Polynomial Report

Chiara Camerini

A.A. 2018-2019

Given the polynomial

$$f(T) = T^8 - 19\,T^7 + 15\,T^6 - 26\,T^5 + 2\,T^4 - 94\,T^3 - 47\,T^2 - 23\,T - 41$$

we want to study it using **PARI/GP**.

```
? f(T)=T^8-19*T^7+15*T^6-26*T^5+2*T^4-94*T^3-47*T^2-23*T-41;
```

Galois group

First we check if the polynomial is irreducible:

```
? polisirreducible(f(T))
%2=1
```

Let us construct the number field:

```
?  F=bnfinit(f(T));
```

then $F = \mathbb{Q}(\alpha)$ is the *number field* where α is a root of $f(T)$.

We can also study the Galois group:

```
? polgalois(f(T))
%4= [40320, -1, 50, "S8"]
```

The *Galois group* has order 40320 and signature -1 then it is not contained in the alternating group.
The third number $k = 50$ is the numbering of the group among all transitive subgroups of S_8, as given in *"The transitive groups of degree up to eleven", G. Butler and J. McKay, Communications in Algebra, vol. 11, 1983.*
The last one says us that it is isomorphic to S_8.

For more information about this click here.

Discriminats and integral basis

Let $K[T]$ be a ring and let $f(T) = \prod_{j=1}^{n}(T - \alpha_j) \in K[T]$.
The *polynomial discriminant* is defined by

$$D_f = \prod_{1\le i<j\le n} (\alpha_i - \alpha_j)^2.$$

```
? Disc=poldisc(f(T))
%5= -2353880929696986070373957632
```

Then $D_f = -2353880929696986070373957632$.

A set of n elements $\omega_1, \cdots \omega_n \in O_F$ such that $O_F = \mathbb{Z}\omega_1 \oplus \cdots \oplus \mathbb{Z}\omega_n$ is called *integral basis* for O_F.

```
? B=nfbasis(f(T))
%6 = [1, T, T^2, 1/2*T^3 - 1/2, 1/2*T^4 - 1/2*T,

 1/2*T^5 - 1/2*T^2, 1/4*T^6 - 1/4, 1/4*T^7 - 1/4*T]

? w_1=B[4];
? w_2=B[7];
```

Then

$$O_F = \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \mathbb{Z}\alpha^2 \oplus \mathbb{Z}\frac{\alpha^3-1}{2} \oplus \mathbb{Z}\frac{\alpha^4-\alpha}{2} \oplus \mathbb{Z}\frac{\alpha^5-\alpha^2}{2} \oplus \mathbb{Z}\frac{\alpha^6-1}{4} \oplus \mathbb{Z}\frac{\alpha^7-\alpha}{4}.$$
$$= \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \mathbb{Z}\alpha^2 \oplus \mathbb{Z}w_1 \oplus \mathbb{Z}w_1\alpha \oplus \mathbb{Z}w_1\alpha^2 \oplus \mathbb{Z}w_2 \oplus \mathbb{Z}w_2\alpha$$

Let F be a number field of degree n and $(\omega_1, \omega_2, \dots, \omega_n)$ an integral basis for O_F. The *field discriminant* is defined by

$$\Delta_F = \Delta(\omega_1, \omega_2, \dots, \omega_n) = \det\left(\varphi(\omega_i)\right)_{i,\varphi}$$

for $i = 1, \cdots, n$ and $\varphi\colon F \hookrightarrow \mathbb{C}$

```
? Delta=nfdisc(f(T))
%9= -143669490337950809959348
```

Then $\Delta_F = -143669490337950809959348$.

The determinants give us an important information about O_F.

$$\boxed{\begin{array}{c} If\ f(\alpha)=0 \text{ and } F=\mathbb{Q}(\alpha) \text{ then } D_f = [O_F\colon \mathbb{Z}[\alpha]]^2 \cdot \Delta_F \\ \Rightarrow [O_F\colon \mathbb{Z}[\alpha]]^2 = \dfrac{D_f}{\Delta_F} \Rightarrow [O_F\colon \mathbb{Z}[\alpha]] = \left(\dfrac{D_f}{\Delta_F}\right)^{1/2} \end{array}}$$

```
? I=(Disc/Delta)^(1/2)
%10 = 128
? factor(I)
%11 =
[2 7]
```

then in our case $[O_F\colon \mathbb{Z}[\alpha]] = 2^7$.

Decomposition of prime ideals

Let F be a number field of degree n and $(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$ the decomposition of prime ideals then $n = \sum_{i=1}^{g} e_i f_i$ where $N(\mathfrak{p}_i) = p^{f_i}$.

The number f_i is called the *inertia index* and e_i is called the *ramification index* of the prime ideal $\mathfrak{p}_i$.
The prime ideals $\mathfrak{p}_i$ for which $e_i > 1$ are called *ramified.*

$$(p)\ is\ said \begin{cases} \text{ramified} & if\ e_i > 1\ \exists i \\ \text{totally ramified} & if\ g = f_1 = 1,\ e_1 = n \\ \text{totally split} & if\ g = n,\ e_i = f_i = 1 \\ \text{inert} & if\ g = e_1 = 1,\ f_1 = n \end{cases}$$

To find the decompositions we use this instructions:

```
? F.zk to declare the basis of the ring of integers
% = [w_1, ... , w_8]
? dec=idealprimedec(F,p);
? #dec
% = g the number g of the prime ideals p_i of p
? [p_1, ... , p_g]=dec;
? pi.e
% = e_i  the ramification index
? pi.f
% =f_i  the inertia index
? pi.gen to have the generators of the ideal
% = [p, [a_1, ... , a_8]~]
```

then

$$\mathfrak{p}_j = (p, \sum_{i=1}^{8} a_i w_i)\ for\ j = 1, \cdots, g$$
$$\Rightarrow (p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}.$$

Decomposition of all ramified primes

To find all ramified primes we use *Dirichlet's Theorem*:

$$\boxed{p \textit{ is ramified in } F \textit{ over } \mathbb{Q} \textit{ if and only if } p \mid \Delta_f}$$

We can find the prime factors of Δ_F:

```
? factor(Delta)
%12=
[          -1 1]

[           2 2]

[        1697 1]

[       19661 1]

[       49211 1]

[21875345651 1]
```

$\Rightarrow \Delta_F = -1 \cdot 2^2 \cdot 1697 \cdot 19661 \cdot 49211 \cdot 21875345651.$

We see a complete example of code:

- $p = 2$:

```
? w=F.zk;
? dec=idealprimedec(F,2);
? #dec
%15 = 3
?[p1,p2,p3]=dec;
? p1.e
%17 = 2
? p2.e
%18 = 1
? p3.e
%19 = 1
? p1.f
%20 = 1
? p2.f
%21 = 2
? p3.f
%22 = 4
```

$\Rightarrow (p) = \mathfrak{p}_1^2 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3$ with $N(\mathfrak{p}_1) = p,\ N(\mathfrak{p}_2) = 2,\ N(\mathfrak{p}_3) = 4$

In particular we have

```
? [p,a]=p1.gen
%23 = [2, [-1, 0, 0, 1, 1, 0, 0, 1]~]

? A=0;
? for(i=1,8, A=a[i]*w[i]+A; )
? A
%27 = 1/2*T^6 - 19/2*T^5 + 15/2*T^4 - 27/2*T^3
      + 21/2*T^2 - 109/2*T - 13
```

$\Rightarrow \mathfrak{p}_1 = (2, (\alpha^5 - 19\alpha^4 + 15\alpha^3 - 27\alpha - 109)\alpha/2 - 13)$

```
? [p,a]=p2.gen
%28 = [2, [0, 0, 0, 0, 0, 1, 0, 0]~]

? A=0;
? for(i=1,8, A=a[i]*w[i]+A; )
? A
%31 = 1/4*T^6 - 5*T^5 + 17/2*T^4
      - 10*T^3 + 2*T^2 - 31/2*T + 11/4
```

$\Rightarrow \mathfrak{p}_2 = (2, (1/4)\alpha^6 - 5\alpha^5 + (17/2)\alpha^4 - 10\alpha^3 + 2\alpha^2 - (31/2)\alpha + (11/4))$

```
? [p3,a]=p3.gen
%32 = [2, [-1, 1, 1, 0, 0, 0, 0, 1]~]

? A=0;
? for(i=1,8, A=a[i]*w[i]+A; )
? A
%36 = 1/4*T^6 - 5*T^5 + 17/2*T^4
      - 10*T^3 + 3*T^2 - 65/2*T + 3/4
```

$\Rightarrow \mathfrak{p}_3 = (2, (1/4)\alpha^6 - 5\alpha^5 + (17/2)\alpha^4 - 10\alpha^3 + 3\alpha^2 - (6/2)\alpha + (3/4))$

Finally we obtain

$$\begin{aligned}(2) = &\Big(2, (\alpha^5 - 19\alpha^4 + 15\alpha^3 - 27\alpha - 109)\alpha/2 - 13\Big)^2 \\ &\Big(2, (1/4)\alpha^6 - 5\alpha^5 + (17/2)\alpha^4 - 10\alpha^3 + 2\alpha^2 - (31/2)\alpha + (11/4)\Big) \\ &\Big(2, (1/4)\alpha^6 - 5\alpha^5 + (17/2)\alpha^4 - 10\alpha^3 + 3\alpha^2 - (6/2)\alpha + (3/4)\Big).\end{aligned}$$

- $p = 1697$:

$$\begin{aligned}(p) &= \mathfrak{p}_1^2 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3 \\ &= (p, \alpha - 628)^2 (p, \alpha + 698)(p, \alpha^5 + 593\alpha^4 + 764\alpha^3 - 715\alpha^2 + 566\alpha + 284)\end{aligned}$$

with $N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = p,\ N(\mathfrak{p}_3) = 5$

- $p = 19661$:

$$\begin{aligned}(p) &= \mathfrak{p}_1^2 \cdot \mathfrak{p}_2 \\ &= (19661, \alpha - 5697)^2 (19661, \alpha^6 - 8286\alpha^5 + 5955\alpha^4 - 5522\alpha^3 + 9001\alpha^2 - 3016\alpha + 4258)\end{aligned}$$

with $N(\mathfrak{p}_1) = p,\ N(\mathfrak{p}_2) = p^6$

- $p = 49211$:

$$(p) = \mathfrak{p}_1^2 \mathfrak{p}_2 \mathfrak{p}_3 = (p, \alpha + 8332)^2 (p, \alpha^3 - 21456\alpha^2 + 22893\alpha + 12282)$$

with $N(\mathfrak{p}_1) = 1,\ N(\mathfrak{p}_2) = N(\mathfrak{p}_3) = p^3$

- $p = 21875345651$:

$$\begin{aligned}(p) &= \mathfrak{p}_1^2 \mathfrak{p}_2 \mathfrak{p}_3 \mathfrak{p}_4 \mathfrak{p}_5 \\ &= (p, \alpha - 9506090252)^2 (p, \alpha - 6742773249)(p, \alpha - 3540845208) \\ &\quad (p, \alpha - 2126331747)(p, \alpha^3 + 9546785038\alpha^2 - 9856687362\alpha + 5317905622)\end{aligned}$$

with $N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = N(\mathfrak{p}_3) = N(\mathfrak{p}_4) = p,\ N(\mathfrak{p}_5) = p^3$

Decomposition of primes less of 100

We can easily describe the other prime ideals:

- $p = 3$:

  $g = e = 1,\ f = n = 8, \Rightarrow (p)$ *is inert.*

- $p = 5$:

  $g = e = 1,\ f = n = 8 \Rightarrow (p)$ *is inert*

- $p = 7$:

$$(p) = \mathfrak{p}_1 \mathfrak{p}_2 = (p, \alpha^4 - 3\alpha^3 - \alpha^2 - 2\alpha - 3)(p, \alpha^4 - 2\alpha^3 + 3\alpha^2 - 3\alpha + 2)$$

with $N(\mathfrak{p}_1) = N(\mathfrak{p}_1) = p^4$

- $p = 11$:

$$(p) = \mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3 \mathfrak{p}_4 = (p, \alpha+3)(p, \alpha+4)(p, \alpha^2+3\alpha-1)(p, \alpha^4+4\alpha^3-2\alpha^2+2\alpha-3)$$

with $N(\mathfrak{p}_1) = (\mathfrak{p}_2) = p,\ N(\mathfrak{p}_3) = p^2,\ N(\mathfrak{p}_4) = p^4$

- $p = 13$:

  $(p) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 = (p, \alpha^2 - 5\alpha - 5)(p, \alpha^2 - 4\alpha - 2)(p, \alpha^4 + 3\alpha^3 + 3\alpha^2 - 3\alpha + 5)$

  with $N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = p^2,\ N(\mathfrak{p}_3) = p^4$

- $p = 17$:

  $$(p) = \mathfrak{p}_1\mathfrak{p}_2 = (p, \alpha - 2)(p, \alpha^7 - 2\alpha^5 + 4\alpha^4 - 7\alpha^3 - 6\alpha^2 - 8\alpha - 5)$$

  with $N(\mathfrak{p}_1) = p,\ N(\mathfrak{p}_2) = p^7$

- $p = 19$:

  $(p) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 = (p, \alpha - 6)(p, \alpha + 8)(p, \alpha^6 - 2\alpha^5 - 9\alpha^4 - 9\alpha^3 + 6\alpha^2 - 6\alpha + 6)$

  with $N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = p,\ N(\mathfrak{p}_3) = p^6$

- $p = 23$:

  $(p) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4 = (p, \alpha - 9)(p, \alpha + 1)(p, \alpha^3 - 9\alpha^2 + 5\alpha - 11)(p, \alpha^3 - 2\alpha^2 + 5\alpha + 4)$

  with $N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = p,\ N(\mathfrak{p}_3) = N(\mathfrak{p}_4) = p^3$

- $p = 29$:

  $(p) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4 = (p, \alpha - 11)(p, \alpha - 6)(p, \alpha - 1)(p, \alpha^5 - \alpha^4 + \alpha^3 - 4\alpha^2 + 13\alpha - 13)$

  with $N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = N(\mathfrak{p}_3) = p,\ N(\mathfrak{p}_4) = p^5$

- $p = 31$:

  $(p) = \mathfrak{p}_1\mathfrak{p}_2 = (p, \alpha^3 + 2\alpha^2 + 2\alpha - 12)(p, \alpha^5 + 10\alpha^4 - 7\alpha^3 + 11\alpha^2 - 10\alpha + 6)$

  with $N(\mathfrak{p}_1) = p^3,\ N(\mathfrak{p}_2) = p^5$

- $p = 37$:

  $g = e = 1,\ f = n = 8 \Rightarrow (p)$ *is inert*

- $p = 41$:

  $(p) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4\mathfrak{p}_5\mathfrak{p}_6 = (p, \alpha - 15)(p, \alpha - 13)(p, \alpha)(p, \alpha + 18)(p, \alpha^2 - 6\alpha - 19)(p, \alpha^2 - 3\alpha - 11)$

  with $N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = N(\mathfrak{p}_3) = N(\mathfrak{p}_4) = p,\ N(\mathfrak{p}_5) = N(\mathfrak{p}_6) = p^2$

- $p = 43$:

  $(p) = \mathfrak{p}_1\mathfrak{p}_2 = (p, \alpha + 9)(p, \alpha^7 + 15\alpha^6 + 9\alpha^5 - 21\alpha^4 + 19\alpha^3 - 7\alpha^2 + 16\alpha + 5)$

  with $N(\mathfrak{p}_1) = p,\ N(\mathfrak{p}_2) = p^7$

- $p = 47$:

  $g = e = 1,\ f = n = 8 \Rightarrow (p)$ *is inert*

- $p = 59$:

  $(p) = \mathfrak{p}_1\mathfrak{p}_2 = (p, \alpha^4 - 27\alpha^3 + 6\alpha^2 - 6\alpha - 26)(p, \alpha^4 + 8\alpha^3 - 11\alpha^2 - 11\alpha + 22)$

  with $N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = p^4$

- $p = 61$:

  $g = e = 1,\ f = n = 8 \Rightarrow (p)$ *is inert*

- $p = 67$:

  $(p) = \mathfrak{p}_1\mathfrak{p}_2 = (p, \alpha - 16)(p, \alpha^7 - 3\alpha^6 - 33\alpha^5 - 18\alpha^4 - 18\alpha^3 + 20\alpha^2 + 5\alpha - 10)$

  with $N(\mathfrak{p}_1) = p,\ N(\mathfrak{p}_2) = p^7$

- $p = 71$:

  $(p) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 = (p, \alpha - 24)(p, \alpha + 20)(p, \alpha^6 - 15\alpha^5 + 9\alpha^4 - 19\alpha^3 - 14\alpha^2 + 31\alpha + 31)$

  with $N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = p,\ N(\mathfrak{p}_3) = p^6$

- $p = 73$:

  $(p) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 = (p, \alpha + 16)(p, \alpha^3 - 30\alpha^2 + 15\alpha + 10)(p, \alpha^4 - 5\alpha^3 - 28\alpha^2 - 29)$

  with $N(\mathfrak{p}_1) = p,\ N(\mathfrak{p}_2) = p^3,\ N(\mathfrak{p}_3) = p^4$

- $p = 79$:

  $(p) = \mathfrak{p}_1\mathfrak{p}_2 = (p, \alpha^2 - 13 * \alpha + 38)(p, \alpha^6 - 6\alpha^5 - 22\alpha^4 - 5\alpha^3 - 17\alpha^2 + 33\alpha + 1)$

  with $N(\mathfrak{p}_1) = p^2,\ N(\mathfrak{p}_2) = p^6$

- $p = 83$:

  $(p) = \mathfrak{p}_1\mathfrak{p}_2 = (p, \alpha + 34)(p, \alpha^7 + 30\alpha^6 - 9\alpha^5 + 31\alpha^4 + 27\alpha^3 - 16\alpha^2 - T + 11)$

  with $N(\mathfrak{p}_1) = p,\ N(\mathfrak{p}_2) = p^7$

- $p = 89$:

  $(p) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 = (p, \alpha - 23)(p, \alpha^2 - 27\alpha + 25)(p, \alpha^5 + 31\alpha^4 + 29\alpha^3 + 40\alpha^2 + 25\alpha + 1)$

  with $N(\mathfrak{p}_1) = p,\ N(\mathfrak{p}_2) = p^2,\ N(\mathfrak{p}_3) = p^5$

- $p = 97$:

  $(p) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 = (p, \alpha + 13)(p, \alpha + 35)(p, \alpha^6 + 30\alpha^5 - 37\alpha^4 + 31\alpha^3 + 23\alpha^2 + 23\alpha + 24)$

  with $N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = p,\ N(\mathfrak{p}_3) = p^6$

Class number and class group

Let O_F a Dedekind domain, we define
$\mathrm{Frac}(F) = \{J \subseteq F : fractional\ ideal\}$ and $\mathrm{Pid}(F) = \{\alpha \in O_F\ \alpha \in F^*\}$
then the *class group* of O_F is $\mathrm{Cl}(O_F) = \mathrm{Frac}(F)/\,\mathrm{Pid}(F)$
The cardinality of $\mathrm{Cl}(O_F)$ is called the *class number* of O_F

```
? F.clgp.no
%37= 1
? F.clgp.cyc
%38 = []
? F.clgp.gen
%39 = []
```

The first tells us the class number, the second the cyclic decomposition of the class group, if it is cyclic, the last tells the generators.

Units group

The *units group* is the group of units of O_F denoted by O_F^*.
Let μ_F be the *group of roots of unity* in O_F^* and define $r = r_1 + r_2 - 1$
with r_1 the real embedding and r_2 the complex one then we can define
the *fundamental units* like the set $\{\varepsilon_1, \cdots \varepsilon_{r_1+r_2-1}\} \in O{*}_F$ such that

$$O_F^* = \{\varsigma\varepsilon_1^{n_1} \cdot \cdots \cdot \varepsilon_r^{r} \colon \varsigma \in \mu_F\ and\ n_i \in \mathbb{Z}\}$$

By default, the instruction `bnfinit` only computes fundamental units if they are not too large.

```
? F.fu
%40 = 0
```

In this case they are large so we can force the computation of fundamental units with `bnfinit(,1)`.

```
 ? K=bnfinit(f(T),1);
 ? lift(K.fu)
 %44 = [10729593627049*T^7 - 848798130141705/4*T^6 + 650912241487947/2*T^5
       - 523745865834891*T^4 + 402610435697903*T^3 - 2554298041914395/2*T^2
       + 451335268428027*T - 2301484415952723/4,
         14793552470607590532172781560971061*T^7
       - 123303125911108162748967935957827839 1/4*T^6
       + 74719699580596275442270827778468542 5*T^5
       - 92281552480650793480637759780851428 8*T^4
       + 161353007677360590432550289468582185/2*T^3
       + 17595754690590341025860057455265957 6*T^2
       - 35909960636454187793864072298980114 9*T
       + 683160277072341247293293941592234389/4,
       1287340257528726220177381749193753131160047638 6909/4*T^7
```

```
- 57725569221058218430279332882480330225990486763492*T^6
- 17334040495962044163475767219620779341896205096954*T^5
- 23574185234336547838445604555064213033869082340712*T^4
- 103900419461362098438767730322905809710587447196249/2*T^3
- 30318114870221144588867924974949286271614192778331 6*T^2
- 177871267810789438048921587458231122425655524917326 1/4*T
- 341946677862098392944903039045642316750211336142193/2,
  41863376888563965708258 85/4*T^7 - 2110613857859839154564729 7*T^6
 + 3794870575512482081102965 5*T^5 - 2709134775314922170363068 1*T^4
 + 2532366434179285302432446 5/2*T^3 - 7952266584778674964271755 8*T^2
 + 2367796916371384288901933 83/4*T + 2265796474999510007195999 01/2].
```

Minkowski constant

The *Minkowski constant* is

$$M_F = \frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^{r_2} \cdot |\Delta_F|^{1/2}$$

where r_2 is the number of complex embedding.

```
? [r1,r2]=F.sign
%45 = [2, 3]
? M=(8!/8^8) *(4/ Pi)^r2 * abs(Delta)^(1/2)
%46 = 1880239876.1374187359639308703476680300
```

Then $M_F = 1880239876.1374187359639308703476680300$.

Regulator

Let $\varphi_1, \cdots, \varphi_{r_1+r_2} : F \hookrightarrow \mathbb{C}$ then the *regulator* of F is defined like

$$R_F = |\det(\log \parallel \varphi_j(\varepsilon_i) \parallel)_{i,j}|$$

$\varepsilon_1, \cdots \varepsilon_r$ are a set of fundamental units and $\varphi_j \in \{\varphi_1, \cdots, \varphi_{r_1+r_2}\}$ except one.

```
? F.reg
%47 = 580210756.69648105199322127176395750871
```

Then $R_F = 580210756.69648105199322127176395750871$.