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 ।

$$f = x^8 - 91x^7 - 4x^6 + 36x^5 - 17x^4 - 60x^3 - 33x^2 - 18x - 54$$

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 स्ट्टकच्र र : S8 (आठवटा अक्षर को पर्मुतेसन ग्रुप)
2. डिस्कृमिनेन्त पोलिनोमिअल को (Discriminant of polynomial):
   पत्तालगाउनको लागि निम्न कमाण्ड प्रयोग गरिन्छ
   poldisc(f)
   डिस्कृमिनेन्त = -14080029096887545776391705180914O
3. नम्बर फिल्ड को डिस्कृमिनेन्त (Discriminant of Number Field)
   नम्बर फिल्ड = K(α) , α 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 = -2384465910104397663621238O
   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

$$-2384465910104397663621238 60$$
$$= -2^2 \times 3 \times 5 \times 47 \times 13151 \times 22622629 \times 2842104522287$$

4. 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]
```

5. 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 $13151,22622629,2842104522287$ हुन

   $disc(f) = [O_K : Z]^2 \, \Delta_K$

   Δ_K = नम्बर फिल्ड को डिस्कृमिनेन्त

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

   $[O_K : Z]^2 = 3^{10}$ र $[O_K : Z] = 3^5$

   एदी $p \neq 3$ भयोभने, p ले $[O_K : Z]$ लाई भाग जादैन , तेसकारण $p \neq 3$ 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

$$\bar{f} = x^2(x+1)(x^2+x+1)(x^3+x^2+1)\ (mod\ 2)$$

तेसकारण,

$(2) = (\alpha\ \ ,2)^2(\alpha+1,2\ )(\alpha^2+\alpha+1,2)(\alpha^3+\alpha^2+1,2).$

यसरीनै सबै आइडिएल लाई फेक्तोरैजेसन सकिन्छ ।

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

(5):

$$\bar{f} = (x+3)(x+4)^2(x^2+4x+1)(x^3+\ 4x^2+x+2)\ (mod\ 5)$$

$$(5) = (\alpha+3,5)((\alpha+4)\ \ ,5)^2\ \ (\alpha^2+4\alpha+1,5)(\alpha^3+\ 4\alpha^2+\alpha+2,5)$$

(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]
```

$$\bar{f} = (x^2+6x+3)(x^6+2x^5+3x^4+x^3+\ x^2+8x+4)\ \ (mod\ 11)$$

$$(11) = (\alpha^2+6\alpha+3,11)(\alpha^6+2\alpha^5+3\alpha^4+\alpha^3+\ \alpha^2+8\alpha+4,11)$$

(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]
```

$$(13) = (\alpha + 1{,}13)(\alpha^2 + 5\alpha + 8{,}13)(\alpha^5 + 7\alpha^4 + 6\alpha^3 + 5\,\alpha^2 + \alpha + 3{,}11)$$

```
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]
```

$$(17) = (\alpha + 14{,}17)(\alpha^2 + 11\alpha + 6{,}17)(\alpha^5 + 3\alpha^4 + 16\alpha^3 + 7\alpha^2 + 5\alpha + 3{,}17)$$

```
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]
```

$$(19) = (\alpha + 6{,}19)(\alpha^2 + 8\alpha + 1{,}19)(\alpha^5 + 9\alpha^4 + 11\alpha^3 + 5\alpha^2 + 4\alpha + 10{,}19)$$

```
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]
```

$$(23) = (\alpha + 20{,}23)(\alpha^7 + 4\alpha^6 + 8\alpha^5 + 14\alpha^4 + 2\alpha^3 + 15\alpha^2 + 12\alpha + 8{,}23)$$

```
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]
```

$$(29) = (\alpha + 11{,}29)(\alpha + 21{,}29)(\alpha^2 + 19\alpha + 10{,}29)(\alpha^4 + 3\alpha^3 + 9\alpha^2 + 6\alpha + 17{,}29)$$

```
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]
```

$$(31) = (\alpha + 29{,}31)(\alpha^7 + 4\alpha^6 + 4\alpha^5 + 13\alpha^4 + 9\alpha^3 + 20\alpha^2 + 7\alpha + 27{,}31)$$

```
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]
```

$$(37) = (\alpha + 8{,}37)(\alpha + 15{,}37)(\alpha + 22{,}37)(\alpha + 35{,}37)(\alpha^4 + 14\alpha^3 + 5\alpha^2 + 31\alpha + 22{,}37)$$

```
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]
```

$$(41) = (\alpha + 16{,}41)(\alpha^7 + 16\alpha^6 + 27\alpha^5 + 14\alpha^4 + 5\alpha^3 + 24\alpha^2 + 34\alpha + 12{,}41)$$

```
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]
```

$$(43) = (\alpha + 11{,}43)(\alpha + 14{,}43)(\alpha^6 + 13\alpha^5 + 33\alpha^4 + 4\alpha^3 + 4\alpha^2 + 41\alpha + 3{,}43)$$

```
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]
```

$$(47) = (\alpha + 37{,}47)^2(\alpha^2 + 16\alpha + 24{,}47)(\alpha^4 + 7\alpha^3 + 32\alpha^2 + 40\alpha + 29{,}47)$$

```
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]
```

$$(53) = (\alpha + 35{,}53)(\alpha^7 + 33\alpha^6 + 7\alpha^5 + 3\alpha^4 + 37\alpha^3 + 23\alpha^2 + 10\alpha + 3{,}53)$$

```
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]
```

$$(67) = (\alpha^2 + 2\alpha + 22{,}67)(\alpha^6 + 41\alpha^5 + 26\alpha^4 + 20\alpha^3 + 41\alpha^2 + 21\alpha + 28{,}67)$$

```
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]
```

$$(71) = (\alpha + 15{,}71)(\alpha^7 + 36\alpha^6 + 24\alpha^5 + 31\alpha^4 + 15\alpha^3 + 70\alpha^2 + 53\alpha + 39{,}71)$$

```
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]
```

$$(73) = (\alpha + 21{,}73)(\alpha + 61{,}73)(\alpha^2 + 7\alpha + 57{,}73)(\alpha^4 + 39\alpha^3 + 15\alpha^2 + 63\alpha + 14{,}73)$$

```
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]
```

$$(79) = (\alpha^3 + 61\alpha^2 + 36\alpha + 74{,}79)(\alpha^5 + 6\alpha^4 + 68\alpha^3 + 22\alpha^2 + 15\alpha + 74{,}79)$$

```
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]
```

$$(83) = (\alpha^4 + 30\alpha^3 + 16\alpha^2 + 30\alpha + 16{,}83)(\alpha^4 + 45\alpha^3 + 41\alpha^2 + 48\alpha + 7{,}83)$$

```
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]
```

$$(89) = (\alpha + 69{,}89)(\alpha^2 + 2\alpha + 49{,}89)(\alpha^2 + 81\alpha + 45{,}89)(\alpha^3 + 24\alpha^2 + 66\alpha + 19{,}89)$$

```
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]
```

$$(97) = (\alpha^4 + 39\alpha^3 + 90\alpha^2 + 58\alpha + 51{,}97)(\alpha^4 + 64\alpha^3 + 29\alpha^2 + 71\alpha + 56{,}97)$$

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 .