由于二次域 K 是伽罗瓦扩张，故 $Q(\omega)=Q(\overline{\omega})$，而 $pO_k=\beta_1\beta_2$，$\beta_1\mid\omega$，则有结论：$\beta_1\mid\omega$ 且 $\beta_2\mid\omega$ 和 $\beta_1\mid\overline{\omega}$ 且 $\beta_2\mid\overline{\omega}$ 不能同时成立。若不然，则有 $\beta_1\beta_2\mid\omega$ 和$\beta_1\beta_2\mid\overline{\omega}$。故有 $p\mid\omega$ 和 $p\mid\overline{\omega}$，于是 $p^2\mid\omega\overline{\omega}=a_0$，这与 $p^2\nmid a_0$ 相矛盾。所以有以下结论。

i) 若 $\beta_2\nmid\omega$，并且假设 $p\mid|O_k/Z[\omega]|$，则存在 $\mu\in O_k-Z[\omega]$，$p\mu=x_0+x_1\omega\in Z[\omega]$，故有

$$x_0+x_1\omega=p\mu\in\beta_1\beta_2\Rightarrow\beta_1\mid x_0\Rightarrow x_0\in\beta_1\cap Z=pZ\Rightarrow p\mid x_0\Rightarrow x_1\omega\in\beta_1\beta_2\Rightarrow x_1\in\beta_2\Rightarrow p\mid x_1$$

于是就有 $\mu\in Z[\omega]$，这与假设 $\mu\notin Z[\omega]$ 相矛盾，从而得到 $p\nmid|O_k/Z[\omega]|$。

ii) 若设 $\beta_2\nmid\overline{\omega}$，则由上面的证明知 $\beta_1\mid\overline{\omega}$，所以由 i)的证明可知 $p\nmid|O_k/Z[\overline{\omega}]|$。而由于 $Z[\omega]\cong Z[\overline{\omega}]$，所以就有 $O_k/Z[\omega]\cong O_k/Z[\overline{\omega}]$。故 $|O_k/Z[\omega]|=|O_k/Z[\overline{\omega}]|$，于是就有 $p\nmid|O_k/Z[\omega]|$ 成立。

注 3　由于 $p\nmid|O_k/Z[\omega]|$，则 $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_0\equiv x^{n-1}(x+a_{n-1})\pmod p$，故有此可得到 $pO_k=\beta_1^{n-1}\beta_2$，并且 $\beta_1=(p,\omega^{n-1})$，$\beta_2=(p,\omega+a_{n-1})$。

通过定理 1 可以得到广(E,p)型数域的几个性质。

性质 1　若 $K=Q(\omega)$是广(E,p)型数域，$[K:Q]=n$。若 $n>2$，则 K/Q 不是数域的伽罗瓦扩张。

证明　反证法。假设 K/Q 是数域的伽罗瓦扩张，则由于 $K=Q(\omega)$是广(E,p)型数域，故 $pO_k=\beta_1^{n-1}\beta_2$，由此可得 $V_{\beta_1}(p)=V_{\beta_2}(p)$。所以有 $n-1=1$，即 $n=2$。这与 $n>2$ 矛盾。所以 K/Q 不是数域的伽罗瓦扩张。　证毕

推论 2　若 $K=Q(\omega)$是广(E,p)型数域，$[K:Q]=n$。若 $n=2$，则 $p\nmid d(K)$。

证明　由于若 $K=Q(\omega)$是广(E,p)型数域，$n=2$，则 $pO_k=\beta_1\beta_2$，故 p 在 K 中不分歧(是完全分裂的)，所以可得 $p\nmid d(K)$。　证毕

性质 2　若 $K=Q(\omega)$是广(E,p)型数域，并且 $pO_k=\beta_1^{n-1}\beta_2$，则有限域为 $O_k/\beta_1\cong O_k/\beta_2$。

证明　由于由定理 1 的证明知 $f_1=f_2=1$，f_i 为剩余类域次数。则 $[O_k/\beta_1:Z/pZ]=1$，$[O_k/\beta_2:Z/pZ]=1$。于是又有 $O_k/\beta_1\cong Z/pZ$ 和 $O_k/\beta_2\cong Z/pZ$。故有 $O_k/\beta_1\cong O_k/\beta_2$。　证毕

性质 3　若 $K=Q(\omega)$是广(E,p)型数域，则 $(p)+(\omega)$是 K 的素理想。

证明　由于 $pO_k=\beta_1^{n-1}\beta_2$，故：1)当 $n>2$ 时，由定理 1 的证明可知 $\omega\in\beta_1-\beta_1^2$，$\omega\notin\beta_2$。$(p)+(\omega)$是 (p) 和 (ω)的最大公因理想。所以 $(p)+(\omega)=\beta_1$，故 $(p)+(\omega)$是 K 的素理想。

2)当 $n=2$ 时，由定理 1 的注可知 $\beta_1=(p,\omega)$，$\beta_2=(p,\omega+a_1)$。所以 $(p)+(\omega)=(p,\omega)=\beta_1$，故亦可得 $(p)+(\omega)$是 K 的素理想。　证毕

注 4　由定理 1 可进一步得到对于素理想分解 $pO_k=\beta_1^{n-1}\beta_2$，$n\geqslant2$，都有 $\beta_1\mid\omega$，$\beta_2\nmid\omega$。这个结论由性质 3 容易得证，这里就不在多加叙述。

参考文献：

[1] 冯克勤，李尚志，查建国，等. 近世代数引论[M]. 合肥：中国科学技术大学出版社，2002：120-124.
Feng K Q，Li S Z，Zha J G，et al. Modern algebra introduction[M]. Hefei：University of Science and Technology of China，2002：120-124.

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

[3] 冯克勤，章璞. 近世代数三百题[M]. 北京：高等教育出版社，2010：126-127.
Feng K Q，Zhang P. Questions of modern algebra[M]. Beijing：Higher Education Press，2010：126-127.

[4] 乔明云,刘裕文. 艾森斯坦因判别法的推广[J]. 数学通报 1997(5):41-42.
Qiao Y M, Liu Y W. The generalization of Eisenstein criterion[J]. Bulletion des Sciences Mathematics, 1997(5): 41-42.

[5] 孔庆兰. 不可约多项式的判别[J]. 枣庄师专学报,2000(2):33-34.
Kong L Q. The criterion of irreducible polynomial[J]. Journal of Zaozhuang Teachers' College, 2000(2): 33-34.

[6] 马跃超. 整系数不可约多项式的两个判别法[J]. 数学通报,1988(6):18-19.
Ma Y C. Two criterions for integral coefficient' integral irreducible polynomial[J]. Bulletion des Sciences Mathematics, 1988(6): 18-19.

[7] 施武杰,戴桂生. 高等代数[M]. 北京:高等教育出版社,2009:129-130.
Shi W J, Dai G S. Higher algebra[M]. Beijing: Higher Education Press, 2009: 129-130.

[8] 霍元极,寇福来. 高等代数[M]. 北京:北京师范大学出版社,2009:63-65.
Huo Y J, Kou F L. Higher algebra[M]. Beijing: BeiJing Normal University Press, 2009: 63-65.

[9] 卫星. 关于(E,p)型数域的一些讨论[J]. 四川师范大学学报:自然科学版,2002,25(3):240-242.
Wei X. Some dicussions on number fields of (E,p)-Type [J]. Journal of Sichuan Normal University: Natural Science, 2002, 25(3): 240-242.

The Generalization of Eisenstein Criterion and Number Fields of (E,p)-Type

TAO Xin'en, SONG Xinxin, ZHUANG Yuanyuan, LUO Ming

(School of Mathematics, Chongqing Normal University, Chongqing 401331, China)

Abstract: Eisenstein criterion is an important way of finding the reducibility of integer polynomial under rational number field in higher algebra, and also a hot issue in studying polynomial. It has a great many forms of generalization, and the definition of the number fields of (E,p)-Type comes from the primitive from. On the basic of Eisenstein criterion, this paper extends the number fields of (E,p)-Type, and then study its properties: give the decomposition of prime ideal type in the generalized number fields. The specific method: prove Lemma 3 and use point 3, then get the decomposed form of the prime ideal. And this paper give this prime an important property (refer to Theorem 1). This is the main contents of this paper. Besides, by Theorem 1 and its proof can we get prime under generalized number fields of (E,p)-Type and some properties related to prime ideal. So we can generalize Eisenstein criterion and the number fields of (E,p)-Type and get more properties and make this theory more consummate.

Key words: Eisenstein criterion; number fields of (E,p)-type; prime ideal

(责任编辑 黄 颖)