

## ON A THEOREM OF JORDAN

JEAN-PIERRE SERRE

ABSTRACT. The theorem of Jordan which I want to discuss here dates from 1872. It is an elementary result on finite groups of permutations. I shall first present its translations in Number Theory and Topology.

### 1. STATEMENTS

**1.1. Number theory.** Let  $f = \sum_{m=0}^n a_m x^m$  be a polynomial of degree  $n$ , with coefficients in  $\mathbf{Z}$ . If  $p$  is prime, let  $N_p(f)$  be the number of zeros of  $f$  in  $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ .

**Theorem 1.** *Assume*

- (i)  $n \geq 2$ ,
- (ii)  $f$  is irreducible in  $\mathbf{Q}[x]$ .

*Then*

- (a) *There are infinitely many  $p$ 's with  $N_p(f) = 0$ .*
- (b) *The set  $P_0(f)$  of  $p$ 's with  $N_p(f) = 0$  has a density  $c_0 = c_0(f)$  which is  $> 0$ .*

[Recall that a subset  $P$  of the set of primes has density  $c$  if

$$\lim_{X \rightarrow \infty} \frac{\text{number of } p \in P \text{ with } p \leq X}{\pi(X)} = c,$$

where  $\pi(X)$  is as usual the number of primes  $\leq X$ .]

Moreover,

**Theorem 2.** *With the notation of Theorem 1, one has  $c_0(f) \geq \frac{1}{n}$ , with strict inequality if  $n$  is not a power of a prime.*

**Example.** Let  $f = x^2 + 1$ . One has  $p \in P_0(f)$  if and only if  $p \equiv -1 \pmod{4}$ ; this set is well-known to have density  $1/2$ . We shall see more interesting examples in §5.

**1.2. Topology.** Let  $\mathbf{S}_1$  be a circle.

Let  $f : T \rightarrow S$  be a finite covering of a topological space  $S$ . Assume:

- (i)  $f$  has degree  $n$  (i.e. every fiber of  $f$  has  $n$  elements), with  $n \geq 2$ ,
- (ii)  $T$  is arcwise connected and not empty.

**Theorem 3.** *There exists a continuous map  $\varphi : \mathbf{S}_1 \rightarrow S$  which cannot be lifted to the covering  $T$  (i.e. there does not exist any continuous map  $\psi : \mathbf{S}_1 \rightarrow T$  such that  $\varphi = f \circ \psi$ ).*

---

Received by the editors March 1, 2003.

2000 *Mathematics Subject Classification.* Primary 06-XX, 11-XX, 11F11.

This text first appeared in *Math Medley* **29** (2002), 3–18. The writing was done with the help of Heng Huat Chan. ©2002 Singapore Mathematical Society. Reprinted with permission.

**1.3. Finite groups.** Let  $G$  be a group acting on a finite set  $X$ . Put  $n = |X|$ .<sup>1</sup>

**Theorem 4** (Jordan [9]). *Assume that*

- (i)  $n \geq 2$ ,
- (ii)  $G$  acts transitively on  $X$ .

*Then there exists  $g \in G$  which acts on  $X$  without fixed point.*

Assume that  $G$  is finite (which is the case if  $G$  acts faithfully on  $X$ ). Let  $G_0$  be the set of  $g \in G$  with no fixed point. Call  $c_0$  the ratio  $\frac{|G_0|}{|G|}$ .

**Theorem 5** (Cameron-Cohen [4]). *One has  $c_0 \geq \frac{1}{n}$ . Moreover, if  $n$  is not a power of a prime,  $c_0 > \frac{1}{n}$ .*

## 2. PROOFS OF THE GROUP THEORETICAL STATEMENTS

**2.1. Burnside's Lemma.** Let  $G$  be a finite group acting on a finite set  $X$ . If  $g \in G$ , let  $\chi(g)$  be the number of fixed points of  $g$  on  $X$ , i.e.  $\chi(g) = |X^g|$ .

**Burnside's Lemma** (cf. [6, §4.2], [3, §145]). *The number of orbits of  $G$  in  $X$  is equal to*

$$\langle \chi, 1 \rangle = \frac{1}{|G|} \sum_{g \in G} \chi(g) = \int \chi.$$

(If  $\varphi$  is a function on  $G$ , and  $S$  is a subset of  $G$ , we denote by  $\int_S \varphi$  the number  $\frac{1}{|G|} \sum_{g \in S} \varphi(g)$ . When  $S = G$ , we write  $\int \varphi$  instead of  $\int_G \varphi$ .)

By decomposing  $X$  into orbits, it is enough to prove the lemma for  $X \neq \emptyset$  and  $G$  transitive on  $X$ , i.e.  $X \simeq G/H$  for some subgroup  $H$  of  $G$ .

We give three proofs, in different styles.

*First Proof: "Analytic Number Theory Style".*

$$\begin{aligned} \sum_{g \in G} \chi(g) &= \sum_{g \in G} \sum_{\substack{x \in X \\ g \cdot x = x}} 1 \\ &= \sum_{x \in X} \sum_{\substack{g \in G \\ g \cdot x = x}} 1 \\ &= \sum_{x \in X} |H| = |H| \cdot |X| = |G|. \end{aligned}$$

*Second Proof: "Combinatorics Style".* Let  $\Omega \subset G \times X$  be the set of pairs  $(g, x)$  with  $g \cdot x = x$ . We compute  $|\Omega|$  by projecting on each factor. In the projection  $\Omega \rightarrow G$ , the fiber of  $g \in G$  has  $\chi(g)$  elements and hence

$$|\Omega| = \sum_{g \in G} \chi(g).$$

On the other hand, in the projection  $\Omega \rightarrow X$ , the fiber of  $x \in X$  is a conjugate of  $H$  and hence

$$|\Omega| = \sum_{x \in X} |H| = |H| \cdot |G/H| = |G|.$$

---

<sup>1</sup>If  $S$  is a finite set, we denote by  $|S|$  the number of elements of  $S$ .

*Third Proof: "Algebra Style".* The function  $\chi$  is the character of the permutation representation defined by  $X$ . Hence,  $\langle \chi, 1 \rangle$  is the dimension of the space of  $G$ -invariant elements of that representation, which is obviously 1.

## 2.2. Proof of Theorem 5.

**Lemma.**  $\int \chi^2 \geq 2$ .

*First Proof (by Burnside's Lemma).* If  $g \in G$ ,  $\chi^2(g)$  is the number of points of  $X \times X$  fixed by  $g$  and  $\int \chi^2$  is the number of orbits of  $G$  on  $X \times X$ , which is  $\geq 2$ , as one sees by decomposing  $X \times X$  into the diagonal and its complement.

This also shows that  $\int \chi^2 = 2$  if and only if  $G$  is doubly transitive on  $X$ .

*Second Proof (by Group Representations).* We have  $\chi = 1 + \chi'$ , where  $\chi'$  is a non-zero real character with  $\int \chi' = 0$ . Therefore,

$$\int \chi^2 = 1 + \int \chi'^2 \geq 2,$$

with equality if and only if  $\chi'$  is irreducible.

We now prove Theorem 5. Recall that  $G_0$  is the set of  $g \in G$  with  $\chi(g) = 0$ . If  $g \notin G_0$ , we have  $1 \leq \chi(g) \leq n$  and therefore

$$(\chi(g) - 1)(\chi(g) - n) \leq 0.$$

Hence,

$$\int_{G-G_0} (\chi(g) - 1)(\chi(g) - n) \leq 0,$$

i.e.,

$$\int_G (\chi(g) - 1)(\chi(g) - n) \leq \int_{G_0} (\chi(g) - 1)(\chi(g) - n) = n \int_{G_0} 1.$$

The right hand side is

$$n \int_{G_0} 1 = nc_0,$$

and the left hand side is

$$\int_G (\chi^2 - (n+1)\chi + n).$$

By the lemma, and the fact that  $\int \chi = 1$ , we have

$$\int_G (\chi^2 - (n+1)\chi + n) \geq 2 - (n+1) + n = 1,$$

hence

$$1 \leq nc_0.$$

**2.3. Equality in Theorem 5.** The proof of Theorem 5 shows that equality holds if and only if  $\int \chi^2 = 2$  and  $(\chi(g) - 1)(\chi(g) - n) = 0$  for every  $g \in G - G_0$ , i.e. if and only if  $G$  is doubly transitive and no element of  $G - \{1\}$  fixes 2 points. By a theorem of Frobenius [8], the set  $N = \{1\} \cup G_0$  is then a normal subgroup of  $G$ , and  $G$  is a semi-direct product:  $G = H \cdot N$ . Hence,  $|N| = n$ , and  $(n-1)/|G| = |G_0|/|G| = c_0 = 1/n$ , i.e.  $|G| = n(n-1)$ ,  $|H| = n-1$ . Moreover, the action of  $H$  on  $N - \{1\}$  by conjugation is a free action. Since  $H$  and  $N - \{1\}$  have the same number of elements, one sees that  $H$  acts freely and transitively on  $N - \{1\}$ . This implies that  $N$  is a  $p$ -group for some prime  $p$  (and even more:  $N$  is an elementary abelian  $p$ -group). Hence,  $n$  is a power of a prime.

*Remarks.*

1. It is only for convenience that we have used Frobenius's Theorem [8]. It is possible to give a direct proof, as was already done in Jordan's paper [9].
2. Conversely, if  $n$  is a power of a prime, there exists a pair  $(G, X)$  with  $|X| = n$  and  $c_0 = 1/n$ : take  $X = k$ , a finite field with  $n$  elements, and define  $G$  as the group of affine transformations  $x \mapsto ax + b$  with  $a \in k^*, b \in k$ .

### 3. PROOF OF THE COVERING SPACE STATEMENT

With the same notation as in §1.2, choose a point  $s \in S$ . Let  $X = f^{-1}(s)$  be the fiber of  $s$ . Let  $G = \pi_1(S, s)$  be the fundamental group of  $S$  at the point  $s$ . There is a natural action of  $G$  on  $X$ , and the hypothesis that  $T$  is arcwise connected implies that every two points in  $X$  can be connected by a path and hence  $G$  acts transitively on  $X$ . Since  $n = |X| \geq 2$ , Theorem 4 shows that there exists  $g \in G$  which has no fixed point on  $X$ . If we represent  $g$  by a loop

$$\varphi : (\mathbf{S}_1, s_0) \rightarrow (S, s),$$

where  $s_0$  is a chosen point in  $\mathbf{S}_1$ , then  $\varphi$  cannot be lifted to  $T$ . Indeed, if  $\psi : \mathbf{S}_1 \rightarrow T$  were a lift of  $\varphi$ , the point  $x = \psi(s_0)$  would be a fixed point of  $g$ .

### 4. PROOF OF THE NUMBER THEORETIC STATEMENT

We now prove Theorems 1 and 2 with the help of Theorems 4 and 5. Let  $x_1, \dots, x_n$  be the roots of  $f$  in an algebraic closure  $\overline{\mathbf{Q}}$  of  $\mathbf{Q}$ . Let  $E = \mathbf{Q}(x_1, \dots, x_n)$  and let  $G = \text{Aut } E =$  the Galois group of  $E/\mathbf{Q}$ . The action of  $G$  on the set  $X = \{x_1, \dots, x_n\}$  is transitive since  $f$  is irreducible over  $\mathbf{Q}$ . Let  $G_0$  be the subset of  $G$  having no fixed points. By Theorems 4 and 5, we have

$$\frac{|G_0|}{|G|} \geq \frac{1}{n}.$$

Let us define a finite set  $S$  of "bad" prime numbers, namely, those which divide the discriminant of  $f$  or divide the coefficient of  $x^n$ . Assume now that  $p \notin S$ . Then the reduction  $f_p$  of  $f$  modulo  $p$  is a polynomial of degree  $n$ , whose  $n$  roots (in an algebraic closure  $\overline{\mathbf{F}}_p$  of  $\mathbf{F}_p$ ) are distinct. Let  $X_p$  be the set of such roots. We may identify  $X_p$  and  $X$  in the following way:

Let  $R = \mathbf{Z}[x_1, x_2, \dots, x_n]$  be the ring generated by the  $x_i$ 's. Choose a homomorphism  $\varphi : R \rightarrow \overline{\mathbf{F}}_p$  (such a homomorphism exists since  $p \nmid a_0$ , and any other such homomorphism is of the form  $\varphi \circ s$ , with  $s \in G$ ). Such a  $\varphi$  defines a bijection  $\varphi_p : X \rightarrow X_p$ , which is well-defined up to an element of  $G$ . Let  $\pi_p$  be the Frobenius automorphism of  $\overline{\mathbf{F}}_p$ , i.e.,  $\lambda \mapsto \lambda^p$ . The map  $\pi_p$  acts on  $X_p$ . If we identify  $X_p$  with  $X$  via  $\varphi_p$ , we get a permutation  $\sigma_p$  of  $X$  (depending on the choice of  $\varphi$ ). One proves that this permutation belongs to  $G$ . It is called the *Frobenius substitution of  $p$*  (relative to the choice of  $\varphi$ ); it is well-defined up to inner conjugation in  $G$ . We have

(\*) If  $p \notin S$ ,  $N_p$  is the number of  $x \in X$  fixed by  $\sigma_p$ .

This follows from the corresponding fact for  $X_p$  and  $\pi_p$ . (More generally, if  $\sigma_p$  is a product of disjoint cycles of lengths  $l_\alpha$ , then  $f_p$  decomposes into a product of  $\mathbf{F}_p$ -irreducible polynomials of degrees  $l_\alpha$ .) Hence,  $N_p = 0$  if and only if  $\sigma_p \in G_0$ , where  $G_0$  is the set of  $s \in G$  which acts on  $X$  without fixed point. Note that  $G_0$  is stable under conjugation so that " $\sigma_p \in G_0$ " makes sense.

We now recall Chebotarev’s Density Theorem (see Notes for Part 4):

**Chebotarev’s Density Theorem** ([19], [1]). *Let  $C$  be a subset of  $G$ , stable under conjugation (i.e. a union of conjugacy classes). Then the set  $P_{C,S}$  of primes  $p \notin S$  with  $\sigma_p \in C$  has a density, which is equal to  $\frac{|C|}{|G|}$ .*

Applying this theorem to the case  $C = G_0$  shows that the set  $P_0(f)$  of Theorem 1 has density  $c_0 = \frac{|G_0|}{|G|}$ ; by Theorems 4 and 5, this completes the proofs of Theorems 1 and 2.

5. EXAMPLE:  $N_p(f)$  FOR  $f = x^n - x - 1$

5.1. In this section, we consider the special case of  $f = x^n - x - 1$ ,  $n \geq 2$ , and we relate the numbers  $N_p(f)$  to the coefficients of suitable power series. We limit ourselves to stating the results; for the proofs, see the hints given in the Notes.

Here is a small table of  $N_p(f)$  for  $f = x^n - x - 1$ ,  $n = 2, 3, 4, 5$ :

$p$	$n = 2$	$n = 3$	$n = 4$	$n = 5$
2	0	0	0	0
3	0	0	0	0
5	1	1	0	0
7	0	1	1	0
11	2	1	1	0
13	0	0	1	0
17	0	1	2	2
19	2	1	0	1
23	0	2	1	1
...	...	...	...	...
59	2	3	1	0
...	...	...	...	...
83	0	1	4	0

5.2. **The case  $n = 2$ .** The discriminant of  $f = x^2 - x - 1$  is 5; the polynomial  $f$  has a double root mod 5; hence  $N_5(f) = 1$ . For  $p \neq 5$ , we have

$$N_p(f) = \begin{cases} 2 & \text{if } p \equiv \pm 1 \pmod{5} \\ 0 & \text{if } p \equiv \pm 2 \pmod{5}. \end{cases}$$

If one defines a power series  $F(q) = \sum_{m=0}^{\infty} a_m q^m$  by

$$F = \frac{q - q^2 - q^3 + q^4}{1 - q^5} = q - q^2 - q^3 + q^4 + q^6 - q^7 - q^8 + q^9 + \dots,$$

the above formula can be restated as

$$N_p(f) = a_p + 1 \quad \text{for all primes } p.$$

Note that the coefficients of  $F$  are *strongly multiplicative*: one has  $a_{mm'} = a_m a_{m'}$  for every  $m, m' \geq 1$ . The corresponding Dirichlet series  $\sum_{m=1}^{\infty} a_m m^{-s}$  is the  $L$ -series  $\prod_p (1 - (\frac{p}{5})p^{-s})^{-1}$ .

5.3. **The case  $n = 3$ .** The discriminant of  $f = x^3 - x - 1$  is  $-23$ ; the polynomial  $f$  has a double root and a simple root mod 23; hence  $N_{23}(f) = 2$ . For  $p \neq 23$ , one has:

$$N_p(f) = \begin{cases} 0 \text{ or } 3 & \text{if } \left(\frac{p}{23}\right) = 1 \\ 1 & \text{if } \left(\frac{p}{23}\right) = -1. \end{cases}$$

Moreover, in the ambiguous case where  $\left(\frac{p}{23}\right) = 1$ ,  $p$  can be written either as  $x^2 + xy + 6y^2$  or as  $2x^2 + xy + 3y^2$  with  $x, y \in \mathbf{Z}$ ; in the first case, one has  $N_p(f) = 3$ ; in the second case, one has  $N_p(f) = 0$ . (The smallest  $p$  of the form  $x^2 + xy + 6y^2$  is  $59 = 5^2 + 5 \cdot 2 + 6 \cdot 2^2$ , hence  $N_{59}(f) = 3$ ; cf. table above.)

Let us define a power series  $F = \sum_{m=0}^{\infty} a_m q^m$  by the formula

$$\begin{aligned} F &= q \prod_{k=1}^{\infty} (1 - q^k)(1 - q^{23k}) \\ &= \frac{1}{2} \left( \sum_{x,y \in \mathbf{Z}} q^{x^2 + xy + 6y^2} - \sum_{x,y \in \mathbf{Z}} q^{2x^2 + xy + 3y^2} \right) \\ &= q - q^2 - q^3 + q^6 + q^8 - q^{13} - q^{16} + q^{23} - q^{24} + \dots \end{aligned}$$

The formula for  $N_p(f)$  given above can be reformulated as:

$$N_p(f) = a_p + 1 \quad \text{for all primes } p.$$

Note that the coefficients of  $F$  are *multiplicative*: one has  $a_{mm'} = a_m a_{m'}$  if  $m$  and  $m'$  are relatively prime. The  $q$ -series  $F$  is a newform of weight 1 and level 23. The associated Dirichlet series is

$$\sum_{m=1}^{\infty} \frac{a_m}{m^s} = \prod_p \left( 1 - \frac{a_p}{p^s} + \left(\frac{p}{23}\right) \frac{1}{p^{2s}} \right)^{-1}.$$

5.4. **The case  $n = 4$ .** The discriminant of  $f = x^4 - x - 1$  is  $-283$ . The polynomial  $f$  has two simple roots and one double root mod 283, hence  $N_{283}(f) = 3$ . If  $p \neq 283$ , one has

$$N_p(f) = \begin{cases} 0 \text{ or } 4 & \text{if } p \text{ can be written as } x^2 + xy + 71y^2 \\ 1 & \text{if } p \text{ can be written as } 7x^2 + 5xy + 11y^2 \\ 0 \text{ or } 2 & \text{if } \left(\frac{p}{283}\right) = -1. \end{cases}$$

(These cases correspond to the Frobenius substitution of  $p$  being conjugate in  $S_4$  to (12)(34) or 1, (123), (1234) or (12) respectively.)

A complete determination of  $N_p(f)$  can be obtained via a newform  $F = \sum_{m=0}^{\infty} a_m q^m$  of weight 1 and level 283 given in [5, p. 80, example 2]:

$$F = q + \sqrt{-2}q^2 - \sqrt{-2}q^3 - q^4 - \sqrt{-2}q^5 + 2q^6 - q^7 - q^9 + 2q^{10} + q^{11} + \sqrt{-2}q^{12} + \dots$$

One has:

$$N_p(f) = 1 + (a_p)^2 - \left(\frac{p}{283}\right) \quad \text{for all primes } p \neq 283.$$

I do not know any closed formula for  $F$ , but one can give one for its reduction mod 283; see Notes. This is more than enough to determine the integers  $N_p(f)$ , since they are equal to 0, 1, 2 or 4.

5.5. **The case  $n \geq 5$ .** Here the only known result seems to be that  $f = x^n - x - 1$  is irreducible (Selmer [15]) and that its Galois group is the symmetric group  $S_n$ . No explicit connection with modular forms (or modular representations) is known, although some must exist because of the Langlands program.

NOTES

- 1.1. Here is another interpretation of  $c_0(f)$ . Let  $K = \mathbf{Q}[x]/(f)$  be the number field defined by  $f$ . We have  $[K : \mathbf{Q}] = n \geq 2$ . For every  $d \geq 1$ , let  $a_d(K)$  be the number of the ideals  $\mathfrak{a}$  of the ring of integers of  $K$  with  $N(\mathfrak{a}) = d$ . The zeta function of  $K$  is the Dirichlet series

$$\zeta_K(s) = \sum_{d \geq 1} \frac{a_d(K)}{d^s}.$$

Using standard recipes in analytic number theory, one can show that Theorem 1 is equivalent to saying that  $\zeta_K$  is *lacunary*: most of its coefficients are zero. More precisely, if we denote by  $N_K(X)$  the number of  $d \leq X$  with  $a_d(K) \neq 0$ , one has

$$N_K(X) \sim c_K \frac{X}{(\log X)^{c_0(f)}} \quad \text{for } X \rightarrow \infty,$$

where  $c_K$  is a strictly positive constant (cf. Odoni [13] and Serre [16, §3.5]). As for Theorem 2, it can be reformulated as

$$N_K(X) = O\left(\frac{X}{(\log X)^{1/n}}\right) \quad \text{for } X \rightarrow \infty,$$

with “ $O$ ” replaced by “ $o$ ” if  $n$  is not a power of a prime.

- 1.2. **Jordan’s Theorem (Theorem 4).** The standard proof of Theorem 4 relies on the fact that the stabilizer  $H_x$  of a point  $x$  of  $X$  has  $|G|/n$  elements, since  $X \simeq G/H_x$ . When  $x$  runs through the  $n$  points of  $X$ , the subgroups  $H_x$  have at least one point in common, namely the element 1. Hence, their union has at most  $n \cdot |H_x| - (n - 1)$  elements, i.e. at most  $|G| - (n - 1)$  elements. This shows that there are at least  $n - 1$  elements of  $G$  which do not belong to any  $H_x$ , i.e. which have no fixed point. The interest of Theorem 5 is that it replaces the crude lower bound  $n - 1$  by  $|G|/n$ , which is close to being optimal.

*Remark.* Another way of stating Theorem 4 is:

**Theorem 4’.** *If  $H$  is a proper subgroup of a finite group  $G$ , there is a conjugacy class of  $G$  which does not meet  $H$ .*

In group-character language, this can be restated as:

**Theorem 4’’.** *There exist two characters of  $G$  which are distinct but have the same restriction to  $H$ .*

In other words, the characters of  $G$  cannot be detected by their restriction to a proper subgroup of  $G$ . One needs at least two such subgroups (such as, for  $\mathbf{GL}_2(\mathbf{F}_q)$ , a Borel subgroup and a non-split Cartan subgroup). This is quite different from the case of compact connected Lie groups, where just one maximal torus is enough.

**1.3. Theorem 5.** Theorem 5 originated with a question of Lenstra, in relation with Theorem 2. See Boston et al. [2] for more on this story.

**2. Burnside's Lemma.** The first two proofs we offer are basically the same. Only their styles are different: analytic number theorists love to write  $\sum 1$  and to permute summations, while combinatorists are fond of counting the elements of a set by mapping it into another one.

Note that Burnside's Lemma implies directly the weak form of Jordan's Theorem (Theorem 4 above). Indeed, since the mean value of  $\chi(g)$  is 1, and the element  $g = 1$  contributes  $n > 1$ , there has to be some  $g \in G$  with  $\chi(g) < 1$ , hence  $\chi(g) = 0$ .

Note also that Burnside's Lemma, combined with Chebotarev's Density Theorem, gives the following result:

*If  $f$  is as in §1.1, the mean value of  $N_p(f)$  for  $p \rightarrow \infty$  is equal to 1.*

In other words:

$$\sum_{p \leq X} N_p(f) \sim \pi(X) \quad \text{for } X \rightarrow \infty.$$

This is due to Kronecker [10] and Frobenius [7], in the slightly weaker form where "natural density" is replaced by "analytic density".

**3. Lifting circles to coverings.** Theorem 3 does not extend to infinite coverings. Indeed, it is easy to construct an infinite free group  $G$  having a subgroup  $H$  of infinite index such that  $\cup gHg^{-1} = G$ . If one chooses a connected graph  $S$  with fundamental group isomorphic to  $G$ , the covering  $T \rightarrow S$  associated with  $H$  has the property that every continuous map  $\mathbf{S}_1 \rightarrow S$  can be lifted to  $T$ .

**4. Chebotarev Density Theorem.** The original proof can be found in [19]; it uses "analytic density" instead of "natural density". The more precise form we give was pointed out by Artin [1], even before Chebotarev's Theorem was proved.

For the history of this theorem, see [11], which also includes a sketch of a proof. For applications, see for instance [16] or [18].

Note that, for the application we make to Theorems 1 and 2, a weaker version of the theorem would be enough, namely the one proved by Frobenius [7] (with, once again, the proviso that "analytic density" has to be replaced by the "natural density").

**5.1. Computation of  $N_p(f)$ .** For a given polynomial  $f$ , such as  $x^3 - x - 1$ ,  $x^4 - x - 1$ , etc., the numerical computation of  $N_p(f)$  is an interesting question, especially for large values of the prime  $p$ . There are essentially two methods:

- The naive one is to try successively all the values of  $x \bmod p$ , and count those which are zeros of  $f \bmod p$ . This is slow; it requires exponential time (with respect to the number of digits of  $p$ ); it is reasonable for very small primes only (up to 5 digits, say).
- The second method is much faster ("P" instead of "NP") and can handle primes of about 100 digits. It relies on the standard fact that computing  $x^p$  by successive squarings takes about  $\log p$  operations. One applies this principle to the finite  $\mathbf{F}_p$ -algebra  $A_p = \mathbf{F}_p[X]/(f)$ ,

with  $x$  equal to the image of  $X$  in  $A_p$ . Once  $x^p$  is computed, one gets  $N_p(f)$  by the formula:

$$n - N_p(f) = \text{rank of the linear endomorphism } u \mapsto (x^p - x)u \text{ of } A_p.$$

Note that a variant of this method is incorporated in programs such as “PARI”, where one has only to ask “polrootsmod( $f, p$ )?” to get the list of the roots of  $f \bmod p$ .

- 5.2.**  $N_p(f)$  for  $f = x^2 - x - 1$ . For  $p \neq 2, 5$ , the roots of  $f_p$  in  $\overline{\mathbf{F}}_p$  are  $(1 \pm \sqrt{5})/2$ ; hence  $N_p(f) = 2$  if 5 is a square (mod  $p$ ), and  $N_p(f) = 0$  if not. By quadratic reciprocity, the first case occurs if and only if  $p \equiv \pm 1 \pmod{5}$ . A direct proof is as follows: call  $z$  a primitive 5<sup>th</sup> root of unity in  $\overline{\mathbf{F}}_p$  and put  $x = -(z + z^4), x' = -(z^2 + z^3)$ . One has  $x + x' = 1$  and  $xx' = -1$  because  $1 + z + z^2 + z^3 + z^4 = 0$ . Hence,  $x, x'$  are the zeros of  $f_p$ . The action of the Frobenius  $\sigma_p$  on  $X = \{x, x'\}$  is clear: we have  $\sigma_p(x) = -(z^p + z^{-p})$ . If  $p \equiv \pm 1 \pmod{5}$ , we have  $z^p = z^{\pm 1}$ , hence  $\sigma_p(x) = x, \sigma_p(x') = x'$ , and  $N_p(f) = 2$ ; if  $p \equiv \pm 2 \pmod{5}$ , the same argument shows that  $\sigma_p$  permutes  $x$  and  $x'$ , hence  $N_p(f) = 0$ .

*Remark.* Even though the two cases  $N_p(f) = 0$  and  $N_p(f) = 2$  arise “equally often” (in an asymptotic sense, when  $p \rightarrow \infty$ ), yet there is a definite bias towards the first case. This is an example of what Rubinstein and Sarnak call “Chebyshev Bias”; cf. [14].

- 5.3.**  $N_p(f)$  for  $f = x^3 - x - 1$ . Let  $E = \mathbf{Q}[X]/(f)$  be the cubic field defined by  $f$ , and let  $L$  be its Galois closure. We have  $\text{Gal}(L/\mathbf{Q}) = S_3$ . The field  $L$  is a cubic cyclic extension of the quadratic field  $K = \mathbf{Q}(\sqrt{-23})$ ; it is unramified, and, since  $h(-23) = 3$ , it is the Hilbert class field of  $K$ , i.e. the maximal unramified abelian extension of  $K$  (as a matter of fact, it is also the maximal unramified extension—abelian or not—of  $K$ , as follows from the Odlyzko bounds; see e.g. Martinet [12].)

If  $p \neq 23$ , let  $\sigma_p$  be the Frobenius substitution of  $p$  in  $S_3 = \text{Gal}(L/\mathbf{Q})$ ; it is well-defined, up to conjugation. The image of  $\sigma_p$  by  $\text{sgn} : S_3 \rightarrow \{\pm 1\}$  is  $\epsilon(p)$ , where  $\epsilon$  is the quadratic character associated with  $K/\mathbf{Q}$ , i.e.,  $\epsilon(p) = (\frac{p}{23})$ . This shows that  $\sigma_p$  is a transposition if  $(\frac{p}{23}) = -1$ , hence  $N_p(f) = 1$  in that case. When  $(\frac{p}{23}) = 1$ ,  $\sigma_p$  is of order 1 or 3, hence  $N_p(f) = 3$  or  $N_p(f) = 0$ . To distinguish between these two cases, one decomposes  $p$  in  $K$  as  $\mathfrak{p} \cdot \overline{\mathfrak{p}}$ , and one has to decide whether  $\mathfrak{p}$  is principal or not. The standard correspondence between ideal classes and binary quadratic forms shows that  $\mathfrak{p}$  is principal is equivalent to  $p$  being representable by the form  $x^2 + xy + 6y^2$ , while  $\mathfrak{p}$  is non-principal is equivalent to  $p$  being representable by the form  $2x^2 + xy + 3y^2$ . This gives the recipe we wanted, namely,

$$N_p(f) = \begin{cases} 3 & \text{if } p \text{ is representable by } x^2 + xy + 6y^2 \\ 0 & \text{if } p \text{ is representable by } 2x^2 + xy + 3y^2 \\ 1 & \text{if } (\frac{p}{23}) = -1. \end{cases}$$

The natural embedding  $\rho$  of  $S_3 = \text{Gal}(L/\mathbf{Q})$  in  $\mathbf{GL}_2(\mathbf{C})$  gives rise to an Artin  $L$ -function

$$L(\rho, s) = \sum_{m=1}^{\infty} \frac{a_m}{m^s},$$

with coefficients  $a_m \in \mathbf{Z}$ . One may characterize it by

$$L(\rho, s) = \zeta_E(s)/\zeta(s),$$

where  $\zeta_E(s)$  is the zeta function of the cubic field  $E$ . This is equivalent to saying that the linear representation  $\rho \oplus 1$  is isomorphic to the 3-dimensional permutation representation of  $S_3$ . By comparing the traces of  $\sigma_p$  in both representations, we get  $N_p(f) = a_p + 1$  for every prime  $p$  (including  $p = 23$ ). Since  $S_3$  is a dihedral group, Hecke's theory applies and shows that the power series  $F = \sum_{m=1}^{\infty} a_m q^m$  with the same coefficients as  $L(\rho, s)$  is a cusp form of weight 1 and level 23, with respect to the character  $\epsilon$ . The explicit expressions of  $F$  given in the text can be checked by standard modular methods.

- 5.4.**  $N_p(f)$  for  $f = x^4 - x - 1$ . Let  $E$  be the quartic field defined by  $f$  and  $L$  its Galois closure; the Galois group  $G = \text{Gal}(L/\mathbf{Q})$  is isomorphic to  $S_4$ . Let  $H$  be the unique normal  $(2, 2)$ -subgroup of  $G$ ; the quotient  $G/H$  is isomorphic to  $S_3$ . The field  $L^H$  is the Hilbert class field of  $\mathbf{Q}(\sqrt{-283})$ ; note that  $h(-283) = 3$ . The same argument as in Note 5.3 gives the image of the Frobenius  $\sigma_p$  in  $G/H$  in terms of  $(\frac{p}{283})$  and of the binary forms  $x^2 + xy + 71y^2$  and  $7x^2 + 5xy + 11y^2$  with discriminant  $-283$ .

To go further, one needs a result of Tate (reproduced in [17], [12], [5]) which says that the field  $L$  has a quadratic extension  $\tilde{L}$  having the following two properties:

- $\tilde{L}$  is unramified over  $L$  (and hence also over  $\mathbf{Q}(\sqrt{-283})$ );
- $\tilde{L}$  is a Galois extension of  $\mathbf{Q}$ .

(An explicit construction of  $\tilde{L}$ , due to Tate, is:  $\tilde{L} = L(\sqrt{4 - 7x^2})$ , where  $x$  is a root of  $f$  in  $L$ ; the construction given in Crespo [5] is more complicated.)

Martinet [12] has shown that  $\tilde{L}$  is the maximal unramified extension of  $\mathbf{Q}(\sqrt{-283})$ ; in other words, the fundamental group of the ring  $\mathbf{Z}[(1 + \sqrt{-283})/2]$  is isomorphic to the "binary tetrahedral group"  $\tilde{A}_4 = \mathbf{SL}_2(\mathbf{F}_3)$ .

The group  $\tilde{G} = \text{Gal}(\tilde{L}/\mathbf{Q})$  is isomorphic to  $\mathbf{GL}_2(\mathbf{F}_3)$ ; it has a natural embedding  $\rho$  in  $\mathbf{GL}_2(\mathbf{C})$ ; its character has values in  $\mathbf{Z}[\sqrt{-2}]$ . By a well-known theorem of Langlands and Tunnell (see the references in [5]), the  $L$ -series attached to  $\rho$  corresponds to a modular form  $F = \sum_{m=0}^{\infty} a_m q^m$  of weight 1 and level 283 whose first hundred coefficients are computed in [5]. One checks (by a character computation) that one has

$$\rho \otimes \rho = \epsilon \oplus (\theta - 1),$$

where  $\theta$  is the 4-dimensional permutation representation of  $G$  and  $\epsilon$  is the sign character of  $G$ . By taking traces, this gives

$$(a_p)^2 = \left(\frac{p}{283}\right) + N_p(f) - 1, \quad \text{for all primes } p \neq 283.$$

*Remark.* One may give an explicit formula for  $F \pmod{283}$  as follows: by a known result [17, 9.3.1]  $F$  is congruent mod 283 to a modular form  $\varphi$  of weight  $(283 + 1)/2 = 142$ , and of level 1. Hence,  $\varphi$  can be written as a linear combination, with coefficients in  $\mathbf{F}_{283}$ , of the standard basis:

$$QR^{23}\Delta, QR^{21}\Delta^2, \dots, QR\Delta^{11}$$

(with Ramanujan's notation:

$$Q = 1 + 240 \sum_{n=1}^{\infty} \frac{n^3 q^n}{1 - q^n}, \quad R = 1 - 504 \sum_{n=1}^{\infty} \frac{n^5 q^n}{1 - q^n},$$

and  $\Delta = (Q^3 - R^2)/1728 = q \prod_{n=1}^{\infty} (1 - q^n)^{24}$ .

A computation, using only the first eleven coefficients of  $F$ , gives the coefficients of  $\varphi$  in that basis:

$$[1, 24, 52, 242, 40, 232, 164, 217, 262, 274, 128].$$

In other words, we have

$$F \equiv QR^{23}\Delta + 24QR^{21}\Delta^2 + \cdots + 128QR\Delta^{11} \pmod{283}.$$

(In these computations, I have selected 127 as " $\sqrt{-2}$ " mod 283.)

#### REFERENCES

1. E. Artin, Über eine neue Art von L-Reihen, *Hamb. Abh.* **3** (1923), 89–108 (= Coll. Papers, 105–124).
2. N. Boston, W. Dabrowski, T. Foguel, P. J. Gies, D. A. Jackson, J. Leavitt and D. T. Ose, The proportion of fixed-point-free elements of a transitive permutation group, *Comm. Algebra* **21** (1993), 3259–3275. MR **94e**:20002
3. W. Burnside, *Theory of Groups of Finite Order*, 2nd edition, Cambridge Univ. Press, 1911 (= Dover Publ., 1955). MR **16**:1086c
4. P. J. Cameron and A. M. Cohen, On the number of fixed point free elements in a permutation group, *Discrete Math.* **106/107** (1992), 135–138. MR **93f**:20004
5. T. Crespo, Galois representations, embedding problems and modular forms, *Collectanea Math.* **48** (1997), 63–83. MR **98j**:11101
6. F. G. Frobenius, Über die Congruenz nach einem aus zwei endlichen Gruppen gebildeten Doppelmodul, *J. Crelle* **101** (1887), 279–299 (= Ges. Abh., II, 304–330).
7. F. G. Frobenius, Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe, *Sitz. Akad. Wiss. Berlin* (1896), 689–703 (= Ges. Abh., II, 719–733).
8. F. G. Frobenius, Über auflösbare Gruppen IV, *Sitz. Akad. Wiss. Berlin* (1901), 1216–1230 (= Ges. Abh., III, 189–203).
9. C. Jordan, Recherches sur les substitutions, *J. Liouville* **17** (1872), 351–367 (= Oe. I. 52).
10. L. Kronecker, Über die Irreducibilität von Gleichungen, *Sitz. Akad. Wiss. Berlin* (1880), 155–162 (= Werke, II, 83–93).
11. H. W. Lenstra, Jr., and P. Stevenhagen, Chebotarëv and his density theorem, *Math. Intelligencer* **18** (1996), 26–37. MR **97e**:11144
12. J. Martinet, Petits discriminants des corps de nombres, *Journées arithmétiques 1980* (J. V. Armitage, ed.), Cambridge Univ. Press, Cambridge, 1982, pp. 151–193. MR **84g**:12009
13. R. W. K. Odoni, On the norms of algebraic integers, *Mathematika* **22** (1975), 71–80. MR **54**:12715
14. M. Rubinstein and P. Sarnak, Chebyshev's Bias, *Experiment. Math.* **3** (1994), 173–197. MR **96d**:11099
15. E. S. Selmer, On the irreducibility of certain trinomials, *Math. Scand.* **4** (1956), 287–302. MR **19**:7f
16. J-P. Serre, Divisibilité de certaines fonctions arithmétiques, *L'Ens. Math.* **22** (1976), 227–260 (= Oe. 108). MR **55**:7958
17. J-P. Serre, Modular forms of weight one and Galois representations, *Algebraic Number Fields* (A. Fröhlich, ed.), Acad. Press, London, 1977, pp. 193–268 (= Oe. 110). MR **56**:8497

18. J-P. Serre, Quelques applications du théorème de densité de Chebotarev, *Publ. Math. I.H.E.S.* **54** (1981), 123–201 (= Oe. 125). MR **83k**:12011
19. N. Tschebotareff (Chebotarev), Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören, *Math. Ann.* **95** (1925), 191–228.

COLLÈGE DE FRANCE, 3, RUE D'ULM, PARIS, FRANCE  
*E-mail address:* `serre@dma.ens.fr`