SPECULATIONS IN GALOIS THEORY

NICHOLAS M. KATZ AND IGOR RIVIN

To Gerard Laumon, with the utmost admiration

Contents

1. The speculations

The starting point of these speculations is the 1930 theorem of Schur. Some of the "evidence" for these speculations was presented at the 2017 Cetraro conference in honor of Umberto Zannier.

There is an extensive literature on the Galois groups of various classical polynomials, e.g., those of Bessel, Jacobi, Laguerre, Legendre, see [Grosswald, Chapter 12] and [FT], [CHS], [Hajir], [CH] for a sampling. The consideration of Galois-theoretic aspects of truncations starts with Schur, see [Schur] and [Coleman], see also [CL],[Martin], [RPM].

We are given a power series $f(x) = \sum_{n\geq 0} a_n x^n \in \mathbb{Q}[[x]]$, about which we assume

$$a_n \neq 0 \text{ for all } n.$$

For each $d \geq 1$, we consider its truncation through degree d,

$$f_d(x) := \sum_{n=0}^{d} a_n x^n.$$

We denote by G_d the Galois group of f_d over $\mathbb{Q}$. Schur proved that for $f(x) := \exp(x)$, G_d is the symmetric group S_d unless $4|d$, and G_d is the alternating group A_d if $4|d$.

We wish to understand, for an arbitrary f with all $a_n \neq 0$, how often G_d is either S_d, or A_d, or neither of these. For each integer $N \geq 1$, we define the sets

$$\mathcal{S}(f,N) := \{d \leq N : G_d = S_d\},$$

$$\mathcal{A}(f,N) := \{d \leq N : G_d = A_d\},$$

$$\mathcal{N}(f,N) := \{d \leq N : G_d \text{ is neither } S_d \text{ nor } A_d\}.$$

Question 1.1. Is it true that for any given f, each of the sequences

$$\#\mathcal{S}(f,N)/N, \quad \#\mathcal{A}(f,N)/N, \quad \#\mathcal{N}(f,N)/N,$$

has a limit as $N \uparrow \infty$?

If the answer to Question 1.1 is yes for a given f, denote these limits as

$$\mathcal{S}(f), \quad \mathcal{A}(f), \quad \mathcal{N}(f)$$

respectively.

Question 1.2. If the answer to Question 1.1 is yes for a given f, is it true that $\mathcal{N}(f)$ is either 0 or 1?

2. Some "evidence"

If we start with the geometric series $1/(1-x) = \sum_{n\geq 0} x^n$, then for $d \geq 3$, G_d is never S_d or A_d.

All the rest of our "evidence" is experimental: there are no theorems. To do experiments, we took various input f's and truncations f_d, typically for $d \leq 2000$, and used Magma [Magma]. In the following discussion, calculations are through 2000 unless explicitly stated otherwise.

The Magma program "IsEasySnAn(f_d:Trials:=D)" checks irrreducibility of f_d, then successively tries up to D primes p at which f_d has p-integral coefficients and prime to p discriminant, computes the mod p factorization of f_d, and hopes to find an ℓ cycle with ℓ a prime in the range $d/2 < \ell \leq d-3$, which, if found, proves (Jordan's theorem) that G_d is A_d or S_d. It then looks at the sign it found this way (which is $(-1)^\sigma$ with $\sigma = d-$(the number of mod p factors)). [The default value of D is 50, but we took $D = 1000$ to be safe.] The program returns 1 if it (provably) finds S_d, it returns 2 if it (provably) finds A_d, and it returns 0 if it reaches no provable conclusion.

With input the series $-2+1/(1-x)$, it seemed that G_d was always S_d, see [Martin] for a discussion of (the palindrome of) this case. With inputs the series $1+1/(1-x)$ and $2+1/(1-x)$, G_d was always S_d for $d > 24$, respectively $d > 15$. So in these cases, it seems that $\mathcal{S}(f) = 1, \mathcal{A}(f) = 0 = \mathcal{N}(f)$.

With inputs the series $3 + 1/(1-x)$, $4 + 1/(1-x)$, and $29 + 1/(1-x)$, G_d was always S_d, so in these cases, it seems that $\mathcal{S}(f) = 1, \mathcal{A}(f) = 0 = \mathcal{N}(f)$.

With inputs the series $(1/(1-x))^k$ for $k = 2, 3, 4, 5, 6, 7$, in the range $d \leq 2000$, G_d was always A_d or S_d, and it looked as though $\mathcal{S}(f)$ was 1 and $\mathcal{A}(f)$ was 0, although there would be infinitely many A_d cases.

With inputs the series $\sum_n x^n (n!)^k$ for $k = 1, 2, 3, 4, 5, 6, 7$ in the range $d \leq 2000$, G_d was always S_d.

With inputs the series $\sum_n x^n/(n!)^k$ for $k = 2, 3, 4, 5, 6, 7$ in the range $d \leq 2000$, G_d was always S_d, with two exceptions for $k = 2$: the $d = 2$ truncation is not irreducible (in fact it is $(1 + x/2)^2$), and the $d = 5$ truncation has $G_5 = A_5$.

With inputs the Eisenstein series $E_k(x)$ on $\mathrm{SL}(2, \mathbb{Z})$ for even $k = 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24$, it seemed that G_d was always S_d.

With inputs the four square theta function $(1 + 2\sum_{n\geq 1} x^{n^2})^4$, it seemed that G_d was S_d for $d \geq 16$. With input the five square theta function $(1+2\sum_{n\geq 1} x^{n^2})^5$ or the six square theta function $(1 + 2\sum_{n\geq 1} x^{n^2})^6$, it seemed that G_d was always S_d.

With input the shifted (to have nonzero constant term) Ramanujan Delta function$\Delta(x)/x$, it seemed that G_d was always S_d. [For Delta, it is still not proven that $\tau(n) \neq 0$ for all $n \geq 1$].

With input the partition function $\prod_{n\geq 1}(1/(1-x^n))$, it seemed that G_d was always S_d.

With input the strict partition function $\prod_{n\geq 1}(1 + x^n)$, it seemed that G_d was always S_d.

With inputs the modified log, dilog, trilog, i.e., the series $1+\sum_{n\geq 1} x^n/n^k$ for $k = 1, 2, 3$, it seemed that G_d was always S_d. See [SST] for a discussion of the log case.

With inputs the hypergeometric series ${}_2F_1(1/2, 1/2, 1, x)$, ${}_2F_1(1/3, 2/3, 1, x)$,${}_2F_1(1/4, 3/4, 1, x)$, and ${}_2F_1(1/2, 1/5, 1, x)$, it seemed that G_d was always S_d.

With input each of the Artin Hasse exponentials $E_p(x) = \exp(\sum_{n\geq 0} x^{p^n}/p^n)$, for each prime $p < 100$, it seemed that G_d was always S_d in degree $\geq p$. [In degree $< p$, $E_p(x)$ agrees with $\exp(x)$, whose G_d is given by Schur.]

With input the series for $(1-4x)^{1/2}$ or for $(1-9x)^{1/3}$ or for $(1-49x)^{1/7}$, it seemed that G_d was always S_d. However with input the series for $(1-25x)^{1/5}$, it seemed that G_d was always S_d or A_d, and it looked as though $\mathcal{S}(f)$ was 1 and $\mathcal{A}(f)$ was 0, although there would be infinitely many A_d cases.

With input the series for $(1-4x)^{-1/2}$ or $(1-9x)^{-1/3}$ or $(1-25x)^{-1/5}$ or $(1-49x)^{-1/7}$, it seemed that G_d was always S_d or A_d, and it looked as though $\mathcal{S}(f)$ was 1 and $\mathcal{A}(f)$ was 0, although there would be infinitely many A_d cases. See [RPM, 4.1] for a discussion of the $(1-4x)^{-1/2}$ case. [For the two functions $(1-25x)^{-1/5}$ and $(1-49x)^{-1/7}$, our Magma program got to $d = 2000$ with "Trials:=2000", but with problems: at $1656, 1960$ for $(1-25x)^{-1/5}$, and at $1400, 1760, 1824$ for $(1-49x)^{-1/7}$. Each of these five cases (eventually) turned out to have $G_d = A_d$.]

To conclude this section, we will consider some inputs we learned from Herwig Hauser. For a nonzero, nonsquare integer D, define

$$w := \sqrt{D}, \quad h_D(x) := ((1+wx)/(1-wx))^w.$$

This series in invariant under $w \mapsto -w$, and (hence) lies in $1 + x\mathbb{Q}[[x]]$. For $D > 0$, h_D has all coefficients nonzero. For $D < 0$, this seems to be true unless D is either $-2 \times$ square (in which case the coefficient of x^4 seems to vanish), or D is $-6 \times$ square (in which case the coefficient of x^8 seems to vanish). We tested truncations through $d = 2000$ for h_D with $2 \leq D \leq 32$ a nonsquare, and for h_D with $-1 \geq D \geq -35$. We found $G_d = S_d$ in all cases with $a_d \neq 0$, with four exceptions: for each of $D = -2, -8, -18, -32$, whose $a_4 = 0$, the $d = 3$ truncations were neither S_d nor A_d. [For each of $D = -6, -24$, whose $a_8 = 0$, the f_7 had group S_7, leading to no apparent exceptions, see the remark below.]

Remark 2.1. In the Hauser examples above, for D either $-2 \times$ square or $-6 \times$ square, there is a single coefficient (a_4 in the first case, a_8 in the second case) which vanishes through degree 2000 (possibly(?) the only vanishing coefficient in the series). In general, if a coefficient a_d vanishes, then the d-truncation f_d is equal to the $d-1$-truncation f_{d-1}. Therefore when we ask whether or not IsEasySnAn(a given f) returns $S_{\deg(f)}$, we get the same answer for f_d as for f_{d-1}. So strictly speaking, these Hauser examples, for D either $-2 \times$ square or $-6 \times$ square, belong in the next section.

3. A variant

We are given a power series $f(x) = \sum_{n\geq 0} a_n x^n \in \mathbb{Q}[[x]]$, about which we assume only that $a_0 \neq 0$ and that f is not a polynomial. Let us say that an integer $d \geq 1$ occurs in f if $a_d \neq 0$. We then ask about G_d for each d which occurs in f, and compute the averages over the sets $\{d \leq N : d \text{ occurs in } f\}$. It is natural to pose Question 1.1, but examples suggest that even if Question 1.1 has a positive answer, Question 1.2 may have a negative answer.

Here is one example. For the (normalized, without the $q^{1/24}$ factor) Dedekind eta function, $(\Delta(x)/x)^{1/24}$, as $d \leq 2000$ grows over the exponents which occur, G_d (literally) alterates between being S_d and being neither S_d nor A_d: we seem to have $\mathcal{S}(f) = 1/2, \mathcal{A}(f) = 0, \mathcal{N}(f) = 1/2$. We find exactly the same alternation for $1 + (\Delta(x)/x)^{1/24}$. For $2 + (\Delta(x)/x)^{1/24}$, we seem to have $\mathcal{S}(f) \approx 0.733, \mathcal{A}(f) = 0, \mathcal{N}(f) \approx 0.266$ (here going up to $d = 4000$). Yet for $3 + (\Delta(x)/x)^{1/24}$, we have $G_d = S_d$ (going up to $d = 4000$).

On the other hand, for the elliptic curve $X_1(11)$ (equation $y^2+y=x^3-x^2$), its (shifted, to have nonzero constant term) L function, namely $\eta(x)^2\eta(x^{11})^2/x$, seems to have most G_d being S_d, but with infinitely many cases of neither S_d nor A_d, and we seem to have $\mathcal{S}(f)=1, \mathcal{A}(f)=0, \mathcal{N}(f)=0$.

For the raw theta series $1+2\sum_{n\geq 1} x^{n^2}$, all G_d with $d>4$ are S_d (only up to $d=173^2$), so we seem to have $\mathcal{S}(f)=1, \mathcal{A}(f)=0, \mathcal{N}(f)=0$. For the two square and three square theta functions, $(1+2\sum_{n\geq 1} x^{n^2})^2$ and $(1+2\sum_{n\geq 1} x^{n^2})^3$, G_d is S_d for all $d>13$ and for all $d>24$ respectively, so we seem to have $\mathcal{S}(f)=1, \mathcal{A}(f)=0, \mathcal{N}(f)=0$.

4. Another variant: shifts

We are given a power series $f(x)=\sum_{n\geq 0} a_n x^n \in \mathbb{Q}[[x]]$, about which we assume

$$a_n \neq 0 \quad \text{for all } n.$$

We now look at "shifts" of f: for an integer $r\geq 1$, the r-shift of f is the series

$$\sum_{n\geq 0} a_{n+r}x^n.$$

Having fixed a shift of f, we then look at the Galois groups of its truncations.

On the "not very interesting" side: with any of the inputs $k+1/(1-x)$, any $k\neq -1$, and any r-shift with $r\geq 1$, no truncation of any degree $d\geq 3$ has group S_d or A_d (simply because each shift is $1/(1-x)$).

For the exponential function $\exp(x)$, each of its r-shifts for $r=1,2,3,4,5,6,7$ had $G_d=S_d$ for all $d\leq 2000$.

We then looked at the $1,2$ and 3-shifts of the Eisenstein series $E_k(x)$ on $\mathrm{SL}(2,\mathbb{Z})$ for even $k, 2\leq k\leq 24$, and looked up to $d=2000$.

For E_2 and its 1-shift, $G_d=S_d$ for $d\neq 4$ up to $d=2000$. For E_2 and its 2-shift, $G_d=S_d$ for $d\neq 3$ up to $d=2000$. For E_2 and its 3-shift, $G_d=S_d$ for all d up to $d=2000$.

For each of the Eisenstein series E_k with even $k, 4\leq 4\leq 24$, and each of its $1,2$ and 3 shifts, we found $G_d=S_d$ for all $d\leq 2000$.

For the normalized Delta function $\Delta(x)/x$, and each of its $1,2$ and 3 shifts, we found $G_d=S_d$ for all $d\leq 2000$.

For each of the inputs $(1-4x)^{1/2}$, $(1-9x)^{1/3}$, $(1-25x)^{1/5}$, $(1-49x)^{1/7}$ and $(1-4x)^{-1/2}$,$(1-9x)^{-1/3}$, $(1-25x)^{-1/5}$, $(1-49x)^{-1/7}$, and for each of their $1,2$ and 3 shifts, we found $G_d=S_d$ for all $d\leq 2000$.

We did a few more experiments, with the partition function and the strict partition function.

For the partition function, the 1-shift had $G_d=S_d$ for all $d\leq 2000$, as did both its 2-shift and its 3 shift.

For the strict partition function, the 1-shift had $G_d=S_d$ for all $d\neq 3, d\leq 2000$, the 2-shift had $G_d=S_d$ for all $d\leq 2000$, and the 3-shift had had $G_d=S_d$ for all $d\neq 4, d\leq 2000$.

References

[CH] Cullinan, J., Hajir, F., On the Galois groups of Legendre polynomials, Indag. Math. (N.S.) 25 (2014), no. 3, 534-552.

[CHS] Cullinan, J., Hajir, F., Sell, E., Algebraic properties of a family of Jacobi polynomials, J. Théor. Nombres Bordeaux 21 (2009), no. 1, 97-108.

[CL] Chambert Loir, A.,The theorem of Jentzsch-Szego on an analytic curve : application to the irreducibility of truncations of power series, Int. J. Number Theory, Volume 7 (2011) no. 7, pp. 1807-1823.

[Coleman] Coleman, R., On the Galois groups of the exponential Taylor polynomials, Enseign. Math. (2) 33 (1987), no. 3-4, 183-189.

[FT] Filaseta,M., Trifonov,O.,The irreducibility of the Bessel polynomials, J. Reine Angew. Math., 550 (2002) 125-140.

[Grosswald] Grosswald, E., Bessel polynomials, Lecture Notes in Math. 698, Springer, Berlin, 1978, xiv+182 pp.

[Hajir] Hajir, F., Algebraic properties of a family of generalized Laguerre polynomials, Canad. J. Math. 61 (2009), no. 3, 583-603.

[Jordan] Jordan, C., Sur la limite de transitivité des groupes non alternés, Bull. Soc. Math. France, 1 (1872-3), 40-71.

[Magma] Bosma,,W., Cannon, J., Playoust,C., The Magma algebra system. I. The user language, J. Symbolic Comput., 24 (1997), 235-265, using V2.29-1.

[Martin] Martin, P., The Galois group of $x^n - x^{n-1} - \ldots - x - 1$, J. Pure Appl. Algebra 190 (2004), no. 1-3, 213-223.

[RPM] Rabarison, P., Pazuki, F., Molin, P., Exponentielle tronquée et autres contes galoisiens, Publications mathématiques de Besancon. Algèbre et théorie des nombres (2024), pp. 105-117.

[Schur] Schur,I., Gleichungen ohne Affekt (1930), Gesammelte Abhandlungen, Band III, No. 67, 191-197.

[SST] Shokri, K., Shaffaf, J.,Taleb, R., Galois groups of Taylor polynomials of some elementary functions, Int. J. Number Theory 15 (2019), no. 6, 1127-1141.

Department of Mathematics, Princeton University, Princeton, NJ 08544
E-mail address: `nmk@math.princeton.edu`

Department of Mathematics, Temple University, Philadelphia
E-mail address: `igor.rivin@temple.edu`