CHARACTERS OF FINITE GROUPS, ALGEBRAIC INTEGERS, AND BURNSIDE

The goal of this note is to write down the proofs of results about characters of irreducible representations of finite groups, and specifically, the result (due to Burnside) that each of them vanishes at at least one element of the group. We present various results told to us by various people, and conclude with two theorems by Gallagher, which strengthen or generalize Burnside's theorem for finite groups. As an aside, we write down several other facts (from Isaacs's book [Isa]) involving conjugacy class sums and algebraic integers.

1. Algebraic numbers whose conjugates all lie on a circle

We start with some preliminaries, which are interesting in their own right. We will always work over $\mathbb{C}$. Let us say that a *Weil number* is an algebraic number (i.e., a complex number with minimal polynomial $f \in \mathbb{Q}[T]$), all of whose complex conjugates (i.e., roots of f) have the same absolute value. A *Weil integer* is a Weil number that is also an algebraic integer (i.e., a complex number with minimal polynomial monic in $\mathbb{Z}[T]$).

One may ask if every Weil number of absolute value 1 is necessarily a root of unity. However, this is false. For example, if a is any rational number such that $-2 < a < 2$ and a is not an integer, then the roots of the polynomial $x^2 + ax + 1$ are (nonreal) Weil numbers of absolute value 1. However, they are not roots of unity because, by construction, they are not algebraic integers. (To see this, note that the quadratic is irreducible since it has no rational solutions.)

However, the following is more plausible, and indeed true:

Theorem 1 (Kronecker). *A Weil integer of absolute value 1 is necessarily a root of unity.*

Apparently this observation is due to Kronecker, and the proof goes like this:

Let us define the degree of an algebraic number to be the degree of its minimal polynomial over $\mathbb{Q}$. The first observation is that for a fixed integer $d > 0$, there is a large constant $C > 0$ (depending on d) such that if $z \in \mathbb{C}$ is any Weil number of absolute value 1 and degree at most d, then all coefficients of the minimal polynomial of z are bounded by C (in absolute value).

Proof. Given a Weyl number z of degree d and modulus 1, let the minimal polynomial over $\mathbb{Q}$ be $\sum_{i=0}^d a_i T^i$, with $a_d = 1$. This splits over $\mathbb{C}$ as $\prod_{j=1}^d (T - z_j)$, say, with $z_1 = z$. Then by the triangle inequality,

$$|a_i| = \left| (-1)^i \sum_{1 \leq l_1 < l_2 < \cdots < l_i \leq d} z_{l_1} z_{l_2} \dots z_{l_i} \right| \leq \sum 1 = \binom{d}{i}.$$

In particular, all coefficients of the minimal polynomial of any Weil number of degree at most d and modulus 1, are at most $\binom{d}{\lfloor d/2 \rfloor}$ in modulus. □

This implies that the set of Weil integers of absolute value 1 and degree at most d is actually finite (because all of them are roots of a finite collection of polynomials).

Now let z be any Weil integer of absolute value 1, and let $d > 0$ be the degree of z. If k is any positive integer, then z^k is also a Weil integer of absolute value 1, and the degree of z^k is at most d. It follows that the set of positive integer powers of z is finite. In particular, $z^k = z^m$ for two distinct positive integers m and k, which forces z to be a root of unity. □

This result has the following application, as seen in [Ga1]. It is used later, to strengthen Burnside's Theorem, stated as Theorem 3 below.

Corollary 2. *Suppose z is an algebraic integer with conjugates $z_1, \dots, z_d$. If $z \neq 0$, then $\sum_i |z_i| \geq d$, with equality if and only if z is a root of unity.*

Proof. (As in [Ga1].) By the AM-GM inequality, $\sum_i |z_i| \geq d \sqrt[d]{\prod_i |z_i|}$. But the product of the z_i is the norm of z, and this is a nonzero rational integer. In particular, the inequality is shown, and it is an equality if and only if $\prod_i z_i = \pm 1$ and the $|z_i|$'s are all equal to 1. But then we are done by Theorem 1. □

2. Burnside's theorem from Isaacs's book

The main result that is shown here is:

Theorem 3 (Burnside)**.** *If V is an irreducible representation (over $\mathbb{C}$) of a finite group G, and $\dim V > 1$, then the character χ_V vanishes at at least one $g \in G$.*

The proof is more or less as in [Isa, Chapter 3]. We need a few preliminaries first. For a subset of a group $S \subset G$, let $\langle S \rangle$ be the subgroup generated by S. For $S = \{g\}$, write $\langle g \rangle$.

Lemma 4. *Suppose $\rho : G \to GL(V)$ is a finite-dimensional representation of a finite group G. Then for all $g \in G$, $\chi_\rho(g)$ is an algebraic integer. If S is the set of cyclic generators of $\langle g \rangle$, then*

$$\prod_{s \in S} \chi_\rho(s) \in \mathbb{Z}.$$

Proof. Note that since $\rho(g)$ has finite order, the eigenvalues of $\rho(g)$ are all roots of unity, hence algebraic integers, and hence their sum, which is $\chi_\rho(g)$, is also an algebraic integer. Next, let $\mathbb{F}$ be the subfield of $\mathbb{C}$ obtained by attaching all the roots-of-unity eigenvalues of all $\rho(g)$ to $\mathbb{Q}$. Since all these generate a finite (and hence cyclic) subgroup of roots of unity, hence $\mathbb{F}$ is a cyclotomic extension, and hence Galois. Suppose ζ is a generator of the above cyclic subgroup.

Moreover, the eigenvalues are powers of the eigenvalues of $\rho(g)$, so we may assume that ζ generates the subgroup generated by the eigenvalues of $\rho(g)$. But then $\chi_\rho(g)$ is a polynomial in ζ, whence $\chi_\rho(g^k)$ is a polynomial in ζ^k for all k. It follows that since the order of ζ and $\langle g \rangle$ are equal, hence $\prod_{s \in S} \chi_\rho(s)$ is invariant under the Galois automorphisms of $\mathbb{F}/\mathbb{Q}$: namely, the ones that take ζ to ζ^k (with k coprime to the order of $\langle g \rangle$). Consequently, it is a rational number, by the Fundamental Theorem of Galois Theory.

Finally, every rational number that is also a product of algebraic integers, is itself an algebraic integer, and hence an integer. □

Lemma 5. *Suppose G is a finite cyclic group, and $\rho : G \to GL(V)$ a (finite-dimensional) representation. Let S be the subset of generators of G. If $\chi_\rho(s) \neq 0\ \forall s \in S$, then*

$$\sum_{s \in S} |\chi_\rho(s)|^2 \geq |S|.$$

Proof. We use the AM-GM inequality:

$$\sum_{s \in S} |\chi_\rho(s)|^2 \geq |S| \sqrt[|S|]{\prod_{s \in S} |\chi_\rho(s)|^2}.$$

By Lemma 4, the quantity inside the radical sign is an integer. If no $\chi_\rho(s)$ is zero, then its absolute value must be at least 1, whence so is its $|S|$th root, and we are done. $\square$

We are now ready to show the main result.

Proof of Theorem 3. The row orthogonality of the irreducible character χ_ρ of G can be rewritten as:

$$\sum_{g \in G, g \neq 1} |\chi_\rho(g)|^2 = |G| - (\dim V)^2.$$

Now assume that $\chi_\rho(-)$ is never zero on G. Introduce an equivalence relation $\sim$ on G as follows: $g \sim h$ if they generate the same subgroup: $\langle g \rangle = \langle h \rangle$. The equivalence classes partition G, and for each class S, Lemma 5 applies. Summing over all classes $S \neq \{1\}$, we obtain:

$$|G| - (\dim V)^2 = \sum_{(G \setminus \{1\})/\sim} |\chi_\rho(g)|^2 \geq |G| - 1,$$

whence $\dim V = 1$, as claimed. $\square$

Let us write down another result in this spirit.[1]

Lemma 6. *If G is any compact Lie group and $\rho : G \to GL(V)$ is a finite-dimensional representation such that $|\chi_\rho(-)|$ is constant on all of G, then V is a direct sum of copies of one one-dimensional G-module.*

If instead of $|\chi_\rho(-)|$, we have that $\chi_\rho(-)$ is itself constant on G, then V is a direct sum of copies of the trivial representation.

It may be worthwhile to recall the following facts about compact groups G:

- Every $g \in G$ is contained inside a *maximal torus* T.
- Every pair of maximal tori in G is conjugate; every torus is isomorphic to $(S^1)^r$, where r is the *rank* of G.
- Since the finite order elements in S^1 constitute a dense subset, hence the set of finite order elements in G is dense.
- Every irreducible representation (over $\mathbb{C}$) of a torus is one-dimensional. Every finite-dimensional representation of a torus is completely reducible.
- Every element of a torus acts diagonalizably on a finite-dimensional representation over $\mathbb{C}$, because every Jordan canonical form of finite order is a diagonal matrix.

---

[1] I was told this by Sam Raskin.

- For every compact group G, there exists a short exact sequence
$$1 \to G_0 \to G \to G/G_0 \to 1,$$
where G_0 is the connected component of G that contains the identity, and the group of components $G/G_0 = \pi_0(G)$ of G is finite since G is compact.

Proof. In the first case, we show that every element $g \in G$ acts on every $v \in V$ by the scalar $\chi_\rho(g)/\dim V$. To show this, it is enough to consider g to have finite order, because such elements are dense in G.

So suppose that $\rho(g)$ has finite order; then its eigenvalues λ_i (say) are all roots of unity. Moreover, by the triangle inequality,
$$|\chi_\rho(g)| = \left|\sum_i \lambda_i\right| \leq \sum_i |\lambda_i| = \dim \rho = \chi_\rho(1) = |\chi_\rho(1)|. \tag{7}$$
Hence the inequality is an equality, which means that all eigenvalues are equal, for each g. From the "standard facts" above, every $g \in G$ acts diagonalizably on V, so $\rho(g)$ equals a scalar matrix. The scalar is clearly $\chi_\rho(g)/\dim V$, as claimed above.

But now we are done: since every $\rho(g)$ is a scalar matrix, then V is the direct sum of copies of the one-dimensional representation given by $\rho' = \frac{1}{\dim \rho} \cdot \chi_\rho = \rho_{11}$, the first diagonal entry of ρ.

The proof in the second case is similar. We now require:
$$\chi_\rho(g) = \sum_i \lambda_i = n,$$
whence $|\chi_\rho(g)| = |\chi_\rho(1)|$. But then all eigenvalues are equal by Equation (7). We now conclude that they are all equal to 1. We conclude that the previous part holds, and moreover, the one-dimensional representation is given by: $\rho'(g) = 1 \ \forall g \in G$. We are done. ☐

3. Peter Gallagher's generalizations

Now note the works [Ga1, Ga2] by Gallagher. In [Ga2], he generalizes Burnside's Theorem to all compact groups.

Theorem 8 ([Ga2])**.** *If V is an irreducible representation (over $\mathbb{C}$) of a compact group G, and $\dim V > 1$, then the character χ_V vanishes at at least one $g \in G$.*

In [Ga1], Gallagher also strengthens Burnside's Theorem for finite groups. To explain his results, we need some more notation.

Definition 9. Suppose G is a finite group, $g \in G$, and χ be an irreducible character of G.

- Let $k(G)$ equal the number of irreducible characters of G - equivalently, the number of conjugacy classes of G.
- Let $n(g)$ be the number of χ such that $\chi(g) = 0$, and $n(\chi)$ be the number of g such that $\chi(g) = 0$.
- Let $C(g)$ be the centralizer of g in G, and $K(g)$ be the smallest normal subgroup of G containing $[g, G]$.

- Let $Z(\chi)$ be the subset $\{g \in G : |\chi(g)| = \chi(1)\}$, and let ρ_χ denote the underlying representation. Thus, $\deg \chi = \dim \rho_\chi = \chi(1)$.

Gallagher remarks since $|\chi|$ is a function on $G/Z(\chi)$, hence $n(\chi)$ is a multiple of $|Z(\chi)|$. Another of his remarks follows from Corollary 2. It says that the following are equivalent:

- $g \in Z(\chi)$.
- $\rho(g)$ is a scalar matrix (where ρ is the representation corresponding to χ).
- χ is a character of $G/K(g)$.

In particular, $Z(\chi)$ is a normal abelian subgroup of G.

We can now state and prove both parts of Gallagher's result.

Theorem 10 ([Ga1]). *Suppose G is a finite group.*

1. *For all irreducible characters χ of G,*
$$n(\chi) \geq (\chi(1)^2 - 1)|Z(\chi)|,$$
and unless the image of χ is $\{0, 1, \chi(1)\}$, this can be strengthened to: $n(\chi) \geq \chi(1)^2|Z(\chi)|$.
2. *For all $g \in G$,*
$$n(g) \geq k(G) - |C(g)|,$$
with equality if and only if $K(g) = [G, G]$ and $|\chi(g)| = 0, 1$ for each irreducible χ.

As Gallagher now remarks, the first part shows Burnside's Theorem if $\chi(1) > 1$, and the second part shows that each "larger than average" conjugate class (we now call it "conjugacy class") is a zero for some character.

Proof. Suppose ζ is a primitive $|G|$th root of unity, and $\mathcal{G}$ is the Galois group of the cyclotomic extension $[\mathbb{Q}(\zeta) : \mathbb{Q}]$. Then $\mathcal{G} \cong (\mathbb{Z}/|G|\mathbb{Z})^\times$. The claim is that $\mathcal{G}$ acts both on the set of elements, and on the set of irreducible characters of G, and these are Gallagher's starting points for proving each of the two parts.

1. $\mathcal{G}$ acts as permutations of the elements of G as follows: for $\sigma \in \mathcal{G}$ and $g \in G$, define $\sigma(g) = g^\sigma$. One checks that for any $g \in G$, the order of g is a factor of $|G|$, and hence coprime to σ. This allows us to show that σ is surjective : $G \to G$, and hence injective as well, since G is finite.

   Now for all χ and all $g \in G$, $\rho_\chi(g)$ is a diagonalizable matrix with order dividing $|G|$, so its eigenvalues are all powers of ζ. Writing them as ζ^{n_i}, we compute, for any integer n:
$$\sigma(\chi^n(g)) = \sigma\left(\sum_i \zeta^{n_i}\right)^n = \left(\sigma(\sum_i \zeta^{n_i})\right)^n = \left(\sum_i \zeta^{n_i \sigma}\right)^n = (\chi(\sigma(g)))^n = \chi^n(\sigma(g)).$$

   It follows that the average of $|\chi^2(-)|$ over the $\mathcal{G}$-orbit of $g \in G$ equals the average of (the absolute values of) the conjugates of the algebraic integer $\chi^2(g)$. By Corollary 2, if $\chi(g) \neq 0$, then this average value is at least 1, with equality only if $|\chi(\sigma(g))| = 1\ \forall \sigma$. We also know that $\mathcal{G}$ preserves $Z(\chi)$ for all χ. Thus, we now compute, using the row orthogonality of the irreducible characters:

$$|G| = \sum_{g \in G} |\chi^2(g)| = \sum_{g \in Z(\chi)} |\chi^2(g)| + \sum_{g \notin Z(\chi)} |\chi^2(g)|.$$

Every term in the first sum is $(\dim \rho_\chi)^2 = \chi(1)^2$, and every term in the second sum is 0 or at least 1, from above. We conclude that

$$|G| \geq \chi(1)^2 |Z(\chi)| + (|G| - n(\chi) - |Z(\chi)|),$$

whence we get the desired inequality of the first part. Moreover, equality implies that the image of χ is $\{0, 1, \chi(1)\}$. Otherwise we get: $n(\chi)/|Z(\chi)| > \chi(1)^2 - 1$. But the left-hand side here is an integer by above remarks, which proves the other assertion in this part.

(2) We make a nontrivial assertion here, about the action of $\mathcal{G}$ on the set of (irreducible) characters of G: define, given $\sigma \in \mathcal{G}$ and a character χ, the new map: $\sigma(\chi)(g) = \sigma(\chi(g))$ for all g. That $\sigma(\chi)$ is a character of G follows, for example, from pages 87–88 of Andre Weil's *L'Intégration dans les Groupes Topologiques et ses Applications* (1938). In that book, the author characterizes (irreducible) characters χ as being the normalized solutions of the functional equation

$$|G| \chi(g_1) \chi(g_2) = \chi(1) \sum_{g_0 \in G} \chi(g_1 g_0 g_2 g_0^{-1}).$$

To get back to our result, for each $g \in G$, the size of its centralizer subgroup is (using the column orthogonality relations):

$$|C(g)| = \sum_{\chi} |\chi^2(g)| = \Sigma' + \Sigma'',$$

where the first sum is over those χ such that $|\chi(g)| = \chi(1)$, and the second sum is over the others. By above remarks, the first sum is over the characters of $G/K(g)$, so the column orthogonality relations again yield that the first sum equals the size of $C_{G/K(g)}(g)$. But this is all of $G/K(g)$, which also implies that the number of characters that we sum over in Σ', is precisely $k(G/K(g))$.

Now using the same argument as in the first part,

$$|C(g)| = |G/K(g)| + [k(G) - k(G/K(g)) - n(\sigma)],$$

with equality only if $|\chi(g)| \in \{0, 1, \chi(1)\}$. But we also have $|G/K(g)| \geq k(G/K(g))$, with equality if and only if $G/K(g)$ is abelian, if and only if $K(g) = [G, G]$. Using these facts, it follows that

$$n(g) \geq k(G) - |C(g)|,$$

with equality if and only if $K(g) = [G, G]$ and $|\chi(g)| \in \{0, 1, \chi(1)\}$ for each χ. The proof is complete if we show that $|\chi(g)| = \chi(1) \implies \chi(1) = 1$, in the case of equality. But this is easy: if we have equality as well as $|\chi(g)| = \chi(1)$, then χ must be a character of $G/K(g) = G/[G, G]$ from above remarks. But since this is an abelian group, all irreducible characters are one-dimensional, whence $\chi(1) = 1$.

□

4. CONJUGACY CLASS SUMS AND ALGEBRAIC INTEGERS

In this section, we present an assortment of results from [Isa, Chapter 3], which involve the center of the group algebra of a finite group and algebraic integers. We end by proving Burnside's well-known solvability theorem.

Throughout this section, G is a finite group, and χ an irreducible character (over $\mathbb{C}$). We need one more piece of notation: given an element of a group $g \in G$, define $\mathcal{O}_g$ to be the G-orbit of g under the adjoint action (i.e., the conjugacy class of $g \in G$). Thus, $\mathcal{O}_g$ is in bijection with $G/C(g)$.

Suppose G is a group and $Z(\mathbb{C}G)$ the center of the group algebra; then the center of the *group ring* $\mathbb{Z}G$ has a $\mathbb{Z}$-basis consisting of the *class sums* $\Sigma_{\mathcal{O}} := \sum_{g \in \mathcal{O}} g$, where $\mathcal{O}$ runs over the various orbits in G under the adjoint action. Moreover, for every irreducible character χ of G and central element $z \in Z(\mathbb{C}G)$, $\rho_\chi(z)$ is a scalar matrix by Schur's Lemma. This yields an algebra map

$$\omega_\chi : Z(\mathbb{C}G) \to \mathbb{C}.$$

Proposition 11. *Given a finite group G and χ, define ω_χ as above. Given $g \in G$,*

$$\omega_\chi(\Sigma_{\mathcal{O}_g}) = \frac{\chi(g)|\mathcal{O}_g|}{\chi(1)}$$

is an algebraic integer.

Proof. There are two assertions here. First, we compute the trace in the equation: $\rho_\chi(\Sigma_{\mathcal{O}_g}) = \omega_\chi(\Sigma_{\mathcal{O}_g})\mathrm{Id}$. Thus, we get:

$$\chi(1)\omega_\chi(\Sigma_{\mathcal{O}_g}) = \chi(\mathcal{O}_g) = \sum_{h \in \mathcal{O}_g} \chi(h) = |\mathcal{O}_g|\chi(g).$$

To show the second part, let $\mathcal{O}_i$ be the various conjugacy classes in G, with class sums Σ_i. From above, we have the structure constants $a_{ijk} \in \mathbb{Z}$ such that for all i, j,

$$\Sigma_i \cdot \Sigma_j = \sum_k a_{ijk} \Sigma_k.$$

Let S be the $\mathbb{Z}$-span of $s_i := \omega_\chi(\Sigma_i)$ for all i. Then $\omega_\chi(1) = 1$, whence (from above) $\mathbb{Z} \subset S \subset \mathbb{C}$ as subrings. We now show, more generally, that any element of S is an algebraic integer (whence so is each s_i). So given $s \in S$, suppose $s s_i = \sum_j b_{ij} s_j$, where (from above) $b_{ij} \in \mathbb{Z}$ for all i, j. Then we get: $Bv = sv$, where $B = ((b_{ij}))$ and v is the column vector $(s_j)_j$. Thus, s is an eigenvalue of B, hence a root of the monic polynomial $\det(t\mathrm{Id} - B)$, and we are done. □

Corollary 12. *For all irreducible χ for a finite group G, $\chi(1)$ divides $|G|$.*

A stronger result can be found in [Isa, Chapter 3]: namely, that $\chi(1)$ divides $[G : Z(\chi)]$.

Proof. The row orthogonality relation for χ yields: $|G| = \sum_{g \in G} \chi(g)\chi(g^{-1})$. Decompose this sum over all orbits $\mathcal{O}_i$, and choose and fix elements $g_i \in \mathcal{O}_i$ for all i. Then by Proposition 11,

$$|G| = \sum_i |\mathcal{O}_i|\chi(g_i)\chi(g_i^{-1}) = \sum_i \chi(1)\omega_\chi(\Sigma_i)\chi(g_i^{-1}).$$

Hence $|G|/\chi(1)$ equals both a positive rational number and the sum $\sum_i \omega_\chi(\Sigma_i)\chi(g_i^{-1})$, which is an algebraic integer, again by Proposition 11. Therefore $|G|/\chi(1) \in \mathbb{Z}$ as required. $\square$

We now proceed towards Burnside's solvability theorem. We need a few preliminary results, the first of which is again due to Burnside. Recall the definition of $Z(\chi)$ in an earlier section.

Proposition 13 (Burnside)**.** *Given $g \in G$ such that $\chi(1)$ and $|\mathcal{O}_g|$ are coprime, either $g \in Z(\chi)$, or $\chi(g) = 0$.*

Proof. Choose integers u, v such that $u\chi(1) + v|\mathcal{O}_g| = 1$. Then

$$\frac{\chi(g)(1 - u\chi(1))}{\chi(1)} = v\frac{\chi(g)|\mathcal{O}_g|}{\chi(1)} = v\omega_\chi(\Sigma_{\mathcal{O}_g})$$

is an algebraic integer by Proposition 11. Hence so is

$$v\omega_\chi(\Sigma_{\mathcal{O}_g}) + u\chi(g) = u\chi(g) + v\frac{\chi(g)|\mathcal{O}_g|}{\chi(1)} = \frac{\chi(g)}{\chi(1)}.$$

Call this algebraic integer α; now suppose that $g \notin Z(\chi)$, so that $|\alpha| < 1$. We show that $\alpha = 0$, which proves the result.

To see this, let us choose ζ and $\mathcal{G}$ as in the proof of Theorem 10: ζ is a primitive $|G|$th root of unity, and $\mathcal{G}$ the Galois group of $[\mathbb{Q}(\zeta) : \mathbb{Q}]$. Then for all $\sigma \in \mathcal{G}$, $\sigma(\chi(g))$ is a sum of $\chi(1)$ roots of unity, so $|\sigma(\chi(g))| \leq \chi(1)$. In particular, $|\sigma(\alpha)| = |\sigma(\chi(g))/\chi(1)| \leq 1$ for all σ, so since $|\alpha| < 1$, hence

$$\left| \prod_{\sigma \in \mathcal{G}} \sigma(\alpha) \right| < 1.$$

By the Fundamental Theorem of Galois Theory, this product is a rational number. Moreover, since each $\sigma(\alpha)$ satisfies the same rational polynomials that α does, hence it is also an algebraic integer, whence so is the product of all of these. Thus, the left-hand side above is a rational integer, and hence equals zero. So at least one $\sigma(\alpha)$ vanishes, whence $\alpha = 0$ and we are done. $\square$

Lemma 14. *Let G be a nonabelian simple group. Then $\{1\}$ is the only conjugacy class of G which has prime power size.*

Proof. Suppose χ is irreducible and not the trivial character 1_G. Then $\ker\chi = 1$ since G is simple. Moreover, $Z(\chi)$ is a normal abelian subgroup (from above) of G simple nonabelian, so it is trivial, as is the center of G: $Z(\chi) = Z(G) = 1$.

Suppose $\mathcal{O}_g$ has size p^a for some $g \neq 1$. If $p \nmid \chi(1)$, then $\chi(g) = 0$ by Proposition 13. Moreover, since $g \neq 1$, the column orthogonality relations and the previous sentence yield:

$$0 = \sum_\chi \chi(1)\chi(g) = 1_G(1)\cdot 1_G(g) + \sum_{p|\chi(1)} \chi(1)\chi(g) + \sum_{\chi \neq 1_G, p\nmid\chi(1)} \chi(1)\chi(g) = 1 + \sum_{p|\chi(1)} \chi(1)\chi(g).$$

whence $-1 = p\alpha$, where $\alpha = \displaystyle\sum_{\chi \,:\, p|\chi(1)} \frac{\chi(1)}{p}\chi(g)$ is an algebraic integer. But then $\alpha = -1/p$ is an algebraic integer for some prime p, which is false. $\square$

Finally, we have

Theorem 15 (Burnside)**.** *Suppose* $|G| = p^a q^b$*, where* p, q *are primes. Then* G *is solvable.*

Note that may assume that p, q are distinct, because if G is a finite p-group, then G is solvable for the following reason: G is either trivial, or has nontrivial center N, in which case we can proceed by induction on $|G|$ to assume that both N and G/N are solvable. (It is also true, of course, that G is nilpotent, and hence solvable.)

Proof. Use induction on $|G|$; now assume that $|G| > 1$ and choose a maximal proper normal subgroup N. If $N > 1$, then by the induction hypothesis, both N and G/N are solvable and we are done. So assume now that $N = 1$, whence G is simple. Let $P \neq 1$ be a Sylow subgroup of G, so it has nontrivial center; choose $1 \neq g \in Z(P)$. Then $|\mathcal{O}_g| = [G : C(g)]$ divides $[G : P]$, which is a prime power. By Lemma 14, the simple group G must be abelian, and hence solvable. □

References

[Ga1] P.X. Gallagher, *Group characters and commutators*, Mathematische Zeitschrift **79** (1962), 122–126.

[Ga2] ———, *Zeros of group characters*, Mathematische Zeitschrift **87** (1965), 363–364.

[Isa] I.M. Isaacs, *Character theory of finite groups.*