Advanced algebraic number theory

A. Page

IMB
INRIA/Université de Bordeaux

16/04/2024

Plan

Galois theory

Ramification theory

Class field theory

Galois theory

Reminder

Field extension $K/F \rightsquigarrow$ automorphism group $\mathrm{Aut}(K/F)$

K/F is Galois if $|\mathrm{Aut}(K/F)| = [K : F]$.
Then: **Galois group** $\mathrm{Gal}(K/F) = \mathrm{Aut}(K/F)$.

$$\begin{array}{rcl} \text{subfields } F \subset L \subset K & \longleftrightarrow & \text{subgroups } H \subset \mathrm{Gal}(K/F) \\ F & \longmapsto & \mathrm{Gal}(K/F) \\ K^H & \longmapsfrom & H \end{array}$$

$P \in F[X]$ irreducible, let $K = F(\alpha)$ with $P(\alpha) = 0$; let $n = \deg P$.

Splitting field $\tilde{K}$ of $P =$ **Galois closure** $\tilde{K}/F$ of K/F.
Galois group $\mathrm{Gal}(\tilde{K}/F)$ acts on the n roots of P in $\tilde{K}$.
$\Longrightarrow \mathrm{Gal}(\tilde{K}/F) \subset S_n$.

polgalois

We can compute the Galois group of the Galois closure of a number field, as a transitive permutation group. Restricted to degree ≤ 7, or degree ≤ 11 with the `galdata` optional package.

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

Interpretation: the Galois group has order 8, is not contained in the alternating group ("signature -1"), and is isomorphic to D_4.

polgalois

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

The Galois group has order 12 and signature 1, and is isomorphic to A_4.

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

The Galois group has order 24 and signature -1, and is isomorphic to S_4.

nfsplitting

We can compute a polynomial defining the splitting field of the input polynomial, that is, the smallest field over which the input polynomial is a product of linear factors.

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

This is the same as a defining polynomial for the Galois closure of the number field generated by one root of the input polynomial.

nfsplitting

The polynomial output by nfsplitting can be large.

```
Q3 = nfsplitting(P3)
% = 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^6-204540935496*x^5-111764768888*x^4
 +433089193668*x^3-155456858376*x^2-42280887528 0*x
 +320938557273
```

polredbest

We can use `polredbest` to compute a simpler polynomial defining the same number field.

```
Q3 = polredbest(Q3)
% = 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

We can use `galoisinit` to compute the automorphism group of a number field that is Galois over $\mathbb{Q}$, under certain condition on the group ("weakly super-solvable").

```
gal = galoisinit(Q3);
```

The `gen` component is a list of generators of the automorphism group, expressed as permutations of the roots.

```
gal.gen
% = [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

The `orders` components contains orders of composition factors of the group, and their product is the order of the group.

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

With the function `galoisidentify`, we can obtain the GAP4 index of the group, and with `galoisgetname` its name.

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

Effective Galois theory

`galoissubgroups` computes the list of all subgroups of a group.

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

Then we can compute fixed fields of various subgroups of the Galois group with `galoisfixedfield`.

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

galoissplittinginit

We can replace `nfsplitting` followed by `galoisinit` by `galoissplittinginit`, which is faster and has no restriction on the group.

```
P = x^5+20*x+16;
polgalois(P)
% = [60, 1, 4, "A5"]
```

The polynomial has Galois group A_5.

```
G = galoissplittinginit(P);
G.pol == nfsplitting(P)
% = 1
```

The splitting field is correct.

galoissplittinginit

We check that the Galois group is A_5.

```
galoisidentify(G)
% = [60, 5]
galoisgetname(60,5)
% = "A5"
```

Ramification theory

Reminder

K/F Galois extension of number fields of Galois group G.
$\mathfrak{P}$ prime ideal of $\mathbb{Z}_K$ above $\mathfrak{p}$.

$\mathfrak{P}$ unramified: **Frobenius element** $\mathrm{Frob}_{\mathfrak{P}} \in G$ with

$$\mathrm{Frob}_{\mathfrak{P}}(x) \equiv x^{N(\mathfrak{p})} \bmod \mathfrak{P}.$$

$\mathfrak{P}$ arbitrary: **decomposition group** $G_{\mathfrak{P}} \subset G$:

$$G_{\mathfrak{P}} = \{g \in G \mid g(\mathfrak{P}) = \mathfrak{P}\}.$$

and **ramification groups** $G_{\mathfrak{P}} = G_{\mathfrak{P},-1} \supset G_{\mathfrak{P},0} \supset G_{\mathfrak{P},1} \supset \dots$

$$G_{\mathfrak{P},i} = \{g \in G_{\mathfrak{P}} \mid gx \equiv x \bmod \mathfrak{P}^{i+1}\}.$$

Frobenius elements

At an unramified prime, we can compute the Frobenius element with `idealfrobenius`.

```
nf = nfinit(Q3);
dec2 = idealprimedec(nf,2);
pr2 = dec2[1];
[#dec2, pr2.f, pr2.e]
% = [6, 4, 1]
frob2 = idealfrobenius(nf,gal,pr2);
permorder(frob2)
% = 4
```

We check that the Frobenius element has order equal to the residue degree.

Ramification groups

We can compute ramification groups. Let's first find the ramified primes.

```
factor(nf.disc)
% =
[ 3 28]
[11 16]
```

The ramified primes are 3 and 11.

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

There are 4 prime ideals above 3. They have residue degree 1 and ramification index 6.

Ramification groups

We compute the sequence of ramification groups with `idealramgroups`.

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

There are three nontrivial ramification groups to consider.

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

The decomposition group has order 6, and is isomorphic to S_3.

Ramification groups

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

The inertia group equals the decomposition group (we already knew that since the residue degree is 1).

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

The wild inertia group is the cyclic group C_3, and all the higher ramification groups are trivial.

Ramification groups

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

There are 4 prime ideals above 11. They have residue degree 2 and ramification index 3.

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

The wild ramification group is trivial (which we knew since 11 is coprime to the group order).

Ramification groups

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

The decomposition group is isomorphic to S_3 (we already knew it had index 4 in the Galois group), and the inertia group is C_3 (we already knew it had index 2 in the decomposition group).

Class field theory

Reminder

A modulus $\mathfrak{m}$ of a number field K is a pair $(\mathfrak{m}_f, \mathfrak{m}_\infty)$ of a nonzero ideal $\mathfrak{m}_f$ and a set $\mathfrak{m}_\infty$ of real embeddings of K.

Define $U_K(\mathfrak{m}) \subset K^\times$: we have $\beta \in U_K(\mathfrak{m})$ iff

- $v_\mathfrak{p}(\beta - 1) \geq v_\mathfrak{p}(\mathfrak{m}_f)$ for all $\mathfrak{p} \mid \mathfrak{m}_f$, and
- $\sigma(\beta) > 0$ for all $\sigma \in \mathfrak{m}_\infty$.

The ray class group

$$\mathrm{Cl}_\mathfrak{m}(K) = \frac{(\text{nonzero ideals of } K \text{ coprime to } \mathfrak{m}_f)}{(\text{principal ideals } \beta\mathbb{Z}_K \text{ with } \beta \in U_K(\mathfrak{m}))}.$$

is a finite abelian group.

Reminder

For every modulus $\mathfrak{m}$, there exists a unique Abelian extension of K, the ray class field $K(\mathfrak{m})$, such that

$$\mathrm{Gal}(K(\mathfrak{m})/K) \cong \mathrm{Cl}_{\mathfrak{m}}(K) \text{ with } \mathrm{Frob}_{\mathfrak{P}} \mapsto \mathfrak{p} \text{ when } \mathfrak{p} \mid \mathfrak{P}.$$

The special case $K(1)$ is called the Hilbert class field.

Every Abelian extension L of K is contained in some $K(\mathfrak{m})$, and can therefore be described by a pair $(\mathfrak{m}, H)$ where $H \subset \mathrm{Cl}_{\mathfrak{m}}(K)$:

$$L = K(\mathfrak{m})^H \text{ and } \mathrm{Gal}(L/K) \cong \mathrm{Cl}_{\mathfrak{m}}(K)/H.$$

Hilbert class field

To compute a Hilbert class field, we first need to compute the class group.

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

The class group is isomorphic to $\mathbb{Z}/9\mathbb{Z}$. We compute a relative defining polynomial for the Hilbert class field with the function `bnrclassfield`.

```
R = bnrclassfield(bnf)[1]
% = 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)
```

Hilbert class field

Conversely, from an abelian extension, we can recover its corresponding class group with `rnfconductor`.

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

Here the conductor is trivial, and its norm group is trivial in the class group.

Hilbert class field

We can also ask for an absolute defining polynomial for the Hilbert class field with the optional `flag=2`.

```
R2 = bnrclassfield(bnf,,2)
% = 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
```

Ray class fields

We can also consider class fields with nontrivial conductor. The function `bnrinit` computes $\mathrm{Cl}_{\mathfrak{m}}(K)$.

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

We can compute in advance the absolute degree, signature and discriminant of the corresponding class field with `bnrdisc`.

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

This field is huge!

Ray class fields

For efficiency, we compute the class field as a compositum of several smaller fields.

```
bnrclassfield(bnr)
% = [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)]
```

We can force the computation of a single polynomial with `flag=1`.

```
bnrclassfield(bnr,,1)
% = [... huge polynomial ...]
```

Ray class fields

We can also compute a subfield of the ray class field by specifying a subgroup.

```
bnr = bnrinit(bnf,7)
bnr.cyc
% = [54,3]
bnrclassfield(bnr,3) \\elementary 3-subextension
% = [x^3 + 3*x + (14*a - 7),
 x^3 + (-1008*a - 651)*x + (-1103067*a - 8072813)]
```

Without the explicit field

Computing a defining polynomial with `bnrclassfield` can be time-consuming, so it is better to compute the relevant information without constructing the field, if possible.

We already saw the use of `bnrdisc`; we can also compute splitting information without the explicit field.

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

The Frobenius at $\mathfrak{p}_{41}$ is trivial: this prime splits completely in the degree 162 extension (which we did not compute).

Ray class fields

Let's do a full example with an HNF ideal and a subgroup given by a matrix.

```
bnr = bnrinit(bnf,[102709,43512;0,1]);
bnr.cyc
% = [17010, 27]
bnrclassfield(bnr,[9,3;0,1]) \\subgroup of index 9
% = [x^9 + (-297*a - 4470)*x^7 + ... ]
```

Modulus with infinite places

If the base field has real places, we can specify the modulus at infinity by providing a list of 0 or 1 of length the number of real embeddings.

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

The field $\mathbb{Q}(\sqrt{217})$ has narrow class number 2.

Galois action on the class group

We can compute the Galois action on ray class groups with `bnrgaloismatrix`, i.e. the Galois action on the relative Galois group, without the explicit abelian extension.

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

Questions ?

Have fun with GP !