Part I
Character Theory for the Odd Order Theorem

Introduction

The Feit-Thompson Theorem states that every finite group of odd order is solvable. This statement is clearly equivalent to the following: there is no non-abelian simple group of odd order. The theorem, first conjectured by Burnside, was proved in 1963 by W. Feit and J. G. Thompson in [FT]. Two papers, which prove the theorem in special cases, preceded the appearance of [FT]. In [Su], M. Suzuki proved the theorem for CA-groups of odd order: a group G is a *CA-group* if, for every element $x \neq 1$ of G, $C_G(x)$ is abelian. In [FHT], the theorem was shown for the CN-groups of odd order: a group G is a *CN-group* if, for every element $x \neq 1$ of G, $C_G(x)$ is nilpotent.

Each of these proofs is divided into two parts. In the first part, a minimal counterexample G to the theorem is considered and the structure of the maximal subgroups of G is studied. This part is very short in [Su], but is much more complicated in [FHT], and considerably more so in [FT]. In the second part, a contradiction is obtained by the use of character theory. The existence of isometries between virtual characters of maximal subgroups of G and virtual characters of G is one of the basic tools. In [FT], this second part leaves a residual case in which no contradiction arises. This case is eliminated in the final chapter of [FT], by explicit calculations with relations between elements of G.

The object of the present monograph is a revision of the second part of the proof of the Feit-Thompson Theorem, which corresponds to Chapters III and V of [FT].

From its appearance, [FT] has been the object of several efforts at revision. In [B], H. Bender gave a new proof of the Uniqueness Theorem, one of the principal results of Chapter IV of [FT]. From 1975, G. Glauberman worked on the revision of the first part of the proof of the theorem. In unpublished work [Si2], D. A. Sibley revised almost completely the part concerning characters. In [Pe], a revision of Chapter VI of [FT] was published by the present author. Finally, in 1994, H. Bender and G. Glauberman published a complete revision [BG] of the first part.

The present work may be viewed as a continuation of [BG] and constitutes with that book a complete proof of the Feit-Thompson Theorem. It is possible, however, to read this text without having read [BG] as the results of [BG] are reviewed in § 8.

We assume that the reader has a basic knowledge of ordinary character theory. There are many books which provide this theory. Here the book [Is] of I. M. Isaacs is used as reference. More precisely, the results of [Is] which are assumed known, are as follows:

Chapters 1 and 2;

in Chapter 3, (3.1) to (3.7), (3.11), (3.14);

in Chapter 4, (4.1), (4.2), (4.20), (4.21);

in Chapter 5, (5.1) to (5.5), (5.7) to (5.9);

in Chapter 6, (6.1) to (6.8), (6.10), (6.11), (6.28) (which uses the results (6.16) to (6.20) and (6.24) to (6.27)), (6.32) to (6.34);

in Chapter 7, (7.1) to (7.7).

We also assume known the following result from Problem 2.2 of [Is]:

Let G be a finite group, $|G| = n$, $\chi \in \operatorname{Irr} G$, σ be an automorphism of $\mathbf{Q}_n$ and χ^σ the mapping from G to $\mathbf{C}$ defined by $\chi^\sigma(g) = \chi(g)^\sigma$ for $g \in G$. Then $\chi^\sigma \in \operatorname{Irr} G$.

A certain familiarity with the elementary theory of finite groups is assumed. For the results used in this subject, reference is made to the initial sections of [BG] in so far as is possible. We also use Theorem 12.4 of [HB], Chapter XI, and Satz 8.18 of [H], Kapitel V.

The text is divided into sections. Sections 1 to 7 contain preliminary results. Sections 8 to 14 study a minimal counterexample to the Feit-Thompson Theorem. The hypotheses and results of § 29, for example, would be numbered (29.1), (29.2), ... Intermediate results used in the proof of (29.3) would be numbered (29.3.1), (29.3.2), ... If (29.4) is followed by a statement whose status is not specified, this statement is a lemma or a proposition.

I wish to thank Professor G. Glauberman, who suggested that I write this text and who helped me with advice and by supplying me with the relevant literature. The work of D. A. Sibley was of great utility to me in preparing this text.

Notation

Let G be a finite group.

We denote inclusion in the broad sense by $\subset$ (e.g., $G \subset G$).

$\mathrm{Irr}(G)$ or $\mathrm{Irr}\, G$ is the set of *irreducible characters* of G over the field $\mathbf{C}$.

$\mathrm{CF}(G)$ is the set of *class functions* from G to $\mathbf{C}$.

If $\alpha, \beta \in \mathrm{CF}(G)$, $(\alpha, \beta)_G$ or (α, β) is the usual *scalar product* of α and β, and $\|\alpha\|^2 = (\alpha, \alpha)$.

If $\phi \in \mathrm{CF}(G)$, $\mathrm{Supp}(\phi) = \{x \in G \mid \phi(x) \neq 0\}$.

Let $A \subset G$. Then $\mathrm{CF}(G, A) = \{\phi \in \mathrm{CF}(G) \mid \mathrm{Supp}(\phi) \subset A\}$.

If $\mathcal{X} \subset \mathrm{CF}(G)$ and R is a subring of $\mathbf{C}$, $R[\mathcal{X}]$ or $R\mathcal{X}$ is the set of R-linear combinations of elements of $\mathcal{X}$, and $R[\mathcal{X}, A] = R[\mathcal{X}] \cap \mathrm{CF}(G, A)$.

A *virtual character* of G is an element of $\mathbf{Z}[\mathrm{Irr}\, G]$.

If H is a subgroup of G, Res_H^G is *restriction*, $\mathrm{CF}(G) \to \mathrm{CF}(H)$, and Ind_H^G is *induction*, $\mathrm{CF}(H) \to \mathrm{CF}(G)$.

The symbol 1_G denotes the *principal character* of G. For $\chi \in \mathrm{CF}(G)$, $\overline{\chi}$ is defined by $\overline{\chi}(g) = \overline{\chi(g)}$ for $g \in G$.

If H is a normal subgroup of G, $\theta \in \mathrm{CF}(H)$ and $g \in G$, then θ^g is defined by $\theta^g(x^g) = \theta(x)$ for all $x \in H$. If $\theta \in \mathrm{Irr}(H)$, $I(\theta)$ or $I_G(\theta)$ is the *inertia group* of θ in G, which is the set of $g \in G$ such that $\theta^g = \theta$.

If $n \in \mathbf{N}$, $\mathbf{Q}_n$ is the subfield of $\mathbf{C}$ generated by the nth roots of unity.

A subset A of G is a *TI-subset* of G if, for every $g \in G$, $A^g = A$ or $A^g \cap A = \emptyset$.

If $A \subset G$, $A^\# = A - \{1\}$.

If $A \subset G$ and $L \subset G$, $A^L = \{a^x \mid a \in A, x \in L\}$.

We denote the *exponent* of G by $\exp(G)$. This is the smallest integer $n \geq 1$ such that $g^n = 1$ for every $g \in G$.

The symbol $\pi(G)$ denotes the set of prime divisors of the order $|G|$ of G.

Let σ be a set of prime numbers. We say that G is a *σ-group* if $\pi(G) \subset \sigma$. We denote by σ' the set of prime numbers which do not belong to σ. If $g \in G$, we denote by g_σ and $g_{\sigma'}$ the elements of $\langle g \rangle$ such that $g = g_\sigma g_{\sigma'} = g_{\sigma'} g_\sigma$ and $\pi(\langle g_\sigma \rangle) \subset \sigma$, $\pi(\langle g_{\sigma'} \rangle) \subset \sigma'$. We denote the largest normal σ-subgroup of G by $O_\sigma(G)$. If $\sigma = \{p\}$, we set $g_p = g_\sigma$, $g_{p'} = g_{\sigma'}$, $O_p(G) = O_\sigma(G)$ and $O_{p'}(G) = O_{\sigma'}(G)$.

$F(G)$ is the largest normal nilpotent subgroup of G.

$\Phi(G)$ is the *Frattini subgroup* of G.

The notation $G = H \rtimes K$ means that H and K are subgroups of G, H is normal in G, $G = HK$ and $H \cap K = 1$.

A group H *acts fixed-point-freely* on G, or *without fixed points* on G, if H acts on G and, for $g \in G$ and $h \in H$, $g^h = g$ implies that $h = 1$ or $g = 1$.

If p is a prime number and G is a p-group, $\Omega_1(G)$ is the subgroup of G generated by the elements of G of order p.

Cambridge University Press
978-0-521-64660-4 - Character Theory for the Odd Order Theorem
Thomas Peterfalvi
Excerpt
More information

1. Preliminary Results from Character Theory

Let G be a finite group.

(1.1) *If $|G|$ is odd, $\chi \in \mathrm{Irr}(G)$ and $\chi \neq 1_G$, then $\overline{\chi} \neq \chi$.*

Proof. Let $\langle a \rangle$ be a group of order 2, and set $g^a = g^{-1}$ and $\chi^a = \overline{\chi}$ for $g \in G$ and $\chi \in \mathrm{Irr}(G)$. Then $\langle a \rangle$ acts on the set G and on $\mathrm{Irr}(G)$, and $\chi^a(g^a) = \chi(g)$ for all $g \in G$ and $\chi \in \mathrm{Irr}(G)$. By [Is], Theorem 6.32, the number of $\chi \in \mathrm{Irr}(G)$ such that $\overline{\chi} = \chi$ is then equal to the number of conjugacy classes C of G such that $C^{-1} = C$. Let C be such a class and let $g \in C$. There is an element $x \in G$ such that $g^{-1} = g^x$. It follows that x^2 centralizes g. But x is of odd order, and so $x \in \langle x^2 \rangle \subset C_G(g)$, whence $g^{-1} = g$, and, since g is of odd order, $g = 1$. The only class C such that $C^{-1} = C$ is $\{1\}$, and so 1_G is the only character $\chi \in \mathrm{Irr}(G)$ such that $\overline{\chi} = \chi$. □

(1.2) *Let H be a normal subgroup of G, let $\chi \in \mathrm{Irr}(G)$ be such that $H \not\subset \mathrm{Ker}\,\chi$ and let $g \in G$ be such that $C_H(g) = 1$. Then $\chi(g) = 0$.*

Proof. Let $\overline{g}$ be the image of g in G/H. Since $C_H(g) = 1$, we have $|C_G(g)| = |C_G(g)H/H| \leq |C_{G/H}(\overline{g})|$. If Φ is the set of irreducible characters of G which have H in their kernels, then, by the second orthogonality relation,

$$\sum_{\chi \in \mathrm{Irr}(G)} |\chi(g)|^2 = |C_G(g)| \leq |C_{G/H}(\overline{g})| = \sum_{\phi \in \Phi} |\phi(g)|^2.$$

Thus $\chi(g) = 0$ if $\chi \in \mathrm{Irr}(G) - \Phi$. □

(1.3) *Let H be a subgroup of G and let A be a union of conjugacy classes of H. Let $(\psi_j)_{j\in J}$ be a basis for $\mathrm{CF}(H, A)$ and let $\mathrm{Irr}(H) = \{\chi_i \mid i \in I\}$.*

(a) *Let $\mu \in \mathrm{CF}(G)$ and $d_i \in \mathbf{C}$ for $i \in I$. Then $\mu_{|A} = (\sum_{i\in I} d_i\chi_i)_{|A}$ if and only if, for all $j \in J$, $\sum_{i\in I}(\psi_j, \chi_i)_H\overline{d_i} = (\mathrm{Ind}_H^G \psi_j, \mu)_G$.*

(b) *Suppose that there is an orthonormal family $(\mu_i)_{i\in I}$ of elements of $\mathrm{CF}(G)$ such that, for all $j \in J$, $\mathrm{Ind}_H^G \psi_j = \sum_{i\in I}(\psi_j, \chi_i)\mu_i$. Then $\mu_{i|A} = \chi_{i|A}$ for all $i \in I$, and, if μ is orthogonal to μ_i for all $i \in I$, $\mu_{|A} = 0$.*

Proof. (a) Considering the orthogonal basis of $\mathrm{CF}(H)$ consisting of the characteristic functions of conjugacy classes, we see that the orthogonal complement of $\mathrm{CF}(H, A)$ in $\mathrm{CF}(H)$ is $\mathrm{CF}(H, H - A)$. It follows that

$$\mathrm{Res}_H^G \mu - \textstyle\sum_{i\in I} d_i\chi_i \in \mathrm{CF}(H, H - A)$$

is equivalent to

$$\text{for all } j \in J, \quad \Big(\psi_j, \mathrm{Res}_H^G \mu - \sum_{i\in I} d_i\chi_i\Big) = 0;$$

that is, to

$$\text{for all } j \in J, \quad \textstyle\sum_{i\in I}(\psi_j, \chi_i)\overline{d_i} = (\psi_j, \mathrm{Res}_H^G \mu).$$

The result follows by Frobenius reciprocity.

(b) We apply (a) with $\mu = \mu_i$, $d_i = 1$ and $d_k = 0$ for $k \neq i$, and then with μ orthogonal to μ_i and $d_i = 0$ for all i. □

(1.4) *Let H be a finite group, let $\mathcal{X} = \{\chi_1, \ldots, \chi_n\} \subset \mathrm{Irr}(H)$ be such that $|\mathcal{X}| = n \geq 2$ and $\chi_i(1) = \chi_1(1)$ for all i, $1 \leq i \leq n$, and let τ be an isometry from $\mathbf{Z}[\mathcal{X}, H^\#]$ to $\mathbf{Z}[\mathrm{Irr}\, G, G^\#]$. Then there are pairwise distinct characters $\mu_i \in \mathrm{Irr}(G)$ and an integer $\varepsilon = \pm 1$ such that $(\chi_i - \chi_1)^\tau = \varepsilon(\mu_i - \mu_1)$ for all i, $1 \leq i \leq n$.*

Proof. It suffices to show that there is an orthonormal family (e_i) of $\mathbf{Z}[\mathrm{Irr}\, G]$ such that $(\chi_i - \chi_1)^\tau = e_i - e_1$ for all i. In fact, there are then characters $\mu_i \in \mathrm{Irr}\, G$ and integers $\varepsilon_i = \pm 1$ such that $e_i = \varepsilon_i \mu_i$, while $(\chi_i - \chi_1)^\tau(1) = \varepsilon_i \mu_i(1) - \varepsilon_1 \mu_1(1) = 0$ implies that $\varepsilon_i = \varepsilon_1$. If $n = 2$, $\|(\chi_2 - \chi_1)^\tau\|^2 = 2$, and so $(\chi_2 - \chi_1)^\tau$ can be written as $e_2 - e_1$. If $n = 3$, $(\chi_2 - \chi_1)^\tau$ and $(\chi_3 - \chi_1)^\tau$ are sums of two orthogonal components of norm 1. Since $((\chi_2 - \chi_1)^\tau, (\chi_3 - \chi_1)^\tau) = 1$, they have a component in common, with the same sign, which we can write $-e_1$, and so we obtain the required decompositions. Suppose that $n > 3$ and that $(\chi_i - \chi_1)^\tau = e_i - e_1$ for $2 \leq i < k$, where $3 < k \leq n$. On taking into account the fact that $((\chi_k - \chi_1)^\tau, (\chi_i - \chi_1)^\tau) = 1$ for $i < k$, we see that one of two cases holds:

$$(\chi_k - \chi_1)^\tau = e_k - e_1 \quad \text{or} \quad (\chi_k - \chi_1)^\tau = e_2 + e_3.$$

But, in the second case, $(e_2 + e_3)(1) = (e_2 - e_3)(1) = 0$, and so $e_2(1) = 0$, which is a contradiction. □

(1.5) *Let H be a normal subgroup of G, $\theta \in \mathrm{Irr}(H)$, $r = |I_G(\theta) : H|$ and $\chi = \mathrm{Ind}_H^G \theta$.*

(a) $\mathrm{Res}_H^G \chi = r \sum \theta^g$, *where the sum is taken over the $|G : I_G(\theta)|$ distinct conjugates of θ in G.*

(b) $\|\chi\|^2 = r$. *In particular, χ is irreducible if $r = 1$.*

(c) *Let $\phi \in \mathrm{Irr}(H)$. If ϕ is conjugate to θ in G, then $\mathrm{Ind}_H^G \phi = \chi$, and, if ϕ is not conjugate to θ, then $(\mathrm{Ind}_H^G \phi, \chi) = 0$.*

(d) $\dfrac{\chi(1)\mathrm{Res}_H^G \chi}{\|\chi\|^2} = |G : H| \sum \theta^g(1)\theta^g$, *where the sum is indexed as in* (a).

(e) *If $|G|$ is odd and $\theta \neq 1_H$, then $\overline{\chi}$ is orthogonal to χ.*

Proof. (a) For $h \in H$, $\chi(h) = \dfrac{1}{|H|} \sum_{x \in G} \theta(xhx^{-1}) = \dfrac{1}{|H|} \sum_{x \in G} \theta^x(h)$. But $\theta^x = \theta^y$ if and only if $y \in I(\theta)x$, and the result follows.

(b) By (a) and Frobenius reciprocity, $\|\chi\|^2 = (\mathrm{Res}_H^G \chi, \theta) = r$.

(c) If ϕ is conjugate to θ, then (a) shows that $\mathrm{Ind}_H^G \phi$ and χ coincide on H. As they vanish on $G - H$, they coincide on G. If ϕ is not conjugate to θ, then $(\mathrm{Ind}_H^G \phi, \chi) = (\phi, \mathrm{Res}_H^G \chi) = 0$ by (a).

(d) Using (a) and (b), we see that

$$\frac{\chi(1)\mathrm{Res}_H^G\chi}{\|\chi\|^2} = \frac{|G:H|\theta(1)r\sum\theta^g}{r} = |G:H|\sum\theta^g(1)\theta^g.$$

(e) First of all, $\overline{\chi} = \mathrm{Ind}_H^G\overline{\theta}$. If $\overline{\chi}$ is not orthogonal to χ, then, by (c), there is an element $g \in G$ such that $\overline{\theta} = \theta^g$. Then $\theta^{g^2} = \theta$. But $g \in \langle g^2\rangle$ because $|G|$ is odd, and so $\overline{\theta} = \theta^g = \theta$. By (1.1), it follows that $\theta = 1_H$. □

(1.6) *Let H be a normal subgroup of G, let $\theta \in \mathrm{Irr}(H)$ and let A be a normal subgroup of G contained in H.*

(a) *$A \subset \mathrm{Ker}\,\theta$ if and only if $A \subset \mathrm{Ker}\,\mathrm{Ind}_H^G\theta$.*

(b) *Suppose that $A \subset \mathrm{Ker}\,\theta$. Let θ_1 be the character of H/A for which $\theta_1(xA) = \theta(x)$ for all $x \in H$. Let χ be the character of G/A for which $\chi(xA) = (\mathrm{Ind}_H^G\theta)(x)$ for all $x \in G$. Then $\chi = \mathrm{Ind}_{H/A}^{G/A}\theta_1$.*

Proof. (a) This follows from (1.5.a) and from [Is], Lemma 2.21.

(b) We see that χ and $\mathrm{Ind}_{H/A}^{G/A}\theta_1$ vanish on $G/A - H/A$. For $h \in H$,

$$\begin{aligned}(\mathrm{Ind}_{H/A}^{G/A}\theta_1)(hA) &= \frac{|A|}{|H|}\sum_{xA\in G/A}\theta_1(xhAx^{-1})\\ &= \frac{1}{|H|}\sum_{x\in G}\theta(xhx^{-1}) = \chi(hA).\end{aligned}$$

□

(1.7) *Let H be a normal subgroup of G, $\theta \in \mathrm{Irr}(H)$ and $T = I_G(\theta)$. Set $\mathrm{Ind}_H^T\theta = \sum_{i=1}^n e_i\psi_i$, where $e_i \in \mathbf{N} - \{0\}$ and the characters ψ_i are distinct elements of $\mathrm{Irr}(T)$.*

(a) *Let $\chi_i = \mathrm{Ind}_T^G\psi_i$ $(1 \le i \le n)$. Then the characters χ_i are distinct elements of $\mathrm{Irr}(G)$; furthermore, $\mathrm{Ind}_H^G\theta = \sum_{i=1}^n e_i\chi_i$.*

(b) *Suppose that T/H is abelian. Then $\mathrm{Ind}_H^G\theta = e\sum_{i=1}^n\chi_i$, where $e = e_1$, $n = |T:H|/e^2$ and $\chi_i(1) = |G:T|e\theta(1)$ for all i $(1 \le i \le n)$.*

(c) *Suppose that T/H is abelian and that $|H|$ is prime to the index $|T:H|$. Then $\mathrm{Ind}_H^G\theta = \sum_{i=1}^n\chi_i$, $n = |T:H|$ and, for all i, $\chi_i(1) = |G:T|\theta(1)$.*

Proof. (a) This follows from [Is], Theorem 6.11.

(b) Let $L = \{\lambda \in \mathrm{Irr}\,T \mid H \subset \mathrm{Ker}\,\lambda\}$. Since T/H is abelian, $\sum_{\lambda\in L}\lambda$ is the regular character of T/H, identified with a character of T. With $\psi = \psi_1$, $\sum_{\lambda\in L}(\lambda\psi)(x) = |T:H|\psi(x)$ for $x \in H$ and $\sum_{\lambda\in L}(\lambda\psi)(x) = 0$ for $x \in T - H$. It follows that $\mathrm{Ind}_H^T(\mathrm{Res}_H^T\psi) = \sum_{\lambda\in L}\lambda\psi$. Moreover, $\lambda\psi \in \mathrm{Irr}\,T$ for $\lambda \in L$, because $\lambda(1) = 1$. Since θ is a component of $\mathrm{Res}_H^T\psi$, this proves that the characters ψ_i are of the form $\lambda\psi$, $\lambda \in L$. Furthermore,

$$(\mathrm{Ind}_H^T\theta, \lambda\psi) = (\theta, \mathrm{Res}_H^T(\lambda\psi)) = (\theta, \mathrm{Res}_H^T\psi),$$

and so $\mathrm{Ind}_H^T \theta = e \sum_{i=1}^n \psi_i$, where $e = e_1$. By Clifford's Theorem ([Is], Theorem 6.5), $\mathrm{Res}_H^T \psi = e\theta$, and so, for all i, $\psi_i(1) = \psi(1) = e\theta(1)$, whence

$$|T : H|\theta(1) = (\mathrm{Ind}_H^T \theta)(1) = ne^2\theta(1).$$

Thus $n = |T : H|/e^2$. By (a), it follows that

$$\mathrm{Ind}_H^G \theta = e \sum_{i=1}^n \chi_i \quad \text{and} \quad \chi_i(1) = |G : T|\psi(1) = |G : T|e\theta(1).$$

(c) By [Is], Corollary 6.28, there is an index i such that $e_i = 1$; (b) then gives the desired result. □

(1.8) *Let $\psi \in \mathrm{Irr}\, G$ and let B, C and D be subgroups of G. Assume that B is normal in C, that $B \subset \mathrm{Ker}\, \psi$, that $B \subset D \subset C$, and that $D/B \subset Z(C/B)$. Then $\psi(1) \leq |G|/\sqrt{|C||D|}$.*

Proof. Let χ be an irreducible component of $\mathrm{Res}_C^G \psi$. Then $B \subset \mathrm{Ker}\, \chi$ and, by [Is], Corollary 2.30, $\chi(1)^2 \leq |C : D|$. Since ψ is an irreducible component of $\mathrm{Ind}_C^G \chi$,

$$\psi(1)^2 \leq |G : C|^2 \chi(1)^2 \leq \frac{|G|^2}{|C||D|}.$$

□

(1.9) *Suppose that $|G| = n = ab$, where a and b are relatively prime.*

(a) *Let u be an automorphism of the field $\mathbf{Q}_a$. There is an automorphism v of $\mathbf{Q}_n$ such that $v_{|\mathbf{Q}_a} = u$ and $v_{|\mathbf{Q}_b} = \mathrm{Id}$.*

(b) *Let χ be a character of G and let $k \in \mathbf{Z}$ be such that $(k, a) = 1$. There is an automorphism v of $\mathbf{Q}_n$ such that*

$$\chi^v(g) = \begin{cases} \chi(g^k) & \text{if the order of } g \text{ divides } a, \\ \chi(g) & \text{if the order of } g \text{ is prime to } a. \end{cases}$$

Proof. (a) We may assume that $a, b \geq 2$. Let m be an integer ≥ 2. There is a group isomorphism $f_m : (\mathbf{Z}/m\mathbf{Z})^* \to \mathrm{Aut}(\mathbf{Q}_m)$ such that, if $\phi_m : \mathbf{Z} \to \mathbf{Z}/m\mathbf{Z}$ is the canonical mapping and ε is an mth root of unity, then $f_m(\phi_m(k))(\varepsilon) = \varepsilon^k$ for k prime to m ([L], Chapter VIII, Theorem 3.1). Let

$$i : (\mathbf{Z}/n\mathbf{Z})^* \to (\mathbf{Z}/a\mathbf{Z})^* \times (\mathbf{Z}/b\mathbf{Z})^*$$

be the isomorphism given by the Chinese Remainder Theorem. Let $h = (f_a \times f_b) \circ i \circ f_n^{-1}$. Let $v = f_n(\phi_n(k))$, an automorphism of $\mathbf{Q}_n$. Then $h(v) = (f_a(\phi_a(k)), f_b(\phi_b(k)))$ and, if ε is an nth root of unity,

$$f_a(\phi_a(k))(\varepsilon^b) = f_n(\phi_n(k))(\varepsilon^b) = \varepsilon^{bk}.$$

Thus $h(v) = (v_{|\mathbf{Q}_a}, v_{|\mathbf{Q}_b})$, and the result follows since h is bijective.

(b) Let $u = f_a(\phi_a(k))$ and let v be the automorphism of $\mathbf{Q}_n$ given by (a). For $g \in G$, the restriction of χ to $\langle g \rangle$ is of the form $\sum_{i=1}^{\chi(1)} \psi_i$, where the ψ_i are homomorphisms from $\langle g \rangle$ to $\mathbf{C}^*$. If the order of g divides a, then $\psi_i(g) \in \mathbf{Q}_a$ and so

$$\chi^v(g) = \sum \psi_i(g)^k = \sum \psi_i(g^k) = \chi(g^k)$$

while, if the order of g is prime to a, then $\psi_i(g) \in \mathbf{Q}_b$ and so $\chi^v(g) = \chi(g)$. □

(1.10) *Let p be a prime number, ε a primitive pth root of unity in $\mathbf{C}$, η a primitive $|G|$th root of unity in $\mathbf{C}$ and $A = \mathbf{Z}[\eta]$.*

(a) *Let $x, y \in G$ be such that x has order p and $xy = yx$. Let χ be a virtual character of G. Then $\chi(xy) \equiv \chi(y) \pmod{1 - \varepsilon}$ in A.*

(b) *If $n \in \mathbf{Z}$ and $n \equiv 0 \pmod{1 - \varepsilon}$ in A, then $n \equiv 0 \pmod{p}$ in $\mathbf{Z}$.*

Proof. (a) Let α be an irreducible component of $\mathrm{Res}^G_{\langle x,y \rangle} \chi$. It suffices to show that $\alpha(xy) \equiv \alpha(y) \pmod{1 - \varepsilon}$. Since $xy = yx$, α is of degree 1, and so $\alpha(xy) - \alpha(y) = (\alpha(x) - 1)\alpha(y)$. There is an integer $k \geq 1$ such that $\alpha(x) = \varepsilon^k$. Thus, $\alpha(x) - 1 = (\varepsilon - 1)(\varepsilon^{k-1} + \cdots + 1)$ is divisible by $1 - \varepsilon$ in A. Therefore $\alpha(xy) - \alpha(y)$ is divisible by $1 - \varepsilon$ in A.

(b) If $1 \leq k < p$, there is an integer $r \geq 1$ for which $\varepsilon = \varepsilon^{kr}$, and so $\varepsilon - 1 = (\varepsilon^k - 1)(\varepsilon^{k(r-1)} + \cdots + 1)$ and $1 - \varepsilon^k$ divides n. If $F(X) = X^{p-1} + X^{p-2} + \cdots + 1$, then

$$F(X) = \prod_{1 \leq k < p} (X - \varepsilon^k) \quad \text{and} \quad F(1) = \prod_{1 \leq k < p} (1 - \varepsilon^k) = p.$$

Thus p divides n^{p-1} in A. By [Is], Lemma 3.2 and Corollary 3.5, $A \cap \mathbf{Q} = \mathbf{Z}$, and so p divides n^{p-1} in $\mathbf{Z}$, and, since p is prime, p divides n. □

2. The Dade Isometry

Let G be a finite group, let A be a TI-subset of G and let $L = N_G(A)$. By [Is], Lemma 7.7, Ind_L^G is a linear isometry from $\mathrm{CF}(L, A)$ to $\mathrm{CF}(G)$, which sends each virtual character of $\mathrm{CF}(L, A)$ to a virtual character of G. We give here a generalization of this isometry when A satisfies a condition less restrictive than that of being a TI-subset.

(2.1) *Let G be a finite group. Let $g \in G$ and let H be a subgroup of G such that g normalizes H and such that $\langle g \rangle$ and H have coprime orders. Then Hg is the disjoint union of $|H : C_H(g)|$ subsets which are conjugate to $C_H(g)g$ in $H\langle g \rangle$.*

Proof. Let $K = \bigcup_{x \in H}(C_H(g)g)^x$. Then $K \subset Hg$ since $H \triangleleft H\langle g \rangle$. Let π be the set of prime divisors of the order of g. Let $x, y \in H$ and $u, v \in C_H(g)$ be such that $(ug)^x = (vg)^y$. Then $g^x = ((ug)^x)_\pi = ((vg)^y)_\pi = g^y$, and so $y \in C_H(g)x$. It follows that K is the disjoint union of $(C_H(g)g)^x$ for x running through a system of right coset representatives of $C_H(g)$ in H. We conclude that

$$|K| = |H : C_H(g)||C_H(g)g| = |H| = |Hg|,$$

which proves that $K = Hg$. □

(2.2) Hypothesis. *Assume that G is a finite group, that A is a subset of $G^\#$ and that L is a subgroup of G such that $A \subset L \subset N_G(A)$. Furthermore:*

(a) *If two elements of A are conjugate in G, then they are conjugate in L.*

(b) *For $a \in A$, there is a subgroup $H(a)$ of G such that*

$$C_G(a) = H(a) \rtimes C_L(a).$$

(c) *For $a, b \in A$, $|H(a)|$ is prime to $|C_L(b)|$.*

(2.3) *Let A be a non-empty subset of $G^\#$. Then A is a TI-subset of G with normalizer L if and only if Hypothesis (2.2) holds with $H(a) = 1$ for all $a \in A$.*

Proof. Suppose that A is a TI-subset of G, with normalizer L. Let $a \in A$ and $g \in G$ be such that $a^g \in A$. Then $a^g \in A \cap A^g$ and so $g \in N_G(A) = L$. In particular, if $g \in C_G(a)$, then $g \in L$ and so $C_G(a) = C_L(a)$. Thus, Hypothesis (2.2) holds with $H(a) = 1$ for all $a \in A$. Suppose conversely that Hypothesis (2.2) holds with $H(a) = 1$ for all $a \in A$. Let $g \in G$ be such that $A \cap A^g \neq \emptyset$. Let a be such that $a^g \in A \cap A^g$. By (2.2.a), there is an element $x \in L$ such that $a^{gx} = a$, and so $gx \in C_G(a) = C_L(a)$, whence $g \in L \subset N_G(A)$. Thus A is a TI-subset of G. Let $g \in N_G(A)$. Since $A \neq \emptyset$, $A \cap A^g \neq \emptyset$ and we have seen that then $g \in L$. Thus $N_G(A) = L$. □

In the remainder of § 2, we will assume Hypothesis (2.2).