# The tame-wild principle: a user's guide

John Jones

Arizona State University
Tempe, AZ

Joint work with David Roberts

3 June 2014

# Outline


1. Introduction
2. Statement
3. C.D.-groups
4. Examples

## Notation

Let

- $K =$ a number field
- $D_K$ its discriminant
- $K^{gal} =$ the normal closure for $K/\mathbb{Q}$
- $\mathrm{Gal}(K) = \mathrm{Aut}(K^{gal}/\mathbb{Q})$
- $\mathrm{rd}(K) = |D_K|^{1/[K:\mathbb{Q}]}$
- $\mathrm{grd}(K) = \mathrm{rd}(K^{gal})$ (Galois root discriminant)
- $G =$ a subgroup of $S_n$
- For a field $K_j$, we write abbreviate $D_j = D_{K_j}$

## Tabulating number fields: completeness

Given $n$ and $G$, the set

$$\{K \subseteq \mathbb{C} \mid [K : \mathbb{Q}] = n \text{ and } \mathrm{Gal}(K) = G \text{ and } \dots\}$$

is finite with any of the following restrictions

1. Given $B \in \mathbb{Z}$, $D_K = B$
2. Given a finite set of primes $S$, $\{p \,:\, p \mid D_K\} \subseteq S$
3. Given a bound $B \in \mathbb{Z}$, $|D_K| \leq B$ (equiv. $\mathrm{rd}(K) \leq B'$)
4. Given a bound $B \in \mathbb{R}$, $\mathrm{grd}(K) \leq B$

We will focus mainly on 3.

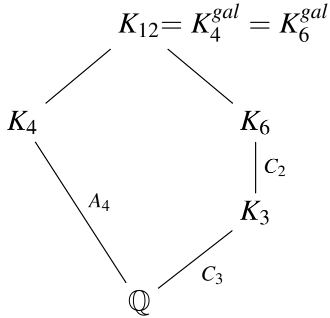
# Where complete tables of number fields come from

- “Hunter search” (bounds on coefficients of a defining polynomial)
- Class field theory
- Galois theory

# Where complete tables of number fields come from

- "Hunter search" (bounds on coefficients of a defining polynomial)
- Class field theory
- Galois theory

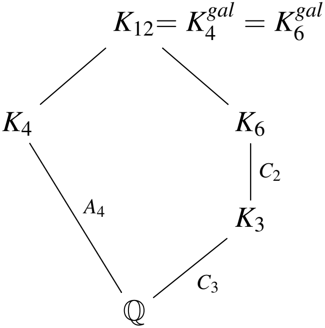
We may have to relate discriminants of one field to another, e.g.,



# Where complete tables of number fields come from

- “Hunter search” (bounds on coefficients of a defining polynomial)
- Class field theory
- Galois theory

We may have to relate discriminants of one field to another, e.g.,




$$D_3 \mid D_4$$

$$D_6 \mid D_4 D_3$$

# Principles

What is a *principle* in mathematics?

Extrapolating from the "local-global principle",

**Definition**

*A* principle *is a mathematical assertion which …*

## Principles

What is a *principle* in mathematics?

Extrapolating from the "local-global principle",

**Definition**

*A* principle *is a mathematical assertion which*

1. *reduces something hard to something which is apparently easier*

...

## Principles

What is a *principle* in mathematics?

Extrapolating from the "local-global principle",

**Definition**

*A* principle *is a mathematical assertion which*

1. *reduces something hard to something which is apparently easier*
2. *is true in some important cases*

. . .

## Principles

What is a *principle* in mathematics?

Extrapolating from the “local-global principle”,

**Definition**

*A* principle *is a mathematical assertion which*

1. *reduces something hard to something which is apparently easier*
2. *is true in some important cases*
3. *is false in general*

## Principles

What is a *principle* in mathematics?

Extrapolating from the "local-global principle",

### Definition

*A* principle *is a mathematical assertion which*

1. *reduces something hard to something which is apparently easier*
2. *is true in some important cases*
3. *is false in general*

Examples:

- The local-global principle

# Principles

What is a *principle* in mathematics?

Extrapolating from the “local-global principle”,

**Definition**

*A* principle *is a mathematical assertion which*

1. *reduces something hard to something which is apparently easier*
2. *is true in some important cases*
3. *is false in general*

Examples:

- The local-global principle
- The tame-wild principle

## Algebras and Permutation Representations

Base field $K$: a finite extension of $\mathbb{Q}$ or $\mathbb{Q}_p$

- Algebra: $A \cong \prod_{i=1}^{r} K_i$, each $K_i$ a field, $[K_i : K] < \infty$
- Equivalently: $A \cong K[x]/\langle f \rangle$
  (where $f$ is non-constant and separable, but not necessarily irreducible)
- $D_{A/K} = \prod D_{K_i/K}$

Given a Galois extension $M/K$, 1-1 correspondence (up to isomorphism):

- Algebras $A/K$ such that $A^{gal} \subseteq M$ gives a permutation representation $\rho : \mathrm{Gal}(M/K) \to S_n, \;\; n = [A : K]$
- Permutation representation $\rho : \mathrm{Gal}(M/K) \to S_n$ gives an algebra $A_\rho$

## Tame Extensions

- $A$ a degree $n$ algebra over $K$
- $\mathfrak{p}$ a maximal ideal of $\mathcal{O}_K$ s.t. $A$ is tame above $\mathfrak{p}$
- Discriminant exponent: $c_{\mathfrak{p}} = v_{\mathfrak{p}}(D_{A/K})$
- Tame implies inertia subgroup is cyclic: $I_{\mathfrak{p}} = \langle \sigma \rangle \leq S_n$
- cycle type of $\sigma$: $n_1, \ldots n_{\ell(\sigma)}$ gives

$$c_{\mathfrak{p}} = \sum_j (n_j - 1) = n - \ell(\sigma)$$

Given $\rho : G \to S_n$ and $\sigma \in G$, define formal tame discriminant exponent:

$$\mathfrak{c}_\rho(\sigma) = n - \ell(\rho(\sigma))$$

# Tame-wild principle

**Definition**

*Given* $\rho$ *and* $\nu$*, permutation representations of* $G$*, define*

$$\rho \precsim_t \nu \iff \forall g \in G, \quad \mathfrak{c}_\rho(g) \leq \mathfrak{c}_\nu(g).$$

**Definition**

*The* local (resp. global) tame-wild principle *holds for a group* $G$ *if for every Galois extension* $L/K$ *of local (resp. global) number fields with* $\mathrm{Gal}(L/K) = G$ *and pair of permutation representations* $\rho$ *and* $\nu$ *on* $G$*,*

$$\rho \precsim_t \nu \implies D_{A_\rho/K} \mid D_{A_\nu/K}.$$

## c.d.-groups

**Definition**

*A finite group is* completely decomposible *if every non-identity element is contained in exactly one maximal cyclic subgroup.*

Examples of c.d.-groups:

- cyclic groups $C_n$
- dihedral groups $D_n$
- groups of exponent $p$
- Frobenius groups of the form $F_p = C_p : C_{p-1}$
- $\mathrm{PGL}_2(q)$, $q$ odd
- Subgroup or quotient of a c.d.-group (so, e.g., $\mathrm{PSL}_2(q)$ with $q$ odd)

This includes $S_5 \cong \mathrm{PGL}_2(5)$ and $A_6 \cong \mathrm{PSL}_2(9)$

## c.d.-groups

**Definition**

*A finite group is* completely decomposible *if every non-identity element is contained in exactly one maximal cyclic subgroup.*

Examples of c.d.-groups:

- cyclic groups $C_n$
- dihedral groups $D_n$
- groups of exponent $p$
- Frobenius groups of the form $F_p = C_p : C_{p-1}$
- $\mathrm{PGL}_2(q)$, $q$ odd
- Subgroup or quotient of a c.d.-group (so, e.g., $\mathrm{PSL}_2(q)$ with $q$ odd)

This includes $S_5 \cong \mathrm{PGL}_2(5)$ and $A_6 \cong \mathrm{PSL}_2(9)$

**Proposition (J, Roberts)**

*If $G$ is a c.d.-group, then the local and global tame-wild principles hold for $G$.*

# First example

- $\mathrm{PGL}_2(5)$ and $\mathrm{PSL}_2(5)$ are naturally transitive subgroups of $S_6$
- $\mathrm{PGL}_2(5) \cong S_5$ and $\mathrm{PSL}_2(5) \cong A_5$

| Quintic cycle type of $g$ | $\mathfrak{c}_\rho(g)$ | Sextic cycle type of $g$ | $\mathfrak{c}_\nu(g)$ |
|---|---|---|---|
| 5 | 4 | 51 | 4 |
| 41 | 3 | 411 | 3 |
| 32 | 3 | 6 | 5 |
| 311 | 2 | 33 | 4 |
| 221 | 2 | 2211 | 2 |
| 2111 | 1 | 222 | 3 |
| 11111 | 0 | 111111 | 0 |

# First example

- $\mathrm{PGL}_2(5)$ and $\mathrm{PSL}_2(5)$ are naturally transitive subgroups of $S_6$
- $\mathrm{PGL}_2(5) \cong S_5$ and $\mathrm{PSL}_2(5) \cong A_5$

| Quintic cycle type of $g$ | $\mathfrak{c}_\rho(g)$ | Sextic cycle type of $g$ | $\mathfrak{c}_\nu(g)$ |
|---|---|---|---|
| 5 | 4 | 51 | 4 |
| 41 | 3 | 411 | 3 |
| 32 | 3 | 6 | 5 |
| 311 | 2 | 33 | 4 |
| 221 | 2 | 2211 | 2 |
| 2111 | 1 | 222 | 3 |
| 11111 | 0 | 111111 | 0 |

So $D_5 \mid D_6$

# First example

- $\mathrm{PGL}_2(5)$ and $\mathrm{PSL}_2(5)$ are naturally transitive subgroups of $S_6$
- $\mathrm{PGL}_2(5) \cong S_5$ and $\mathrm{PSL}_2(5) \cong A_5$

| Quintic cycle type of $g$ | $\mathfrak{c}_\rho(g)$ | Sextic cycle type of $g$ | $\mathfrak{c}_\nu(g)$ |
|---|---|---|---|
| 5 | 4 | 51 | 4 |
| 41 | 3 | 411 | 3 |
| 32 | 3 | 6 | 5 |
| 311 | 2 | 33 | 4 |
| 221 | 2 | 2211 | 2 |
| 2111 | 1 | 222 | 3 |
| 11111 | 0 | 111111 | 0 |

So $D_5 \mid D_6$ (and $D_6 \mid D_5^3$).

# First example

- $\mathrm{PGL}_2(5)$ and $\mathrm{PSL}_2(5)$ are naturally transitive subgroups of $S_6$
- $\mathrm{PGL}_2(5) \cong S_5$ and $\mathrm{PSL}_2(5) \cong A_5$

| Quintic cycle type of $g$ | $\mathfrak{c}_\rho(g)$ | Sextic cycle type of $g$ | $\mathfrak{c}_\nu(g)$ |
|---|---|---|---|
| 5 | 4 | 51 | 4 |
| 41 | 3 | 411 | 3 |
| 32 | 3 | 6 | 5 |
| 311 | 2 | 33 | 4 |
| 221 | 2 | 2211 | 2 |
| 2111 | 1 | 222 | 3 |
| 11111 | 0 | 111111 | 0 |

So $D_5 \mid D_6$ (and $D_6 \mid D_5^3$, and for $A_5$: $D_6 \mid D_5^2$).

# First example

- $PGL_2(5)$ and $PSL_2(5)$ are naturally transitive subgroups of $S_6$
- $PGL_2(5) \cong S_5$ and $PSL_2(5) \cong A_5$

| Quintic cycle type of $g$ | $\mathfrak{c}_\rho(g)$ | Sextic cycle type of $g$ | $\mathfrak{c}_\nu(g)$ |
|---|---|---|---|
| 5 | 4 | 51 | 4 |
| 41 | 3 | 411 | 3 |
| 32 | 3 | 6 | 5 |
| 311 | 2 | 33 | 4 |
| 221 | 2 | 2211 | 2 |
| 2111 | 1 | 222 | 3 |
| 11111 | 0 | 111111 | 0 |

So $D_5 \mid D_6$ (and $D_6 \mid D_5^3$, and for $A_5$: $D_6 \mid D_5^2$). To compute sextic $PGL_2(5)$ or $PSL_2(5)$ fields, search for quintic fields.

# Proof by example

No actual slide, do live demo.

## More Groups

### Definition

*A finite group is p-*inertial *if it is an extension of a cyclic group of order prime to p by a p-group.*
*A finite group is* inertial *if it is p-inertial for some prime p.*

### Proposition (J, Roberts)

1. *To prove that the T-W principle holds for a group G, it suffices to prove it for all inertial subgroups of G*
2. *The tame-wild principle holds for* $S_3 \times C_3$, $A_4 \times C_2$, $C_4 \times C_2$

- The tame-wild principle fails for $C_3 : C_4$ and $C_6 \times C_2$ (as Galois groups for a totally ramified extension)
- The tame-wild principle sometimes fails for $Q_8$ (e.g., ok for Galois group $Q_8$ with $K = \mathbb{Q}_2$, but not over other base fields)

# Sextic Galois groups

See the LMFDB!

## Sextic twinning

$\mathrm{Out}(S_n)$ is trivial for $n \neq 6$

- $\mathrm{PGL}_2(5) \leq S_6$ with index 6
- $S_6$ acts on the left cosets giving rise to an outer automorphism $S_6 \to S_6$
- We refer to the corresponding resolvent as sextic twinning
- It operates on the level of sextic algebras

# Sextic twinning

$\mathrm{Out}(S_n)$ is trivial for $n \neq 6$

- $\mathrm{PGL}_2(5) \leq S_6$ with index 6
- $S_6$ acts on the left cosets giving rise to an outer automorphism $S_6 \to S_6$
- We refer to the corresponding resolvent as sextic twinning
- It operates on the level of sextic algebras

| Cycle type | | $\mathfrak{c}_\nu(g)$ | |
|---|---|---|---|
| 6 | 321 | 5 | 3 |
| 51 | 51 | 4 | 4 |
| 411 | 411 | 3 | 3 |
| 42 | 42 | 4 | 4 |
| 33 | 3111 | 4 | 2 |
| 2211 | 2211 | 2 | 2 |
| 222 | 21111 | 3 | 1 |
| 111111 | 111111 | 0 | 0 |

# TW with Galois theory: part 1

For $6T_9 \cong S_3 \times S_3$,

- "Shortest path" class field theory approach: $C_3$ extension of a $V_4$ field, but bounds are not good: $D_4 \mid D_6$ and $D_{12} \mid D_6^2 \cdot D_4$
- Instead, compute reducible $S_3 \times S_3$ polynomials, and then use twinning
- By Frobenius computation + tame-wild, $D_3 \mid D_6$

| Cycle type | | $\mathfrak{c}_\nu(g)$ | |
|---|---|---|---|
| 6 | 3 | 5 | 2 |
| 33 | 3 | 4 | 2 |
| 3111 | 3 | 2 | 2 |
| 6 | 21 | 5 | 1 |
| 222 | 21 | 3 | 1 |
| 2211 | 21 | 2 | 1 |
| 33 | 111 | 4 | 0 |
| 222 | 111 | 3 | 0 |
| 111111 | 111 | 0 | 0 |

## TW with Galois theory: part 2

- $D_3 \mid D_6$
- if $p \,||\, D_3$, then $p^2 \mid D_6$
- this filters out many cubic discriminants
- in pairing them up, can predict sextic discriminant contribution of tame primes
- relatively few combinations survive
- for those, compute the sextic and check its discriminant

# A standard example: $9T_{16} \cong C_3^2 : D_4$

- $9T_{16}$ is not a c.d. group, but T-W principle holds for all inertial subgroups
- Best route seems to be a $C_3$ extension of a $D_4$ octic

| Cycle types | | | $\mathfrak{c}_j(g)$ | | | |
|---|---|---|---|---|---|---|
| $K_9$ | $K_8$ | $K_{24}$ | $K_9$ | $K_8$ | $K_{24}$ | $\frac{8}{3}\mathfrak{c}_9 + \mathfrak{c}_8$ |
| 222 | 2222 | 222222222222 | 3 | 4 | 12 | 12 |
| 44 | 44 | 444444 | 6 | 6 | 18 | 22 |
| 2222 | 2222 | 222222222222 | 4 | 4 | 12 | $14.\overline{6}$ |
| 63 | 2222 | 66222222 | 7 | 4 | 16 | $22.\overline{6}$ |
| 63 | 2222 | 6666 | 7 | 4 | 20 | $22.\overline{6}$ |
| 333 | 1...1 | 33333333 | 6 | 0 | 16 | 16 |
| 333 | 1...1 | 3333 | 6 | 0 | 8 | 16 |

So $|D_8| \leq |D_9|^{4/3}$

# A standard example: $9T_{16} \cong C_3^2 : D_4$

- $9T_{16}$ is not a c.d. group, but T-W principle holds for all inertial subgroups
- Best route seems to be a $C_3$ extension of a $D_4$ octic

Cycle types

| $K_9$ | $K_8$ | $K_{24}$ |
|---|---|---|
| 222 | 2222 | 222222222222 |
| 44 | 44 | 444444 |
| 2222 | 2222 | 222222222222 |
| 63 | 2222 | 66222222 |
| 63 | 2222 | 6666 |
| 333 | 1...1 | 33333333 |
| 333 | 1...1 | 3333 |

$\mathfrak{c}_j(g)$

| $K_9$ | $K_8$ | $K_{24}$ | $\frac{8}{3}\mathfrak{c}_9 + \mathfrak{c}_8$ |
|---|---|---|---|
| 3 | 4 | 12 | 12 |
| 6 | 6 | 18 | 22 |
| 4 | 4 | 12 | $14.\overline{6}$ |
| 7 | 4 | 16 | $22.\overline{6}$ |
| 7 | 4 | 20 | $22.\overline{6}$ |
| 6 | 0 | 16 | 16 |
| 6 | 0 | 8 | 16 |

So $|D_8| \leq |D_9|^{4/3}$ and $|D_{24}| \leq |D_9|^{8/3} \cdot |D_8|$

## Stem Field/Galois Closure

For $G \leq S_n$, let

$$\alpha(G) = \min_{\sigma \in G - \{1\}} \frac{(n - \ell(\sigma))/n}{(|\sigma| - 1)/|\sigma|}$$

**Theorem (J, Roberts)**

*If $K$ is a degree $n$ number field with $G = \mathrm{Gal}(K) \leq S_n$,*

$$\mathrm{grd}(K)^{\alpha(G)} \leq \mathrm{rd}(K).$$

*Moreover,*

$$\alpha(G) = 1 - \frac{\mathcal{F}(G)}{n}$$

*where $\mathcal{F}(G)$ is the maximal number of fixed points of a non-identity element of $G$.*

## Using Galois closure: a primitive nonic field

- Nonic fields with Galois group $9T_{15} = C_3^2 : C_8$ are primitive
- According to LMFDB, $\mathcal{F}(9T_{15}) = 1$
- So $\alpha(9T_{15}) = 1 - \frac{1}{9} = \frac{8}{9}$
- Computing all such fields with $\mathrm{grd}(K) \leq 40$ gives all such with $\mathrm{rd}(K) \leq 40^{8/9} \approx 26.549$.
- This gives the first few examples of these fields
- Can repeat with totally real fields and a bigger bound to get the first example there (only other signature for this group).
- The grd computation does not need to worry about fancy discriminant bounds since any subfield $L$ of $K^{gal}$ satisfies $\mathrm{rd}(L) \leq \mathrm{grd}(K)$
- Using CFT, find $C_3$ extensions of $C_8$ fields

# The end

Thank you!