PARI/GP day (02/06/2021)

[Tutorial]

The nflist( ) function

Karim Belabas

Number fields and discriminants (1/2)

We are interested in number fields $K = \mathbb{Q}[x]/(P)$ up to isomorphism. Given a monic irreducible polynomial $P \in \mathbb{Z}[x]$, the GP function `nfinit`, determines invariants of K such as

- Its signature (r_1, r_2), $r_1 + 2r_2 = [K : \mathbb{Q}] = \deg P$.
- Its absolute discriminant $\mathrm{disc}(K) \in \mathbb{Z}$, we shall write $\Delta_K := |\mathrm{disc}(K)|$.
- An integral basis, etc.

The integer $\mathrm{disc}(K)$ is congruent to 0 or $1 \pmod 4$, its sign is $(-1)^{r_2}$; it is divisible exactly by the primes that ramify in K.

Theorem. *There are finitely many number fields K (up to isomorphism) satisfying $\Delta_K < B$.*

The function mapping $P \in \mathbb{Z}[x]$ to the number field $K = \mathbb{Q}[x]/(P)$ is many-to-one; the GP function `polredabs` returns a canonical defining polynomial for K. This is the one given in the LMFDB for instance.

Number fields and discriminants (2/2)

Some interesting questions:

- what is the minimum value of Δ_K if $[K : \mathbb{Q}] = n$? or for a given signature (r_1, r_2) ?
- list all number fields K (up to isomorphism) such that $\Delta_K \in [A, B]$?
- as $B \to \infty$, how many number fields with $\Delta_K < B$ do we have ?

There are many variations where we fix the signature or restrict finite ramification, but Galois actions must now be taken into account as they severely restrict possibilities. This requires refining the question to a fixed Galois group for the Galois closure of $K/\mathbb{Q}$. If needed, we can then concatenate contributions of each group at the end.

Galois theory (1/3)

Let $K = \mathbb{Q}[x]/(P)$ be a number field of degree n and let $\hat{K}$ be the splitting field of P: $\hat{K}/\mathbb{Q}$ is the Galois closure of $K/\mathbb{Q}$. We write $G = \mathrm{Gal}(\hat{K}/\mathbb{Q}) = \mathrm{Gal}(P)$ for its Galois group. We can view G as a transitive subgroup of S_n (acting on the roots of P). Transitive subgroups of S_n up to conjugacy are classified for small n, including all $n \leqslant 47$:

- $n = 2$. We have 1 group (C_2)
- $n = 3$. We have 2 groups ($C_3 = A_3$, S_3)
- $n = 4$. We have 5 groups ($C_4, C_2 \times C_2, D_4, A_4, S_4$)
- $n = 5$. We have 5 groups ($C_5, D_5, F_5 = C_5 \rtimes C_4, A_5, S_5$)
- $n = 8/16/32$. We have 50 / 1,954 / 2,801,324 groups.

We write nTk for the k-th transitive subgroup of S_n in this classification. For fixed n, the group order increases with k; in particular, the last two elements in the series are A_n and S_n (and C_n comes first for $n \neq 32$).

Galois theory (2/3)

Some GP functions:

- `polgalois` (with `galdata` package) returns the isomorphism type of $\mathrm{Gal}(P)$ for $\deg P \leqslant 11$; we advise to set `new_galois_format` to 1.
- `nfsplitting` returns a defining polynomial $\hat{P}$ for the splitting field of P. It runs in polynomial time in the degree of $\hat{P}$. Of course, if $\deg P = n$ then $\deg \hat{P}$ may be as large as $n!$ but this works well if $\hat{K}$ is not too large, say a few seconds for $\hat{n} := [\hat{K} : \mathbb{Q}] < 1000$; a multiplicative upper bound for $\hat{n}$ helps a lot.
- for a *Galois* number field $K/\mathbb{Q}$, `galoisinit` returns the Galois group of K as a structure allowing basic Galois theory: conjugacy classes, character table, subgroups and fixed fields.
  (The group must be "weakly super solvable", i.e., have a normal series $H_0 = \{1\} \lhd H_1 \cdots \lhd H_m$ with cyclic factors H_{i+1}/H_i, such that

  $$G/H_m \simeq \{1\}, A_4, S_4, \text{ or } 9T9 = (C_3 \times C_3) \rtimes C_4 .$$

  Most small groups have this property.)
- shortcut: `galoissplittinginit` $\approx$ `nfsplitting` $+$ `galoisinit`.

Galois theory (3/3)

Conjecture (Inverse Galois problem). *Every transitive permutation group G occurs as a Galois group over $\mathbb{Q}$.*

Conjecture (Malle). *Let $n \geqslant 2$. For every transitive $G \hookrightarrow S_n$, there exist computable integers $a(G) > 0$, $b(G) \geqslant 0$ and some positive constant $c(G) > 0$ such that*

$$\#\left\{K/\simeq, \mathrm{Gal}(\hat{K}/\mathbb{Q}) = G, \Delta_K < B\right\} \sim c \cdot B^{1/a} (\log B)^b \ .$$

For many small groups G, the GP function `nflist` returns (defining polynomials for) number fields $K/\mathbb{Q}$ with given Galois group $\mathrm{Gal}(\hat{K}/\mathbb{Q}) = G$, possibly fixing signatures and/or some resolvent subfield of $\hat{K}$. In good cases, *all* fields with $\Delta_K \in [A, B]$.

It relies on the optional package `nflistdata` being installed.

Easy groups (1/4)

For this set of groups, the function can actually compute fields by increasing values of $\Delta_K \in [A, B]$ in a fixed interval. This includes

- all transitive permutation groups nTk in degree $n \leqslant 5$, except S_5; the group A_5 is only supported by a table allowing $\Delta_K < 10^{12}$ (database of 40,314 fields provided by John Jones and David Roberts);
- all cyclic C_ℓ, where ℓ is prime or $\ell \in \{4, 6, 9\}$;
- all dihedral D_ℓ, where ℓ prime or $\ell = 4$.

For $n > 3$, all results *depend on the truth of the GRH*, because of our use of class field theory and ultimately `bnfinit`.

Except for A_5 and $A_5(6)$, fields are computed on the fly. Up to subexponential factors in $\log B$, the complexity is linear in the output size, i.e. $O(B^{1/a(G)+\varepsilon})$ by Malle's conjecture, which is a theorem for many of those fields, for instance Abelian fields or S_n for $n \leqslant 5$. But it's not a theorem for A_4 or D_ℓ for $\ell \geqslant 5$ for instance, and the complexity is conjectural in these cases.

Easy groups (2/4)

`nflist(`$G, [A, B]$`)` or `nflist(`G, Δ_K`)`. The group $G = nTk$ is encoded by `[`n, k`]`. A character string is accepted if G has a simple natural name, such as `"C11"`, `"S3"` or `"A4"`.

```
?  vK = nflist("C3", [1, 10^10]);    \\ in O(B^{1/2+ε})
time = 23 ms.
?  # vK
%2 = 15851
?  vK[1]
%3 = x^3 - x^2 - 2*x + 1
?  nfdisc(%)
%4 = 49
?  nflist("C3", (7 * 13)^2)    \\ single discriminant
%5 = [x^3 - x^2 - 30*x + 64, x^3 - x^2 - 30*x - 27]
?  vD = apply(nfdisc, vK);    \\ sorted by increasing disc. in this case
time = 627 ms.
?  nflist("J4", 1)    \\ unsupported name
```

Easy groups (3/4)

One can add an optional r_2 to set a signature. Two sentinel values

- $r_2 = -1$: all signatures together (default);
- $r_2 = -2$: all signatures, given in a vector by increasing number of complex places.

```
?  vK = nflist("S3", [1, 10^6]); #vK    \\ in O(B^{1+ε})
%1 = 236858
?  v0 = nflist("S3", [1, 10^6], 0); #v0    \\ r2 = 0
%2 = 54441
?  v1 = nflist("S3", [1, 10^6], 1); #v1    \\ r2 = 1
%3 = 182417
?  v = nflist("S3", [1, 10^6], -2);
?  apply(length, v)
%5 = [54441, 182417]
```

Easy groups (4/4)

In the form `nflist(`G`)` one gets a few fields, about 10, of smallish discriminant (no guarantee they will have minimal discriminants).

A final optional argument allows to impose a resolvent field in the galois closure $\hat{K}$ (see `??nfresolvent` for definitions):

```
?  v = nflist("S3", [1,10^7], , x^2+23)    \\ impose Q(sqrt(-23)) ⊂ K̂
?  apply(P -> issquare(nfdisc(P) / -23), v)    \\ disc(K) = -23 f^2
%2 = [1, 1, ..., 1]
?  F = nflist("C3")[1]    \\ some cyclic cubic field F
?  nfdisc(F)
%4 = 49    \\ ... actually of smallest discriminant
?  v = nflist("A4", [1,10^7], , F)    \\ F ⊂ K̂
?  apply(P -> issquare(nfdisc(P) / 49), v)
%6 = [1, 1, ..., 1]
```

Tougher groups (1/4)

`nflist(`G`,'t)` returns a regular extension of K of $\mathbb{Q}(t)$ with group G, i.e. such that $\mathrm{Gal}(\hat{K}/\mathbb{Q}(t)) \simeq G$ and $K \cap \overline{\mathbb{Q}} = \mathbb{Q}$, given by a polynomial $P \in \mathbb{Z}[x,t]$. By Hilbert irreducibility, almost all specializations of $t \in \mathbb{Q}$ will give polynomials with group G over $\mathbb{Q}$. Discriminants of fields produced in this way are large (and the minimal discriminant is usually unknown for these groups).

This is implemented for all nTk, $n \leqslant 11$ with 5 exceptions $(9T14, 9T15, 11T2, 11T3, 11T4)$ and a few more groups in degree up to 15 (115 out of 477). The easy groups A_n and S_n are also available in all degrees.

This database was provided by Jürgen Klüners and Gunter Malle and requires the `nflistdata` package in degree $n \geqslant 8$.

Tougher groups (2/4)

```
?  Pt = nflist([8,1], 't)    \\ or "C8"
%1 = x^8 + (-4*t^4 - 4)*x^6 + (8*t^6 + 2*t^4 + 8*t^2 + 2)*x^4
+ (-4*t^8 - 4*t^6 - 4*t^4 - 4*t^2)*x^2 + (t^8 + t^4)

?  L = List();
?  { for (t = 1, 100,
        P = subst(Pt, 't, t); if (!polisirreducible(P), next);
        [n,s,k] = polgalois(P);
        if ([n,k] == [8,1], listput(~L, P)));
    #L; }
%2 = 100    \\ all our specializations happen to have the right group
?  L = Set(apply(polredabs, L)); #L    \\ remove duplicates
%3 = 100    \\ ...no duplicates
?  D = apply(nfdisc, L); [vecmin(D), vecmax(D)]
%4 = [2147483648, ⟨64 digits⟩]   \\ large discriminants
```

Tougher groups (3/4)

N.B. `polgalois` does not support $n > 11$. To check whether the specialization has the expected Galois group (within `PARI/GP`), we can check whether it is irreducible in $\mathbb{Q}[x]$ then use `nfsplitting` to check whether the Galois closure has the expected degree.

```
?  OK(Pt, t, deg) =
{ my(P = subst(Pt, 't, t));
  polisirreducible(P)
  && poldegree(nfsplitting(P, deg)) == deg;
}
?  Pt = nflist([12, 24], 't);    \\ C2 x S4
?  OK(Pt, 0, 48)
%3 = 0
?  OK(Pt, 3, 48);
%4 = 1
?  [OK(Pt, t, 48) | t <- [1..20]]
%5 = [0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1]
```

Tougher groups (4/4)

Not all signatures are afforded by this construction. The signature is constant between consecutive real roots of `poldisc(P)`, and *may* change when passing a root. Continuing the previous example in degree 12:

```
?  D = poldisc(Pt);
?  D /= gcd(D, D')    \\ make it squarefree
?  polrootsreal(D)
%3 = [-367.2, -71.5, -1.4, -7.E-6, -6.8E-6, 0, 6.4E-4, 1.0, 50.8]
?  polsturm(subst(Pt,'t,-1))    \\ returns r_1
%4 = 0
?  polsturm(subst(Pt,'t, 2))
%5 = 4
```

Checking rational values of t between the above roots, we see that the signature is $(0, 6)$ for $t < 1$ and $(4, 4)$ for $t > 1$.