Representations of Finite Groups

Patrick Gallagher

Transcribed by Ron Wu

This is an advanced undergraduate course, offered in spring 2013 at Columbia University. Recommended books are Serre, *Linear Representations of Finite Groups*, Serre, *Groupes finis* (in French), I.M Isaacs, *Character Theory of Finite Groups*, Curtis, Reiner, *Representation Theory of Finite Groups and Associative Algebras,* Huppert, *Character Theory of Finite Groups.* Office hours: M 8:30-9:30, Th 2-3.

Contents

Course Overview

Lecture 1 (1/23/13)

For those interested in the historical development of the subject may look up brief biographies of

G. Frobenius

I. Schur

E. Artin

R. Brauer

Each one was the the best student of the preceding one. The list should add W. Burnside, I.M Isaacs, G. Navarro.

We will cover the first half of the material below, and pick the ones are interesting from the rest of the list

1. actions of groups on sets
2. actions on power sets and maps, equivalence of actions
3. counting orbits of actions
4. representations: irreducibility, equivalence, Schur's lemma, Maschke's theorem
5. characters of finite groups, first properties
6. seven basic character identities
7. factor groups, direct products, some charter tables
8. abelian groups, duality and basic theorem
9. algebraic integers, application to character values and degrees
10. class multiplication constants, determinant of a representation
11. automorphisms of the m^{th} cyclotomic field, and the norm map
12. applications to Galois actions on characters and classes
13. more applications to character zeros and to groups
14. Sylow's theorems, solvable groups
15. Schur-Zassenhaus theorem for abelian normal Hall subgroup
16. induction and restriction of characters, application to Frobenius groups
17. normal subgroups and Clifford's theorem

18. extensions of stable irreducible characters from normal Hall subgroups
19. theorems of Burnside and Hall for solvable groups
20. Schur-Zassenhaus theorem for arbitrary normal Hall subgroups
21. Glauberman's equivalence theorem, lemma, and class correspondence
22. Navarro's proof of Glauberman's character correspondence
23. end of proof of Glauberman's theorem
24. $\pi-$special characters of a solvable group
25. Brauer's induction and characterization theorem
26. applications Brauer's theorem to zeros and extensions of characters
27. Hilbert space, adjoint, unitary
28. unitary representations, Jordan's theorem
29. spherical functions on finite groups
30. spherical functions as characters of centralizer algebra, bound and integrability

1 Groups Actions

1.1 Actions of Groups on Sets

We will restrict to finite groups and finite sets later, for now G, X are completely arbitrary.

Definition 1. Let G be a group and let X be a set. An *action* of G on X is a map from the Cartesian product to X

$$G \times X \to X$$

$$g \cdot x \mapsto gx$$

and satisfying the two conditions

$$gh \cdot x = g \cdot hx \qquad 1 \cdot x = x \,\forall\, g, h \in G, x \in X \tag{1.1}$$

Here 1 is the identity element of G.

One can see that the two conditions (1.1) are similar to the axioms of groups or semigroups. Notice the in our class, we only look at left action, also the map described above is not given a name. We will give it a name in the next theorem.

Theorem 2. *(1) Given an action of G on X, for each g, the map $\pi_g : x \mapsto gx$ from X to X is a permutation of X, i.e. a bijection from X to X, and the map $g \mapsto \pi_g$ is a homomorphism from G to S_X, the symmetric group of all permutation of X.*

(2) Conversely, given any homomorphism $\pi : g \mapsto \pi_g$ from G to S_X, we get an action of G on X by putting $gx = \pi_g(x)$ for $g \in G$, $x \in X$.

Proof. (1) (1.1) gives

$$\pi_{gh}(x) = \pi_g(\pi_h(x)) \qquad \pi_1(x) = x \,\forall\, g, h \in G,\, x \in X \tag{1.2}$$

That is

$$\pi_{gh} = \pi_g \circ \pi_h \qquad \pi_1 = id_X \,\forall\, g, h \in G \tag{1.3}$$

(Note: the composition here is exactly the multiplication in group G)

It follows that

$$\pi_g \circ \pi_{g^{-1}} = id_X \,\forall\, g$$

which implies that each π_g is surjective (= onto), and each $\pi_{g^{-1}}$ is injective (= 1-1). Replacing g by g^{-1}, it follows that π_g is bijection, i.e. each $\pi_g \in S_X$. The first equation in (1.3) shows that $\pi : g \mapsto \pi_g$ is a homomorphism from G to S_X.

(2) Each homomorphism $\pi : g \mapsto \pi g$ form G to S_X satisfies (1.3), hence (1.2). Putting $gx = \pi_g(x)$, conditions (1.2) become (1.1), i.e. the map $g \cdot x \mapsto gx$ is an action of G on X. □

Remark 3. In short, an action of G on X is a homomorphism $\pi : G \to S_X$.

Definition 4. Given an action of a group G on a set X, for each $x \in X$

$$Gx = \{gx : g \in G\} \text{ is the orbit of } x$$

$$G_x = \{g \in G : gx = x\} \text{ is the stabilizer of } x$$

This is a subgroup of G

$$X^G = \{x \in X : gx = x\} \text{ is the fixed points in the action}$$

Exercise 5. Prove that each action of G on X and $x, x_1, x_2 \in X$. (1) $x \in Gx$ (2) either $Gx_1 \cap Gx_2 = \varnothing$ or $Gx_1 = Gx_2$.

Theorem 6. *For each action of G on X, the distinct orbits partition X, i.e. the orbits are nonempty, pairwise disjoint and they cover X.*

Proof. This follows from the exercise above. By (1), each orbit is nonempty, and they cover X. By (2) distinct orbits are disjoint. □

Theorem 7. *For each action of G on X, each stabilizer is a subgroup of G, and for each x there is a bijection $Gx \to G/G_x$ from the orbit of x to the set of left cosets of G_x in G.*

Proof. First, to be a subgroup

$g, h \in G_x \implies gx = x, hx = x \implies gh \cdot x = g \cdot hx = gx = x \implies gh \in G_x$

$g \in G_x \implies x = gx \implies g^{-1}x = g^{-1}g \cdot x = 1 \cdot x = x \implies g^{-1} \in G_x$

$1 \in G_x$, since $1x = x$ (i.e. subset nonempty)

Second, for $x \in X$ and $g, g' \in G$,

$$g'x = gx \iff g^{-1}g'x = x \iff g^{-1}g' \in G_x \iff g'G_x = gG_x \quad (1.4)$$

For each $x' \in Gx$, that is at least one $g \in G$ with $gx = x'$. In general this g is not uniquely determined but (1.4) shows that the left coset gG_x to which g belongs is uniquely determined by x and x'. Thus we get a map $\psi : Gx \to G/G_x$. It follows easily from (1.4) that this ψ is both injective and surjective. □

Exercise 8. Justify $g^{-1}g' \in G_x \iff g'G_x = gG_x$ in (1.4).

Exercise 9. Justify the last sentence in the proof above.

Corollary 10. *For each action of a finite group G on a set X and each $x \in X$, we have $|Gx| = (G : G_x)$, i.e. the size of the orbit of x is the index of the stabilizer of x.*

Recall $(G : G_x) = |G| \,/\, |G_x|$, so the cor says $|Gx|\,|G_x| = |G|$ order of the group. Notice the corollary stated in term of $(G : G_x)$, because it is an important quantity, that desire a name.

Example 11. Each group G acts on itself, by "left-translation". Check in this case the two axioms in (1.1) are just two of the three axioms in the definitions of group.

Exercise 12. Prove that for each action of a group on a set X, the kernel of the corresponding homomorphism $\pi : G \to S_X$ is $\bigcap_{x \in X} G_x$.

Recall *kernel* of a homomorphism means sending to I in the target.

The following theorem is one of the oldest in group theory. It goes back to 1800's.

Theorem 13. *(Cayley's) Each group G is isomorphic to a subgroup of S_G.*

Proof. In the action of G on itself by left translation, we have $G_x = 1$ for all $x \in G$, so the kernel of the corresponding homomorphism $\pi : G \to S_G$ is $\bigcap_{x \in X} G_x = 1$. Therefore π is injective, so $G \simeq \pi G$, a subgroup of S_G. □

Lecture 2 (1/28/13)

It is sometimes convenient to use *exponential notation* for an action. In this notation gx is replaced by x^g, and the axioms of an action are

$$x^1 = x \,\forall\, x \in X \text{ and } x^{gh} = (x^h)^g \;\forall\, g, h \in G,\, x \in X$$

Example 14. Each group G acts on itself, *by conjugation.* (note: conjugation always refers to action on itself) Hence

$$g \cdot x \mapsto x^g = gxg^{-1}$$

for $g, x \in G$. This clearly satisfies the axioms of an action

$$x^1 = x \qquad x^{gh} = ghx(gh)^{-1} = g(hxh^{-1})g^{-1} = (x^h)^g$$

Theorem 15. *Each $x \mapsto x^g$ by conjugation is an automorphism of G, i.e. isomorphism from G to itself.*

Proof.

$$(xy)^g = gxyg^{-1} = gxg^{-1}gyg^{-1} = x^g y^g$$

$$x^g = 1 \implies gxg^{-1} = 1 \implies x = g^{-1}g = 1$$

so the kernel is 1, so it is injective.

$$y \in G,\; y = gxg^{-1} \text{ for } x = g^{-1}yg$$

this shows it is surjective. □

In action by conjugation, the orbit of x consists of all conjugates x^g for $g \in G$ and is called the *conjugacy class* of x.

The stabilizer of x is the *centralizer* of x in G

$$G_x = C_G(x) \equiv \{g \in G : gx = xg\}$$

The fixed points in this action makes up the *center* of G

$$X^G = Z(G) \equiv \{x \in G : gx = xg \; \forall \, g \in G\}$$

which is equal to

$$\bigcap_{g \in G} C_G(g)$$

Exercise 16. Prove that $Z(G)$ is an abelian normal subgroup of G.

Exercise 17. Denote by S_3 the symmetric group on $X = \{1, 2, 3\}$. Find the three conjugacy classes of S_3. Hint: First prove $(1, 2)(2, 3) = (1, 2, 3)$, where $(1, 2)$ is the transposition $1 \to 2 \to 1$, $3 \to 3$, and $(1, 2, 3)$ is the 3-cycle $1 \to 2 \to 3 \to 1$.

Definition 18. Let p be a prime number. A finite group whose order is a power of p, i.e. $|G| = 1, p, p^2, ...$, is called a p-group.

Lemma 19. *(Fermat) Let P be a p-group, acting on a finite set X. Then*

$$\left|X^P\right| \equiv |X| \mod p$$

where X^P means the fixed points.

Proof. By Corollary 10, each orbit has p-power size. The orbits of size 1 make up X^P, each of the other orbits has size p,$p^2, ...$, i.e. they all have sizes divisible by p. Thus the complement of X^P in X has size divisible by p. □

Theorem 20. *Each nontrivial p-group has nontrivial center.*

Recall a nontrivial group means not $\{1\}$ or order is not 1.

Proof. Consider the action of P on itself by conjugation. Then $P^P = Z(P)$, so

$$\begin{aligned} |Z(P)| &\equiv |P| \mod p \\ &\equiv 0 \mod p \end{aligned}$$

Since $|P| \neq 1$, $|Z(P)| \neq 1$. □

1.2 Actions on Power Set and on Sets of Maps

Definition 21. Given an action of a group G on a set X, G also acts on the *power set*, i.e.

$$\mathcal{P}(X) = \{A : A \subset X\}$$

Thus $\mathcal{P}(X)$ is the set of all subsets of X, including $\varnothing$ and X.

In this action

$$gA = \{gx : x \in A\}$$

for $g \in G$, $A \in \mathcal{P}(X)$.

Exercise 22. Verify the action axioms for this action on $\mathcal{P}(X)$.

Definition 23. We say A is stable if $gA = A$ for all $g \in G$.

This is equivalent to $gA \subset A \; \forall \, g$, since $gA \subset A \implies A \subset g^{-1}A = gA$.

It is also clear that a stable set is just a union of some orbits.

Theorem 24. *If G acts in X, then G also acts on the power set $\mathcal{P}(X)$ by $g \cdot A \mapsto gA$ for $g \in G$, $A \in \mathcal{P}(X)$. Also G acts by restriction on each stable subset $A \subset X$, i.e.*

$$g \cdot x \mapsto gx \text{ for } g \in G,\, x \in A$$

Proof. For $A \subset X$ clearly $1A = A$. For $g, h \in G$

$$gh \cdot A = \{gh \cdot x : x \in A\} = \{g \cdot hx : x \in A\} = \{gx' : x' \in hA\} = g \cdot hA$$

showing the action of G on $\mathcal{P}(X)$.

Also A is stable then $gx \in A$, $\forall \, g \in G, x \in A$, and clearly G on A is an action. □

Theorem 25. *If G acts on sets X and Y, then G also acts on the set*

$$m(X, Y) = \{f : X \to Y\}$$

consisting of all maps from X to Y by (in exponential notation)

$$f^g(x) = g \cdot f(g^{-1}x) \tag{1.5}$$

for $g \in G$, $f \in m(X, Y)$, $x \in X$.

Proof. According to (1.5), f^g is the composite of these maps

$$\begin{array}{ccccccc} X & \to & X & \stackrel{f}{\to} & Y & \to & Y \\ x & \mapsto & g^{-1}x & \mapsto & f(g^{-1}x) & \mapsto & g \cdot f(g^{-1}x) \end{array}$$

so $f^g \in m(X,Y)$, clearly $f^1 = f$, for $g, h \in G$

$$f^{gh}(x) = gh \cdot f(h^{-1}g^{-1}x) = gf^h(g^{-1}x) = (f^h)^g(x)$$

Thus the maps $f \mapsto f^g$ give an action of G on $m(X,Y)$. □

In the proof, we used the fact that $(gh)^{-1} = h^{-1}g^{-1}$. This switch is crucial and this is the reason why in the definition of actions on maps (1.5), it has to be an inverse.

Definition 26. f is stable if $f^g = f \ \forall\, g$, i.e. $f \in m(X,Y)^G$.

The definition is equivalent to

$$g \cdot f(x) = f(gx) \ \forall\, g \in G, x \in X$$

To see this, replace x by $g^{-1}x$.

Theorem 27. *Let G act on X and Y, and let f be a stable map. Then*

(1) if $A \subset X$ is stable, then $fA \subset Y$ is stable.

(2) if $B \subset Y$ is stable, then $f^{-1}B \subset X$ is stable.

Proof. (1) For $A \subset X$, if $y \in fA$ then $y = f(x)$ for some $x \in A$, so for each $g \in G$,

$$gy = gf(x) = f(gx) \in f(gA) = fA$$

showing $gfA \subset fA$.

(2) For $B \subset Y$, if $x \in f^{-1}B$ then $f(x) \in B$, so for $g \in G$

$$f(gx) = gf(x) \in gB = B$$

Thus $gx \in f^{-1}B$, hence $gf^{-1}B \subset f^{-1}B$. □

Lemma 28. *If G acts on X, Y, Z and if $f : X \to Y$ and $g : Y \to Z$ are stable maps, then $gf : X \to Z$ is also stable.*

Exercise 29. Prove the lemma.

1.3 Equivalence of Actions

Definition 30. Actions of G on X, Y are *equivalent* (denoted by $X \sim Y$) if there is a stable bijection $f : X \to Y$.

Theorem 31. *This notion of equivalence is an equivalence relation on the set of all actions of a given group G.*

Proof. (i) Show $X \sim X$. Each action of G on a set X is equivalent to itself, since the identity map is bijection and stable.

(ii) Show $X \sim Y \implies Y \sim X$. Given actions of G on X and on Y, if $X \sim Y$, then $\exists$ stable bijection $f : X \to Y$. Then the inverse map f^{-1} is a bijection. To show it's also stable, apply f^{-1} to $g \cdot f(x) = f(gx)$ gives

$$f^{-1}(g \cdot f(x)) = gx$$

Replacing x by $f^{-1}(y)$ gives

$$f^{-1}(gy) = gf^{-1}(y)$$

(iii) Use the fact that composition of bijection (stable) functions is bijection (stable). □

Lecture 3 (1/30/13)

Definition 32. An action of G on X is *transitive* if for each $x, x' \in X$, there is some $g \in G$ with $gx = x'$.

Remark 33. G on X is transitive, iff there is only one orbit.

Theorem 34. *For each group G and subgroup H, G acts transitively on G/H by left-translation.*

Proof. G acts on itself by left translation, so G acts on $\mathcal{P}(G)$. $G/H \subset \mathcal{P}(G)$, and in this action $G/H = \{lH : l \in G\}$ is a stable subset, for $g \in G$, $lH \in G/H$, apply g, $g \cdot lH = glH \in G/H$, so we have closure, it follows G acts on G/H by left-translation. This action is transitive since $gtH = t'H$ for $g = t't^{-1}$. □

Theorem 35. *For each transitive action of G on X and each $x \in X$, the actions of G on X and on G/G_x are equivalent.*

This theorem says we now understand transitive action completely. It just acts on cosets.

Proof. Define $f : X \to G/G_x$ by

$$f(x') = tG_x \quad \text{for } x' = tx,\ t \in G$$

Since G on X is transitive, such t exists. Suppose

$$x' = t_1x = t_2x \implies t_1t_2^{-1} \in G_x \implies t_1G_x = t_2G_x \tag{1.6}$$

showing f is well defined.

f is clearly surjective. Reverse the arrows in (1.6), shows f is injective.

Now show f is stable, we want

$$gf(x') = f(gx') \quad \text{for } x' \in X,\ x' = tx$$

LHS $= g \cdot t_1G_x$, RHS $= gt_2 \cdot G_x$, using (1.6), we have f is stable. □

Lemma 36. *For each action of a group G on a set X, and each $t \in G$, $x \in X$,*

$$G_{tx} = G_x^t \ (= tG_xt^{-1})$$

Thus the stabilizer subgroups of elements in the same orbit are conjugate.

Proof. $g \in G_{tx} \iff gtx = tx \iff t^{-1}gtx = x \iff t^{-1}gt \in G_x \iff g \in tG_xt^{-1}$. □

Theorem 37. *To each transitive action of G associate the corresponding conjugacy class of stabilizer subgroup. This gives rise to a bijection from*

the set of all equivalence classes of transitive actions of G

to

the set of all conjugacy classes of subgroups of G

Exercise 38. Prove the theorem by constructing the asserted bijection.

Example 39. S_3 has six subgroups of orders 1,2,2,2,3,6, the three subgroups of order 2 being conjugate, thus four conjugacy classes of subgroups, so four equivalence classes of transitive actions.

Theorem 40. *Given actions of G on X and on Y, these actions are equivalent iff there is a bijection from G/X to G/Y so that actions of G on corresponding orbits by restriction are equivalent, where G/X, G/Y denote the orbits.*

Exercise 41. Prove the theorem.

We already know two ways to say actions G on X, Y are equivalent, namely definition 30 and theorem 40. Now we introduce another criterion.

Theorem 42. *(Burnside action equivalence criterion) Actions of a finite group G on finite sets X and Y are equivalent iff*

$$\left|X^H\right| = \left|Y^H\right| \tag{1.7}$$

for each subgroup H of G.

The proof given here is from Isaacs book. Burnside's original proof is also very good. There may be more general statement of the theorem, where (1.7) becomes Cardinal numbers are the same or equivalently there exists some bijection from X^H to Y^H.

Proof. Suppose that $X \sim Y$, let $f : X \to Y$ to be a stable bijection, and let H be any subgroup of G. Claim

$$f(X^H) = Y^H$$

Indeed

$$x \in X^H \implies hx = h \implies hf(x) = f(hx) = f(x) \implies f(x) \in Y^H$$

so $f(X^H) \subset Y^H$, so $\left|X^H\right| \leq \left|Y^H\right|$. But $Y \sim X$, so $\left|Y^H\right| \leq \left|X^H\right|$.
Conversely, suppose (1.7) holds. Pick a $G-$orbit in X or Y of minimal size, say $Gx \subset X$. Let $H = G_x$, so

$$\left|X^H\right| \geq 1$$

so

$$\left|Y^H\right| \geq 1$$

i.e. $\exists\, y \in Y^{G_x}$, so $G_x \subset G_y$, then

$$|Gx| = (G : G_x) \geq (G : G_y) = |Gy|$$

But Gx was the minimal, so

$$|Gx| = |Gy|$$

or

$$G_x = G_y \tag{1.8}$$

By theorem 35

$$Gx \sim G/G_x$$

$$Gy \sim G/G_y$$

(theorem 35 has condition transitivity, which is of course satisfied for the orbits), then use (1.8),

$$Gx \sim Gy$$

Because X, Y can be partitioned into orbits, then use theorem 40 and induction, we conclude

$$X \sim Y$$

□

Here is Burnside's original proof.

Proof. Let $\{H_i\}$ be a set of subgroups of G, one from each conjugacy class of subgroups of G, and ordered so that

$$|H_j| \geq |H_i|$$

for $j \leq i$. In the orbit decompositions of X, Y let there be m_i and n_i orbits on which the action of G is equivalent to the action on G/H_i. Then

$$\left|X^H\right| = \sum m_i \left|(G/H_i)^H\right| \text{ and } \left|Y^H\right| = \sum n_i \left|(G/H_i)^H\right| \tag{1.9}$$

To show that the actions of G on X and on Y are equivalent it is enough to show that $m_i = n_i$ for each i.

In view of the hypothesis and (1.9) it is enough to show that the $\left|(G/H_i)^H\right|$ are linearly independent functions of H. To see this, note first that

$$\begin{aligned} xH_i \in (G/H_i)^H &\iff HxH_i = xH_i \\ &\iff Hx \subset xH_i \\ &\iff H \subset xH_ix^{-1} = H_i^x \end{aligned}$$

It follows that

$$\left|(G/H_j)^H\right| \begin{cases} \neq 0 & j = i \\ = 0 & j < 1 \end{cases}$$

Supposing that

$$\sum c_i \left|(G/H_i)^H\right| = 0 \; \forall \, H$$

we get on substituting $H = H_1$, $H = H_2$, ... in turn that $c_1 = 0$, $c_2 = 0$, ... □

2 Representations

2.1 Definitions

Lecture 4 (2/4/13)

Notation in what follows

U, V, W, ... are finite dimensional complex vector spaces, or briefly spaces. "complex vector spaces" means over complex number field. We will from now assume the space is *not* 0 dimensional, because otherwise many of the theorems follow will have to modify for the 0 vector space. But there are instances we do consider 0 vector space, e.g. when we talk about representations on quotient space, sometimes quotient space has 0 dimension.

$L(V,W)$ the space of all linear maps (i.e. linear transformations), so $T \in L(V,W)$

$$T : V \to W$$

The more standard notation is $Hom(V,W)$.

$E(V) = L(V,V)$ the space of all *endomorphisms* of V, i.e. $T \in E(V)$

$$T : V \to V$$

$\mathcal{G}(V) = E(V)^*$ the group of all bijective endomorphisms of V. The more standard notation is $GL(V)$.

Recall from linear algebra:

(1) If V, W have dimension m, n, then $L(V,W)$ has dimension mn. Recall one can fix base in V, W, then $L(V,W)$ are $m \times n$ matrices.

(2) If $S \in L(U,V)$, $T \in L(V,W)$, then $TS \in L(U,V)$.

(3) In particular $E(V)$ is closed under composition.

(4) The inverse of a bijective linear ma is also linear.

(5) Therefore, $\mathcal{G}(V)$ is indeed a group.

Definition 43. A *representation* of a group G on a space V is a homomorphism $R : G \to \mathcal{G}(V)$.

We borrow the short notation from action often to write gv for $R(g)v$, for $g \in G$, $v \in V$. The definition is also equivalently to the following

Definition 44. A representation of G on V is an action of G on V for which $v \mapsto gv$ is linear, for each $g \in G$.

Theorem 45. *Let R, S be representations of G on spaces V, W. Then we get a representation of $R \boxtimes S$ of G on $L(V,W)$, by*

$$(R \boxtimes S)(g)T = S(g)TR(g^{-1})$$

for $g \in G$, $T \in L(V,W)$.

If we use the exponential notation, write

$$S(g)TR(g^{-1}) = T^g$$

then this looks very like before G acts on X, Y, then G acts on the map $f : X \to Y \in m(X,Y)$ by

$$f^g(x) = gf(g^{-1}x)$$

Proof. We first show this is an action, then we show this action is linear.

Here we have G acts on V, W, so G acts on $m(V,W)$. Since $L(V,W) \subset m(V,W)$ is stabilized by this action, i.e. if $T \in L(V,W)$, then $T^g \in L(V,W)$. That is because composite of linear maps is linear.

Now we show each map $T \mapsto T^g$ is linear

$$(cT)^g = S(g)cTR(g^{-1}) = cS(g)TR(g^{-1}) = cT^g$$

by the linearity of S, and

$$(T_1+T_2)^g = S(g)(T_1+T_2)R(g^{-1}) = S(g)T_1R(g^{-1})+S(g)T_2R(g^{-1}) = T_1^g+T_2^g \tag{2.1}$$

by the distributive properties of linear maps. □

Exercise 46. Prove the distributive properties that was used in the proof (the middle equality of (2.1)). Show for all spaces, all linear maps

$$S(T_1 + T_2) = ST_1 + ST_2 \qquad (T_1 + T_2)R = T_1R + T_2R$$

2.2 Schur's Lemma

Definition 47. Given representations of G on spaces V, W, a linear map $T : V \to W$ is *stable* if

$$gTv = Tgv$$

for all $g \in G$, $v \in V$. In other words T is stable if it is in $L(V,W)^G$.

Definition 48. A representation G on a space $V \neq 0$ is *irreducible* if the only *stable* subspaces of V are 0 and V.

The word irreducible appears so frequently that many effects have been made to simplify the word. Some uses $\hat{G}$, some uses $Irr(G)$ for all irreducible character of G, which is the same thing as all irreducible representation of G.

The meaning of irreducible in representation has its analogous thing in number theory: "prime".

Theorem 49. *(Schur's lemma) Given irreducible representations of G on spaces V, W, each nonzero stable linear map*

$$T : V \to W$$

is bijective.

Or said differently each stable (with respect to the irreducible representation) linear map is either 0 or bijective.

Proof. Let $T \in L(V, W)^G$, by theorem 27, the image TV is a stable subspace of W (since V is stable in V), and the kernel $T^{-1}(0)$ is a stable subspace of V (since 0 is stable in W).

By the irreducibility of the representations on V, W

$$TV = 0 \text{ or } W \text{ and } T^{-1}0 = 0 \text{ or } V$$

If $TV = 0$ or $T^{-1}0 = V$, then $T = 0$, thus if $T \neq 0$, then $TV = W$ and $T^{-1}0 = 0$, hence T is surjective and injective. □

Notice in the proof we used property of linear map, e.g. image of vector space of a linear map is a subspace, etc. This is the reason for representation theory, one is only interested in linear maps.

Corollary 50. *For each irreducible representation of G on finite dimensional V, the only stable endomorphisms of V are the scalar maps cI with $c \in \mathbb{C}$.*

Proof. Let $T \in E(V)^G$. Let v be an eigenvector of T with eigenvalue c, i.e. $Tv = cv$ and $v \neq 0$. (the existence of such c is given by the fundamental theorem of algebra, which implies that the polynomial $det(T - cI)$

has at least one root in $\mathbb{C}$. And this is the reason for representation theory, one is only interested in complex vector space.)

Thus $(T-cI)$ is not injective, since it annihilates both 0 and v, i.e. send 0, v to 0. But $T - cI$ is stable

$$(T - cI)^g = T^g - cI = T - cI$$

by Schur's lemma, $T - cI = 0$. □

Corollary 51. *(of corollary 50) For each irreducible representation R of G on V and each $g \in Z(G)$, the transformation $R(g)$ is a stable map.*

Proof.

$$\begin{aligned} g \in Z(G) &\iff gh = hg \quad \forall\, h \in G \\ &\iff R(g)R(h) = R(h)R(g) \\ &\iff R(g) \text{ is stable} \end{aligned}$$

by corollary 50, $R(g) = cI$, notice that here we need $c \neq 0$, because $R(g^{-1}) = R(g)^{-1}$ the map is invertible. □

Definition 52. The dimension of a representation is the dimension of V.

Corollary 53. *(of corollary 51) Each finite dimensional irreducible representation of an abelian group has dimension 1.*

Proof. Here $Z(G) = G$, so each $R(g)$ is a scalar map, by corollary 51. Therefore each subspace is stable. Since R is irreducible, only 0 and V are stable. It follows that V has dimension 1. (since we don't consider $V = 0$) □

2.3 Equivalent Representations

Definition 54. Representations R, S of G on spaces V, W are *equivalent* if there is a bijective linear map $T : V \to W$ with $S(g) = TR(g)T^{-1}$ for all $g \in G$. Or if $L(V, W)^G$ contains a bijection.

In this case we write $R \sim S$ or more commonly $V \sim W$.

Theorem 55. *Equivalence of representations is an equivalence relation.*

Exercise 56. Prove the theorem.

Corollary 57. *Given irreducible representation of G on V, W*

$$dim L(V,W)^G = \begin{cases} 1 & \text{if } V \sim W \\ 0 & \text{if } V \not\sim W \end{cases}.$$

Proof. If $V \not\sim W$, then $L(V,W)^G$ contains no bijection, so $L(V,W)^G = 0$, by Schur's lemma, giving $\dim L(V,W)^G = 0$.

If $V \sim W$, then $L(V,W)^G$ contains bijections, say T_0. For each $T \in L(V,W)^G$, we have $T_0^{-1}T \in E(V)^G$, so by corollary 50, $T_0^{-1}T = cI$ or $T = cT_0$ for some $c \in \mathbb{C}$. Conversely each $cT_0 \in L(V,W)^G$. Thus $L(V,W)^G$ is a 1-dimesional space spanned by T_0. □

2.4 Maschke's Theorem

Recall in linear algebra

Definition 58. Let V' be a subspace of a vector space V. An endomorphism T of V is a *projection* on V' if

$$TV = V' \quad Tv = v \,\forall\, v \in V'$$

It follows that

$$V = V' \oplus T^{-1}0$$

$\oplus$ denoting direct sum. In fact

$$V' \cap T^{-1}0 = 0$$

for $v \in V' \cap T^{-1}0 \implies Tv = v$, $Tv = 0$. And

$$V = V' + T^{-1}0$$

for $v \in V \implies v = Tv + (v - Tv)$ with $Tv \in V'$ and $T(v - Tv) = Tv - Tv = 0$.

Conversely, for each direct sum decomposition

$$V = V' \oplus V''$$

(so that each $v \in V$ is uniquely $v' + v''$ with $v' \in V'$, $v'' \in V''$) the map $T : V \to V$ defined by $Tv = v'$ is a projection of V on V' with kernel V''.

Theorem 59. *(Averaging lemma) For each representation of a finite group G on a space V,*

$$v \mapsto \bar{v} = \frac{1}{|G|} \sum_{h \in G} hv$$

is a projection of V on V^G, the subspace of fixed points.

Exercise 60. Check that V^G is a subspace.

Proof. Let R to be the representation, the map

$$v \mapsto \bar{v}$$

is the average of the $R(h)$, so it is an endomorphism of V. For $g \in G$, $v \in V$

$$g \sum hv = \sum ghv = \sum hv$$

so we see that the image of the map is in V^G. Since $hv = v$ for $v \in V^G$, the map fixes the elements of V^G, (this is why to do $1/|G|$), so it is a projection. □

Theorem 61. *Let G be a finite group and let V be a finite dimensional vector space. For each representation of G on V and each stable subspace V' of V, we have $V = V' \oplus V''$ for some stable subspace V''.*

Proof. Let T be any projection of V on V'. Put

$$\bar{T} = \frac{1}{|G|} \sum_h T^h,$$

where $T \to T^h$ is the representation on $E(V)$ (cf theorem 45) By theorem 59, $\bar{T}$ is a stable endomorphism of V. Also $\bar{T}$ is a projection of V on V', since

$$T^h V = hTh^{-1}V \subset hTV = hV' \subset V'$$

for each $h \in G$, so $\bar{T}V \subset V'$. And

$$T^h v' = hTh^{-1}v' = Tv' = v'$$

so $\bar{T}v' = v' \; \forall \, v' \in V'$. Since $\bar{T}$ is a projection on V', we have

$$V = V' \oplus \bar{T}^{-1}0$$

Since $\bar{T}$ is stable, $\bar{T}^{-1}0$ is also stable, by theorem 27. □

Definition 62. Given a representation of G on V, and a stable subspace $V' \subset V$, we get a representation of G on V' by *restriction* of the action of G on V to an action of G on V'. If

$$V = V' \oplus V''$$

with both V', V'' stable, then the representation of G on V (say R) is determined by its restrictions (say R', R'') to V', V'', since

$$R(g)v = R(g)(v' + v'') = R(g)v' + R(g)v'' = R'(g)v' + R''(g)v''$$

In this case we write

$$R = R' \oplus R''.$$

Theorem 63. *(Maschke's) (1) For each representation of a finite group G on a space V, there is a direct sum decomposition of V into stable irreducible subspaces,*

$$V = V_1 \oplus ... \oplus V_k \tag{2.2}$$

(2) Furthermore for each irreducible representation of G on a space W, the number of $j \in \{1, ..., k\}$ for which $V_j \sim W$ is $dim L(V, W)^G$, and is therefore independent of the particular decomposition.

Proof. (1) Let V_1 be a stable subspace of V of minimal positive dimension. Then the restriction of the representation to V_1 is irreducible since otherwise V_1 would have a stable subspace of even smaller positive dimension. By the previous Theorem,

$$V = V_1 \oplus \tilde{V}_1$$

with $\tilde{V}_1$ stable. By induction on $\dim V$, we have the result. □

Exercise 64. Prove (2) of the theorem. Hint: first using (1) to derive

$$L(V, W)^G = L(V_1, W)^G \oplus ... \oplus L(V_k, W)^G$$

then use corollary 57.

Exercise 65. In the only representation of a group of order 1 on a space of dimension 2, show that the decomposition (2.2) is not unique.

3 Characters of Finite Groups

3.1 Characters and Some Properties

Lecture 5 (2/6/13)

Definition 66. The *trace* trA of an $n \times n$ (square) matrix $A = (a_{ij})$ is the sum of its diagonal elements

$$trA = \sum_{i=1}^{n} a_{ii}$$

Theorem 67. *For $n \times n$ matrices A, B,...*

(0) $tr(A+B) = trA + trB \qquad trcA = ctrA$

(1) $tr(AB) = tr(BA)$

(2) $tr(BAB^{-1}) = tr(A)$ *for B invertible*

(3) $trI_n = n$ *for I $n \times n$ identity matrix.*

(4) $trA = trA' + trA''$ *for* $A = \begin{pmatrix} A' & 0 \\ 0 & A'' \end{pmatrix}$ *with A', A'' square*

Exercise 68. Prove (1) by interchanging summation signs, then (2) is automatic.

Definition 69. Let V be a vector space of dimension n. The trace of an endomorphism T of V is the trace of the matrix A of T relative to any choice of basis $v_1, ..., v_n$of V, here

$$A = (a_{ij}) \quad \text{with } Tv_j = \sum_{i=1}^{n} a_{ij} v_i$$

If another basis $v'_1, ..., v'_n$of V, then the matrix A' of T, but since $A' = BAB^{-1}$ for a suitable invertible B, we have $trA' = trA$.

Theorem 70. *The trace function $tr = tr_V : E(V) \to \mathbb{C}$ has the following properties:*

(0) tr is linear

(1) $trST = trTS$ *for* $S, T \in E(V)$

(2) $tr(STS^{-1}) = trT$ *for* $T \in E(V)$, $S \in GL(V)$

(2') $tr_{V'}(STS^{-1}) = tr_V T$ *for* $T \in E(V)$, *bijective* $S \in L(V, V')$

(3) $trI_n = n$ *for I_n identity endomorphism of V*

(4) $tr_V T = tr_{V'} T' + tr_{V''} T''$ *for* $V = V' \oplus V''$ *and T is thus defined as* $T = T' \oplus T''$ *with* $T' \in E(V')$, $T'' \in E(V'')$

Exercise 71. Prove these formulas.

Theorem 72. *Given spaces V, W and endomorphism $R \in E(V)$, $S \in E(W)$, map $T \mapsto STR$ from $L(V,W)$ to $L(V,W)$ is an endomorphism of $L(V,W)$, and the trace of this endomorphism is*

$$tr_{L(V,W)}(R \boxtimes S) = (tr_V R)(tr_W S)$$

This is a great utility of defining trace on an endomorphism, although for matrices A,B, in general $trAB \neq trAtrB$.

Exercise 73. Prove the theorem. Hint: that $T \mapsto STR$ is an endomorphism is easy. To calculate its trace we choose a special basis of $L(V,W)$: let $v_1, ..., v_m$ and $w_1, ..., w_n$ be bases of V, W. Let T_{ij} be the linear map from V to W sending v_j to w_i and $v_{j'}$ to 0 if $j \neq j'$. show that the T_{ij} form a basis for $L(V,W)$. Then express the elements of the matrix, relative to this basis, of the endomorphism $T \mapsto STR$ in terms of the elements of the matrices A of R and B of S. Finally calculate the trace of $T \mapsto STR$ and get $(tr_V R)(tr_W S)$.

Definition 74. The *character* χ, χ_R, or χ_V of a representation $R : G \to GL(V)$ is defined by

$$\chi(g) = trR(g)$$

for $g \in G$.

Thus χ is a complex function on G. Later we will see representation theory is really character theory.

The following theorem follows easily from theorem 70.

Theorem 75. *(1) $\chi(hg) = \chi(gh)$*

(2) $\chi(g^h) = \chi(g)$ here $g^h = hgh^{-1}$

(2') $\chi_R = \chi_S$ if $R \sim S$

(3) $\chi(1) = n$, where $n = dimV$ (is also the degree of χ or the dim of R)

(4) $\chi = \chi' + \chi''$ for $R = R' \oplus R''$

Remark 76. According to (2), for each character χ of G, the value $\chi(g)$ depends only on the conjugacy class of g, i.e. character is a class function. Also by (2') $\chi(g)$ depends only on the equivalence class. Later we will show the converse of (2') is also true.

The following follows from theorem 72.

Theorem 77. *The character of the representation $R \boxtimes S$ of G defined in theorem 45 satisfies*

$$\chi_{R\boxtimes S}(g) = \chi_R(g^{-1})\chi_S(g)$$

for $g \in G$.

Definition 78. Given a representation R of G on V, the dual representation R^* of G on the dual space $V^* = L(V, \mathbb{C})$ is defined by

$$R^*(g)T = TR(g^{-1})$$

for $g \in G$, $T \in L(V, \mathbb{C})$. Thus $R^* = R \boxtimes 1$, here 1 stands for the trivial representation on the 1-dimensional space $\mathbb{C}$, defined by $1(g)c = c$ for all $g \in G$, $c \in \mathbb{C}$.

There was a story in summer of 1942 at our university, Samuel Eilenberg and Saunders Mac Lane received a grand from navy to do some research. At the time they worked on dual of a dual $V \approx V^{**}$, they needed to define natural transformation, then they invented functor, giving the birth of category theory. Since then category theory gained two reputations: one regards it as abstract of non-sense; the other believes it gives an alternative to the base of mathematics, replacing set theory.

Theorem 79. *The character of R^* is given by*

$$\chi_{R^*}(g) = \chi_R(g^{-1}) \tag{3.1}$$

Proof. This follows from $R^* = R \boxtimes 1$, use previous theorem, and the fact $\chi_1 = 1$. □

Corollary 80. *For all representations R, S of G,*

$$\chi_{R\boxtimes S} = \chi_{R^*}\chi_S \tag{3.2}$$

Theorem 81. *The product of two characters of G is a character of G (on $R^* \boxtimes S$).*

Proof. By (3.1), with g replaced by g^{-1} we have

$$\chi_{R^{**}}(g) = \chi_{(R^*)^*}(g) = \chi_{R^*}(g^{-1}) = \chi_R(g)$$

so by (3.2)

$$\chi_R\chi_S = \chi_{(R^*)^*}\chi_S = \chi_{R^*\boxtimes S}$$

□

Theorem 82. *For each group G, the characters of G of degree 1 are just the homomorphisms*

$$\chi : G \to \mathbb{C}^*$$

$\mathbb{C}^* = \mathbb{C} - \{0\}$.

Exercise 83. Prove the theorem. Hint: start from $dimV = 1$, $\mathcal{G}(V) = \mathbb{C}^*$...

Theorem 84. *For each representation R of G and each $g \in G$,*

$$\chi_R(g^{-1}) = \bar{\chi}_R(g)$$

i.e. $\chi_{R^*} = \bar{\chi}_R$. In particular, the complex conjugate of a character of G is a character of G.

Proof. Let $\langle g \rangle$ be the cyclic group generated by g. The restriction R to $\langle g \rangle$ is a representation of $\langle g \rangle$, so it is a direct sum of irreducible representations of $\langle g \rangle$. Since $\langle g \rangle$ is abelian, each of these is 1-dimensional, so these characters w_i are homomorphisms from G to $\mathbb{C}^*$.

It follows that the character χ_R of R satisfies

$$\chi_R|_{\langle g \rangle} = \sum w_i$$

Since $\langle g \rangle$ has finite order, each $w_i(g)$ is a root of unity. In particular, each $|w_i(g)| = 1$, so

$$w_i(g^{-1}) = w_i(g)^{-1} = \overline{w_i(g)}$$

that is

$$\chi_R(g^{-1}) = \sum w_i(g^{-1}) = \sum \overline{w_i(g)} = \bar{\chi}_R(g).$$

□

3.2 Seven Basic Character Identities

Lecture 6 (2/11/13)

The seven identities are equations (3.3), (3.4), (3.5), (3.7), (3.8), (3.9) and (3.10) below.

From now on, G is always a finite group.

Notation 85. Let G be a finite group. A character $\chi = \chi_R$ of a representation $R : G \to \mathcal{G}(V)$ with V a finite dimensional complex vector space is irreducible if R is irreducible. We put

$$\hat{G} = Irr(G) = \text{the set of all irreducible characters of } G$$

$$\breve{G} = Cl(G) = \text{the set of all conjuguacy classes of } G$$

Also for $\chi \in \hat{G}$, the degree d_χ of χ is the dimension of V.

Exercise 86. Prove that for each representation $R : G \to \mathcal{G}(V)$, with character χ, we have

$$dimV = \chi(1)$$

Theorem 87. *(Convolution Formula) Let χ, $\chi' \in \hat{G}$ with $\chi = \chi_R$, $\chi' = \chi_S$. Then*

$$\frac{1}{|G|}\sum_{h\in G}\chi(gh^{-1})\chi'(h) = \begin{cases} \frac{\chi(g)}{d_\chi} & R \sim S \\ 0 & R \not\sim S \end{cases} \tag{3.3}$$

Theorem 88. *(First Orthogonality Relation) With the same hypothesis,*

$$\frac{1}{|G|}\sum_{h\in G}\bar{\chi}(h)\chi'(h) = \begin{cases} 1 & R \sim S \\ 0 & R \not\sim S \end{cases} \tag{3.4}$$

Proof. (of two identities) The map

$$T_{\chi\chi'} = \frac{1}{|G|}\sum_{h\in G}\chi'(h)R(h^{-1}) \in E(V)$$

commutes with each $R(g)$. In fact

$$R(g)TR(g^{-1}) = \frac{1}{|G|}\sum_{h\in G}\chi'(h)R(gh^{-1}g^{-1})$$

Make the change of variable $h_1 = ghg^{-1}$, and use $\chi'(h) = \chi'(h_1)$, to get

$$R(g)TR(g^{-1}) = \frac{1}{|G|}\sum_{h_1\in G}\chi'(h_1)R(h_1^{-1}) = T$$

By Schur's lemma and the fact that R is irreducible it follows that T is a scalar map, i.e.

$$\frac{1}{|G|}\sum_{h\in G}\chi'(h)R(h^{-1}) = c_{R,S}I_V$$

for some $c_{R,S} \in \mathbb{C}$. Multiply this equation on the left by $R(g)$ and take trace

$$\frac{1}{|G|}\sum_{h\in G}\chi'(h)\chi(gh^{-1}) = c_{R,S}\chi(g)$$

For $g = 1$, this gives

$$\begin{aligned} c_{R,S}d_\chi &= \frac{1}{|G|}\sum_{h\in G}\chi(h^{-1})\chi'(h) \\ &= dimL(V,W)^G \text{ by theorems 77, 59} \\ &= \begin{cases} 1 & V \sim W \\ 0 & V \not\sim W \end{cases} \text{ by corollary 57} \end{aligned}$$

So the two identities are proven. □

Exercise 89. Use theorem 88, show $R \sim S \implies \chi_R = \chi_S$. Hence two irreducible representations are equivalent $\iff$ their characters are equal.

Notation 90. For complex functions α and β on G, the scalar product

$$\langle \alpha, \beta \rangle = \frac{1}{|G|}\sum_{h\in G}\bar{\alpha}(h)\beta(h)$$

and the convolution

$$(\alpha * \beta)(g) = \frac{1}{|G|}\sum_{h\in G}\alpha(gh^{-1})\beta(h)$$

In this notation, for χ, $\chi' \in \hat{G}$, the previous two theorems read

$$\chi * \chi' = \delta_{\chi\chi'}\frac{\chi}{d_\chi}$$

$$\langle \chi, \chi' \rangle = \delta_{\chi\chi'}$$

Exercise 91. Prove

(a) the associative law $(\alpha * \beta) * \gamma = \alpha * (\beta * \gamma)$ for convolution.

(b) $\alpha * \beta = \beta * \alpha$ for all complex functions β on $G \iff \alpha$ is a class function.

(c) the space of class functions on G has dimension $|\breve{G}|$.

Theorem 92. *(Functional Equation) For each $\chi \in \hat{G}$ and all $g, g' \in G$*

$$\chi(g)\chi(g') = \frac{d_\chi}{|G|} \sum_{h \in G} \chi(g^h g') \tag{3.5}$$

where $g^h = hgh^{-1}$.

Proof. Let $\chi = \chi_R$, for $g \in G$, put

$$T_g = \frac{1}{|G|} \sum_{h \in G} R(g^h)$$

then T_g commutes with all $R(g')$: indeed

$$T_g^{R(g')} = \frac{1}{|G|} \sum_{h \in G} R(g' g^h g'^{-1}) = \frac{1}{|G|} \sum_{h \in G} R(g^{g'h}) = T_g$$

By Schur's lemma, T_g is a scalar map

$$\frac{1}{|G|} \sum_{h \in G} R(g^h) = c_{g,R} I_V \tag{3.6}$$

take trace and use $\chi(g^h) = \chi(g)$ to get

$$\chi(g) = c_{g,R} d_\chi$$

Multiply (3.6) on the right by $R(g')$ and take trace to get

$$\frac{1}{|G|} \sum_{h \in G} \chi(g^h g') = c_{g,R} \chi(g')$$

which with (3.6) proves the theorem. □

Exercise 93. Given an action of a group G on a finite set X, show that the action of G on the space $V = m(X, \mathbb{C})$ by

$$f^g(x) = f(g^{-1}x)$$

for $f \in m(X, \mathbb{C})$, $g \in G$, $x \in X$ is a representation of G on V, and the character χ of this representation is given by

$$\chi(g) = \text{number of } x \in X \text{ s.t. } gx = x$$

note: dimension of $m(X, \mathbb{C})$ is $|X|$.

Definition 94. The *regular representation* of a finite group on the space $m(G, \mathbb{C})$ comes from the action of G on G by left translation as in the above exercise. It follows that the character χ_{reg} of the regular representation of G satisfies

$$\chi_{reg}(g) = \begin{cases} |G| & g = 1 \\ 0 & g \neq 1 \end{cases}$$

($\because$if $g \neq 1$, $g'g \neq g'$)

Theorem 95. *For each $g \in G$*

$$\chi_{reg}(g) = \sum_{\chi \in \hat{G}} d_\chi \chi(g) = \begin{cases} |G| & g = 1 \\ 0 & g \neq 1 \end{cases} \tag{3.7}$$

In particular

$$\sum_{\chi \in \hat{G}} d_\chi^2 = |G| \tag{3.8}$$

Proof. Let R_{reg} be the regular representation of G. We have

$$R_{reg} = R_1 \oplus ... \oplus R_m$$

with the R_j irreducible, so

$$\chi_{reg} = \chi_1 + ... + \chi_m$$

with χ_j the character of R_j. For $\chi \in \hat{G}$ denote by a_χ the number of i with $\chi_i = \chi$, then

$$\chi_{reg} = \sum_{\chi \in \hat{G}} a_\chi \chi$$

By orthogonality

$$a_\chi = \langle \chi_{reg}, \chi \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_{reg}(g)\chi(g) = \frac{1}{|G|}(\underbrace{|G| d_\chi}_{\chi_{reg}(1)\chi(1)} + 0 + ... + 0) = d_\chi$$

for each $\chi \in \hat{G}$. □

Theorem 96. *(Second Orthogonality Relation) For $g, g' \in G$*

$$\sum_{\chi \in \hat{G}} \bar{\chi}(g)\chi(g') = \begin{cases} |C_G(g)| & g \sim g' \\ 0 & g \not\sim g' \end{cases} \tag{3.9}$$

here $g \sim g'$ means g conjugate to g'.

Proof. By theorems 92, 95, the left side (3.9) is

$$\begin{aligned}\frac{1}{|G|}\sum_{\chi\in\hat{G}} d_\chi \sum_{h\in G}\chi((g^{-1})^h g') &= \frac{1}{|G|}\sum_{h\in G}\chi_{reg}((g^{-1})^h g') \\ &= \text{number of } h \text{ with } g^h = g'\end{aligned}$$

which is 0 if $g' \not\sim g$ and is $|C_G(g)|$ for $g \sim g'$, since the h with $g^h = g'$ make up a coset of $C_G(g)$. □

Theorem 97. *Each finite group G has equally many irreducible characters and conjugacy classes*

$$|\hat{G}| = |\breve{G}| \tag{3.10}$$

and $\hat{G}$ is an orthonormal basis for the class functions on G.

Proof.

$$\begin{aligned}|\hat{G}| &= \sum_{\chi\in\hat{G}} \frac{1}{|G|}\sum_{g\in G}\bar{\chi}(g)\chi(g) \text{ by (3.4)} \\ &= \frac{1}{|G|}\sum_{g\in G}\sum_{\chi\in\hat{G}}\bar{\chi}(g)\chi(g) \\ &= \frac{1}{|G|}\sum_{g\in G}|C_G(g)| \text{ by (3.9)} \\ &= \sum_{g\in G}\frac{1}{(G:C_G(g))} \\ &= \sum_{A\in\breve{G}}\frac{1}{|A|}\sum_{g\in A} 1 \text{ because } G/G_g \simeq Gg \\ &= |\breve{G}|\end{aligned}$$

Since the $\chi \in \hat{G}$ are orthonormal, they are linearly independent class functions, so they span a subspace of the space of class functions of dimension $|\hat{G}| = |\breve{G}|$, which is the dimension of the full space of all class functions. □

Corollary 98. *(of (3.8), (3.10)) A finite group G is abelian $\iff$ each $\chi \in \hat{G}$ has degree 1.*

Proof. G is abelian $\iff$ each class has size 1 $\iff$ $|\breve{G}| = |G|$ $\iff$ $|\hat{G}| = |G|$ $\iff$ each $d_\chi = 1$. □

Exercise 99. Use the corollary and (3.8) to show that for non abelian G,

$$|G| = 6 \implies |\hat{G}| = 3$$
$$|G| = 8 \implies |\hat{G}| = 5$$

there is only 1 G with order 6, and there are two G with order 8.

Lecture 7 (2/18/13)

We can rewrite (3.5) as

$$\theta(g)\theta(g') = \frac{1}{|G|}\sum_{h\in G}\theta(g^h g')\ \forall\, g, g' \in G \tag{3.11}$$

which

$$\theta = \chi/d_\chi \tag{3.12}$$

now the converse

Theorem 100. *Each complex function θ on G with $\theta \not\equiv 0$ which satisfies* (3.11) *is of the form* (3.12) *for some unique $\chi \in \hat{G}$.*

Proof. Put $g = 1$ in (3.11), and get $\theta(1)\theta(g') = \theta(g')\ \forall\, g' \in G$. Since $\theta \not\equiv 0$ this shows that $\theta(1) = 1$. Next put $g' = 1$ in (3.11), and get

$$\theta(g) = \frac{1}{|G|}\sum_{h\in G}\theta(g^h) \quad \forall\, g \in G$$

which shows that θ is a class function. Since $\theta \not\equiv 0$, it follows that $\langle\theta, \chi\rangle \neq 0$ for some $\chi \in \hat{G}$. For such χ and all $g_1 \in G$,

$$\begin{aligned}
\langle\theta, \chi\rangle\, \theta(g_1) &= \frac{1}{|G|}\sum_{g}\theta(g)\bar{\chi}(g)\theta(g_1) \\
&= \frac{1}{|G|^2}\sum_{g}\sum_{h}\theta(gg_1^h)\bar{\chi}(g) \\
&= \frac{1}{|G|^2}\sum_{g'}\sum_{h}\theta(g')\bar{\chi}(g'g_1^{-h}) \\
&= \frac{1}{|G|}\sum_{g'}\theta(g')\bar{\chi}(g')\chi(g_1)/d_\chi \\
&= \langle\theta, \chi\rangle\, \chi(g_1)/d_\chi
\end{aligned}$$

by cancellation, giving $\theta = \chi/d_\chi$. □

3.3 Character Tables

Theorem 101. *For each character χ of G, put $K(\chi) = \{g \in G : \chi(g) = d_\chi\}$, then $K(\chi)$ is the kernel of each representation $R : G \to \mathcal{G}(V)$ with character χ.*

Proof. For each $g \in G$, the group $\langle g \rangle$ generated by g is cyclic, hence abelian, so

$$\chi|_{\langle g \rangle} = \xi_1 + ... + \xi_d$$

$d = d_\chi$, with each $\xi_j = \widehat{\langle g \rangle}$, i.e. each ξ_j a character of $\langle g \rangle$ of degree 1, i.e. a homomorphism from G to $\mathbb{C}^*$ by theorem (82), so $|\xi_j(g)| = 1$. This gives $|\chi(g)| \leq d_\chi$ and shows that for each representation R with character χ,

$$g \in K(\chi) \iff \text{each } \xi_i(g) = 1 \iff R(g) = I_V \iff g \in Ker\, R$$

□

Theorem 102. *Let N be a normal subgroup of G (written $N \lhd G$), and let $g \mapsto \tilde{g} = gN$ be the canonical surjective homomorphism from G to G/N with kernel N. For $w \in \widehat{G/N}$, put $\tilde{w}(g) = w(\tilde{g})$ for $g \in G$. Then the lift map $w \mapsto \tilde{w}$ is an injection from $\widehat{G/N}$ to $\hat{G}$, with image $\{\chi \in \hat{G} : K(\chi) \supset N\}$.*

We often just write w for $\tilde{w}$ when the meaning is clear. We will see why this is a good idea.

Proof. We first show that $w \in \widehat{G/N} \implies \tilde{w} \in \hat{G}$. In fact, let $R : G/N \to \mathcal{G}(V)$ be an irreducible representation of G/N with character w. The composite map $\tilde{R}$ defined by $\tilde{R}(g) = R(\tilde{g})$ is then a homomorphism from G to $\mathcal{G}(V)$, i.e. a representation of G with

$$tr\tilde{R}(g) = trR(\tilde{g}) = w(\tilde{g}) = \tilde{w}(g)$$

thus $\tilde{w}$ is a character of G. Clearly $\tilde{R}$ is irreducible, so $\tilde{w} \in \hat{G}$.

The map $w \mapsto \tilde{w}$ is injective since $w_1 \neq w_2 \implies \tilde{w}_1 \neq \tilde{w}_2$.

For each $w \in \widehat{G/N}$, we have $w(\tilde{1}) = d_w$, so $\tilde{w}(g) = d_w = d_{\tilde{w}}$ for all $g \in N$, showing $K(\tilde{w}) \supset N$. Conversely, if $\chi \in \hat{G}$ with $K(\chi) \supset N$, then by the previous theorem a representation with character χ has kernel $\supset N$, so it is $\tilde{R}$ for some irreducible R of G/N, so $\chi = \tilde{w}$ for some $w \in \widehat{G/N}$. □

Example 103. (character tables) Each G has irreducible character denoted by 1, the principle character, constantly 1. It is the character of the trivial representation of G on $\mathbb{C}$, with $R(g) = I_{\mathbb{C}}$. For general G, the character table looks like this

G	1	S_2	...	S_j	...	S_k
1						
χ_2						
$\vdots$						
χ_j				$\chi_j(g)$		
$\vdots$						
χ_k						

where $k = |\breve{G}| = |\hat{G}|$, $\chi_j(g)$ for $g \in$ conjugacy class S_j.

In the special case $G = 1$ (i.e. $|G| = 1$) 1 is the only irreducible character of G. Its character table is

1	1 = class $\{1\}$
1 = character 1	1 = number $1 \in \mathbb{C}$

For $|G| = 2$, C_2(cyclic)= $\{1, t\}$, with t of order 2. There are two conjugacy classes 1 and $T = \{t\}$, hence two irreducible characters 1 and ε, each of degree 1, (because $\sum deg^2 = 2$)

C_2	1	T
1	1	1
ε	1	-1

here -1 because $\sum d_\chi \chi(g) = 0$ for $g \neq 1$, i.e. $1(T) + \varepsilon(T) = 0$.

For $G = S_3$, which is non abelian of order 6, since

$$\sum_{\chi \in \hat{G}} d_\chi^2 = 6$$

and not all $d_\chi = 1$. It follows that there are 3 irreducible characters of degrees 1,1,2. Since $S_3/A_3 \simeq C_2$, the characters 1 and ε of C_2 lift to the two characters of degree 1 of S_3, also denoted 1 and ε.

S_3	1	R	T
1	1	1	1
$\tilde{\varepsilon}$(or simply ε)	1	1	-1
χ	2	-1	0

where $R = \{(123), (132)\}$, $T = \{(12), (23), (13)\}$. Just use $\sum d_\chi \chi(g) = 0$ for $g \neq 1$ we can figure out the table. Later we will prove Brauer-Nesbitt theorem, which will explain the 0 in the table.

Lemma 104. *Let ξ be a character of G. Then $\xi \in \hat{G} \iff \langle \xi, \xi \rangle = 1$.*

Proof. We know that

$$\xi = \sum_{\chi \in \hat{G}} n_\chi \chi$$

with n_χ integers ≥ 0, so by the first orthogonality relation,

$$\langle \xi, \xi \rangle = \sum n_\chi^2 = 1 \iff \xi = \chi \text{ for some } \chi \in \hat{G}.$$

□

In general product of two irreducible representations need not be irreducible. But we have the following

Corollary 105. *If λ, $\chi \in \hat{G}$, with $d_\lambda = 1$, then $\lambda\chi \in \hat{G}$.*

Proof. $\lambda\chi$ is a character, and $\langle \lambda\chi, \lambda\chi \rangle = \langle \bar{\lambda}\lambda\chi, \chi \rangle = \langle \chi, \chi \rangle = 1$, since $|\lambda| = 1$. □

Example 106. (multiplication table for irreducible characters) Here is the multiplication table for the irreducible characters of S_3

	1	ε	χ
1	1	ε	χ
ε	ε	1	χ
χ	χ	χ	$1 + \varepsilon + \chi$

That $\varepsilon\chi = \chi$ follows from the corollary above and the fact that S_3 has only one irreducible character of degree 2. χ^2 has values 4, 1, 0 on 1, R, T, the same values as $1 + \varepsilon + \chi$, which is a reducible representation written as linear combination with non-negative coefficients.

Direct product comes with two different flavor: external and internal direct products. Below we refer to external direct product.

Theorem 107. *Let H, K be finite groups and let $H \times K$ be their direct product, thus*

$$H \times K = \{(h, k) : h \in H, k \in K\}$$

and

$$(h_1, k_1)(h_2, k_2) = (h_1 h_2, k_1 k_2)$$

For $\psi \in \hat{H}$ and $\phi \in \hat{K}$, define $\psi \times \phi$ on $H \times K$ by

$$(\psi \times \phi)(h, k) = \psi(h)\phi(k)$$

then $\psi \times \phi \in \widehat{H \times K}$, and the map $\psi, \phi \mapsto \psi \times \phi$ bijects $\hat{H} \times \hat{K}$ to $\widehat{H \times K}$.

Proof. Let $\tilde{\psi}$ and $\tilde{\phi}$ be the lift of ψ and ϕ from $H \simeq H \times K/K$ and $K \simeq H \times K/H$ to $H \times K$, then $\psi \times \phi = \tilde{\psi}\tilde{\phi}$, so $\psi \times \phi$ is a character of $H \times K$. Since

$$\langle \psi \times \phi, \psi' \times \phi' \rangle_{H\times K} = \langle \psi, \psi' \rangle_H \langle \phi, \phi' \rangle_K = \delta_{\psi\psi'}\delta_{\phi\phi'} = \delta_{(\psi,\phi)(\psi',\phi')} \tag{3.13}$$

each $\psi \times \phi$ is irreducible by the lemma above, and the map $\psi, \phi \mapsto \psi \times \phi$ is injective from $\hat{H} \times \hat{K}$ to $\widehat{H \times K}$. The number of irreducible characters of $H \times K$ that we get in this way is

$$|\hat{H}||\hat{K}| = |\check{H}||\check{K}| = |H \mathbin{\check{\times}} K| = |\widehat{H \times K}| \tag{3.14}$$

Thus the map $\psi, \phi \mapsto \psi \times \phi$ is surjective. □

Exercise 108. Prove (3.13), and (3.14).

4 Algebraic Integers and its Application to Characters

Lecture 8 (2/20/13)

One of the motives of studying algebraic integers in representation theory is to prove several facts. One due to Frobenius, that

$$d_\chi \text{ divides } |G|, \text{ for each } \chi \in \hat{G} \tag{4.1}$$

and a certain refinement of this due to Schur. The fact (4.1) is analogous to the fact about actions of G on finite sets X, that

$$|X| \text{ divides } |G|, \text{ if } G \text{ acts transitively on } X \tag{4.2}$$

While (4.2) is elementary, X being an orbit Gx of size $(G : G_x)$, all known proofs of (4.1) use algebraic integers. This is remarkable, since d_χ and $|G|$ are ordinary integers.

4.1 Algebraic Integers

Definition 109. A complex number α is an algebraic integer if α is a root of a monic (i.e. $a_0 = 1$) polynomial with integer coefficients, i.e. for some $n \in \mathbb{N}$,

$$\alpha^n + a_1\alpha^{n-1} + ... + a_n = 0 \tag{4.3}$$

for some $a_1, ..., a_n \in \mathbb{Z}$. We denote the set of all algebraic integers by $\mathbb{A}$.

Theorem 110.

$$\mathbb{A} \cap \mathbb{Q} = \mathbb{Z}$$

Proof. Each $a \in \mathbb{Z}$ is an algebraic integer, since it is a root of $z - a$, thus $\mathbb{Z} \subset \mathbb{A}$. Since also $\mathbb{Z} \subset \mathbb{Q}$, we have $\mathbb{Z} \subset \mathbb{A} \cap \mathbb{Q}$.

Now let $\alpha \in \mathbb{A} \cap \mathbb{Q}$, since $\alpha \in \mathbb{A}$, we may suppose that (4.3) holds, for some $a_1, ..., a_n \in \mathbb{Z}$. Since $\alpha \in \mathbb{Q}$, we have $\alpha = a/q$ with $a \in \mathbb{Z}$ and $q \in \mathbb{N}$. We may suppose that a and q are relatively prime. Substituting $\alpha = a/q$ into (4.3) and multiplying by q^n gives

$$a^n + a_1 a^{n-1} q + ... + a_n q^n = 0$$

from which q divides a^n. Since a and q are relatively prime, it follows that $q = 1$, i.e. $\alpha = a \in \mathbb{Z}$. Thus $\mathbb{A} \cap \mathbb{Q} \subset \mathbb{Z}$. □

Next we give an often more useful definition of $\mathbb{A}$

Lemma 111. *Let $\alpha \in \mathbb{C}$. Then $\alpha \in \mathbb{A}$ if and only if, for some $n \in \mathbb{N}$,*

$$\alpha z_j = \sum_{i=1}^{n} c_{ij} z_i \text{ for } j = 1, ..., n \tag{4.4}$$

for some z_1,...,$z_n \in \mathbb{C}$, not all 0, and some $c_{ij} \in \mathbb{Z}$, $(i, j = 1, ..., n)$

Proof. If $\alpha \in \mathbb{A}$, then (4.3) holds for some $a_1, ..., a_n \in \mathbb{Z}$, so α satisfies (4.4) with $z_1, .., z_n = 1, \alpha, ..., \alpha^{n-1}$ and certain $c_{ij} \in \mathbb{Z}$

$$\alpha \alpha^{j-1} = \alpha^j \text{ for } j = 1, .., n-1$$

$$\alpha \alpha^{n-1} = -a_n - ... - a_1 \alpha^{n-1}$$

Since $z_1 = 1 \neq 0$, not all 0.

Conversely, if (4.4) holds with z_i and c_{ij} as in the lemma, then

$$\sum_{i=1}^{n} (\delta_{ij} \alpha - c_{ij}) z_i = 0 \text{ for } j = 1, ..., n$$

with $\delta_{ij} = 1$ for $i = j$ and 0 for $i \neq j$. Since $z_1, .., z_n$ are not all 0,

$$det(\delta_{ij} \alpha - c_{ij}) = 0$$

Since the c_{ij} are all in $\mathbb{Z}$, the above equation is indeed monic and of the form (4.3) with $a_1, ..., a_n \in \mathbb{Z}$, so $\alpha \in \mathbb{A}$. □

Theorem 112. *If α and β are algebraic integers, so are $\alpha+\beta$ and $\alpha\beta$.*

This shows $\mathbb{A}$ form a ring.

Proof. Suppose α satisfies (4.3), and β satisfies

$$\beta^m + b_1\beta^{m-1} + ... + b_m = 0$$

with all a_k and $b_l \in \mathbb{Z}$. Then for $k = 0, ..., n-1$ and $l = 0, ..., m-1$

$$(\alpha+\beta)(\alpha^k\beta^l) = \alpha^{k+1}\beta^l + \alpha^k\beta^{l+1}$$

For $k = n-1$

$$\alpha^{k+1}\beta^l = -a_n\beta^l - ... - a_1\alpha^{n-1}\beta^l$$

and for $l = m-1$

$$\alpha^k\beta^{l+1} = -b_m\alpha^k - ... - b_1\alpha^k\beta^{m-1}$$

It follows that with $z_1, ..., z_{mn}$ equal in some order to the $\alpha^k\beta^l$ with $k = 0, ..., n-1$ and $l = 0, ..., m-1$, we do have

$$(\alpha+\beta)z_v = \sum_{u=1}^{mn} c_{uv}z_u \text{ for } v = 1, ..., mn$$

with all $c_{uv} \in \mathbb{Z}$. Since $\alpha^0\beta^0 = 1 \neq 0$, not all z_u are 0, therefore $\alpha+\beta \in \mathbb{A}$, by the lemma.

Similarly, for $k = 0, ..., n-1$ and $l = 0, ..., m-1$

$$(\alpha\beta)(\alpha^k\beta^l) = \alpha^{k+1}\beta^{l+1}$$

so, as above, with the same $z_1, ..., z_{mn}$, we have

$$\alpha\beta z_v = \sum_{n=1}^{mn} d_{nv}z_n \text{ for } v = 1, .., mn$$

with all $d_{nv} \in \mathbb{Z}$, so $\alpha\beta \in \mathbb{A}$. □

Corollary 113. *Each root of unity in $\mathbb{C}$ is an algebraic integer. Each $\chi(g)$ is an algebraic integer, for each character χ of a finite group G and each $g \in G$.*

Proof. If $\xi \in \mathbb{C}$ is a root of unity, i.e. $\xi^n = 1$ for some $n \in \mathbb{N}$, then ξ is a root of $z^n - 1$, so $\xi \in \mathbb{A}$.

For each character χ of G and each $g \in G$

$$\chi(g) = \xi_1(g) + ... + \xi_d(g)$$

where d is the degree of χ and $\xi_1, ..., \xi_d$ are characters of $\langle g \rangle$ of degree 1. Since each ξ_j is a homomorphism from $\langle g \rangle$ to $\mathbb{C}^*$, each $\xi_j(g)$ is a root of unity and therefore belongs to $\mathbb{A}$. By previous theorem, $\chi(g) \in \mathbb{A}$ $\square$

Theorem 114. *$\mathbb{A}$ is integrally closed, i.e. if $\alpha \in \mathbb{C}$ and α is a root of a monic polynomial with coefficients in $\mathbb{A}$, then $\alpha \in \mathbb{A}$.*

Proof. Let $\alpha \in \mathbb{C}$ satisfy

$$\alpha^m + \alpha_1 \alpha^{m-1} + ... + \alpha_m = 0$$

with $\alpha_1, ..., \alpha_m \in \mathbb{A}$. Thus there are $a_{ij} \in \mathbb{Z}$ for which

$$\begin{cases} \alpha_1^{n_1} + a_{11}\alpha_1^{n_1-1} + ... + a_{1n_1} = 0 & (1) \\ \vdots & \vdots \\ \alpha_j^{n_j} + a_{j1}\alpha_j^{n_j-1} + ... + a_{jn_j} = 0 & (j) \\ \vdots & \vdots \\ \alpha_m^{n_m} + a_{m1}\alpha_m^{n_m-1} + ... + a_{mn_m} = 0 & (m) \end{cases} \tag{4.5}$$

It suffices to show that α satisfies (4.4) with $z_1, ..., z_n$ ($n = n_1 n_2 \cdot ... \cdot n_m$) equal in some order to

$$z_k = \alpha_1^{k_1} \cdot ... \cdot \alpha_m^{k_m} \cdot \alpha^k$$

with $0 \leq k_1 < n_1, ..., 0 \leq k_m < n_m$, $0 \leq k < m$.

In fact each αz_v is of the form z_μ except if $k = m - 1$, in which case

$$\alpha z_v = -(\alpha_1^{k_1} \cdot ... \cdot \alpha_m^{k_m+1}) - ... - (\alpha_1^{k_1+1} \cdot ... \cdot \alpha_m^{k_m})\alpha^{m-1}$$

Any term on the right is some z_μ unless it has $k_j + 1 = n_j$, then it can be substituted by using $(4.5j)$, and then it becomes a linear combination of the $z_\mu$with integer coefficients $(a_{j1}, a_{j2}, ...)$, giving (4.4). Since the particular z_v with $k_1 = ... = k_m = k = 0$ is $1 (\neq 0)$, not all of the z_μ are 0, so $\alpha \in \mathbb{A}$, by the lemma. $\square$

1896 was a big year for mathematics, in which Frobenius invented character of finite group and Hadamard discovered prime number theorem. Both of them used very surprising and seemingly unrelated tools. Frobenius used property of algebraic number to prove characters. Hadamard used complex analysis (Riemann-Zeta function) to prove prime number theorem.

Theorem 115. *(Frobenius) For each $\chi \in \hat{G}$, d_χ is a divisor of $|G|$.*

This proof from Frobenius is hard, later we will give a simpler proof.

Proof. From the convolution formula with $\chi' = \chi$

$$\frac{\chi(g)}{d_\chi} = \frac{1}{|G|} \sum_{h \in G} \chi(gh^{-1})\chi(h) \; \forall \, g \in G$$

writing this as

$$\sum_{h \in G} (\frac{|G|}{d_\chi} \delta_{g,h} - \chi(gh^{-1}))\chi(h) = 0 \quad \forall \, g \in G$$

and using the fact that not all $\chi(h) = 0$ (e.g. $\chi(1) = d_\chi \neq 0$), it follows that

$$det(\frac{|G|}{d_\chi} \delta_{g,h} - \chi(gh^{-1})) = 0$$

which says that $|G|/d_\chi$ is a root of the characteristic polynomial of the square matrix $[\chi(gh^{-1})]_{g,h \in G}$. Since the matrix entries are in $\mathbb{A}$ by corollary 113, the coefficients of this polynomial, which are sums of products of matrix elements and -1 are also in $\mathbb{A}$. By previous theorem, the root $|G|/d_\chi$ is in $\mathbb{A}$. Since $|G|/d_\chi \in \mathbb{Q}$, we conclude by theorem 110 that $|G|/d_\chi \in \mathbb{Z}$, d_χ divides $|G|$. □

Theorem 116. *For each $\chi \in \hat{G}$,*

(a) restriction $\chi | Z(G) = d_\chi \xi$ for some $\xi \in \widehat{Z(G)}$.

(b) $\chi(gz) = \chi(g)\xi(z) \; \forall \, g \in G$, $z \in Z(G)$

Proof. Let $\chi = \chi_R$ with R a representation of G on V. By corollary 51 of Schur's lemma,

$$R(z) = \xi(z) I_V \text{ for } z \in Z(G), \text{ for some } \xi(z) \in \mathbb{C}^*$$

Since R is a homomorphism, so is $R|Z(G)$, so is $\xi : Z(G) \to \mathbb{C}^*$, i.e. $\xi \in \widehat{Z(G)}$. From above

$$R(gz) = \xi(z)R(g) \text{ for } g \in G, z \in Z(G)$$

Taking trace gives (b). Putting $g = 1$ in (b) gives (a). □

Here is the improved result of Frobenius

Theorem 117. *(Schur) For each $\chi \in \hat{G}$, d_χ divides $|G_1|$. where $G_1 = G/Z(G)$.*

Proof. Let h_i be coset representation for G modules $Z(G)$, $i = 1, ..., |G_1|$. Thus each $h \in G$ can be written uniquely as $h = h_i z$ for some i and some $z \in Z(G)$. From previous theorem (b),

$$\chi(gh^{-1})\chi(h) = \chi(gh_i^{-1})\xi(z^{-1})\chi(h_i)\xi(z) = \chi(gh_i^{-1})\chi(h_i)$$

since $\xi(z^{-1})\xi(z) = 1$. Therefore the convolution formula for $\chi' = \chi$ may be written

$$\frac{\chi(g)}{d_\chi} = \frac{1}{|G_1|}\sum_{i=1}^{|G_1|}\chi(gh_i^{-1})\chi(h_i) \text{ for } g \in G$$

Putting $g = h_j$ this gives as before

$$\sum_{i=1}^{|G_1|}(\frac{|G_1|}{d_\chi}\delta_{ij} - \chi(h_j h_i^{-1})\chi(h_i) = 0 \text{ for } j = 1, ..., |G_1|$$

Since not all $\chi(h_i) = 0$ (since $\chi \not\equiv 0$), this implies that $d_\chi | |G_1|$, by the same argument as in the proof of Frobenius. □

4.2 Class Multiplication Constants

Lecture 9 (2/27/13)

Notation 118. For $\chi \in \hat{G}$, $A \in \breve{G}$, put

$$w_\chi(A) = \frac{|A|\chi(a)}{d_\chi} \text{ for } a \in A \tag{4.6}$$

this makes sense since χ is a class-function.

For each pair of conjugacy classes A, B in G and each element $c \in G$, put

$$m_{AB}^c = |\{(a, b) \in A \times B : ab = c\}| \tag{4.7}$$

Theorem 119. *For each triple of conjugacy classes A, B, C and each $c \in C$*

$$|C| m_{AB}^c = \frac{1}{|G|} \sum_{\chi \in \hat{G}} d_\chi^2 w_\chi(A) w_\chi(B) \bar{w}_\chi(C) \tag{4.8}$$

In particular, m_{AB}^c depends only on A, B, C so we may write

$$m_{AB}^C = m_{AB}^c \text{ for } c \in C$$

Proof. Recall the special character χ_{reg}, which satisfies

$$\chi_{reg} = \sum_{\chi \in \hat{G}} d_\chi \chi \qquad \chi_{reg}(g) = \begin{cases} |G| & g = 1 \\ 0 & g \neq 1 \end{cases}$$

From this and (4.7) we get

$$m_{AB}^c = \frac{1}{|G|} \sum_{a \in A, b \in B} \chi_{reg}(abc^{-1}) = \frac{1}{|G|} \sum_{\chi \in \hat{G}} d_\chi \sum_{a \in A, b \in B} \chi(abc^{-1})$$

so it suffices to show that for each $\chi \in \hat{G}$, each A, B, $C \in \breve{G}$ and each $c \in C$,

$$|C| \sum_{a \in A, b \in B} \chi(abc^{-1}) = d_\chi w_\chi(A) w_\chi(B) \bar{w}_\chi(C) \tag{4.9}$$

To see above, start with the functional equation for χ, written as

$$\sum_{g \in G} \chi(a^g b) = \frac{|G|}{d_\chi} \chi(a) \chi(b)$$

Replacing b by $b^h c^{-1}$ in this, and summing on $h \in G$ gives

$$\sum_{g,h \in G} \chi(a^g b^h c^{-1}) = \frac{|G|}{d_\chi} \chi(a) \sum_{h \in G} \chi(b^h c^{-1}) = \frac{|G|^2}{d_\chi^2} \chi(a) \chi(b) \bar{\chi}(c) \tag{4.10}$$

The double sum on the left is

$$\frac{|G|^2}{|A||B|} \sum_{a \in A, b \in B} \chi(abc^{-1})$$

so (4.9) follows from (4.10) and using the definition of w_x of (4.6). □

Exercise 120. Prove the above assertion about the double sum on the left in (4.10).

Theorem 121. *For all $A, B \in \breve{G}$ and all $\chi \in \hat{G}$,*

$$w_\chi(A)w_\chi(B) = \sum_{C\in\breve{G}} m_{AB}^C w_\chi(C)$$

Proof. Write (4.8) as

$$m_{AB}^C = \frac{1}{|G|}\sum_{\chi'\in\hat{G}} d_{\chi'} w_{\chi'}(A)w_{\chi'}(B)\bar{\chi}'(c) \text{ for } c \in C$$

Multiply this by $\chi(c)$ and sum on $c \in G$ to get

$$d_\chi \sum_{C\in\breve{G}} m_{AB}^C w_\chi(C) = \frac{1}{|G|}\sum_{\chi'\in\hat{G}} d_{\chi'} w_{\chi'}(A)w_{\chi'}(B)\sum_{c\in G}\bar{\chi}'(c)\chi(c)$$

The inner sum on the right is $|G|\delta_{\chi\chi'}$, so the right side reduces to $d_\chi w_\chi(A)w_\chi(B)$. □

Theorem 122. *For each $\chi \in \hat{G}$ and $A \in \breve{G}$,*

$$w_\chi(A) \in \mathbb{A}$$

Proof. This follows from the previous theorem and the second definition of $\mathbb{A}$. Let $z_1, ..., z_k$ be $w_\chi(C)$ for $C \in \breve{G}$, in some order, then

$$w_\chi(A)z_j = \sum_{i=1}^{k} c_{ij}z_j$$

with the $c_{ij}(= m_{AB}^C) \in \mathbb{Z}$ and not all $z_j = 0$, since e.g. $w_\chi(1) = 1 \neq 0$. It follows that each $w_\chi(A) \in \mathbb{A}$. □

Corollary 123. *The degree of each irreducible character of G divides the order of G.*

This is a second proof, not using the fact that $\mathbb{A}$ is integrally closed. (cf proof of theorem115)

Proof. We have

$$\frac{|G|}{d_\chi} = \sum_{a\in G}\frac{|\chi(a)|^2}{d_\chi} = \sum_{A\in\breve{G}}\bar{\chi}(a)w_\chi(A) \text{ for any } a \in A$$

Since each $\bar{\chi}(a)$ and $w_\chi(A)$ is in $\mathbb{A}$, so is the sum of the products, so $|G|/d_\chi \in \mathbb{A}$. But $|G|/d_\chi \in \mathbb{Q}$, so $|G|/d_\chi \in \mathbb{A} \cap \mathbb{Q} = \mathbb{Z}$. □

4.3 Determinant of a Representation.

Definition 124. For each character $\chi = \chi_R$ of a group G

$$det\chi = detR$$

i.e.

$$(det\chi)(g) = det(R(g)) \text{ for } g \in G$$

Exercise 125. Show that $det\chi$ is a character of G of degree 1 which is independent of the choice of R with character χ, i.e. if R_1 and R_2 are representations with character χ, then $detR_1 = detR_2$.

Exercise 126. Consider S_3 with its three irreducible characters $1, \varepsilon, \chi$

	1	R	T
1	1	1	1
ε	1	1	-1
χ	2	-1	0

Show that in this example, $det1 = 1$ and $det\varepsilon = \varepsilon$.

We will show that, in this example, $det\chi = \varepsilon$. First $det\chi$ being a character of degree 1, $det\chi = 1$ or ε, we rule out $det\chi = 1$ by showing

$$(det\chi)(t) = -1 \text{ for } t \text{ of order } 2$$

Let's consider the restriction of $1, \varepsilon, \chi$ to the cyclic group $\langle t \rangle$. There are two irreducible characters of $\langle t \rangle$, each of degree 1. Here is the table

	1	t
1	1	1
δ	1	-1

Since $\chi(1) = 2$ and $\chi(t) = 0$, we see that

$$\chi|\langle t \rangle = 1 + \delta$$

Exercise 127. Prove that for all characters χ' and χ'' of a finite group G,

$$det(\chi' + \chi'') = (det\chi')(det\chi'')$$

Hint consider $R' \oplus R''$ and the corresponding square matrices.

It follows from $\chi|\langle t \rangle = 1 + \delta$ that $(det\chi)(t) = -1$.

Exercise 128. For each finite group G, show the characters δ of degree 1 form a group under multiplication. Thus each such δ has an order, as an element of this group.

Notation 129. For each character χ of G, $det\chi = detR$ where $\chi = \chi_R$, and o_χ denotes the order of $det\chi$.

Example 130. For χ the irreducible character of degree 2 of S_3, $o_\chi = 2$.

The following is an improved result of Schur's

Theorem 131. *For each* $\chi \in \hat{G}$,

$$o_\chi \text{ divides } 2|G|/d_\chi$$

Equivalently,

$$d_\chi \text{ divides } 2|ker\, det\chi|$$

Exercise 132. Prove the equivalence of the two statements above.

Example 133. The character of degree 2 of S_3 has $d_\chi = 2$ and $o_\chi = 2$. Here $|ker\, det\chi| = 3$, so the "2" in the theorem can not be dropped.

Lecture 10 (3/4/13)

Notation 134. For each $a \in G$, let

n = order of a;

C = the cyclic subgroup generated by a (so $C = \{1, a, ..., a^{n-1}\}$);

ψ = a generator for $\hat{C}$ (so $\hat{C} = \{1, \psi, ..., \psi^{n-1}\}$);

A = the conjugacy class of a, so $|A| = (G : C_G(a))$.

Theorem 135. *For each* $\chi \in \hat{G}$ *and* $a \in G$,

$$det\chi|C = \psi^e$$

with

$$2e|A| \text{ divisible by } d_\chi$$

We show theorem 135 implies theorem 131: From

$$|G| = (G : C_G(a))(C_G(a) : \langle a\rangle)|\langle a\rangle| = |A|(C_G(a) : \langle a\rangle)n$$

Then

$$(det\chi|C)^{2|G|/d_\chi} = \psi^{2|G|e/d_\chi} = ((\psi^n)^{2e|A|/d_\chi})^{(C_G(a):\langle a\rangle)} = 1$$

the last equality is given by theorem 135, because $2e|A|/d_\chi(C_G(a) : \langle a\rangle) \in \mathbb{Z}$.

Lemma 136. *With same notation as in theorem 135,*

$$det\chi|C = \psi^e$$

with

$$e = \frac{n-1}{2}d_\chi - \sum_{k=1}^{n-1} \frac{\chi(a^k)}{1-\bar{\psi}(a^k)} \tag{4.11}$$

Proof. We have

$$\chi|C = \sum_{j=0}^{n-1} c_j\psi^j \text{ for certain non-negative integers } c_j$$

with $c_j = \langle \chi|C, \psi^j \rangle = \langle \chi, \psi^j \rangle_C$, so

$$det\chi|C = \prod_{j=0}^{n-1} det(c_j\psi^j) = \prod_{j=0}^{n-1} [det(\psi^j)]^{c_j} = \prod_{j=0}^{n-1} \psi^{jc_j} = \psi^e$$

with

$$e = \sum_{j=0}^{n-1} jc_j = \sum_{j=0}^{n-1} j \langle \chi, \psi^j \rangle_C = \left\langle \chi, \sum_{j=0}^{n-1} j\psi^j \right\rangle_C$$

The formula for e in the lemma follows from this, together with the following lemma. □

Lemma 137. *For each $n \in \mathbb{N}$ and each n^{th} root of unity ξ in $\mathbb{C}$*

$$\sum_{j=0}^{n-1} j\xi^j = \begin{cases} -\frac{n}{1-\xi} & \xi \neq 1 \\ \frac{n(n-1)}{2} & \xi = 1 \end{cases}$$

Proof. For $z \in \mathbb{C}$ with $z \neq 1$,

$$\sum_{j=0}^{n-1} jz^j = z\frac{d}{dz}\sum_{j=0}^{n-1} z^j = z\frac{d}{dz}\frac{1-z^n}{1-z} = \frac{-nz^n}{1-z} + z\frac{1-z^n}{(1-z)^2}$$

Plugging in $z = \xi \neq 1$ with $\xi^n = 1$ gives the first statement. The second statement $1 + 2 + ... + (n-1)$ is obvious. □

Lemma 138. *For $n \in \mathbb{N}$, put*

$$v_n = \prod_{\substack{p \text{ prime} \\ p|n}} p^{\frac{1}{p-1}}$$

then $v_n \in \mathbb{A}$, and for each nth root of unity ξ, except $\xi = 1$,

$$\frac{v_n}{1-\xi} \in \mathbb{A} \tag{4.12}$$

also for $d, m, n \in \mathbb{N}$,

$$\text{if } v_n \frac{m}{d} \in \mathbb{A}, \text{ then } \frac{2m}{d} \in \mathbb{N} \tag{4.13}$$

We now prove theorem 135.

Proof. By (4.11)

$$\frac{e|A|}{d_\chi} = \frac{n-1}{2}|A| - \sum_{k=1}^{n-1} \frac{|A|\chi(a^k)/d_\chi}{1-\bar{\psi}(a^k)} \tag{4.14}$$

The numerator of each term in the sum is in $\mathbb{A}$: Since $C_G(a) \subset C_G(a^k)$,

$$\begin{aligned} |A|\chi(a^k)/d_\chi &= (G : C_G(a))\chi(a^k)/d_\chi \\ &= \Big[(G : C_G(a^k))\chi(a^k)/d_\chi\Big]\Big[(C_G(a^k) : C_G(a))\Big] \end{aligned}$$

where $(G : C_G(a^k))\chi(a^k)/d_\chi \in \mathbb{A}$ by thereon 122, and $(C_G(a^k) : C_G(a)) \in \mathbb{N}$

Multiplying (4.14) by v_n and applying (4.12) gives

$$v_n \frac{e|A|}{d_\chi} = v_n \frac{n-1}{2}|A| - \sum_{k=1}^{n-1} \frac{|A|\chi(a^k)}{d_\chi} \frac{v_n}{1-\bar{\psi}(a^k)} \in \mathbb{A}$$

It follows from above and (4.13) that

$$2e\frac{|A|}{d_\chi} \in \mathbb{N}$$

□

Now prove (4.12).

Proof. First show $v_n \in \mathbb{A}$. Since $p^{\frac{1}{p-1}}$ is root of $z^{p-1} - p$, v_n is product of algebraic numbers, so $v_n \in \mathbb{A}$.

For $n \in \mathbb{N}$ and $z \in \mathbb{C}$,

$$\Phi_n(z) = \prod_{ord\,\xi = n} (z - \xi)$$

so called nth *cyclotomic polynomial* of order $\varphi(n)$. Here $ord\,\xi$ is the least n so that $\xi^n = 1$. (e.g. $\Phi_4 = (z+i)(z-i)$) For all $n \in \mathbb{N}$,

$$\prod_{d|n} \Phi_d(z) = \prod_{\xi^n = 1} (z - \xi) = z^n - 1$$

(e.g. $z^4 - 1 = \Phi_1\Phi_2\Phi_4 = (z-1)(z+1)(z+i)(z-i)$)

Since $\Phi_1(z) = z - 1$, this gives

$$\prod_{1<d|n} \Phi_d(z) = \frac{z^n - 1}{z - 1} \text{ for } z \neq 1$$

Letting $z \to 1$, it follows by L'Hopital that

$$\prod_{1<d|n} \Phi_d(1) = n \tag{4.15}$$

It follows that for $n \in \mathbb{N}$ with $n > 1$,

$$\Phi_n(1) = \begin{cases} p & n = p^\alpha,\ p \text{ prime},\ \alpha \geq 1 \\ 1 & \text{otherwise} \end{cases} \tag{4.16}$$

In fact, for $n = p^v$ with $v \geq 1$, $\Phi_n(1) = p$ follows from (4.15) by induction on α. For $n = \prod_p p^\alpha$ with more than one prime occurring, the prime-power divisors of n already contribute $\prod p^\alpha = n$, and the other divisors d of n with $d < n$ each contribute 1 by induction so $\Phi_n(1) = 1$ by (4.15).

On the other hand,

$$\Phi_n(1) = \prod_{ord\,\xi' = n} (1 - \xi') = (1 - \xi)^{\varphi(n)} \prod_{ord\,\xi' = n} \frac{1 - \xi'}{1 - \xi}$$

where ξ is any root of unity of order n. $\varphi(n)$ is Euler's function, counts the number of positive integers less than or equal to n that are relatively prime to n.

Since each ξ' is of the form ξ^k, we have

$$\frac{1-\xi'}{1-\xi} = 1 + \xi + ... + \xi^{k-1} \in \mathbb{A}$$

giving

$$\frac{\Phi_n(1)^{\frac{1}{\varphi(n)}}}{1-\xi} \in \mathbb{A} \quad \text{for } \xi \text{ of order } n > 1 \tag{4.17}$$

Using (4.16), we can also show that

$$\frac{v_n}{\Phi_n(1)^{\frac{1}{\varphi(n)}}} \in \mathbb{A} \tag{4.18}$$

To prove above, it suffices to prove this for $n = p^\alpha$, $\alpha \geq 1$. In this case $\Phi_n(1) = p$, so

$$\frac{v_n}{\Phi_n(1)^{\frac{1}{\varphi(n)}}} = p^{\frac{1}{p-1} - \frac{1}{\varphi(n)}} = p^{\text{rational} \geq 0} \in \mathbb{A}$$

Multiplying (4.17), (4.18) gives (4.12) in the case ξ has order $n > 1$.

If $ord\,\xi = d$ with $1 < d|n$, then $v_d|v_n$, so

$$\frac{v_n}{1-\xi} = \frac{v_n}{v_d}\frac{v_d}{1-\xi} \in \mathbb{A}$$

too proving (4.12). □

Now we prove (4.13)

Proof. Let

$$N = \prod_{\substack{p \text{ prime} \\ p|n}} (p-1)$$

Raising $v_n \frac{m}{d} \in \mathbb{A}$ to the Nth power gives

$$0 < v_n^N \frac{m^N}{d^N} \in \mathbb{A}$$

with $v_n^N = \prod_{p|n} p^{N/(p-1)} \in \mathbb{N}$, thus by theorem 110,

$$v_n^N \frac{m^N}{d^N} \in \mathbb{N}$$

Let p^{δ_p} and p^{μ_p} be the highest power of p dividing d and m respectively. Then

$$N\delta_p \leq N\mu_p + \frac{N}{p-1} \text{ for } p|n$$

and

$$N\delta_p \leq N\mu_p \text{ for } p \nmid n$$

Thus for all p, we have

$$\delta_p \leq \mu_p + \frac{1}{1-p}$$

showing $\delta_p \leq \mu_p$ for $p \neq 2$ and $\delta_2 \leq \mu_2 + 1$(this shows why there is an extra "2" in (4.13)). □

4.4 Cyclotomic Polynomial

Lecture 11 (3/6/13)

We now formally study cyclotomic polynomials, which used in the proof from last time.

Notation 139. For $m \in \mathbb{N}$,

$$C_m = \{\xi \in \mathbb{C} : \xi^m = 1\}$$

i.e. C_m is the set of all mth roots of unity, i.e. roots of $z^m - 1$.

Observe that C_m is a cyclic group, generated e.g. by $\xi_m = e^{2\pi i/m}$, so

$$C_m = \{\xi_m^j : j = 0, 1, ..., m-1\}$$

Definition 140. An element $\xi \in C_m$ is a primitive mth root of unity if ξ has order m, rather than a proper divisor of m.

For example $C_4 = \{1, i, -1, -i\}$ but only $\pm i$ are primitive 4th roots of unity.

Lemma 141. *The primitive mth roots of unity are the ξ_m^k with $0 \leq k < m$ and $(k, m) = 1$.*

Proof. Let's calculate the order of each ξ_m^k. For $l \in \mathbb{N}$,

$$(\xi_m^k)^l = \xi_m^{kl} = 1 \iff m|kl \iff \frac{m}{(k,m)} \Big| \frac{k}{(k,m)} l \iff \frac{m}{(k,m)} \Big| l$$

the last $\iff$ is because $m/(k, m)$ are $k/(k, m)$ are relatively prime.

It follows that the order of ξ_m^k, which is the least $l \in \mathbb{N}$ with $(\xi_m^k)^l = 1$ is $m/(k, m)$. In particular ξ_m^k is primitive $\iff$ $(k, m) = 1$. □

Theorem 142. *The automorphisms of C_m (i.e. bijective homomorphism $\sigma : C_m \to C_m$) are the maps σ_k for $0 \leq k < m$ with $(k, m) = 1$ defined by*

$$\sigma_k(\xi) = \xi^k \text{ for } \xi \in C_m$$

Proof. For each homomorphism $\sigma : C_m \to C_m$, we have

$$\sigma(\xi_m) = \xi_m^k \tag{4.19}$$

for some k with $0 \leq k < m$, and then

$$\sigma(\xi) = \xi^k$$

for all $\xi \in C_m$, since $\xi \in C_m$ implies $\xi = \xi_m^j$ for some j with $0 \leq j < m$, so (4.19) gives

$$\begin{aligned} \sigma(\xi) &= \sigma_k(\xi_m^j) \\ &= \sigma_k(\xi_m)^j \text{ because } \sigma_k \text{ is a homomorphism} \\ &= (\xi_m^k)^j \text{ by (4.19)} \\ &= (\xi_m^j)^k \\ &= \xi^k \end{aligned}$$

Conversely for each k with $0 \leq k < m$, the map $\sigma_k : C_m \to C_m$ defined by

$$\sigma_k(\xi) = \xi^k \ \forall\, \xi \in C_m$$

is a homomorphism. In fact for ξ,$\xi' \in C_m$,

$$\sigma_k(\xi\xi') = (\xi\xi')^k = \xi^k \xi'^k = \sigma_k(\xi)\sigma_k(\xi')$$

The m homomorphisms $\sigma_k : C_m \to C_m$ for $0 \leq k < m$ are distinct, since if $0 \leq k, k' < m$ and $\sigma_k = \sigma_{k'}$, then

$$\xi_m^k = \sigma_k(\xi_m) = \sigma_{k'}(\xi_m) = \xi_m^{k'}$$

so

$$\xi_m^{k-k'} = 1, \implies k = k'. \tag{4.20}$$

Among the m homomorphism $\sigma_k : C_m \to C_m$ with $0 \leq k < m$, which ones are automorphism? Since $\sigma_k C_m \simeq C_m / ker\sigma_k$, we see that σ_k is injective $\iff$ $ker\sigma_k = 1$ $\iff$ $\sigma_k C_m = C_m$ $\iff$ σ_k is surjective. Since $\sigma_k C_m$ is generated by ξ_m^k, we see that σ_k is surjective $\iff$ σ_m^k has order m $\iff$ $(k, m) = 1$. □

Exercise 143. Justify (4.20) in the proof.

Exercise 144. Prove

$$AutC_m \simeq (\mathbb{Z}/m\mathbb{Z})^*$$

Notation 145. For $m \in \mathbb{N}$,

$$\mathbb{A}_m = \{ \sum_{\xi \in C_m} a_\xi \xi : \text{ all } a_\xi \in \mathbb{Z}\}$$

i.e.

$$\mathbb{A}_m = \{f(\xi_m) : f \in \mathbb{Z}[x]\}$$

i.e. f is a polynomial with coefficients in $\mathbb{Z}$.

We will see that $\mathbb{A}_m$ has more structure than C_m.

Note that $\mathbb{A}_m$ is a subring of $\mathbb{C}$, i.e. $\mathbb{A}_m$ is an abelian group under $+$, and also $\alpha, \beta \in \mathbb{A}_m \implies \alpha\beta \in \mathbb{A}_m$. Just like group homomorphism, e.g. permutation, preserves multiplication. Ring homomorphism preserves $+, \times$.

Definition 146. An automorphism of $\mathbb{A}_m$ is a bijective map $\sigma : \mathbb{A}_m \to \mathbb{A}_m$ satisfying

(i) $\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta)$ and (ii) $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$

for all $\alpha, \beta \in \mathbb{A}_m$.

Note that the automorphisms of $\mathbb{A}_m$ form a group under composition. It is called the *Galois group* of $\mathbb{A}_m$. We denote it by $\mathcal{G}_m$.

Remark 147. Each $\sigma \in \mathcal{G}_m$ restricts to an automorphism σ_k of C_m, i.e. there is a k with $0 \leq k < m$ and $(k, m) = 1$ for which

$$\sigma(\xi) = \xi^k \text{ for all } \xi \in C_m,$$

so by definition 146 (i), we must have more generally

$$\sigma(\alpha) = \sigma(\sum_{\xi \in C_m} a_\xi \xi) = \sum_{\xi \in C_m} a_\xi \xi^k \tag{4.21}$$

for all $\alpha = \sum_{\xi \in C_m} a_\xi \xi \in \mathbb{A}_m$. However it is not obvious that such $\sigma_k \in AutC_m$ extends to an element of $\mathcal{G}_m$, only that if it does, then it must be given by (4.21).

We will prove the following:

(1) Each automorphism $\sigma \in \mathcal{G}_m$ restrict to an automorphism σ_k of C_m.

(2) Each automorphism $\sigma_k \in C_m$ extends to at most one automorphism $\sigma \in G_m$.

(3) Each automorphism $\sigma_k \in C_m$ extends to at least one automorphism $\sigma \in G_m$.

(4) Each automorphism $\sigma_k \in C_m$ extends to exactly one automorphism $\sigma \in G_m$.

Proof of (1) is easy. Let σ automorphism of $\mathbb{A}_m$

$$\sigma(\xi_m)^m = \sigma(\xi_m^m) = \sigma(1) = 1$$

$$\therefore \sigma C_m \subset C_m$$

Since σ is bijective,

$$\sigma C_m = C_m$$

hence $\sigma | C_m \in Aut C_m$.

Proof of (2) is easy too. Suppose $\sigma \in Aut\mathbb{A}_m$ and $\sigma | C_m = \sigma_k$ by theorem 142, let $\alpha \in \mathbb{A}_m$

$$\begin{aligned} \alpha &= f(\xi_m) \text{ for some } f \in \mathbb{Z}[x] \\ &= a_0\xi_m^n + a_1\xi_m^{n-1} + ... + a_n \end{aligned}$$

then

$$\sigma(\alpha) = a_0\xi_m^{kn} + a_1\xi_m^{k(n-1)} + ... + a_n = f(\xi_m^k)$$

so σ extends σ_k via $\sigma f(\xi_m) = f(\xi_m^k)$.

The hard part is to prove (3), then combining (2), (3) gives (4). So the ultimate goal of the next section is to prove that each $\sigma_k \in Aut C_m$ does extend uniquely to an element of $Aut\mathcal{G}_m$. The key tool is an important result from the 1800's.

Theorem 148. *(Irreducibility of the Cyclotomic Polynomial) For each $m \in \mathbb{N}$, the cyclotomic polynomial*

$$\Phi_m(z) = \prod_{ord\,\xi = m} (z - \xi) = z^{\varphi(n)} + \textit{lower degree terms}$$

which has all coefficients in $\mathbb{Z}$, is irreducible over $\mathbb{Q}$, i.e.,

$$\textit{If } \Phi_m = fg \textit{ with } f, g \in \mathbb{Z}[z], \textit{ then } f \textit{ or } g \textit{ is } \pm 1$$

For $m = p$ this was proved by Gauss in 1808. For general m, it's proved by Kronecker (1854), Dedekind (1857), Mertens, Landau, Schur, Artin,... We will give Schur's proof.

The fact that each $\Phi_m \in \mathbb{Z}[x]$ is easy, by induction on m. For $m = 1$, $\Phi_1 = z - 1$. So it is true. For $m > 1$, we use $\prod_{d|m} \Phi_d = z^m - 1$. By induction we may suppose that each $\Phi_m \in \mathbb{Z}[x]$ for $d < m$, so

$$\Phi_m = \frac{z^m - 1}{\prod_{d|m, d<m} \Phi_d}$$

is a quotient of monic polynomials in $\mathbb{Z}[x]$. By long division of polynomials, i.e. if f, g, h are polynomials with $fg = h$ and f monic, and $f, h \in \mathbb{Z}[x]$, then $g \in \mathbb{Z}[x]$. (we'll prove this next lecture), therefore

$$\Phi_m \in \mathbb{Z}[x]$$

Exercise 149. Prove: $\alpha, \beta, \gamma, \alpha_1, ... \in \mathbb{A}_m$,

(0) $\beta|\alpha$, $\gamma|\beta \implies \gamma|\alpha$.

(1) $\beta|\alpha_1$, $\beta|\alpha_2 \implies \beta|\alpha_1 + \alpha_2$; $\beta|\alpha$, $\delta \in \mathbb{A}_m \implies \beta|\delta\alpha$.

(2) $\alpha \equiv \alpha \, mod \, \beta$; $\alpha_1 \equiv \alpha_2 \, mod \, \beta \implies \alpha_2 \equiv \alpha_1 \, mod \, \beta$; $\alpha_1 \equiv \alpha_2, \alpha_2 \equiv \alpha_3 \implies \alpha_1 \equiv \alpha_3$.

Lemma 150. *For prime p,*

(1) $(\alpha + \beta)^p \equiv \alpha^p + \beta^p \, mod \, p$ for $\alpha, \beta \in \mathbb{A}_m$

(2) $c^p \equiv c \, mod \, p$ for $c \in \mathbb{Z}$.

Proof. By the Binomial theorem

$$(\alpha + \beta)^p = \sum_{j=0}^{p} \left(\begin{array}{c} p \\ j \end{array} \right) \alpha^j \beta^{p-j}$$

gives (1) since $\left(\begin{array}{c} p \\ j \end{array} \right) = \frac{p!}{j!(p-j)!}$ is a positive integer divisible by p for $j = 1, ..., p-1$.

For $c \in \mathbb{N}$, induction on c gives

$$c^p \quad = \quad [(c-1) + 1]^p \equiv (c-1)^p + 1 \equiv c - 1 + 1 \equiv c \, mod \, p$$

also $0^p = 0 \equiv 0 \, mod \, p$.

For $-c \in \mathbb{N}$ and $p \neq 2$, so p odd,

$$c^p = -(-c)^p \equiv -(-c) = c$$

For all $c \in \mathbb{Z}$, $c(c-1)$ is even, hence

$$c^2 \equiv c \, mod \, 2$$

□

Now we do Schur's proof of theorem 148.

Proof. Suppose $\Phi_m = fg$ with $f, g \in \mathbb{Z}[z]$, say

$$f = c_0 z^r + ... \text{ and } g = d_0 z^s + ...$$

Since Φ is monic, we have $c_0 d_0 = 1$. So we may suppose $c_0 = d_0 = 1$ (after perhaps multiplying f, g by -1)

Each root of Φ_m is a root of f or g but not both, and each root of f or g is a root of Φ_m. We may suppose $f(\xi_m) = 0$. Let S be the set of all roots of f. It suffices to show that

$$\xi \in S \implies \xi^p \in S \tag{4.22}$$

for each prime p with $p \nmid m$.

In fact, assuming (4.22), let $(k, m) = 1$, then $k = p_1 \cdot ... \cdot p_t$ with each $p_j \nmid m$, so by (4.22)

$$S \ni \xi_m \implies S \ni \xi_m^{p_1} \implies S \ni \xi_m^{p_1 p_2} \implies ... \implies S \ni \xi_m^k$$

Thus each primitive mth root of unity is a root of f, so $g = 1$, $f = \Phi_m$.

It remains to prove (4.22). Since $f(\xi) = 0$, i.e.

$$\xi^r + c_1 \xi^{r-1} + ... + c_r = 0$$

for some $c_1, ..., c_r \in \mathbb{Z}$, lemma 150 gives

$$\xi^{pr} + c_1 \xi^{p(r-1)} + ... + c_r \equiv 0 \, mod \, p$$

i.e.

$$p | f(\xi^p) \tag{4.23}$$

We have $f(\xi^p) = \prod_{\xi' \in S}(\xi^p - \xi')$, so assuming $\xi^p \notin S$,

$$f(\xi^p) \mid \prod_{\substack{\xi' \in C_m \\ \xi' \neq \xi^p}} (\xi^p - \xi') \tag{4.24}$$

Finally, differentiating $z^m - 1 = \prod_{\xi' \in C_m}(z - \xi')$ gives

$$mz^{m-1} = \sum_{\xi'' \in C_m} \prod_{\substack{\xi' \in C_m \\ \xi' \neq \xi''}} (z - \xi')$$

Since $\xi^p \in C_m$, this reduces to

$$m\xi^{p(m-1)} = \prod_{\substack{\xi' \in C_m \\ \xi' \neq \xi^p}} (\xi^p - \xi')$$

Showing

$$\prod_{\substack{\xi' \in C_m \\ \xi' \neq \xi^p}} (\xi^p - \xi') | m \tag{4.25}$$

combining (4.23), (4.24), and (4.25) shows that $p|m$, a contradiction. Therefore

$$\xi^p \in S.$$

□

Lecture 12 (3/11/13)

Lemma 151. *(long division)*

(a) For $f, g \in \mathbb{Q}[x]$ with f monic, there are $q, r \in \mathbb{Q}[x]$ so that

$$g = qf + r, \text{ with either } r = 0 \text{ or } \deg r < \deg f$$

(b) If in (a) both g and $f \in \mathbb{Z}[x]$, then both $q, r \in \mathbb{Z}[x]$.

Proof. If $g = 0$, put $q = 0$ and $r = 0$.

If $g \neq 0$ and $\deg g < \deg f$, put $q = 0$ and $r = g$.

If $g \neq 0$ and $\deg g \geq \deg f$, let

$$f = a_0 + a_1 z + ... + a_n z^n \quad g = b_0 + b_1 z + ... + b_m z^m$$

with $m \geq n$, $a_n = 1$, $b_m \neq 0$. Observe that $b_m x^{m-n} f$ and g have the same degree and the same top coefficient b_m. Put

$$\tilde{g} = g - b_m x^{m-n} f \tag{4.26}$$

then either $\tilde{g} = 0$ or $\deg \tilde{g} < m$. In the first case we are done, with $q = b_m x^{m-n}$ and $r = 0$. In the second case by induction on m, there are $\tilde{q}$ and $r \in \mathbb{Q}[z]$ so that

$$\tilde{g} = \tilde{q} f + r \tag{4.27}$$

with either $r = 0$ or $\deg r < \deg f$.

By (4.26), (4.27)

$$g = (\tilde{q} + b_m x^{m-n}) f + r = qf + r$$

with either $r = 0$ or $\deg r < \deg f$. □

Exercise 152. Prove (b) and observe how little changes in the proof of (b).

Lemma 153. *Let $m \in \mathbb{N}$*

(1) Φ_m is a polynomial in $\mathbb{Q}[z]$ of least degree with $\Phi_m(\xi_m) = 0$

(2) If $g \in \mathbb{Z}[z]$ and $g(\xi_m) = 0$, then $g = q\Phi_m$ for some $q \in \mathbb{Z}[z]$.

Proof. (1) $f \in \mathbb{Q}[z]$ be monic of minimal degree with $f(\xi_m) = 0$. By the previous lemma,

$$\Phi_m = qf + r$$

with $q, r \in \mathbb{Q}[z]$ and $r = 0$ or $\deg r < \deg f$.

Since both $\Phi_m(\xi_m) = 0$ and $f(\xi_m) = 0$, we have $r(\xi_m) = 0$. If $r \neq 0$, then cr is monic for some $c \in \mathbb{Q}$ and $(cr)(\xi_m) = 0$ contrary to minimality. Thus $r = 0$, so $\Phi_m = qf$. From

$$\Phi_m(z) = \prod_{ord\, \xi = m} (z - \xi)$$

we have

$$f(z) = \prod_{\xi \in S} (z - \xi) \quad q(z) = \prod_{\xi \in T} (z - \xi)$$

where S, T are disjoint subsets of $\{ord\, \xi = m\}$with $S \cup T = \{ord\, \xi = m\}$, both f, q have coefficients in $\mathbb{A} \cap \mathbb{Q} = \mathbb{Z}$ and are monic. Since Φ_m is irreducible in $\mathbb{Z}[z]$ and $\deg f \geq 1$ we conclude that $q = 1$, $f = \Phi_m$.

(2) Now let $g \in \mathbb{Q}[z]$ with $g(\xi_m) = 0$ By the previous lemma,

$$g = q\Phi_m + r$$

with $q, r \in \mathbb{Q}[z]$ and $r = 0$ or $\deg r < \deg \Phi_m$. Since both $g(\xi_m) = 0$ and $\Phi_m(\xi_m) = 0$, we get $r(\xi_m) = 0$. As before we conclude by minimality that $r = 0$, so $g = q\Phi_m$. Since $g, \Phi_m \in Z[z]$, and Φ_m is monic, it follows from the previous lemma(b) that $q \in \mathbb{Z}[z]$. □

Theorem 154. *For $m \in \mathbb{N}$, $k \in \mathbb{Z}$ with $(k, m) = 1$, the automorphism σ_k of C_m extends uniquely to an automorphism, also denoted σ_k of $\mathbb{A}_m$ with*

$$\sigma_k f(\xi_m) = f(\xi_m^k) \tag{4.28}$$

for $f \in \mathbb{Z}[z]$.

Proof. The definition (4.28) seems at first ambiguous, since a given $\alpha \in \mathbb{A}_m$ does not uniquely determine $f \in \mathbb{Z}[x]$ with $\alpha = f(\xi_m)$. However if $f_1, f_2 \in \mathbb{Z}[x]$ and $f_1(\xi_m) = f_2(\xi_m)$, then $g = f_1 - f_2$ satisfies $g(\xi_m) = 0$. So by the previous lemma

$$g = q\Phi_m$$

for some $q \in \mathbb{Z}[x]$, so for $(k, m) = 1$, since $\Phi_m(\xi_m^k) = 0$, we have

$$f_1(\xi_m^k) - f_2(\xi_m^k) = g(\xi_m^k)\Phi_m(\xi_m^k) = 0$$

i.e.

$$f_1(\xi_m^k) = f_2(\xi_m^k)$$

Thus the map $\sigma_k : \mathbb{A}_m \to \mathbb{A}_m$ is well defined by (4.28).

For $\alpha, \beta \in \mathbb{A}_m$, choose any $f, g \in \mathbb{Z}[z]$ with $\alpha = f(\xi_m)$, $\beta = g(\xi_m)$, then

$$\sigma_k(\alpha+\beta) = \sigma_k((f+g)(\xi_m)) = (f+g)(\xi_m^k) = f(\xi_m^k)+g(\xi_m^k) = \sigma_k(\alpha)+\sigma_k(\beta)$$

and

$$\sigma_k(\alpha\beta) = \sigma_k((fg)(\xi_m)) = (fg)(\xi_m^k) = f(\xi_m^k)g(\xi_m^k) = \sigma_k(\alpha)\sigma_k(\beta)$$

Thus each σ_k satisfies (i) and (ii) in the definition (146).

For $(k_1, m) = 1$ and $(k_2, m) = 1$, we have $(k_1k_2, m) = 1$ and

$$\sigma_{k_1}\sigma_{k_2}(\alpha) = \sigma_{k_1}(f(\xi_m^{k_2})) = f(\xi_m^{k_1k_2}) = \sigma_{k_1k_2}(\alpha) \tag{4.29}$$

For $k \equiv 1 \, mod \, m$, we have $\sigma_k(\alpha) = \alpha$ for all $\alpha \in \mathbb{A}_m$ since $\xi_m^k = \xi_m$.

It follows that

$$\sigma_{k_1} \circ \sigma_{k_2} = id_{\mathbb{A}_m} \text{ for } k_1 k_2 \equiv 1 \, mod \, m$$

Using the above equation, it follows that each σ_k with $(k, m) = 1$ is both injective and surjective, hence bijective, hence an automorphism of $\mathbb{A}_m$. □

Exercise 155. Prove (4.29) and the last statement in the proof above.

Remark 156. It follows from the definition (4.28), with $f = a \in \mathbb{Z} \subset \mathbb{Z}[x]$, that

$$\sigma_k(a) = a \text{ for } a \in \mathbb{Z} \text{ and } (k, m) = 1$$

vice verse:

If $\alpha \in \mathbb{A}_m$ and $\sigma_k(\alpha) = \alpha$ for all $k \in \mathbb{Z}$ with $(k, m) = 1$, then $\alpha \in \mathbb{Z}$. This follows from Galois theory.

5 Galois Group and its Applications to Characters

We now formally study Galois group.

5.1 Actions of $\mathcal{G}_m$ on $\hat{G}$ and $\check{G}$

In what follows we will identify the group

$$\mathcal{G}_m = (\mathbb{Z}/m\mathbb{Z})^*$$

with

$$Aut\mathbb{A}_m$$

and for $(k, m) = 1$ write (k) for $k + m\mathbb{Z} \in \mathcal{G}_m$.

Notation 157. For $\sigma = \sigma_k \in \mathcal{G}_m$ and $\alpha \in \mathbb{A}_m$ we write $\alpha^{(k)}$ for $\sigma_k(\alpha)$.

In this notation, operation in the previous proof become

$$(\alpha + \beta)^{(k)} = \alpha^{(k)} + \beta^{(k)}; \; (\alpha\beta)^{(k)} = \alpha^{(k)}\beta^{(k)}; \; a^{(k)} = a \text{ for } a \in \mathbb{Z}$$

and if $\alpha = f(\xi_m)$, then $\alpha^{(k)} = f(\xi_m^k)$. And $\xi^{(k)} = \xi^k \iff \xi \in C_m$.

Theorem 158. *For each finite group G and each $m \in \mathbb{N}$ divisible by the exponent of G, (the exponent of G is the least common multiple of orders of the elements of G), $\mathcal{G}_m$ acts on the four sets $\mathbb{A}_m$, G, $\check{G}$, and $\hat{G}$ as follows: for $(k) \in \mathcal{G}_m$,*

(1) $\alpha^{(k)}$ is defined as in theorem 154, i.e. $f(\xi)^{(k)} = f(\xi^{(k)})$

(2) $g^{(k)} = g^k$ for $g \in G$ and $(k) \in \mathcal{G}_m$

(3) $A^{(k)} = \{a^k : a \in A\}$ for $A \in \check{G}$

(4) $\chi^{(k)}(g) = \chi(g)^{(k)}$ for $\chi \in \hat{G}$, $g \in G$

These actions are related by

(5) $\chi^{(k)}(g) = \chi(g^k)$ for $\chi \in \hat{G}$, $g \in G$

We will prove parts of the theorem, and the rests are exercises.

Proposition 159. *Prove that $\chi^{(k)} \in \hat{G}$ for $\chi \in \hat{G}$ and $(k) \in \mathcal{G}_m$.*

We will need the following result

Exercise 160. Prove that $\bar{\alpha}^{(k)} = \overline{\alpha^{(k)}}$ for all $\alpha \in \mathbb{A}_m$, $(k) \in \mathcal{G}_m$. Hint $\bar{\alpha} = \alpha^{(-1)}$, and $\mathcal{G}_m$ is abelian.

Proof. (proposition 159) By theorem 92,

$$|G|\chi(g_1)\chi(g) = d_\chi \sum_{h \in G} \chi(g_1 g^h)$$

for all $g_1, g \in G$, $\chi \in \hat{G}$.

Apply (k) to this equation, using the fact that (k) commutes with sums and products of elements of $\mathbb{A}_m$ and fixes each element of $\mathbb{Z}$:

$$|G|\chi(g_1)^{(k)}\chi(g)^{(k)} = d_\chi \sum_{h \in G} (\chi(g_1 g^h))^k$$

i.e.

$$|G|\chi^{(k)}(g_1)\chi^{(k)}(g) = d_\chi \sum_{h \in G} \chi^{(k)}(g_1 g^h)$$

Thus $\theta = \chi^{(k)}/d_\chi$ satisfies the hypothesis of theorem 100, so

$$\chi^{(k)}/d_\chi = \chi'/d_{\chi'} \tag{5.1}$$

for some $\chi' \in \hat{G}$, depending on χ and (k).

Using exercise 160, it follows that

$$\sum_{g\in G}\chi^{(k)}(g)\overline{\chi^{(k)}(g)}=\left(\sum_{g\in G}\chi(g)\bar{\chi}(g)\right)^{(k)}=|G|^{(k)}=|G|$$

i.e. $\left\langle\chi^{(k)},\chi^{(k)}\right\rangle=1$, which with $\langle\chi',\chi'\rangle=1$ and (5.1) gives $(d_\chi/d_{\chi'})^2=1$, so $d_\chi=\pm d_{\chi'}$. Since d_χ,$d_{\chi'}\in\mathbb{N}$, we get $d_\chi=d_{\chi'}$ so $\chi^{(k)}=\chi'$, proving $\chi^{(k)}\in\hat{G}$. □

We now prove (5) in the theorem 158.

Proposition 161. *Prove that $\chi(a)^{(k)}=\chi(a^k)$ for $\chi\in\hat{G}$, $a\in G$ and $(k)\in\mathcal{G}_m$.*

Proof. Let C be the cyclic subgroup generated by a. Then

$$\chi|C=\sum_{j=1}^{d}\xi_j$$

for certain $\xi_j\in\hat{C}$, so

$$(\chi(a))^{(k)}=\sum_{j=1}^{d}\xi_j(a)^{(k)}=\sum_{j=1}^{d}\xi_j(a)^k=\sum_{j=1}^{d}\xi_j(a^k)=\chi(a^k)$$

□

Exercise 162. Complete the proof of theorem 158, hence we now have well-defined actions of $\mathcal{G}_m$.

Theorem 163. *(Burnside) For each finite group G of exponent dividing m, each $(k)\in\mathcal{G}_m$, and each $A,B,C\in\check{G}$, we have*

$$m_{AB}^{C}=m_{A'B'}^{C'}$$

with $A'=A^{(k)}$, $B'=B^{(k)}$, $C=C^{(k)}$.

Proof. By theorem 119,

$$|G||C|m_{AB}^{C}=\sum_{\chi\in\hat{G}}d_\chi^2w_\chi(A)w_\chi(B)\bar{w}_\chi(C)$$

applying (k) to this gives

$$\begin{aligned} |G||C|m_{AB}^{C} &= \sum_{\chi\in\hat{G}} d_\chi^2 w_\chi(A)^{(k)} w_\chi(B)^{(k)} \bar{w}_\chi(C)^{(k)} \\ &= \sum_{\chi\in\hat{G}} d_\chi^2 w_\chi(A') w_\chi(B') \bar{w}_\chi(C') \\ &= |G||C'|m_{A'B'}^{C'} \end{aligned}$$

Since $|C'| = |C|$, this proves the theorem. □

Corollary 164. *For each finite group G with exponent dividing m, and $(k,m) = 1$ and each $a, b \in G$ there are elements $a_1, b_1 \in G$ with a_1 conjugate to a and b_1 conjugate to b so that*

$$(ab)^k = a_1^k b_1^k$$

i.e. raising to the kth power is a homomorphism up to conjugacy.

Proof. Let A, B, C be the conjugacy classes of a, b, $c = ab$. Then $m_{AB}^{C} > 0$, so $m_{A^{(k)}B^{(k)}}^{C^{(k)}} > 0$, so

$$c^k = a_1^k b_1^k$$

for some $a_1 \in A$ and $b_1 \in B$. □

Remark 165. This corollary has apparently never been proved without characters. There are some elementary cases, e.g. $k \equiv 1 \, mod \, m$ and $k \equiv -1 \, mod \, m$, the second one since

$$(ab)^{-1} = b^{-1}a^{-1} = (b^{-1}ab)^{-1}b^{-1} = a_1^{-1}b_1^{-1}$$

But e.g. for $m = 5$ and $k = 2$, there seems to be no elementary proof that

$$(ab)^2 = a_1^2 b_1^2$$

for some a_1 conjugate to a, b_1 conjugate to b in every finite group of exponent 5.

5.2 Zeros of Characters

Lecture 13 (3/13/13)

Definition 166. For each $m \in \mathbb{N}$ and $\alpha \in \mathbb{A}_m$, the *norm* of α, denoted $N_m(\alpha)$, is defined by

$$N_m(\alpha) = \prod_{(k)\in\mathcal{G}_m} \alpha^{(k)}$$

For example, $\alpha = 3 - \xi_5 \in \mathbb{A}_5$,

$$N_5(\alpha) \;=\; \prod_{k=1}^{4}(3-\xi_5^k) = \Phi_5(3) = 3^4+3^3+3^2+3+1 = 121$$

Theorem 167. *For each $m \in \mathbb{N}$ and $\alpha, \beta \in \mathbb{A}_m$*

(a) $N_m(\alpha\beta) = N_m(\alpha)N_m(\beta)$

(b) $N_m(\alpha) = 0 \iff \alpha = 0$

(c) $N_m(\alpha) \in \mathbb{Z}$

Proof. (a)

$$\begin{aligned} N_m(\alpha\beta) &= \prod_{(k)\in\mathcal{G}_m} (\alpha\beta)^{(k)} = \prod_{(k)\in\mathcal{G}_m} \alpha^{(k)}\beta^{(k)} \\ &= \prod_{(k)\in\mathcal{G}_m} \alpha^{(k)} \prod_{(k)\in\mathcal{G}_m} \beta^{(k)} = N_m(\alpha)N_m(\beta) \end{aligned}$$

(b) If $\alpha = 0$, then each $\alpha^{(k)} = 0$ so $N_m(\alpha) = 0$. If $N_m(\alpha) = 0$, then some $\alpha^{(k)} = 0$, so $\alpha = 0$, since $\alpha \mapsto \alpha^{(k)}$ is injective.

(c) This is can be proved easily from Galois theory, that $\alpha \in \mathbb{A}_m$ and $\alpha^{(k)} = \alpha$ for all $(k) \in \mathcal{G}_m$ implies $\alpha \in \mathbb{Q}$, we could complete the proof simply as follows.

Put $\beta = N_m(\alpha)$, then for $(l) \in \mathcal{G}_m$,

$$\beta^{(l)} = \left(\prod_{(k)\in\mathcal{G}_m} \alpha^{(k)}\right)^{(l)} = \prod_{(k)\in\mathcal{G}_m} \alpha^{(l)(k)} = \prod_{(j)\in\mathcal{G}_m} \alpha^{(j)} = \beta$$

The third equality follows from $\alpha^{(l)(k)} = \alpha^{(lk)}$ the composition, and $(k,m) = 1, (l,m) = 1 \implies (j,m) = 1$.

So $\beta \in \mathbb{Q}$. Since also $\beta \in \mathbb{A}_m$, we conclude that $N_m(\alpha) = \beta \in \mathbb{A}_m \cap \mathbb{Q} = \mathbb{Z}$. □

But since we don't assume people know Galois theory, we will show (c) in another way. First show for $\alpha \in \mathbb{A}_m$, $\alpha^{(k)} \in \mathbb{A}_m$, so $N_m(a) \in \mathbb{A}_m$. Then we need to show N_m maps to $\mathbb{Q}$.

Theorem 168. *For $f, g \in \mathbb{Q}[z]$, with neither $\equiv 0$*

$$\prod_{g(\beta)=0} f(\beta) \in \mathbb{Q}$$

In the product above, factors corresponding to multiple roots of g are repeated, with the corresponding multiplicity. If g is non zero constant, interpret the product as 1.

Proof. (complete proof of theorem 167(3)) Assuming theorem 168, let $\alpha = f(\xi_m)$ with $f \in \mathbb{Z}[z] \subset \mathbb{Q}[z]$. Then

$$N_m(\alpha) = \prod_{(k)\in\mathcal{G}_m} \alpha^{(k)} = \prod_{\substack{k=1 \\ (k,m)=1}}^{m} f(\xi_m^k) = \prod_{\Phi_m(\xi)=0} f(\xi) \in \mathbb{Q}$$

□

Lemma 169. *For $f, g \in \mathbb{Q}[z]$, neither $\equiv 0$, with leading coefficients a_0 and b_0 and degrees m, n*

$$b_0^m \prod_{g(\beta)=0} f(\beta) = (-1)^{mn} a_0^n \prod_{f(\alpha)=0} g(\alpha) \tag{5.2}$$

Interpret the product in the same way as in theorem 168.

Proof. If $m = 0$, then $f = a_0$ and f has no roots so (5.2) is clear. Similarly if $n = 0$.

For $m > 0$ and $n > 0$,

$$f(z) = a_0 z^m + ... + a_m = a_0 \prod_{i=1}^{m} (z - \alpha_i) \tag{5.3}$$

and

$$g(z) = b_0 z^n + ... + b_n = b_0 \prod_{j=1}^{n} (z - \beta_j) \tag{5.4}$$

Also

$$\prod_{j=1}^{n} \prod_{i=1}^{m} (\beta_j - \alpha_i) = (-1)^{mn} \prod_{i=1}^{m} \prod_{j=1}^{n} (\alpha_i - \beta_j)$$

Multiplying the above equation by $a_0^n b_0^m$ and using (5.3), (5.4) gives (5.2). □

Now prove theorem 168.

Proof. By lemma 169, we have

$$\prod_{g(\beta)=0} f(\beta) \in \mathbb{Q} \iff \prod_{f(\alpha)=0} g(\alpha) \in \mathbb{Q}$$

so after possibly interchanging f and g, we may suppose $n \leq m$

By lemma 151, there are $q, r \in \mathbb{Q}[z]$ with

$$f = qg + r$$

and either $r \equiv 0$ or $l = \deg r < \deg g = n$.

It follows that

$$\prod_{g(\beta)=0} f(\beta) = \prod_{g(\beta)=0} r(\beta)$$

If $r \equiv 0$, then the product on the right is $0 \in \mathbb{Q}$. If $r \not\equiv 0$, then $l < n \leq m$, so $l + n < m + n$, so by induction on $m + n$ the product on the right is in $\mathbb{Q}$. □

Lemma 170. *(Inequality between arithmetic and geometric means) For $n \in \mathbb{N}$ and $x_1, ..., x_n \geq 0$,*

$$(x_1 \cdot ... \cdot x_n)^{\frac{1}{n}} \leq \frac{1}{n}(x_1 + ... + x_n) \tag{5.5}$$

Proof. For $n = 1$, this is clear. For $n = 2$, it follows from

$$x_1 + x_2 - 2\sqrt{x_1 x_2} = (\sqrt{x_1} - \sqrt{x_2})^2 \geq 0$$

Assuming (5.5) is true for n, then it is true for $m = 2n$, since

$$\begin{aligned}(x_1 \cdot ... \cdot x_m)^{\frac{1}{m}} &= (\sqrt{x_1 \cdot ... \cdot x_m})^{\frac{1}{n}} \\ &\leq \frac{1}{n}(\sqrt{x_1 x_2} + ... + \sqrt{x_{m-1} x_m}) \leq \frac{1}{n}(\frac{x_1 + x_2}{2} + ... + \frac{x_{m-1} + x_m}{2})\end{aligned}$$

Thus (5.5) is true for $n = 2^r$, for each $r \in \mathbb{N}$.

For arbitrary $n \in \mathbb{N}$, choose $N = 2^r$ with $r \in \mathbb{N}$, so that $N > n$. Put

$$x_k = x \text{ for } n < k \leq N,$$

with $x = \frac{1}{n}(x_1 + ... + x_n)$

By the N case, we have

$$(x_1 \cdot ... \cdot x_N)^{\frac{1}{N}} \leq \frac{1}{N}(x_1 + ... + x_N)$$

i.e. $LHS = (x_1 \cdot ... \cdot x_n \cdot x \cdot ... \cdot x)^{\frac{1}{N}} = (x_1 \cdot ... \cdot x_n)^{\frac{1}{N}} x^{1-\frac{n}{N}}$; $RHS = \frac{1}{N}(nx + (N-n)x) = x$, from which (5.5) follows. □

Theorem 171. *For each $\alpha \in \mathbb{A}_m$ with $\alpha \neq 0$,*

$$\frac{1}{|\mathcal{G}_m|} \sum_{(k)\in\mathcal{G}_m} \left|\alpha^{(k)}\right|^2 \geq 1$$

Proof. By the previous lemma and theorem (167)(b&c)

$$\frac{1}{|\mathcal{G}_m|} \sum_{(k)\in\mathcal{G}_m} \left|\alpha^{(k)}\right|^2 \geq |N_m(\alpha)|^{\frac{2}{|\mathcal{G}_m|}} \geq 1$$

□

Theorem 172. *(Burnside) Each $\chi \in \hat{G}$ with $d_\chi > 1$ has at least one zero.*

Proof. Apply $(k) \in \mathcal{G}_m$ with $m = |G|$ to

$$\sum_{g\in G} |\chi(g)|^2 = |G| \tag{5.6}$$

and get

$$\sum_{g\in G} \left|\chi(g)^{(k)}\right|^2 = |G| \tag{5.7}$$

In more detail, since $\bar{\alpha} = \alpha^{(-1)}$ for $\alpha \in \mathbb{A}_g$ and $(-1)(k) = (-k) = (k)(-1)$, we have

$$|\chi(g)|^{2^{(k)}} = (\chi(g)\bar{\chi}(g))^{(k)} = \chi(g)^{(k)}\overline{\chi(g)^{(k)}} = \left|\chi(g)^{(k)}\right|^2$$

so (5.7) follows from (5.6), since (k) commutes with addition and fixes $|G|$.

Averaging (5.7) over all $(k) \in \mathcal{G}_m$ and interchanging summation signs gives

$$\sum_{g\in G} \frac{1}{|\mathcal{G}_m|} \sum_{(k)\in\mathcal{G}_m} \left|\chi(g)^{(k)}\right|^2 = |G|$$

If χ has no zeros, then for each $g \in G$ the average is ≥ 1, by the previous theorem, so each of these averages must be 1. Since $\chi(1) = d_\chi$, this forces $d_\chi = 1$. □

The theorem doesn't tell us where the zeros are. For example S_3, the theorem only infers that there is zero for $d_\chi = 2$ row.

S_3	1	R	T
1	1	1	1
ε	1	1	-1
χ	2	-1	0

Here is a dual problem: why R has no zero? One can see that R has no central elements.

Exercise 173. One can go back the proof and modify the proof to see why we are unable to use from

$$\sum_{\chi \in \hat{G}} |\chi(g)|^2 = |C_G(g)|$$

to get that each $g \notin Z(G)$ is a zero for some $\chi \in \hat{G}$, since, e.g. no $\chi \in \hat{S}_3$ has a zero at $(123) \in R$.

Definition 174. For each group G the commutator group G' is the subgroup of G generated by all commutators

$$[g, h] = ghg^{-1}h^{-1}$$

Exercise 175. Prove that (a) G' is a normal subgroup of G; (b) G/G' is abelian; (c) $G' \subset N$ for each normal subgroup N of G for which G/N is abelian.

Exercise 176. Prove that for $\chi \in \hat{G}$,

$$d_\chi = 1 \iff \chi \in \widehat{G/G'}$$

more precisely $\chi = \tilde{w}$ for some $w \in \widehat{G/G'}$.

Theorem 177. *(Brauer, Wielandt 1954) Let G be a finite group, $g \in G$, and let $A_1, ..., A_k$ be all the conjugacy classes in G, in any order. Then the number, $n(g)$, of $k-$tuples $g_1, ..., g_k$ with $g_1 \in A_1, ..., g_k \in A_k$ so that $g_1 \cdot ... \cdot g_k = g$ is 0 unless g is in a certain coset g^*G' of G', in which case this number is*

$$n(g) = |A_1| \cdot ... \cdot |A_k|/|G'|$$

Corollary 178. *For each finite group G with conjugacy classes $A_1, ..., A_k$,*

$$|G'| \text{ divides } |A_1| \cdot ... \cdot |A_k|$$

The proof of theorem 177 has never been given without characters.

Proof. Since $\chi_{reg} = 0$ except at 1 and $|G|$ at 1, the number we seek is by theorem 95,

$$n(g) = \frac{1}{|G|} \sum_{g_1 \in A_1} ... \sum_{g_k \in A_k} \chi_{reg}(g_1 ... g_k g^{-1}) = \sum_{\chi \in \hat{G}} \frac{d_\chi}{|G|} \sum_{g_1 \in A_1} ... \sum_{g_k \in A_k} \chi(g_1 ... g_k g^{-1}) \tag{5.8}$$

Pick $a_1 \in A_1, ..., a_k \in A_k$, the inner k-fold sum on the right is

$$\frac{1}{|C_G(a_1)| \cdot ... \cdot |C_G(a_k)|} \sum_{h_1 \in G} ... \sum_{h_k \in G} \chi(a_1^{h_1} ... a_k^{h_k} g^{-1}) \tag{5.9}$$

Using the functional equation of $\chi \in \hat{G}$ in the form

$$\sum_{h \in G} \chi(a^h g) = \frac{|G|}{d_\chi} \chi(a)\chi(g)$$

the k-fold sum in (5.9) reduces to

$$\left(\frac{|G|}{d_\chi}\right)^k \chi(a_1)...\chi(a_k)\bar{\chi}(g) = \begin{cases} 0 & d_\chi > 1 \text{ by theorem 172} \\ |G|^k \chi(a_1 ... a_k g^{-1}) & d_\chi = 1 \end{cases}$$

Thus by exercise 176 the right side of (5.8) simplifies to

$$\frac{|G|^{k-1}}{|C_G(a_1)|...|C_G(a_k)|} \sum_{\chi \in \widehat{G/G'}} \chi(g^* g^{-1}) = \begin{cases} \frac{|A_1|...|A_k|}{|G'|} & g \in g^* G' \\ 0 & \text{otherwise} \end{cases}$$

where $g^* = a_1 ... a_k$, and $\sum_{\chi \in \widehat{G/G'}} \chi(g^* g^{-1})$ is the regular character of G/G'. □

Lecture 14 (3/25/13)

Notation 179. For $\chi \in \hat{G}$, the codegree

$$c_\chi = \frac{|G|}{d_\chi}$$

All proof to date that $c_\chi \in \mathbb{N}$ use algebraic integers. Similarly with the following:

Theorem 180. *(Braner-Nesbitt, 1941) Let $\chi \in \hat{G}$ and let p be a prime with $p \nmid c_\chi$. Then $\chi(g) = 0$ for each element g with order divisible by p.*

Example 181. Let χ be the irreducible character of degree 2 of S_3. Here $c_\chi = 6/2 = 3$ and $\chi(g) = 0$ for each transposition g, i.e. each element of order 2 in G.

The original proof of theorem 180 can be found in Isaacs's book, he uses characterization of character theory and Brauer's theorem of modulus. But we will follow a much elementary proof by Leitz in 2000.

Definition 182. For $\alpha, \delta \in \mathbb{A}$ we say δ divides α and write $\delta|\alpha$ if $\alpha = \delta\gamma$ for some $\gamma \in \mathbb{A}$.

Lemma 183. *For $\alpha \in \mathbb{A}$ and $c, d \in \mathbb{N}$, if $d|c\alpha$ and $(d, c) = 1$, then $d|\alpha$.*

Proof. From $(d, c) = 1$ we get $ud + vc = 1$ for some $u, v \in \mathbb{Z}$, so

$$\alpha = ud\alpha + vc\alpha$$

From $d|c\alpha$ we get $\gamma \in \mathbb{A}$ with

$$c\alpha = d\gamma$$

combining the two above gives

$$\alpha = d(u\alpha + v\gamma) = d\beta \text{ with } \beta \in \mathbb{A}$$

so $d|\alpha$. □

Lemma 184. *If $0 \neq \alpha \in \mathbb{A}$, then $d|\alpha$ for only finitely many $d \in \mathbb{N}$.*

Proof. Since $\alpha \in \mathbb{A}$, we have

$$\alpha^m + c_1\alpha^{m-1} + ... + c_m = 0 \tag{5.10}$$

for some $c_1, ..., c_m \in \mathbb{Z}$. Since $\alpha \neq 0$ we may suppose $c_m \neq 0$. If $c_m = 0$, cancel nonzero α from the equation. Repeat until constant term is $\neq 0$. If $d \in \mathbb{N}$ divides α, then d divides each term in (5.10) except c_m, so d divides c_m. □

Exercise 185. Use in the proof of lemma above. Prove

(1) If $d|\alpha$ and $d|\beta$, then $d|\alpha + \beta$.

(2) If $d|\alpha$ and $\gamma \in \mathbb{A}$, then $d|\alpha\gamma$.

(3) If each nonzero $c \in \mathbb{Z}$ has only finitely many divisors $d \in \mathbb{N}$.

Proof. (of theorem 180) Write the convolution identity as

$$c_\chi\chi(g) = \sum_{h_1h_2=g} \chi(h_1)\chi(h_2)$$

Multiply by c_χ and treat $c_\chi\chi(h_2)$ in the same way, giving

$$c_\chi^2\chi(g) = \sum_{h_1h_2h_3=g} \chi(h_1)\chi(h_2)\chi(h_3)$$

etc, giving for each integer $n > 1$

$$c_\chi^{n-1}\chi(g) = \sum_{h_1...h_n=g} \chi(h_1)...\chi(h_n)$$

Let A be the conjugacy class of g. Since χ is constant on A,

$$c_\chi^{n-1}\chi(g)|A| = \sum_{h_1...h_n\in A} \chi(h_1)...\chi(h_n) \tag{5.11}$$

We see that assuming

$$p \nmid c_\chi \text{ and } \chi(g) \neq 0 \tag{5.12}$$

the left side of (5.11) is divisible by p^b for only finitely many b, independently of n.

In fact if $p^b \mid c_\chi^{n-1}\chi(g)|A|$, then since $(p^b, c_\chi^{n-1}) = 1$, lemma 183 implies $p^b \mid \chi(g)|A|$. Since $0 \not\equiv \chi(g)|A| \in \mathbb{A}$, it can happen for only finitely many b, according to lemma 184.

Now for the right side of (5.11):

Let $C = \mathbb{Z}/n\mathbb{Z}$, a cyclic group of order n, and regard $\{1, ..., n\}$ as the corresponding residue classes mod n, i.e. elements of C. Since C acts on itself by left translation (additively), C also acts on $m(C, G)$

$$m(C, G) = \text{the set of all } n\text{-tuples } \underline{h} = (h_1, ..., h_n) \in G^n$$

In this action, C stabilizes

$$m_A(C, G) = \{\underline{h} \in m(C, G) : h_1...h_n \in A\}.$$

In fact, if $r \in C$ and $\underline{h} = (h_1, ..., h_n) \in m_A(C, G)$, then

$$(-r)\underline{h} = (h_{1+r}, ..., h_{n+r}),$$

and

$$h_{1+r}, ..., h_{n+r} = (h_1...h_r)^{-1}(h_1...h_n)(h_{n+1}...h_{n+r}) \in A$$

showing that $(-r)\underline{h} \in m_A(C, G)$.

Let $\underline{h} \in m_A(C,G)$ and let $C_{\underline{h}}$ be the corresponding stabilizer subgroup of C. Since C is cyclic of order n, $C_{\underline{h}}$ is cyclic of order d for some $d|n$, and is generated by the residue class of e mod n, where $de = n$. In particular

$$(-e)\underline{h} = \underline{h}, \text{ i.e. } h_{j+e} = h_j \ \forall\, j$$

so

$$h_1...h_n = (h_1...h_e)^d \tag{5.13}$$

Let p^a be the highest power of p dividing $|G|$. Then for no $h \in G$ is the order of h^{p^a} divisible by p. On the other hand, we are assuming that

$$\text{the order of } g \text{ is divisible by } p \tag{5.14}$$

and $h_1...h_n$ is conjugate to g, so the order of $h_1...h_n$ is divisible by p. It thus follows from (5.13) and (5.14) that

$$p^a \nmid d \tag{5.15}$$

Now choose $n = p^{a+b-1}$ with arbitrary $b \in \mathbb{N}$. Since $n = de$, it follows from (5.15) that

$$p^b \mid e \tag{5.16}$$

But e is the index of $C_{\underline{h}}$ in C, which is the size of the orbit of $\underline{h}$ in the action of C on $m_A(C,G)$. Also

$$\chi(h_1)...\chi(h_n) \text{ is constant on each orbit} \tag{5.17}$$

(Since the factors are just permuted when C acts on $m_A(C,G)$.)

Since the terms in the sum on the right in (5.11) are in $\mathbb{A}$, it follows from (5.16) and (5.17) that

$$p^b \mid \sum_{h_1...h_n \in A} \chi(h_1)...\chi(h_n)$$

for $n = p^{a+b-1}$ with $b \in \mathbb{N}$ arbitrary, contrary to the statement right after (5.12), thus (5.12) and (5.14) are inconsistent. □

6 Relations with Subgroups and Factor Groups

6.1 Restriction to and Induction from Subgroups

Lecture 15 (3/27/13)

Notation 186. $C(G)$ denotes the space of all complex valued class functions on G, i.e. $C(G) = m(G,\mathbb{C})^G$, where G acts on $m(G,\mathbb{C})$ by $\theta^g(g_1) = \theta(g^{-1}g, g)$.

For each subgroup H of G, and each $\theta \in C(G)$, we denote by θ_H the restriction of θ to H. Thus $\theta_H : H \to \mathbb{C}$ and $\theta_H(h) = \theta(h)$ for $h \in H$. Observe that $\theta \mapsto \theta_H$ is a linear map from $C(G)$ to $C(H)$.

For each subgroup H of G, and each $\psi \in C(H)$, we denote by $\dot{\psi}$ the complex function on G which agrees with ψ on H and is 0 off H. While $\dot{\psi}$ is in general not a class function on G, the induced function

$$\psi^G = \frac{1}{|H|} \sum_{g \in G} \dot{\psi}^g = \sum_{g \bmod H} \dot{\psi}^g \tag{6.1}$$

($g \bmod H$ means take one g from each left coset of H.) is a class function on G, and $\psi \mapsto \psi^G$ is a linear map from $C(H)$ to $C(G)$.

Exercise 187. Show that for each $\psi \in C(H)$, the function $\dot{\psi}$ is an H-class function on G, i.e.

$$\dot{\psi}(g_1^h) = \dot{\psi}(g_1)$$

for all $g_1 \in G$, $h \in H$.

Exercise 188. Using preceding exercise, justify the second equality in (6.1) by showing

$$\dot{\psi}^{gh} = \dot{\psi}^g$$

for $g \in G$, $h \in H$.

Theorem 189. *(Frobenius Reciprocity) For each subgroup $H \subset G$, $\psi \in C(H)$, $\theta \in C(G)$,*

$$\left\langle \psi^G, \theta \right\rangle_G = \langle \psi, \theta_H \rangle_H$$

Remark 190. perhaps the subscripts G and H on the scalar products are unnecessary given the four functions. In linear algebra language it says "induction is adjoint to restriction".

Proof. $\left\langle \dot{\psi}^g, \theta \right\rangle_G = \left\langle \dot{\psi}^g, \theta^g \right\rangle_G = \left\langle \dot{\psi}, \theta \right\rangle_G = \frac{1}{(G:H)} \langle \psi, \theta_H \rangle_H$, ... □

Exercise 191. Justify each step above and complete the proof.

Theorem 192. *Characters induce characters. More precisely, let*

$$\chi_H = \sum_{\psi \in \hat{H}} c_{\chi,\psi} \psi \text{ for } \chi \in \hat{G}$$

then

$$\psi^G = \sum_{\chi \in \hat{G}} c_{\chi,\psi} \chi \text{ for } \psi \in \hat{H} \tag{6.2}$$

Thus the same coefficients for induction as for restriction.

Proof. Equality of the two $c_{\chi,\psi}$'s come from Frobenius reciprocity:

$$\langle \chi_H, \psi \rangle_H = \langle \chi, \psi^G \rangle_G = \langle \psi^G, \chi \rangle_G ,$$

the second equality since the coefficients are non negative integers, in particular real. □

(6.2) shows that ψ^G is a very likely reducible character.

Theorem 193. *(Transitivity of Induction) For subgroups $H \subset L \subset G$ and $\psi \in C(H)$*

$$(\psi^L)^G = \psi^G$$

Proof. Restriction is clearly transitive: for $H \subset L \subset G$ and $\theta \in C(G)$,

$$(\theta_L)_H = \theta_H$$

It follows that for $\psi \in C(H)$ and $\theta \in C(G)$,

$$((\psi^L)^G, \theta)_G = (\psi^L, \theta_L)_L = (\psi, (\theta_L)_H)_H = (\psi, \theta_H)_H = (\psi^G, \theta)_G$$

Therefore $(\psi^L)^G - \psi^G$ is orthogonal to all θ, in particular to itself, so this difference is 0. □

Notation 194. For $\chi \in \hat{G}$ and $\theta \in C(G)$ we write $\chi \in \theta$ if $\langle \chi, \theta \rangle_G \neq 0$. Thus for $\chi \in \hat{G}$ and $\psi \in \hat{H}$, we have

$$\psi \in \chi_H \iff \chi \in \psi^G$$

Exercise 195. Prove that $\psi^G(1) = (G : H)\psi(1)$ for all $\psi \in C(H)$.

Exercise 196. Prove that if G has an abelian subgroup of index n, then $d_\chi \leq n$ for each $\chi \in \hat{G}$.

Exercise 197. Using the preceding exercise, prove that $|A|^2 \leq |\check{G}||G|$, for each abelian subgroup A of G.

Example 198. (of induction and restriction with $G = S_3$)

$$\begin{array}{ccccccccccc} & & S_3 & & 1 & & & & \epsilon & & \chi \\ & & |2 & & & \backslash & & / & & / & | \\ A_3 & = & H & & & & 1 & & \psi & & \bar{\psi} \\ & & |3 & & & & & \backslash & | & / & \\ & & 1 & & & & & & 1 & & \end{array}$$

or

$$\begin{array}{ccccccc} S_3 & & 1 & & & \chi & & \epsilon \\ |3 & & & \backslash & / & & \backslash & | \\ T & & & & 1 & & & \epsilon \\ |2 & & & & \backslash & / & & \\ 1 & & & & & 1 & & \end{array}$$

We write

$$\begin{array}{c} G \\ |n \\ H \end{array}$$

to say that H is a subgroups of index n, and

$$\begin{array}{c} \chi \\ | \\ \psi \end{array}$$

to say that $\psi \in \chi_H$ i.e. $\chi \in \psi^G$. In the above examples all the multiplicities are 1. We would write

$$\begin{array}{c} \chi \\ |c \\ \psi \end{array}$$

for $\langle \chi_H, \psi \rangle_H = c$.

6.2 Clifford's Theorem

Example 199. We know that for χ', $\chi'' \in \hat{G}$, the product $\chi'\chi''$ is a character of G, not necessary irreducible, so some non negative integers $c^{\chi}_{\chi',\chi''}$,

$$\chi'\chi'' = \sum_{\chi \in \hat{G}} c^{\chi}_{\chi',\chi''}\chi$$

we have $c^{\chi}_{\chi',\chi''} = \langle \chi' \times \chi'', \chi \rangle_G$ where $\chi' \times \chi'' \in \widehat{G \times G}$ and $G = \{(g,g) : g \in G\}$.

Theorem 200. *(Cauchy-Frobenius-Burnside Orbit-counting formula) For each action of a finite group G on a finite set X, the number of orbits is given by*

$$|G\backslash X| = \frac{1}{|G|}\sum_{g\in G}|X^g|$$

where X^g is the set of x fixed by g.

Proof. We count, in two ways, the number of pairs $(x,g) \in X \times G$ with $gx = x$

$$\sum_{g\in G}\sum_{\substack{x\in X\\ gx=x}} 1 = \sum_{x\in X}\sum_{\substack{g\in G\\ gx=x}} 1$$

The left side is $\sum_{g\in G}|X^g|$. The right side is

$$\sum_{x\in X}|G_x| = |G|\sum_{x\in X}\frac{1}{(G:G_x)} = |G|\sum_{A\in G\backslash X}\frac{1}{|A|}\sum_{x\in A}1 = |G||G\backslash X|$$

□

Theorem 201. *Let N be a normal subgroup of G (written $N \lhd G$), and put $F = G/N$. The group F acts by conjugation both on $\hat{N}$ and on $\check{N}$. Each element $f \in F$ fixes equally many elements in $\hat{N}$ and in $\check{N}$. There are equally many orbits in the two actions, i.e. $|F\backslash\hat{N}| = |F\backslash\check{N}|$.*

Exercise 202. Prove the first assertion above.

Proof. (rest of theorem) For each $g \in G$

$$\sum_{\psi\in\hat{N}}\langle\psi^g,\psi\rangle_N = \frac{1}{|N|}\sum_{n\in N}\sum_{\psi\in\hat{N}}\psi(n^{g^{-1}})\bar{\psi}(n) = \frac{1}{N}\sum_{n\in N}{}'|c_N(n)| = \sum_{A\subset\check{N}}{}''\frac{1}{|A|}\sum_{n\in A}1 = \sum_{A\in\check{N}}{}''1$$

the dash indicating that only n with $n^{g^{-1}}$ in same N class are taken, the double dash meaning $A^{g^{-1}} = A$. The third assertion follows from the second using theorem 200. □

Theorem 203. *(Clifford 1937) For $N \lhd G$ and $\psi \in \hat{N}$, put $T = G_\psi = \{g : \psi^g = \psi\}$. then induction from T to G gives a bijection from*

$$\{\xi \in \hat{T} : \xi \in \psi^T\} \text{ to } \{\chi \in \hat{G} : \chi \in \psi^G\}$$

Proof. By Frobenius reciprocity

$$\begin{aligned}\left\langle \psi^G, \psi^G \right\rangle_G &= \left\langle \psi^G, \psi \right\rangle_N = \sum_{\substack{g \bmod N \\ g \in G}} \langle \psi^g, \psi \rangle_N \\ &= \sum_{\substack{g \bmod N \\ g \in T}} \langle \psi^g, \psi \rangle_N = \left\langle \psi^T, \psi \right\rangle_N = \left\langle \psi^T, \psi^T \right\rangle_N\end{aligned}$$

Let

$$\psi^T = \sum_{\xi \in \hat{T}} c_{\xi,\psi} \xi, \text{ so } \psi^G = \sum_{\xi \in \hat{T}} c_{\xi,\psi} \xi^G \tag{6.3}$$

Then

$$\left\langle \psi^T, \psi^T \right\rangle_T = \sum_{\xi \in \hat{T}} c_{\xi,\psi}^2, \text{ and } \left\langle \psi^G, \psi^G \right\rangle_G = \sum_{\xi,\eta \in \hat{T}} c_\xi c_\eta \left\langle \xi^G, \eta^G \right\rangle_G \tag{6.4}$$

Combining (6.3), (6.4) gives

$$\sum_{\xi,\eta \in \hat{T}} c_\xi c_\eta \left\langle \xi^G, \eta^G \right\rangle_G = \sum_{\xi,\eta \in \hat{T}} c_{\xi,\psi}^2$$

Since all terms are non negative and each $\left\langle \xi^G, \eta^G \right\rangle_G$ is ≥ 1, we conclude that the ξ^G for $\xi \in \psi^T$ are irreducible and distinct. □

Corollary 204. *For $N \lhd G$, $\psi \in \hat{N}$, $\chi \in \hat{G}$ with $\chi \in \psi^G$, put $T = G_\psi$, then there is a unique $\xi \in \hat{T}$ for which $\xi \in \psi^T$ and $\chi \in \xi^G$. For this ξ we have $\xi^G = \chi$ and $\xi_N = c\psi$ with $c = \left\langle \psi^G, \chi \right\rangle_G$ Therefore*

$$\chi_N = c \sum_{g \bmod T} \psi^g$$

Exercise 205. Prove the corollary.

Theorem 206. *Let $N \lhd G$, $\chi \in \hat{G}$and suppose $\psi = \chi_N \in \hat{N}$. Put $F = G/N$, then*

$$\psi^G = \sum_{w \in \hat{F}} d_w \tilde{w} \chi \tag{6.5}$$

and $\tilde{w}\chi$ are irreducible and distinct.

Proof. Let v be the regular character of F. Both ψ^G and $\tilde{v}$ vanish off N, and $(\psi^G)_N = |F|\psi$, $\tilde{v}_N = |F|$, giving (6.5), we have

$$|F| = (\psi^G, \psi)_N = \left\langle \psi^G, \psi^G \right\rangle_G = \sum_{w,w'} d_w d_{w'} \left\langle \tilde{w}\chi, \tilde{w}'\chi \right\rangle_G \geq \sum_w d_w^2 = |F|$$

so there $\geq$is equality, from which the $\tilde{w}\chi$ are irreducible and distinct. □

Corollary 207. *Let $N \triangleleft G$, $\psi \in \hat{N}$, $F = G/N$. If ψ extends to a character $\chi \in \hat{G}$, then all the extensions of ψ to characters of G are the $\tilde{w}\chi$'s with $w \in \hat{F}$, $d_w = 1$.*

Remark 208. Let $N \triangleleft G$, $F = G/N$. A necessary condition for $\psi \in \hat{N}$ to extend to a $\chi \in \hat{G}$is that ψ be fixed by F, but this condition is not sufficient.

For example, let G be a non abelian group of order 8. There are two such groups up to isomorphism the quaternion group

$$\{\pm 1, \pm i, \pm j, \pm k\}$$

and the dihedral group of order 8

$$\{\text{symmetries of the rectangular parallelepiped with } a \neq b\}$$

The possible irreducible character degrees are 1 and 2, so they are 1,1,1,1,2. It follows that G/G' has order 4. The characters of G' are 1 and ϵ, both fixed by G, but ϵ does not extend to a character of G, since if it did then corollary should imply every $\chi \in \hat{G}$ would have degree 1.

Lecture 16 (4/1/13)

Theorem 209. *(Clifford) Let $N \triangleleft G$ with G/N cyclic, and let $\psi \in \hat{N}$. Then ψ extends to an element of $\hat{G}$ iff ψ is stabilized by G.*

Proof. If ψ extends to a character χ of G, then since χ is a class function it follows that $\psi(h^{-1}nh) = \psi(n)$ for $n \in N$ and $h \in G$, i.e. $\psi^h = \psi$ for $h \in G$.

Now suppose only that ψ is stabilized by G. Let $m = |B/N|$ and let $gN = Ng$ be a generator for G/N. Then each element of G has the standard form ng^i with $n \in N$ and $0 \leq j < n$.

Multiplication in G is given by

$$(n'g^h)(ng^l) = r'r^{(g^k)} \cdot g^{k+l} \text{ with } n^h = hnh^{-1}$$

If $h+l<n$, then the right side is in standard form, but not if $k+l \geq n$. Let $n_0 = g^n \in N$, then for all $n', n \in N$ and $0 \leq h, l < n$,

$$(n'g^k)(ng^l) = \begin{cases} n'n^{(g^k)} \cdot g^{k+l} & k+l<n \\ n'n^{(g^k)} n_0 \cdot g^{k+l-n} & k+l \geq n \end{cases} \qquad (1)$$

The right side of (1) is in standard form in both cases.

Thus multiplication in G is determined by three things: multiplication in N, the map $n \mapsto n^g$ and the element n_0.

Let $\psi \in \hat{N}^G$, and let $R : N \to \mathcal{G}(V)$ be a representation of N with character ψ. Since $\psi^g = \psi$, it follows that R^g is equivalent to R, as for some $T \in \mathcal{G}(V)$, we have $R(n^g) = TR(n)T^{-1}$ for $n \in N$, so

$$R(n^{(g^j)} = T^j R(n) T^{-j} \text{ for } n \in N \text{ and integers } j \geq 0 \qquad (2)$$

In particular,

$$R(n_0)R(n)R(n_0)^{-1} = R(n^{n_0}) = R(n^{(g^n)}) = R^n R(n) T^{-n}$$

for $n \in N$, i.e. $T^{-n}R(n_0)$ commutes with all $R(n)$. Since R is irreducible, Schur's lemma gives $T^{-m}R(n_0) = \lambda I_v$ for some $\lambda \in \mathbb{C}^x$. Since any scalar multiple of T will do as well in (2), we can replace T by $T\lambda^{\frac{1}{n}}$ any nth root, and have

$$T^n = R(n_0) \qquad (3)$$

Using this T, we extend R to a map from G to $\mathcal{G}(V)$ by putting

$$R(ng^j) = R(n)T^j \text{ for } n \in N, 0 \leq j < n \qquad (4)$$

The extended R is a representation of G. In fact for $n, n' \in N$ and $0 \leq k, l < n$

$$\begin{aligned} R(n'g^k ng^l) &\overset{(1)}{=} \begin{cases} R(n'n^{(g^k)}, g^{k+l}) & k+l<n \\ R(n'n^{(g^k)}n_0, g^{k+l-n}) & k+l \geq n \end{cases} \\ &\overset{(4)}{=} \begin{cases} R(n'n^{(g^k)})T^{k+l} & k+l<n \\ R(n'n^{(g^k)}n_0)T^{k+l-n} & k+l \geq n \end{cases} \\ &\overset{(3)}{=} R(n')R(n^{(g^k)})T^{k+l} \\ &= R(n')T^k R(n) T^l \\ &= R(n'g^k)R(ng^l) \end{aligned}$$

Since R extends to a representation of G, the character ψ of R extends to a character of G, the character of the extended representation. $\square$

Theorem 210. *(Burnside) Let $N \triangleleft G$ with G/N of prime order, and let $\psi \in \hat{N}$. Then either ψ extends to a character $\chi \in \hat{G}$, or $\psi^G \in \hat{G}$, not both.*

Proof. Let $G_\psi$be the stabilizer of ψ in G. Since $N \subset G_\psi \subset G$ and $|G/N|$ is a prime number, either $G_\psi = G$ or $G_\psi = N$.

If $G_\psi = G$, then ψ extends to some $\chi \in \hat{G}$ by theorem 209.

If $G_\psi = N$, then reciprocity gives

$$\left\langle \psi^G, \psi^G \right\rangle_G = \left\langle (\psi^G)_N, \psi \right\rangle_N = \left\langle \sum_{g \bmod N} \psi^g, \psi \right\rangle_N = \sum_{g \bmod N} \langle \psi^g, \psi \rangle_N = 1$$

so $\psi^G \in \hat{G}$. □

6.3 Cyclic Factor Groups & Good Classes in Factor Groups

Notation 211. Let $N \triangleleft G$ and $\psi \in \hat{N}^G$. Put $F = G/N$. For $f \in F$, denote by G_f the subgroup of G containing N, for which G_f/N is the cyclic subgroup of F generated by f.

Denote by χ_f an extension of ψ to G_f, generated by theorem 209.

Denote by C_f the subgroup of G containing G_f for which $C_f/N = C_F(G_f/N)$, thus $G_f \triangleleft C_f$.

If $h \in C_f$, then χ_f^h is also an extension of ψ to G_f, so

$$\chi_f^h = w_h \chi_f$$

for some unique $w_h \in \widehat{G_f/N}$, by theorem 206.

Definition 212. $f \in F = G/N$ and χ_f and C_f as above, we say f is good for ψ if $\chi_f^h = \chi_f$ i.e. $w_h = 1$ for all $h \in C_f$.

Lemma 213. *Goodness of f is independent of the choice of extension χ_f of $\psi$to G_f, and depends only on the conjugacy class of f in F.*

Exercise 214. Prove the lemma.

Theorem 215. *For $N \triangleleft G$, $\psi \in \hat{N}^G$ and $F = G/N$, the number of $\chi \in \hat{G}$ over ψ equals the number of conjugacy classes of F which are good for ψ.*

Corollary 216. *For $N \lhd G$, $\psi \in \hat{N}^G$ and $F = G/N$, then number of $\chi \in \hat{G}$ over ψ is at most $k(F)$.*

The proof of thereon 215 is by a concatenation of lemmas.

Lemma 217. *For $\chi \in \hat{G}$*

$$\frac{1}{|G|^2} \sum_{g,h \in G} \chi([g,h]) = \frac{1}{d_\chi}$$

$[g,h] = g^{-1}h^{-1}gh$.

Exercise 218. Prove lemma, using functional equation.

Lemma 219. *For $N \lhd G$ and $\psi \in \hat{N}^G$*

$$d_\psi \psi^G = \sum_{\chi \in \hat{G}}{}' d_\chi \chi$$

the dash meaning χ over ψ'.

Proof. Let $\psi^G = \sum_{\chi \in \hat{G}} c_{\chi\psi}\chi$. For each χ over ψ i.e. $c_{\chi\psi} \neq 0$ we have $\chi_\psi = c_{\chi\psi}\psi$, so $d_\chi = c_{\chi\psi}d_\psi$. Combine with the formula for ψ^G this gives the formula for $d_\psi \psi^G$. □

Lemma 220. *For $N \lhd G$, $\psi \in \hat{N}^G$, $f \in F = G/N$ and $g \in f$,*

$$\sum_{h \in C_f} \psi([g,h]) = \frac{|C_f||\chi_f(g)|^2}{d_\psi}$$

if f is good for ψ, 0 otherwise.

Proof. Let R_f be a representation of G_f with character χ_f then

$$\sum_{h \in C_f} \psi([g,h]) = \mathrm{tr}(R_f(g^{-1})) \sum_{h \in C_f} R_f(h^{-1}gh)$$

The sum on the right commutes with $R_f(g_1)$ for each $g_1 \in G_f$, so it has the form λI with $\lambda \in \mathbb{C}$, by Schur's lemma. Taking trace

$$\lambda d_\psi = \sum_{h \in C_f} \chi_f^h(g) = [\sum_{h \in C_f} w_h(g)]\chi_f(g) = |C_f|\chi_f(g)$$

if f is good for ψ, 0 otherwise. □

Lemma 221. *For each subgroup H of G,*

1) $\sum_{h\in H}\xi(gh)=0$ for all $\xi\in\hat{G}$ with $\langle\xi_H,1\rangle_H=0$

2) $\sum_{h\in H}|\chi(gh)|^2=|H|$ for all $\chi\in\hat{G}$ with $\chi_H\in\hat{H}$.

Proof. 1) Let R be a representation of G on V with character ξ. Then

$$\sum_{h\in H}\xi(gh)=\mathrm{tr}(R(g)\sum_{h\in H}R(h))$$

so it suffices to show that the sum on the right is $0\in\xi(V)$. Let

$$\xi_H=\sum_{\psi\in\hat{H}}c_{\xi\psi}\psi \text{ with } c_{\xi 1}=0$$

Then

$$R_H\simeq\bigoplus_{\psi\in\hat{H}}c_{\xi\psi}R_\psi$$

where $R_\psi$is a representation of H on a space V_ψ with character ψ so

$$\sum_{h\in H}R_H(h)=\bigoplus_{\psi\in\hat{H}}c_{\xi\psi}\sum_{h\in H}R_\psi$$

Thus it suffices to show that $\sum_{h\in H}R_\psi=0\in\xi(V_\psi)$ for each $\psi\in\hat{H}$ with $c_{\xi\psi}\neq 0$. In fact the inner sum on the right commutes with all $R_\psi(h_1)$, so has the form λI_ψ with some $\lambda\in\mathbb{C}$. Taking trace

$$\lambda d_\psi=\sum_{h\in H}\psi(h)=0$$

for $\psi\neq 1$. Since $c_{\xi\psi}\neq 0$ implies $\psi\neq 1$, we get what we want.

2) Let

$$|\chi|^2=\chi\bar{\chi}=\sum_{\xi\in\hat{G}}b_{\chi\xi}\xi$$

Since $\chi\in\hat{G}$ we have $b_{\chi 1}=1$. Since $\chi_H\in\hat{H}$, we have $\sum b_{\chi\xi}\langle\xi_H,1\rangle_H=1$, so

$$b_{\chi\xi}=0 \text{ for } \langle\xi_H,1\rangle\neq 0$$

Thus by 1),

$$\sum_{h\in H}|\chi(gh)|^2=\sum_{\xi\in\hat{G}}b_{\chi\xi}\sum_{h\in H}\xi(gh)=b_{\chi 1}|H|$$

□

Now prove thereon 215

Proof.

$$\begin{aligned}
\sum_{\chi\in\psi^G} 1 &= \frac{1}{|G|^2}\sum_{g,h\in G}\sum_{\chi\in\psi^G} d_\psi\chi([g,h]) \text{ by lemma 217}\\
&= \frac{1}{|G|^2}\sum_{g,h\in G} d_\psi\psi^G([g,h]) \text{ by lemma 219}\\
&= \frac{1}{|G||N|}\sum_{f\in F}\sum_{g\in f}\sum_{h\in C_f} d_\psi\psi([g,h])\\
&= \frac{1}{|G||N|}\sum_{\substack{f\in F\\ f \text{ good for } \psi}} |C_f|\sum_{g\in f}|\chi_f(g)|^2 \text{ by lemma 220}\\
&= \frac{1}{|F|}\sum_{\substack{f\in F\\ f \text{ good for } \psi}} |C_F(f)|
\end{aligned}$$

The third equality is because $\psi^G = |G/N|\psi$ on N, 0 off N, and $[g,h] \in N \iff h \in C_f$. The last step is by lemma 221 with $G = G_f$, $H = N$.

Finally, F acts by conjugation on itself, the orbits being the classes of F. In this action the elements of F which are good for ψ form a stable subset T. By the orbit counting formula the average above is the umber of classes of F which are good for ψ. □

7 Applications to the theory of Finite Groups

7.1 Sylow Subgroups

Lecture 17 (4/8/13)

Definition 222. A Sylow p subgroup of a finite group G is a p subgroup G_p with $p \nmid (G : G_p)$, equivalently, if $|G| = p^a m$ with $p \nmid m$, then $|G_p| = p^a$.

Theorem 223. *(Sylow 1872) For each finite group G and each prime p,*

1) The number n_p of Sylow p subgroups of G satisfies $n_p \equiv 1$ mod p ($\therefore n_p \neq 0$)

2) Any two Sylow p subgroups of G are conjugate

3) Each p subgroup of G is contained in some Sylow p subgroup of G.

Exercise 224. Prove that different subgroups of G have different right cosets.

Exercise 225. Prove that each finite cyclic group C has exactly one subgroup of each order dividing $|C|$.

Proof. 1) Let G be a group of order $p^a m$ with $p \nmid m$. Let $\mathcal{S}$ be the set of all subsets $S \subset G$ with $|S| = p^a$. G acts by left translation on $\mathcal{S}$ (since $|gS| = |S|$ for $g \in G$, $S \subset G$). For $S \in \mathcal{S}$, the stabilizer G_S satisfies $G_S S = S$, so S is a disjoint union of right cosets of G_S. It follows that $|G_S|$ divides p^a, with equality iff G_S is a Sylow p subgroup of G and S is a right coset of G_S.

By exercise 224 the number such S is mn_p. Each of the other $S \in \mathcal{S}$ belongs to an orbit of size $(G : G_S) \equiv 0 \bmod p$. Therefore

$$|\mathcal{S}| \equiv mn_p \bmod p$$

In particular this congruence holds if G is replaced by a cyclic group C of order $p^a m$, for which $|\mathcal{S}|$ has the same size as for G, bu for which $n_p = 1$, by exercise 225, Thus $mn_p \equiv m \bmod p$, from which

$$n_p \equiv 1 \bmod p$$

2&3) Let P be a p subgroup of G, and let G_p be any Sylow p subgroup of G which exists by 1). Since G acts by left translation on G/G_p so does P, and

$$\begin{aligned} |(G/G_p)^P| &\equiv |G/G_p| \bmod p \\ &\not\equiv 0 \bmod p \end{aligned}$$

In particular $(G/G_p)^P$ is not empty, i.e. P fixes some coset gG_p

$$PgG_p = gG_p, \text{ so } Pg \subset gG_p, \text{ i.e. } P \subset gG_p g^{-1} = G_p^g$$

Thus each p subgroup of G is contained in some conjugate of G_p, which proves both 2&3). □

7.2 Solvable Groups

Definition 226. A finite group G is solvable if either $G = 1$ or G/A is solvable, for some abelian normal subgroup $A \neq 1$ (In particular, each finite abelian group is solvable).

Example 227. S_3 is solvable, since $A_3 \triangleleft S_3$ with $|A_3| = 3$ and $|S_3/A_3| = 2$ so both A_3 and S_3/A_3 are cyclic, hence abelian, hence solvable.

Exercise 228. Prove that each p group P is solvable by induction on $|P|$, using the induction definition of solvabilily and the fact that $P \neq 1 \implies Z(p) \neq 1$.

Theorem 229. *Let G be a solvable group, then*

1) Each subgroup of G is solvable.

2) For each normal subgroup N, the factor group G/N is solvable.

Lemma 230. *(i) If $N \triangleleft G$, and H is a subgroup of G with $H \supset N$, then H/N is a subgroup of G/N, each subgroup of G/N is of this from.*

(ii) If $N \triangleleft G$ and M is a subgroup of G with $M \supset N$, then $M \triangleleft G \iff M/N \triangleleft G/N$ and in that case

$$(G/N)/(M/N) \simeq G/M$$

(iii)(Second isomorphism theorem) If $N \triangleleft G$ and H is a subgroup of G, then $H \cap N \triangleleft H$, HN is a subgroup of G with $HN \supset N$, and

$$HN/N \simeq H/(H \cap N)$$

For proofs of the lemma, see any algebra texts.

Proof. 1) We man suppose $1 \neq H \neq G$, so $G \neq 1$, so there is an abelian $A \triangleleft G$ with $A \neq 1$ and G/A solvable. Since HA/A is a subgroup of G/A, induction gives HA/A solvable, so $H/H \cap A$ is solvable, by (iii). If $H \cap A = 1$, then H is solvable immediately, while if $H \cap A \neq 1$, then H is solvable by the inductive definition of solvability.

2) We may suppose $|G| \neq 1$, so G has an abelian $A \triangleleft G$ with $A \neq 1$ G/A solvable. If $A \subset N$ then by (ii), $N/A \triangleleft G/A$ and

$$G/N \simeq (G/A)/(N/A)$$

which is solvable by induction, since $|G/A| < |G|$

If $A \not\subset N$, then $A \cap N \neq A$, and

$$AN/N \simeq A/A \cap N$$

shows that AN/N is an abelian subgroup $\neq 1$ of G/N. Since $A \triangleleft G$ & $N \triangleleft G$, we have $AN \triangleleft G$, so $AN/N \triangleleft G/N$, by (ii). Since

$$(G/N)/(AN/N) \simeq G/AN \simeq (G/A)/(AN/A)$$

and the right side, as a factor group of G/A, is solvable by induction, we conclude that G/N is solvable, by the induction definition of solvability. □

Definition 231. A subgroup K of G is characteristic, written $K \blacktriangleleft G$, if $K^\alpha = K \ \forall \, \alpha \in Aut(G)$.

Example 232. In $G = C_2 \times C_2$, each of the three subgroups of order 2 is normal, since G is abelian, but none of the three are characteristic, since the automorphism of order 3 permutes these three subgroups cyclically.

Example 233. The commutator subgroup G' (generated by all commutators $[g,h]$) is characteristic in G, as is the center $Z(G)$. In fact for each $\alpha \in Aut(G)$, we have $[g,h]^\alpha = [g^\alpha, h^\alpha]$ so α satisfies the set of all commutators and $\therefore$ G' also $zg = gz \ \forall \, g \implies z^\alpha g^\alpha = g^\alpha z^\alpha \ \forall \, g$ so $z \in Z(G) \implies z^\alpha \in Z(G)$,...

Lemma 234. *1) If $K \blacktriangleleft N$ and $N \blacktriangleleft G$, then $K \blacktriangleleft G$.*

2) If $K \blacktriangleleft G$ and $N \triangleleft G$, then $K \triangleleft G$.

Proof. 1) Let $\alpha \in Aut(G)$. If $N \blacktriangleleft G$, then α satisfies N, so α_N (the restriction of α to N) satisfies $\alpha_N \in Aut(N)$ If also $K \blacktriangleleft N$, then α_N satisfies K, i.e. α satisfies K. Thus $K \blacktriangleleft G$.

2) Let $h \in G$. If $N \triangleleft G$, then the inner automorphism $\alpha_h : g \mapsto hgh^{-1}$ of G stabilizes N, i.e. $(\alpha_h)_N \in Aut(N)$ If also $K \blacktriangleleft N$, then $(\alpha_h)_N$ stabilize K, i.e. α_h stabilizes K thus $K \triangleleft G$. □

Lemma 235. *Each finite solvable group N has a finite sequence of subgroups $N_g \triangleleft G$ with*

$$1 = N_0 \subsetneq N_1 \subsetneq ... \subsetneq N_k = N$$

and

$$N_{g+1}/N_j \ \textit{abelian for} \ 0 \leq j < k$$

Proof. If $N = 1$ take $k = 0$, $N_0 = N$. If $N \neq 1$, let N_1 be an abelian normal subgroup $\neq 1$ with G/N solvable. By induction there is a sequence of normal subgroups N_j/N_1 of G/N,

$$1 = N_1/N_1 \subsetneq ... \subsetneq N_k/N_1 = N/N_1$$

with

$$(N_{j+1}/N_1)/(N_j/N_1) \simeq N_{j+1}/N_j \text{ abelian for } 1 \leq j < k$$

□

Theorem 236. *Each finite solvable group $N \neq 1$ has an abelian characteristic subgroup $A \neq 1$.*

Proof. By the proceeding lemma, there is a subgroup $M \triangleleft G$ with N/M abelian and $\neq 1$ (e.g. take $M = N_{k-1}$). For each $g, h \in N$, we have $[gN, hN] = 1$ in N/M, so $[g, h] \in M$ thus $N' \subset M$ so $N' \neq N$

If $N' = 1$, then take $A = N$.

If $N' \neq 1$, then N' being solvable of order $< |N|$, N' has an abelian characteristic subgroup $A \neq 1$. Since $A \blacktriangleleft N'$ and $N' \triangleleft N$, we have $A \blacktriangleleft N$. □

Theorem 237. *Let G be a finite group. If both $N \triangleleft G$ and G/N are solvable, then G is solvable.*

Proof. We may suppose $N \neq 1$, Let $1 \neq A \blacktriangleleft N$ with A abelian as in theorem 236. Since N/A and $(G/A)/(N/A) = G/N$ are solvable, we get G/A solvable by induction, so G is solvable, by the inductive definition of solvability. □

7.3 Schur-Zassenhaus Theorem

Lecture 18 (4/10/13)

Theorem 238. *(Schur 1910 Zassenhaus 1937) Let G be a finite group with a normal subgroup N, put $F = G/N$. If $(|F|, |N|) = 1$, then G has a subgroup $M \simeq F$.*

The proof has two parts: The first part, in which N is assumed to be abelian, was done by Schur, by an ingenious device, which as developed by Schreier(1920s), Artin(1930s) and others into something now called "cohomology theory" of groups. The second part, with N arbitrary, was done by Zassenhaus, making use of the Sylow theorems and the N abelian case.

Theorem 239. *(Schur) This is the case of theorem 238 with N abelian.*

Proof. In each coset $f \in F$ (right or left coset of a normal subgroup are the same), choose any coset representation $r(f)$. This gives a map

$$r : F \to G$$

with $r(f) \in f \; \forall f \in F$. From r we get a second map

$$n : F \times G \to N$$

with $n(f,g) = gr(g^{-1}f)r(f)^{-1} \in gg^{-1}ff^{-1} = N \; \forall f \in F, g \in G$, we have

$$n(f,g) = g \tag{7.1}$$

$\forall f \in F$, $g \in N$. Since $g^{-1}f = f$ for $g \in N$. Also n satisfies a key functional equation

$$n(f,gh) = n(f,g)n(g^{-1}f,h)^g \tag{7.2}$$

$\forall f \in F$, $g,h \in G$. Indeed we rewrite left side by introducing canceling factors

$$\begin{aligned} ghr(h^{-1}g^{-1}f)r(f)^{-1} &= gr(g^{-1}f)r(f)^{-1}r(f)r(g^{-1}f)^{-1}hr(h^{-1}g^{-1}f)r(g^{-1}f)^{-1}r(g^{-1}f)r(f)^{-1} \\ &= n(f,g)n(h,g^{-1}f)^u \end{aligned}$$

with $u = r(f)r(g^{-1}f)^{-1} \in ff^{-1}g \in gN$.

Sine N is abelian, we have $n(h,g^{-1}f)^u = n(h,g^{-1}f)^g$. Since N is abelian, we can unambiguously (i..e without ordering the factors) multiply equation (7.2) for all $f \in F$, and write the result as

$$\prod_{f \in F} n(f,gh) = \prod_f n(f,g) \left(\prod_f n(f,h) \right)^g \tag{7.3}$$

$\forall g,h \in G$. (In the second product on the right we may conjugate the whole product by g. Since $x \to x^g$ is a homomorphism, and we may eliminate the g^{-1} in $g^{-1}f$ since $f \mapsto g^{-1}f$ termites the factors and N is abelian.)

Since $|F|$ and $|N|$ are relatively prime the map $x \mapsto x^{|F|}$ for $x \in N$ is an automorphism of $|N|$. We denote by $x \mapsto x^{|F|}$ the inverse automorphism.

Using the inverse map, we define a third map

$$\bar{n} : G \to N \text{ by } \bar{n}(g) = \left(\prod_{f \in F} n(f, g) \right)^{\frac{1}{|F|}}$$

$\forall\, g \in G$. From (7.1), (7.3) we get

$$\bar{n}(g) = g \quad \forall\, g \in N \tag{7.4}$$

and

$$\bar{n}(gh) = \bar{n}(g)\bar{n}(h)^g \quad \forall\, g, h \in G \tag{7.5}$$

Finally we define a map

$$m : G \to G \text{ by } m(g) = \bar{n}(g)^{-1} g \;\forall\, g \in G \tag{7.6}$$

From (7.4) we get

$$m(g) = 1 \quad \forall\, g \in N \tag{7.7}$$

From (7.5) we get

$$m(gh) = m(g)m(h) \qquad \forall\, g, h \in G \tag{7.8}$$

Since the left side is

$$\begin{aligned} \bar{n}(gh)^{-1} gh &= (\bar{n}(h)^g)^{-1} \bar{n}(g)^{-1} gh \\ &= \bar{n}(g)^{-1} (\bar{n}(h)^g)^{-1} gh \quad \because N \text{ is abelian} \\ &= \bar{n}(g)^{-1} g \bar{n}(h)^{-1} h \quad \because \bar{n}(h)^g = g\bar{n}(h)g^{-1} \\ &= m(g)m(h) \end{aligned}$$

From (7.8), (7.7) m is a homomorphism with kernel $\supset N$. Put

$$M = m(G)$$

then M is a subgroup of G with

$$M = |\mathrm{Im} m| = |G/\mathrm{ker} m| \leq |G/N| = |F| \tag{7.9}$$

From (7.6), each $g \in G$ has the form $g = \bar{n}(g)m(g) \in NM = MN$, so

$$|F| = |G/N| = |MN/N| = |M/(M \cap N)| \leq |M| \tag{7.10}$$

combining (7.9), (7.10) gives $|M| = |F|$, actually $M \simeq F$... $\square$

7.4 Hall Subgroups

Definition 240. A subgroup H of G is a Hall subgroup if $(|H|, (G : H)) = 1$

Definition 241. Subgroups M and N of G are complementary if $MN = G$ and $M \cap N = 1$.

In this language, theorem 238 says that if N is a normal Hall subgroup of G, then there is a complementary subgroup M, i.e. a subgroup M with $|M| = |G/N|$.

Proof. (of theorem 238) We may suppose $N \neq 1$. Let p be a prime divisor of N and let N_p be a Sylow p subgroup of N.

If $N_p \triangleleft G$, then $1 \neq Z(N_p) \blacktriangleleft N_p$ so $1 \neq Z(N_p) \triangleleft G$. By induction $G/Z(N_p)$ is an abelian normal Hall subgroup of L, theorem 239 implies that L has a complement M to $Z(N_p)$, which is then a complement to N in G.

If $N_p \not\triangleleft G$, let L be the normalizer of N_p in G, i.e. $l \in L \iff N_p^l = N_p$. Then $L \neq G$, and

$$G = LN$$

In fact, for $g \in G$ both N_p and N_p^g are Sylow subgroups of N, so they are conjugate in N, i.e. $N_p^g = N_p^n$ for some $n \in N$, i.e. $n^{-1}g \in L$ so $g \in NL = LN$. Thus $G = LN$. So $L \cap N$ is a normal Hall subgroups of L. Since $L \neq G$, induction give a complement M to $L \cap N$ in L, which is then a complement to N in G. □

The complement M to a normal Hall subgroup N of G is in fact determined up to conjugacy in G.

Lecture 19 (4/15/13)

Lemma 242. *For each normal subgroup N of G, each subgroup H of G acts by conjugation, both on N and also on $\hat{N}$:*

$$n^h = hnh^{-1};\ \textit{also}\ \psi^h(n) = \psi(n^{h^{-1}}) = \psi(h^{-1}nh),\ \textit{for}\ h \in H, n \in N, \psi \in \hat{N}$$

Proof. G acts by conjugation on G, stabilizing N, so G acts by conjugation on N. It follows that each subgroup H of G acts, by restriction on N. Therefore H also acts on the set $m(N, \mathbb{C})$ of all complex functions θ on N, by

$$\theta^h(n) = \theta(n^{h^{-1}})$$

It suffices to prove that $\hat{N}$ is stabilized by this action. Let $\psi \in \hat{N}$, and let R be a representation of N with character ψ then ψ^h is the character of the representation $n \mapsto n^{h^{-1}} \mapsto R(n^{h^{-1}})$. That $\psi^h \in \hat{N}$ follows, e.g. from

$$\left\langle \psi^h, \psi^h \right\rangle_N = \frac{1}{|N|} \sum_{n \in N} |\psi(n^h)|^2 = \frac{1}{|N|} \sum_{n \in N} |\psi(n)|^2 = \langle \psi, \psi \rangle_N$$

□

Lemma 243. *If $N \triangleleft G$ and H is complementary to N, then the multiplication in G is indeterminate by (i) the multiplication in N, (ii) the multiplication in H, (iii) the action of H on N:*

$$(n_1 a)(nb) = n_1 n^a ab \text{ for } n_1, n \in N \text{ and } a, b \in H \tag{7.11}$$

Proof. Each element of G is uniquely na for $n \in N$ $a \in H$ and $an = n^a a$ $\forall\, a \in H$ $n \in N$. □

Theorem 244. *If N is a normal Hall subgroup of G and H is complementary to N, then each $\psi \in \hat{N}$ which is stabilized by H extends to a character of G.*

Proof is similar to Schur part of proof of Schur-Zassenhaus.

Proof. Let $R : N \to \mathcal{G}(V)$ be an irreducible representation of N with character ψ. It suffices to extend R to a representation of G. For $a \in H$, the map $n \mapsto R(n^a)$ is also a representation of N on V with character $\psi^{a^{-1}} = \psi$ (since ψ is stabilized by H), so this representation is equivalent to R, i.e. there is a bijection endomorphism $T(a)$ of V with

$$R(n^a) = T(a)R(n)T(a)^{-1} \quad \forall\, n \in N \tag{7.12}$$

The maps $T(a)$ are only determined up to a nonzero scalar factor by Schur's lemma. For each $a \in H$ we choose one $T(a)$ satisfying (7.12), the formula $n^{ab} = (n^b)^a$ combined with (7.12) gives

$$T(ab)R(n)T(ab)^{-1} = R(n^{ab}) = T(a)T(b)R(n)T(b)^{-1}T(a)^{-1}$$

from which $T(b)^{-1}T(a)^{-1}T(ab)$ commutes with $R(n)$ for each $n \in N$ and $a, b \in H$, so by Schur's lemma there is a scalar function $\gamma : H \times H \to \mathbb{C}^\times$ so that

$$T(ab) = \gamma(ab)T(a)T(b) \quad \forall\, a, b \in H \tag{7.13}$$

We will show that after multiplication of each $T(b)$ by an invertible factor from $\mathbb{C}^\times$ all the $\gamma(a,b)$ become 1, simplifying (7.19).

First use the associative law in H together with (7.19). For $a, b, c \in H$,

$$T(a)T(b)T(c) = \gamma(a,b)T(ab)T(c) = \gamma(a,b)\gamma(a,b,c)T(a,b,c)$$

$$LHS = T(a)\gamma(b,c)T(bc) = \gamma(a,bc)\gamma(b,c)T(abc)$$

It follows that γ is a 2-cocycle, i.e.

$$\gamma(a,b)\gamma(ab,c) = \gamma(a,bc)\gamma(b,c) \quad \forall\, a,b,c \in H \tag{7.14}$$

For each $a, b \in H$, take the product of (7.14) over $c \in H$

$$\gamma(a,b)^H \prod_{c\in H} \gamma(ab,c) = \prod_{c\in H} \gamma(a,bc) \prod_{c\in H} \gamma(b,c)$$

i.e,

$$\gamma(a,b)^H = \epsilon(a)\epsilon(b)\epsilon(ab)^{-1} \quad \forall\, a,b \in H \tag{7.15}$$

with

$$\epsilon(a) = \prod_{c\in H} \gamma(a,c) \quad \forall\, a \in H$$

Secondly take the determinant of (7.19)

$$\det T(ab) = \gamma(a,b)^{d_\psi} \det T(a) \det T(b)$$

i.e.

$$\gamma(a,b)^{d_\psi} = \delta(a)\delta(b)\delta(ab)^{-1} \;\forall\, a,b \in H \tag{7.16}$$

with

$$\delta(a) = (\det T(a))^{-1} \;\forall\, a \in H$$

Thirdly since $(|N|, |H|) = 1$ and d_ψ divides $|N|$, it follows that $(d_\psi, |H|) = 1$ so there are d and e in $\mathbb{Z}$ so that

$$d|H| + ed_\psi = 1 \tag{7.17}$$

From (7.15), (7.16), (7.17)

$$\gamma(a,b) = \gamma(a,b)^{d|H|}\gamma(a,b)^{ed_\psi} = (\epsilon(a)\epsilon(b)\epsilon(ab)^{-1})^d(\delta(a)\delta(b)\delta(ab)^{-1})^e$$

i.e.

$$\gamma(a,b) = \beta(a)\beta(b)\beta(ab)^{-1} \;\forall\, a,b \in H \tag{7.18}$$

with

$$\beta = \epsilon^d \delta^e$$

Fourthly defined a map $S : H \to \mathcal{G}(V)$ by

$$S(a) = \beta(a)^{-1} T(a) \qquad \forall\, a \in H \tag{7.19}$$

From (7.18) and (7.19), (7.13) becomes

$$S(ab) = S(a)S(b) \quad \forall\, a, b \in H \tag{7.20}$$

Since $S(a)$ differs from $T(a)$ only by a scalar factor, (7.12) gives

$$R(n^a) = S(a)R(n)S(a)^{-1} \quad \forall\, a \in H, n \in N \tag{7.21}$$

At last, extended R to G by putting

$$R(na) = R(n)S(a) \quad \forall\, n \in N, a \in A \tag{7.22}$$

This extended R is a representation of G, since for all $n_1, n \in N$ and $a, b \in H$

$$\begin{aligned}
R(n_1 anb) &\overset{(7.11)}{=} R(n_1 n^a ab) \\
&\overset{(7.22)}{=} R(n_1 n^a) S(ab) \\
&\overset{(7.20)}{=} R(n_1) R(n^a) S(a) S(b) \\
&\overset{(7.21)}{=} R(n_1) S(a) R(n) S(a)^{-1} S(a) S(b) \\
&= R(n_1) S(a) R(n) S(b) \\
&\overset{(7.22)}{=} R(n_1 a) R(nb)
\end{aligned}$$

□

7.5 Solomon's Induction Theorem

Lecture 20 (4/17/13)

Definition 245. A finite group U is quasi-elementary if for some prime p,

$$U/C \simeq U_p \text{ for some cyclic } C \triangleleft U$$

Example 246. S_3 is quasi-elementary since $|S_3/C_3| = 2$.

Theorem 247. *(Solomon 1961) For each finite group G,*

$$1_G = \sum_{U \in \tilde{\xi}} a_U 1_U^G \text{ with all } a_U \in \mathbb{Z}$$

where $\tilde{\xi}$ is the set of all quasi-elementary subgroups $U \subset G$.

Lemma 248. *(Banashewshi) Let S be a nonempty finite set, and let R be a subset of $m(S, \mathbb{Z})$ closed under addition, subtraction and multiplication. Assume also that*

$$\forall\, s \in S, \forall\, \text{prime } p\, \exists\, f_s \in R \text{ with } f_s(s) \not\equiv 0 \bmod p \tag{7.23}$$

Then the constant function 1_s is in R.

Proof. For each $s \in S$, let $I_s = \{f(s) : f \in R\}$, then I_s is a subgroup of $\mathbb{Z}^+$, so that $I_s = \{0\}$ or $I_s = m\mathbb{Z}$ for some $m \in \mathbb{N}$. Then (7.23) excludes $I_s = \{0\}$ and also excludes $I_s = m\mathbb{Z}$ for any $m > 1$, since $I_x = m\mathbb{Z} \subset p\mathbb{Z}$ (any $p|m$) contradicts (7.23).

It follows that for each $s\ \exists$ an $f_s \in R$ with $f_s(s) = 1$. Therefore

$$\prod_{s \in S} (1_S - f_s) = 0$$

so

$$1_S = \sum_{T \subset S} (-1)^{|T|-1} \prod_{s \in T} f_s \in R$$

□

Exercise 249. If G acts on a finite set X transitively, and $x \in X$ and $U = G_x$ is stabilizer of x, then for each $g \in G$,

$$1_U^G(g) = |X^{\langle g \rangle}|$$

the number of fixed points of the cyclic subgroup $\langle g \rangle$.

Lemma 250. *Let U and V be subgroups of G, then*

$$(I_U^G)(I_V^G) = \sum a_w 1_w^G$$

with all $a_W = a_{U,V,W}$ integers ≥ 0, the sum over certain $W = U^{g_1} \cap V^{g_2}$.

Proof. Given actions of G on finite sets X, Y we get an action of G on the Cartesian product $X \times Y$ by $g(x, y) = (gx, gy)$. Even if the actions on X, Y are transitive, the action on $X \times Y$ usually is not. But we may split it up into orbits Z on each of which the action is transitive:

$$X \times Y = \sum_{Z \in G \backslash X \times Y} Z$$

For each $g \in G$, we have $g(x, y) = (x, y) \iff gx = x$ and $gy = y$, so

$$|X^{\langle g \rangle}||Y^{\langle g \rangle}| = |(X \times Y)^{\langle g \rangle}| = \sum_{Z \in G \backslash X \times Y} |Z^{\langle g \rangle}| \tag{7.24}$$

Now take $X = G/U$ and $Y = G/V$, for each Z, pick $(x, y) \in Z$. Easily seen $G_{(x_1,y_2)} = G_{x_1} \cap G_{y_2}$ and $G_{x_1} = U^{g_1}$and $G_{y_2} = V^{g_2}$ for some $g_1, g_2 \in G$. Thus we get the action on Z equivalent to the action by left translation on G/N with $W = U^{g_1} \cap V^{g_2}$. Combined with (7.24), and exercise 249 gives the result. □

Lemma 251. *For each finite group G and each prime p, there is a quasi-elementary subgroup U for which*

$$1_U^G(g) \not\equiv 0 \ mod\ p \tag{7.25}$$

Proof. Let C be the largest subgroup of $\langle g \rangle$ for which $\langle g \rangle / C$ is a p group. Let H be the normalizer of C in G, i.e.

$$h \in H \iff C^h = C$$

Clearly $g \in H$, let U/C be a Sylow p subgroup of H/C, chosen to contain the p subgroup $\langle g \rangle / C$

Since $C \lhd U$, U/C is a p group and $p \nmid |C|$, we see that U is quasi-elementary. It remains to prove 7.25.

We know that

$$1_U^G(g) = |(G/U)^{\langle g \rangle}|$$

now

$$ghU = hU \iff \langle g \rangle^{h^{-1}} \subset U \implies C^{(h^{-1})} \subset U \implies C^{(h^{-1})} = C \implies h \in H$$

Therefore

$$\left|(G/U)^{\langle g \rangle}\right| = \left|(H/U)^{\langle g \rangle}\right|$$

In the action of $\langle g \rangle$ on H/U, the subgroup C acts trivially, since

$$h \in H \implies ChU = hC^{h^{-1}}U = hCU = hU$$

therefore

$$\begin{aligned} \left|(H/U)^{\langle g \rangle}\right| &= \left|(H/U)^{\langle g \rangle / C}\right| \\ &\equiv |H/U| \not\equiv 0 \bmod p \end{aligned}$$

we used the facts that $\langle g \rangle / C$ is a group and U/C is a Sylow subgroup of H/C. □

Exercise 252. Show that each subgroup of a quasi-elementary group is quasi-elementary.

Proof. (of theorem 247) let R be the set of all $\mathbb{Z}$ linear combination of functions on G of the form 1_U^G with U quasi-elementary. Clearly R is an additive subgroup of $m(G, \mathbb{Z})$. Lemma 250 combined with experience 252 shows that R is closed under multiplication. Lemma 251 shows that the hypotheses of lemma 248 is satisfied, thus

$$1 = 1_G \in R$$

□

7.6 Supersolvable Groups

Lecture 21 (4/22/13)

Definition 253. A finite group G is supersolvable if either $G = 1$, or G has a normal subgroup P of prime order with G/P supersolvable.

Exercise 254. Prove by induction:

1) Each abelian group is supersolvable.

2) Each p group is supersolvable

3) Each quasi-elementary group is supersolvable

4) Each supersolvable group is solvable.

Example 255. If G is a non abelian group of order 12 with a normal Sylow 2 subgroup

$$G_2 \simeq C_2 \times C_2$$

then G is not supersolvable. In fact each G_3acts on G_2 by permuting the three subgroups of order 2 cyclic. Therefore $G_3 \not\lhd G$, and no subgroup of order 2 is normal in G either. Explicit take G to be the group of symmetries of a regular tetrahedron, consisting of three 180^0 rotations about lines through centers of opposite edges, eight 120^0 or 240^0 rotations about lines through vertices and centers of opposite faces, and 1.

Theorem 256. *Each subgroup and each factor group of a supersolvable group is supersolvable.*

Proof. (By induction on $|G|$) If $G = 1$, clear. If $G \neq 1$, let $P \lhd G$ with $|P| = p$ and G/P supersolvable.

Let H be a subgroup of G, then $H \cap P = 1$ or P. If $H \cap P = 1$, then $H \simeq HP/P$, a subgroup of G/P, so supersolvable by induction. If $H \cap P = P$ i.e. $H \supset P$ so H/P is a subgroup of G/P, so H/P is supersolvable by induction, so H is supersolvable by induction.

Let N be a normal subgroup of G then $N \cap P = 1$ or P.

If $N \cap P = 1$, then $NP/N \simeq P$ also $NP \lhd G$, so

$$(G/N)/(NP/N) \simeq G/NP \simeq (G/P)/(NP/P)$$

a factor group of a smaller supersolvable group so supersolvable by induction.

Therefore G/N is supersolvable, by induction.

If $N \cap P = P$, i.e. $N \supset P$, so $G/N \simeq (G/P)/(N/P)$ a factor group of a smaller supersolvable group so supersolvable by induction. □

Theorem 257. *(Zassenhaus 1930s) let $N \lhd G$ with G/N supersolvable. For each $\chi \in \hat{G}$,$\psi \in \hat{N}$ with $\psi \in \chi_N$ there is a subgroup $U \supset N$ and a $\xi \in \hat{U}$ with*

$$\xi^G = \chi \text{ and } \xi_N = \psi$$

Proof. (By induction on $|G/N|$) if $G = N$ clear. If $G \neq N$ let $M/N \lhd G/N$ with $|M/N| = p$ and G/M supersolvable.

$$G/M \simeq (G/N)/(M/N)$$

If $\psi \in \hat{N}^M$, then by theorem 209 or theorem 210 ψ extends to a character ${}^M\psi$ of M which by theorem 206 may be chosen $\in \chi_M$. By induction

there is a subgroup $U \supset M$ and a $\xi \in \hat{U}$ with $\xi^G = X$ and $\xi_M =^M \psi$, so $\xi_N = \psi$.

If $\psi \notin \hat{N}^M$, then $\psi \notin \hat{N}^G$ so $G_\psi \neq G$ By Clifford's theorem there is a $\xi \in G_\psi$ with $\xi^G = \chi$ and $\psi \in \xi_N$. Since G_ψ/N a supersolvable, induction gives U with $N \subset U \subset G_\psi$ and $\xi \in \hat{U}$ with $\xi^{G_\psi} = \xi$ and $\xi_N = \psi$.

By transitivity of induction

$$\xi^G = (\xi^{G_\psi})^G = \chi$$

□

Lemma 258. *For each subgroup $H \subset G$, each class function θ on G and each class function ψ on H, we have*

$$(\psi^G)\theta = (\psi\theta_H)^G$$

Proof. For each class function θ_1 on G,

$$\langle \psi^G\theta, \theta_1\rangle_G = \langle \psi^G, \bar{\theta}\theta_1\rangle_G = \langle \psi, (\bar{\theta}\theta_1)_H\rangle_H = \langle \psi\theta_H, \theta_1\rangle_H = \langle (\psi\theta_H)^G, \theta_1\rangle$$

the second equality is by Frobenius reciprocity. It follows that

$$\langle \psi^G\theta - (\psi\theta_H)^G, \theta_1\rangle = 0$$

for each class function θ_1 on G, in particular for $\theta_1 = \psi^G\theta - (\psi\theta_1)^G$, so that $\theta_1 = 0$. □

Theorem 259. *Let $N \triangleleft G$ and $\psi = \hat{N}^G$, put $F = G/N$ Assume that for each subgroup $U \supset N$ for which $U/N \in \tilde{\xi}(F)$ there is a ${}^U\psi \in \hat{U}$ with ${}^U\psi_U - \psi$, and that these "partial extensions ${}^U\psi$" can be chosen coherently, i.e. so that*

$$({}^U\psi)^g = W_\psi \quad \forall \text{ such } U, \forall\, g \in G$$

$$({}^U\psi)_W = W_\psi \quad \forall \text{ such } U \supset W \supset G$$

Then ψ extends to a unique $\chi \in \hat{G}$ satisfying

$$\chi_U =^U \psi \quad \forall \text{ such } U \tag{7.26}$$

Proof. There is certainly a unique class function χ on G satisfying (7.26). Since even that $U \supset N$ with U/N cyclic cover G (since the cyclic U/N cover F). By Solomon's theorem applied to F,

$$1_F = \sum_{E \in \tilde{\xi}(F)} a_E 1_E^F \quad \text{for certain } a_E \in \mathbb{Z}$$

It follows that

$$1_G = \sum_{U/N \in \tilde{\xi}(F)} a_U 1_U^G \quad \text{with } a_U = a_{U/N} \tag{7.27}$$

Let χ be the class function on G satisfying (7.26). Then

$$\chi = 1_G \chi = \sum_U a_U 1_U^G \chi = \sum_U a_U (1_U \chi_U)^G = \sum_U a_U ({}^U\psi)^G \tag{7.28}$$

the third equality is by lemma 258 and the last equality is by (7.27). It follows from (7.28) that χ is a generalized character, i.e. a $\mathbb{Z}$ linear combination of irreducible characters of G.

We will show that $\langle \chi, \chi \rangle_G = 1$, forcing χ or $-\chi \in \hat{G}$. Since $\chi_N = \psi$ the case $U = N$ of (7.26) we will then have $\chi \in \hat{G}$. From (7.28)

$$\langle \chi, \chi \rangle_G = \sum_{U,V} a_U a_V \left\langle ({}^U\psi)^G, ({}^V\psi)^G \right\rangle_G \tag{7.29}$$

By reciprocity

$$\left\langle ({}^U\psi)^G, ({}^V\psi)^G \right\rangle_G = \left\langle {}^V\psi, (({}^V\psi)^G)_U \right\rangle_U \tag{7.30}$$

Since

$$({}^V\psi)^G = \sum_{g \bmod V} (({}^V\psi)^0)^g = \sum_{g \bmod V} ({}^{V^g}\psi)^0$$

$$\begin{aligned} \left\langle {}^V\psi, (({}^V\psi)^G)_U \right\rangle_U &= \sum_{g \bmod V} \left\langle {}^V\psi, ({}^{V^g}\psi)^0 \right\rangle_U \\ &= \sum_{g \bmod V} \left\langle {}^W\psi, {}^W\psi \right\rangle_W \frac{1}{(U:W)} \quad \text{with } W = U \cap V^g \\ &= \sum_{g \bmod V} \frac{1}{(U:W)} \end{aligned} \tag{7.31}$$

The second equality is by coherence and the last equality is by irreducibility of ${}^W\psi$. Combining (7.29), (7.30), (7.31)

$$\langle \chi, \chi \rangle_G = \sum_{U,V} a_U a_V \sum_{g \bmod V} \frac{1}{(V:W)} \tag{7.32}$$

Since (7.32) holds equally for $\psi = 1$ (with all ${}^U\psi = 1$ and $\chi = 1$), we conclude that

$$\langle \chi, \chi \rangle_G = \langle 1, 1 \rangle_G = 1$$

□

Theorem 260. *Let $N \triangleleft G$ and $\psi \in \hat{N}^G$. Put $F = G/N$ Assume that*

a) $(d_\psi, |F|) = 1$

b) $\det \psi$ *extends to a (degree 1) character* δ *of* G.

Then there is a unique $\chi \in \hat{G}$ *for which* $\chi_N = \psi$ *and* $\det \chi = \delta$.

Proof. Granted for a moment the existence of such a χ we show that uniqueness: The,l most general extension of ψ to a character of G is $w\chi$ with $w \in \hat{F}$, $d_w = 1$. We have $\det(w\chi) = w^{d_\chi} \det \chi = w^{d_\chi}\delta$, so if also $\det(w\chi) = \delta$, then $w^{d_\chi} = 1$. Since $w : F \to \mathbb{C}^\times$ has order dividing $|F|$, condition a) implies $w = 1$.

Next we prove (260) for this case in which F is supersolvable, bu induction on $|F|$. If $F = 1$, put $\chi = \psi$. If $F \neq 1$, there is a normal subgroup M/N of prime order in F, for which $G/M = (G/N)/(M/N)$ is supersolvable. By theorem 210, since $\psi \in \hat{N}^M$, ψ extends to a character of M. By the previous paragraph there is just one such extension ${}^M\psi$ with $\det({}^M\psi) = \delta_M$. Since $\delta_M \in \hat{M}^G$ we conclude that ${}^M\psi \in \hat{M}^G$ By induction there is a unique $\chi \in \hat{G}$ with $\chi_M = {}^M\psi$ so $\chi_N = \psi$ and $\det \chi = \delta$.

Finally the general case: since quasi-elementary subgroups are supersolvable, ψ has a unique extension ${}^V\psi \in \hat{U}$ for which $\det({}^V\psi) = \delta_V$. Coherence of those ${}^V\psi$ follows easily from this uniqueness, thus ψ extends to a $\chi \in \hat{G}$, by theorem 259. □

Exercise 261. Justify the last sentence of the proof in details.

Lemma 262. *Let $N \triangleleft G$, $\lambda \in \hat{N}^G$ with $d_\lambda = 1$, put $F = G/N$. If $(o_w, |F|) = 1$, then λ extends uniquely to a $\mu \in \hat{G}$ with $d_\mu = 1$ and $o_\mu = o_\lambda$.*

Proof. We may suppose that $k = \ker \lambda = 1$. Thus $o_\lambda = |N|$, so N is a normal Hall subgroup of G. By Schur-Zassenhaus

$$G = NH \text{ with } N \cap H = 1 \text{ for some subgroup } H \simeq F$$

Define $\mu : G \to \mathbb{C}^\times$ by

$$\mu(nh) = \lambda(n) \ \forall\, n \in N, h \in H$$

Thus $\mu_N = \lambda$ and $\mu \in \hat{G}$ since [1]

$$\mu(n_1hnh_1) = \mu(nn_1^h hh_1) = \lambda(nn_1^h) = \lambda(n)\lambda(n_1) = \mu(n_1h)\mu(nh_1)$$

[1] "mehr der Setzer als der leser zulieben"

using $\lambda \in \hat{N}^G$ at the third equality. Clearly this μ has $o_\mu = o_\lambda$.The most general extension of λ is $w\mu$ with $w \in \hat{F}$, so the condition $o_{w\lambda} = o_\lambda$ implies $w = 1$. □

Theorem 263. *(Isaacs) Let $N \triangleleft G$, $\psi \in \hat{N}^G$ and put $F = G/N$ Assume*

1) $(d_\psi, |F|) = 1$

2) $(o_\psi, |F|) = 1$

Then there is a unique $\chi \in \hat{G}$ for which $\chi_N = \psi$ and $o_\chi = o_\psi$. (where o_ψ is the order of $\det \psi$.)

Proof. By lemma 262, $\det \psi$ extends to a character δ of G with $d_\delta = 1$ and $o_\delta = o_\lambda$. By theorem 260 ψ extends to $\chi \in \hat{G}$ with $\det \chi = \delta$... □

Exercise 264. Finish the proof.

8 Introduction to the Glauberman Correspondence

Lecture 22 (4/24/13)

Notation 265. In the section, $\mathcal{G}$ is a finite group with a normal Hall subgroup G and complementary subgroup A. Since A normalizes G, A acts on G by conjugation. Since $(gh)^a = g^a h^a$ for $g, h \in G$, $a \in A$, the action of G on A is a homomorphism from A into $AutG$, the group of automorphism of G.

8.1 Glauberman Theorem

Definition 266. We say that A operates on G if there is given a homomorphism $A \to AutG$.

Exercise 267. Prove if A operates on G, then A acts on $\check{G}$ and on $\hat{G}$.

Theorem 268. *(Glanberman, 1968) If $\mathcal{G}$ is a finite group with a normal Hall subgroup G, and A is a complement to G in $\mathcal{G}$, then provided A is solvable, the actions of A on $\check{G}$ and on $\hat{G}$ are equivalent.*

Remark 269. This equivalence, i.e. a bijection $\check{G} \to \hat{G}$ commuting with the action by A is not canonical, any more than any bijection $\check{G} \to \hat{G}$ is canonical (case $\mathcal{G} = G$).

The proof of Glanberman depends on two others:

Theorem 270. *With the same hypotheses in Glanberman, there is a bijection $\check{G}^A \to \check{G^A}$, i.e. from the set of those classes of G fixed by A to the set of all classes of $G^A = C_G(A)$.*

Theorem 271. *With the same hypotheses in Glanberman, there is a bijection $\hat{G}^A \to \hat{G^A}$, i.e. from the set of those irreducible characters of G fixed by A to the set of all irreducible characters of $G^A = C_G(A)$.*

Proof. (of Glanberman) we have

$$|\check{G}^A| = |\check{G^A}| = |\hat{G^A}| = |\hat{G}^A|$$

i.e. G has equally many classes fixed by A as irreducible characters fixed by A. The first and last equalities are given by theorems 270, 271. The middle is by Frobenius applied to G^A. Replacing $\mathcal{G} = GA$ in this by GB for each subgroup $B \subset A$ gives $|\check{G}^B| = |\hat{G}^B|$, $\forall\, B$. Therefore by Burnsides equivalence criterion theorem 42, the actions of A on $\check{G}$ and on $\hat{G}$ are equivalent. □

The proof of theorem 270 depends on the remarkable lemma:

Lemma 272. *(Glanberman's lemma) Let $\mathcal{G}$ have a normal Hal subgroup G and complement A. If $\mathcal{G}$ acts on a finite set X with G acting transitively, then*[2]

1) $X^A \neq \varnothing$

2) G^A acts transitively on X^A.

Glanberman's lemma is regarded the greatest thing 30 years later follows from Schur-Zassenanis theorem. To prove Glanberman's lemma we need complete statement of Schur-Zassenanis theorem.

Theorem 273. *(Schur-Zassenanis) If G has a normal Hall subgroup H, then*

1) G has a subgroup M complementary to N;

2) any two complements to N are conjugate.

[2]provided either A or G is solvable. In 1963 Feit and Thompson, setting an old conjecture of Burside, proved that each group of odd order is solvable. By this deep result, the proviso is always satisfied, since not both $|A|$ and $|G|$ can be even.

Proof. (of Glanberman's lemma)

1) Let $x \in X$ and let $\mathcal{G}_x$ and G_x be the stabilizers of x in $\mathcal{G}$ and G. Clearly $G \cap \mathcal{G}_x = G_x$. Since both $\mathcal{G}$ and G act transitively, both $|\mathcal{G}/\mathcal{G}_x|$ and $|G/G_x|$ are $|X|$, so the those two indices are equal.

$$\begin{array}{cc} \mathcal{G} & G \\ | & | \\ \mathcal{G}_x & G_x \end{array}$$

Since the indices $\backslash^a$ are equal, it follows that $\mathcal{G} = G\mathcal{G}_x$. Since the indices $/^b$ are equal, it follows that $\mathcal{G}_x/G_x = \mathcal{G}/G \simeq A$.

$$\begin{array}{ccccc} & & \mathcal{G} & & \\ & & | & & \\ & & G\mathcal{G}_x & & \\ & /^b & & \backslash^a & \\ G & & & & \mathcal{G}_x \\ & \backslash^a & & /^b & | \\ & & G \cap \mathcal{G}_x & & | \\ & & | & & | \\ & & G_x & & M \\ & & | & / & \\ & & 1 & & \end{array}$$

Therefore G_x is a normal Hall subgroup of $\mathcal{G}_x$.

By theorem 2731), there is a complement M to G_x in $\mathcal{G}_x$ Since $M \simeq \mathcal{G}_x/G_x$, it follows that M is also a complement to G in $\mathcal{G}$. By theorem 2732), M is conjugate to A in $\mathcal{G}$, i.e. fro some $ga \in \mathcal{G}$, $M = A^{ga} = A^g$, so $A \subset M^{g^{-1}}$. Since $M \subset \mathcal{G}_x$ we get $A \subset \mathcal{G}_x^{g^{-1}} = \mathcal{G}_{g^{-1}x}$, showing $g^{-1}x \in X^A$, so $X^A \neq \varnothing$.

2) Let $x', x \in X^A$. Since G is transitive on X, we have $g_0 x' = x$ for some $g_0 \in G$, Put

$$Y = \{g \in G : gx' = x\} \text{ i.e. } Y = G_x g_0 \tag{8.1}$$

We need the following claim by Sablemma: GA acts on G semi directly via $ga * g_1 = gg_1^a$.

Proof of claim: The multiplication in the semi direct product GA is

$$(ga)(hb) = gaha^{-1}ab = gh^a ab \; \forall \, g, h \in G \; a, b \in A$$

Thus from (8.1), $\forall\, g_1 \in G$

$$((ga)(hb)) * g_1 = (gh^a ab) * g_1 = gh^a g_1^{ab} = g(hg_1^b)^a = (ga) * ((hb) * g_1)$$

also $(1 \cdot 1) * g_1 = 1g_1^1 = g_1$ for all $g_1 \in G$. So we proved the claim.

It follows from $x \in X^A$ that A normalizes $G_x : G_x^a = G_{ax} = G_x \ \forall\, a \in A$. Therefore $G_x A$ is a group with a normal Hall subgroup G_x and complement A. This subgroup of GA also acts semi directly on G. In this action, Y is stable: For all $h \in G_x$, $a \in A$, $g \in Y$

$$(ha * g)x' = hg^a x' = haga^{-1}x' = hagx' = hahx = x$$

i.e. $ha * g \in Y$. In the action of $G_x A$ on Y, the subgroup G_x is transitive: In fact, for $g, g' \in G_x$ i.e. $g'g_0$, gg_0 any two elements of Y,

$$(g'g^{-1}1) * gg_0 = g'g^{-1}gg_0 = g'g_0$$

By part 1) applied to $G_x A$ acting on Y with G_x acting transitively, we conclude that $Y^A \neq \varnothing$, i.e. $\exists\, g \in Y$ with $(1a) * g = g$ i.e. $g^a = g\ \forall\, a \in A$, i.e. $g \in G^A$. Thus in the original action G^A acts transitively on X^A. □

We now prove theorem (270).

Proof. $\mathcal{G} = GA$ acts by conjugation on each $S \in \check{G}^A$ with G acting transitively, so by lemma 272 1) $S^A \neq \varnothing$, and by 2) G^A acts transitively on S^A, so $S^A \in \check{G}^A$. Since the S's are disjoint, the map $S \mapsto S^A$ from $\check{G}^A$ to $\check{G}^A$ is injective. For $h \in G^A$, $g \in G$, $a \in A$ we have $(h^g)^a = h^{(g^a)}$, so the class S of h in G is in $\check{G}^A$, so the map is surjective. □

We already stated and proved (1) of theorem 273 before. Now prove 2)

Proof. First the case with N abelian: For each complement M to N in G, we have $G/N = F \simeq M$. For $f \in F$, denote by $m(f)$ the unique element of M in the coset f. then $f \mapsto m(f)$ is an isomorphism from F to M.

If $\tilde{M}$ is another complement to N in G, we get another isomorphism $f \mapsto \tilde{m}(f)$ from F to $\tilde{M}$. Since $\tilde{m}(f)$ and $m(f)$ are in the same coset f, we have

$$n(f) = \tilde{m}(f)m(f)^{-1} \in N \qquad \forall\, f \in F \tag{8.2}$$

Thus we get a map $n : F \to N$. For $e, f \in N$

$$\begin{aligned} n(ef) &= \tilde{m}(ef)m(ef)^{-1} = \tilde{m}(e)\tilde{m}(f)m(f)^{-1}m(e)^{-1} \\ &= \tilde{m}(e)n(f)m(e)^{-1} = \tilde{m}(e)m(e)^{-1}n(f)^{m(e)} = n(e)n(f)^e \end{aligned}$$

Since N is abelian, $F = G/N$ acts by conjugation on N, $m(e)$ acting like e, justifying the last equality. Thus

$$n(ef) = n(e)n(f)^e \quad \forall\, e, f \in F$$

As before, using N abelian and $(|F|, |N|) = 1$, we can take the geometric mean of above

$$\prod_f n(ef) = n(e)^{|F|}(\prod_f n(f))^e \;\forall\, e \in F$$

so

$$\bar{n} = n(e)\bar{n}^e \quad \forall\, e \text{ with } \bar{n} = (\prod_f n(f))^{\frac{1}{|F|}} \tag{8.3}$$

From (8.2), (8.3) (with f in place of e),

$$\tilde{m}(f) = n(f)m(f) = \bar{n}(\bar{n}^f)^{-1}m(f) = \bar{n}m(f)\bar{n}^{-1} = m(f)^{\bar{n}} \;\forall\, f \in F$$

from which $\tilde{M} = \tilde{m}(F) = m(F)^{\bar{n}} = M^{\bar{n}}$, so $\tilde{M}$ is conjugate to M by $\bar{n}$.

Next the case of N solvable, by induction on $|N|$. We may suppose $N \neq 1$. Let K be a minimal characteristic subgroup of N. Thus KM/K and $K\tilde{M}/N$ complement N/K in G/K. Since N/K is a normal Hall subgroup of G/K , induction gives $K\tilde{M}/K = (KM/K)^{gK}$ for some $gK \in G/K$, i.e. $K\tilde{M} = KM^g$, so $\tilde{M}$ and M^g are complements to K in $K\tilde{M}$, the abelian case implies $\tilde{M}$ and $M^g$are conjugate in $K\tilde{M}$, so $\tilde{M}$ and M are conjugate in G.

Finally, the case of G/N solvable by induction on $|G/N|$. We may suppose $G/N \neq 1$. Let L/N be a minimal normal subgroup of G/N. Thus $1 \neq L/N \lhd G/N$. Let both M and $\tilde{M}$ complement N in G. Then $L \cap M$ and $L \cap \tilde{M}$ complement N in L. By minimality L/N is an abelian p group for some prime p, so $L \cap M$ and $L \cap \tilde{M}$ are Sylow p subgroups of L, from which $L \cap \tilde{M} = L \cap M^l$ for some $l \in L$.

Clearly $L \cap \tilde{M} \lhd \tilde{M}$ and $L \cap M^l \lhd M^l$, since $L \lhd G$. It follows that both $\tilde{M}$ and M^l normalize $D = L \cap \tilde{M}$. Letting it be the normalizer of D in G, we have $\tilde{M}$ and $M^l \subset H$, and $\tilde{M}/D$ and M^l/D complement the normal Hall subgroup $(N \cap H)D/D$ of H/D. By induction, since $\tilde{M}/D \simeq G/L$ is smaller than G/N, we have $\tilde{M}/D$ and M^l/D conjugate in H/D, so $\tilde{M}$ is conjugate to M^l and therefore to M in G. □

Exercise 274. Show that $(N \cap H)D/D$ is a normal Hall subgroup of H/D, complemented by $\tilde{M}/D$. Hint: show if H is a Hall subgroup of G, and $N \lhd G$, then HN/N is a Hall subgroup of G/N, and $H \cap N$ is a Hall subgroup of N. If N is a normal Hall subgroup of G, and H is a subgroup then $H \cap N$ is a normal Hall subgroup of H.

8.2 Character Correspondence

Lecture 23 (4/29/13)

To prove theorem (271), we use some technique studied earlier. Recall the functional equation which characterize the elements of $\hat{G}$. To express this simply, we used $c_\chi = |G|/d_\chi \in \mathbb{N}$ for the co degree of χ.

We learned before

Lemma 275. *Let $\theta : G \to \mathbb{C}$ and assume $\theta \neq 0$ then*

$$\theta = c_\chi \chi \text{ for some } {}^!\chi \in \hat{G}$$

iff

$$\theta(g)\theta(g') = \sum_{h \in G} \theta(g^h g') \quad \forall\, g, g' \in G \tag{8.4}$$

Theorem 276. *(Navarro 1989) Let $\theta : G \to \mathbb{A}_m$, m is any multiple of $|G|$, θ a class function, p prime, $p \nmid \theta(1)$. If*

$$\theta(g)\theta(g') \equiv \sum_{h \in G} \theta(g^h g') \bmod p \quad \forall\, g, g' \in G \tag{8.5}$$

and

$$\theta(g)^k = \theta(g^k) \forall\, g \in G \forall\, k \in \mathbb{Z} \text{ with } (k, m) = 1 \tag{8.6}$$

then

$$\theta \equiv c_\chi \chi \bmod p \text{ for some } {}^!\chi \in \hat{G}. \tag{8.7}$$

Remark 277. It follows from $p \nmid \theta(1)$ and (8.5) with $g = g' = 1$ that $\theta(1) \equiv |G| \bmod p$ so $p \nmid |G|$.

Proof. For each $F : G \times G \to \mathbb{C}$ change of variables gives

$$\sum_{g' \in G} F(fg', g') = \sum_{g'' \in G} F(g'', f^{-1} g'') \quad \forall\, f \in G$$

Put $F(u, v) = \theta(u)\bar{\chi}(v)$ for any $\chi \in \hat{G}$ replace f by g^h and sum on h:

$$\sum_{g', h \in G} \theta(g^h g')\bar{\chi}(g') = \sum_{g'', h \in G} \theta(g'')\bar{\chi}(g^{-h} g'') \; \forall\, \chi \in \hat{G} \, \forall\, g \in G$$

Using (8.5) on the h sum on the left and (8.4) on the h sum on the right gives

$$\langle |G|\theta, \chi \rangle_G \, \theta(g) \equiv \langle |G|\theta, \chi \rangle \, c_\chi \chi(g) \bmod p \quad \forall\, \chi \in \hat{G}, \forall\, g \in G \tag{8.8}$$

Using (8.6) we show next that

$$\langle |G|\theta, \chi\rangle_G \in \mathbb{Z} \quad \forall\, \chi \in \hat{G}$$

Since both θ and χ take values in $\mathbb{A}_m$, this scalar product is in $\mathbb{A}_m$. For $k \in \mathbb{Z}$ with $(k, m) = 1$, (8.6) gives

$$\langle |G|\theta, \chi\rangle^{(k)} = \sum_g \theta^{(k)}(g)\bar{\chi}(g)^{(k)} = \sum_g \theta(g^k)\bar{\chi}(g^k) = \langle |G|\theta, \chi\rangle$$

It follows from Galois theory, that

$$\langle |G|\theta, \chi\rangle \in \mathbb{Q} \cap \mathbb{A} = \mathbb{Z}$$

Since θ is a class function,

$$|G|\theta = \sum \langle |G\theta, \chi\rangle\, \chi$$

In particular

$$|G|\theta(1) = \sum \langle |G\theta, \chi\rangle\, d_\chi$$

Since by the remark 277, $p \nmid |G|\theta(1)$, we must have

$$\langle |G|\theta, \chi\rangle \not\equiv 0 \bmod p \text{ for some } \chi \in \hat{G}$$

Using above we may cancel $\langle |G|\theta, \chi\rangle$ from the congruence (8.8), giving (8.7) except for the uniqueness of χ.

If also $\theta \equiv c_{\chi'}\chi'$ with $\chi' \in \hat{G}$ and $\chi \neq \chi'$ then $c_\chi\chi \equiv c_{\chi'}\chi' \bmod p$, so

$$|G|c_\chi^2 = \sum_g c_\chi\chi(g)c_\chi\bar{\chi}(g) \equiv \sum_g c_{\chi'}\chi'(g)c_{\chi'}\bar{\chi}(g) = c_\chi c_{\chi'}|G|\left\langle \chi, \chi'\right\rangle = 0$$

First and last equalities are by orthogonality, thus p divides $|G|c_\chi^2$, which divides $|G|^3$, so $p \mid |G|$, contradiction. □

Lemma 278. *Let A be a p group acting on a finite set X. If A fixes a map $\theta : X \to A$, i.e. θ is constant on each A orbit of X, then*

$$\sum_{x \in X^A} \theta(x) \equiv \sum_{x \in X} \theta(x) \ \textit{mod}\ p$$

Remark 279. The case $\theta = 1$ gives the standard Fermat lemma: $|X^A| \equiv |X| \bmod p$.

Proof. Each A orbit on $X - X^A$ has size $\equiv 0 \bmod p$, so contributes 0 mod p to the right side. □

The proof of theorem 271 will be reduced by induction to the case in which A is a group. In this case there is a more precise statement:

Theorem 280. *Let $\mathcal{G} = GA$ with $G \lhd \mathcal{G}$, $G \cap A = 1$, A a p group and $p \nmid |G|$. We abbreviate $G^A = C_G(A)$, which will come up often, by H, then*

1) For each $\chi \in \hat{G}^A$ there is a unique $\psi \in \hat{G^A} = \hat{H}$ satisfying

$$(c_\chi \chi)_H \equiv c_\psi \psi \ mod\ p \tag{8.9}$$

2) The map $\chi \to \psi$ bijects $\hat{G}^A$ to $\hat{G^A}$

3) There is a map $\epsilon : \hat{G}^A \to \{\pm 1\}$ so that

$$\left\langle \chi_H, \psi' \right\rangle_H \equiv \begin{cases} \epsilon(\chi) & \psi = \psi' \\ 0 & \psi \neq \psi' \end{cases} \ mod\ p$$

Proof. 1) Given $\chi \in \hat{G}$, put $\theta = c_\chi \chi$, then

$$\theta(g)\theta(g') = \sum_{h \in G} \theta(g^h g') \quad \forall\, g, g' \in G \tag{8.10}$$

If $\chi \in \hat{G}^A$, then $\theta^a = \theta$ for all $a \in A$, so $\forall\, g, g' \in G^A$

$$\theta(g^h g') = \theta((g^h g')^a) = \theta(g^{(h^a)} g') \quad \forall\, a \in A$$

i.e. the summand in (8.10), as a function of h, is fixed by A. By lemma 278

$$\theta(g)\theta(g') \equiv \sum_{h \in G^A} \theta(g^h g') \bmod p \ \forall\, g, g' \in G^A$$

Thus θ_H satisfies (8.5) with G replaced by G^A. Clearly $p \nmid \theta_H(1)$, θ_H is a class function, and θ_H satisfies (8.6), so we have (8.9).

2) Multiply (8.9) by $\bar{\psi}$ and sum over H:

$$c_\chi |H| \left\langle \chi_H, \psi' \right\rangle_H \equiv c_\psi |H| \left\langle \psi, \psi' \right\rangle_H \mod p \tag{8.11}$$

$\forall\, \chi \in \hat{G}^A$, $\forall\, \psi' \in \hat{H}$. Since $p \nmid c_\chi |H|$, it follows that ψ is unique $\psi' \in \hat{H}$ with $\langle \chi_H, \psi \rangle \not\equiv 0 \bmod p$. Now let $\chi, \chi' \in \hat{G}^A$, corresponding to $\psi, \psi' \in \hat{H}$ by 1). By lemma (278),

$$\sum_{g \in G} \bar{\chi}\chi'(g) \equiv \sum_{g \in H} \bar{\chi}\chi'(g) \bmod p$$

which with 1) for χ and for χ'.

$$c_\chi c_{\chi'} |G| \left\langle \chi, \chi' \right\rangle_G \equiv c_\psi c_{\psi'} |H| \left\langle \psi, \psi' \right\rangle_H \mod p \tag{8.12}$$

Since the codegrees and group orders are relatively prime to p, it follows that

$$\chi \neq \chi' \implies \left\langle \chi, \chi' \right\rangle_G = 0 \implies \left\langle \psi, \psi' \right\rangle_H \equiv 0 \mod p \implies \left\langle \psi, \psi' \right\rangle_H \neq 1 \implies \psi \neq \psi'$$

Thus the map is injective.

Next show the map is surjective. Suppose $\psi' \in \hat{G^A}$ is not in the image of this map. Then by 1)

$$\left\langle \chi_H, \psi' \right\rangle_H \equiv 0 \mod p \, \forall \, \chi \in \hat{G}^A$$

Let $\xi = \psi'^G$, then

$$\xi = \sum_{\chi \in \hat{G}} \langle \xi, \chi \rangle_\chi = \sum_{\chi \in \hat{G}} \left\langle \chi_H, \psi' \right\rangle_H \chi$$

so

$$(G : H) d_\psi = \xi(1) = \sum_{\chi \in \hat{G}} \left\langle \chi_H, \psi' \right\rangle_H d_\chi \equiv \sum_{\chi \in \hat{G}^A} \left\langle \chi_H, \psi' \right\rangle d_\chi \equiv 0 \mod p$$

a contradiction, since $p \nmid |G|$ and $(G : H) d_\psi \mid (G : H)|H| = |G|$. The application of lemma 278 is justified since $d_\chi a = d_\chi$ and $(\chi^a)_H = (\chi_H)^a = \chi_H$.

3) Finally we show the map $\chi \mapsto \psi$ from $\hat{G}^A$ to H satisfies

$$\langle \chi_H, \psi \rangle_H \equiv \pm 1 \mod p \tag{8.13}$$

In fact from 8.12 with $\chi = \chi'$,

$$c_\chi^2 |G| \equiv c_\psi^2 |H| \mod p$$

Since $|G| \equiv |G^A| = |H| \mod p$ and $p \nmid |G|$, this yields $c_\chi^2 \equiv c_\psi^2 \mod p$, so $c_\chi \equiv \pm c_\psi \mod p$, which with (8.11) with $\psi = \psi'$ gives (8.13). □

Lemma 281. *If a group A acts on a set X and $B \triangleleft A$, put $C = A/B$. Then A stabilizes X^B with kernel $\supset B$, so C acts on X^B also $X^A = (X^B)^C$.*

Proof. Let $x \in X^B$, for $a \in A$, $b \in B$ we have $b^{a^{-1}} \in B$, so

$$(x^a)^b = x^{ba} = x^{aa^{-1}ba} = (x^{(b^{a^{-1}})})^a = x^a$$

showing $x^a \in X^B$. Thus A stabilizes B.

For $b \in B$ and $x \in X^B$we have $x^b = x$ so b is in the kernel of the action of A on X^B. If $x \in X^A$, then $x \in X^B$ and C also fixes x, showing $X^A \subset (X^B)^C$ vice versa, if $x \in (X^B)^C$ then B fixes x so

$$x^a = x^{aB} = x^C = x$$

showing $(X^B)^C = X^A$. □

Now we can complete the proof of theorem 271.

Proof. To show $|\hat{G^A}| = |\hat{G^A}|$. For G a normal Hall subgroup of G with solvable complement A. If A is a p group, this follows from theorem 280 2), thus we may suppose that A is not a p group for any prime p. Let B be a minimal $\neq 1$ normal subgroup of A, then B is abelian so $B_p \neq 1$ for some prime p, so by minimality $B = B_p$ is a p group. with $1 \neq B \neq A$.

By lemma 281, $C = A/B$ acts on $\hat{G}^B$ and on $\hat{G^B}$. It will suffice to show that

$$\left|(\hat{G}^B)^C\right| = \left|(\hat{G^B})^C\right| \tag{8.14}$$

In fact using (8.14), induction on A, and lemma 281, we get

$$|\hat{G}^A| = \left|(\hat{G}^B)^C\right| = \left|(\hat{G^B})^C\right| = \left|\widehat{(G^B)^C}\right| = |\hat{G^A}|$$

So it remains to show (8.14). let $\chi \to \psi$ be the bijection from $\hat{G}^B$ to $\hat{G^B}$ of theorem 280 2) with A replaced by B. For $x \in \hat{G}^B$ and $a \in A$, we have $\chi^a \in \hat{G}^B$ by lemma 281. Since A stabilizes G^B, each $a \in A$ permutes G^B, so

$$\left\langle \chi^a_{G^B}, \psi^a \right\rangle_{G^B} = \langle \chi_{G^B}, \psi \rangle_{G^B} \not\equiv 0 \bmod p$$

so by theorem 280 2), $\chi^a \to \psi^a$, so $\chi^a = \chi \iff \psi^a = \psi$, i.e. the map $\chi \mapsto \psi$from $\hat{G}^B$ to $\hat{G^B}$ satisfies

$$\chi \in (\hat{G}^B)^C \iff \psi \in (\hat{G^B})^C$$

this bijection by restriction proving (8.14). □

9 Spherical Functions on Finite Groups

9.1 Spherical Functions

Lecture 24 (5/1/13)

First some properties of of convolution. For $\alpha, \beta : G \to \mathbb{C}$,

$$(\alpha * \beta)(g) = \frac{1}{|G|} \sum_{\substack{a,b \in G \\ ab = g}} \alpha(a)\beta(b) = \frac{1}{|G|} \sum_{h \in G} \alpha(gh^{-1})\beta(h)$$

Lemma 282. *For α,β, γ, $\xi : G \to \mathbb{C}$*

1) convolution is associative: $(\alpha * \beta) * \gamma = \alpha * (\beta * \gamma)$

2) class functions are commute: $\alpha * \xi = \xi * \alpha$ for all α iff ξ is a class function

3) connection with $\langle\ ,\ \rangle_G$: $(\alpha * \beta)(1) = \langle \alpha, \beta^\dagger \rangle$, $\beta^\dagger(g) = \overline{\beta(g^{-1})}$

Proof. 1) Each side evaluate at g to

$$\sum_{\substack{a,b,c \in G \\ abc = g}} \alpha(a)\beta(b)\gamma(c)$$

2) $\alpha * \xi = \xi * \alpha$ for all

$$\xi : G \to \mathbb{C} \iff \delta_c * \xi = \xi * \delta_c \tag{9.1}$$

$\forall\, c \in G$ with $\delta_c(x) = 1$ if $x = c$, 0 if $x \neq c$ we have

$$\begin{aligned} (\delta_c * \xi)(x) &= \xi(b) \text{ with } cb = a \\ &= \xi(c^{-1}x) \end{aligned}$$

$$\begin{aligned} (\xi * \delta_c)(x) &= \xi(a) \text{ with } ac = x \\ &= \xi(xc^{-1}) \end{aligned}$$

Putting $g = c^{-1}x$, i.e. $xc^{-1} = cyc^{-1} = y^c$, we see that (9.1) $\iff$ $\xi(x) = \xi(x^c)\ \forall\, x, c$.

3) $(\alpha*\beta)(1) = \frac{1}{|G|}\sum_{h\in G} \alpha(h)\beta(h^{-1}) = \frac{1}{|G|}\sum_{h\in G} \alpha(h)\overline{\beta(h^{-1})} = \langle \alpha, \beta^\dagger \rangle_G$ □

Remark 283. Each character χ of G satisfies $\chi^\dagger = \chi$.

Definition 284. Let G be a finite group, H a subgroup. For $\chi \in \hat{G}$, $\psi \in \hat{H}$ the corresponding spherical function

$$\psi_{\chi\psi} : G \to \mathbb{C}$$

is defined by

$$\begin{aligned} \psi_{\chi\psi}(g) &= \frac{1}{|H|}\sum_{h\in H}\chi(gh^{-1}\psi(h)) \\ &= \frac{1}{|G|}\sum \chi(gh^{-1})\psi^{\#}(h) \end{aligned} \tag{9.2}$$

with $\psi^{\#} = (G:H)\psi^{\circ}$; i.e. $\psi_{\chi\psi} = \chi * \psi^{\#}$.

Theorem 285. *For all G, H, χ, ψ put*

$$c_{\chi\psi} = \langle \chi_H, \psi\rangle_H = \left\langle \chi, \psi^G\right\rangle_G$$

1) $\psi_{\chi\psi}(1) = c_{\chi\psi}$.

2) $\bar{\psi}_{\chi\psi}(g) = \psi_{\bar{\chi}\bar{\psi}}(g) = \psi_{\chi\psi}(g^{-1})$ *i.e.* $\psi^\dagger_{\chi\psi} = \psi_{\chi\psi}$

3) $\psi_{\chi\psi}$ *is an H class function i.e.* $\psi_{\chi\psi}(g^h) = \psi_{\chi\psi}(g)\ \forall\, g \in G,\ h \in H$

4) $\psi_{\chi\psi} * \psi_{\chi'\psi'} = \frac{\delta_{\chi\chi'}\delta_{\psi\psi'}}{f_\chi f_\psi}\psi_{\chi\psi}\ \forall\, \chi, \chi' \in \hat{G},\ \forall\, \psi, \psi' \in \hat{H}$

5) $\left\langle \psi_{\chi\psi}, \psi_{\chi'\psi'}\right\rangle = \frac{\delta_{\chi\chi'}\delta_{\psi\psi'}}{f_\chi f_\psi}c_{\chi\psi}\ \forall\, \chi, \chi' \in \hat{G},\ \forall\, \psi, \psi' \in \hat{H}$

Proof. 1) By 3) lemma (282)

$$\psi_{\chi\psi}(1) = (\chi * \psi^{\#})(1) = \left\langle \chi, \psi^{\#}\right\rangle_G = \langle \chi_H, \psi\rangle_H = c_{\chi\psi}$$

since $(\psi^{\#})^\dagger = \psi^{\#}$.

2) The first equality follows from (9.1). The second equality is because

$$|H|\psi_{\chi\psi}(g^{-1}) = \sum_{h\in H}\chi(g^{-1}h^{-1})\psi(h) = \sum_{h\in H}\bar{\chi}(hg)\psi(h) = \overline{\sum_{h\in H}\chi(gh)\psi(h^{-1})} = |H|\bar{\psi}_{\chi\psi}(g)$$

3) Replace g by $g^{h_1}$and h be h^{h_1} in (9.2) and use that ψ and χ are H class function.

$$\psi_{\chi\psi}(g^{h_1}) = \frac{1}{|H|}\sum_{h\in H}\chi(g^{h_1}h^{h_1})\psi(h^{h_1}) = \frac{1}{|H|}\sum_{h\in H}\chi((gh^{-1})^{h_1})\psi(h^{h_1}) = \frac{1}{|H|}\sum_{h\in H}\chi(gh^{-1})\psi(h)$$

4) $\psi_{\chi\psi} * \psi_{\chi'\psi'} = \chi * \psi^{\#} * \chi' * \psi'^{\#} = \chi * \chi' * \psi^{\#} * \psi'^{\#} = \delta_{\chi\chi'} \frac{\chi}{d_\chi} * \delta_{\psi\psi'} \frac{\psi^{\#}}{d_\psi}$, because

$$\frac{1}{|G|} \sum_{\substack{a,b \in G \\ ab=g}} \psi^{\#}(a)\psi^{\#}(b) = \frac{(G:H)^2}{|G|} \sum_{\substack{a,b \in H \\ ab=g}} \psi(a)\psi'(b) = (G:H) g_{\psi\psi'} \frac{\psi^{\circ}(g)}{d_\psi} = \delta_{\psi\psi'} \frac{\psi^{\#}}{d_\psi}$$

5) $\left\langle \psi_{\chi\psi}, \psi_{\chi'\psi'} \right\rangle_G = (\psi_{\chi\psi} * \psi_{\chi'\psi'})(1) = \delta_{\chi\chi'}\delta_{\psi\psi'} \frac{\psi_{\chi\psi}(1)}{f_\chi f_\psi} = \frac{\delta_{\chi\chi'}\delta_{\psi\psi'}}{f_\chi f_\psi} c_{\chi\psi}$. □

Corollary 286. $\psi_{\chi\psi} = 0 \iff c_{\chi\psi} = 0$, *i.e. the nonzero spherical functions are for* $c_{\chi\psi} \neq 0$.

Corollary 287. *Since the nonzero spherical functions are orthogonal, they are linearly independent* H *class functions.*

Definition 288. The subgroup H is multiplicity-free in G if the $c_{\chi\psi}$ are 0 or 1.

Theorem 289. *The nonzero* $\psi_{\chi\psi}$*'s make a basis for the space of* H *class functions iff* H *is multiplicity free in* G.

Proof. The space of H class functions has the characteristic functions of the H classes as one basis, so the dimension of the space is the number of H class. By the orbit connecting formula this is

$$\frac{1}{|H|} \sum_{h \in H} |C_G(h)| = \frac{1}{|H|} \sum_{h \in H} \sum_{\chi \in \hat{G}} \chi(h)\bar{\chi}(h) = \sum_{\chi \in \hat{G}} \langle \chi_H, \chi_H \rangle_H = \sum_{\substack{\chi \in \hat{G} \\ \chi \in \hat{H}}} c_{\chi\psi}^2 \geq \sum_{c_{\chi\psi} \neq 1} 1$$

The second last step is by

$$\langle \chi_H, \chi_H \rangle_H = \left\langle \sum_{\psi \in \hat{H}} c_{\chi\psi}\psi, \sum_{\psi \in \hat{H}} c_{\chi\psi'}\psi' \right\rangle = \sum_{\psi \in \hat{H}} c_{\chi\psi}^2$$

The last inequality follows from $\iff$ all $c_{\chi\psi}$ are 0 or 1 $\iff$ H is multiplicity free in G. This is the case in which the number of nonzero $\psi_{\chi\psi}$'s equal the dimension of the space of H class functions i.e. the case in which the $\psi_{\chi\psi}$'s are a basis. □

Corollary 290. *If* H *is multiplicity free in* G, *then the* $\sqrt{d_\chi d_\psi}\psi_{\chi\psi}$*'s are an orthonormal basis for this space.*

Theorem 291. *If H is multiplicity free, then denoting by A the H class of g*

$$\sum_{\chi,\psi} d_\chi d_\psi \psi_{\chi\psi}(g)\bar{\psi}_{\chi\psi}(g') = \begin{cases} |G|/|A| & g' \in A \\ 0 & otherwise \end{cases}$$

Proof. Express the characteristic function of A in terms of the orthonormal basis of corollary (290). □

9.2 Spherical Function's Values and Properties

Lecture 25 -Last Lec- (5/6/13)

Notation 292. For each $\theta : G \to \mathbb{C}$ and subset $S \subset G$,

$$\theta(S) = \sum_{s\in S} \theta(s)$$

Theorem 293. *(Roester, Travis, 1970s) Given G, H, $\chi \in \hat{G}$, $\psi \in \hat{H}$ and an H class $B \subset G$,*

$$\psi_{\chi\psi}(B) = \mathbb{A} \tag{9.3}$$

Remark 294. (9.3) generalizes both $\chi(g) \in \mathbb{A}$ and $w_\chi(A) \in \mathbb{A}$ for $\mathbb{A} \in \check{G}$, to which (9.3) reduces in the special cases $H = 1$, $\psi = 1$ and $H = G$, $\chi = \psi$.

Exercise 295. For $a, b, d, e \in \mathbb{N}$ and $\gamma \in \mathbb{A}$, show

1) $d|a\gamma$ & $d|b\gamma \iff d|(a,b)\gamma$

2) $d|s\gamma \iff d/(d,s)|\gamma$

3) $d|\gamma$ & $e|\gamma \iff [d,e]|\gamma$

The fact that $w_\chi(A) \in \mathbb{A}$ may be written as

$$d_\chi \text{ divides } s_g\chi(g) \qquad \text{with } s_g \text{ the size of the } G \text{ class of } g \tag{9.4}$$

Equivalently using the exercise 2) above and (9.3) we get generalization

$$d_\chi \text{ divides } \chi(g) \qquad \text{with } m_{\chi,g} = d_\chi/(d_\chi, s_g) \tag{9.5}$$

Theorem 296. *Given G, H, $\chi \in \hat{G}$, $g \in G$,*

$$d_{\chi,H} \text{ divides } s_{g,H}\chi(g) \tag{9.6}$$

with

$$\begin{cases} d_{\chi,H} = \text{gcd of } d_\psi \text{ with } \psi \in \chi_H \\ s_{g,H} = \text{gcd of } |B| \text{ with } H \text{ classes } B \subset A = G \text{ class of } g \end{cases}$$

Lemma 297. *For each $\chi \in \hat{G}$ and each H*

$$\chi = \sum_{\psi \in \hat{H}} d_\psi \psi_{\chi\psi} \tag{9.7}$$

characters split up into spherical functions.

Proof. For $g \in G$

$$\sum_{\psi \in \chi_H} d_\psi \psi_{\chi\psi}(g) = \sum_{\psi \in \chi_H} d_\psi \frac{1}{|H|} \sum_{h \in H} \chi(gh^{-1})\psi(h) = \sum_{h \in H} \chi(gh^{-1}) \frac{1}{|H|} \sum_{\psi \in \hat{H}} d_\psi \psi(h) = \chi(g)$$

□

Prove theorem 296

Proof. Combining (9.3), (9.7), for each H class B in the G class of g,

$$|B|\chi(g) = \chi(B) = \sum_{\psi \in H} d_\psi \dot{\psi}_{\chi\psi}(B) \equiv 0 \bmod d_{\chi,H}$$

from which (9.6)follows, using 1) in the exercise 295. □

The results (9.6) for all $H \subset G$ can be packaged into a generalization of (9.6):

Theorem 298. *Given G, $\chi \in \hat{G}$, $g \in G$,*

$$m^*_{\chi,H} \text{ divides } \chi(g) \tag{9.8}$$

with

$$m^*_{\chi,g} = \operatorname*{lcm}_{H \subset G} d_{\chi,H}/(d_{\chi,H}, s_{g,H})$$

Proof. As with (9.4), (9.5), condition (9.6) can be written as

$$d_{\chi,H}/(d_{\chi,Hg}s_{g,H})|\chi(g) \quad \forall\, \chi \in \hat{G}, g \in G, H \in G$$

which are collectively equivalent to (9.8) by 3) of exercise 295. □

Before proving theorem 293, we get examples of the case of (9.5) and (9.8).

Theorem 299. *For each $\chi \in \hat{G}$ and at least 3/4 of the elements $g \in G$.*

$$\textit{either } d_\chi | s_g \textit{ or } \chi(g) = 0$$

Proof. From (9.5), we have

$$\chi(g) = m_{\chi,g} d_{\chi,g} \text{ with } d_{\chi,g} \in \mathbb{A}$$

therefore

$$|G| = \sum_{g \in G} |\chi(g)|^2 = \sum_{g \in G} m_{\chi,g}^2 |\alpha_{\chi,g}|^2$$

Acting on this by $(k) \in \mathcal{G}_m$ with $|G| \mid m$ gives as in the proof of Burnside's zero theorem

$$|G| \geq \sum_{\substack{g \in G \\ \chi(g) \neq 0}} \geq 4 \sum_{\substack{g \in G \\ \chi(g) \neq 0 \\ d_\chi \nmid s_g}} 1$$

Since $d_\chi \nmid s_g \implies (d_\chi, s_g) \leq \frac{1}{2} d_\chi$. □

With equal case, (9.8) gives

Theorem 300. *For each $\chi \in \hat{G}$ and at least 3/4 of the elements $g \in G$,*

$$\textit{either } d_{\chi,H} | s_{g,H} \textit{ for all subgroups } H \subset G, \textit{ or } \chi(g) = 0$$

Proof. As above, with $m_{\chi,g}$ replaced by $m_{\chi,g}^*$. □

Our proof of theorem 293 reduces it to a recent result of Isaacs and Navarro.

Definition 301. For each subgroup H of G we get an action of $H \times H$ on G by $(h', h)g = h'gh^{-1}$ for $h, h' \in H$ and $g \in G$. The orbit space here is denoted by $H \backslash G / H$ and consists of double cosets $S = HgH$.

Theorem 302. *(Isaacs & Navarro) For each $H \subset G$, $S \in H \backslash G / H$, $\chi \in \hat{G}$*

$$|H| \textit{ divides } \chi(S)$$

i.e. $\chi(S) \in |H| \mathbb{A}$.

Proof. (of theorem 293) In theorem 302, instead of $G \supset H$, S, χ, we take

$$G \times H \supset D = \{(h,h) : h \in H\}\ S = D(g,1)D,\ \chi \times \bar{\psi}$$

we have

$$S = \sum_{h \in H} (Bu, u) \tag{9.9}$$

where B is the H class of g. In fact

$$S = \{(h,h)(g,1)(h',h') : h,h' \in H\} = \{(hgh', hh') : h,h' \in H\} = \{(g^h u, u) : h,u \in H\}$$

It follows from (9.9) that

$$(\chi \times \bar{\psi})(S) = \sum_{u \in H} \chi(Bu)\bar{\psi}(u) = |H|\psi_{\chi\psi}(B)$$

Since $D \simeq H$, theorem 302 shows that $|H|\psi_{\chi\psi}(B) \in |H|\mathbb{A}$, so $\psi_{\chi\psi}(B) \in \mathbb{A}$. □

Definition 303. For each finite group G, the group algebra $\mathbb{C}G$ is the set of all formal linear combinations of the elements of G with arbitrary complex coefficients $x = \sum c_g g$. Sum and product are defined in $\mathbb{C}G$ as follows. For $y = \sum d_g g$, we put

$$x + y = \sum (c_g + d_g)g \quad \& \ x \cdot y = \sum_g (\sum_{g_1 g_2 = g} c_{g_1} d_{g_2})g$$

It is easily verified that $\mathbb{C}G$ is a ring, i.e. $\mathbb{C}G^+$ is an abelian group, and multiplication is associative and distributive over additions i.e. $\forall\, x,y,z \in \mathbb{C}G$,

$$xy \cdot z = x \cdot yz,\ x(y+z) = xy + xz,\ (x+y)z = xz + yz$$

The identity element $1 = 1_G$ of G (as $1_{\mathbb{C}} 1_G$) services as $1_{\mathbb{C}G}$, i.e. $1x = x = x1\ \forall\, x \in \mathbb{C}G$. Finally $\mathbb{C}G$ contains a copy of $\mathbb{C}$, as $\{c1_G : c \in \mathbb{C}\}$.

Each representation R of G on V, i.e. an algebra homomorphism $R : \mathbb{C}G \to \mathcal{E}(V)$, as follows: For $x = \sum c_g g$, we put $R(x) = \sum c_g R(g)$. Then for $x,y \in \mathbb{C}G$, $c \in \mathbb{C}$,

$$R(x+y) = R(x) + R(y),\ R(xy) = R(x)R(y), R(cx) = cR(x),\ R(1) = I_V$$

Notation 304. For each subset S of G we put $\hat{S} = \sum_{s \in G} s \in \mathbb{C}G$.

Lemma 305. *For each subgroup $H \subset G$ and all $S, T \in H\backslash G/H$*

$$\hat{S}\hat{T} = \sum_{U \in H\backslash G/H} c_{S,T,U}\hat{U}$$

with the $c_{S,T,U}$ integers ≥ 0, all divisible by $|H|$.

Proof. For given S and $T \in H\backslash G/H$, we have

$$\hat{S}\hat{T} = \sum c_g g \tag{9.10}$$

c_g depends also on S and T,

$$c_g = |\{(g_1, g_2) \in S \times T : g_1 g_2 = g\}| \tag{9.11}$$

H acts on the set in (9.11) via $h(g_1 g_2) = (g_1 h^{-1}, h g_2)$, only $h = 1$ fixing any pair (g_1, g_2), so each orbit has size $|H|$, therefore $|H|$ divides each c_g.

For each $h, h' \in H$, the map $(g_1, g_2) \mapsto (h' g_1, g_2 h)$ bijects the set in (9.11) to the corresponding set for $h' g h$. Therefore $c_{h' g h} = c_g$ for all $g \in G$, $h' h \in H$. This gives (9.10), with $c_{S,T,U} = c_g$ for $g \in U$. □

Lastly we prove theorem 302.

Proof. Given $\chi \in \hat{G}$, let R be a representation of G on V with character χ. R extends to a representation of $\mathbb{C}G$ on V, so from

$$\hat{T}\hat{S} = \sum_U c_{T,S,U}\hat{U}$$

in lemma 305, we get

$$R(\hat{T})R(\hat{S}) = \sum_U c_{T,S,U} T(\hat{U})$$

Let λ be an eigenvalue of $R(\hat{S})$. Thus

$$R(\hat{S})v = \lambda v$$

for some $v \in V$ with $v \neq 0$. It follows that

$$\lambda \hat{R}(T)v = \sum_U c_{T,S,U} R(\hat{U})v \tag{9.12}$$

Extend v to a basis $v, v', v'', ...$ of V. Then for each U

$$\hat{R}(U)v = z_U v + z'_U v' + z''_U v'' + ... \tag{9.13}$$

for some z_U, z'_U, z''_U,... in $\mathbb{C}$.

Substituting (9.13) for all U (and the corresponding formula for T) into (9.12) and equating the coefficient of v on both sides gives

$$\lambda z_T = \sum_U c_{T,S,U} z_U \qquad \forall T, U \in H\backslash G/H$$

By lemma 305, we have $c_{T,S,U} = a_{T,S,U}|H|$ with all $a_{T,S,U} \in \mathbb{Z}$, so $\lambda = \alpha|H|$ with

$$\alpha z_T = \sum_U a_{T,S,U} z_T \qquad \forall T, U \in H\backslash G/H$$

Since $z_S = \lambda$, it follows that if $\lambda \neq 0$ then $\alpha \in \mathbb{A}$ so $\lambda \in |H|\mathbb{A}$, so

$$\chi(S) = \mathrm{tr}R(\hat{S}) = \text{the sum of the eigenvalues of } R(\hat{S}) \in |H|\mathbb{A}.$$

□