Lecture 4-8: Values of characters

April 8, 2024

We now explore the values $\chi(g)$ of characters at elements of g in more detail. We begin with a brief digression into ring theory. Given a commutative ring B with a subring A, we say that $b \in B$ is integral over A if there is a *monic* polynomial $p \in A[x]$ such that $p(b) = b^n + \sum_{i=0}^{n-1} a_i b^i = 0$ (so that $a_i \in A$ for all i). Equivalently, the subring $B' = A[b]$ of B generated by A and b is a finitely generated A-module $\sum Ab_i$ for some $b_i \in B'$; for then if we write each b_i as a polynomial in b of degree d_i with coefficients in A and choose $d > d_i$ for all i, then b^d, as a combination of b_i, must be an A-linear combination of lower powers of b.

Moreover, if b is integral over A, then so are all elements of the subring $A[b]$. To see this, let $b_1, \ldots, b_n$ be a set of generators for $B' = A[b]$ as an A-module. For $c \in B'$ write each product cb_i as a combination $\sum_{j=1}^n c_{ji} b_j$, where the c_{ji} lie in A, and let C be the $n \times n$ matrix over A with ij entry c_{ij}. Given a combination $d = \sum a_i b_i \in B'$ with $a_i \in A$ the matrix product $C(a_1, \ldots, a_n)^t$ is a column vector $(a'_1, \ldots, a'_n)^t$; the definition of C shows that $cd = \sum a'_i b_i$. If we now make B' into a module over the polynomial ring $A[t]$ by decreeing that t act by multiplication by c, then we see that the matrix $C - tI$ over $A[t]$ acts by 0 on B'. Multiplying this matrix on the left by the transpose of its cofactor matrix, we get the scalar matrix $p(t)I$, where $p(t)$ is the characteristic polynomial of C; it too acts by 0 on B', whence $p(c) = 0$ and c is integral over A. More generally, given any ring extension $A \subset B$, the set of elements of B integral over A is a subring of B containing A.

In particular, the algebraic integers in $\mathbb{C}$, i.e. the complex numbers integral over $\mathbb{Z} \subset \mathbb{C}$ in this sense, form a subring of $\mathbb{C}$. .

But the algebraic integers, unlike the algebraic numbers, do not form a subfield of $\mathbb{C}$. On the contrary, if the rational number $\frac{r}{s}$ in lowest terms is an algebraic integer, then we have a relation $(\frac{r}{s})^n + \sum_{i=0}^{n-1} z_i(\frac{r}{s})^i = 0, r^n + \sum_{i=0}^{n-1} z_i r^i s^{n-i} = 0$. If s has any prime divisor p, then p cannot divide any power of r, since $\frac{r}{s}$ is in lowest terms, whence p does not divide the left side of this last equation, a contradiction. We conclude that the integers are the only rational numbers that are algebraic integers. Indeed, ordinary integers are sometimes called *rational integers* for emphasis, so as to distinguish them from algebraic integers.

We now return to character theory. Any character value $\chi(g)$ is the sum of the eigenvalues of a matrix, each of which is a root of unity, so $\chi(g)$ is an algebraic integer. In particular, $\chi(g) \in \mathbb{Q}$ if and only if $\chi(g) \in \mathbb{Z}$: there are no fractions in character tables. Now let V be an irreducible representation of G with character χ. Let $C_1, \ldots C_m$ be the conjugacy classes in G, with C_i of size c_i. For each i denote the common value of χ on all elements of C_i by d_i.

Proposition 4, DF p. 887

The element $x_i = \sum_{g \in C_i} g \in \mathbb{C}G$ acts by the scalar $e_i = \frac{c_i d_i}{\chi(1)}$ on V and e_i is an algebraic integer.

Proof.

We know that x_i is central in $\mathbb{C}G$, whence it acts by a scalar on V by Schur's Lemma; taking traces, we see that this scalar is indeed e_i. For any i, j, the product $x_i x_j$ is also central in $\mathbb{C}G$, whence it is a nonnegative integral combination of x_k. It follows that the $\mathbb{Z}$-submodule of $\mathbb{C}$ generated by the e_i is also a subring, whence the e_i are algebraic integers, as claimed. □

Corollary 5, DF p. 888

The degree $n_i = \chi_i(1)$ of any irreducible character χ_i of G divides the order n of G.

Proof.

Let d_j be the common value of χ_i on the elements of C_j. By Schur orthogonality, the sum $\sum_{j=1}^{m} e_j \overline{d_j} = \frac{n}{\chi_i(1)}$; but this sum is generated by algebraic integers and so is an algebraic integer, forcing $\frac{n}{\chi_i(1)}$ to be an integer, as claimed. □

Under an extra hypothesis on the size c_j of a conjugacy class C_j and the degree n_i of an irreducible representation $\pi_i : G \to GL(V_i)$ we get a severe constraint on the value d_j of the corresponding character χ_i on the elements of C_j. This is

Lemma 6, DF p. 889

With notation as above, if $n_i = \chi_i(1)$ and c_j are relatively prime, then either $d_j = 0$ or $\pi_i(x)$ is a scalar matrix for all $x \in C_j$.

Proof.

Under the hypothesis both $\frac{c_j d_j}{n_i}$ and $d_j = \frac{n_i d_j}{n_i}$ are algebraic integers, whence upon taking a suitable integral combination $f_j = \frac{d_j}{n_i}$ is an algebraic integer. Now d_j is the sum of n_i roots of 1 in $\mathbb{C}$ (the eigenvalues of $\pi_i(x)$) divided by n_i, so its norm as a complex number is at most 1, with equality holding if and only if all the roots of 1 coincide, which in turn holds if and only if $\pi_i(x)$ is a scalar. But the minimal polynomial of f_j over $\mathbb{Q}$ (or $\mathbb{Z}$) must have integer coefficients, by Gauss's Lemma from last quarter. The product of the Galois conjugates of these roots equals the constant term of this polynomial, up to sign, so must be an integer. Yet each of these conjugates, like f_j itself, is the sum of n_i roots of 1 divided by n_i, so has absolute value at most 1. Thus if none of the roots is 0, then $\pi_i(x)$ is a scalar, while otherwise all roots are 0 and $d_j = 0$, as claimed. □

Thus it is no coincidence, for example, that the two-dimensional character χ_r of S_3 takes the value 0 on the conjugacy class of transpositions, since this class has size 3 and 2 and 3 are relatively prime.

Under an even stronger hypothesis on the size of a conjugacy class we get a consequence for the structure of G.

Burnside's Nonsimplicity Criterion: DF p. 890

Let G be a nonabelian group such that some nonidentity conjugacy class C has size a power of a prime p. Then G is not simple; that is, it has a proper normal subgroup.

Proof.

Suppose first that there is a nontrivial irreducible representation π of G with $\pi(g)$ a scalar matrix for some $g \in G, g \neq 1$. Then the set of all $h \in G$ with $\pi(h)$ a scalar matrix is a nontrivial normal subgroup of G; if it is all of G, then the kernel K of π, consisting of all $k \in G$ with $\pi(k) = 1$, is another normal subgroup of G. If $K = 1$, then G is isomorphic to a subgroup of $\mathbb{C}^*$ and so is abelian, contrary to hypothesis; so in any event G is not simple. Now suppose that there is no such representation π. Then every irreducible character χ_i of G either has degree $n_i = \chi_1(1)$ a multiple of p or has $\chi_i(g) = 0$ for all $g \in C$. Applying the second Schur orthogonality relation, we get $1 + \sum_i \chi_i(1)\chi_i(g) = 0$, where the sum ranges over the nontrivial characters of G, for all $g \in C$. Omitting the terms where $\chi_i(g) = 0$ and dividing all the remaining $\chi_i(1)$ by p, we deduce that $-1/p$ is an algebraic integer, a contradiction. Thus G is not simple, as claimed. □

For example, Burnside's Criterion implies that the alternating group $G = A_4$ is not simple, since it has a conjugacy class C of 3-cycles of size $4 = 2^2$. Note however that while A_r does have a nontrivial irreducible representation π such that $\pi(x)$ is a scalar matrix for all $x \in C$, it is *not* true that C lies in a proper normal subgroup of G. Instead the kernel of π is the proper normal subgroup, consisting of another conjugacy class of G together with the identity. A further famous consequence of Burnside's Criterion is

Burnside's Theorem: Theorem 1, DF p. 886

Any group G whose order is the product $p^a q^b$ of two prime powers is solvable.

Indeed, given any such G, choose a nonidentity central element g of a Sylow p-subgroup, which exists by the theory of p-groups. Then its conjugacy class has order dividing $\frac{p^a q^b}{p^a} = q^b$, so this order is a power of q, whence G is not simple by Burnside's Criterion. Passing to a quotient G/N and arguing by induction on the order of G, we may assume that G has a solvable normal subgroup N such that G/N is also solvable, whence so is G. On the other hand, a group whose order is the product of three prime powers need not be nonsimple, as the example of the alternating group A_5 shows.