An ABC construction of number fields

David P. Roberts
University of Minnesota, Morris

I. An example.

II. Matrix step. $ABC = 1$
(Katz’s theory of rigid local systems)

III. Polynomial step. $A(x) + B(x) + C(x) = 0$
(Theory of dessins d’enfants)

IV. Integer step. $ax^p + by^q + cz^r = 0$
(Along the lines of the ABC conjecture)

V. Further directions.
I. An example. The polynomial

\[ f(x) = x^{27} - 432 x^{21} - 810 x^{19} - 7056 x^{18} - 39852 x^{15} + 93312 x^{13} - 254016 x^{12} - 98415 x^{11} + 625968 x^{10} - 1168560 x^9 + 1705860 x^7 - 1796256 x^6 - 944784 x^5 + 979776 x^4 + 31104 x^3 - 571536 x - 592704 \]

is unusual in two ways:

- The Galois group of its splitting field is \( PSp_4(F_3).2 \), which is nonsolvable of order 51,840 = 2^73^45.

- The discriminant of the root field \( \mathbb{Q}[x]/f(x) \) is \( 2^{20}3^{84} \), reflecting tame ramification at 2 and wild ramification at 3.

How can we systematically produce polynomials of this sort?
II. Matrix Step. Consider matrices $A$, $B$, $C \in GL_n(\overline{F}_\ell)$ such that

- $ABC = I$
- $\langle A, B, C \rangle$ acts irreducibly on $\overline{F}_\ell$.
- the sum of the centralizer dimensions of the matrices is maximal, namely
  \[ \text{cd}(A) + \text{cd}(B) + \text{cd}(C) = n^2 + 2. \]

Such a triple is **rigid** in the sense that the individual conjugacy classes $[A]$, $[B]$, $[C]$ determine the conjugacy class of the triple $(A, B, C)$.

See (Katz, Rigid Local systems) for the very rich theory: rigid matrix triples are classified and they all come by reduction modulo $\ell$ from motivic monodromy representations.
Example of a rigid matrix triple in $GL_4(F_3)$:

$$A = \begin{pmatrix} 0121 \\ 0102 \\ 1011 \\ 0100 \end{pmatrix} \sim \begin{pmatrix} 1100 \\ 0110 \\ 0011 \\ 0001 \end{pmatrix}$$

$$B = \begin{pmatrix} 0001 \\ 0020 \\ 0100 \\ 2000 \end{pmatrix} \sim \begin{pmatrix} i000 \\ 0i00 \\ 00i0 \\ 000i \end{pmatrix}$$

$$C = \begin{pmatrix} 0010 \\ 0002 \\ 1000 \\ 0200 \end{pmatrix} \sim \begin{pmatrix} 1000 \\ 0100 \\ 00i0 \\ 000i \end{pmatrix}$$

$ABC = I$ holds by direct computation. Irreducibility holds because $\langle A, B, C \rangle = Sp_4(F_3)$. The two sides of the rigidity condition are

$$(1 + 1 + 1 + 1) + (4 + 4) + (4 + 1 + 1) = 18$$

and

$$4^2 + 2 = 18$$

so the rigidity condition holds.
III. Polynomial step. Consider permutations \( A, B, C \in S_N \) such that \( ABC = e \). Such a triple determines a covering of algebraic curves over \( \overline{\mathbb{Q}} \)

\[
F : X \to \mathbb{P}^1
\]

ramified only above 0, 1, \( \infty \in \mathbb{P}^1 \).

**Theorem. (1960’s; Grothendieck)** \( F \) has bad reduction within the primes dividing the order of the **global** monodromy group \( \langle A, B, C \rangle \).

**Theorem. (1990’s; Katz)** If \( A, B, C \) come from the rigid matrix situation of Part II via some representation \( \langle A, B, C \rangle \to GL_n(\overline{\mathbb{F}}_\ell) \) then \( F \) has bad reduction within the primes dividing the orders of the **local** monodromy groups \( \langle A \rangle, \langle B \rangle, \langle C \rangle \) and \( \ell \).

(Intuitively, “Katz three point covers” are extremal among all three point covers, and are very special, sharing some of the features of \( X_0(\ell) \to j \)-line.)
From degree 27 permutations corresponding to the matrices $A$, $B$, $C$ of Part II, we computed

\[
\begin{align*}
    a(x) &= 2^{12}(3x^3 - 3x - 1)^9 \\
    b(x) &= f_{10}(x)^2 f_6(x) \\
    c(x) &= (48x^3 + 108x^2 + 63x + 11)g_6(x)^4
\end{align*}
\]

with

\[ a(x) + b(x) + c(x) = 0. \]

The corresponding cover is

\[ F : \mathbb{P}^1 \to \mathbb{P}^1 : x \mapsto -\frac{a(x)}{c(x)}, \]

The discriminant of $f(t, x) = a(x) + tc(x)$ is

\[ D(t) = 2^{336}3^{450}t^{24}(t - 1)^{10}, \]

illustrating the good reduction theorems.

(Summary so far: $f(t, x)$ is an analog of division polynomials corresponding to $\ell$-torsion points on a general elliptic curve. Katz’s theory gives a hierarchy of such polynomials, but at present they are hard to compute.)
IV. Integer step. Continuing with our example, for generic $\tau \in \mathbb{Q} - \{0, 1\}$, $f(\tau, x)$ is irreducible and

$$K_\tau = \mathbb{Q}[x]/f(\tau, x)$$

is a number field. If $\tau = -ax^9/cz^4$ with

$$ax^9 + by^2 + cz^4 = 0,$$

then $K_\tau$ is ramified within the primes dividing $6abc$. The specialization point $\tau = -48$, corresponding to

$$2^4 3 - 7^2 + 1 = 0$$

gives our field $K_{-48}$, which has the unusual property mentioned before of being only tamely ramified at 2.

V. Future directions. Systematically study the ramification in these “ABC number fields” $\mathbb{Q}[x]/f(\tau, x)$, as a function of the discrete group-theoretic data defining the Katz three point cover and the continuous parameter $\tau$. 