The handle http://hdl.handle.net/1887/20880 holds various files of this Leiden University dissertation.

**Author:** Duong, Hoang Dung  
**Title:** Profinite groups with a rational probabilistic zeta function  
**Issue Date:** 2013-05-14
Chapter 4

Linear groups of dimension two

This chapter is devoted for a proof of Theorem B as the following.

Theorem B. Let \( G \) be a finitely generated profinite group such that almost every nonabelian composition factor is isomorphic to \( \text{PSL}(2, p) \) for some prime \( p \geq 5 \). Then \( P_G(s) \) is rational only if \( G/\text{Frat}(G) \) is finite.

4.1 Maximal subgroups of \( \text{PSL}(2, q) \)

Let \( X \) be an almost simple group with socle \( S \cong \text{PSL}(2, q) \) where \( q \geq 5 \) is a prime. Since \( \text{Aut}(S) = \text{PGL}(2, q) \) and \( |\text{PGL}(2, q) : \text{PSL}(2, q)| = 2 \), either \( X = \text{PSL}(2, q) \) or \( X = \text{PGL}(2, q) \). We will now look for the smallest index of maximal subgroups supplementing \( S \) in \( X \) that is divisible by \( q \) and not divisible by 2.

Theorem 4.1.1 \( (\text{Dic58}) \). Let \( X = \text{PGL}(2, q) \) with \( q \geq 5 \) a prime. Then the maximal subgroups of \( X \) not containing \( \text{PSL}(2, q) \) are

\[(a) \ C_q \rtimes C_{q-1}; \]
\[(b) \ D_{2(q-1)} \text{ for } q \neq 5; \]
\[(c) \ D_{2(q+1)}; \]
\[(d) \ Sym(4) \text{ for } q \equiv \pm 3 \mod 8. \]
We list those maximal subgroups of $\text{PGL}(2, q)$ and their indices in the following table:

<table>
<thead>
<tr>
<th>maximal subgroup</th>
<th>order</th>
<th>index</th>
</tr>
</thead>
<tbody>
<tr>
<td>$C_q \rtimes C_{q-1}$</td>
<td>$q(q - 1)$</td>
<td>$q + 1$</td>
</tr>
<tr>
<td>$D_{2(q-1)}$, $q \neq 5$</td>
<td>$2(q - 1)$</td>
<td>$q(q + 1)/2$</td>
</tr>
<tr>
<td>$D_{2(q+1)}$</td>
<td>$2(q + 1)$</td>
<td>$q(q - 1)/2$</td>
</tr>
<tr>
<td>$\text{Sym}(4)$, $q \equiv \pm 3 \mod 8$</td>
<td>$4!$</td>
<td>$q(q^2 - 1)/4!$</td>
</tr>
</tbody>
</table>

Table 4.1: Maximal subgroups of $\text{PGL}(2, q)$

We consider indices divisible by $q$.

- Assume that $q(q - 1)/2$ is odd. If there exists a maximal subgroup $M$ such that $|\text{PGL}(2, q) : M|$ is odd and smaller than $q(q - 1)/2$, then $M \cong \text{Sym}(4)$. In this case, $q \equiv \pm 3 \mod 8$, and we have
  \[
  \frac{q(q^2 - 1)}{4!} < \frac{q(q - 1)}{2} \iff q < 11
  \]
  so $q = 5$. For $q = 5$, we have $q(q^2 - 1)/4! = 5$, while $q(q - 1)/2 = 10$ and $q(q + 1)/2 = 15$.

- Assume now that $q(q + 1)/2$ is odd. If there exists a maximal subgroup $M$ such that $|\text{PGL}(2, q) : M|$ is odd and smaller than $q(q - 1)/2$, then $M \cong \text{Sym}(4)$. Also in this case, $q \equiv \pm 3 \mod 8$, and we have
  \[
  \frac{q(q^2 - 1)}{4!} < \frac{q(q + 1)}{2} \iff q < 12
  \]
  The candidates are $q = 5 \equiv 1 \mod 4$ and $q = 11 \equiv 3 \mod 4$. The case $q = 5$ was already eliminated above. In the case $q = 11$, we choose index $q(q - 1)/2 = 55$ which is not divisible by 2.

**Theorem 4.1.2 ([Dic58]).** Let $X = \text{PSL}(2, q)$ with $q \geq 5$ a prime. Then the maximal subgroups of $X$ are the following

(a) $C_q \rtimes C_{q-1}$;

(b) $D_{q-1}$ for $q \geq 13$;
(c) $D_{q+1}$ for $q \neq 7, 9$;

(d) $\text{Sym}(4)$ for $q \equiv \pm 1 \mod 8$;

(e) $\text{Alt}(4)$ for $q \equiv \pm 3 \mod 10$

(f) $\text{Alt}(5)$ for $q \equiv \pm 1 \mod 10$.

We have a table of maximal subgroups of $\text{PSL}(2, q)$ and their indices as follows.

<table>
<thead>
<tr>
<th>maximal subgroup $M$</th>
<th>order</th>
<th>index</th>
</tr>
</thead>
<tbody>
<tr>
<td>$C_q \rtimes C_{q-1}$</td>
<td>$q(q-1)$</td>
<td>$q+1$</td>
</tr>
<tr>
<td>$D_{(q-1)}, q \geq 13$</td>
<td>$2(q-1)$</td>
<td>$q(q+1)/2$</td>
</tr>
<tr>
<td>$D_{(q+1)}, q \neq 7, 9$</td>
<td>$2(q+1)$</td>
<td>$q(q-1)/2$</td>
</tr>
<tr>
<td>$\text{Sym}(4), q \equiv \pm 1 \mod 8$</td>
<td>$4!$</td>
<td>$q(q^2 - 1)/2.4!$</td>
</tr>
<tr>
<td>$\text{Alt}(4), q \equiv \pm 3 \mod 10 &amp; q \neq \pm 1 \mod 10$</td>
<td>$4!/2$</td>
<td>$q(q^2 - 1)/4!$</td>
</tr>
<tr>
<td>$\text{Alt}(5), q \equiv \pm 1 \mod 10$</td>
<td>$5!/2$</td>
<td>$q(q^2 - 1)/5!$</td>
</tr>
</tbody>
</table>

Table 4.2: Maximal subgroups of $\text{PSL}(2, q)$

We look for the smallest odd integer divisible by $q$ which is the index of a maximal subgroup $M$ of $\text{PSL}(2, q)$. We have two cases:

(a) If $q(q-1)/2$ is odd, then either $|\text{PSL}(2, q) : M| = q(q-1)/2$ or one of the following cases occurs:

In case $M = \text{Alt}(4)$ with $q \equiv \pm 3 \mod 10$, we have

$$\frac{q(q^2-1)}{4!} < \frac{q(q-1)}{2} \iff q < 11.$$ 

The only candidate is $q = 5 \equiv 1 \mod 4$. For $q = 5$ we have $q(q^2-1)/4! = 5$, while $q(q-1)/2 = 10$, and $q(q+1)/2 = 15$.

In case $M = \text{Sym}(4)$ with $q \equiv \pm 1 \mod 8$, we have

$$\frac{q(q^2-1)}{2.4!} < \frac{q(q-1)}{2} \iff q < 23.$$ 

The only candidate is $q = 7 \equiv 3 \mod 4$. For $q = 7$ we have $q(q^2-1)/2.4! = 7$, while $q(q-1)/2 = 21$. 

81
In case $M = \text{Alt}(5)$ with $q \equiv \pm 1 \mod 10$, we have
\[
\frac{q(q^2 - 1)}{5!} < \frac{q(q - 1)}{2} \iff q < 59.
\]
The candidates are $q = 11 \equiv 3 \mod 4$, $q = 19 \equiv 3 \mod 4$, $q = 29 \equiv 1 \mod 4$, $q = 31 \equiv 3 \mod 4$, $q = 41 \equiv 1 \mod 4$, $q = 49 \equiv 1 \mod 4$.

For $q = 11$ we have $q(q^2 - 1)/5! = 11$ while $q(q - 1)/2 = 55$.
For $q = 19$ we have $q(q^2 - 1)/5! = 19 \cdot 3$ while $q(q - 1)/2 = 19 \cdot 9$.
For $q = 29$ we have $q(q^2 - 1)/5! = 29 \cdot 7$ while $q(q - 1)/2 = 29 \cdot 14$.
For $q = 31$ we have $q(q^2 - 1)/5! = 31 \cdot 8$ while $q(q - 1)/2 = 31 \cdot 15$.
For $q = 41$ we have $q(q^2 - 1)/5! = 41 \cdot 14$ while $q(q - 1)/2 = 41 \cdot 20$.
For $q = 49$ we have $q(q^2 - 1)/5! = 49 \cdot 20$ while $q(q - 1)/2 = 49 \cdot 24$.

(b) If $q(q + 1)/2$ is odd, then, similarly, either $|\text{PSL}(2, q) : M| = q(q + 1)/2$ or one of the following cases occurs:

In case $M = \text{Alt}(4)$ with $q \equiv \pm 3 \mod 10$ and $q \not\equiv \pm 1 \mod 10$, we have
\[
\frac{q(q^2 - 1)}{4!} < \frac{q(q + 1)}{2} \iff q < 13.
\]
Candidates are $q = 5 \equiv 1 \mod 4$ and $q = 11 \equiv 3 \mod 4$ which are already eliminated above.

In case $M = \text{Sym}(4)$ with $q \equiv \pm 1 \mod 8$, we have
\[
\frac{q(q^2 - 1)}{2.4!} < \frac{q(q + 1)}{2} \iff q < 25.
\]
The remaining candidate is $q = 23 \equiv 3 \mod 4$. But in this case, we choose $q(q - 1)/2 = 23 \cdot 11$ instead of $q(q + 1)/2 = 23 \cdot 12$.

In case $M = \text{Alt}(5)$ with $q \equiv \pm 1 \mod 10$, we have
\[
\frac{q(q^2 - 1)}{5!} < \frac{q(q + 1)}{2} \iff q < 61.
\]
The remaining candidate is $q = 59 \equiv 3 \mod 4$. Again, in this case, we choose $q(q - 1)/2 = 59 \cdot 29$ instead of $q(q + 1)/2 = 59 \cdot 30$. 

82
Theorem 4.1.3. Let $L$ be a monolithic primitive group with $\text{soc}(L) = (\text{PSL}(2,q))^r$ for some prime $q \geq 5$, and $X$ the associated almost simple group. Define $w$ as follows:

$$w = w(X) = \begin{cases} \frac{q(q - 1)}{2} & \text{if } q \equiv 3 \mod 4 \text{ and } q \not\in \{5, 7, 11, 19, 29\}, \\ \frac{q(q + 1)}{2} & \text{if } q \equiv 1 \mod 4 \text{ and } q \not\in \{5, 7, 11, 19, 29\}, \\ 5 & \text{if } q = 5, \\ 7 & \text{if } q = 7 \text{ and } X = \text{PSL}(2,7), \\ 3 \cdot 7 & \text{if } q = 7 \text{ and } X = \text{PGL}(2,7), \\ 11 & \text{if } q = 11 \text{ and } X = \text{PSL}(2,11), \\ 11 \cdot 5 & \text{if } q = 11 \text{ and } X = \text{PGL}(2,11), \\ 19 \cdot 3 & \text{if } q = 19 \text{ and } X = \text{PSL}(2,19), \\ 19 \cdot 3^2 & \text{if } q = 19 \text{ and } X = \text{PGL}(2,19), \\ 29 \cdot 7 & \text{if } q = 29 \text{ and } X = \text{PSL}(2,29), \\ 29 \cdot 3 \cdot 5 & \text{if } q = 29 \text{ and } X = \text{PGL}(2,29). \end{cases}$$

Then $b_{w^r} < 0$ and $w^r$ is the smallest odd $q$-useful index in $L$.

4.2 The main result

In this section, we give a proof for Theorem B. In this proof, we consider a finitely generated profinite group $G$ such that $P_G(s)$ is rational and that there is an open normal subgroup $H$ of which every composition factor is either cyclic or isomorphic to a group $\text{PSL}(2,p)$ for some prime $p \geq 5$.

We fix a descending normal series $\{G_i\}$ of $G$ with the properties that $\bigcap G_i = 1$ and $G_i/G_{i+1}$ is a chief factor of $G/G_{i+1}$. Let $J$ be the set of indices $i$ with $G_i/G_{i+1}$ non-Frattini. Then by Section 2.1 the probabilistic zeta function $P_G(s)$ can be factorized as

$$P_G(s) = \prod_{i \in J} P_i(s)$$

where for each $i$, the finite Dirichlet series $P_i(s) = \sum_n b_{i,n}/n^s$ is associated to the chief factor $G_i/G_{i+1}$. We have the the following crucial result.

Proposition 4.2.1. The set $\pi(G)$ is finite.

Proof. Let $\Gamma$ be the set of simple groups that appear as composition factors in non-Frattini chief factors of $G$, that is, the set of simple groups $S_i$ for $i \in J$. Since $P_G(s)$ is rational, the set $\pi(P_G(s))$ is finite. Therefore, it follows from Lemma 2.6.1 that $\Gamma$ contains only finitely
many abelian groups. Assume by contradiction that $\Gamma$ is infinite. By our assumption, the subset $\Gamma^*$ of the simple groups in $\Gamma$ that are isomorphic to $\text{PSL}(2, p)$ for some prime $p$ is infinite. Let

$$I := \{ j \in J \ | \ S_j \in \Gamma^* \}, \ A(s) := \prod_{i \in I} P_i(s) \text{ and } B(s) := \prod_{i \notin I} P_i(s).$$

Notice that $\pi(B(s)) \subseteq \bigcup_{\Gamma \setminus \Gamma^*} \pi(S)$ is a finite set. Since $P_G(s) = A(s)B(s)$ and $\pi(P_G(s))$ is finite, it follows that the set $\pi(A(s))$ is finite. In particular, there exists a prime number $q \geq 5$ such that $q \notin \pi(A(s))$ but $\text{PSL}(2, q) \in \Gamma^*$. Let $\Lambda$ be the set of the odd integers $n$ divisible by $q$ but not divisible by any prime strictly greater than $q$ and set

$$r := \min\{ r_i \ | \ S_i = \text{PSL}(2, q) \},$$

$$I^* := \{ i \in I \ | \ S_i = \text{PSL}(2, q) \text{ and } r_i = r \},$$

$$w := \min\{ w(X_i) \ | \ S_i = \text{PSL}(2, q) \text{ and } r_i = r \},$$

$$\alpha := \min\{ n > 1 \ | \ n \in \Lambda, v_q(n) = r \text{ and } b_{i,n} \neq 0 \text{ for some } i \in I \}.$$

Assume $i \in I$, $n \in \Lambda$ and $b_{i,n} \neq 0$. We have that $S_i \cong \text{PSL}(2, q_i)$ for a suitable prime $q_i$. Since $b_{i,n} \neq 0$, there is a subgroup $H \leq L_i$ such that $L_i = H \cdot \text{soc}(L_i)$ and $n = [L_i : H]$. Hence $n = |L_i : H| = |\text{soc}(L_i) : \text{soc}(L_i) \cap H|$. Since $q \mid n$, and $q$ is the largest prime divisor of $|S_i| = |\text{PSL}(2, q_i)| = q_i(q_i^2 - 1)/2$, we get that $q_i \geq q$. Since $\alpha$ is an odd useful index for $L_i$, we have by Lemma 2.2.6 that $n = x^q$, where $x$ is an odd useful index for the almost simple group $X_i$ where $\text{soc}(X_i) = S_i = \text{PSL}(2, q_i)$. So, there is a maximal subgroup of $X_i$, which supplements $S_i$, of odd index $x'$ dividing $x$. If $q_i > q$, then $q_i$ does not divide $n$ by definition of $n \in \Lambda$, so $x'$ is not divisible by $q_i$. It means that $X_i$ has a maximal subgroup of odd index divisible by $q$ and not divisible by $q_i$, which contradicts the tables we have above. Hence $q_i = q$. It follows that $\alpha = w^r$ and $b_{i,0} \neq 0$ if and only if $i \in I^*$ and $w(X_i) = w$; moreover in the last case $b_{i,0} < 0$. Hence the coefficient $c_\alpha$ of $1/c_\alpha$ in $A(s)$ is

$$c_\alpha = \sum_{i \in I^*, w(X_i) = w} b_{i,0} < 0.$$ 

This implies that $q \in \pi(A(s))$, which is a contradiction. Thus $\Gamma^*$, and hence $\Gamma$, is finite.

By Corollary 2.6.2, it follows that $\pi(G)$ is also finite. □

**Proof of Theorem B.** Assume that $P_G(s) = \prod_{i \in J} P_i(s)$ where $J$ is the set of indices $i$ such that $G_i/G_{i+1}$ is non-Frattini. Let $\mathcal{T}$ be the set of almost simple groups $X$ such that there
exist infinitely many $i \in J$ with $X_i \cong X$ and let $I$ be the set of indices $i \in J$ such that $X_i \in \mathcal{T}$. By Proposition 2.6.3, the set $J \setminus I$ is finite. We have to prove that $J$ is finite; this is equivalent to show that $I = \emptyset$. Assume that $I \neq \emptyset$ and let $i \in I$. By the hypothesis of Theorem B, there exists a prime $q_i$ such that $S_i \in \{C_{q_i}, \text{PSL}(2, q_i)\}$. Set $q = \max\{q_i : i \in I\}$ and let $\Lambda$ be the set of odd integers $n$ divisible by $q$. Assume $n \in \Lambda$ and $b_i, n \neq 0$ for some $i \in I$. If $S_i$ is cyclic, then $P_i(s) = 1 - c_n/n^s$ where $n = |G_i/G_{i+1}| = q_i^{r_i}$ and $c_n$ is the number of complements of $G_i/G_{i+1}$ in $G/G_{i+1}$. This implies $q = q_i$ and $v_q(n) = r_i$.

If $S_i = \text{PSL}(2, q_i)$, then by the proof of Proposition 4.2.1, we have $q_i \geq q$, and by the maximality of $q$, we obtain that $q_i = q$. In addition, $n$ is an odd useful index for $L_i$, so, by Lemma 2.2.6, we have $n = x_i^{r_i}$, where $x_i$ is an odd useful index of a subgroup $Y_i$ supplementing $S_i$ in the almost simple group $X_i$ with $\text{soc}(X_i) = S_i$. Since $q|n = x_i^{r_i}$, then $q|x_i$, so $v_q(x_i) \geq 1$. Since $q_i = q$ and $q_i^2$ does not divide the order of $X_i$, we obtain $v_q(x_i) = 1$, hence $v_q(n) = r_i$. Let

$$w = \min\{x \in \Lambda | v_q(x) = 1 \text{ and } b_i x_i \neq 0 \text{ for some } i \in I\}.$$ 

Since $J \setminus I$ is finite and $P_G(s) = \prod_{i \in J} P_i(s)$ is rational, also $\prod_{i \in I} P_i(s)$ is rational. This implies by Lemma 1.2.5 that the product $Q(s) = \prod_{i} P_i^{(2)}(s)$ is also rational. Let $I^* = \{i \in I \mid b_i w_i \neq 0\}$. By the above considerations and Theorem 4.1.3, we have $i \in I^*$ if and only if either $S_i \cong C_q$ and $w = q$ or $\text{soc}(X_i) = \text{PSL}(2, q)$ and $w_i = w$. In particular, if $i \in I^*$ then there exist infinitely many $j \in I$ with $X_j \cong X_j$ and all of them are in $I^*$, hence $I^*$ is an infinite set. Moreover, $b_i w_i < 0$ for every $i \in I^*$, and therefore applying Proposition 2.4.3 to the Dirichlet series $Q(s)$, we deduce that the product

$$H(s) = \prod_{i \in I} \left(1 + \frac{b_i w_i}{w r_i s}\right) = \prod_{i \in I^*} \left(1 + \frac{b_i w_i}{w r_i s}\right)$$

is rational. By Corollary 2.5.5, the set $I^*$ must be finite, a contradiction. \qed