de Gruyter Expositions in Mathematics 25

de Gruyter Expositions in Mathematics

1 The Analytical and Topological Theory of Semigroups, *K. H. Hofmann, J. D. Lawson, J. S. Pym* (Eds.)

2 Combinatorial Homotopy and 4-Dimensional Complexes, *H. J. Baues*

3 The Stefan Problem, *A. M. Meirmanov*

4 Finite Soluble Groups, *K. Doerk, T. O. Hawkes*

5 The Riemann Zeta-Function, *A. A. Karatsuba, S. M. Voronin*

6 Contact Geometry and Linear Differential Equations, *V. E. Nazaikinskii, V. E. Shatalov, B. Yu. Sternin*

7 Infinite Dimensional Lie Superalgebras, *Yu. A. Bahturin, A. A. Mikhalev, V. M. Petrogradsky, M. V. Zaicev*

8 Nilpotent Groups and their Automorphisms, *E. I. Khukhro*

9 Invariant Distances and Metrics in Complex Analysis, *M. Jarnicki, P. Pflug*

10 The Link Invariants of the Chern-Simons Field Theory, *E. Guadagnini*

11 Global Affine Differential Geometry of Hypersurfaces, *A.-M. Li, U. Simon, G. Zhao*

12 Moduli Spaces of Abelian Surfaces: Compactification, Degenerations, and Theta Functions, *K. Hulek, C. Kahn, S. H. Weintraub*

13 Elliptic Problems in Domains with Piecewise Smooth Boundaries, *S. A. Nazarov, B. A. Plamenevsky*

14 Subgroup Lattices of Groups, *R. Schmidt*

15 Orthogonal Decompositions and Integral Lattices, *A. I. Kostrikin, P. H. Tiep*

16 The Adjunction Theory of Complex Projective Varieties, *M. C. Beltrametti, A. J. Sommese*

17 The Restricted 3-Body Problem: Plane Periodic Orbits, *A. D. Bruno*

18 Unitary Representation Theory of Exponential Lie Groups, *H. Leptin, J. Ludwig*

19 Blow-up in Quasilinear Parabolic Equations, *A.A. Samarskii, V.A. Galaktionov, S. P. Kurdyumov, A. P. Mikhailov*

20 Semigroups in Algebra, Geometry and Analysis, *K. H. Hofmann, J. D. Lawson, E. B. Vinberg* (Eds.)

21 Compact Projective Planes, *H. Salzmann, D. Betten, T. Grundhöfer, H. Hähl, R. Löwen, M. Stroppel*

22 An Introduction to Lorentz Surfaces, *T. Weinstein*

23 Lectures in Real Geometry, *F. Broglia* (Ed.)

24 Evolution Equations and Lagrangian Coordinates, *A. M. Meirmanov, V. V. Pukhnachov, S. I. Shmarev*

Character Theory of Finite Groups

by

Bertram Huppert

W DE G

Walter de Gruyter · Berlin · New York 1998

Author

Bertram Huppert
Fachbereich Mathematik
Universität Mainz
Staudingerweg 9
D-55099 Mainz

1991 Mathematics Subject Classification: 20-02; 20 Dxx, 20 Exx, 20 Fxx

⊗ Printed on acid-free paper which falls within the guidelines of the ANSI to ensure permanence and durability.

Library of Congress – Cataloging-in-Publication Data

Huppert, B. (Bertram), 1927–
Character theory of finite groups / by Bertram Huppert.
p. cm. – (De Gruyter expositions in mathematics, ISSN 0938-6572 ; 25)
Includes bibliographical references and indexes.
ISBN 978-3-11-015421-4 (alk. paper)
1. Finite groups. 2. Characters of groups. I. Title. II. Series.
QA177.H87 1998
512'.2–dc21 98-8805
CIP

Die Deutsche Bibliothek – Cataloging-in-Publication Data

Huppert, Bertram:
Character theory of finite groups / by Bertram Huppert. – Berlin ; New York : de Gruyter, 1998
(De Gruyter expositions in mathematics ; 25)
ISBN 978-3-11-015421-4

Typesetting: ASCO Trade Typesetting Ltd., Hong Kong.
Printing: Druckerei Hildebrand, Berlin. Binding: Lüderitz & Bauer GmbH, Berlin.
Cover design: Thomas Bonnie, Hamburg.

Contents

Introduction

In 1976, I.M. Isaacs published his "Character Theory of Finite Groups". This book has often been on my desk since then, doing research or teaching. To offer now one more book on the same subject needs some justification, certainly more than only the author's pleasure to write it.

How does this book differ from Isaacs' book? There have been achieved many interesting results in character theory since 1976, several by Isaacs himself. Questions about character degrees had already been taken up by Isaacs in chapter 12 of his book. Since 1984 many more results in this direction have been found. As research of my students and myself was for some years concentrated in this area, I devote considerable space to degree problems. Also, the similarity with several results about lengths of conjugacy classes, still not at all understood, is considered in some detail in § 33.

There is another, minor difference compared with Isaacs' book. Occasionally my treatment is just a bit more module-theoretic. But in general I also prefer here a short and elegant character-theoretic approach to a more elaborate module-theoretic proof. So I make no attempt to prepare the reader for the study of modular representation theory. I do not try at all to give an impression of this wide field, only rarely I make some remarks.

Another difference with Isaacs' book is the inclusion of many examples, where I calculate the character table or at least the character degrees of groups. Permutation representations will often be very useful in the study of special groups. I think that it is extremely important for a serious student of character theory to know many examples. After all, several theorems are of the type that some statement is true, except for some very special groups. Certainly, I want the reader to "meet many groups". To enable the reader to find information about special groups I add a list of examples treated in this book.

The amount of group theory needed in this book is most of the time rather moderate. A one-term lecture suffices nearly everywhere. In a first section I fix notations and collect the facts needed later on, some of them used only rarely. The reader might contact this section only if needed.

As the present book is intended to be self-contained, there are naturally sections where I deviate only slightly from other books. Some special areas, where I cannot improve on Isaacs' treatment, have been touched only slightly. This concerns for instance some questions about splitting fields and the Schur index. Projective representations are only treated as far as they are needed for Clifford theory, the theory of the Schur multiplier is left out.

Some more remarks are necessary about the relation between this book and the rather recent book by O. Manz and Th. Wolf. This important book presents some fundamental recent developments, concerning mainly solvable groups. Except for occasional references I have avoided the topics treated there. So the book by O. Manz and T. Wolf may be considered as a kind of extension of the present book in some directions.

The theory of exceptional characters and coherence is not included. The reader can find a detailed presentation of this theory and some applications in the book by M. Collins, listed in the bibliography. I only include just enough of these techniques to prove in §45 that generalized quaternion groups (even of order 8) cannot be Sylow-2-subgroups of simple groups.

For a one-term lecture (and the less experienced reader) I suggest the following program: §1–6; at least some examples from §7; §8, §17. The "classical" applications in §15 and parts of §16 should follow here. Also §42 about faithful irreducible representations can already be presented here.

Coherent sections for further study could be §18–25, on Clifford theory and applications to solvable groups. After this might follow §40, 41.

Another line might be Brauer's main theorem and applications in §34, 35, 37–39, or §43–45.

The list of references makes no attempt to be complete. Classical results, already in many books, are usually quoted only with the name of the author. More recent results and extensions of the text are contained in the bibliography. Names usually refer to the bibliography, with numbers if an author appears more than once. (Isaacs without numbers refers to Isaacs' book.)

For contribution of unpublished material, critical remarks and references I have to thank H. Bender (Kiel), C. Casolo and S. Dolfi (Firenze), St. Gagula, I.M. Isaacs (Madison), T. Keller (formerly Mainz), B. Külshammer (Jena), U. Meierfrankenfeld (East Lansing), G. Navarro (Valencia), J. Neubüser (Aachen), G. Pazderski (Halle) and Judith Pense (Mainz), J.M. Riedl (Madison).

For assistance with the proofs I owe thanks to W. Jehne, G. Pazderski and T. Keller.

I like to thank the Asco Company for producing this book from a handwritten manuscript.

Finally I want to thank Dr. M. Karbe of de Gruyter Verlag.

Examples of groups

The examples are ordered by their first appearance in the text.

Notations and results from group theory

In this section we collect notations and theorems about **finite** groups, which will be used frequently, often without reference. But several of the facts we mention here are used only rarely.

Let G always be a finite group.

(1) If U is a subgroup of G, we write $U \leqslant G$ resp. $U < G$ and denote by $|G : U|$ the index of U in G. If U is normal in G, we write $U \trianglelefteq G$ resp. $U \triangleleft G$ and denote by G/U the factor group of G by U. We write $N \triangleleft\triangleleft G$ and call N subnormal in G, if there exists a series

$$N = N_1 \triangleleft N_2 \triangleleft \cdots \triangleleft N_k = G$$

(where $k = 1$, hence $N = G$, is allowed).

If M is any finite set, by $|M|$ we denote the number of elements in M.

If $M \subseteq G$, we denote by $\langle M \rangle$ the subgroup of G generated by M.

If $g \in G$, we put $\operatorname{ord} g = |\langle g \rangle|$. Then $\operatorname{ord} g$ is the smallest integer m such that $g^m = 1$. The smallest integer m such that $g^m = 1$ for all $g \in G$, we call the exponent of G and denote it by $\operatorname{Exp} G$.

(2) If $U, V \leqslant G$, then the set

$$UV = \{uv | u \in U, v \in V\}$$

contains

$$|UV| = \frac{|U||V|}{|U \cap V|}$$

elements. UV is a subgroup of G, if and only if $UV = VU$; this is certainly the case if $U \trianglelefteq G$. If $U, V \leqslant G$, then

$$|G\colon U \cap V| \leqslant |G : U||G : V|.$$

If in particular $|G : U|$ and $|G : V|$ are coprime, then

$$|G\colon U \cap V| = |G : U||G : V|$$

and hence $G = UV$.

(3) For $g, h \in G$ we put $g^h = h^{-1}gh$. The conjugacy class g^G of g in G is defined by

$$g^G = \{g^h | h \in G\}.$$

If $M \subseteq G$ and $g \in G$, we put

$$M^g = \{g^{-1}mg | m \in M\}$$

and call M^g a conjugate of M. If $M \subseteq G$, we define normalizer and centralizer of M in G by

$$N_G(M) = \{g | g \in G, M^g = M\}$$

and

$$C_G(M) = \{g | g \in G, gm = mg \text{ for all } m \in M\}.$$

Then

$$|g^G| = |G : C_G(g)|$$

and we obtain a partition

$$G = \bigcup_{i=1}^{h} g_i^G.$$

We call $h = h(G)$ the class number of G.

If $U \leqslant G$, then $C_G(U) \trianglelefteq N_G(U)$ and $N_G(U)/C_G(U)$ is isomorphic to a subgroup of the group Aut U of automorphisms of U.

(4) If $g, h \in G$, we define the commutator of g and h by

$$[g, h] = g^{-1}h^{-1}gh.$$

If $A, B \leqslant G$, we put

$$[A, B] = \langle [a, b] | a \in A, b \in B \rangle.$$

In particular, we write $G' = G^{(1)} = [G, G]$ and define recursively

$$G^{(i+1)} = [G^{(i)}, G^{(i)}].$$

If $G^{(k-1)} > G^{(k)} = E = \{1\}$, we call G solvable and $k = \mathrm{dl}\, G$ the derived length of G.

(5) **Sylow's theorem.**
Suppose that p is a prime, $|G| = p^a m$ and $p \nmid m$. Then the set

$$\mathrm{Syl}_p\, G = \{P \mid P \leqslant G, |P| = p^a\}$$

is non-empty. The members of $\mathrm{Syl}_p\, G$ are called the Sylow-p-subgroups of G. They all are conjugate in G, and if $P \in \mathrm{Syl}_p\, G$, then

$$|\mathrm{Syl}_p\, G| = |G : N_G(P)| \equiv 1 \pmod{p}.$$

If $U \leqslant G$ and $|U|$ is a power of p, then there exists $P \in \mathrm{Syl}_p\, G$ such that $U \leqslant P$.
If $M \trianglelefteq G$ and $P \in \mathrm{Syl}_p\, M$, then $G = MN_G(P)$ (Frattini argument).

(6) **P. Hall's theorem.**
Let G be solvable and $|G| = mn$ with $(m, n) = 1$. Then G contains subgroups of order m, and all these are conjugate in G. If $U \leqslant G$ and $|U|$ divides m, then there exists $H \leqslant G$ such that $|H| = m$ and $U \leqslant H$.

(7) **Zassenhaus–Schur Theorem.**
Suppose $N \lhd G$ and $(|N|, |G/N|) = 1$. Then there exists $H \leqslant G$ with $|H| = |G/N|$, hence $G = NH$ and $N \cap H = E$.
If N or G/N is solvable, all such H are conjugate in G. (At least one of the groups N, G/N has odd order, hence by the theorem of Feit and Thompson is solvable.)

(8) We define the centre of G by

$$Z(G) = \{z \mid z \in G, zg = gz \text{ for all } g \in G\}.$$

The ascending central series of G is then defined recursively by $Z_0(G) = E$ and

$$Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G)).$$

Then

$$Z_\infty(G) = \bigcup_i Z_i(G)$$

is a subgroup of G, the hypercentre of G.
The descending central series of G is defined by $K_1(G) = G$, $K_2(G) = G'$ and

$$K_{i+1}(G) = [K_i(G), G].$$

(9) The following statements are equivalent:
(i) $Z_c(G) = G$ for some c.
(ii) $K_{c+1}(G) = E$ for some c.
(iii) All Sylow-subgroups of G are normal in G, and G is their direct product.

Then we call G nilpotent. If $Z_{c-1}(G) < Z_c(G) = G$, then $K_c(G) > K_{c+1}(G) = E$, and we call $c = c(G)$ the nilpotency class of G. In particular, G is of class 2 if $E < G' \leqslant Z(G)$.

(10) The product of all nilpotent normal subgroups of G is a nilpotent normal subgroup, the Fitting group $F(G)$ of G. We define the Fitting series of G by $F_0(G) = E$ and

$$F_{i+1}(G)/F_i(G) = F(G/F_i(G)).$$

If G is solvable, then $F_{n-1}(G) < F_n(G) = G$ for some n. Then we call $n = n(G)$ the nilpotent length of G.

If G is solvable, then

$$C_G(F(G)) \leqslant F(G).$$

The Frattini subgroup $\Phi(G)$ of G is defined as the intersection of all maximal subgroups of G. Then $\Phi(G) \leqslant F(G)$ and even $\Phi(G) < F(G)$ if $G > E$ is solvable.

G is nilpotent if and only if $G' \leqslant \Phi(G)$.

(11) Let π be a set of primes. We call G a π-group, if all prime divisors of $|G|$ are in π.

The product of all normal π-subgroups of G is a normal π-subgroup of G which we denote by $O_\pi(G)$. If $\pi = \{p\}$ or $\pi = \{q | q \neq p\}$, we write $O_p(G)$ resp. $O_{p'}(G)$ instead of $O_\pi(G)$.

By $O^\pi(G)$ sometimes we denote the smallest normal subgroup of G such that $G/O^\pi(G)$ is a π-group.

The ascending p-series of G is defined by $P_0 = E$, $P_1 = O_{p'}(G)$ and recursively

$$P_{2i}/P_{2i-1} = O_p(G/P_{2i-1})$$

$$P_{2i+1}/P_{2i} = O_{p'}(G/P_{2i}).$$

G is called p-solvable if $P_k = G$ for some k. If $P_{2k-1} < G = P_{2k+1}$, we call $k = l_p(G)$ the p-length of G. If even $P_2 = G$, hence $G/O_{p'}(G)$ is a p-group, then we call G p-nilpotent.

(12) We call G supersolvable if there exists a series

$$E = G_0 \lhd G_1 \lhd \cdots \lhd G_m = G$$

such that $G_i \trianglelefteq G$ and $|G_{i+1}/G_i|$ is a prime. If G is supersolvable, then the following properties hold:
(i) G' is nilpotent.
(ii) If

$$|G| = \prod_{i=1}^{k} p_i^{a_i}$$

with primes

$$p_1 > p_2 > \cdots > p_k$$

and $P_i \in \mathrm{Syl}_{p_i} G$, then

$$P_1 \dots P_i \trianglelefteq G.$$

(We say that G has a Sylow tower.)

(13) If A is an abelian p-group, then

$$A = \langle x_1 \rangle \times \cdots \times \langle x_m \rangle$$

is the direct product of cyclic groups $\langle x_i \rangle$. If ord $x_i = p^{a_i}$, then the p^{a_i} are uniquely determined by A. We call $(p^{a_1}, \dots, p^{a_m})$ the type of A. If Exp $A = p$, we call A elementary abelian.

(14) The largest common divisor of integers m, n we denote by (m, n). If p is a prime, $p^a | n$ and $p^{a+1} \nmid n$, we write $p^a \top n$.

(15) Notations from linear algebra are standard. We use freely factor spaces and tensor products of vector spaces. The transpose of a matrix A we denote by A^t.

§ 1 Representations and representation modules

Let G always be a finite group and K any commutative field.

1.1 Definition. a) Let V be a K-vector space with $\dim_K V = n < \infty$. A representation D of G on V is a group homomorphism of G into the group $GL(V)$ of all invertible linear mappings of V onto itself. Then we call V a G-module over K for D and $n = \dim_K V$ the degree of D. We write linear mappings always to the right of the vectors, hence we write $vD(g)$. As the neutral element 1 of G is mapped onto the neutral element in $GL(V)$, we obtain

$$vD(1) = v \quad \text{for all } v \in V.$$

b) The kernel of D, defined by

$$\operatorname{Ker} D = \operatorname{Ker} V = \{g \mid g \in G, D(g) = E_n\}$$

is a normal subgroup of G. The representation theory is sometimes a powerful tool to show the existence of normal subgroups of G. (We shall meet important examples in 15.3, 16.1, 17.9 and 45.1.)

We call D faithful and V a faithful G-module if $\operatorname{Ker} D = \{1\}$.

To connect representation theory of groups with the more general theory of algebras, following Emmy Noether, we introduce the group algebra.

1.2 Definition. We introduce the group algebra KG of G over K by

$$KG = \bigoplus_{g \in G} Kg,$$

where the basis elements g of KG are multiplied according to the multiplication in G. Then KG is an associative K-algebra with $\dim_K KG = |G|$. The neutral element of KG is the neutral element of G.

1.3 Definition. By a K-algebra A we always understand an associative K-algebra with neutral element 1 and with $\dim_K A < \infty$.

a) An A-module V is a right A-module such that $\dim_K V < \infty$ and $v1 = v$ for all $v \in V$.

b) Let V_1 and V_2 be A-modules. We define

$$\begin{aligned}&\operatorname{Hom}_A(V_1, V_2)\\&\quad = \{\alpha \mid \alpha \in \operatorname{Hom}_K(V_1, V_2), (v_1 a)\alpha = (v_1 \alpha)a \quad \text{for all } v_1 \in V_1, a \in A\}.\end{aligned}$$

Obviously $\operatorname{Hom}_A(V_1, V_2)$ is a K-vector space and $\operatorname{Hom}_K(V, V)$ a K-algebra.

We call V_1 and V_2 isomorphic A-modules if there does exist a bijective α in $\operatorname{Hom}_A(V_1, V_2)$. Isomorphism is an equivalence relation.

c) Let V be an A-module. A subset $U \neq \varnothing$ is called an A-submodule if $ua \in U$ for all $u \in U$ and $a \in A$. (Then U is a K-subspace of V.) The factor space

$$V/U = \{v + U \mid v \in V\}$$

then becomes an A-module by the obviously well defined definition

$$(v + U)a = va + U \quad \text{for } v \in V, a \in A.$$

d) If U_1, U_2, U_3 are A-submodules of V, then $U_1 \cap U_2$ and

$$U_1 + U_2 = \{u_1 + u_2 \mid u_i \in U_i\}$$

are A-submodules. If $U_1 \cap U_2 = 0$, we write $U_1 + U_2 = U_1 \oplus U_2$.

We have the isomorphism as A-modules

$$(U_1 + U_2)/U_2 \cong U_1/(U_1 \cap U_2)$$

by the mapping α with

$$(u_1 + U_2)\alpha = u_1 + U_1 \cap U_2.$$

Finally we have the socalled Dedekind identity: If $U_1 \subseteq U_3$, then

$$(U_1 + U_2) \cap U_3 = U_1 + (U_2 \cap U_3).$$

The notions in 1.1 and 1.3 do agree:

1.4 Remarks. a) If V is a G-module over K in the sense of 1.1, then V becomes a KG-module in the sense of 1.3 by

$$v \sum_{g \in G} a_g g = \sum_{g \in G} a_g v D(g)$$

for $v \in V$, $a_g \in K$.

b) Conversely, if V is a KG-module in the sense of 1.3, then we obtain a representation D of G over K by

$$vD(g) = vg \quad \text{for } v \in V, g \in G.$$

For then

$$vD(g_1 g_2) = v(g_1 g_2) = (vg_1)g_2 = (vD(g_1))D(g_2),$$

hence D is a homomorphism of G into the linear group $GL(V)$.
c) Let V be a KG-module. Introducing a K-basis of V, we obtain a homomorphism

$$g \to D(g) = (a_{ij}(g))$$

of G into the group of invertible matrices in the full matrix algebra $(K)_n$, where $n = \dim_K V$. We speak then of a matrix representation. We call two such matrix representations D_1 and D_2 equivalent, if the corresponding KG-modules V_i are isomorphic in the sense of 1.3b). This means the existence of a non-singular matrix T such that

$$T^{-1}D_1(g)T = D_2(g) \quad \text{for all } g \in G.$$

An important "internal" application of representation theory in group-theory appears in the following way.

1.5 Application. Let N be an elementary abelian normal subgroup of G (for instance a minimal normal subgroup of a solvable group G). Then

$$N = \langle x_1 \rangle \times \cdots \times \langle x_n \rangle$$

and $x_j^p = 1$ for some prime p. If $g \in G$, we have equations

$$x_i^g = g^{-1}x_i g = \prod_{j=1}^{n} x_j^{a_{ij}(g)},$$

where $a_{ij}(g) \in GF(p)$. Putting $D(g) = (a_{ij}(g))$ we obtain a matrix representation D of G over $GF(p)$, for the equation

$$\prod_{j=1}^{n} x_j^{a_{ij}(g_1 g_2)} = g_2^{-1}(g_1^{-1}x_i g_1)g_2 = g_2^{-1} \prod_{k=1}^{n} x_k^{a_{ik}(g_1)} g_2$$

$$= \prod_{k=1}^{n} (g_2^{-1}x_k g_2)^{a_{ik}(g_1)} = \prod_{j,k=1}^{n} x_j^{a_{kj}(g_2)a_{ik}(g_1)}$$

shows

$$a_{ij}(g_1 g_2) = \sum_{k=1}^{n} a_{ik}(g_1) a_{kj}(g_2),$$

hence

$$D(g_1 g_2) = D(g_1) D(g_2).$$

Obviously

$$\operatorname{Ker} D = \{g \mid xg = gx \quad \text{for all } x \in N\} = C_G(N) \geqslant N.$$

Unfortunately, our later standard assumptions "K algebraically closed and Char $K \nmid |G|$" are not fulfilled in this case. It belongs to the "modular representation theory" over fields of characteristic different from 0.

We describe several procedures to construct representations:

1.6 Examples.
a) Let V be a KG-module with Ker $V = N$. Then V is also a KG/N-module by

$$v(gN) = vg.$$

If conversely V is a KG/N-module, it becomes a KG-module by

$$vg = v(gN).$$

b) If D is a representation of G over K, then λ, defined by

$$\lambda(g) = \det D(g)$$

defines a representation λ of degree 1. If in particular $G = G'$, then $G = \operatorname{Ker} \lambda$ and so $\det D(g) = 1$ for all $g \in G$.
c) Let D be a representation of G over K and $\lambda \in \operatorname{Hom}(G, K^\times)$. Then D', defined by $D'(g) = \lambda(g)D(g)$ is obviously also a representation of G. (This is a special case of forming products of representations, as we shall see in § 8.)
d) Let D be a matrix representation of G over K, say

$$D(g) = (a_{ij}(g)).$$

Let α be a field automorphism of K. Then D^α, defined by

$$D^\alpha(g) = (a_{ij}(g)^\alpha)$$

is also a representation, for we have

$$a_{ij}(g_1g_2)^\alpha = \left(\sum_{k=1}^{n} a_{ik}(g_1)a_{kj}(g_2)\right)^\alpha = \sum_{k=1}^{n} a_{ik}(g_1)^\alpha a_{kj}(g_2)^\alpha.$$

e) Suppose D is a representation of G on a KG-module V and K_0 is a subfield of K with $(K:K_0) < \infty$. As

$$\dim_{K_0} V = (K:K_0)\dim_K V < \infty,$$

so V is also a K_0G-module. Let $\{v_1, \dots, v_n\}$ be a K-basis of V and $\{k_1, \dots, k_m\}$ a K_0-basis of K. Then

$$V = \bigoplus_{i=1}^{n} Kv_i = \bigoplus_{i=1}^{n}\bigoplus_{j=1}^{m} K_0k_jv_i.$$

Suppose the matrix representation of G on the KG-module is given by

$$v_ig = \sum_{k=1}^{n} a_{ik}(g)v_k,$$

where $a_{ik}(g) \in K$. We also have formulas

$$k_jx = \sum_{r=1}^{m} b_{jr}(x)k_r \quad \text{for } x \in K,$$

where $b_{jr}(x) \in K_0$. Then

$$(k_jv_i)g = k_j\sum_{k=1}^{n} a_{ik}(g)v_k = \sum_{k=1}^{n}\sum_{r=1}^{m} b_{jr}(a_{ik}(g))k_rv_k.$$

The trace of the K_0-linear mapping induced by g on V is therefore

$$\sum_{r=1}^{m}\sum_{k=1}^{n} b_{rr}(a_{kk}(g)) = \sum_{r=1}^{m} b_{rr}\left(\sum_{k=1}^{n} a_{kk}(g)\right) = \mathrm{trace}_{K:K_0}(\mathrm{trace}(a_{ij}(g))).$$

Here $\mathrm{trace}_{K:K_0}$ is the usual trace of the field-extension $K:K_0$.

f) Let V be a KG-module and let $V^* = \mathrm{Hom}_K(V, K)$ be the K-vector space dual to V. We write conventionally $\alpha(v)$ for $\alpha \in V^*$, $v \in V$. Then V^* becomes a KG-module by

$$(\alpha g)(v) = \alpha(vg^{-1}).$$

For we have

$$(\alpha(g_1g_2))(v) = \alpha(vg_2^{-1}g_1^{-1}) = (\alpha g_1)(vg_2^{-1}) = ((\alpha g_1)g_2)(v).$$

Let $\{v_1, \ldots, v_n\}$ be a K-basis of V and $\{\alpha_1, \ldots, \alpha_n\}$ the dual basis of V^*, defined by

$$\alpha_i(v_j) = \delta_{ij} \quad (i, j = 1, \ldots, n).$$

Suppose

$$v_i g = \sum_{r=1}^{n} a_{ir}(g) v_r$$

and

$$\alpha_j g = \sum_{k=1}^{n} b_{jk}(g)\alpha_k.$$

Then we have

$$(\alpha_j g)(v_i) = \sum_{k=1}^{n} b_{jk}(g)\alpha_k(v_i) = b_{ji}(g) = \alpha_j(v_i g^{-1}) = \alpha_j\left(\sum_{r=1}^{n} a_{ir}(g^{-1})v_r\right) = a_{ij}(g^{-1}).$$

Hence the matrix representation of G on V^* with respect to the basis $\{\alpha_1, \ldots, \alpha_n\}$ is given by

$$D^*(g) = (b_{ij}(g)),$$

where $b_{ij}(g) = a_{ji}(g^{-1})$. Hence

$$D^*(g) = D(g^{-1})^t = (D(g)^{-1})^t,$$

where t is the transposition operator. D^* is often called the representation contragredient to D.

(For general algebras, V^* would be a left A-module. The antiautomorphism of KG given by $g \to g^{-1}$ allows in the case of group algebras to consider V^* again as a right module.)

Exercises

E1.1 Let $Q = \langle a, b \rangle$ be the quaternion group of order 8, where

$$a^4 = 1, \quad a^2 = b^2, \quad b^{-1}ab = a^{-1}.$$

a) Let K be a field with Char $K \neq 2$, which contains elements c, d with

$$c^2 + d^2 = -1.$$

Then a faithful representation D of Q is given by

$$D(a) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad D(b) = \begin{pmatrix} c & d \\ d & -c \end{pmatrix}.$$

b) Suppose that there exists a faithful KQ-module V of dimension 2. Then there exist $c, d \in K$ with $c^2 + d^2 = -1$. (Show at first that there is a basis of V such that $D(a) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.)

c) If K is a finite field with Char $K \neq 2$, there exists a faithful KQ-module of dimension 2.

d) There does not exist a faithful $\mathbb{R}Q$-module of dimension 2, but there exists a faithful $\mathbb{R}Q$-module of dimension 4.

E1.2 Let V be a KG-module and U a submodule of V.

a) $U^\perp = \{\alpha \mid \alpha \in V^*, \alpha(u) = 0 \text{ for all } u \in U\}$ is a submodule of V^*, and we have the KG-isomorphism $V^*/U^\perp \cong U^*$.

b) $V \cong V^{**}$ as KG-modules.

§ 2 Simple and semisimple modules

2.1 Definition. Let A be a K-algebra.
a) An A-module V is called simple (irreducible) if $V \neq 0$ and if 0 and V are the only A-submodules of V.

In the case $A = KG$ we call the representation D of G on a simple KG-module V irreducible. If D is not irreducible we call it reducible.
b) An A-module V is called semisimple, if

$$V = \bigoplus_{j=1}^{k} V_j$$

with simple A-modules V_j. (Here we allow also $k = 0$, hence the zero-module is called semisimple, but not simple!)

2.2 Proposition. *Let V be an A-module. Then the following statements are equivalent*:
a) *V is semisimple.*
b) *$V = \sum_{j=1}^{n} V_j$ with simple A-modules V_j.*
c) *If U is an A-submodule of V, there exists an A-submodule U' such that $U \cap U' = 0$, $V = U + U'$, hence $V = U \oplus U'$.*

Proof. a) $\Rightarrow$ b): As V is semisimple, we have

$$V = \bigoplus_{j=1}^{k} V_j = \sum_{j=1}^{k} V_j$$

with simple KG-modules V_j.
b) $\Rightarrow$ c): Let U' be a submodule of V such that $U \cap U' = 0$ and $\dim_K U'$ maximal. Suppose $U + U' < V$. As $V = \sum_{j=1}^{k} V_j$ with simple V_j, there exists j such that $V_j \nleq U + U'$. As V_j is simple, we obtain

$$(U + U') \cap V_j = 0.$$

Hence $U' < U' + V_j$ and by maximality of U' therefore

$$0 \neq U \cap (U' + V_j).$$

Take

$$0 \neq u = u' + v_j,$$

where $u \in U$, $u' \in U'$ and $v_j \in V_j$. Then

$$v_j = u - u' \in V_j \cap (U + U') = 0.$$

This shows

$$u = u' \in U \cap U' = 0,$$

a contradiction. Hence $V = U + U' = U \oplus U'$.
c $\Rightarrow$ a): We prove this by induction on $\dim_K V$. We can assume $V \neq 0$. As $\dim_K V < \infty$, there exists a simple A-submodule V_1 of V. By property c) we have

$$V = V_1 \oplus V'$$

with an A-module V'. We claim that also V' has the property stated in c):

Let U be a submodule of V'. Then $V = U \oplus U'$ for some submodule U' of V. Then by Dedekind's identity in 1.3d)

$$V' = V' \cap (U \oplus U') = U \oplus (V' \cap U').$$

By induction $V' = \bigoplus_{j=2}^{k} V_j$ for some simple modules V_j, so

$$V = \bigoplus_{j=1}^{k} V_j.$$

q.e.d.

The next theorem is very elementary, but one of the most effective tools. It allowed I. Schur to give a new foundation of the character theory of Frobenius, as we shall see in § 3.

2.3 Theorem (Schur's lemma). *Let V be an A-module.*
a) *If V is simple, then* $\mathrm{Hom}_A(V, V)$ *is a skew field.*
b) *If V is simple and K algebraically closed, then* $\mathrm{Hom}_A(V, V) = K$.
c) *If V is semisimple and* $\mathrm{Hom}_A(V, V)$ *is a skew field, then V is simple.*

Proof. a) Suppose $0 \neq \alpha \in \mathrm{Hom}_A(V, V)$. Then $0 < V\alpha \leqslant V$. If $v \in V$ and $a \in A$, then

$$(v\alpha)a = (va)\alpha \in V\alpha.$$

Hence $V\alpha$ is an A-submodule of V. As V is simple, so $V\alpha = V$. As $\dim_K V < \infty$, we see that α is invertible, hence there exists $\alpha^{-1} \in \mathrm{Hom}_K(V, V)$. (We could show as easily that $\mathrm{Ker}\,\alpha = 0$, hence finite dimension of V is not really needed in the proof of a).)

Take $v \in V$. Then $v = w\alpha$ for some $w \in V$. For every $a \in A$ follows

$$va = (w\alpha)a = (wa)\alpha,$$

hence

$$(va)\alpha^{-1} = wa = (v\alpha^{-1})a.$$

This proves $\alpha^{-1} \in \mathrm{Hom}_A(V, V)$, so $\mathrm{Hom}_A(V, V)$ is a skew field.
b) If $\alpha \in \mathrm{Hom}_A(V, V)$, then α has an eigenvalue c in the algebraically closed field K. Then

$$\alpha - c1_V \in \mathrm{Hom}_G(V, V).$$

As $\alpha - c1_V$ is not invertible, by a) $\alpha = c1_V$.
c) If V is not simple, then $V = V_1 \oplus V_2$ with A-modules $V_i \neq 0$. We define the projections $\pi_j \in \mathrm{Hom}_A(V, V)$ by

$$(v_1 + v_2)\pi_1 = v_1, \quad (v_1 + v_2)\pi_2 = v_2$$

for $v_j \in V_j$. Then $\pi_j \neq 0$, but $\pi_1\pi_2 = 0$. Hence $\mathrm{Hom}_A(V, V)$ is not a skew field, a contradiction. q.e.d.

(The statement in c) is in general *not* true without the assumption that V is semisimple; see exercise E2.4.)

2.4 Lemma. *Let K be a field and U a finite subgroup of the multiplicative group $K^\times$ of K. Then U is cyclic.*

Proof. Let

$$U = U_1 \times \cdots \times U_m$$

be the decomposition of U into its Sylow subgroups U_i, where $|U_i| = p_i^{a_i}$. As the number of zeros of the polynomial $x^{p_i} - 1$ in K is at most p_i, so U_i is cyclic, say $U_i = \langle z_i \rangle$. Then we easily see

$$U = \langle z_1 \rangle \times \cdots \times \langle z_m \rangle = \langle z_1 \ldots z_m \rangle,$$

and U is cyclic. q.e.d.

2.5 Proposition. *Let V be a simple, faithful KG-module and D the representation of G on V.*
a) *The center $Z(G)$ of G is cyclic.*
b) *If G is abelian, then G is cyclic.*
c) *If K is algebraically closed, then*

$$D(z) = \lambda(z)1_V \quad \textit{for } z \in Z(G),$$

where $\lambda \in \mathrm{Hom}(Z(G), K^\times)$.

d) *If G is abelian and K algebraically closed, then* $\dim_K V = 1$.

Proof. a) For $v \in V$, $g \in G$ and $z \in Z(G)$ we have

$$vD(z)D(g) = vD(zg) = vD(gz) = vD(g)D(z).$$

Hence

$$D(z) \in \mathrm{Hom}_G(V, V).$$

By 2.3a) $\mathrm{Hom}_G(V, V)$ is a skew field. Hence

$$S = \{D(z) | z \in Z(G)\}$$

is a finite subgroup of the commutative subfield

$$L = K(D(z) | z \in Z(G))$$

of $\mathrm{Hom}_G(V, V)$. By 2.4 S is cyclic. As D is faithful, also $Z(G)$ is cyclic.
b) follows from a) as $G = Z(G)$ for abelian G.
c) In this case, we have by 2.3b)

$$D(z) \in \mathrm{Hom}_G(V, V) = K1_V.$$

d) follows from c). q.e.d.

2.6 Proposition. *Let K be algebraically closed, V a simple KG-module and A an abelian subgroup of G. Then*

$$\dim_K V \leqslant |G : A|.$$

Proof. Let $G = \bigcup_{j=1}^m Ag_j$, where $m = |G : A|$. Let V_0 be a simple KA-submodule of V. By 2.5d) $\dim_K V_0 = 1$, hence $V_0 = Kv_0$. Now $v_0 a = \lambda(a)v_0$ for

$a \in A$, where $\lambda \in \mathrm{Hom}(A, K^\times)$. We consider the K-subspace

$$W = \langle v_0 g_1, \ldots, v_0 g_m \rangle$$

of V. If $g \in G$, then $g_j g = a_j g_{j'}$ for some $a_j \in A$ and some $g_{j'}$. Then

$$v_0 g_j g = v_0 a_j g_{j'} = \lambda(a_j) v_0 g_{j'} \in W.$$

Hence W is a KG-module. As V is simple, so $V = W$ and

$$\dim_K V = \dim_K W \leqslant m = |G : A|. \qquad \text{q.e.d.}$$

2.7 Remark. The inequality in 2.6 is in most cases not very useful. A much more important fact is the following theorem of N. Ito:

Let K be algebraically closed with $\mathrm{Char}\, K = 0$, V a simple KG-module and A an abelian normal subgroup of G. Then $\dim_K V$ divides $|G/A|$. (We will prove this in 19.9.)

2.8 Example. Let A be an abelian subgroup of G with $|G : A| = 2$. Then $A \lhd G$. Suppose

$$G = A \cup Ab,$$

where $b^2 = a_0 \in A$. Let K be algebraically closed and V a simple KG-module. By 2.6 $\dim_K V \leqslant |G : A| = 2$. Suppose $\dim_K V = 2$. By 2.5d) there exists $0 \neq v_1 \in V$ such that

$$v_1 a = \lambda(a) v_1 \quad \text{for all } a \in A,$$

where $\lambda \in \mathrm{Hom}(A, K^\times)$. As Kv_1 is not a KG-submodule, so $v_2 = v_1 b \notin Kv_1$. Hence $\{v_1, v_2\}$ is a K-basis of V. As $bab^{-1} \in A$, we obtain

$$v_2 a = v_1 bab^{-1} b = \lambda(bab^{-1}) v_1 b = \lambda(bab^{-1}) v_2$$

and

$$v_2 b = v_1 b^2 = \lambda(a_0) v_1.$$

Hence the matrix representation of G with respect to the basis $\{v_1, v_2\}$ is given by

$$D(a) = \begin{pmatrix} \lambda(a) & 0 \\ 0 & \lambda(bab^{-1}) \end{pmatrix} \quad \text{for } a \in A,$$

$$D(b) = \begin{pmatrix} 0 & 1 \\ \lambda(a_0) & 0 \end{pmatrix}.$$

It is easy to see conversely that D is really a representation of G. If $\lambda(bab^{-1}) = \lambda(a)$ for all $a \in A$, then $G' \leqslant \operatorname{Ker} D$ and by 2.5d) D has to be reducible.

Assume there is some $a_1 \in A$ such that $\lambda(ba_1b^{-1}) \neq \lambda(a_1)$. Then the only subspaces invariant under $D(a_1)$ are Kv_1 and Kv_2. As these are permuted by $D(b)$, so V in this case is simple.

The set of available $\lambda \in \operatorname{Hom}(A, K^\times)$ depends on Char K and the structure of A. We come back to this example in 7.1.

2.9 Lemma. *Suppose $U \leqslant G$ and $G = \bigcup_{j=1}^n Ug_j$ with $n = |G:U|$. Let V be a KG-module and $\alpha \in \operatorname{Hom}_{KU}(V, V)$. Then β, defined for $v \in V$ by*

$$v\beta = \sum_{j=1}^{n} vg_j^{-1}\alpha g_j,$$

lies in $\operatorname{Hom}_{KG}(V, V)$.

Proof. Suppose $g \in G$ and

$$g_j g = u_j g_{j'} \in Ug_{j'}.$$

Then

$$(vg^{-1})\beta = \sum_{j=1}^{n} vg^{-1}g_j^{-1}\alpha g_j = \sum_{j=1}^{n} vg_{j'}^{-1}u_j^{-1}\alpha g_j = \sum_{j=1}^{n} vg_{j'}^{-1}\alpha u_j^{-1} g_j$$

$$= \sum_{j=1}^{n} vg_{j'}^{-1}\alpha g_{j'} g^{-1} = (v\beta)g^{-1}.$$

(For the last step observe that $j \to j'$ is bijective.) q.e.d.

2.10 Theorem. *Let V be a KG-module and $U \leqslant G$. Suppose W is a KG-submodule of V and $V = W \oplus W'$ with some KU-submodule W' of V. If* Char $K = 0$ *or* Char $K \nmid |G:U|$, *then there exists a KG-submodule W'' of V such that $V = W \oplus W''$.*

Proof. We define the projection $\pi \in \mathrm{Hom}_{KU}(V, V)$ by

$$v\pi = \begin{cases} v & \text{for } v \in W \\ 0 & \text{for } v \in W'. \end{cases}$$

If $G = \bigcup_{j=1}^{n} Ug_j$, we form by 2.9 $\beta \in \mathrm{Hom}_{KG}(V, V)$ such that

$$v\beta = \frac{1}{|G:U|} \sum_{j=1}^{n} vg_j^{-1}\pi g_j.$$

This is possible as Char $K \nmid |G:U|$.
(1) For $v \in W$ we have $vg_j^{-1} \in W$, as W is a KG-submodule, hence

$$(vg_j^{-1})\pi g_j = vg_j^{-1}g_j = v.$$

Hence $v\beta = v$ for $v \in W$.
(2) For every $v \in V$ we have

$$(vg_j^{-1})\pi g_j \in V\pi g_j = Wg_j = W,$$

hence also $V\beta \leqslant W$.

Put $W'' = \mathrm{Ker}\,\beta$. Then W'' is a KG-module. By (1) $W \cap W'' = 0$. If $v \in V$, then $v\beta \in W$ and

$$(v - v\beta)\beta = v\beta - v\beta = 0.$$

From

$$v = v\beta + (v - v\beta)$$

finally follows $V = W \oplus W''$. q.e.d.

2.11 Theorem (Maschke, I. Schur). *The following statements are equivalent:*
a) $K\sum_{g \in G} g$ *is a direct summand of the KG-module KG (KG being a KG-module by right multiplication.)*
b) Char $K \nmid |G|$. (*This should always include the case* Char $K = 0$.)
c) *Every KG-module is semisimple.*

Proof. a) $\Rightarrow$ b): Suppose

$$KG = K \sum_{g \in G} g \oplus A$$

with some KG-submodule A. As

$$\left(\sum_{g \in G} g\right)(1 - h) = 0$$

for every $h \in G$, we obtain

$$1 - h \in KG(1 - h) = A(1 - h) \subseteq A.$$

As $\dim_K A = |G| - 1$, this implies

$$\begin{aligned} A &= \langle 1 - h | h \in G \rangle \quad \text{(as } K\text{-space)} \\ &= \left\{ \sum_{g \in G} a_g g \mid a_g \in K \quad \text{and} \quad \sum_{g \in G} a_g = 0 \right\}. \end{aligned}$$

As $\sum_{g \in G} g \notin A$, we see that

$$\sum_{g \in G} 1 = |G| \neq 0.$$

In case of Char $K = p > 0$ this means $p \nmid |G|$.
b) $\Rightarrow$ c): Let V be any KG-module and W a KG-submodule of V. Then $V = W \oplus W'$ for some K-vector space W'. As Char $K \nmid |G : E|$, by 2.10 there exists a KG-submodule W'' of V such that $V = W \oplus W''$. By 2.2 V is semisimple.
c) $\Rightarrow$ a): As in particular KG is a semisimple KG-module, the KG-submodule $K \sum_{g \in G} g$ is a direct summand of KG. q.e.d.

2.12 Theorem. *Suppose* Char $K \nmid |G|$.
a) *If D is a matrix representation of G over K, there exists a nonsingular matrix T such that*

$$T^{-1}D(g)T = \begin{bmatrix} D_1(g) & & 0 \\ & \ddots & \\ 0 & & D_k(g) \end{bmatrix}$$

for all $g \in G$, where the D_i are irreducible matrix representations of G.
b) *If G is abelian and K algebraically closed, then*

$$T^{-1}D(g)T = \begin{bmatrix} \lambda_1(g) & & 0 \\ & \ddots & \\ 0 & & \lambda_k(g) \end{bmatrix},$$

where $\lambda_j \in$ Hom$(G, K^{\times})$.

Proof. a) Let V be a KG-module for D. By 2.11

$$V = V_1 \oplus \cdots \oplus V_k$$

with simple KG-module V_i. Taking a K-basis of V which is the union of K-bases of the V_i, we obtain the statement.
b) If G is abelian and K algebraically closed, then $\dim_K V_i = 1$ by 2.5d).

q.e.d.

We describe now the original approach by Maschke, which only works over the fields $\mathbb{R}$ or $\mathbb{C}$:

2.13 Theorem (Maschke). *Let V be a KG-module for $K = \mathbb{R}$ or $K = \mathbb{C}$.*
a) *There exists on V a positive definite symmetric or hermitean scalar product $[\cdot, \cdot]$ such that*

$$[v_1 g, v_2 g] = [v_1, v_2]$$

for all $v_i \in V$ and all $g \in G$.
b) *If $\{v_1, \ldots, v_n\}$ is an orthonormal basis of V with respect to $[\cdot, \cdot]$, the corresponding matrices $D(g)$ are orthogonal resp. unitary.*
c) *If W is a KG-submodule of V, then $V = W \oplus W^\perp$, where*

$$W^\perp = \{v \mid [v, w] = 0 \quad \textit{for all } w \in W\}$$

is a KG-module. In particular V is semisimple.

Proof. a) Let $(\cdot, \cdot)$ by any positive definite scalar product on V. We put

$$[v_1, v_2] = \sum_{g \in G} (v_1 g, v_2 g), \quad \text{for } v_j \in V.$$

Then $[\cdot, \cdot]$ is a scalar product, and obviously

$$[v_1 g, v_2 g] = [v_1, v_2].$$

If $v \neq 0$, then

$$[v, v] \geqslant (v, v) > 0,$$

hence $[\cdot, \cdot]$ is positive definite.
b) follows from a).
c) As $[\cdot, \cdot]$ is positive definite, we have $V = W \oplus W^\perp$. If $w \in W$, $w' \in W^\perp$ and $g \in G$, then

$$[w'g, w] = [w', wg^{-1}] = 0$$

as $wg^{-1} \in W$. Hence $w'g \in W^{\perp}$, so $W^{\perp}$ is a KG-submodule. q.e.d.

Observe that we used the process of averaging over the group G in the proofs of 2.9 and again in 2.13. The proof of 2.13a) would not work over fields of positive characteristic, for the scalar product $[\cdot, \cdot]$ might very well become singular or even identically zero.

We add an important theorem on semisimplicity, which is true for any field:

2.14 Theorem (A.H. Clifford). *Let K be any field, V a simple KG-module and $N \trianglelefteq G$. Then V, considered as a KN-module, is semisimple.*

Proof. Let W be a simple KN-submodule of V of smallest possible dimension.
If $g \in G$ and $h \in N$, then

$$Wgh = Wghg^{-1}g = Wg$$

as $ghg^{-1} \in N$. Hence Wg is a KN-module. As $\dim_K Wg = \dim_K W$, so Wg is also a simple KN-module. As $\sum_{g \in G} Wg$ is a KG-module, so the simplicity of V implies $V = \sum_{g \in G} Wg$. Hence by 2.2 V is a semisimple KN-module. q.e.d.

2.15 Remark. It is easy to see that in 2.14 we have

$$V = \bigoplus_{j=1}^{m} Wg_j$$

for some g_j. Hence the simple KN-modules Wg_j are all of the same dimension.
Considerably deeper is the following fact: If K is algebraically closed and Char $K = 0$, then m divides $|G/N|$. Hence in particular if $(\dim_K V, |G/N|) = 1$, then V is also a simple KN-module. (We come back to this topic in great detail in § 19–22.)
Finally we state a fact that shows that theorem 2.11 can become totally wrong if Char $K = p$ divides $|G|$:

2.16 Proposition. *Suppose* Char $K = p$ *and* $|G| = p^a$.
a) *The vector space K with trivial action of G is the only simple KG-module.*
b) *If V is a semisimple KG-module, then $vg = v$ for every $v \in V$, $g \in G$.*

Proof. a) Take $0 \neq v \in V$, where V is a simple KG-module and form

$$W = \sum_{g \in G} GF(p)vg.$$

Then W is a $GF(p)$-vector space, hence $|W| = p^b$ for some b. The orbits of G on W have lengths which are powers of p. Hence there are at least p orbits of length 1, so there exists $0 \neq v \in W$ with $vg = v$ for all $g \in G$. Then $V = Kv$ and $\dim_K V = 1$.
b) This follows from a). q.e.d.

Exercises

E2.1 Determine the isomorphism types of simple KG-modules for the symmetric group $G = S_3$. (The number of such types is 3 if Char $K \neq 2, 3$; 2 if Char $K = 2$ or 3.)

E2.2 a) Let V be a vector space of dimension n over the finite field $K = GF(q)$ and let A be an abelian group such that V is a simple, faithful KA-module. Show $|A| \mid q^n - 1$, and n is the smallest integer with this property. Also A is cyclic. (Use that $A \subseteq \mathrm{Hom}_A(V, V)$ and $v_0 \,\mathrm{Hom}_A(V, V) = V$ for any $0 \neq v_0 \in V$.)
b) Take $V = GF(q^n)$. Then V is a simple $GF(q)A$-module for $A = GF(q^n)^\times$.

E2.3 Suppose Char $K = p$ and $|G| = p^a$.
a) The only maximal submodule of KG, considered as KG-module by right multiplication, is the so-called augmentation module

$$\left\{\sum_{g \in G} a_g g \,|\, a_g \in K, \sum_{g \in G} a_g = 0\right\}$$

b) $K \sum_{g \in G} g$ is the only minimal submodule of KG.

E2.4 Suppose K is a finite field with $|K| = q > 2$ and $V = Kv_1 \oplus Kv_2$. Let G be the group of all linear mappings in $GL(V)$ such that

$$v_1 g = a_{11}(g) v_1$$

$$v_2 g = a_{21}(g) v_1 + a_{22}(g) v_2,$$

where $a_{11}(g) a_{22}(g) \neq 0$. Show that V is reducible, but $\mathrm{Hom}_K(V, V) = K$. (Hence by 2.3c) V is not semisimple.)

§ 3 Orthogonality relations

In this section we prove some of the most fundamental theorems in representation theory.

3.1 Notations. Suppose $g_1, g_2 \in G$. We call g_1 and g_2 conjugate in G if there exists some $y \in G$ such that

$$g_2 = y^{-1}g_1y = g_1^y.$$

Conjugacy is obviously an equivalence relation. We form the conjugacy classes

$$K_i = g_i^G = \{g_i^y \mid y \in G\} \qquad (i = 1, \ldots, h(G)).$$

Then

$$G = \bigcup_{i=1}^{h(G)} K_i$$

is a partition of G, hence

$$|G| = \sum_{i=1}^{h(G)} |K_i|.$$

$h(G)$ is called the class number of G. We put

$$C_G(g_i) = \{y \mid y \in G,\, yg_i = g_iy\}.$$

If

$$G = \bigcup_{j=1}^{h_i} C_G(g_i)y_{ij} \quad \text{(disjoint)},$$

then we easily see that

$$K_i = \{g_i^{y_{ij}} \mid j = 1, \ldots, h_i\}.$$

Therefore

$$|K_i| = |G : C_G(g_i)| = h_i.$$

Hence

$$|G| = \sum_{i=1}^{h(G)} h_i.$$

(Usually we make the choice $g_1 = 1$, hence $h_1 = 1$.)

3.2 Definition. a) A function f from G into a field K is called a class function on G, if $f(g^h) = f(g)$ for all $g, h \in G$. Hence f is constant on the conjugacy classes $K_1, \ldots, K_{h(G)}$ of G. The set $C(G, K)$ of all class functions on G is obviously a K-vector space of dimension $h(G)$.
b) Let V be a KG-module and D the representation of G on V. We call the function χ, defined by

$$\chi(g) = \operatorname{trace} D(g),$$

the character of V and of D.

3.3 Proposition. *Let V be a KG-module with character χ.*
a) *$\chi(g^h) = \chi(g)$ for all $g, h \in G$. Hence χ is a class function on G.*
b) *Isomorphic KG-modules have the same character.*
c) *If*

$$V = V_1 \oplus \cdots \oplus V_m$$

with KG-modules V_i, then

$$\chi = \sum_{k=1}^{m} \chi_i,$$

where χ_i is the character of V_i.

Proof. a) Let D be the representation of G on V. Then

$$\chi(g^h) = \operatorname{trace} D(h^{-1}gh) = \operatorname{trace} D(h)^{-1}D(g)D(h) = \operatorname{trace} D(g) = \chi(g)$$

by a well-known property of the trace.
b) Let V_1 and V_2 be isomorphic KG-modules and D_i the corresponding representations. Then there exists a $T \in \operatorname{Hom}_K(V_1, V_2)$ such that

$$D_1(g)T = TD_2(g).$$

Hence

$$\text{trace } D_1(g) = \text{trace } TD_2(g)T^{-1} = \text{trace } D_2(g).$$

c) is obvious. q.e.d.

3.4 Theorem (I. Schur). *Suppose that D_1 and D_2 with*

$$D_1(g) = (a_{ij}(g)), \quad D_2(g) = (b_{kl}(g))$$

are irreducible matrix representations of G over K.
a) *If D_1 and D_2 are not equivalent, then*

$$\sum_{g \in G} a_{ij}(g) b_{kl}(g^{-1}) = 0$$

for all i, j, k, l.
b) *Suppose that K is algebraically closed and* Char $K \nmid |G|$. *Then* Char K *does not divide the degree n_1 of D_1 and*

$$\sum_{g \in G} a_{ij}(g) a_{kl}(g^{-1}) = \delta_{jk} \delta_{il} \frac{|G|}{n_1}.$$

Proof. We put degree $D_j = n_j$. Let $X = (x_{rs})$ be an arbitrary matrix of type (n_1, n_2) over K. We form

$$T(X) = \sum_{g \in G} D_1(g) X D_2(g^{-1}).$$

Then for all $h \in G$ we obtain

$$\begin{aligned} D_1(h)T(X) &= \sum_{g \in G} D_1(h) D_1(g) X D_2(g^{-1}) D_2(h^{-1}) D_2(h) \\ &= \sum_{g \in G} D_1(hg) X D_2((hg)^{-1}) D_2(h) \\ &= T(X) D_2(h). \end{aligned}$$

If V_i are KG-modules for D_i, this means $T(X) \in \mathrm{Hom}_G(V_1, V_2)$.
a) Suppose D_1 and D_2 are not equivalent, hence $V_1 \not\cong V_2$. As V_i is simple, so $\mathrm{Hom}_G(V_1, V_2) = 0$, hence $T(X) = 0$ for every choice of X. We specialize $x_{rs} = \delta_{rj} \delta_{sk}$. Then the (i, l)-entry of $T(X)$ is

$$0 = \sum_{g \in G} \sum_{r,s} a_{ir}(g) x_{rs} b_{sl}(g^{-1}) = \sum_{g \in G} a_{ij}(g) b_{kl}(g^{-1}).$$

b) If K is algebraically closed, then by 2.3b)

$$\operatorname{Hom}_G(V_1, V_1) = K.$$

If we form $T(X)$ with $D_1 = D_2$, this implies

$$T(X) = t(X)E_{n_1} \text{ for some } t(X) \in K.$$

Then

$$t(X)n_1 = \text{trace } T(X) = \text{trace} \sum_{g \in G} D_1(g)XD_1(g)^{-1} = |G| \text{ trace } X.$$

Again we specialize $X_{jk} = (x_{rs})$ with $x_{rs} = \delta_{rj}\delta_{sk}$. Then trace $X_{jk} = \delta_{jk}$ and

$$t(X_{jk})n_1 = |G|\,\delta_{jk}.$$

Taking $j = k$, we see that Char $K \nmid n_1$ as Char $K \nmid |G|$. Hence we obtain

$$\sum_{g \in G} D_1(g)X_{jk}D_1(g^{-1}) = \delta_{jk}\frac{|G|}{n_1}E_{n_1}.$$

This implies

$$\sum_{g \in G} a_{ij}(g)a_{kl}(g^{-1}) = \delta_{jk}\delta_{il}\frac{|G|}{n_1}. \qquad \text{q.e.d.}$$

3.5 Theorem (Frobenius). a) *Let V_i $(i = 1, 2)$ be simple KG-modules with characters χ_i. If $V_1 \not\cong V_2$, then*

$$\sum_{g \in G} \chi_1(g)\chi_2(g^{-1}) = 0.$$

b) *Suppose K is algebraically closed and* Char $K \nmid |G|$. *If V is a simple KG-module with character χ, then*

$$\sum_{g \in G} \chi(g)\chi(g^{-1}) = |G| \neq 0.$$

c) *Suppose K is algebraically closed with* Char $K \nmid |G|$. *If V_1 and V_2 are simple non-isomorphic KG-modules, they have different characters. (Hence the simple modules are distinguished by their characters.)*

Proof. a) Let D_i be a matrix representation for V_i and

$$D_1(g) = (a_{ij}(g)), \quad D_2(g) = (b_{kl}(g)).$$

By 3.4a) we obtain

$$\sum_{g \in G} \chi_1(g)\chi_2(g^{-1}) = \sum_{g \in G} \sum_{i,j} a_{ii}(g)b_{jj}(g^{-1}) = \sum_{i,j} \sum_{g \in G} a_{ii}(g)b_{jj}(g^{-1}) = 0.$$

b) Similarly by 3.4b) we have

$$\sum_{g \in G} \chi(g)\chi(g^{-1}) = \sum_{g \in G} \sum_{i,j} a_{ii}(g)a_{jj}(g^{-1}) = \sum_{i,j} \delta_{ij} \frac{|G|}{n} = |G|,$$

if $n = \dim_K V$.
c) follows immediately by comparing a) and b). q.e.d.

3.6 Lemma. *Suppose* Char $K = 0$ *and let* χ *be the character of some* KG-*module.*
a) *If* ord $g = m$, *then* $\chi(g)$ *is the sum of some* m-*th roots of unity, hence lies in the cyclotomic field* $\mathbb{Q}_m = \mathbb{Q}(\varepsilon)$, *where* ε *is a primitive* m-*th root of unity.*
b) $\chi(g^{-1}) = \overline{\chi(g)}$. (*Observe that the complex conjugate is defined on* $\mathbb{Q}_m$, *but not necessarily on* K.) *In particular*

$$\sum_{g \in G} \chi(g)\chi(g^{-1}) > 0.$$

Proof. a) Let D be a representation belonging to χ. As

$$D(g)^m = D(g^m) = D(1) = E,$$

the eigenvalues of $D(g)$ are m-th roots of unity. As $\chi(g) = \text{trace } D(g)$ is the sum of the eigenvalues of $D(g)$, so $\chi(g) \in \mathbb{Q}_m$.
b) If $D(g)$ has the eigenvalues $\varepsilon_1, \ldots, \varepsilon_n$, then $D(g^{-1}) = D(g)^{-1}$ has the eigenvalues $\varepsilon_1^{-1}, \ldots, \varepsilon_n^{-1}$. Therefore

$$\chi(g^{-1}) = \sum_{j=1}^{n} \varepsilon_j^{-1} = \sum_{j=1}^{n} \bar{\varepsilon}_j = \overline{\chi(g)}.$$

Hence

$$\sum_{g \in G} \chi(g)\chi(g^{-1}) = \sum_{g \in G} |\chi(g)|^2 > 0. \qquad \text{q.e.d.}$$

3.7 Theorem. *Suppose K is algebraically closed and* Char $K \nmid |G|$.
We consider KG as a right KG-module. Suppose

$$KG = \bigoplus_{j=1}^{s} n_j V_j$$

with simple, non-isomorphic KG-modules V_j. If ρ is the character of KG and χ_j of V_j, then $n_j = \chi_j(1)$ and

$$\sum_{j=1}^{s} \chi_j(1)\chi_j(g) = \rho(g) = \begin{cases} |G| & \text{if } g = 1 \\ 0 & \text{if } g \neq 1. \end{cases}$$

The modules V_i ($i = 1, \ldots, s$) are all the simple KG-modules, up to isomorphism. (ρ is called the regular character of G.) If Char $K = 0$, *then $n_j = \dim_K V_j$ and*

$$|G| = \sum_{j=1}^{s} n_j^2.$$

Proof. As the basis G of KG is permuted without fixed points by right multiplication with any $1 \neq g \in G$, we obtain

$$\sum_{j=1}^{s} n_j\chi_j(g) = \rho(g) = \begin{cases} |G| & \text{if } g = 1 \\ 0 & \text{if } g \neq 1. \end{cases}$$

Let χ be the character of any simple KG-module. By 3.5 we obtain

$$\chi(1) = \frac{1}{|G|}\sum_{g \in G} \rho(g)\chi(g^{-1}) = \sum_{j=1}^{s} n_j \frac{1}{|G|}\sum_{g \in G} \chi_j(g)\chi(g^{-1})$$

$$= \begin{cases} n_j & \text{if } \chi = \chi_j \\ 0 & \text{if } \chi \neq \chi_1, \ldots, \chi_s. \end{cases}$$

By 3.4b), Char K does not divide the degree of a KG-module for χ, hence $\chi(1) \neq 0$ and $\chi = \chi_j$ for some j. Therefore

$$\rho(g) = \sum_{j=1}^{s} \chi_j(1)\chi_j(g) = \begin{cases} |G| & \text{if } g = 1 \\ 0 & \text{if } g \neq 1. \end{cases}$$

If Char $K = 0$, then

$$n_j = \chi_j(1) = \dim_K V_j$$

and

$$|G| = \sum_{j=1}^{s} n_j^2 \qquad \text{q.e.d.}$$

3.8 Lemma. *In the algebra KG we form the class sums*

$$k_i = \sum_{g \in K_i} g \quad (i = 1, \ldots, h(G)).$$

a) $\{k_1, \ldots, k_{h(G)}\}$ *is a K-basis of*

$$Z(KG) = \{x | x \in KG, xy = yx \textit{ for all } y \in KG\}.$$

b) *There exist nonnegative integers c_{ijl}* such that

$$k_i k_j = \sum_{l=1}^{h(G)} c_{ijl} k_l.$$

c) *Suppose $K_1 = \{1\}$ and*

$$K_{i'} = K_i^{-1} = \{g^{-1} | g \in K_i\}.$$

Then

$$c_{ij1} = \begin{cases} 0 & \textit{if } j \neq i' \\ h_i = |K_i| & \textit{if } j = i'. \end{cases}$$

Proof. a) $x = \sum_{g \in G} a_g g \in Z(G)$ is true if and only if $x = h^{-1}xh$ for all $h \in G$. This means that a_g is constant on the conjugacy classes K_i, hence

$$x = \sum_{i=1}^{h(G)} c_i k_i.$$

As the sets K_i are pairwise disjoint, the k_i are obviously linearly independent over K.

b) As $Z(KG)$ is an algebra, we have relations

$$k_i k_j = \sum_{l=1}^{h(G)} c_{ijl} k_l.$$

Here

$$c_{ijl} = |\{(g, g')|g \in K_i, g' \in K_j, gg' = g_l \in K_l\}|.$$

So c_{ijl} is a nonnegative integer.
c) If $j \neq i'$, then 1 does not appear in $k_i k_j$. If $j = i'$, for every $g \in K_i$ we have $g^{-1} \in K_j$. Hence 1 appears in $k_i k_{i'}$ with the multiplicity $h_i = |K_i|$. q.e.d.

3.9 Theorem. *Suppose K is algebraically closed and* Char $K \nmid |G|$. *Let χ be the character of a simple KG-module.*
a) $\dfrac{h_i\chi(g_i)}{\chi(1)} \cdot \dfrac{h_j\chi(g_j)}{\chi(1)} = \sum_{l=1}^{h(G)} c_{ijl} \dfrac{h_l\chi(g_l)}{\chi(1)}$, *where the c_{ijl} are as in* 3.8b).
b) $\dfrac{h_i\chi(g_i)}{\chi(1)}$ *is an eigenvalue of the integral matrix $(c_{ijl})_{j,l}$. (Statement* b) *will play in important role in* 6.5.)

Proof. a) Let D be a representation belonging to χ. We extend D linearly to a homomorphism of the group algebra KG. As $D(k_i)$ commutes with all $D(g)$ $(g \in G)$, by Schur's lemma 2.3b) we obtain

$$D(k_i) = \omega_i E \quad \text{for some } \omega_i \in K.$$

If $n =$ degree D and $g_i \in K_i$, we have

$$\omega_i\chi(1) = \text{trace } \omega_i E = \text{trace} \sum_{g \in K_i} D(g) = h_i\chi(g_i).$$

As Char $K \nmid n$ by 3.4b), so

$$\omega_i = \frac{h_i\chi(g_i)}{\chi(1)}.$$

Now we obtain from 3.8b)

$$D(k_i)D(k_j) = \sum_{l=1}^{h(G)} c_{ijl} D(k_l),$$

which implies the assertion.
b) We put

$$C_i = (c_{ijl}) \quad \text{and} \quad \mathfrak{f} = \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_{h(G)} \end{pmatrix}.$$

The equation in a) shows

$$\omega_i \mathfrak{f} = C_i \mathfrak{f}.$$

As $\omega_1 = 1 \neq 0$, so $\mathfrak{f} \neq 0$ and ω_i is an eigenvalue of C_i. q.e.d.

3.10 Theorem (Frobenius). *Let K be algebraically closed and* Char $K \nmid |G|$. *Let $\chi_1, \dots, \chi_s$ be the characters of the simple KG-modules. Then*

$$\sum_{k=1}^{s} \chi_k(g)\chi_k(h^{-1}) = \begin{cases} 0 & \text{if } h \notin g^G \\ |C_G(g)| & \text{if } h \in g^G. \end{cases}$$

Proof. By 3.9a) we have

$$h_i\chi_k(g_i)h_j\chi_k(g_j) = \sum_{l=1}^{h(G)} c_{ijl}h_l\chi_k(g_l)\chi_k(1).$$

Summation over $k = 1, \dots, s$ implies by 3.7

$$h_ih_j \sum_{k=1}^{s} \chi_k(g_i)\chi_k(g_j) = \sum_{l=1}^{h(G)} c_{ijl}h_l \sum_{k=1}^{s} \chi_k(g_l)\chi_k(1) = c_{ij1}h_1|G| = c_{ij1}|G|.$$

By 3.8c)

$$c_{ij1} = \begin{cases} 0 & \text{if } g_j^{-1} \notin K_i \\ h_i & \text{if } g_j^{-1} \in K_i. \end{cases}$$

Hence we finally obtain

$$\sum_{k=1}^{s} \chi_k(g_i)\chi_k(g_j^{-1}) = \delta_{ij}\frac{|G|}{h_i}.$$

(Observe $|K_i| = |K_i^{-1}|$.) q.e.d.

3.11 Definition. Let $C(G, \mathbb{C})$ be the set of all $\mathbb{C}$-valued class functions on G. We define a positive definite, hermitean scalar product $(\cdot, \cdot)_G$ on $C(G, \mathbb{C})$ by

$$(f_1, f_2)_G = \frac{1}{|G|} \sum_{g \in G} f_1(g)\overline{f_2(g)}.$$

3.12 Theorem (Frobenius). *Now suppose $K = \mathbb{C}$.*

a) *Up to isomorphism there exist exactly $h = h(G)$ simple* $\mathbb{C}G$-modules *$V_1, \dots, V_h$.*

b) *The characters χ_i ($i = 1, \dots, h(G)$) of the V_i form an orthonormal basis of $C(G, \mathbb{C})$, which means*

$$(\chi_i, \chi_j)_G = \delta_{ij}.$$

Also

$$\sum_{i=1}^{h} \chi_i(1)^2 = |G|.$$

c) *Now let K be any subfield of $\mathbb{C}$. Let W_i $(i = 1, \ldots, s)$ be all the simple KG-modules and ψ_i the character of W_i. If W is a KG-module with character ψ, then*

$$W \cong \bigoplus_{i=1}^{s} m_i W_i, \qquad (*)$$

where the multiplicity m_i is uniquely determined by ψ, namely as

$$m_i = \frac{(\psi, \psi_i)_G}{(\psi_i, \psi_i)_G}.$$

Hence the character ψ determines the isomorphism type of W, and the multiplicities m_i in $(*)$ are uniquely determined. (This last statement is a very special case of the "Jordan–Hölder theorem" for modules; see Huppert *I, p.* 64.)

As non-isomorphic modules have different characters, now it is legal to call a character irreducible if it is the character of some simple $\mathbb{C}G$-module.

d) *A character χ is irreducible if and only if $(\chi, \chi)_G = 1$.*

e) *Elements g_1, g_2 of G are conjugate in G if and only if*

$$\chi_i(g_1) = \chi_i(g_2) \quad \textit{for } i = 1, \ldots, h(G).$$

(The irreducible characters separate the conjugacy classes of G.)

Proof. a) Let $\chi_1, \ldots, \chi_s$ be the characters of the simple $\mathbb{C}G$-modules. By 3.6b) and 3.5 we have

$$(\chi_i, \chi_j)_G = \frac{1}{|G|} \sum_{g \in G} \chi_i(g)\overline{\chi_j(g)} = \frac{1}{|G|} \sum_{g \in G} \chi_i(g)\chi_j(g^{-1}) = \delta_{ij}.$$

Hence $\chi_1, \ldots, \chi_s$ are linearly independent over $\mathbb{C}$, which proves

$$s \leqslant \dim_{\mathbb{C}} C(G, \mathbb{C}) = h(G).$$

Now suppose $s < h = h(G)$. We consider the matrix

$$A = \begin{bmatrix} \chi_1(g_1) & \dots & \chi_s(g_1) \\ \vdots & & \vdots \\ \chi_1(g_h) & \dots & \chi_s(g_h) \end{bmatrix},$$

where $g_1, \dots, g_h$ are representatives of the conjugacy classes of G. Then

$$\operatorname{rank} A \leqslant s < h.$$

Therefore the h rows of A are linearly dependent, say

$$\sum_{j=1}^{h} c_j \chi_i(g_j) = 0 \quad (i = 1, \dots, s)$$

for some $c_j \in \mathbb{C}$, not all c_j equal to zero. By 3.10 we obtain

$$0 = \sum_{i=1}^{s} \left(\sum_{j=1}^{h} c_j \chi_i(g_j) \right) \chi_i(g_k^{-1}) = \sum_{j=1}^{h} c_j \sum_{i=1}^{s} \chi_i(g_j) \chi_i(g_k^{-1})$$

$$= \sum_{j=1}^{h} c_j \delta_{jk} \frac{|G|}{h_j} = c_k \frac{|G|}{h_k}.$$

Hence $c_j = 0$ for $j = 1, \dots, h$, a contradiction. This proves $s = h(G)$.
b) As $\dim C(G, \mathbb{C}) = h(G)$, the irreducible characters of G form an orthonormal basis of $C(G, \mathbb{C})$. Also by 3.7

$$\sum_{i=1}^{h(G)} \chi_i(1)^2 = |G|.$$

c) As W is a semisimple KG-module, so

$$W \cong \bigoplus_{i=1}^{s} m_i W_i$$

for some multiplicities m_i. Then

$$\psi = \sum_{j=1}^{s} m_j \psi_j$$

and by 3.5

$$(\psi, \psi_i)_G = \sum_{j=1}^{s} m_j (\psi_j, \psi_i)_G = m_i (\psi_i, \psi_i)_G.$$

Observe that

$$(\psi_i, \psi_i)_G = \frac{1}{|G|} \sum_{g \in G} |\psi_i(g)|^2 > 0.$$

d) If

$$\chi = \sum_{i=1}^{h} m_i \chi_i,$$

then

$$(\chi, \chi)_G = \sum_{i=1}^{h} m_i^2.$$

Hence χ is irreducible if and only if $(\chi, \chi)_G = 1$.
e) If g_1 and g_2 are not conjugate in G, there exists $f \in C(G, \mathbb{C})$ such that $f(g_1) \neq f(g_2)$. By b)

$$f = \sum_{j=1}^{h} c_j \chi_j$$

for some $c_j \in \mathbb{C}$. Hence there exists χ_j such that $\chi_j(g_1) \neq \chi_j(g_2)$. q.e.d.

From now on we shall most of the time restrict ourselves to the "classical" case of representation theory over $\mathbb{C}$. Hence we define:

3.13 Definition. a) Let Irr G be the set of irreducible characters of G over $\mathbb{C}$. Hence

$$\operatorname{Irr} G = \{\chi_1, \ldots, \chi_h\},$$

where $h = h(G)$ is the class number of G. We introduce the **degree set** of G by

$$\operatorname{cd} G = \{\chi(1) \mid \chi \in \operatorname{Irr} G\};$$

this is considered as a set, not containing information how often a particular degree appears. We also introduce the **degree pattern** of G as

$$(\chi_1(1), \ldots, \chi_h(1))$$

(in arbitrary order).

b) If χ is a character of G and D is a representation of G with character χ, we write $\operatorname{Ker} \chi = \operatorname{Ker} D$. (As χ determines D up to equivalence, so $\operatorname{Ker} \chi$ is well-defined.) We call D and χ faithful if $\operatorname{Ker} D = E$.
c) Let $g_1, \ldots, g_h$ be representatives of the conjugacy classes of G. Then we call $(\chi_i(g_j))_{i,j=1,\ldots,h}$ the character table of G.

3.14 Proposition (L. Solomon [1]). *Suppose*

$$\operatorname{Irr} G = \{\chi_1, \ldots, \chi_h\}$$

and let $g_1, \ldots, g_h$ be representatives of the conjugacy classes of G. Then

$$\sum_{j=1}^{h} \chi_i(g_j)$$

is a nonnegative integer. (By a different argument, also $\sum_{i=1}^{h} \chi_i(g_j)$ is an integer, but it need not be nonnegative. If $G = M_{11}$ is the Mathieu group of degree 11 *and g an element of order* 11 *in M_{11}, then $\sum_i \chi_i(g) = -2$; see* Isaacs, *p.* 291.)

Proof. We consider $\mathbb{C}G$ as a G-module, but not as in 3.7 by right multiplication, but rather by conjugation. Hence we define

$$hD(g) = g^{-1}hg$$

for $h \in \mathbb{C}G$, $g \in G$. This defines obviously a representation D of G on $\mathbb{C}G$. Let

$$\psi = \sum_{i=1}^{h} m_i \chi_i$$

with nonnegative integers m_i be its character. Then

$$\psi(g) = |\{h \mid g^{-1}hg = h \in G\}| = |C_G(g)|.$$

Hence

$$\begin{aligned} m_i = (\psi, \chi_i)_G &= \frac{1}{|G|} \sum_{g \in G} |C_G(g^{-1})| \chi_i(g) = \frac{1}{|G|} \sum_{j=1}^{h} h_j |C_G(g_j)| \chi_i(g_j) \\ &= \sum_{j=1}^{h} \chi_i(g_j) \geqslant 0. \end{aligned}$$

q.e.d.

3.15 Example. Let $G = S_n$ be the symmetric group and $\sigma(y) = \operatorname{sgn} g$. Then by 3.14

$$0 \leqslant \sum_{j=1}^{h} \sigma(g_j) = h_+ - h_-,$$

where
h_+ is the number of classes of even permutations in S_n,
h_- is the number of classes of odd permutations in S_n.

We can do better and claim $(\psi, \sigma)_G \geqslant 1$ if $n > 2$ and ψ as in 3.14.
Observe $(\psi, \sigma)_G = \dim_{\mathbb{C}} W$, where

$$W = \{w | w \in \mathbb{C}G, g^{-1}wg = \sigma(g)w \text{ for all } g \in S_n\}.$$

Certainly, W decomposes into summands in the $\mathbb{C}$-linear span of a conjugacy class $K_i = g_i^G$ $(i = 1, \ldots, h(G))$. Suppose $G = \bigcup_j C_G(g_i)y_{ij}$ with $y_{i1} = 1$ and

$$t_i = \sum_j c_j g_i^{y_{ij}}$$

with $t_i^g = \sigma(g)t_i$. Then

$$\sum_j c_j g_i^{y_{ij}} = t_i = \sigma(y_{ik})t_i^{y_{ik}} = \sigma(y_{ik})(c_1 g_i^{y_{ik}} + \cdots).$$

Hence all coefficients $c_k = \sigma(y_{ik})c_1$ are determined by c_1.
(1) Suppose at first that $C_G(g_i) \nleqslant A_n$. Hence there exists $h \in C_G(g_i)$ such that $\operatorname{sgn} h = -1$. Then

$$-t_i = -(c_1 g_i + \cdots) = t_i^h = c_1 g_i + \cdots,$$

therefore $t_i = 0$.
(2) Now suppose that $C_G(g_i) \leqslant A_n$. Then $t_i = \sum_j \sigma(y_{ij}) \cdot g_i^{y_{ij}}$ is obviously independent of the choice of the coset representatives y_{ij} of $C_G(g_i)$. As $\{y_{ij}h | j = 1, \ldots, h_i\}$ is also a set of coset representatives of $C_G(g_i)$, therefore

$$t_i = \sum_j \sigma(y_{ij}h) g_i^{y_{ij}h} = \sigma(h)\left(\sum_j \sigma(y_{ij}) g_i^{y_{ij}}\right)^h = \sigma(h) t_i^h \neq 0.$$

Hence $(\psi, \sigma)_G$ is equal to the number of conjugacy classes g_i^G such that $C_G(g_i) \leqslant A_n$. We easily see that these are the g_i with a cycle decomposition of type $(z_1, \ldots, z_r)$, where $1 \leqslant z_1 < \cdots < z_r$ and all z_r odd. As for every $n \geqslant 3$ either $(1\,2 \ldots n)$ or $(1)(2 \ldots n)$ describes such a class, we obtain $(\psi, \sigma)_G \geqslant 1$.

Incidentally, we have proved the following combinatorial result: We consider partitions

$$n = n_1 + \cdots + n_k, \quad \text{where } n_j > 0.$$

Let $p_j(n)$ be the number of partitions where
(1) the number of even n_i is even for $j = 1$,
(2) the number of even n_i is odd for $j = 2$,
(3) all n_i are odd and distinct for $j = 3$.
Then

$$p_1(n) - p_2(n) = p_3(n).$$

We mention two further constructions of characters and representations:

3.16 Proposition. *Suppose $\chi \in \operatorname{Irr} G$. Suppose further that $\chi(g) \in L$ for all $g \in G$, where L by 3.6a) is a subfield of some cyclotomic field.*
a) *Let α be an automorphism of L and define χ^α as in* 1.6d) *by $\chi^\alpha(g) = \chi(g)^\alpha$. Then $\chi^\alpha \in \operatorname{Irr} G$.*
b) *Let the automorphism α_m of the field $\mathbb{Q}_{|G|} = \mathbb{Q}(\varepsilon)$ of $|G|$-th roots of unity be defined by $\varepsilon^{\alpha_m} = \varepsilon^m$, where $(m, |G|) = 1$. Then $\chi^{\alpha_m}(g) = \chi(g^m)$.*

Proof. a) A slight problem arises from the fact that there may not exist a matrix representation D of G with character χ and entries of the $D(g)$ in L (see exercise E1.1). But we shall see in 4.8 that there always exists a field $L' \supseteq L$, such that L' is normal over $\mathbb{Q}$ and there exists a matrix representation D of G such that $D(g) = (a_{ij}(g))$, all $a_{ij}(g) \in L'$ with trace $D(g) = \chi(g)$. As well-known, we can extend α to an automorphism $\bar{\alpha}$ of L' over $\mathbb{Q}$. If we define $D^{\bar{\alpha}}$ as in 1.6d) by $D^{\bar{\alpha}}(g) = (a_{ij}(g)^{\bar{\alpha}})$, then $D^{\bar{\alpha}}$ is a representation with character χ^α. Finally from

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

we see by 3.12d) that $\chi^\alpha \in \operatorname{Irr} G$.
b) Let ε^{k_i} $(i = 1, \ldots, n)$ be the eigenvalues of $D(g)$, where ε is a primitive $|G|$-th root of unity. The eigenvalues of $D(g^m) = D(g)^m$ are ε^{mk_i} $(i = 1, \ldots, n)$. Therefore

$$\chi(g^m) = \sum_{i=1}^{n} \varepsilon^{mk_i} = \left(\sum_{i=1}^{n} \varepsilon^{k_i} \right)^{\alpha_m} = \chi(g)^{\alpha_m}. \qquad \text{q.e.d.}$$

Sometimes the following proposition allows to control that D is a representation of G.

3.17 Proposition. *Let the group G be presented by generators $g_1, \ldots, g_d$ and defining relations*

$$r_j(g_1, \ldots, g_d) = 1 \quad (j = 1, \ldots, m).$$

Suppose $A_1, \ldots, A_d$ are matrices in a linear group $GL(V)$ and

$$r_j(A_1, \ldots, A_d) = E \quad \text{for } j = 1, \ldots, m.$$

Then there exists a homomorphism D of G into $GL(V)$ such that $D(g_i) = A_i$ $(i = 1, \ldots, d)$.

Proof. Let $F = \langle f_1, \ldots, f_d \rangle$ be a free group with free generators f_i. Then there exists a homomorphism D' of F into $GL(V)$ such that $D'(f_i) = A_i$. Obviously

$$\operatorname{Ker} D \geqslant \langle r_j(f_1, \ldots, f_n)^f \mid j = 1, \ldots, m, f \in F \rangle \doteqdot R.$$

As $F/R \cong G$ (this is the meaning of defining relations!), we obtain a homomorphism of G into $GL(V)$ by

$$D(g_i) = D'(f_i). \qquad \text{q.e.d.}$$

For several applications it is important that normal subgroups of a group G can be recognized by the character table of G.

3.18 Lemma. *Let χ be a character of an $\mathbb{C}G$-module.*
a) $|\chi(g)| \leqslant \chi(1)$ *for all* $g \in G$.
b) $\operatorname{Ker} \chi = \{g \mid g \in G, \chi(g) = \chi(1)\}$.
c) $Z(G/\operatorname{Ker} \chi) = \{g \operatorname{Ker} \chi \mid |\chi(g)| = \chi(1)\}$.

Proof. Let D be a representation for χ. Then $\chi(g)$ is the sum of the eigenvalues ε_j of $D(g)$,

$$\chi(g) = \varepsilon_1 + \cdots + \varepsilon_n \quad (n = \chi(1))$$

say. As $|\varepsilon_j| = 1$, so

$$|\chi(g)| \leqslant \sum_{j=1}^{n} |\varepsilon_j| = \chi(1).$$

Equality occurs only if all the complex numbers ε_j are equal. As the representation D, reduced to $\langle g \rangle$, is semisimple, we obtain $D(g) = \varepsilon_1 E_n$. This shows $g \operatorname{Ker} \chi \in Z(G/\operatorname{Ker} \chi)$. And $g \in \operatorname{Ker} \chi$ happens exactly if $\varepsilon_1 = 1$, hence if $\chi(g) = \chi(1)$. q.e.d.

3.19 Theorem. a) *The character table of G determines the lattice of normal subgroups of G, including the indices.*
b) *The character table of G determines solvability and nilpotency of G.*

Proof. a) Suppose $N \trianglelefteq G$. As the characters separate conjugacy classes by 3.12e), we obtain

$$N = \bigcap_{\chi \in \operatorname{Irr} G/N} \operatorname{Ker} \chi = \bigcap_{N \leqslant \operatorname{Ker} \chi} \operatorname{Ker} \chi,$$

and by 3.18 $\operatorname{Ker} \chi$ is determined by the character values. Then $|G/N|$ is determined by

$$|G/N| = \sum_{N \leqslant \operatorname{Ker} \chi} \chi(1)^2.$$

b) To control solvability of G by the character table, we have to find a chief-series

$$E = N_0 \lhd N_1 \lhd \cdots \lhd N_k = G,$$

where $N_j \trianglelefteq G$ and $|N_{j+1}/N_j|$ is a power of a prime. Also by 3.18c) we can determine $Z(G)$, then $Z(G/Z(G))$ and so on. This determines nilpotency of G, even its nilpotency class. q.e.d.

3.20 Remarks. a) It is a natural question how much information about the structure of G is determined by the character table of G.

S. Mattarei [1], [2] recently gave examples of groups G and H with the same character table, where $G'' = E \neq H''$. Hence the derived length of G is **not** determined by the character table.

b) It can be proved that the composition factors of G can be determined also in the insolvable case from the character table of G (Sandling, Lyons). This is mainly due to the following fact, which is a consequence of the classification of simple groups:

Suppose A and B are simple non-abelian groups such that

$$|A \times \underset{m}{\cdots} \times A| = |B \times \underset{n}{\cdots} \times B|.$$

Then $m = n$. The only pairs with $A \not\cong B$ are

$$\begin{aligned}(A, B) &= (A_8, PSL(3, 4)) \\ &= (PSp(2n, q), P\Omega O(2n+1, q)) \quad \text{where } 2 \nmid q \text{ and } n \geqslant 3.\end{aligned}$$

It is possible to distinguish these cases by inspecting the conjugacy classes of some 2-elements (see Kimmerle et al.).

3.21 Remark. In § 4 we shall present an approach to the orthogonality relations, using the ring structure of KG. The approach in § 3 has still some advantages. It provides the relations in 3.4. The averaging process over G, which was the basis of the proofs in 2.13 and 3.4, can also be used for compact topological groups. For there exists a process of integration over G (the Haar integral), such that for "reasonable" functions f on G the integrals of $f(g)$ and $f(gh)$ over $g \in G$ are equal. This approach provides for instance an elementary access to the representation theory of the orthogonal group $SO(3, \mathbb{R})$ and the unitary group $SU(2, \mathbb{C})$, which is used in some problems of quantum mechanics.

§ 4 The group algebra

In this section we describe a different approach to the basic theorems of representation theory, in particular to the orthogonality relations 3.5 and 3.10. It does not give Schur's equations in 3.4, but in some respects it is superior, in particular working over any field whose characteristic does not divide $|G|$. The connection between representation theory of groups and of algebras was observed by E. Noether.

4.1 Definition. a) An algebra A is called semisimple if A itself is a semisimple right A-module.
b) If A is a K-algebra, we define the algebra A^{op} as the set A, equipped with its structure as K-vector space, but with a new multiplication $\circ$, defined by $a \circ b = ba$.

4.2 Lemma. *Let A be K-algebra. Then $A^{op} \cong \mathrm{Hom}_A(A, A)$.*

Proof. Suppose $\alpha \in \mathrm{Hom}_A(A, A)$. As

$$a\alpha = (1a)\alpha = (1\alpha)a,$$

so α is determined by $1\alpha \doteqdot a(\alpha)$. And conversely for every $b \in A$, then $a\alpha = ba$ defines an $\alpha \in \mathrm{Hom}_A(A, A)$. The mapping of α onto 1α is obviously K-linear. For $\alpha, \beta \in \mathrm{Hom}_A(A, A)$ we obtain

$$a(\alpha\beta) = 1(\alpha\beta) = (1\alpha)\beta = (1a(\alpha))\beta = (1\beta)a(\alpha) = a(\beta)a(\alpha).$$

This proves

$$a(\alpha\beta) = a(\beta)a(\alpha) = a(\alpha) \circ a(\beta),$$

hence $\mathrm{Hom}_A(A, A) \cong A^{op}$. q.e.d.

4.3 Theorem (Wedderburn). *Let A be a semisimple algebra and as A-module*

$$A \cong \bigoplus_{i=1}^{k} n_i V_i,$$

where the V_i are non-isomorphic simple A-modules and

$$n_i V_i = V_i \oplus \underset{n_i}{\cdots} \oplus V_i.$$

By Schur's lemma 2.3

$$F_i \doteqdot \operatorname{Hom}_A(V_i, V_i)$$

is a skew field.

a) $\operatorname{Hom}_A(n_i V_i, n_i V_i) \cong (F_i)_{n_i}$, *where* $(F_i)_{n_i}$ *is the algebra of all matrices of type* (n_i, n_i) *over the skew field* F_i.

b) *Then*

$$A \cong \bigoplus_{i=1}^{k} (F_i^{op})_{n_i}.$$

The summands $(F_i^{op})_{n_i}$ *are 2-sided ideals in* A, *annihilating each other.*

c) *If* W *is a simple* A*-module, so* W *is isomorphic to some* V_i.

d) *If* $A = (F)_n$ *with a skew field* F, *then* A *is a simple algebra. The set*

$$V = F^n = \{(f_1, \ldots, f_n) | f_i \in F\}$$

is (up to isomorphism) the only simple A*-module. Further* $A = W_1 \oplus \cdots \oplus W_n$, *where*

$$W_k = \{(f_{ij}) | f_{ij} \in F, f_{ij} = 0 \text{ if } i \neq k\}$$

and $W_k \cong V$ *as* A*-module. Finally* F *is uniquely determined by* $\operatorname{Hom}_A(V, V) \cong F^{op}$.

Proof. a) Let V be a simple A-module. We consider nV as the set

$$\{(v_1, \ldots, v_n) | v_i \in V\}.$$

Suppose $\alpha, \beta \in \operatorname{Hom}_A(nV, nV)$. Then $(0, \ldots, 0, v_i, 0, \ldots, 0)\alpha = (v_i\alpha_{i1}, \ldots, v_i\alpha_{in})$, where obviously $\alpha_{ij} \in \operatorname{Hom}_A(V, V) = F$. Then $\alpha \to (\alpha_{ij})$ is K-linear and

$$(0, \ldots, 0, v_i, 0, \ldots, 0)\alpha\beta = (v_i\alpha_{i1}, \ldots, v_i\alpha_{in})\beta = \sum_{j=1}^{n} (v_i\alpha_{ij}\beta_{j1}, \ldots, v_i\alpha_{ij}\beta_{jn})$$

$$= \left(v_i \sum_{j=1}^{n} \alpha_{ij}\beta_{j1}, \ldots, v_i \sum_{j=1}^{n} \alpha_{ij}\beta_{jn}\right).$$

Hence $\alpha\beta$ corresponds to the matrix $(\alpha_{ij})(\beta_{ij})$. This proves

$$\operatorname{Hom}_A(nV, nV) \cong (F)_n.$$

b) Obviously $\mathrm{Hom}_A(\cdot, \cdot)$ is additive with respect to both arguments and $\mathrm{Hom}_A(V_i, V_j) = 0$ if $V_i \not\cong V_j$. Hence by 4.2 and a)

$$A^{op} = \mathrm{Hom}_A(A, A) \cong \bigoplus_{i=1}^{k} \mathrm{Hom}_A(n_i V_i, n_i V_i) \cong \bigoplus_{i=1}^{k} (F_i)_{n_i}.$$

So

$$A \cong \bigoplus_{i=1}^{k} (F_i)_{n_i}^{op}.$$

Finally observe that $(F_i)_{n_i}^{op} \cong (F_i^{op})_{n_i}$ by the mapping γ with

$$(\alpha_{ij})\gamma = (\alpha_{ij})^t \quad \text{(transposition);}$$

for if $\circ$ denotes the multiplication in $(F_i^{op})_{n_i}$, then

$$(\alpha_{ij})\gamma(\beta_{ij})\gamma = (\alpha_{ij})^t \circ (\beta_{ij})^t = (\tau_{ij}),$$

where

$$\tau_{ij} = \sum_k \alpha_{ki} \circ \beta_{jk} = \sum_k \beta_{jk}\alpha_{ki},$$

therefore

$$(\alpha_{ij})\gamma(\beta_{ij})\gamma = ((\beta_{ij})(\alpha_{ij}))^t = ((\beta_{ij})(\alpha_{ij}))\gamma.$$

c) Let W be a simple A-module. Then $\mathrm{Hom}_A(A, W) \cong W$ (as K-vector spaces) by $\alpha \to 1\alpha$ for $\alpha \in \mathrm{Hom}_A(A, W)$. Hence

$$0 \neq W \cong \mathrm{Hom}_A(A, W) \cong \bigoplus_{i=1}^{k} \mathrm{Hom}_A(n_i V_i, W).$$

Therefore $\mathrm{Hom}_A(V_i, W) \neq 0$ for some i, which proves $W \cong V_i$.
d) We use for $A = (F)_n$ the usual F-basis

$$\{e_{ij} | i, j = 1, \ldots, n\}.$$

Hence any $a \in A$ is written uniquely as

$$a = \sum_{i,j} e_{ij} f_{ij} \quad \text{with } f_{ij} \in F.$$

Suppose $\mathfrak{i} \neq 0$ is a 2-sided ideal in A and

$$0 \neq a = \sum_{i,j} e_{ij} f_{ij} \in \mathfrak{i}$$

with $f_{kl} \neq 0$. For any s, t then

$$e_{sk} a e_{lt} = e_{sk} e_{kl} e_{lt} f_{kl} = e_{st} f_{kl} \in \mathfrak{i}.$$

Hence all e_{st} are in $\mathfrak{i}$, which shows $\mathfrak{i} = A$. So A is a simple algebra.

If

$$0 \neq (f_1, \ldots, f_n) \in V \quad \text{and} \quad f_i \neq 0,$$

then

$$(f_1, \ldots, f_n) \sum_j e_{ij} f_i^{-1} c_j = (c_1, \ldots, c_n).$$

Hence

$$(f_1, \ldots, f_n) A = V,$$

so V is a simple A-module. By c) then V is the only simple A-module. The rows of $(F)_n$ obviously are A-modules isomorphic to V.

Suppose $\alpha \in \operatorname{Hom}_A(V, V)$. We put

$$v_i = (0, \ldots, 0, \underset{i}{1}, 0, \ldots, 0).$$

Then

$$v_i \alpha = (v_i e_{ii}) \alpha = (v_i \alpha) e_{ii} = (0, \ldots, 0, \underset{i}{a_i}, 0, \ldots, 0),$$

for some $a_i \in F$. If $i \neq j$, then

$$\begin{aligned}(v_i e_{ij}) \alpha = v_j \alpha = (0, \ldots, 0, \underset{j}{a_j}, 0, \ldots, 0) &= (v_i \alpha) e_{ij} = (0, \ldots, 0, \underset{i}{a_i}, 0, \ldots, 0) e_{ij} \\ &= (0, \ldots, 0, \underset{j}{a_i}, 0, \ldots, 0).\end{aligned}$$

This proves $a_i = a_j$. If we put $a_i = a(\alpha)$, then

$$(v_i d) \alpha = (v_i \alpha) d = (0, \ldots, 0, a(\alpha) d, \ldots, 0),$$

so $v\alpha = a(\alpha) v$ for all $v \in V$.

The mapping $\alpha \to a(\alpha)$ is K-linear and bijective. Finally for $\alpha, \beta \in \mathrm{Hom}_A(V, V)$ we obtain

$$a(\alpha\beta)v = v(\alpha\beta) = (v\alpha)\beta = (a(\alpha)v)\beta = a(\beta)a(\alpha)v.$$

This shows $\mathrm{Hom}_A(V, V) \cong F^{op}$. q.e.d.

4.4 Remark. If K is algebraically closed, then $F_i = K$ by 2.3b). If K is finite, then also F_i is finite, hence F_i is commutative by a famous theorem of Wedderburn. In the case where $K = \mathbb{R}$, by a theorem of Frobenius only the cases $F_i = \mathbb{R}$, $\mathbb{C}$ or the quaternions $\mathbb{H}$ are possible. But for other fields K, for instance $K = \mathbb{Q}$, there may be many possibilities for F_i.

4.5 Theorem. *Let K be algebraically closed and* Char K *not dividing* $|G|$.

a) *Then*

$$KG \cong \bigoplus_{i=1}^{h} (K)_{n_i},$$

where $h = h(G)$ is the class number of G, and KG has $h(G)$ irreducible modules V_i. (This implies 3.12.)

b) *If χ_i is the character of V_i, then*

$$\sum_{i=1}^{h} \chi_i(1)\chi_i(g) = \begin{cases} |G| & \text{if } g = 1 \\ 0 & \text{if } g \neq 1. \end{cases}$$

(*This is* 3.7.)

c) *The neutral element of $(K)_{n_i}$ is*

$$e_i = \frac{\chi_i(1)}{|G|} \sum_{g \in G} \chi_i(g^{-1})g.$$

As $e_i \neq 0$, so Char K *does not divide* $\chi_i(1)$.

d) *We have*

$$\frac{1}{|G|} \sum_{x \in G} \chi_i(x^{-1}g)\chi_j(x) = \delta_{ij}\frac{\chi_i(g)}{\chi_i(1)},$$

in particular for $g = 1$

$$\sum_{x \in G} \chi_i(x^{-1})\chi_j(x) = \delta_{ij}|G|.$$

(*This is* 3.5).

e) *If* $g_1, \ldots, g_h$ *are representatives of the conjugacy classes of* G, *then*

$$\sum_{k=1}^{h} \chi_k(g_i)\chi_k(g_j^{-1}) = \delta_{ij}|C_G(g_i)|.$$

(*This is* 3.10.)

Proof. a) By 2.11 KG is a semisimple algebra, hence by 4.3

$$KG \cong \bigoplus_{i=1}^{k} (K)_{n_i}.$$

Using 3.8a), we obtain

$$h(G) = \dim_K Z(KG) = \sum_{i=1}^{k} \dim_K Z((K)_{n_i}) = k.$$

b) By 4.3d), $(K)_{n_i}$ as KG-module is the direct sum of n_i simple KG-modules, the rows of $(K)_{n_i}$. If $g \in G$, then the character of g on KG is therefore

$$\rho(g) = \sum_{i=1}^{h} n_i\chi_i(g) = \sum_{i=1}^{h} \chi_i(1)\chi_i(g).$$

If $g \neq 1$, then the basis G of KG is by right multiplication with g permuted without fixed points, hence

$$\rho(g) = \begin{cases} |G| & \text{if } g = 1 \\ 0 & \text{if } g \neq 1. \end{cases}$$

c) Let D_i be the irreducible representation corresponding to $(K)_{n_i}$. Put

$$e_i = \sum_{g \in G} a_i(g)g.$$

As $e_i h$ for $h \in G$ lies in the 2-sided ideal $(K)_{n_i}$, we obtain

$$\delta_{ij}D_j(h) = D_j(e_i)D_j(h) = D_j(e_i h) = \sum_{g \in G} a_i(g)D_j(gh).$$

Hence forming traces we obtain

$$\delta_{ij}\chi_j(h) = \sum_{g \in G} a_i(g)\chi_j(gh).$$

By b) this implies

$$\chi_i(h)\chi_i(1) = \sum_{j=1}^{h} \delta_{ij}\chi_j(h)\chi_j(1) = \sum_{g \in G} a_i(g) \sum_{j=1}^{h} \chi_j(gh)\chi_j(1)$$

$$= a_i(h^{-1}) \sum_{j=1}^{h} \chi_j(1)^2 = a_i(h^{-1})|G|.$$

Hence

$$e_i = \frac{\chi_i(1)}{|G|} \sum_{g \in G} \chi_i(g^{-1})g.$$

d) By c) we obtain

$$\delta_{ij}\frac{\chi_i(1)}{|G|} \sum_{g \in G} \chi_i(g^{-1})g = \delta_{ij}e_i = e_ie_j = \frac{\chi_i(1)\chi_j(1)}{|G|^2} \sum_{x,y \in G} \chi_i(x^{-1})\chi_j(y^{-1})xy.$$

This proves

$$\delta_{ij}\frac{\chi_i(1)}{|G|}\chi_i(g^{-1}) = \frac{\chi_i(1)\chi_j(1)}{|G|^2} \sum_{xy=g} \chi_i(x^{-1})\chi_j(y^{-1}).$$

Hence

$$\delta_{ij}\frac{\chi_i(g)}{\chi_i(1)} = \frac{1}{|G|} \sum_{xy=g^{-1}} \chi_i(x^{-1})\chi_j(y^{-1}) = \frac{1}{|G|} \sum_{t \in G} \chi_i(t^{-1}g)\chi_j(t).$$

e) Let

$$h_j = |g_j^G| = |G : C_G(g_j)|.$$

We define matrices of type $(h(G), h(G))$ by

$$A = (a_{ik}), \quad \text{where } a_{ik} = \chi_k(g_i)$$

and

$$B = (b_{kj}), \quad \text{where } b_{kj} = \frac{h_j}{|G|}\chi_k(g_j^{-1}).$$

Then d) says

$$\delta_{ij} = \frac{1}{|G|} \sum_{g \in G} \chi_i(g)\chi_j(g^{-1}) = \frac{1}{|G|} \sum_{k=1}^{h} h_k \chi_j(g_k^{-1})\chi_i(g_k) = \sum_{k=1}^{h} b_{jk} a_{ki}.$$

This shows $BA = E$. Hence also $AB = E$, which implies

$$\delta_{ij} = \sum_{k=1}^{h} a_{ik} b_{kj} = \sum_{k=1}^{h} \chi_k(g_i) \frac{h_j}{|G|} \chi_k(g_j^{-1}),$$

hence

$$\sum_{k=1}^{h} \chi_k(g_i)\chi_k(g_j^{-1}) = \delta_{ij} \frac{|G|}{h_i} = \delta_{ij} |C_G(g_i)|. \qquad \text{q.e.d.}$$

From now on we assume again usually that Char $K = 0$ and K is algebraically closed.

4.6 Theorem. *As in* 3.8 *we introduce the class sums*

$$k_i = \sum_{g \in K_i} g \quad (i = 1, \ldots, h(G)),$$

which constitute a K-basis of $Z(KG)$. Then if

$$k_i k_j = \sum_{l=1}^{h(G)} c_{ijl} k_l,$$

we have

$$c_{ijl} = \frac{|K_i|\,|K_j|}{|G|} \sum_{\chi \in \operatorname{Irr} G} \chi(g_i)\chi(g_j) \frac{\chi(g_l^{-1})}{\chi(1)}.$$

(*These c_{ijk} are nonnegative integers by* 3.8, *if* Char $K = 0$.)

Proof. Let D be an irreducible representation of G with character χ. By Schur's lemma

$$D(k_i) = \omega(k_i) E_{\chi(1)},$$

where as in the proof of 3.9a)

$$\omega(k_i) = \frac{|K_i|\,\chi(g_i)}{\chi(1)}$$

if $K_i = g_i^G$. As ω is a homomorphism of $Z(KG)$ into K, we obtain

$$\frac{|K_i||K_j|}{\chi(1)^2}\chi(g_i)\chi(g_j) = \omega(k_i)\omega(k_j) = \omega(k_ik_j) = \sum_{l=1}^{h(G)} c_{ijl}\omega(k_l)$$

$$= \sum_{l=1}^{h(G)} c_{ijl}|K_l|\frac{\chi(g_l)}{\chi(1)}.$$

This implies by 4.5e)

$$|K_i||K_j| \sum_{\chi\in\operatorname{Irr} G} \chi(g_i)\chi(g_j)\frac{\chi(g_m^{-1})}{\chi(1)} = \sum_{l=1}^{h(G)} c_{ijl}|K_l| \sum_{\chi\in\operatorname{Irr} G} \chi(g_l)\chi(g_m^{-1})$$

$$= \sum_{l=1}^{h(G)} c_{ijl}|K_l|\delta_{lm}|C_G(g_l)| = c_{ijm}|G|. \qquad \text{q.e.d.}$$

We add a remarkable consequence.

4.7 Proposition. a) *Suppose $g, h \in G$. Then g is conjugate to a commutator $[h, y]$ for some $y \in G$ if and only if*

$$\sum_{\chi\in\operatorname{Irr} G} |\chi(h)|^2\frac{\chi(g^{-1})}{\chi(1)} \neq 0.$$

b) *g is a commutator if and only if*

$$\sum_{\chi\in\operatorname{Irr} G} \frac{\chi(g^{-1})}{\chi(1)} \neq 0.$$

c) *Suppose $(|G|, m) = 1$. If $g \in G$ and if g is a commutator, so is g^m.*

Proof. a) g conjugate to

$$[h, y] = h^{-1}y^{-1}hy$$

for some $y \in G$ means that k_g is involved in $k_{h^{-1}} \cdot k_h$, hence by 4.6

$$0 < c_{h^{-1},h,g} = \frac{|K_h|^2}{|G|} \sum_{\chi\in\operatorname{Irr} G} |\chi(h)|^2\frac{\chi(g^{-1})}{\chi(1)}.$$

b) $$\sum_{h\in G} c_{h^{-1},h,g}\frac{|G|}{|K_h|^2} = \sum_{\chi\in\operatorname{Irr} G} \frac{\chi(g^{-1})}{\chi(1)} \sum_{h\in G} |\chi(h)|^2 = |G| \sum_{\chi\in\operatorname{Irr} G} \frac{\chi(g^{-1})}{\chi(1)}$$

is positive exactly if some $c_{h^{-1},h,g} > 0$, hence if g is conjugate to some $[h, y]$, which means that g is a commutator.
c) By 3.16 there exists a field automorphism α_m such that

$$\chi^{\alpha_m}(g) = \chi(g^m).$$

Hence as

$$\sum_{\chi \in \operatorname{Irr} G} \frac{\chi(g^{-1})}{\chi(1)}$$

is fixed by all field automorphisms, so lies in $\mathbb{Q}$, we obtain

$$\sum_{\chi \in \operatorname{Irr} G} \frac{\chi(g^{-m})}{\chi(1)} = \sum_{\chi \in \operatorname{Irr} G} \frac{\chi(g^{-1})}{\chi(1)}. \qquad \text{q.e.d.}$$

4.8 Remark. a) Let K be the field of all algebraic numbers. Then by 4.5

$$KG \cong \bigoplus_{i=1}^{h} (K)_{n_i}.$$

The representation D_i is given by the projection onto $(K)_{n_i}$, hence

$$D_i(g) = (a_{jk}^{(i)}(g))$$

with $a_{jk}^{(i)}(g) \in K$. Then

$$K_0 = \mathbb{Q}(a_{jk}^{(i)}(g) | i = 1, \ldots, h; j, k = 1, \ldots, n_i, g \in G)$$

is an algebraic number field with $(K_0 : \mathbb{Q}) < \infty$, in which all the matrix representations D_i can be realized. Enlarging K_0 if necessary, we can assume that $K_0 : \mathbb{Q}$ is a normal extension.
b) The idempotent e_i, corresponding to $(K)_{n_i}$, is by 4.5c) given as

$$e_i = \frac{\chi_i(1)}{|G|} \sum_{g \in G} \chi_i(g^{-1})g,$$

hence can be written over the field

$$\mathbb{Q}(\chi_i) = \mathbb{Q}(\chi_i(g) | g \in G).$$

This shows that a matrix representation for the character $\chi_i(1)\chi_i$ can be written over $\mathbb{Q}(\chi_i)$. In general, a matrix representation with character χ_i cannot be obtained over $\mathbb{Q}(\chi_i)$ (see E1.1). There exists a uniquely determined smallest integer $s(\chi_i)$, such that a matrix representation for $s(\chi_i)\chi_i$ can be realized over $\mathbb{Q}(\chi_i)$. This $s(\chi_i)$ is called the Schur index of χ_i. It is closely related to the skew fields F_i appearing in theorem 4.3. We come back to this question in § 38.

4.9 Remarks. The situation is dramatically changed if K is an algebraically closed field with Char $K = p$, where p divides $|G|$.
(1) If $J = J(KG)$ is the maximal nilpotent ideal of KG, then

$$KG/J(KG) = \bigoplus_{i=1}^{s} (K)_{n_i}.$$

The number s of simple KG-modules is equal to the number of conjugacy classes g^G such that $p \nmid |g^G|$. Unfortunately, precise information about $J(KG)$ is not known in the general case. If $p^a \Vert |G|$, then

$$p^a - 1 \leqslant \dim_K J(KG) \leqslant |G| - \frac{|G|}{p^a}. \tag{$*$}$$

(The upper inequality is only proved if G is p-solvable.) The groups G, where the lower or upper bound is reached, are well known and very special. But in general $(*)$ is a very weak information.
(2) As right KG-module we have a decomposition

$$KG = \bigoplus_{i=1}^{s} n_i P_i$$

with indecomposable "projective" modules P_i. Then P_i has only one maximal submodule $P_i \cap J(KG)$ and one simple submodule $S(P_i)$, moreover $n_i = \dim_K S(P_i)$ and

$$S(P_i) \cong P_i/P_i \cap J(KG).$$

If $p^a \Vert |G|$, then $p^a \mid \dim_K P_i$.
(3) The number of isomorphism types of indecomposable KG-modules is finite if and only if the Sylow-p-subgroups of G are cyclic. Hence the modules that can be studied are mainly the simple modules and the indecomposable projective modules P_i in (2).
(4) The decomposition

$$KG = \bigoplus_{i=1}^{t} B_i$$

of KG into two-sided, indecomposable ideals B_i (called p-blocks) plays a central role. But the number t of blocks cannot easily be connected with the structure of G.

For an introduction to modular representation theory we refer the reader to Blackburn–Huppert II, p. 1–237 or (shorter) Representation Theory in Arbitrary Characteristic, (Trento 1990/91). The most comprehensive treatment is still the book by W. Feit.