अल्जेब्रैक नम्बर थेओरी प्रतिबेदन

मनोज ज्ञवाली

सुपरिबेक्षक प्रा. Francesco Pappalardi

तल दियिएको बहुपदिएको अल्जेब्रैक नम्बर थेओरी अचल (constants) हरु पत्ता लगैएको छ । यसको लागि पारी(PARI) प्रोग्राम प्रयोग गरिएको छ ।

polisirreducible(f) : Irreducible छ कि छैन चेक गर्न प्रयोग गर्ने, polisirreducible(f) = 1 (छ)

1. ग्याल्वा ग्रुप (Galois Group):

ग्याल्वा ग्रुप पत्तालगाउनको लागि निम्न कमाण्ड प्रयोग गरिन्छ

polgalois(f)

[40320,-1,50,”S8”]

जसको अर्थ हुन्छ, ग्रुप अडर : 40320,

सिग्नेचर : -1 अल्टर्नेटिग ग्रुप को सबसेट होईन ( अल्टर्नेटिग भए 1 नत्र - 1)

ग्रुप स्त्टकच्र र : S8 (आठवटा अक्षर को पर्मुतेसन ग्रुप )

1. डिस्कृमिनेन्त पोलिनोमिअल को (Discriminant of polynomial):

पत्तालगाउनको लागि निम्न कमाण्ड प्रयोग गरिन्छ

poldisc(f)

डिस्कृमिनेन्त = -140800290968875457763917051809140

1. नम्बर फिल्ड को डिस्कृमिनेन्त (Discriminant of Number Field)

नम्बर फिल्ड = K() , एउटा f को रूट हो

सर्ब प्रथम नम्बर फिल्ड को लागि K= nfinit(f) र

नम्बर फिल्ड को डिस्कृमिनेन्त K.disc प्रयोग गरिन्छ

नम्बर फिल्ड को डिस्कृमिनेन्त = -238446591010439766362123860

र एस्लाई फ्याक्टोर गर्न को लागि कमान्ड : factor(K.disc) प्रयोग गरिन्छ

एस्लाई फ्याक्टोर गर्दा एस्तो आयो

[-1,1]

[2,2]

[3,1]

[5,1]

[47,1]

[13151,1]

[22622629,1]

[2842104522287 , 1]

गर्दा एस्तो आयो जस्को अर्थ हुन्छ । हरेक कोम्पोनेन्ट को पहिलो नम्बर र दोर्सो पाओर जनाउछ

1. नम्बर फिल्ड को इन्टिग्रल बेसिस (Integral Basis):

इन्टिग्रल बेसिस को लागि निम्न कमाण्ड प्रयोग गरिन्छ, एहा हाम्रो फिल्ड K हो तेसैले:

K.zk कमान्ड प्रयोग गरिन्छ

एस्तो आयो

[1, -1/9\*x^7 + 91/9\*x^6 + 4/9\*x^5 - 4\*x^4 + 17/9\*x^3 + 20/3\*x^2 + 11/3\*x + 2, -1/9\*x^7 + 94/9\*x^6 - 269/9\*x^5 - 16/3\*x^4 + 125/9\*x^3 + x^2 - 49/3\*x - 6, -1/27\*x^7 + 97/27\*x^6 - 551/27\*x^5 + 253/9\*x^4 + 269/27\*x^3 - 122/9\*x^2 - 58/9\*x + 22/3, -5/81\*x^7 + 458/81\*x^6 - 271/81\*x^5 + 491/27\*x^4 - 2192/81\*x^3 - 169/27\*x^2 + 421/27\*x + 50/9, x - 11, -1/9\*x^7 + 88/9\*x^6 + 277/9\*x^5 - 8/3\*x^4 - 82/9\*x^3 - 236/3\*x^2 + 59/3\*x + 24, 4/81\*x^7 - 388/81\*x^6 + 2150/81\*x^5 + 635/27\*x^4 - 3317/81\*x^3 - 169/27\*x^2 - 1595/27\*x + 95/9]

1. प्राईम आइडिएल को फेक्तोरैजेसन । (Decomposition of primes)

सर्ब प्रथम रामिफएड प्राईमहरु : जस्ले नम्बर फिल्ड को डिस्कृमिनेन्त लाई भाग जान्छ, यहाँ रामिफएड प्राईमहरु 2, 3, 5,47 हुन

= नम्बर फिल्ड को डिस्कृमिनेन्त

यहाँ , poldisc(f)/K.disc = 59049 = 3^10

र

एदी भयोभने, ले लाई भाग जादैन , तेसकारण प्राईम को लागि कुमार थेओरेम प्रयोग गर्न सकिन्छ

प्राईम आइडिएल को फेक्तोरैजेसन को लागि हामीले कुमार थेओरम (Kummer’s Lemma) प्रयोग गरिएको छ

(2) को लागि :

सर्बप्रथम मोड २ मा एस्तो हुन्छ

Mod(f,2)

%5 = Mod(1, 2)\*x^8 + Mod(1, 2)\*x^7 + Mod(1, 2)\*x^4 + Mod(1, 2)\*x^2

factor(Mod(f,2))

%6 = [Mod(1, 2)\*x, 2; Mod(1, 2)\*x + Mod(1, 2), 1; Mod(1, 2)\*x^2 + Mod(1, 2)\*x + Mod(1, 2), 1; Mod(1, 2)\*x^3 + Mod(1, 2)\*x^2 + Mod(1, 2), 1]

अतार्थ,

मोड २ मा हेर्दा र फेक्तोरैजेसन गर्दा

तेसकारण,

.

यसरीनै सबै आइडिएल लाई फेक्तोरैजेसन सकिन्छ ।

(3): एसको लागि सिधै idealprimedec(K,3) कमान्ड प्रयोग गरी निकाल्न सकिन्छ ।

(5):

(7) : इनर्ट (चेन्ज हुँदैन )

(11):

factor(Mod(f,11)):

[Mod(1, 11)\*x^2 + Mod(6, 11)\*x + Mod(3, 11), 1; Mod(1, 11)\*x^6 + Mod(2, 11)\*x^5 + Mod(3, 11)\*x^4 + Mod(1, 11)\*x^3 + Mod(1, 11)\*x^2 + Mod(8, 11)\*x + Mod(4, 11), 1]

(13):

[Mod(1, 13)\*x + Mod(1, 13), 1; Mod(1, 13)\*x^2 + Mod(5, 13)\*x + Mod(8, 13), 1; Mod(1, 13)\*x^5 + Mod(7, 13)\*x^4 + Mod(6, 13)\*x^3 + Mod(5, 13)\*x^2 + Mod(1, 13)\*x + Mod(3, 13), 1]

lift(factor(Mod(f,13)))

%14 = [x + 1, 1; x^2 + 5\*x + 8, 1; x^5 + 7\*x^4 + 6\*x^3 + 5\*x^2 + x + 3, 1]

lift(factor(Mod(f,17)))

%15 = [x + 14, 1; x^2 + 11\*x + 6, 1; x^5 + 3\*x^4 + 16\*x^3 + 7\*x^2 + 5\*x + 3, 1]

lift(factor(Mod(f,19)))

%16 = [x + 6, 1; x^2 + 8\*x + 1, 1; x^5 + 9\*x^4 + 11\*x^3 + 5\*x^2 + 4\*x + 10, 1]

lift(factor(Mod(f,23)))

%19 = [x + 20, 1; x^7 + 4\*x^6 + 8\*x^5 + 14\*x^4 + 2\*x^3 + 15\*x^2 + 12\*x + 18, 1]

lift(factor(Mod(f,29)))

%20 = [x + 11, 1; x + 21, 1; x^2 + 19\*x + 10, 1; x^4 + 3\*x^3 + 9\*x^2 + 6\*x + 17, 1]

lift(factor(Mod(f,31)))

%21 = [x + 29, 1; x^7 + 4\*x^6 + 4\*x^5 + 13\*x^4 + 9\*x^3 + 20\*x^2 + 7\*x + 27, 1]

lift(factor(Mod(f,37)))

%22 = [x + 8, 1; x + 15, 1; x + 22, 1; x + 35, 1; x^4 + 14\*x^3 + 5\*x^2 + 31\*x + 22, 1]

lift(factor(Mod(f,41)))

%23 = [x + 16, 1; x^7 + 16\*x^6 + 27\*x^5 + 14\*x^4 + 5\*x^3 + 24\*x^2 + 34\*x + 12, 1]

lift(factor(Mod(f,43)))

%24 = [x + 11, 1; x + 14, 1; x^6 + 13\*x^5 + 33\*x^4 + 4\*x^3 + 4\*x^2 + 41\*x + 3, 1]

lift(factor(Mod(f,47)))

%25 = [x + 37, 2; x^2 + 16\*x + 24, 1; x^4 + 7\*x^3 + 32\*x^2 + 40\*x + 29, 1]

lift(factor(Mod(f,53)))

%26 = [x + 35, 1; x^7 + 33\*x^6 + 7\*x^5 + 3\*x^4 + 37\*x^3 + 23\*x^2 + 10\*x + 3, 1]

lift(factor(Mod(f,59)))

%27 = Mat([x^8 + 27\*x^7 + 55\*x^6 + 36\*x^5 + 42\*x^4 + 58\*x^3 + 26\*x^2 + 41\*x + 5, 1])

(59) इनर्ट (चेन्ज हुँदैन ) (inert)

lift(factor(Mod(f,61)))

%28 = Mat([x^8 + 31\*x^7 + 57\*x^6 + 36\*x^5 + 44\*x^4 + x^3 + 28\*x^2 + 43\*x + 7, 1])

(61) इनर्ट (चेन्ज हुँदैन )( inert)

lift(factor(Mod(f,67)))

%29 = [x^2 + 2\*x + 22, 1; x^6 + 41\*x^5 + 26\*x^4 + 20\*x^3 + 41\*x^2 + 21\*x + 28, 1]

lift(factor(Mod(f,71)))

%30 = [x + 15, 1; x^7 + 36\*x^6 + 24\*x^5 + 31\*x^4 + 15\*x^3 + 70\*x^2 + 53\*x + 39, 1]

lift(factor(Mod(f,73)))

%31 = [x + 21, 1; x + 61, 1; x^2 + 7\*x + 57, 1; x^4 + 39\*x^3 + 15\*x^2 + 63\*x + 14, 1]

lift(factor(Mod(f,79)))

%32 = [x^3 + 61\*x^2 + 36\*x + 74, 1; x^5 + 6\*x^4 + 68\*x^3 + 22\*x^2 + 15\*x + 74, 1]

lift(factor(Mod(f,83)))

%33 = [x^4 + 30\*x^3 + 16\*x^2 + 30\*x + 16, 1; x^4 + 45\*x^3 + 41\*x^2 + 48\*x + 7, 1]

lift(factor(Mod(f,89)))

%34 = [x + 69, 1; x^2 + 2\*x + 49, 1; x^2 + 81\*x + 45, 1; x^3 + 24\*x^2 + 66\*x + 19, 1]

lift(factor(Mod(f,97)))

%35 = [x^4 + 39\*x^3 + 90\*x^2 + 58\*x + 51, 1; x^4 + 64\*x^3 + 29\*x^2 + 71\*x + 56, 1]

क्लास ग्रुप :

K2 = bnfinit(K);

क्लास ग्रुप को लागि K2.no प्रयोग गर्ने

K2.no = 1

औटा मात्र एलेमेन्ट छ (Trivial class group )

रेगुलाटोर : रेगुलाटोर को लागि K2.reg

K2.reg

%40 = 1168113564963.523077765132945

टोर्सन युनिट हरु : टोर्सन पोइन्टस को लागि (फाइनाइट अर्डर भएको एलेमेन्टस हरु )

K2.tu

[2,-1]

दुइ वटा रूट हरु (एन थ्) छन ±1 .