ISSN: 1401-5617

On the number of solutions of some equations in finite groups

Torbjörn Tambour

Research Reports in Mathematics
Number 15, 1998

Department of Mathematics
Stockholm University

Electronic versions of this document are available at
http://www.matematik.su.se/reports/1998/15

Date of publication: December 11, 1998

Postal address:
Department of Mathematics
Stockholm University
S-106 91 Stockholm
Sweden

Electronic addresses:
http://www.matematik.su.se
info@matematik.su.se

On the number of solutions of some equations in finite groups

Torbjörn Tambour

Abstract

We compute the number of solutions to some equations in finite groups and give a new proof of the fact that the degrees of the irreducible characters divide the order of the group.

1 On a result of Frobenius

In this note G will be a finite group with neutral element 1. $\mathrm{Irr}(G)$ denotes the set of irreducible characters. For $\chi \in \mathrm{Irr}(G)$ we let $\Theta_\chi : G \to GL(V_\chi)$ be a representation affording χ. All representations below are over the complex numbers. The scalar product on the space of class functions on G will be denoted by $[\ ,\ ]$. By 1_V we denote the identity map on the vector space V and by tr the trace map $\mathrm{End}_{\mathbf{C}}(V) \to \mathbf{C}$. The number of elements of a finite set S will be denoted by $|S|$.

We are going to study the two equations

$$g = x_1 x_2 \dots x_n x_1^{-1} x_2^{-1} \dots x_n^{-1} \text{ and} \tag{1}$$
$$g = [x_1, y_1] \dots [x_n, y_n] \tag{2}$$

in G, where $[x, y]$ is the commutator $xyx^{-1}y^{-1}$, and we let $N_n(g)$ and $M_n(g)$ denote the number of solutions of (1) and (2) respectively (hence $N_2 = M_1$). Clearly both N_n and M_n are class functions, i.e. they are constant on the conjugacy classes, and therefore they can be expanded into irreducible characters. Frobenius [1] showed that

$$N_2(g) = \sum_{\chi \in \mathrm{Irr}(G)} \frac{|G|}{\chi(1)} \chi(g),$$

and we will compute the coefficients in the expansions of N_n and M_n and use them to give a new proof of the fact that the degrees of the irreducible characters divide $|G|$. We will also see that the numbers $N_n(1)$ actually determine the degrees of the irreducible characters.

Remark: Although maybe not apparent from the definition, elements of the form $g = x_1 \dots x_n x_1^{-1} \dots x_n^{-1}$ belong to the commutator subgroup. For if λ is a one-dimensional character, then clearly $\lambda(g) = 1$. Hence g lies in the kernel of every one-dimensional character, the intersection of which is the commutator subgroup.

Theorem 1 *The expansions into irreducible characters are*

$$N_n(g) = \sum_{\chi \in \mathrm{Irr}(G)} \frac{|G|^{n-1}}{\chi(1)^{n-\epsilon_n}} \chi(g),$$

where $\epsilon_n = 1$ *if* n *is even and* 2 *if* n *is odd, and*

$$M_n(g) = \sum_{\chi \in \mathrm{Irr}(G)} \frac{|G|^{2n-1}}{\chi(1)^{2n-1}} \chi(g).$$

Proof. We first prove two useful relations. For an irreducible character χ,

$$\sum_{x \in G} \Theta_\chi(xyx^{-1}) = \frac{|G|}{\chi(1)} \chi(y) 1_{V_\chi} \tag{3}$$

$$\sum_{x \in G} \chi(x) \Theta_\chi(x^{-1}) = \frac{|G|}{\chi(1)} 1_{V_\chi}. \tag{4}$$

Denote the left hand side of (3) by $F(y)$; then apparently $F(y)$ commutes with all $\Theta_\chi(g)$, so by Schur's lemma $F(y) = \lambda(y) 1_{V_\chi}$ for some scalar $\lambda(y)$. The trace of $F(y)$ is $trF(y) = \sum_x \chi(xyx^{-1}) = |G|\chi(y)$ and the trace of the right hand side is $\lambda(y)\chi(1)$.

The left hand side of (4) also commutes with all $\Theta_\chi(g)$, since

$$\Theta_\chi(g) \sum_{x \in G} \chi(x) \Theta_\chi(x^{-1}) \Theta_\chi(g^{-1}) = \sum_{x \in G} \chi(x) \Theta_\chi(gx^{-1}g^{-1})$$
$$= \sum_{x \in G} \chi(g^{-1}xg) \Theta_\chi(x^{-1}) = \sum_{x \in G} \chi(x) \Theta_\chi(x^{-1})$$

after a change of variables. Hence $\sum_x \chi(x)\Theta_\chi(x^{-1}) = \mu 1_{V_\chi}$ for some scalar μ. Taking the trace gives

$$|G| = \sum_{x \in G} \chi(x)\chi(x^{-1}) = \mu\chi(1)$$

by the first orthogonality relation. This proves the claim.

Combining (3) and (4) now gives

$$\sum_{x,y \in G} \Theta_\chi(xyx^{-1}y^{-1}) = \frac{|G|}{\chi(1)} \sum_{y \in G} \chi(y)\Theta_\chi(y^{-1}) = \left(\frac{|G|}{\chi(1)}\right)^2 1_{V_\chi}. \tag{5}$$

Hence

$$\sum_{x_1,y_1,\dots,x_n,y_n \in G} \Theta_\chi(x_1y_1x_1^{-1}y_1^{-1}\dots x_ny_nx_n^{-1}y_n^{-1}) = \left(\frac{|G|}{\chi(1)}\right)^{2n} 1_{V_\chi},$$

which on taking the trace gives

$$\begin{aligned}[M_n,\chi] &= \frac{1}{|G|}\sum_{g \in G} M_n(g)\chi(g) \\ &= \frac{1}{|G|}\sum_{x_1,y_1,\dots,x_n,y_n \in G} \chi(x_1y_1x_1^{-1}y_1^{-1}\dots x_ny_nx_n^{-1}y_n^{-1}) = \frac{|G|^{2n-1}}{\chi(1)^{2n-1}}.\end{aligned}$$

The expansion of M_n follows.

If we take the trace of both sides of (5) we get

$$[N_2,\chi] = \frac{1}{|G|}\sum_{g \in G} N_2(g)\chi(g) = \frac{1}{|G|}\sum_{x,y \in G} \chi(xyx^{-1}y^{-1}) = \frac{|G|}{\chi(1)},$$

and Frobenius's expansion of N_2 follows.

By (3) again we have

$$\sum_{x,y,z \in G} \Theta_\chi(xyzx^{-1}y^{-1}z^{-1}) = \frac{|G|}{\chi(1)} \sum_{y,z \in G} \chi(yz)\Theta_\chi(y^{-1}z^{-1})$$

and so

$$\sum_{x,y,z \in G} \chi(xyzx^{-1}y^{-1}z^{-1}) = \frac{|G|}{\chi(1)} \sum_{y,z \in G} \chi(yz)\chi(y^{-1}z^{-1}).$$

Now

$$\sum_{z\in G}\chi(yz)\chi(y^{-1}z^{-1})=\sum_{z\in G}\chi(z)\chi(y^{-1}z^{-1}y)=\sum_{z\in G}\chi(z)\chi(z^{-1})=|G|$$

which finally gives

$$\sum_{g\in G}N_3(g)\chi(g)=\sum_{x,y,z\in G}\chi(xyzx^{-1}y^{-1}z^{-1})=\frac{|G|}{\chi(1)}\sum_{y\in G}|G|=\frac{|G|^3}{\chi(1)}$$

and $[N_3,\chi]=|G|^2/\chi(1)$.

To finish the proof we are going to show that for $n\geq 3$,

$$[N_n,\chi]=\Big(\frac{|G|}{\chi(1)}\Big)^2[N_{n-2},\chi].$$

By (3),

$$\sum_{x_1\in G}\Theta_\chi(x_1x_2\dots x_nx_1^{-1})=\frac{|G|}{\chi(1)}\chi(x_2\dots x_n)1_{V_\chi}$$

and

$$\begin{aligned}\sum_{x_1,x_2\in G}\Theta_\chi(x_1x_2\dots x_nx_1^{-1}x_2^{-1}) &= \frac{|G|}{\chi(1)}\sum_{x_2\in G}\chi(x_2\dots x_n)\Theta_\chi(x_2^{-1})\\ &= \frac{|G|}{\chi(1)}\Theta_\chi(x_3\dots x_n)\sum_{t\in G}\chi(t)\Theta_\chi(t^{-1})\\ &= \Big(\frac{|G|}{\chi(1)}\Big)^2\Theta_\chi(x_3\dots x_n)\end{aligned}$$

where we have made the change of variables $t=x_2\dots x_n$. Hence

$$\sum_{x_1,\dots,x_n\in G}\Theta_\chi(x_1\dots x_nx_1^{-1}\dots x_n^{-1})$$

$$=\Big(\frac{|G|}{\chi(1)}\Big)^2\sum_{x_3,\dots,x_n\in G}\Theta_\chi(x_3\dots x_nx_3^{-1}\dots x_n^{-1})$$

wherefore

$$\sum_{x_1,\dots,x_n\in G}\chi(x_1\dots x_n x_1^{-1}\dots x_n^{-1}) = \Big(\frac{|G|}{\chi(1)}\Big)^2 \sum_{x_3,\dots,x_n\in G}\chi(x_3\dots x_n x_3^{-1}\dots x_n^{-1}),$$

that is, $[N_n,\chi] = (|G|/\chi(1))^2[N_{n-2},\chi]$. The theorem is proved.

Remark: Since the coefficients in the expansion of N_2 (or of any N_n) are integers, N_2 is actually a character and it is tempting to try to find a nice description of some representation affording N_2. This does not seem to be so easy, though. For instance, one can see that N_2 cannot in general be the character of a permutation representation. For let $G = S_3$, the symmetric group on three letters, and assume that there exists a G-set affording N_2. The orbits have length 1, 2, 3 or 6. Since $N_2(1) = 18$ and the number of orbits is 6 (by Burnside's lemma), there must be either 6 orbits of length 3 or 1 orbit of length 6, 2 of length 3 and 3 of length 2. In any case there is an orbit of length 3. The permutation representation of G on this orbit is equivalent to one with G acting on the cosets of some subgroup with $6/3 = 2$ elements, i.e. a subgroup consisting of the identity 1 and a transposition (ab). The coset $\{1,(ab)\}$ is fixed by the element (ab). But $N_2((ab)) = 0$, so there are no fixed points of (ab) and we have a contradiction.

2 On the degrees of the irreducible characters

By Theorem 1

$$\frac{1}{|G|}N_{2n+2}(1) = \sum_{\chi\in\mathrm{Irr}(G)}\Big(\frac{|G|}{\chi(1)}\Big)^{2n}.$$

Put $a_\chi = |G|/\chi(1)$ and let p_k be the kth power sum symmetric function, $p_k(x_1,\dots,x_m) = x_1^k+\dots+x_m^k$. Then

$$\frac{1}{|G|}N_{2n+2}(1) = p_n(a_\chi^2;\chi\in\mathrm{Irr}(G)).$$

Denote the kth elementary symmetric function by e_k. By Newton's formulæ the numbers $e_k(a_\chi^2)$ are determined by the $p_k(a_\chi^2)$, hence they are determined by the $N_{2n}(1)$. But then the quotients a_χ and therefore the degrees $\chi(1)$ are determined by the $N_{2n}(1)$ (and the order $|G|$ of course).

It is a classical result of Frobenius that the degrees of the irreducible characters divide the order of G and there are well-known improvements of this. We will give a new proof of Itô's theorem that $\chi(1)$ divides the index $|G : A|$ for any normal abelian subgroup A of G. Other proofs of these results can be found in any textbook on character theory, e.g. [2].

We first prove a lemma.

Lemma 2 *Let $y_1, \dots, y_r$ be rational numbers and suppose that there is an integer $s \neq 0$ such that $s \cdot p_m(y_1, \dots, y_r)$ are integers for all $m \geq 1$. Then the y_i are integers.*

Proof. We will prove the lemma by contradiction. Suppose then that the claim is not true and let $y_1, \dots, y_k$ be those y_i that are not integers (if necessary we can of course renumber the y_i). Since $p_m(y_1, \dots, y_r) = p_m(y_1, \dots, y_k) + p_m(y_{k+1}, \dots, y_r)$ we have $s \cdot p_m(y_1, \dots, y_k) \in \mathbf{Z}$ for all m. Hence we may replace k by r and assume that no y_i is an integer.

We first consider the case $s = 1$. We use the following convenient notation: When q is a prime and a an integer, $o_q(a) = n$, where a is divisible by q^n, but not by q^{n+1}. When a/b is a rational number, $o_q(a/b) = o_q(a) - o_q(b)$. By Newton's formulæ, $m!e_m$ is a polynomial with integer coefficients in the p_k, so $m!e_m(y_1, \dots, y_r) \in \mathbf{Z}$ for all m. Let q be a prime such that $o_q(y_i) < 0$ for some i. Renumbering if necessary, we may assume that $o_q(y_i) < 0$ for $i = 1, 2, \dots, j$ and ≥ 0 for $i = j+1, \dots r$. Consider $j!e_j(y_1, \dots, y_r)$. If $\{i_1, \dots, i_j\} \neq \{1, \dots, j\}$, then $o_q(y_{i_1} \dots y_{i_j}) > o_q(y_1 \dots y_j)$, so $o_q(e_j(y_1, \dots, y_r)) = o_q(y_1 \dots y_j)$. Since $o_q(y_i) < 0$ for $i = 1, \dots, j$, we have $o_q(e_j(y_1, \dots, y_r)) \leq -j$ and it follows that $q^j | j!$. But the exact power of q dividing $j!$ is

$$\left[\frac{j}{q}\right] + \left[\frac{j}{q^2}\right] + \cdots < \frac{j}{q} + \frac{j}{q^2} + \cdots = \frac{j}{q-1} \leq j,$$

where [ ] denotes the integer part, and we have a contradiction.

Now we consider the general case. We get

$$p_m(sy_1, \dots, sy_r) = s^m p_m(y_1, \dots, y_r) \in \mathbf{Z},$$

so $sy_i \in \mathbf{Z}$ for all i by the first part of the proof. Put $y_i = t_i/s$, where $t_i \in \mathbf{Z}$. Then $\sum_i t_i^m / s^{m-1} \in \mathbf{Z}$ for all m. If p is a prime dividing s, then $p^{m-1} | \sum_i t_i^m$

for all m. We will prove that $p|t_i$ for all i. By induction on the number of prime factors of s, this will show that $s|t_i$ for all i. Suppose that there is some t_i that is not divisible by p. We can then as above assume that no t_i is divisible by p. Since p and t_i are coprime and $\varphi(p^k) = p^{k-1}(p-1)$ we have

$$t_i^{p^{k-1}(p-1)} \equiv 1 \bmod p^k.$$

Because $\sum_i t_i^{p^{k-1}(p-1)}$ is divisible by $p^{p^{k-1}(p-1)-1}$ and $k \leq p^{k-1}(p-1)-1$ if k is sufficiently large, $p^k|r$ for all k. This is impossible and the lemma is proved.

An immediate consequence of the lemma is that $\chi(1)$ divides $|G|$ for all irreducible χ. For we saw in the beginning of this section that $|G|p_n(a_\chi^2)$ is an integer for all n, and then a_χ^2 and also a_χ are all integers. We proceed to prove Itô's theorem.

Theorem 3 (Itô) *Let A be a normal abelian subgroup of G. Then the degrees of the irreducible characters divide the index $|G : A|$.*

Proof. We will use the notation

$$[x_1, x_2, \ldots, x_n] = x_1 x_2 \ldots x_n x_1^{-1} x_2^{-1} \ldots x_n^{-1}.$$

For $a \in A$, let $\Omega_{n,a}$ be the set of all $(x_1, \ldots, x_n) \in G^n$ such that

$$[x_1, \ldots, x_n] = a.$$

Also let Ω_n denote the union of all $\Omega_{n,a}$ for $a \in A$. Notice that $|\Omega_{n,1}| = N_n(1)$.

We first claim that there is an action of A^n on Ω_n given by

$$(a_1, \ldots, a_n).(x_1, \ldots, x_n) = (a_1 x_1, \ldots, a_n x_n)$$

and we need to show that $(a_1 x_1, \ldots, a_n x_n)$ lies in Ω_n if $(x_1, \ldots, x_n)$ does. To simplify the formulæ we write $x^y = yxy^{-1}$. Using induction one easily proves that

$$x_0 a_1 x_1 a_2 x_2 \ldots a_n x_n = a_1^{x_0} a_2^{x_0 x_1} \ldots a_n^{x_0 x_1 \ldots x_{n-1}} x_0 x_1 \ldots x_n$$

for any a_i and x_i. This gives

$$a_1 x_1 a_2 x_2 \ldots a_n x_n = a_1 a_2^{x_1} \ldots a_n^{x_1 \ldots x_{n-1}} x_1 \ldots x_n$$

and

$$x_1 \dots x_n x_1^{-1} a_1^{-1} x_2^{-1} a_2^{-1} \dots x_n^{-1} a_n^{-1}$$

$$= (a_1^{-1})^{x_1 \dots x_n x_1^{-1}} (a_2^{-1})^{x_1 \dots x_n x_1^{-1} x_2^{-1}} \dots (a_n^{-1})^{x_1 \dots x_n x_1^{-1} \dots x_n^{-1}} [x_1, \dots, x_n].$$

Combining these we get

$$[a_1 x_1, \dots, a_n x_n] = f_{\bar{x}}(a_1, \dots, a_n)[x_1, \dots, x_n],$$

where $\bar{x} = (x_1, \dots, x_n)$ and

$$f_{\bar{x}}(a_1, \dots, a_n) = a_1 a_2^{x_1} a_3^{x_1 x_2} \dots a_n^{x_1 \dots x_{n-1}} (a_1^{-1})^{x_1 \dots x_n x_1^{-1}} \dots (a_n^{-1})^{x_1 \dots x_n x_1^{-1} \dots x_n^{-1}}.$$

Since $A \lhd G$, $f_{\bar{x}}(a_1, \dots, a_n) \in A$ and indeed we have an action of A^n on Ω_n. Furthermore, $f_{\bar{x}} \colon A^n \to A$ is a homomorphism since A is abelian. Let $\bar{x} = (x_1, \dots, x_n) \in \Omega_{n,1}$ and $\bar{a} = (a_1, \dots, a_n) \in A^n$. Then $\bar{a}.\bar{x} \in \Omega_{n,1}$ if and only if $f_{\bar{x}}(\bar{a}) = 1$, i.e., if and only if $\bar{a} \in \ker f_{\bar{x}}$. Hence

$$|\mathrm{orb}_{A^n}(\bar{x}) \cap \Omega_{n,1}| = |\ker f_{\bar{x}}|,$$

where $\mathrm{orb}_{A^n}(\bar{x})$ is the orbit through $\bar{x}$ under the action of A^n. We have $|\ker f_{\bar{x}}| \cdot |\mathrm{im}\ f_{\bar{x}}| = |A|^n$ or

$$|\ker f_{\bar{x}}| = \frac{|A|}{|\mathrm{im}\ f_{\bar{x}}|} \cdot |A|^{n-1},$$

where the first factor is an integer, since the image is a subgroup of A. It follows that $|\mathrm{orb}_{A^n}(\bar{x}) \cap \Omega_{n,1}|$ is divisible by $|A|^{n-1}$ for all $\bar{x}$. But $\Omega_{n,1}$ is the disjoint union of all sets $\mathrm{orb}_{A^n}(\bar{x}) \cap \Omega_{n,1}$ for $\bar{x} \in \Omega_{n,1}$, wherefore $N_n(1)$ is divisible by $|A|^{n-1}$ for all n.

By Theorem 1

$$\frac{1}{|A|^{2n}} N_{2n+2}(1) = |G| \sum_{\chi} \Big(\frac{|G:A|}{\chi(1)} \Big)^{2n}$$

and then by Lemma 2, $|G:A|/\chi(1)$ is indeed an integer for all $\chi \in \mathrm{Irr}(G)$.

The most obvious example of a normal abelian subgroup is of course the centre $Z = Z(G)$. For an irreducible character χ the (normal) subgroup $Z(\chi)$

is defined as set of all elements g such that $\Theta_\chi(g)$ is a scalar multiple of the identity. It is easy to see that $Z(\chi)$ consists of all g such that $|\chi(g)| = \chi(1)$. Moreover, $Z(G)$ is the intersection of all $Z(\chi)$ for $\chi \in \mathrm{Irr}(G)$. For by Schur's lemma, $Z(G) \subseteq Z(\chi)$ for all χ. On the other hand, if $g \in \cap_\chi Z(\chi)$, then $\Theta_\chi(gxg^{-1}x^{-1}) = 1_{V_\chi}$ for all x and χ. Hence $gxg^{-1}x^{-1} \in \cap_\chi \ker \Theta_\chi = \{1\}$ for all x, so $g \in Z(G)$, which proves the claim.

The image of $Z(\chi)$ under Θ_χ is the centre of $\Theta_\chi(G)$. The identity map $GL(V) \to GL(V)$ gives by restriction an irreducible representation of $\Theta_\chi(G)$. Hence by the theorem, $\chi(1)$ divides the index $|\Theta_\chi(G) : Z(\Theta_\chi(G))|$. But

$$\frac{\Theta_\chi(G)}{Z(\Theta_\chi(G))} = \frac{\Theta_\chi(G)}{\Theta_\chi(Z(\chi))} \cong \frac{G/\ker\Theta_\chi}{Z(\chi)/\ker\Theta_\chi} \cong \frac{G}{Z(\chi)},$$

which proves (a like-wise well-known)

Corollary 4 *The degree $\chi(1)$ divides the index $|G : Z(\chi)|$ for all $\chi \in \mathrm{Irr}(G)$.*

3 A remark

It follows of course from the above that $N_n(1)$ is divisible by $|G|$ for all n. This can also be proved directly, which gives some information on the structure of $\Omega_{n,1}$. Let

$$\Psi_n = \{(x_1, \ldots x_n) \in G^n; x_1 \ldots x_n = gx_n \ldots x_1 g^{-1} \text{ for some } g \in G\}$$

and define a map

$$\begin{array}{rcl} f : \Omega_{n,1} & \to & \Psi_{n-1} \\ (x_1, \ldots, x_n) & \mapsto & (x_1, \ldots, x_{n-1}) \end{array}$$

($(x_1, \ldots, x_{n-1}) \in \Psi_{n-1}$ since we may take $g = x_n$). Let $(x_1, \ldots, x_n) \in \Omega_{n,1}$. Then the inverse image of $(x_1, \ldots, x_{n-1}) = f(x_1, \ldots, x_n)$ consists of those $(x_1, \ldots, x_{n-1}, y)$ for which $x_n x_{n-1} \ldots x_1 x_n^{-1} = y x_{n-1} \ldots x_1 y^{-1}$. Hence $f(x_1, \ldots, x_n) = f(x_1, \ldots, x_{n-1}, y)$ if and only if $x_n^{-1} y \in C_G(x_1 \ldots x_{n-1})$, the centralizer of $x_1 \ldots x_{n-1}$, and it follows that

$$|f^{-1}(x_1, \ldots, x_{n-1})| = |C_G(x_1 \ldots x_{n-1})|.$$

This shows that

$$N_n(1) = |\Omega_{n,1}| = \sum_{\bar{x} \in \Psi_{n-1}} |C_G(\pi\bar{x})|,$$

where we have used the notation $\pi\bar{x} = x_1 \dots x_{n-1}$ if $\bar{x} = (x_1, \dots, x_{n-1})$.

G acts on Ψ_{n-1} by

$$g.(x_1, \dots, x_{n-1}) = (gx_1g^{-1}, \dots, gx_{n-1}g^{-1}).$$

If $\bar{x}$ and $\bar{x}'$ belong to the same orbit, $\bar{x}' = g.\bar{x}$, then $\pi\bar{x}' = g(\pi\bar{x})g^{-1}$, so $|C_G(\pi\bar{x}')| = |C_G(\pi\bar{x})|$. If we denote the orbit through $\bar{x}$ by $O(\bar{x})$ and let $\bar{x}_1, \dots, \bar{x}_m$ be representatives for the orbits, then these observations show that

$$N_n(1) = \sum_{j=1}^{m} |O(\bar{x}_j)| \cdot |C_G(\pi\bar{x}_j)|.$$

Clearly the stabilizer $\mathrm{stab}(\bar{x})$ of $\bar{x} \in \Psi_{n-1}$ is a subgroup of $C_G(\pi\bar{x}_j)$. Since

$$|O(\bar{x}_j)| \cdot |\mathrm{stab}(\bar{x})| = |G|$$

and $|\mathrm{stab}(\bar{x})|$ divides $|C_G(\pi\bar{x}_j)|$ by Lagrange's theorem, $|G|$ divides $|O(\bar{x}_j)| \cdot |C_G(\pi\bar{x}_j)|$ and thus also $N_n(1)$.

References

[1] F.G. Frobenius, *Über Gruppencharaktere*, Gesammelte Abhandlungen Band III, p. 1-37 (J.P. Serre, ed.), Springer-Verlag, Berlin, 1968.

[2] I.M. Isaacs, Character theory of finite groups, Academic Press, New York 1976.