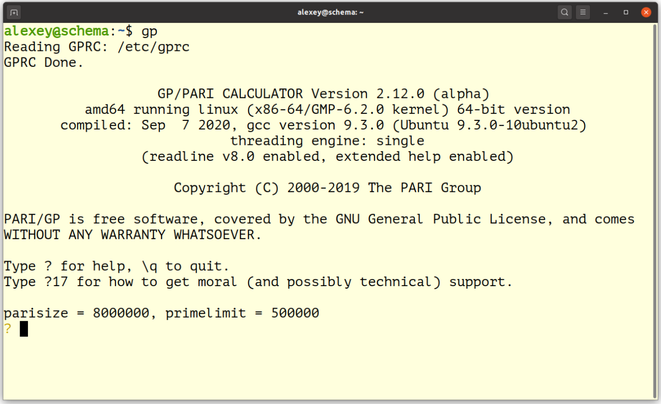
Teoría de números algebraicos en PARI/GP

Parte I: campos de números, anillos de enteros

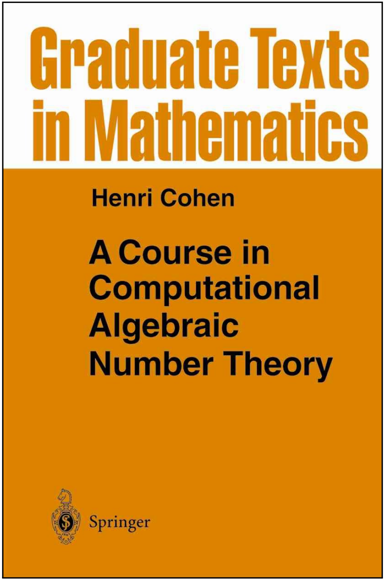
23/09/2020

PARI/GP

- Sistema de álgebra computacional
- Enfoque en la teoría de números
- `https://pari.math.u-bordeaux.fr/`



¿Cómo funciona?



Comandos útiles

- [→] — completar la palabra
- `\l "log.txt"` — guardar la sesión en `log.txt`
- Otra vez `\l` — dejar de hacerlo
- ?xxxxx — ayuda sobre xxxxx
  ??xxxxx — ayuda detallada
- `\quit` — salir del programa

```
? ?idealprimedec
idealprimedec(nf,p,{f=0}): prime ideal
decomposition of the prime number p in the
number field nf as a vector of prime ideals.
If f is present and non-zero, restrict the
result to primes of residue degree <= f.
```

Resultado de cálculo

- `%` — resultado del cálculo anterior

```
? 2^2
%1 = 4
? %^2
%2 = 16
? %^2
%3 = 256
? %1 + %2
%4 = 20
```

Cuando algo va mal...

```
? mcd(2,3)
  ***   at top-level: mcd(2,3)
  ***                 ^--------
  ***   not a function in function call
  ***   Break loop: type 'break' to go back
  ***   to GP prompt
break> break

? gcd(2,3)
% = 1
```

Polinomios

Irreducibilidad

```
? polisirreducible(x^3 - 3*x + 1)
% = 1
? polisirreducible(x^4 + x^3 + x^2 + x + 1)
% = 1
? polisirreducible(x^3 + x^2 + x + 1)
% = 0
```

Factorización

```
? factor (x^8-1)
% =
[  x - 1 1]
[  x + 1 1]
[x^2 + 1 1]
[x^4 + 1 1]

? factor (x^3 + x^2 - x - 1)
% =
[x - 1 1]
[x + 1 2]
```

Polinomios mód p

- f*`Mod(1,p)` — reducción mód p para $f \in \mathbb{Z}_{(p)}[x]$

```
? factor (polcyclo(8)*Mod(1,2))
% =
[Mod(1, 2)*x + Mod(1, 2) 4]

? factor (polcyclo(8)*Mod(1,3))
% =
[Mod(1, 3)*x^2 + Mod(1, 3)*x + Mod(2, 3) 1]
[Mod(1, 3)*x^2 + Mod(2, 3)*x + Mod(2, 3) 1]

? factor (polcyclo(8)*Mod(1,5))
% =
[Mod(1, 5)*x^2 + Mod(2, 5) 1]
[Mod(1, 5)*x^2 + Mod(3, 5) 1]
```

Discriminante

- $\Delta(f) =$ `poldisc`(f)

```
? poldisc (polcyclo(7))
% = -16807
? factor(%)
% =
[-1 1]

[ 7 5]
```

Campos de números

nfinit

$f \in \mathbb{Q}[x]$ irreducible.
Especificar $K = \mathbb{Q}[x]/(f)$, calcular invariantes básicos:

K`=nfinit(`f`);`

* `nf` = *number field*.

Algunos invariantes:

- K`.pol` — polinomio f
- K`.zk` — $\mathbb{Z}$-base $\mathcal{O}_K$ en términos de la $\mathbb{Q}$-base $1, x, x^2, \ldots, x^{n-1} \pmod{f}$
- K`.disc` — discriminante Δ_K
- K`.sign` — signatura $[r_1, r_2]$

Ejemplo: $\mathbb{Q}(\sqrt[3]{19})$

```
? K = nfinit(x^3-19);
? K.sign
% = [1, 1]
? K.disc
% = -1083
? factor (%)
% =
[-1 1]
[ 3 1]
[19 2]

? K.zk
% = [1, 1/3*x^2 + 1/3*x + 1/3, x]
```

$$\mathcal{O}_K = \mathbb{Z} \oplus \frac{1}{3}(\alpha^2 + \alpha + 1)\mathbb{Z} \oplus \alpha\mathbb{Z}.$$

Para qué sirve punto y coma

```
alexey@schema: ~

Type ? for help, \q to quit.
Type ?17 for how to get moral (and possibly technical) support.

parisize = 8000000, primelimit = 500000
? K = nfinit(x^3-19)
%1 = [x^3 - 19, [1, 1], -1083, 3, [[1, 3.5962563358746461731364126245315359494,
2.6684016487219448673396273719708303351; 1, -1.298128167937323086568206312265767
9747 - 1.2851718005977173028291930464034941571*I, -1.33420082436097243366981368
59854151676 + 2.3109036152934841170271125629077024990*I], [1, 3.5962563358746461
731364126245315359494, 2.6684016487219448673396273719708303351; 1, -2.58329996853
504038939739935866926213 18, 0.97670279093251168335729887692228733147; 1, -0.0129
5636733960578373901326586227381763 7, -3.6451044396544565506969262488931176666],
[1, 4, 3; 1, -3, 1; 1, 0, -4], [3, 1, 0; 1, 13, 19; 0, 19, 0], [57, 0, 20; 0, 19
, 16; 0, 0, 1], [19, 0, -1; 0, 0, 3; -1, 3, -2], [57, [-19, 6, -1; 0, -18, 3; 1,
 0, -20]], [3, 19]], [2.6684016487219448673396273719708303351, -1.33420082436097
2433669813685985415167 6 + 2.3109036152934841170271125629077024990*I], [3, x^2 +
x + 1, 3*x], [1, 0, -1; 0, 0, 3; 0, 1, -1], [1, 0, 0, 0, 4, 6, 0, 6, -1; 0, 1, 0
, 1, 1, 1, 0, 1, 3; 0, 0, 1, 0, 2, 0, 1, 0, -1]]
? 
```

Isomorfismo

- `nfisisom(`K`,`L`)` — $K \overset{?}{\cong} L$
- K y L: polinomios irreducibles o estructuras `nfinit`

```
? nfisisom(x^4 + 2*x^2 + 4*x + 2, polcyclo(8))
% = [x^2 - x, x^2 + x, -x^3 - x^2, x^3 - x^2]

? nfisisom(x^4 + 2, polcyclo(8))
% = 0
```

Uno de los isomorfismos:

$$\mathbb{Q}[\alpha]/(\alpha^4 + 2\alpha^2 + 4\alpha + 2) \cong \mathbb{Q}(\zeta_8),$$
$$\alpha \mapsto \zeta_8^2 - \zeta_8.$$

Inclusión

- `nfisincl(`K`,`L`)` — $K \overset{?}{\subseteq} L$
- K y L: polinomios irreducibles o estructuras `nfinit`

```
? nfisincl(x^2-7, polcyclo(7))
% = 0
? nfisincl(x^2+7, polcyclo(7))
% = [-2*x^4 - 2*x^2 - 2*x - 1, 2*x^4 + 2*x^2 + 2*x + 1]
```

Significado: $\mathbb{Q}(\sqrt{7}) \not\subset \mathbb{Q}(\zeta_7)$, $\mathbb{Q}(\sqrt{-7}) \subset \mathbb{Q}(\zeta_7)$.

* Más adelante: teoría de Galois

polredbest

- `polredbest(`f`)`: polinomio g tal que $\mathbb{Q}[x]/(f) \cong \mathbb{Q}[x]/(g)$
- Coeficientes de g «pequeños»

Ejemplo: $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$

- $K = \mathbb{Q}(\alpha)$, $\alpha = \sqrt{2} + \sqrt{3}$
- $f_{\mathbb{Q}}^{\alpha} = x^4 - 10x^2 + 1$

```
? f = x^4 - 10*x^2 + 1;
? poldisc(f)
% = 147456

? K = nfinit(f);
? K.disc
% = 2304

? sqrtint(poldisc(f)/K.disc)
% = 8
```

$$\mathbb{Z}[\alpha] = 2^{14} \cdot 3^2, \quad \Delta_K = 2^8 \cdot 3^2, \quad [\mathcal{O}_K : \mathbb{Z}[\alpha]] = 8.$$

¡polredbest!

```
? g = polredbest(f)
% = x^4 - 4*x^2 + 1
? poldisc(g)
% = 2304
? % == K.disc
% = 1
```

- Encontramos $\mathbb{Z}[\beta]$, $\beta^4 - 4\beta^2 + 1 = 0$
- Resulta que $\mathcal{O}_K = \mathbb{Z}[\beta]$

Otro ejemplo: $K = \mathbb{Q}(\sqrt[3]{19})$

```
? f = x^3-19;
? K = nfinit(f);
? sqrtint(poldisc(f)/K.disc)
% = 3
? polredbest(f,1)   /* expr. raíz de f mód g */
% = [x^3 - x^2 - 6*x - 12,
     Mod(1/2*x^2 - 1/2*x - 2, x^3 - x^2 - 6*x - 12)]
? sqrtint(poldisc(%[1])/K.disc)
% = 2
```

- $[\mathcal{O}_K : \mathbb{Z}[\alpha]] = 3$
- $\mathbb{Z}[\beta] \subset \mathcal{O}_K$, $\beta^3 - \beta^2 - 6\beta - 12 = 0$
- $[\mathcal{O}_K : \mathbb{Z}[\beta]] = 2$
- $\alpha = \frac{1}{2}\beta^2 - \frac{1}{2}\beta - 2$

Elementos de $K/\mathbb{Q}$

En la $\mathbb{Q}$-base $1, x, x^2, \ldots, x^{n-1}$

Elemento $\alpha \in \mathbb{Q}[x]/(f) \longleftrightarrow$ polinomio $g \in \mathbb{Q}[x]$ módulo f

```
? a = Mod(x^4 - x^3 - x^2 + x, polcyclo(5))
% = Mod(-2*x^3 - 2*x^2 - 1, x^4 + x^3 + x^2 + x + 1)
? a^2
% = Mod(5, x^4 + x^3 + x^2 + x + 1)
```

En la $\mathbb{Z}$-base de $\mathcal{O}_K$

- K`.zk`: $\mathbb{Z}$-base de $\mathcal{O}_K$ calculada por `nfinit`
- $\mathcal{O}_K = \alpha_1\mathbb{Z} \oplus \cdots \oplus \alpha_n\mathbb{Z}$
- $\alpha \in K \longleftrightarrow \mathbb{Q}$-vector `[`$a_1$`, ..., `$a_n$`]~`
- $\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n$
- `[`a_1`, ..., `a_n`]~` — vector-columna

Recordatorio: si $K = \mathbb{Q}(\alpha)$, no necesariamente $\mathcal{O}_K = \mathbb{Z}[\alpha]$

nfalgtobasis y nfbasistoalg

- `nfalgtobasis(`K`,`$g(x)$`)`
- `nfbasistoalg(`K`,[`a_1`, …, `a_n`]~)`

```
? K = nfinit(x^2-5);
? K.zk
% = [1, 1/2*x - 1/2]
? nfalgtobasis(K, 2+x)
% = [3, 2]~
? K.zk * %
% = x + 2
? nfbasistoalg(K,[3,2]~)
% = Mod(x + 2, x^2 - 5)
```

Aritmética básica

- `nfeltadd(`K`,`α`,`β`)` = $\alpha + \beta$
- `nfeltmul(`K`,`α`,`β`)` = $\alpha\beta$
- `nfeltpow(`K`,`α`,`n`)` = α^n
- `nfeltdiv(`K`,`α`,`β`)` = α/β
- Operadores habituales +, -, *, /, ... para `Mod(`$g(x)$`,`f`)`

```
? K = nfinit(x^2-2);
? for (n=1,8, print(nfeltpow(K,1+x,n)))
[1, 1]~
[3, 2]~
[7, 5]~
[17, 12]~
[41, 29]~
[99, 70]~
[239, 169]~
[577, 408]~
```

Aritmética básica

```
? for (n=1,8, print(Mod(1+x,x^2-2)^n))
Mod(x + 1, x^2 - 2)
Mod(2*x + 3, x^2 - 2)
Mod(5*x + 7, x^2 - 2)
Mod(12*x + 17, x^2 - 2)
Mod(29*x + 41, x^2 - 2)
Mod(70*x + 99, x^2 - 2)
Mod(169*x + 239, x^2 - 2)
Mod(408*x + 577, x^2 - 2)
```

Normas y trazas

- `nfeltnorm(`K`,`α`)` o `norm(Mod(`g`,`f`))` — norma
- `nfelttrace(`K`,`α`)` o `trace(Mod(`g`,`f`))` — traza
- `charpoly(Mod(`g`,`f`))` — polinomio característico
- `minpoly(Mod(`g`,`f`))` — polinomio mínimo

Normas y trazas

```
? K = nfinit(polcyclo(7));
? nfelttrace(K,x)
% = -1
? nfeltnorm(K, 1-x)
% = 7
? charpoly (Mod (x, K.pol))
% = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1
? charpoly (Mod (1-x, K.pol))
% = x^6 - 7*x^5 + 21*x^4 - 35*x^3 + 35*x^2 - 21*x + 7

? charpoly(Mod (x + x^-1, K.pol))
% = x^6 + 2*x^5 - 3*x^4 - 6*x^3 + 2*x^2 + 4*x + 1
? minpoly(Mod (x + x^-1, K.pol))
% = x^3 + x^2 - 2*x - 1
```

Extensiones $L/K/\mathbb{Q}$ (brevemente)

Ejemplo: $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$

```
? K = nfinit(t^3-2);
? L = rnfinit(K, polcyclo(3));
? L.polabs
% = x^6 + 3*x^5 + 6*x^4 + 11*x^3 + 12*x^2 - 3*x + 1
? rnfeltreltoabs(L,x+t)
% = Mod(-4/9*x^5 - 14/9*x^4 - 28/9*x^3 - 52/9*x^2
                                    - 65/9*x - 4/9,
        x^6 + 3*x^5 + 6*x^4 + 11*x^3 + 12*x^2
                                           - 3*x + 1)
? minpoly(%)
% = x^6 + 3*x^5 + 6*x^4 + 3*x^3 + 9*x + 9
? nfisisom(%, L.polabs)
% = [-x - 1, .....]
```

rnf = relative number field

- K `= nfinit(f(t));`
- L `= rnfinit(`K`,g(x));`
- L`.polabs` = polinomio $h(x)$ tal que $L \cong \mathbb{Q}[x]/(h)$
- Calculamos el polinomio mínimo de $\sqrt[3]{2} + \zeta_3$:

$$x^6 + 3x^5 + 6x^4 + 3x^3 + 9x + 9.$$

Invariantes relativos

```
? L.zk
% = [[1, x-1], [1, [1,0,1/3; 0,1,2/3; 0,0,1/3]]]
? L.disc
% = [[3, 1, 2; 0, 1, 0; 0, 0, 1], -3]
? nfinit(L).disc
% = -34992

? factor(%)
% =
[-1 1]
[ 2 4]
[ 3 7]
```

Próxima sesión: cálculos con $\mathcal{O}_K$-ideales

¡Gracias por su atención!