Pacific Journal of Mathematics

SOME PROPERTIES OF THE PROBABILISTIC ZETA FUNCTION OF FINITE SIMPLE GROUPS

Erika Damian, Andrea Lucchini, and Fiorenza Morini

Volume 215 No. 1 May 2004

PACIFIC JOURNAL OF MATHEMATICS
Vol. 215, No. 1, 2004

SOME PROPERTIES OF THE PROBABILISTIC ZETA FUNCTION OF FINITE SIMPLE GROUPS

Erika Damian, Andrea Lucchini, and Fiorenza Morini

In the factorial ring of Dirichlet polynomials we explore the connections between how the Dirichlet polynomial $P_G(s)$ associated with a finite group G factorizes and the structure of G. If $P_G(s)$ is irreducible, then $G/\mathrm{Frat}\, G$ is simple. We investigate whether the converse is true, studying the factorization in the case of some simple groups. For any prime $p \geq 5$ we show that if $P_G(s) = P_{\mathbf{Alt}(p)}(s)$, then $G/\mathrm{Frat}\, G \cong \mathbf{Alt}(p)$ and $P_{\mathbf{Alt}(p)}(s)$ is irreducible. Moreover, if $P_G(s) = P_{\mathbf{PSL}(2,p)}(s)$, then $G/\mathrm{Frat}\, G$ is simple, but $P_{\mathbf{PSL}(2,p)}(s)$ is reducible whenever $p = 2^t - 1$ and $t = 3 \mod 4$.

1. Introduction

In [**5**] Hall introduced the Eulerian function ϕ_G of a finite group G; if $t \in \mathbb{N}$, then $\phi_G(t)$ is the number of ordered t-tuples of elements that generate G. He proved that

$$\phi_G(t) = \sum_{H \leq G} \mu_G(H)|H|^t \tag{1.1}$$

where μ_G is the Möbius function of the subgroup lattice of G which is defined inductively as $\mu_G(G) = 1$ and $\sum_{H \leq K} \mu_G(K) = 0$ if $H < G$. Clearly $\mathrm{Prob}_G(t) = \phi_G(t)/|G|^t$ is the probability that a random t-tuple generates G and, in view of (1.1), we may write:

$$\mathrm{Prob}_G(t) = \sum_{H \leq G} \frac{\mu_G(H)}{|G : H|^t}. \tag{1.2}$$

This means that we may define a complex function $P_G(s)$ with the property that $P_G(t) = \mathrm{Prob}_G(t)$ for any $t \in \mathbb{N}$, associating a Dirichlet polynomial with G which is defined as follows:

$$P_G(s) = \sum_{n=1}^{\infty} \frac{a_n(G)}{n^s} \qquad \text{with} \quad a_n(G) = \sum_{|G:H|=n} \mu_G(H). \tag{1.3}$$

The inverse (complex) function $1/P_G(s)$ is usually called the probabilistic zeta function of G, see Mann [**9**] and Boston [**1**] as references.

As it is explained in Section 2, the ring R of Dirichlet polynomials is a factorial domain. We ask whether information about how $P_G(s)$ factorizes in R gives us insights into the structure of the group G. We gain evidence that such a connection exists by observing that, for any $N \trianglelefteq G$, the polynomial $P_{G/N}(s)$ divides $P_G(s)$ and the quotient $P_G(s)/P_{G/N}(s)$ is nontrivial if $N \not\leq \operatorname{Frat} G$. This implies that if $P_G(s)$ is irreducible then $G/\operatorname{Frat} G$ is a simple group.

A question that arises quite naturally is whether there exist examples of groups G such that $P_G(s)$ has a nontrivial factorization which does not come from normal subgroups. In particular is $P_G(s)$ irreducible when G is a simple group? The answer is positive for all abelian simple groups, being $P_{\mathbb{Z}_p}(s) = 1-1/p^s$. In the present paper we deal with some nonabelian simple groups.

We start with the alternating groups of prime degree. We prove that $P_{\mathrm{Alt}(p)}(s)$ is irreducible, for any prime number $p \geq 5$. The tools employed in this case allow us to prove that $P_G(s)$ is irreducible for other simple groups. However the analysis of the projective special linear groups $\mathrm{PSL}(2,p)$ provides examples of simple groups whose associated Dirichlet polynomial is reducible. More precisely $P_{\mathrm{PSL}(2,p)}(s)$ is reducible if and only if p is a Mersenne prime such that $p = 2^t - 1$ and $t = 3 \mod 4$.

Although $P_{\mathrm{PSL}(2,p)}(s)$ is reducible for some choices of p, we prove that if a finite group G satisfies $P_G(s) = P_{\mathrm{PSL}(2,p)}(s)$, then $G/\operatorname{Frat} G$ is a finite simple group. We conjecture that this is true in general: If S is a finite simple group and $P_G(s) = P_S(s)$ then $G/\operatorname{Frat} G$ is simple.

2. Preliminary results

Definition 1. A Dirichlet series is a series of the form

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}, \qquad s \in \mathbb{C},$$

where $\{a_n\}_{n\in\mathbb{N}}$ is an arbitrary sequence of complex numbers.

Let R be the ring of Dirichlet polynomials with integer coefficients, i.e.,

$$R = \left\{ f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} \;\middle|\; a_n \in \mathbb{Z} \text{ for all } n \geq 1,\ \left|\{n : a_n \neq 0\}\right| < \infty \right\}.$$

Let Π be the set of all prime numbers; we associate an indeterminate x_p with any $p \in \Pi$. Let X_Π be the set of all these indeterminates. Since R is generated as a ring by $\{1/p^s\}_{p\in\Pi}$, we may consider the following ring isomorphism between R and $\mathbb{Z}[X_\Pi]$:

$$\begin{array}{rccc} \phi: & R & \to & \mathbb{Z}[X_\Pi] \\ & 1/p^s & \mapsto & x_p. \end{array}$$

Given a set π of prime numbers, let R_π be the subring of R defined as follows:

$$R_\pi = \left\{ \sum_{n=1}^{\infty} \frac{a_n}{n^s} \in R \;\middle|\; \text{if } a_n \neq 0 \text{ then } n \text{ is a } \pi\text{-number} \right\}.$$

Let $f(s) \in R$; define $\pi_f = \{p \in \Pi \mid \text{there exists } n \text{ such that } a_n \neq 0 \text{ and } p \text{ divides } n\}$. Notice that $\pi_f = \{p_1, \ldots, p_r\}$ is a finite set and $f(s) \in R_{\pi_f}$. Moreover $R_{\pi_f} \cong \mathbb{Z}[x_{p_1}, \ldots, x_{p_r}]$ is a factorial domain and any divisor $g(s)$ of $f(s)$ in R belongs to R_{π_f}. In particular R also is a factorial domain.

Note that for any prime number p we may define a ring endomorphism of R as follows:

$$\begin{array}{rccc} \alpha_p : & R & \longrightarrow & R \\ & f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} & \mapsto & f^{(p)}(s) = \sum_{n=1}^{\infty} \frac{b_n}{n^s} \end{array}$$

where

$$b_n = \begin{cases} a_n & \text{if } (p,n) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

We can now translate well-known facts about polynomial rings as results on Dirichlet polynomials.

Lemma 2. *Let $f(s) = \sum_{n=1}^{\infty} a_n/n^s \in R$. Assume p to be a prime number such that p^2 does not divide m whenever $a_m \neq 0$ and there exists n divisible by p with $a_n \neq 0$. Then $f(s)$ is reducible in R if and only if $\gcd(\alpha_p(f(s)), f(s)) \neq 1$.*

Proof. Our lemma may be restated as follows: Let $D = \mathbb{Z}[X_\Pi \setminus \{x_p\}]$ and $g(x_p) \in D[x_p]$ such that $\deg(g(x_p)) = 1$; then $g(x_p)$ is reducible in $D[x_p]$ if and only if $\gcd(g(0), g(x_p)) \neq 1$. Namely we are taking $g(x_p) = \phi(f(s))$. Note that the units of $D[x_p]$ are the units of $\mathbb{Z}$, hence if $d = \gcd(g(0), g(x_p))$ and $d \neq 1$, then d is a nontrivial factor of $g(x_p)$. On the other hand, if $g(x_p)$ has a nontrivial factorization in $D[x_p]$, then we may write $g(x_p) = b(x_p)c(x_p)$ and assume that $\deg(b(x_p)) = 1$, $\deg(c(x_p)) = 0$. Thus we get $g(0) = b(0)c(x_p)$, hence $c(x_p)$ is a non-unit element that divides d. □

Lemma 3. *Let $n \in \mathbb{N}$ with $n > 1$. Then $1 - n/n^s$ is reducible in R if and only if n is a power in $\mathbb{Z}$.*

Proof. If n is a power in $\mathbb{Z}$, then there exist m, $d \in \mathbb{Z}$ and $d > 1$ such that $n = m^d$. Then we obtain the following nontrivial factorization:

$$\left(1 - \frac{n}{n^s}\right) = \left(1 - \frac{m^d}{m^{ds}}\right) = \left(1 - \frac{m}{m^s}\right)\left(\sum_{j=0}^{d-1} \frac{m^j}{m^{js}}\right).$$

Conversely assume that $1 - n/n^s$ is reducible in R. Write $n = \prod_{i=1}^{r} p_i^{k_i}$, being $p_1, \ldots, p_r$ distinct prime numbers. Set $D = \mathbb{Z}$ if $r = 1$ and $D =$

$\mathbb{Z}[x_{p_1}, \ldots, x_{p_{r-1}}]$ otherwise, then $g(x_{p_r}) = \phi(1 - n/n^s)$ is reducible in $D[x_{p_r}]$. Note that $g(x_{p_r}) = 1 - x_{p_r}^{k_r} nf$ being $f \in D$ and $\gcd(f, n) = 1$. Since $g(x_{p_r})$ is reducible in $D[x_{p_r}]$, then $x_{p_r}^{k_r} - \frac{1}{nf}$ is reducible in $F[x_{p_r}]$ where F is the field of fractions of D. Let us recall (see [**8**], Chap. VI, Theorem 9.1) that given a field K, if $x^m - a$ is reducible in $K[x]$ then either $a \in K^p$, being p a suitable prime divisor of m, or $-4a \in K^4$ and 2 divides m. In our case, since $-4nf \notin F^4$, there exists $z \in F$ and a prime number p dividing k_r such that $nf = z^p$. As $nf \in D$ and D is factorial then z lies in D; moreover, since $\gcd(n, f) = 1$ we get that $n = z^p/f$ is a p-th power in $\mathbb{Z}$.

3. How to factorize $P_G(s)$

Let G be a finite group. Define a Dirichlet polynomial $P_G(s)$ as follows:

$$P_G(s) := \sum_{n=1}^{\infty} \frac{a_n(G)}{n^s} \qquad \text{with} \quad a_n(G) := \sum_{|G:H|=n} \mu_G(H).$$

We find it useful to stress some straightforward consequences of this definition:

Remark 4. $a_n(G) \neq 0$ implies that n divides $|G|$.

Remark 5. If $\mu_G(H) \neq 0$ then H is the intersection of some maximal subgroups of G (see [**5**]) and it contains the Frattini subgroup $\operatorname{Frat} G$. This implies $a_n(G) = a_n(G/\operatorname{Frat} G)$ for all $n \in \mathbb{N}$, in particular $P_G(s) = P_{G/\operatorname{Frat} G}(s)$.

In the previous section we noticed that R is a factorial domain. An important role in the factorization of $P_G(s)$ is played by the normal subgroups of G. In fact given a normal subgroup N of G we define a Dirichlet polynomial $P_{G,N}(s)$ as follows:

$$P_{G,N}(s) := \sum_{n=1}^{\infty} \frac{a_n(G,N)}{n^s} \qquad \text{with} \quad a_n(G,N) := \sum_{\substack{|G:H|=n \\ HN=G}} \mu_G(H).$$

Then $P_{G,N}(s)$ divides $P_G(s)$ in the ring R. More precisely (see for example [**2**] Section 2.2)

$$P_G(s) = P_{G/N}(s) P_{G,N}(s). \tag{3.1}$$

Notice that $P_G(s) = P_{G,G}(s)$. Moreover, N admits a proper supplement in G if and only if N is not contained in the Frattini subgroup of G; this implies:

Lemma 6. *$P_{G,N}(s) = 1$ if and only if $N \leq \operatorname{Frat} G$.*

Proof. Let $\mathcal{H}_n = \{H \leq G \mid HN = G \text{ and } |G : H| = n\}$. If $N \leq \operatorname{Frat} G$, then, for any $n > 1$, $\mathcal{H}_n = \emptyset$ and $a_n(G, N) = 0$. So if $N \leq \operatorname{Frat} G$, then $P_{G,N}(s) = 1$. Conversely assume that $N \not\leq \operatorname{Frat} G$. There exists a minimal integer $n > 1$

for which $\mathcal{H}_n \neq \emptyset$; the minimality of n implies that any $H \in \mathcal{H}_n$ is a maximal subgroup of G and $\mu_G(H) = -1$. Therefore $a_n(G, N) = -|\mathcal{H}_n| \neq 0$. □

Corollary 7. *If $P_G(s)$ is irreducible, than $G/\operatorname{Frat} G$ is simple.*

Proof. Suppose that N is a proper normal subgroup of G. We have that $P_{G/N}(s) \neq 1$; moreover, by (3.1) $P_G(s) = P_{G/N}(s)P_{G,N}(s)$. Since $P_G(s)$ is irreducible, we deduce $P_{G,N}(s) = 1$, hence, by Lemma 6, $N \leq \operatorname{Frat} G$. This proves that $G/\operatorname{Frat} G$ is a simple group. □

If t is a positive integer then, as it was noticed in [**5**] by Hall, $P_G(t)$ is the probability that t randomly chosen elements of G generate G. More in general, if $N \trianglelefteq G$ and the factor G/N can be generated by t elements, then $P_{G,N}(t)$ is the probability that t elements generate G given that they generate G modulo N. This statement has the following consequence, that will be used in the sequel:

Lemma 8. *Let t be a positive integer such that G can be generated by t elements. Then for any normal subgroup N of G such that $\operatorname{Frat} G < N < G$, we obtain $0 < P_{G/N}(t)$, $P_{G,N}(t) < 1$ and $0 < P_G(t) < \min\{P_{G/N}(t), P_{G,N}(t)\}$.*

4. The alternating groups Alt(p)

We shall show that for any prime number $p \geq 5$ the Dirichlet polynomial associated with $\operatorname{Alt}(p)$ is irreducible in R. In order to obtain this result we need some technical lemmas.

Lemma 9. *Let $p \geq 5$ be a prime number, then $a_{p(p-1)}(\operatorname{Alt}(p)) = p(p-1)$.*

Proof. Set $G = \operatorname{Alt}(p)$, we shall show that any subgroup $H \leq G$ with index $p(p-1)$ such that $\mu_G(H) \neq 0$ is the intersection of two point-stabilizers.

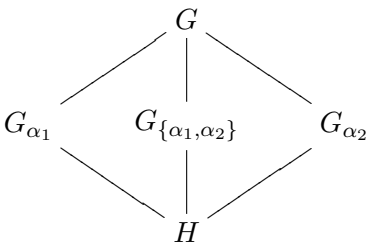
First note that H cannot be contained in a transitive maximal subgroup of G. Indeed, if M is a transitive maximal subgroup of G containing H, then we get that $p \cdot |H|$ divides $|M|$ and $|G : M| \leq (p-1)$ which is impossible. Moreover, as $\mu_G(H) \neq 0$, then H is the intersection of some intransitive maximal subgroups of G. Let M be a maximal subgroup of G containing H, we shall prove that there exist $\alpha, \beta \in \Omega$ (possibly equal) such that $M = G_{\{\alpha,\beta\}}$, being $\Omega = \{1, \ldots, p\}$. Indeed, if $p > 7$, then $|G : M| < \binom{p}{3}$ and by Theorem 5.2A in [**4**] we get that there exists $\Delta \subseteq \Omega$ with $0 < |\Delta| < 3$ such that $M = G_\Delta$. On the other hand, if $p = 5$, then clearly one of the two orbits of M has size less than 3; if $p = 7$, then M cannot have an orbit of size 3 as in this case we get $M \leq \operatorname{Sym}(3) \times \operatorname{Sym}(4)$, thus 5 divides $|G : M|$ which is impossible. As a consequence we get that $|G : M| \leq p(p-1)/2 < p(p-1)$ and $H \neq M$. Hence H is not a maximal subgroup of G and the maximal subgroups of G containing H are setwise stabilizers G_Δ where $\Delta \subset \Omega$ and $1 \leq |\Delta| \leq 2$. Assume by contradiction that H is not the intersection of

two point-stabilizers. Then there exist $\Delta_1, \Delta_2 \subseteq \Omega$ with $\Delta_1 \not\subseteq \Delta_2$ and $|\Delta_1| \leq |\Delta_2| = 2$, such that $H \leq G_{\Delta_1} \cap G_{\Delta_2}$. Set $N = G_{\Delta_2}$ hence $H \leq N_{\Delta_1}$. In both cases $|\Delta_1| = 1$ and $|\Delta_1| = 2$ we get that $|N : N_{\Delta_1}| \geq (p-2)$, hence

$$|G : H| \geq |G : N||N : N_{\Delta_1}| \geq p(p-1)(p-2)/2 > p(p-1)$$

against our hypothesis.

Thus there exist $\alpha_1, \alpha_2 \in \Omega$ with $\alpha_1 \neq \alpha_2$ such that $H = G_{\alpha_1} \cap G_{\alpha_2}$. Note that the lattice of all subgroups K such that $H \leq K \leq G$, is the following:



Thus $\mu_G(H) = 2$. Moreover note that we have $\binom{p}{2}$ choices for H; as a consequence we get that $a_{p(p-1)}(G) = 2\binom{p}{2} = p(p-1)$. □

Lemma 10. *Let $p \geq 5$ be a prime number, then $a_{(p-2)!}(\mathrm{Alt}(p)) \neq 0$.*

Proof. Let us recall that using the classification of finite simple groups it is possible to obtain a complete list of transitive groups of prime degree, (see [**4**] as a reference). If H is a proper subgroup of $G = \mathrm{Alt}(p)$ with order divisible by p, then it is transitive, furthermore either $H \leq N_G(\sigma)$ for a suitable cycle σ of length p or $\operatorname{soc} H$ is a nonabelian simple group and in the latter case $|G : H| < (p-2)!$. Therefore if $|G : H| = (p-2)!$ then H is the normalizer of a Sylow p-subgroup $P = \langle\sigma\rangle$ of G. In particular all the subgroups of index $(p-2)!$ are conjugated to $X = N_G(P)$ and

$$a_{(p-2)!}(G) = |G : N_G(X)|\mu_G(X) = (p-2)!\mu_G(X).$$

Therefore in order to show that $a_{(p-2)!}(G) \neq 0$ it suffices to prove that $\mu_G(X) \neq 0$. If $p \neq 7, 11, 17, 23$, then X is a maximal subgroup of G ([**10**], Corollary 3) and $\mu_G(X) = -1$. If $p = 7, 11, 17, 23$, then X is the intersection of precisely two maximal subgroups of G (isomorphic to $\mathrm{PSL}(3,2), M_{11}, \mathrm{P\Gamma L}(2,16)$ and M_{23} respectively) and $\mu_G(X) = 1$. □

Lemma 11. *Let $p \geq 5$ be a prime number, then $\alpha_p(P_{\mathrm{Alt}(p)}(s)) \neq 1$ and it is irreducible in R.*

Proof. Set $G = \mathrm{Alt}(p)$ and $\sum_n \frac{b_n}{n^s} = \alpha_p(P_G(s))$. By Lemma 10, $b_{(p-2)!} = a_{(p-2)!}(G) \neq 0$, hence $\alpha_p(P_G(s)) \neq 1$. By a Theorem of Bertrand-Chebychev (see [**6**], Theorem 418) there exists a prime number ξ such that $\frac{p}{2} < \xi \leq p-2$. Suppose $r > 1$ and $b_r \neq 0$. There exists a proper subgroup H in G with index r coprime with p. It follows that H is transitive, hence one of the following occurs:

1) H is soluble and $|H|$ divides $p(p-1)/2$;
2) $p = (q^n - 1)/(q - 1)$ and H is isomorphic to a subgroup of $\mathrm{P\Gamma L}(n, q)$ containing $\mathrm{PSL}(n, q)$;
3) $p = 11$, and either $H \cong M_{11}$ or $H \cong \mathrm{PSL}(2, 11)$;
4) $p = 23$ and $H \cong M_{23}$.

In all these cases trivial computations show that ξ does not divide $|H|$, hence $r = |G : H|$ is divisible by ξ. This implies that $\alpha_\xi(\alpha_p(P_G(s))) = 1$; moreover, as $\xi > p/2$ we get that ξ^2 does not divide $p!$ thus it does not divide r whenever $b_r \neq 0$. By Lemma 2 we conclude that $\alpha_p(P_G(s))$ is irreducible. □

Now we are ready to prove the main result of this section.

Theorem 12. *Let $p \geq 5$ be a prime, then the Dirichlet polynomial $P_{\mathrm{Alt}(p)}(s)$ is irreducible in R.*

Proof. Set $G = \mathrm{Alt}(p)$. Assume, by contradiction, that $P_G(s)$ is reducible in R. By Lemma 2 we get that $\gcd(\alpha_p(P_G(s)), P_G(s)) \neq 1$. Since, by Lemma 11, $\alpha_p(P_G(s)) = \sum_n b_n/n^s$ is irreducible, we deduce that there exists $Q(s) = \sum_n c_n/n^s \in R$ such that $P_G(s) = \alpha_p(P_G(s))Q(s)$. By Lemma 9 $a_{p(p-1)}(G) \neq 0$. Since

$$a_{p(p-1)}(G) = \sum_{rl=p(p-1)} b_r c_l$$

and noting that $b_r \neq 0$ implies $(r, p) = 1$ and either $r = 1$ or $r > p - 1$, it follows that $a_{p(p-1)}(G) = c_{p(p-1)} \neq 0$. Therefore

$$m = \max\{n \in \mathbb{N} \mid c_n \neq 0\} \geq p(p-1).$$

Since by Lemma 10 we get $k = \max\{n \in \mathbb{N} \mid b_n \neq 0\} \geq (p-2)!$, it follows that

$$a_{mk}(G) = c_m b_k \neq 0.$$

This implies $p! \leq mk \leq |G| = p!/2$, a contradiction. □

Corollary 13. *Let $p \geq 5$ be a prime number and let $f(s) = P_{\mathrm{Alt}(p)}(s)$. Assume that G is a finite group with $P_G(s) = f(s)$. Then $G/\operatorname{Frat} G \cong \mathrm{Alt}(p)$.*

Proof. By Theorem 12, $P_G(s) = f(s)$ is irreducible, hence by Corollary 7, $G/\operatorname{Frat} G$ is a simple group. Moreover the subgroups of index p in $\mathrm{Alt}(p)$ are precisely the point-stabilizers and they are maximal in $\mathrm{Alt}(p)$; hence $0 \neq a_p(\mathrm{Alt}(p)) = a_p(G)$ and this implies that G contains a maximal subgroup H of index p. Since $G/\operatorname{Frat} G$ is simple, we get that $\mathrm{Core}_G(H) = \operatorname{Frat} G$ and $G/\operatorname{Frat} G$ is isomorphic to a transitive subgroup Γ of $\mathrm{Alt}(p)$. Moreover, by Lemma 10, $0 \neq a_{(p-2)!}(\mathrm{Alt}(p)) = a_{(p-2)!}(G) = a_{(p-2)!}(\Gamma)$, thus $|\Gamma|$ is divisible both by $(p-2)!$ and p. So $|\mathrm{Alt}(p) : \Gamma| \leq (p-1)/2$ which implies $\mathrm{Alt}(p) = \Gamma \cong G/\operatorname{Frat} G$. □

Actually, we are able to prove the irreducibility of the Dirichlet polynomials associated with other simple groups. In the following table we resume the list of these simple groups together with the primes that allow us to use Lemma 2 in order to prove the irreducibility of the associated Dirichlet polynomial.

G	Alt(6)	Alt(8)	Alt(9)	Alt(10)	Sz(8)
p	5	7	7	7	13

G	M_{11}	M_{12}	M_{22}	M_{23}	M_{24}	J_1	J_2	J_3	He	McL	Co_3	Hs
p	11	11	11	23	23	19	7	19	17	11	23	11

Hence we have a large list of simple groups such that the associated Dirichlet polynomial is irreducible and one may be inclined to think that this property is shared by all finite simple groups. Actually this fails to be true and in the next section we shall show that the Dirichlet polynomial of a projective linear group $\mathrm{PSL}(2,p)$ is not always irreducible.

5. The projective linear groups PSL(2, p)

Let $p \geq 5$ be a prime number, in this section we shall describe when the Dirichlet polynomial $P_{\mathrm{PSL}(2,p)}(s)$ is reducible in R. Let us recall that the subgroups of $\mathrm{PSL}(2,p)$ are known for any prime p (see [**7**] as a reference). Moreover, in [**5**] P. Hall describes the Möbius function of the lattice of subgroups of $\mathrm{PSL}(2,p)$, furthermore he shows that $\mu_{\mathrm{PSL}(2,p)}$ depends only on the congruence properties of the prime number p modulo 5 and 8 with three exceptions, i.e., $p \in \{5,\ 7,\ 11\}$. We will use also [**3**] as a more recent reference on this subject.

Let us recall that a prime number p is a Mersenne prime if there exists a prime number t such that $p = 2^t - 1$.

Proposition 14. *Let $p \geq 5$ be a prime number which is not a Mersenne prime, then $P_{\mathrm{PSL}(2,p)}(s)$ is irreducible in R.*

Proof. Let p be a prime number and $G = \mathrm{PSL}(2,p)$. If $p = 5$, then $\mathrm{PSL}(2,5) \cong \mathrm{Alt}(5)$ and the conclusion follows from Theorem 12. So we may assume $p > 5$. We find it useful to stress that $a_{\frac{p(p+1)}{2}}(G) \neq 0$. Indeed G has a single conjugacy class of subgroups of order $(p-1)$; moreover if $H \leq G$ and $|H| = (p-1)$, then either H is a maximal subgroup of G or $p = 7, 11$ and $\mu_G(H) = 1$. In addition, let us recall that G has a single conjugacy class of maximal subgroups M such that $(|G : M|, p) = 1$, furthermore M is the normalizer of a Sylow p-subgroup of G and $|G : M| = (p+1)$. Hence if H is a subgroup of G such that $(|G : H|, p) = 1$ and $\mu_G(H) \neq 0$,

then H is a maximal subgroup of G. Thus $a_{(p+1)}(G) = -(p+1)$ and $\alpha_p(P_G(s)) = 1-(p+1)/(p+1)^s$.

Note that by Lemma 3 $\alpha_p(P_G(s)) = 1-(p+1)/(p+1)^s$ is reducible in R if and only if there exist a, $d \in \mathbb{N}$ such that $p+1 = a^d$ and this is equivalent to say that p is a Mersenne prime.

Now assume that p is not a Mersenne prime, it follows that $\alpha_p(P_G(s)) = 1-(p+1)/(p+1)^s$ is irreducible. Since p^2 does not divide $|G|$ and $a_{\frac{p(p+1)}{2}}(G) \neq 0$ then by Lemma 2 we get that $P_G(s)$ is reducible in R if and only if $\alpha_p(P_G(s))$ divides $P_G(s)$. Hence if $P_G(s)$ is reducible, then there exists $B(s) = \sum_n b_n/n^s \in R$ such that $P_G(s) = (1-(p+1)/(p+1)^s)B(s)$ and $b_{\frac{p(p+1)}{2}} = a_{\frac{p(p+1)}{2}}(G) \neq 0$. Then if we take $m = \max\{n \in \mathbb{N} \mid b_n \neq 0\}$, we obtain a contradiction as $a_{m(p+1)}(G) = -(p+1)b_m \neq 0$ but $m(p+1) \geq p(p+1)^2/2 > |G| = p(p^2-1)/2$ thus $a_{m(p+1)}(G) = 0$. Hence $P_G(s)$ is irreducible. □

Now we shall discuss the reducibility of $P_{\mathrm{PSL}(2,p)}(s)$ when p is a Mersenne prime, $p = 2^t - 1$ being t a prime number. It is easy to show that either $t = 1 \mod 4$ and $p = 1 \mod 5$ or $t = 3 \mod 4$ and $p = 2 \mod 5$.

Proposition 15. *Let $p = 2^t - 1$ be a Mersenne prime, then $P_{\mathrm{PSL}(2,p)}(s)$ is reducible in R if and only if $t = 3 \mod 4$.*

Proof. By using [**3**] we are able to write down the Dirichlet polynomial associated with $\mathrm{PSL}(2,p)$ for any Mersenne prime p. Set $G = \mathrm{PSL}(2,p)$, $q = \frac{1}{2}(p-1) = 2^{t-1}-1$, $r = \frac{1}{2}(p+1) = 2^{t-1}$, $g = 2pqr = |G| = (2^t-1)(2^{t-1}-1)2^t$.

Let $t = 3 \mod 4$.

If $p = 7$, then

$$\begin{aligned} P_G(s) &= 1 - \frac{8}{8^s} - \frac{14}{7^s} + \frac{21}{21^s} + \frac{28}{28^s} + \frac{56}{56^s} - \frac{84}{84^s} \\ &= \left(1 - \frac{2}{2^s}\right)\left(1 + \frac{2}{2^s} + \frac{4}{4^s} - \frac{14}{7^s} - \frac{28}{14^s} - \frac{28}{28^s} + \frac{21}{21^s} + \frac{42}{42^s}\right); \end{aligned}$$

hence it is reducible in R.

If $p \neq 7$, then we get

$$\begin{aligned} P_G(s) = 1 &- \frac{pq}{(pq)^s} - \frac{pr}{(pr)^s} - \frac{2r}{(2r)^s} + \frac{2pr}{(2pr)^s} \\ &- \frac{g/12}{(g/24)^s} + \frac{g/4}{(g/8)^s} + \frac{g/3}{(g/6)^s} - \frac{g/2}{(g/2)^s}. \end{aligned}$$

Set $f = q/3$, then

$$\begin{aligned}P_G(s) &= 1 - \frac{2^t}{2^{ts}}\left(1 - \frac{p}{p^s}\right) - \frac{2^{t-1}}{(2^{t-1})^s}\left(\frac{p}{p^s} - \frac{2pf}{(pf)^s} + \frac{3pf}{(3pf)^s}\right)\\ &\quad - \frac{2^{t-2}}{(2^{t-3})^s}\left(\frac{pf}{(pf)^s} - \frac{3pf}{(3pf)^s}\right) - \frac{3pf}{(3pf)^s}\\ &= \left(1 - \frac{2}{2^s}\right)\cdot\left(\frac{2^{t-1}}{(2^{t-1})^s}\left(1 - \frac{p}{p^s}\right)\right.\\ &\quad + \left(\frac{2^{t-2}}{(2^{t-2})^s} + \frac{2^{t-3}}{(2^{t-3})^s}\right)\left(1 - \frac{2pf}{(pf)^s} + \frac{3pf}{(3pf)^s}\right)\\ &\quad \left. + \left(1 + \frac{2}{2^s} + \cdots + \frac{2^{t-4}}{(2^{t-4})^s}\right)\left(1 - \frac{3pf}{(3pf)^s}\right)\right).\end{aligned}$$

Hence if $t = 3 \mod 4$, then $P_G(s)$ is reducible.

Let $t = 1 \mod 4$, we shall show that $P_G(s)$ is irreducible in R.

$$\begin{aligned}P_G(s) &= 1 - \frac{pq}{(pq)^s} - \frac{pr}{(pr)^s} - \frac{2r}{(2r)^s} + \frac{2pr}{(2pr)^s} - \frac{g/30}{(g/60)^s}\\ &\quad - \frac{g/12}{(g/24)^s} + \frac{g/6}{(g/12)^s} + \frac{g/5}{(g/10)^s} + \frac{g/4}{(g/8)^s} + \frac{2g/3}{(g/6)^s}\\ &\quad - \frac{2g/3}{(g/3)^s} - \frac{5g/2}{(g/2)^s} + \frac{2g}{g^s}.\end{aligned}$$

By using Lemma 2 we get that $P_G(s)$ is reducible in R if and only if $\gcd(\alpha_p(P_G(s)), P_G(s)) \neq 1$. Observe that here we obtain $\alpha_p(P_G(s)) = 1 - \frac{2r}{(2r)^s} = \left(1 - \frac{2}{2^s}\right)\left(\sum_{j=0}^{t-1}\frac{2^j}{(2^j)^s}\right)$. Note that $\sum_{j=0}^{t-1}\frac{2^j}{(2^j)^s}$ is irreducible in R as $\phi\left(\sum_{j=0}^{t-1}\frac{2^j}{(2^j)^s}\right) = \sum_{j=0}^{t-1}(2x_2)^j$ is irreducible in $\mathbb{Z}[x_2]$ being t a prime number. Thus $P_G(s)$ is reducible in R if and only if it is divisible either by $(1 - \frac{2}{2^s})$ or by $\sum_{j=0}^{t-1}\frac{2^j}{(2^j)^s}$. By using the decomposition we found in the previous case we get:

$$\begin{aligned}P_G(s) &= \left(1 - \frac{2}{2^s}\right)\cdot\left(\frac{2^{t-1}}{(2^{t-1})^s}\left(1 - \frac{p}{p^s}\right)\right.\\ &\quad + \left(\frac{2^{t-2}}{(2^{t-2})^s} + \frac{2^{t-3}}{(2^{t-3})^s}\right)\left(1 - \frac{2pf}{(pf)^s} + \frac{3pf}{(3pf)^s}\right)\\ &\quad \left. + \left(1 + \frac{2}{2^s} + \cdots + \frac{2^{t-4}}{(2^{t-4})^s}\right)\left(1 - \frac{3pf}{(3pf)^s}\right)\right)\\ &\quad - \frac{g/30}{(g/60)^s}\left(1 - \frac{5}{5^s} - \frac{6}{6^s} - \frac{10}{10^s} + \frac{20}{20^s} + \frac{60}{30^s} - \frac{60}{60^s}\right).\end{aligned}$$

Since $\left(1-\frac{5}{5^s}-\frac{6}{6^s}-\frac{10}{10^s}+\frac{20}{20^s}+\frac{60}{30^s}-\frac{60}{60^s}\right)$ is not divisible by $\left(1-\frac{2}{2^s}\right)$ we get that $\left(1-\frac{2}{2^s}\right)$ does not divide $P_G(s)$.

It remains to prove that $Q(s)=\sum_{j=0}^{t-1}\frac{2^j}{(2^j)^s}$ does not divide $P_G(s)$. Let $\{p_1,\dots,p_l\}$ be the set of prime divisors of q and consider $\beta=\alpha_{p_1}\cdot\dots\cdot\alpha_{p_l}$. If $Q(s)$ divides $P_G(s)$, then $Q(s)=\beta(Q(s))$ divides

$$\beta(P_G(s))=1-\frac{2^t}{(2^t)^s}+\frac{2^{t-2}p}{(2^{t-2}p)^s}\left(\frac{4}{4^s}-\frac{2}{2^s}-\beta\left(\frac{2q/15}{(q/15)^s}\right)\right)$$

and this is false. □

Proposition 16. *Let $p\geq 5$ be a prime number and let $f(s)=P_{\mathrm{PSL}(2,p)}(s)$. Assume that G is a finite group with $P_G(s)=f(s)$. Then $G/\operatorname{Frat}G$ is simple.*

Proof. Notice that, by Propositions 14, 15, $f(s)$ is irreducible, except for $p=2^t-1$ and $t=3 \mod 4$. Furthermore, by Corollary 7, $f(s)$ irreducible implies $G/\operatorname{Frat}G$ simple. So we reduce to consider p to be a Mersenne prime, where $p=2^t-1$ with $t=3 \mod 4$. From the proof of the previous theorem, we get

$$f(s)=P_{\mathrm{PSL}(2,p)}(s)=\left(1-\frac{2}{2^s}\right)h(s) \tag{5.1}$$

being $h(s)$ irreducible in R. Let N be a normal subgroup of G and assume by contradiction that $\operatorname{Frat}G<N<G$. By Lemma 6, $f(s)$ has a nontrivial factorization

$$f(s)=P_G(s)=P_{G/N}(s)P_{G,N}(s). \tag{5.2}$$

By comparing (5.1) and (5.2), either $P_{G/N}(s)$ or $P_{G,N}(s)$ coincides with $1-2/2^s$. By Lemma 8, we get $0<f(t)<1-2/2^t$ when $t\in\mathbb{N}$ is large enough.

In particular

$$\lim_{t\to\infty}\left(1-\frac{2}{2^t}-f(t)\right)=\lim_{t\to\infty}\left(-\frac{2}{2^t}-\sum_{n\geq 2}\frac{a_n(\mathrm{PSL}(2,p))}{n^t}\right)>0.$$

On the other hand, since $a_2(\mathrm{PSL}(2,p))=0$,

$$\lim_{t\to\infty}\left(-\frac{2}{2^t}-\sum_{n\geq 2}\frac{a_n(\mathrm{PSL}(2,p))}{n^t}\right)=\lim_{t\to\infty}\left(-\frac{2}{2^t}-\sum_{n\geq 3}\frac{a_n(\mathrm{PSL}(2,p))}{n^t}\right)<0,$$

a contradiction. □

References

[1] N. Boston, *A probabilistic generalization of the Riemann zeta function*, Analytic number theory, Vol. 1 (Allerton Park, IL, 1995), Progr. Math., **138**, Birkhäuser, Boston, 1996, 155-162, MR 1399336, Zbl 0853.11075.

[2] K.S. Brown, *The coset poset and probabilistic zeta function of a finite group*, J. Algebra, **225**(**2**) (2000), 989-1012, MR 1741574, Zbl 0973.20016.

[3] F. Dalla Volta, A. Lucchini and F. Morini, *Some remarks on the probability of generating an almost simple group*, Glasgow Math. J., **45** (2003), 281-291, MR 1997706.

[4] J.D. Dixon and B. Mortimer, *Permutation Groups*, Graduate Texts in Mathematics, **163**, Springer-Verlag, New York, 1996, MR 1409812, Zbl 0951.20001.

[5] Ph. Hall, *The Eulerian functions of a group*, Quart. J. Math., **7** (1936), 134-151, Zbl 0014.10402.

[6] G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers*, fifth ed., The Clarendon Press Oxford University Press, New York, 1979, MR 0568909, Zbl 0423.10001.

[7] B. Huppert, *Endliche Gruppen*, I, Die Grundlehren der Mathematischen Wissenschaften, Band 134, Springer-Verlag, Berlin, 1967, MR 0224703, Zbl 0217.07201.

[8] S. Lang, *Algebra*, third ed., Graduate Texts in Mathematics, **211**, Springer-Verlag, New York, 2002, MR 1878556, Zbl 0984.00001.

[9] A. Mann, *Positively finitely generated groups*, Forum Math., **8**(**4**) (1996), 429-459, MR 1393323, Zbl 0852.20019.

[10] P.P. Pálfy, *On Feit's examples of intervals in subgroup lattices*, J. Algebra, **116**(**2**) (1988), 471-479, MR 0953164, Zbl 0651.20028.

Received August 7, 2003.

Dipartimento di Matematica
Università di Brescia
Via Valotti 9, 25133 Brescia
Italy
E-mail address: erika.damian@ing.unibs.it

Dipartimento di Matematica
Università di Brescia
Via Valotti 9, 25133 Brescia
Italy
E-mail address: andrea.lucchini@ing.unibs.it

Dipartimento di Matematica
Università di Brescia
Via Valotti 9, 25133 Brescia
Italy
E-mail address: morini@ing.unibs.it