Théorie algébrique des nombres avancée

B. Allombert et A. Page

IMB
CNRS/Université de Bordeaux/INRIA

15/06/2023

polgalois

Nous pouvons déterminer le groupe de Galois de la clôture Galoisienne d'un corps de nombres, comme groupe abstrait. Restreint aux degrés ≤ 7, ou degrés ≤ 11 avec le paquet optionnel `galdata`.

```
? default(new_galois_format,1);
? P1 = x^4-5;
? polgalois(P1)
%3 = [8, -1, 3, "D(4)"]
```

Interprétation : le groupe de Galois est d'ordre 8, n'est pas contenu dans le groupe alterné A_4 (signature -1) et est isomorphe à D_4.

polgalois

```
? P2 = x^4-x^3-7*x^2+2*x+9;
? polgalois(P2)
%5 = [12, 1, 4, "A4"]
```

Le groupe de Galois est d'ordre 12 et est de signature 1, et isomorphe à A_4.

```
? P3 = x^4-x^3-3*x^2+x-1;
? polgalois(P3)
%7 = [24, -1, 5, "S4"]
```

Le groupe de Galois est d'ordre 24 et de signature -1, et isomorphe à S_4.

nflist

`nflist` donne la listes des corps de nombres ayant un groupe de Galois fixé et un discriminant donné.

```
? nflist([4,3],2000)
%8 = [x^4-5]
? nflist([4,4],[1,10000])
%9 = [x^4-2*x^3+2*x^2+2,x^4-x^3+5*x^2-4*x+3,x^4-2*x
? nflist([4,5],[1,5000],0)
%10 = [x^4-26*x^2-8*x+1,x^4-454*x^2-8*x+51389,x^4-1
```

nfsplitting

Nous pouvons déterminer un polynôme définissant le corps de décomposition d'un polynôme, c'est à dire le plus petit corps où ce polynôme est totalement décomposé.

```
? Q1 = nfsplitting(P1)
%11 = x^8 + 70*x^4 + 15625
? Q2 = nfsplitting(P2)
%12 = x^12 - 59*x^10 + 1269*x^8 - 12231*x^6
%  + 51997*x^4 - 79707*x^2 + 26569
```

Cela correspond aussi a un polynôme définissant la clôture galoisienne du corps défini par une racine du polynôme.

nfsplitting

`nfsplitting` renvoie souvent des polynômes avec de gros coefficients.

```
? Q3 = nfsplitting(P3)
%13 = x^24+12*x^23-66*x^22-1232*x^21+735*x^20
% +54012*x^19+51764*x^18-1348092*x^17-2201841*x^16
% +21708244*x^15+41344014*x^14-241723272*x^13
% -454688929*x^12+1972336584*x^11+3130578366*x^10
% -12348327032*x^9-13356023346*x^8+59757161004*x^7
% +32173517686*x^6-20454093549 6*x^5-11176476888*x^4
% +4330891936 68*x^3-155456858376*x^2-422808875280*x
% +320938557273
```

polredbest

Nous pouvons utiliser `polredbest` pour obtenir un polynôme plus simple définissant le même corps de nombres :

```
? Q3 = polredbest(Q3)
%14 = x^24-6*x^23+18*x^22-38*x^21+60*x^20-54*x^19
% -13*x^18+126*x^17-228*x^16+220*x^15+24*x^14
% -396*x^13+521*x^12-216*x^11-48*x^10-32*x^9-66*x^8
% +666*x^7-1013*x^6+348*x^5+510*x^4-654*x^3+234*x^2
% +36*x+9
```

galoisinit

Nous pouvons utiliser `galoisinit` pour calculer le groupe des automorphismes d'un corps de nombre qui est galoisien sur $\mathbb{Q}$, sous certaines conditions.

```
? gal = galoisinit(Q3);
? gal.gen
%16 = [Vecsmall([19,11,17,14,13,12,10,9,8,7,2,6,5,
% 4,23,22,3,21,1,24,18,16,15,20]),Vecsmall([14,10,5
% 19,3,24,11,16,22,2,7,20,17,1,21,8,13,23,4,12,15,9
% 18,6]),Vecsmall([5,15,6,13,20,19,23,7,11,18,21,4,
% 12,17,16,2,24,22,3,1,9,10,8,14]),Vecsmall([2,1,9,
% 10,16,21,14,17,3,4,19,18,22,7,20,5,8,12,11,15,6,
% 13,24,23])]
```

galoisinit

La composante `orders` indique l'ordre des facteurs de composition du groupe et leur produit est l'ordre du groupe.

```
? ord = gal.orders
%17 = Vecsmall([2, 2, 3, 2])
? prod(i=1,#ord,ord[i])
%18 = 24
```

La fonction `galoisidentify` permet d'obtenir le numéro GAP4 du groupe et son nom.

```
? galoisidentify(gal)
%19 = [24, 12]
? galoisgetname(24,12)
%20 = "S4"
```

Théorie de Galois effective

`galoissubgroups` permet d'obtenir la liste des sous-groupes d'un groupe.

```
? L = galoissubgroups(gal);
? #L
%22 = 30
```

Nous pouvons calculer les corps fixes correspondants avec `galoisfixedfield`.

```
? R1 = galoisfixedfield(gal,L[25])[1];
? polgalois(R1)
%24 = [24, 1, 1, "S_4(6d) = [2^2]S(3)"]
? R2 = galoisfixedfield(gal,L[28])[1];
? polgalois(R2)
%26 = [24, -1, 1, "S_4(6c) = 1/2[2^3]S(3)"]
```

Groupes de ramification

Nous pouvons calculer des groupes de ramification. Trouvons des idéaux ramifiés :

```
? nf = nfinit(Q3);
? factor(nf.disc)
%23 =
%[ 3 28]
%[11 16]
```

Les premiers ramifiés sont 3 et 11.

```
? dec3 = idealprimedec(nf,3);
? pr3 = dec3[1];
? [#dec3, pr3.f, pr3.e]
%31 = [4, 1, 6]
```

Il y a 4 idéaux premiers au-dessus de 3. Leur degré résiduel est 1 et leur indice de ramification est 6.

Groupes de ramification

Nous calculons la suite des groupes de ramification (en notation inférieure) avec `idealramgroups`.

```
? ram3 = idealramgroups(nf,gal,pr3);
? #ram3
%33 = 3
```

Il y a trois groupes de ramification non-trivaux à considérer.

```
? galoisidentify(ram3[1])
%34 = [6, 1]
? galoisisabelian(ram3[1])
%35 = 0
```

Le groupe de décomposition est d'ordre 6, et est isomorphe à S_3.

Groupes de ramification

```
? galoisidentify(ram3[2])
%36 = [6, 1]
```

Le groupe d'inertie est égal au groupe de décomposition (car le degré résiduel est 1).

```
? galoisidentify(ram3[3])
%37 = [3, 1]
```

La groupe d'inertie sauvage est le groupe cyclique C_3, et tout les groupes de ramification d'indice plus élevé sont triviaux.

Groupes de ramification

```
? dec11 = idealprimedec(nf,11);
? pr11 = dec11[1];
? [#dec11, pr11.f, pr11.e]
%40 = [4, 2, 3]
```

Il y a 4 idéaux premiers au-dessus de 11. Leur degré résiduel est 2 et leur indice de ramification est 3.

```
? ram11 = idealramgroups(nf,gal,pr11);
? #ram11
%42 = 2
```

Le groupe d'inertie sauvage est trivial (car 11 est premier avec l'ordre du groupe).

Groupes de ramification

```
? galoisidentify(ram11[1])
%43 = [6, 1]
? galoisidentify(ram11[2])
%44 = [3, 1]
```

Le groupe de décomposition est isomorphe à S_3 (car il est d'indice 4 dans le groupe de Galois), et le groupe d'inertie est C_3 (car il est d'indice 2 dans le groupe de décomposition).

Frobenius

Pour un nombre premier non ramifié, nous pouvons calculer l'élément de Frobenius avec `idealfrobenius`.

```
? dec2 = idealprimedec(nf,2);
? pr2 = dec2[1];
? [#dec2, pr2.f, pr2.e]
%47 = [6, 4, 1]
? frob2 = idealfrobenius(nf,gal,pr2);
? permorder(frob2)
%49 = 4
```

Nous vérifions que l'ordre de l'élément de Frobenius est égal au degré résiduel.

Kronecker–Weber explicite

Nous pouvons construire des extensions abéliennes de $\mathbb{Q}$ avec `polsubcyclo`.

```
? N = 7*13*19;
? L1 = polsubcyclo(N,3);
```

Cela donne la liste des sous-corps de degré 3 de $\mathbb{Q}(\zeta_N)$, où $N = 7 \cdot 13 \cdot 19$.

```
? L2 = [P | P <- L1, #factor(nfinit(P).disc)[,1]==3
%52 = [x^3+x^2-576*x+5123, x^3+x^2-576*x-64,
%       x^3+x^2-576*x-5251, x^3+x^2-576*x+1665]
```

Cela extrait les corps ramifiés au trois premiers 7, 13 et 19.

Kronecker–Weber

Nous calculons la structure et les générateurs de $(\mathbb{Z}/N\mathbb{Z})^\times$ avec `znstar`.

```
? G = znstar(N)
%53 = [1296, [36, 6, 6], [Mod(743, 1729),
%       Mod(248, 1729), Mod(407, 1729)]]
```

Nous construisons la matrice d'un sous-groupe spécifique d'indice 3 :

```
? H = mathnfmodid([1,0;-1,1;0,-1],3);
```

Kronecker–Weber explicite

Nous construisons l'extension abélienne correspondante.

```
? pol = galoissubcyclo(G,H)
%55 = x^3 + x^2 - 576*x - 64
? factor(nfinit(pol).disc)
%56 =
%[ 7, 2]
%[13, 2]
%[19, 2]
```

Nous vérifions la ramification du corps de nombre correspondant.

Corps de classe de Hilbert

Pour calculer le corps de classe de Hilbert, nous avons d'abord besoin de calculer le groupe de classe.

```
? bnf = bnfinit(a^2-a+50);
? bnf.cyc
%58 = [9]
```

Le groupe de classe est isomorphe à $\mathbb{Z}/9\mathbb{Z}$. Nous calculons un polynôme de définition relatif pour le corps de classe de Hilbert avec `bnrclassfield`.

```
? R = bnrclassfield(bnf)[1]
%59 = x^9 - 24*x^7 + (2*a - 1)*x^6 + 495*x^5
% + (-12*a + 6)*x^4 - 30*x^3 + (18*a - 9)*x^2
% + 18*x + (-2*a + 1)
```

Corps de classes de Hilbert

Inversement, pour une extension abélienne, nous pouvons retrouver son conducteur et son groupe de congruence avec `rnfconductor`.

```
? [cond,bnr,subg] = rnfconductor(bnf,R);
? cond
%61 = [[1, 0; 0, 1], []]
? subg
%62 = [9]
```

Le conducteur est trivial et le groupe de norme est trivial dans le groupe de classe.

Corps de classes de Hilbert

Nous pouvons demander un polynôme de définition absolu pour le corps de classe de Hilbert avec l'option `flag=2`.

```
? R2 = bnrclassfield(bnf,,2)
%63 = x^18 - 48*x^16 + 1566*x^14 - 23621*x^12
% + 244113*x^10 - 19818*x^8 - 3170*x^6
% + 17427*x^4 - 3258*x^2 + 199
```

Corps de classe de rayon

Nous pouvons aussi calculer des corps de classes de rayon.

```
? bnr = bnrinit(bnf,12);
? bnr.cyc
%65 = [72,2]
```

Nous pouvons déterminer le degré, la signature et le discriminant du corps de classe de rayon sans le calculer avec `bnrdisc`.

```
? [deg,r1,D] = bnrdisc(bnr);
? [deg,r1]
%67 = [288,0]
? D
%68 = 92477896[...538 digits...]84942237696
```

Ce corps est énorme !

Corps de classe de rayon

Pour des raisons d'éfficacité, `bnrclassfield` renvoie le corps de classe comme compositum de corps plus petits.

```
? bnrclassfield(bnr)
%69 = [x^2 - 3, x^8 + (-27*a+24)*x^6
% + (-294*a-3273)*x^4 + (-3*a-3852)*x^2 - 3,
% x^9 - 24*x^7 + (2*a-1)*x^6 + 495*x^5
% + (-12*a+6)*x^4 - 30*x^3 + (18*a-9)*x^2
% + 18*x + (-2*a+1)]
```

Nous pouvons obtenir un unique polynôme relatif avec `flag=1`.

```
? bnrclassfield(bnr,,1)
%70 = [... gros polynôme ...]
```

Corps de classe de rayon

Nous pouvons aussi calculer un sous-corps du corps de classe de rayon en précisant le sous-groupe de congruence.

```
? bnr = bnrinit(bnf,7);
? bnr.cyc
%72 = [54,3]
? bnrclassfield(bnr,3) \\3-sous-ext. élémentaire
%73 = [x^3 + 3*x + (14*a - 7),
% x^3 + (-1008*a - 651)*x + (-1103067*a - 8072813)]
```

Calcul sans le corps de définition

Calculer un polynôme de définition avec `bnrclassfield` peut être lent, donc il est toujours préférable de calculer les informations dont on a besoin sans construire le corps, si possible.

Nous avons déjà utilisé `bnrdisc` ; nus pouvons aussi calculer la loi de décomposition sans le corps explicite.

```
? pr41 = idealprimedec(bnf,41)[1];
? bnrisprincipal(bnr,pr41,0)
%75 = [0,0]~
```

Le Frobenius en $\mathfrak{p}_{41}$ est trivial : cet idéal est totalement décomposé dans l'extension de degré 162 (que nous n'avons pas calculé).

Corps de classe de rayon

Essayons un exemple ou l'idéal et le sous groupe sont donné sous forme HNF.

```
? bnr = bnrinit(bnf,[102709,43512;0,1]);
? bnr.cyc
%77 = [17010, 27]
? M = [9,3;0,1]; \\sous-groupe d'indice 9
? bnrclassfield(bnr,M)
%79 = [x^9 + (-297*a - 4470)*x^7 + ... ]
```

Rayons avec places infinies

Si le corps de base à des plongements réels, il est possible de spécifier le module à l'infini en donnant une liste de 0 et de 1 de longueur le nombre de plongements réels.

```
? bnf=bnfinit(a^2-217);
? bnf.cyc
%81 = []
? bnr=bnrinit(bnf,1);
? bnr.cyc
%83 = []
? bnrinit(bnf,[1,[1,1]]).cyc
%84 = [2]
```

Le corps $\mathbb{Q}(\sqrt{217})$ a un nombre de classe au sens restreint égal à 2.

Formule analytique du nombre de classes

```
? bnf = bnfinit(a^2+23);
? bnr = bnrinit(bnf,1);
? bnr.cyc
%87 = [3]
```

Nous calculons la valeur en 0 de la dérivée de la fonction L de Hecke attaché au caractère non-trivial χ de notre groupe de classe avec `lfun`.

```
? r = lfun([bnr,[1]],0,1)
%88 = 0.28119957432296184651205076406787829979+0.E-
```

Formule analytique du nombre de classes

Par la factorisation de la fonction zêta de Dedekind et la formule analytique du nombre de classe, nous pouvons trouver une unité du corps de classe.

```
? R2 = algdep(exp(r),3)
%89 = x^3-x-1
? nfdisc(R2)
%90 = -23
```

Nous avons reconstruit le corps de classe en utilisant la fonction L.

Méthodes transcendantes

Pour les corps quadratiques, les corps de classes de rayons peuvent être calculés par des méthodes transcendantes avec `quadhilbert` et `quadray`.

```
? quadhilbert(-31)
%91 = x^3 + x^2 + 1
? lift(quadray(13,7))
%92 = x^3 + (-7*y - 11)*x^2 + (56*y + 73)*x
% + (-91*y - 118)
```

Avec `bnrclassfield`, le temps de calcul dépend surtout du degré de l'extension et peu du conducteur, alors que pour les méthodes transcendantes, c'est l'inverse.

Action galoisienne sur le groupe des classes

Nous pouvons calculer l'action du groupe de Galois sur le groupe de classe de rayon avec `bnrgaloismatrix`, c'est à dire l'action sur le groupe de Galois relatif sans calculer explicitement l'extension abélienne.

```
? bnf = bnfinit(x^2+2*3*5*7*11);
? bnf.cyc
%94 = [4, 2, 2, 2]
? bnr = bnrinit(bnf,1,1);
? gal = galoisinit(bnf);
? m = bnrgaloismatrix(bnr,gal)[1]
%97 =
%[3 0 0 0]
%[0 1 0 0]
%[0 0 1 0]
%[0 0 0 1]
```

Classes de Steinitz

Nous considérons l'anneau d'entier du corps de classe de Hilbert de $\mathbb{Q}(\sqrt{-47})$ comme $\mathbb{Z}[\frac{1+\sqrt{-47}}{2}]$ module de dimension 5.

```
? bnf=bnfinit(a^2+47);
? bnf.cyc
%99 = [5]
? P=quadhilbert(-47)
%100 = x^5+2*x^4+2*x^3+x^2-1
? [A,J] = rnfpseudobasis(bnf,P);
? A
%102 = [1,0,0,8,13;0,1,0,-3,9;0,0,1,16,23;0,0,0,1,0
? J
%103 = [1,1,1,[1,24/47;0,1/47],[1,24/47;0,1/47]]
```

Classes de Steinitz

```
? [As,Js] = rnfsteinitz(bnf,[A,J]);
? Js
%105 = [1,1,1,1,[1,0;0,1]]
? bnfisprincipal(bnf, Js[#Js])
%106 = [[0]~,[1,0]~]
```

La classe de Steinitz est triviale.

Questions ?

À vos claviers !