CHARACTERS OF FINITE GROUPS.

ANDREI YAFAEV

As usual we consider a finite group G and the ground field $F = \mathbb{C}$.

Let U be a $\mathbb{C}[G]$-module and let $g \in G$. Then g is represented by a matrix $[g]$ in a certain basis.

We define $\chi_U \colon G \longrightarrow \mathbb{C}$ by

$$\chi_U(g) = tr([g])$$

As 1 is represented by the identity matrix, we have

$$\chi(1) = \dim_{\mathbb{C}}(U)$$

The property $tr(AB) = tr(BA)$ shows that $tr(P^{-1}[g]P) = tr([g])$ and hence χ_U is independent of the choice of the basis and that isomorphic representations have the same character.

Suppose that $U = \mathbb{C}[G]$ with its basis given by the elements of G. This is the regular representation. The entries of the matrix $[g]$ are zeroes or ones and we get one on the diagonal precisely for those $h \in G$ such that $gh = h$. Therefore we have

$$\chi_U(g) = |\{h \in G : gh = h\}|$$

In particular we see that

$$\chi_U(1) = |G| \text{ and } \chi_U(g) = 0 \text{ if } g \neq 1$$

This character is called the **regular** character and it is denoted χ_{reg}.

Let

$$\mathbb{C}[G] = S_1^{n_1} \oplus \cdots \oplus S_r^{n_r}$$

be the decomposition into simple modules. The characters $\chi_i = \chi_{S_i}$ are called **irreducible characters**. By convention $n_1 = 1$ and S_1 is the trivial representation. The corresponding character χ_1 is called **principal character**. A character of a one dimensional representation is called a **linear character**. A character of an irreducible representation (equivalently simple module) is called an **irreducible character**. As one-dimensional modules are simple, linear characters are irreducible.

Let us look at linear character a bit closer : let χ be a linear character arising from a one dimensional module U, we have for any $u \in U$:

$$\chi(gh)u = (gh)u = \chi(g)\chi(h)u$$

hence χ is a homomorphism from G to $\mathbb{C}^*$.

Conversely, given a homomorphism $\phi\colon G \longrightarrow \mathbb{C}^*$, one constructs a one dimensional module $\mathbb{C}[G]$-module U by

$$gu = \phi(g)u$$

Linear characters are exactly the same as homomorphisms $\phi\colon G \longrightarrow \mathbb{C}^*$.

Here is a collection of facts about characters:

Theorem 0.1. *Let U be a $\mathbb{C}[G]$-module and let $\rho\colon G \longrightarrow \mathrm{GL}(U)$ be a representation corresponding to U. Let g be an element of G of order n. Then*

(1) *$\rho(g)$ is diagonalisable.*
(2) *$\chi_U(g)$ is the sum of eigenvalues of $[g]$.*
(3) *$\chi_U(g)$ is the sum of $\chi_U(1)$ nth roots of unity.*
(4) $\chi_U(g^{-1}) = \overline{\chi_U(g)}$
(5) $|\chi_U(g)| \leq \chi_U(1)$
(6) *$\{x \in G : \chi_U(x) = \chi_U(1)\}$ is a normal subgroup of G.*

Proof. (1) $x^n - 1$ is split hence the minimal polynomial splits.
(2) trivial
(3) The eigenvalues are roots of $x^n - 1$ hence are roots of unity. Then use that $\dim_{\mathbb{C}}(U) = \chi_U(1)$.
(4) If v is an eigenvactor for $[g]$, then $gv = \lambda v$. By applying g^{-1} we see that $g^{-1}v = \lambda^{-1}v$. As eigenvalues are roots of unity, $\lambda^{-1} = \overline{\lambda}$. The result follows.
(5) $\chi_(g)$ is a sum of $\chi_U(1)$ roots of unity. Apply triangle inequality.
(6) Suppose $\chi_U(x) = \chi_U(1)$, then in the sum all eigenvalues must be one (they are roots of 1 and lie on one line and sum is real). Hence $[g]$ is the identity matrix. Coversely, if $[g]$ is the identity, then of couse $\chi_U(g) = \chi_U(1)$. Hence $\ker(\rho) = \{x \in G : \chi_U(x) = \chi_U(1)\}$ is a normal subgroup of G.

□

1. Inner product of characters.

Let α and β be two class functions on G, their **inner product** is defined as the complex number :

$$(\alpha, \beta) = \frac{1}{|G|}\sum_{g\in G} \alpha(g)\overline{\beta(g)}$$

One easily checks that $(,)$ is indeed an inner product.

Therefore :

(1) $(\alpha, \alpha) \geq 0$ and $(\alpha, \alpha) = 0$ if and only if $\alpha = 0$.

(2) $(\alpha, \beta) = \overline{(\beta, \alpha)}$.
(3) $(\lambda\alpha, \beta) = \lambda(\alpha, \beta)$ for all α, β and $\lambda \in \mathbb{C}$.
(4) $(\alpha_1 + \beta_2) = (\alpha_1, \beta) + (\alpha_2, \beta)$

We have the following:

Proposition 1.1. *Let r be the number of conjugacy classes of G with representatives $g_1, \dots, g_r$. Let χ and ψ be two characters of G.*

(1)
$$< \chi, \psi > = < \psi, \chi > = \frac{1}{|G|} \sum_{g \in G} \chi(g)\psi(g^{-1})$$
and this is a real number.

(2)
$$< \chi, \psi > = \sum_{i=1}^{r} \frac{\chi_i(g_i)\overline{\psi(g_i)}}{|C_G(g_i)|}$$

Proof. We have $\overline{\psi(g)} = \psi(g^{-1})$, hence
$$< \chi, \psi > = \frac{1}{|G|} \sum_{g \in G} \chi_i(g_i)\overline{\psi(g_i^{-1})}$$
As $G = \{g^{-1} : g \in G\}$, we get the first formula. And the inner products of characters are real because $< \chi, \psi > = \overline{< \psi, \chi >}$.

The second formula is easy using the fact that characters are constant on conjugacy classes. □

We have seen already that irreducible characters form a basis of the space of class functions. We are now going to prove that it is in fact an **orthonormal** basis.

Let us write
$$\mathbb{C}[G] = W_1 \oplus W_2$$
where W_1 and W_2 have no simple submodule in common (we will say they do not have a common composition factor). Write $1 = e_1 + e_2$ with $e_1 \in W_1$ and $e_2 \in W_2$, uniquely determined.

Proposition 1.2. *For all $w_1 \in W_1$ and $w_2 \in W_2$ we have*
$$e_1 w_1 = w_1, \ e_2 w_2 = 0$$
$$e_2 w_1 = 0, \ e_2 w_2 = w_2$$
In particular $e_1^2 = e_1$ and $e_2^2 = e_2$ and $e_1 e_2 = e_2 e_1 = 0$. These elements are called idempotent.

Proof. Let $x \in W_1$. The function $w \mapsto wx$ is a $\mathbb{C}[G]$-homomorphism from W_2 to W_1. But, as W_1 and W_2 do not have any common composition factor, by Shur's lemma, this morphism is zero.

Therefore, for **any** $w \in W_2$ and $x \in W_1$,

$$wx = 0$$

and simiplarly $xw = 0$.

It follows that

$$w_1 = 1w_1 = (e_1 + e_2)w_1 = e_1 w_1$$

and

$$w_2 = 1w_2 = (e_1 + e_2)w_2 = e_2 w_2$$

□

We can calculate e_1 :

Proposition 1.3. *Let χ be the character of W_1, then*

$$e_1 = \frac{1}{|G|} \sum_{g \in G} \chi(g^{-1}) g$$

Proof. Fix $x \in G$. The function

$$\phi\colon w \mapsto x^{-1} e_1 w$$

is an endomorphism of $\mathbb{C}[G]$ (endomorphism of $\mathbb{C}$-vector spaces).

We have $\phi(w_1) = x^{-1} w_1$ and $\phi(w_2) = 0$. In other words, ϕ is the multiplication by x^{-1} on W_1 and zero on W_2. It follows that

$$tr(\phi) = \chi(x^{-1})$$

Now write

$$e_1 = \sum_{g \in G} \lambda_g g$$

For $g \neq x$, the trace of $w \mapsto x^{-1} g w$ is zero and for $g = x$, this trace is $|G|$.

Now, $\phi(w) = \sum x^{-1} \lambda g w$ hence $tr(\phi) = \lambda_x |G|$, hence

$$\lambda_x = \frac{\chi(x^{-1})}{|G|}$$

□

Corollary 1.4. *Let χ be the character of W_1, then*

$$< \chi, \chi >= \chi(1) = \dim W_1$$

Proof. We have $e_1^2 = e_1$ hence the coefficients of 1 in e_1 and e_1^2 are equal. In e_1, its $\frac{\chi(1)}{|G|}$ and in e_1^2 it's

$$\frac{1}{|G|^2} \sum_{g \in G} \chi(g^{-1})\chi(g) = \frac{1}{|G|} < \chi, \chi >$$

□

We now prove the following:

Theorem 1.5. *Let U and V be two non-isomorphic* **simple** $\mathbb{C}[G]$-*modules with characters χ and ψ. Then*

$$< \chi, \chi >= 1 \textit{ and } < \chi, \psi >= 0$$

Proof. Write

$$\mathbb{C}[G] = W \oplus X$$

where W is the sum of all simple $\mathbb{C}[G]$-submodules isomorphic to U (there are $m = \dim(U)$ of them) and X is the complement. In particular W and X have no common composition factor The character of W is $m\chi$. We have

$$< m\chi, m\chi >= m\chi(1) = m^2 \text{ because } \chi(1) = m$$

It follows that

$$< \chi, \chi >= 1$$

Let Y be the sum of all simple submodules isomorphic either to U or V and Z the complement of Y. Let $n = \dim(V)$. We have

$$\chi_Y = m\chi + n\psi$$

and we have

$m\chi(1)+n\psi(1) =< m\chi+n\psi, m\chi+n\psi >= m^2 < \chi, \chi > +n^2 < \psi, \psi > +mn(< \chi, \psi > + < \psi,$

We have $< \chi, \chi >=< \psi, \psi >= 1$ and $\chi(1) = m, \psi(1) = n$, hence

$$< \chi, \psi > + < \psi, \chi >= 2 < \chi, \psi >= 0$$

□

Let now $S_1, \dots, S_r$ be the complete list of non-isomorphic simple $\mathbb{C}[G]$-modules. If χ_i is a character of S_1, then

$$< \chi_i, \chi_j >= \delta_{ij}$$

(notice in particular that this imples that irreducible characters are distinct).

Let V be a $\mathbb{C}[G]$-module, write

$$V = S_1^{k_1} \oplus \cdot \oplus S_r^{k_r}$$

We have
$$\chi_V = k_1\chi_1 + \cdots + k_r\chi_r$$
We have
$$< \chi_V, \chi_i >=< \chi_i, \chi_V >= k_i$$
and
$$< \chi_V, \chi_V >= k_1^2 + \cdots + k_r^2$$
This gives a **criterion** to determine whether a given $\mathbb{C}[G]$-module is simple.

Theorem 1.6. *Let V be a $\mathbb{C}[G]$-module. Then V is simple if and only if*
$$< \chi_V, \chi_V >= 1$$

Proof. The if part is already dealt with.

Suppose $< \chi_V, \chi_V >= 1$. We have
$$1 =< \chi_V, \chi_V >= k_1^2 + \cdots + k_r^2$$
It follows that all k_is but one are zero. □

We also recover

Theorem 1.7. *Let V and W be two $\mathbb{C}[G]$-modules. Then $V \cong W$ if and only if $\chi_V = \chi_W$.*

Proof. Write $V = S_1^{n_1} \oplus \cdots \oplus S_r^{n_r}$ and $W = S_1^{k_1} \oplus \cdots \oplus S_r^{k_r}$ and let, as usual χ_is be the characters of S_i. Then we have $n_i =< \chi_V, \chi_i >$ and $k_i =< \chi_W, \chi_i >=< \chi_V, \chi_i >= n_i$. □

We see that characters form an **orthonormal** basis of the space of class functions.

We also obtain a way of decomposing the $\mathbb{C}[G]$-module V into simple submodules.

Proposition 1.8. *Let V be a $\mathbb{C}[G]$-module and χ an irreducible character of G. Then*
$$(\sum_{g\in G} \chi(g^{-1}g)V$$
is equal to the sum of those $\mathbb{C}[G]$-submodules of V with character χ.

Proof. Write
$$\mathbb{C}[G] = S_1^{n_1} \oplus \cdots \oplus S_r^{n_r}$$
and write W_1 be the sum of those submodules S_i having character χ (recall that χ is an irreducible character). Notice that W_1 is some $S_i^{n_i}$. Note that $n_i = \chi(1)$. The character of W_1 is $n_i\chi$. Let W_2 be the

complement of W_1. Let e_1 be as previously (idempotent corresponding to W_1). Then

$$e_1 = \frac{n_i}{|G|}\sum_{g\in G}\chi(g^{-1})g$$

Let V_1 be the sum of submodules of V having the character χ. Then $e_1V = V$ (recall $e_1v_1 = v_1$ for $v_1 \in V_1$), hence

$$V_1 = (\sum_{g\in G}\chi(g^{-1})g)V$$

□

This gives a procedure for decomposing a $\mathbb{C}[G]$-module V into simple submodules (for example $\mathbb{C}[G]$ itself).

(1) Choose a basis $v_1, \dots, v_n$ of V.
(2) For each irreducible character χ of G calculate $(\sum_{g\in G}\chi(g^{-1}g)v_i$ and let V_χ be the subspace generated by these vectors.
(3) V is now the direct sum of the V_χ where χ runs over irreducible characters. The character of V_χ is a multiple of χ.

Let's take an example. Let G be S_n and χ the trivial character. Let V be the permutation module and $v_1, \dots, v_n$ its basis. Then

$$(\sum_{g\in G}\chi(g^{-1})g)V = Span(v_1 + \cdots + v_n)$$

Hence V has a unique trivial $\mathbb{C}[G]$ submodule.

Character tables.

We now turn to character tables. Let G be a finite group, r the number of conjugacy classes and $g_1, \dots, g_r$ its representatives. There are exactly r irreducible characters, they are $\chi_1, \dots, \chi_r$. The character table is the $r \times r$ matrix with entries $\chi_i(g_j)$. There is always a row consisting of 1s corresponding to the trivial one dimensional representation.

Proposition 1.9. *The character table is invertible.*

Proof. This is because the irreducible characters form a basis of class fuctions. □

Recall the orthogonality relations.

$$< \chi_r, \chi_s >= \delta_{rs}$$

Rewrite this as:

$$\sum_{i=1}^{k}\frac{\chi_r(g_i)\overline{\chi_s(g_i)}}{|C_G(g_i)|} = \delta_{rs}$$

This gives the **row orthogonality** conditions.

Now,

$$\sum_{i=1}^{k} \chi_i(g_r)\overline{\chi_i(g_s)} = \delta_{rs}|C_G(g_r)| = \delta_{rs}|C_G(g_r)|$$

is the **column orthogonality**.

This needs proving.

Define class functions ψ_s for $1 \leq s \leq k$ by

$$\psi_s(g_r) = \delta_{rs}$$

As characters form a basis of the space of class functions, ψ_is are linear combinations of χ_i. We have

$$\psi_s = \sum_{i=1}^{k} \lambda_i \chi_i$$

As we know that $< \chi_i, \chi_j >= \delta_{ij}$, we have

$$\lambda_i =< \psi_s, \chi_i >= \frac{1}{|G|}\sum_{g\in G} \psi_s(g)\overline{\chi_i(g)}$$

By definition of ψ_s, we know that $\psi_s(g) = 1$ if g is conjugate to g_s and $\psi_s(g) = 0$ otherwise. The number of elements of G conjugate to g_s is

$$|g_s^G| = \frac{|G|}{|C_G(g_s)|}$$

It follows that

$$\lambda_i = \frac{\overline{\chi_i(g_s)}}{|C_G(g_s)|}$$

Now, using that $\delta_{rs} = \psi_s(g_r)$, we get the column orthogonality.

These relations are useful because sometimes they help to complete character tables.

Let S_3 be the symmetric group, it is isomorphic to D_6 by sending $(1, 2)$ to b and $(1, 2, 3)$ to a. There are three conjugacy classes, they are $\{1\}$, $\{a, a^2\}$, $\{b, ab, a^2b\}$ of sizes 1, 2 and 3 repsectively. We have two linear characters χ_1 and χ_2 corresponding to the trivial representation and the nontrivial of degree one (the sign of a permutation or $a \mapsto 1$ and $b \mapsto -1$). Let χ_3 be the character of the non-trivial two dimensional.

g_i	1	a	b
$\vert C_G(g_i)\vert$	6	3	2
χ_1	1	1	1
χ_2	1	1	-1
χ_3	?	?	?

We want to find the values of χ_3.

First of all, we already know that

$$6 = |G| = \chi_1(1)^2 + \chi_2^(1)^2 + \chi_3(1)^2$$

which gives $\chi_3(1)^2 = 1$, it follows that $\chi_3(1) = 2$ (this is the degree of the representation).

Let us write column orthogonality

$$\chi_1(g_r)\chi_1(g_s) + \chi_2(g_r)\chi_2(g_s) + \chi_3(g_r)\chi_3(g_s) = \delta_{rs}|C_G(g_r)|$$

Take $r = 2$, $g_2 = a$ and $s = 1$, $g_s = 1$ then

$$\chi_1(a)\chi_1(1) + \chi_2(a)\chi_2(1) + \chi_3(a)\chi_3(1) = 0$$

Then

$$1 + 1 + 2\chi_3(a) = 0$$

hence $\chi_3(a) = -1$.

Now take $r = 3$ and $s = 1$, we get

$$\chi_1(b)\chi_1(1) + \chi_2(b)\chi_2(1) + \chi_3(b)\chi_3(1) = 0$$

Hence $1 - 1 + 2\chi_3(b) = 0$.

We completely determined χ_3 and did not even need to use the sizes of conjugacy classes.

Another example which demonstrates the use of orthogonality.

Let G be a group of order 12 which has exactly four conjugacy classes. Suppose we are given the following characters χ_1, χ_2 and χ_3. Of course there is a fourth irreducible character χ_4. The question is to determine χ_4.

g_i	g_1	g_2	g_3	g_4
$\|C_G(g_i)\|$	12	4	3	3
χ_1	1	1	1	1
χ_2	1	1	ω	ω^2
χ_3	1	1	ω^2	ω

Of course we always have : $1 + 1 + 1 + \chi_4(1)^2 = 12$, hence

$$\chi_4(1)^2 = 9$$

hence $\chi_4(1) = 3$ and the representation is 3-dimensional.

Now, we apply column orthogonality to the first and second column:

$$1 + 1 + 1 + 3\overline{\chi_4(g_2)} = 0$$

which gives $\chi_4(g_2) = -1$.

The orthogonality between columns one and 3 and 4 gives

$$\chi_3(g_3) = \chi_4(g_4) = 0$$

In what follows we will prove that the integers k_i that occur in the decomposition of $\mathbb{C}[G]$ actually divide G.

Recall that a complex number α is called **algebraic integer** if it is a root of a monic polynomial with integer coefficients. The set of algebraic integers is a subring of $\mathbb{C}$, in particular the sum an product of two of them is an algebraic integer.

The property we are groing to use is the following:

Lemma 1.10. *Let $a = \frac{p}{q}$ be a rational number, we suppose that p and q are* **coprime**. *Suppose that a is an algebraic integer, then a is an integer.*

Proof. By assumption a satisfies

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

where a_is are integers.

This gives $p^n = q \times (*)$ where $(*)$ is some integer. It follows that $q = 1$ because p and q are coprime. □

Proposition 1.11. *Let g_i be in G and let $c_i := [G : C_G(g_i)]$ be the index of the centraliser of g_i in G. Then for any character χ_j of G, the value*

$$\frac{c_i \chi_j(g_i)}{\chi_j(1)}$$

is an algebraic integer.

Proof. Let χ_j be a character correspondig to S_j. Let K_i be the conjugacy class of g_i and a be the sum (in $\mathbb{C}[G]$) of all elements in K_i. Of course a is in the centre of $\mathbb{C}[G]$, therefore left multiplication by a is an endomorphism of $\mathrm{End}_{\mathbb{C}[G]}(S_j)$. But, by a version of Shur's lemma, we know that

$$as = cs$$

for some $c \in \mathbb{C}$ and all $s \in S_j$. It follows that the trace of a is $c\chi_j(1)$ (recall that $\chi_j(1) = \dim(S_j)$). On the other hand, the trace of the matrix defined by multiplication by a is $c_j \chi_j(g_i)$. We therefore have

$$c = \frac{c_i \chi_j(g_i)}{\chi_j(1)}$$

As a is central, left multiplication by a also defines a $\mathbb{C}[G]$-endomorphism of $\mathbb{C}[G]$. Let M_a be the corresponding matrix. Each entry of M_a is an integer, as a is a sum of group elements, therefore $\det(xI - M_a)$ is a polynomal with integer coefficients. But c is an eigenvalue of a (the eigenspace is preciesely S_j), hence c is a root of $\det(xI - M_a)$ and hence it's an algebraic integer. □

We can now prove:

Theorem 1.12. *For any irreducible character χ_i, $\chi_i(1)$ divides $|G|$.*

Proof. Let $g_1, \ldots, g_r$ be the set of representatives of conjugacy classes. of G and let $c_i = [G : C_G(g_i)]$ be the size of the conjugacy class. As we have $< \chi_i, \chi_i >= 1$, we have

$$\frac{1}{|G|} \sum_{g \in G} \chi_j(g)\overline{\chi_j(g)} = 1$$

It follows that

$$\begin{aligned} \frac{|G|}{\chi_j(1)} &= \frac{1}{\chi_j(1)} \sum_{i=1}^{r} c_j \chi_j(g_i)\overline{\chi_j(g_i)} \\ &= \sum_{i=1}^{r} \frac{c_i \chi_j(g_i)}{\chi_j(1)} \overline{\chi_j(g_i)} \end{aligned}$$

and therefore $\frac{|G|}{\chi_j(1)}$ is an algebraic integer. But it is also a rational number, hence an integer. □

As application, recall that A_4 has order 12 and 4 conjugacy classes. We have

$$1 + k_2^2 + k_3^2 + k_4^2 = 12$$

Divisors of 12 are $1, 2, 3, 4, 6, 12$ but only $1, 2, 3$ can occur as others squared are bigger than 12. Therefore the only possibility is $1, 1, 1, 3$.

Look at S_4. The order is 24, there are 5 conjugacy classes :

$$(1), (1, 2), (1, 2, 3), (1, 2)(3, 4), (1, 2, 3, 4)$$

and we have two irreducible representations of degree one : the trivial one and the sign.

We have therefore :

$$1 + 1 + k_3^2 + k_4^2 + k_5^2 = 24$$

and therefore $k_3^2 + k_4^2 + k_5^2 = 22$ and the possible divisors of 24 ate $1, 2, 3, 4, 6, 8, 12, 24$. Only $1, 2, 3, 4$ can occur, others squared are too large.

The only possibility is $3, 3, 2$. The irreducible representations of S_4 are $1, 1, 2, 3, 3$.

Our aim now is to prove the following theorem of Burnside:

Theorem 1.13 (Burnside)**.** *Let G be a finite group with $|G| = p^a q^b$ with p and q prime numbers. Then G is solvable.*

Lemma 1.14. *Let χ_i be an irreducible character of G corresponding to a representation ρ_i. If G has a conjugacy class K_j such that $|K_j|$ and $\chi_i(1)$ are relatively prime, then for any $g \in K_j$, either $\chi_i(g) = 0$ or $|\chi_i(g)| = \chi_i(1)$.*

Proof. Suppose we are in the situation of the lemma. There exists integers m, n such that

$$m|K_j| + n\chi_i(1) = 1$$

Multiplying by $\frac{\chi_i(g)}{\chi_i(1)}$, we obtain

$$m|K_j|\frac{\chi_i(g)}{\chi_i(1)} + n\chi_i(g) = \frac{\chi_i(g)}{\chi_i(1)}$$

Therefore, $a = \frac{\chi_i(g)}{\chi_i(1)}$ is an algebraic integer. On the other hand, $\chi_i(g)$ is a sum of $\chi_i(1)$ roots of unity. Therefore a is an average of $\chi_i(1)$ roots of unity.

We apply the following lemma:

Lemma 1.15. *Let c be a complex number that is an average of mth roots of unity.* **If** *c is an algebraic integer, then $c = 0$ or $|c| = 1$.*

Proof. Write

$$c = \frac{a_1 + \cdots + a_d}{d}$$

where a_is are roots of $x^m - 1$. Since $|a_i| = 1$ for $1 \leq i \leq d$, the triangle inequality shows that

$$|c| \leq 1$$

Now, we assumed that c is an algebraic integer.

Let G be the Galois group of $\mathbb{Q}(a_1, \ldots, a_d)/\mathbb{Q}$. Let $\sigma \in G$, all $\sigma(a_i)$ are mth roots of unity. It follows that

$$|\sigma(c)| \leq 1$$

Let

$$b = \prod_{\sigma \in G} \sigma(c)$$

Of course all $\sigma(c)$ are algebraic integers and b is an algebraic integer. Of course $\sigma(b) = b$ hence $b \in \mathbb{Q}$ and algebraic integer hence $b \in \mathbb{Z}$. But $|c| \neq 1$ implies $|b| < 1$, therefore $b = 0$, this forces $c = 0$. ☐

The lemma shows that either $|a| = 1$ or $a = 0$., therefore either $\chi_i(g) = 0$ or $|\chi_i(g)| = \chi_i(1)$. ☐

We derive the following:

Theorem 1.16. *Let G be a non-abelian* **simple** *group. Then $\{1\}$ is the only conjugacy class whose cardinality is a prime power.*

Remark 1.17. *If the conjugacy class has just one element (1 for example), then its cardinality is a prime power : p^0.*

Proof. Let $g \in G$, $g \neq 1$ such that g^G has order p^n **with** $n > 0$.

(if n is zero, then g is in the centre of G hence G is either not simple or abelian...)

By column orthogonality, we have

$$\sum_{i=1}^{r} \chi_i(g)\chi_i(1) = 0$$

where χ_is are distinct irreducible characters of G with χ_1 being the character of the trivial representation.

We have

$$1 + \sum_{i=2}^{r} \chi_i(g)\chi_i(1) = 0$$

This gives

$$1/p = -\sum_{i=1}^{r} \frac{\chi_i(g)\chi_i(1)}{p}$$

Suppose p is a factor of $\chi_i(1)$ for all $i > 1$ such that $\chi_i(1) \neq 0$, then the relation above shows that $1/p$ is an alegebraic integer and this is not the case. Hence $\chi_i(g) \neq 0$ and p does not divide $\chi_i(1)$ for some i. Because $\chi_i(g) \neq 0$, and $|g^G| = p^m$ and $\chi_i(1)$ are coprime by what we have just seen above, the lemma above shows that $|\chi_i(g)| = \chi_i(1)$. But $\{g \in G : |\chi_i(g)| = \chi_i(1)\}$ is a normal subgroup of G (it is the kernel of the corresponding representation). As G is simple, $g = 1$. This finishes the proof. □

This theorem can be reformulated as follows: if the finite group G has a conjugacy class of order p^k, then G is not simple.

Before proving Burnside's theorem, let us recall some notions from group theory.

Let G be a finite group and p a prime number. A subgroup P is called a **Sylow p-subgroup** of G if $|P| = p^n$ for some integer $n \geq 1$ such that p^n is a divisor of $|G|$ but p^{n+1} is not a divisor of $|G|$.

If $p||G|$, then Sylow's first theorem guarantees that G contains a Sylow p-subgroup.

A chain of subgroups $G = N_0 \supset N_1 \supset \cdots \supset N_n$ such that

(1) N_i is a normal subgroup in N_{i-1} for $i = 1, 2, \ldots, n$.
(2) N_{i-1}/N_i is simple for $i = 1, 2, \ldots, n$.

(3) $N_n = \{1\}$.

is called a **composition series**. The factors N_{i-1}/N_i are called **composition factors**. A group is called **solvable** if there exists a composition series with N_{i-1}/N_i **abelian**.

In Galois theory it is proved that a polynomial $f(x)$ is solvable by radicals if and only if it's Galois group is solvable.

Theorem 1.18 (Burnside). *If G is a finite group of order $p^a q^b$ where p, q are prime, then G is solvable.*

Proof. Let G_i be a composition factor. We need to show that G_i is abelian. By assumption G_i is simple and $|G_i|$ divides $|G|$ therefore $|G_i| = p^{a'} q^{b'}$ for some $a' \leq a, b' \leq b$.

Let P be a p-Sylow of G_i. Any p-group has a non-trivial centre (*) and let g be a non-trivial element of the centre. Then $P \subset C_G(g)$ and $|P| = p^a$. It follows that $[G : C_G(g)]$ is not divisible by p and is therefore a power of q. But $[G : C_G(g)] = |g^G|$, this contradicts the theorem above unless G is abelian. ☐

(*) **Any p-group has a non-trivial centre.**

Indeed, let G be a group of order p^n. Each conjugacy class has order p^{k_i} dividing p^n, hence we get

$$p^n = |Z(G)| + \sum_i p^{k_i}$$

It follows that $|Z(G)| \equiv 0 \bmod p$ hence is not trivial.