Group Theory
Lecture Notes for MTH 912/913
04/05

Ulrich Meierfrankenfeld

May 1, 2013

Contents

1 Group Theory **5**

1.1 Group Action 5

1.2 Balanced Products of G-sets 8

1.3 Central by finite groups 13

1.4 Finite p-Groups 14

1.5 A p-complement Theorem 17

2 General Representation Theory **21**

2.1 Basic Definitions 21

2.2 Krull-Schmidt Theorem 29

2.3 Maschke's Theorem 34

2.4 Jacobson Radical 35

2.5 Simple modules for algebras 39

2.6 Tensor Products 47

2.7 Induced and Coinduced Modules 59

2.8 Tensor Induction and Transfer 63

2.9 Clifford Theory 65

3 Character Theory **69**

3.1 Semisimple Group Algebra 69

3.2 Characters 71

3.3 Burnside's $p^a q^b$ Theorem 78

3.4 An hermitian form 79

3.5 Frobenius' Theorem 82

3.6 Quaternion Groups 84

3.7 Groups with quaternion Sylow 2-subgroup 87

4 Linear Algebra **91**

4.1 Bilinear Forms 91

5 Representations of the Symmetric Groups 101

5.1 The Symmetric Groups 101

5.2 Diagrams,Tableaux and Tabloids 102

5.3 The Specht Module 108

5.4 Standard basis for the Specht module 112

5.5 The number of simple modules 116

5.6 p-regular partitions 119

5.7 Series of R-modules 123

5.8 The Branching Theorem 124

5.9 $S^{(n-2,2)}$ 126

5.10 The dual of a Specht module 132

6 Brauer Characters 135

6.1 Brauer Characters 135

6.2 Algebraic integers 137

6.3 The Jacobson Radical II 143

6.4 A basis for $\mathbb{C}\tilde{G}$ 145

6.5 Blocks 150

6.6 Brauer's Frist Main Theorem 156

6.7 Brauer's Second Main Theorem 165

Chapter 1

Group Theory

1.1 Group Action

Definition 1.1.1 [**def:group action**] *Let G be a group and Ω a set. An action of G on Ω is a binary operation*

$$\cdot : G \times \Omega \to \Omega, (g, \omega) \to g\omega$$

such that

(a) [**a**] $(g\tilde{g})\omega = g(\tilde{g}\omega)$

(b) [**b**] $1\omega = \omega$

for all $g, \tilde{g} \in G$ and $\omega \in \Omega$.

If $\cdot$ is an action for G on Ω we say that G acts on Ω and that Ω is a G-set.

Let Ω be a set. Then $\mathrm{Sym}(\Omega)$ denotes the set of all bijections of Ω. Note that $\mathrm{Sym}(\Omega)$ is a group under composition. The map $(\alpha, \omega) \to \alpha(\omega)$ is an action of $\mathrm{Sym}(\Omega)$ on Ω.

We some times refer to an action as a left action. A right action of G on Ω is map $\Omega \to G \to \Omega$ with $\omega(g\tilde{g}) = (\omega g)\tilde{g}$. If we denote by G^{op} the group which is G as set and with binary operation $g \cdot_{\mathrm{op}} h = hg$, then we se that a right action for $\Omega \times G \to\to \Omega$, $(\omega, g) \to \omega g$ of G gives rise to a left action $G^{\mathrm{op}} \times \Omega \to \Omega, (g, \omega) \to \omega g$ and vice versa.

Definition 1.1.2 [**bi-set**] *Let G and H be groups. A (G, H)-biset is a set I together with a left G- and right-H-action on I such that $gi \cdot h = g \cdot ih$ for all $g \in G, i \in I, h \in H$. In this case we just write gih for $gi \cdot h$.*

We remark that a (G, H)-biset the same as a $G \times H^{\mathrm{op}}$-set and right $G^{\mathrm{op}} \times H$-set.

Definition 1.1.3 [**def:equivariant**] *Let G be a group, I and J G-sets, $\alpha : I \to J$ a function and $K \subset I$ and $H \subseteq G$.*

(a) [**a**] *α is G-*equivariant *if $\alpha(gi) = g\alpha(i)$ for all $g \in G, i \in I$.*

(b) [**b**] *α is a G-isomorphism if α is a bijection and G-*equivariant .

(c) [**c**] *I and J are isomorphic G-sets if there exists a G-isomorphism $\beta : I \to J$.*

(d) [**d**] *$HK = \{hk \mid h \in H, k \in K\}$, $hK = \{h\}K$ and $Hk = H\{k\}$ for $h \in H$, $k \in K$.*

(e) [**e**] *$N_H(K) = \{h \in H \mid hK = K\}$.*

(f) [**f**] *$C_H(K) = \{h \in H \mid hk = k \forall k \in K\}$.*

(g) [**g**] *$C_K(H) = \{k \in K \mid hk = k \forall h \in H\}$.*

(h) [**h**] *$K \subseteq I$ is called H-invariant of $hK = K$ for all $h \in H$, that is if $N_H(K) = K$.*

We will usually write $C_H(k)$ for $C_H(\{k\}$. But observe that G via 1.1.3(d), G also acts on the set of subsets of I. So $C_H(K)$ could now be intepreted as $C_H(\{K\}$, for this reason we will not use $C_H(k)$ for $C_H(\{k\}$, then k itself is a set. Also observe that $C_H(\{K\} = N_H(K)$.

Lemma 1.1.4 [**cayley**] *Let G is a (G,G)-biset via left and right multiplication.*

Proof: This holds since multiplication is assocative. □

Lemma 1.1.5 [**diagonal action**] *G be a group, $\alpha : G \to A$ and $\beta : G \to B$ be group homomorphisms and I an (A,B)-biset. Then G acts on I via $gi = \alpha(g)i\beta(g^{-1})$.*

Proof: $gh \cdot i = \alpha(gh)i\beta((gh)^{-1}) = \alpha(g)\alpha(h)i\beta(h^{-1})\beta(g^{-1}) = g \cdot hi.$ □

Lemma 1.1.6 [**conj**] *Let G be a group. Then $G \times G \to G, (g,h) \to ghg^{-1}$ is an action of G on G.*

Proof: 1.1.4 and 1.1.5 □

Lemma 1.1.7 [**orbits**] *Let G be a group acting on set I. For $i,j \in I$ define $i \sim_G j$ if $j = gi$ for some $g \in G$. Then $\sim$ is an equivalence relation.*

Proof: $i = 1i$, if $j = gi$ then $g^{-1}j = g^{-1}gi = 1i = i$ and if $j = gi$ and $k = hj$, then $k = h \cdot gi = hg \cdot i$. □

Definition 1.1.8 [**def:orbit**]

(a) [**a**] *Let G be a group acting on a set I. Then the equivalence classes of the relation $\sim_G$ on I are called the* orbits *of G on I. Note that the orbit G on I containing i is $Gi = \{gi \mid g \in G\}$.*

(b) [**b**] *Let I be a (G, H)-biset. An orbit for (G, H) on I is an orbit for $G \times H^{\mathrm{op}}$ on I. The orbit $\{gih \mid g \in G, h \in H\}$ of (G, H) on I containing i is denoted by GiH.*

(c) [**c**] *Let G be acting on a set I. Then G acts* transitively *on I provided that there exists exactly one G orbit on I, that is $I \neq \emptyset$ and for all $i, j \in I$ there exists $g \in G$ with $gi = j$.*

Lemma 1.1.9 (Frattini Argument) [**frattini argumnet**] *Let G be groups acting on a set I, $i \in I$ and $H \in G$. If H acts trainisitively on I, then $G = HC_G(i)$.*

Proof: Let $g \in G$. Then there exists $h \in H$ with $gi = hi$. Thus $h^{-1}g \in C_H(i)$ and $g = h \cdot h^{-1}g \in HC_G(i)$. □

Lemma 1.1.10 [**orbits on pairs**] *Let G be a groups acting tranistively on the sets I and J. Let K a G-invariant subset of $I \times J$. Let $(i, j) \in K$. Then the following are equivalent.*

A [**A**] *G acts tranisitively on K.*

B [**B**] *$C_G(i)$ acts transitively on $\{k \in J \mid (i, k) \in K\}$.*

C [**C**] *$C_G(j)$ acts tranistively on $\{k \in I \mid (k, j) \in K\}$.*

Proof: (A)$\Longrightarrow$ (B): Let $(i, k) \in K$. Then there exists $g \in G$ eith $g \cdot (i, j) = (i, k)$. Thus $g \in C_G(i)$, $gj = k$ and (B) holds.

(B)$\Longrightarrow$ (A): Let $((k, l) \in K$. Since G is transitive on I there exists $g \in G$ wit $g \cdot k = i$. Then $(i, gl) = g \cdot (i, gl) \in K$ and so (B), there exists $h \in C_H(i)$ with $hgl = j$. Thus $hg \cdot (k, l) = (i, j)$ and (A) holds.

By symmetry (A)$and(C)$ are equivalent. □

Definition 1.1.11 [**def:conjugation**] *Let G be a group, $g, h \in G$ and $A \leq G$.*

(a) [**a**] *${}^g h := ghg^{-1}$. ${}^g h$ is called the* conjugate *of h under g.*

(b) [**b**] *The action of G on G with $(g, h) \to {}^g h$ is called the action by* conjugation*.*

(c) [**c**] *An orbits of G on G for the action by conjugation is called a* conjugacy classe *of G.*

(d) [**d**] *${}^G h = \{{}^g h \mid g \in G\}$ is the conjugacy class of G containing h.*

(e) [**e**] *An orbit for A on G by right multiplication is called a (left) coset of H, $G/A = \{gA \mid g \in G\}$ is the set of cosets of H.*

Lemma 1.1.12 [**bisets**]

(a) [**a**] *Let I be (G,H)-biset. Then G acts on the set of orbits of H on I via $gO = \{gi \mid i \in O\}$.*

(b) [**b**] *Let G be group and H a subgroup of then G acts on G/H via $gT = \{gt \mid t \in T\}$.*

Proof: (a) $g \cdot iH = gi \cdot H$.

(b) is special case of (a). □

Definition 1.1.13 [**def: transversal**] *Let Δ be a partition of a set I. A* transversal *to Δ is a set T with $|T \cap D| = 1$ for all $D \in \Delta$. If H is a subgroup of G, then a transversal to H is a transversal to the partition G/H of G.*

Lemma 1.1.14 [**transitive**] *Let G be acting on a set I, $i \in I$ and $H = C_G(i)$. Then the map*

$$G/H \to Gi \mid gH \to gi$$

is a well defined G-isomorphism, in particular $|Gi| = |G/C_G(i)|$.

Proof: Let $g \in G$ and $h \in H$. Then $gh \cdot i = g \cdot hi = gi$ and the map is well defined. Clearly it is onto. If $gi = ki$, then $k^{-1}gi = i$, $k^{-1}g \in H$ and so $gH = kH$. Thus the map is 1-1. Finally observe that the map is G-equivariant. □

Corollary 1.1.15 (Orbit Equation) [**orbit equation**] *Let G be acting on a set I, let $\mathcal{O}$ be the set of orbits for G on I and $\mathcal{T}$ a transversal to $\mathcal{O}$. Then*

$$|I| = \sum_{O \in \mathcal{O}} |O| = \sum_{t \in \mathcal{T}} |G/C_G(t)|$$

Proof: The first equality is obvious. For the second let $O \in \mathcal{O}$ and $O \cap \mathcal{T} = \{t\}$. Then by 1.1.14 $|O| = |G/C_G(t)|$ and the second equality holds. □

1.2 Balanced Products of G-sets

Definition 1.2.1 [**def:balanced product**] *Let G be a group, I a right- and J a left G set. Let K be any set and $f : I \times J \to K$ function.*

(a) [**a**] *f is called G-balanced if $f(ig, j) = f(i, gj)$ for all $i \in I$, $j \in J$ and $g \in G$.*

(b) [**b**] *f is called universal G-balanced if f is G-balanced and for all G-balanced functions $g : I \times J \to L$, there exists a unique function $h : K \to L$ with $g = h \circ f$.*

(c) [**c**] *If f is universal G-balanced, K is called the G-balanced product of I and J. We write $I \times_G J$ for K and $(i\,,_G\, j)$ for $f(i,j)$.*

Proposition 1.2.2 [**balanced product**] *Let G be a group, I a right- and J a left G sets. Then there exists a universal G-balanced map $f : I \times J \to K$. Moreover, f is unique up to an isomorphisms of G-balanced maps.*

Note that $I \times J$ is left H-module via the action $g \cdot (i,j) = (ig^{-1}, gj)$. Let K be the set of orbits of G on $I \times J$ and define $f : I \times J \to K, (i,j) \to G \cdot (i,j)$. Observe that a function $f : I \times J \to L$ is G-balanced iff $f(i,j) = f(ig^{-1}, gj)$ for all $i \in I, j \in J, g \in G$, that is iff f is constant on each G-orbit on $I \times J$. So any G-balanced map uniquely factors through K.□

Proposition 1.2.3 [**bi-product**] *Let F, G, H be groups, I an (F,G)- and J an (G,H)-biset. Then $I \times_H J$ is a (F,H)-biset via $f(i\,,_h\, j)h = (fi\,,_H\, jh)$ for all $f \in F, i, j \in J, h \in H$.*

Proof: Just observe that for given $f \in F, h \in H$ the map $I \times J \to I \times_H J$, $(i,j) \to (fi\,,_H\, jg)$ is G-balanced. □

Proposition 1.2.4 [**induced set**] *Let G be a group, H a subgroup and I a G set. View G as a right H-set by right multiplication. Then $G \times_H I$ is an G set via $k(g\,,_H\, i) = (kg\,,_H\, i)$ for all $k, g \in G, i \in I$. The map $\alpha : I \to G \times_H I, i \to (1\,,_H\, i)$ is H-equivariant and universal in the following sense: If J is a G-set and $\beta : I \to K$ is H-equivariant, then there exists a unique G-equivariant map $\gamma : G \times_H I \to J$ with $\beta = \gamma \circ \alpha$.*

Proof: For a fixed $k \in G$ then map $G \times I \to G \times_H I, (g,i) \to (kg\,,_H\, i)$ is clearly H balanced and induces a map

$$G \times_H I \to G \times_H I, (g\,,_H\, i) \to (kg\,,_H\, i).$$

Clearly this defines an action of G on $G \times_H I$. Now let $h \in H$. Then

$$h \cdot \alpha(i) = h \cdot (1\,,_H\, i) = (h\,,_H\, i) = (1\,,_H\, hi) = \alpha(hi)$$

So α is H-invariant.

Given a G-set J and an H-equivariant $\beta : I \to J$. Then the map $G \times I \to J, (g,i) \to g\beta(i)$ is H-equivariant and so induces a unique map $\gamma : G \times_H I \to J, (g\,,_H\, i) \to g\beta(i)$. Then $\gamma(k \cdot (g\,,_H\, i)) = (kg)\beta(i) = k \cdot (g\beta(i)) = k\gamma((g\,,_H\, i))$ and γ is G-equivariant. Also $\gamma(\alpha(i)) = \gamma((1\,,_H\, i)) = 1\beta(i) = \beta(i)$. The uniqueness of γ is obvious. □

Definition 1.2.5 [**def:multi-equivariant**] *Let A be an abelian group, I an A set, $(I_s, s \in S)$ a family of A-sets and $\alpha : \textcircled{\Pi}_S I_s \to I$ a function.*

(a) [**a**] *α is called A-multi-equivariant if α is A-equivariant in each coordinate.*

(b) [**b**] *α is called universal A-multi-equivariant if α is A-multi-equivariant and for each A-multi-equivariant $\beta : \mathop{\textcircled{Π}}_S I_s \to J$ there exists a unique A-equivariant $\gamma : I \to J$ with $\beta = \gamma \circ \alpha$.*

(c) [**c**] *If α is universal A multi-equivariant, I is called the A-multi-equivariant product of $(I_s, s \in S)$. We denote I be ${}_A\mathop{\textcircled{Π}}_S I_s$ and $\alpha(m)$ by ${}_Am$.*

Proposition 1.2.6 [**easy m-product**] *Let A be an abelian group and $(I_s, s \in S)$ a family of A-sets and I an A-set.*

(a) [**a**] *$\bigoplus_S A$ acts on $\mathop{\textcircled{$\Pi$}}_S I_s$ via $(a_s)(i_s) = (a_s i_s)$ and on I via $(a_s)i = \prod_S a_s \cdot i$.*

(b) [**b**] *A map $f : \mathop{\textcircled{Π}}_S I_s \to I$ is A-multi-equivariant iff it is $\bigoplus_S A$-equivariant.*

Proof: Obvious.

Proposition 1.2.7 [**m-product**] *Let A be an abelian group and $(I_s, s \in S)$ a family of A-sets. Then there exists a universal H-multi-equivariant map $\alpha : \mathop{\textcircled{Π}}_S I_s \to I$ and α is unique up to isomorphism of A-multi-equivarinat maps.*

Proof: Let $B = \{(i_s) \in \bigoplus_{s \in S} A \mid \prod_{i \in I} i_s = 1\}$. Let I be the set of orbits of B on $\mathop{\textcircled{$\Pi$}}_S I_s \to I$ and define $\alpha : \mathop{\textcircled{Π}}_S I_s, i \to Bi$. Let $\beta : \mathop{\textcircled{Π}}_S I_s \to J$ be A-multi-equivariant. Since B acts trivially on J, 1.2.6(b) implies that β is constant on the orbits of B. Thus β induces a unique function $\gamma : I \to J$ with $\beta = \gamma \circ \alpha$. □

Lemma 1.2.8 [**decomposing universal**] *Suppose A is an abelian group and $(I_s, s \in S)$ a family of A-sets. Let $\mathcal{O}_s$ be the sets of orbits for A on I_s. Then*

$$
{}_A\mathop{\textcircled{Π}}_S I_s \cong \biguplus \{ {}_A\mathop{\textcircled{Π}}_S O_s \mid (O_s)_{s \in S} \in \mathop{\textcircled{Π}}_S \mathcal{O}_s \}
$$

as an A-set.

Proof: For $O = (O_s)_s \in \mathop{\textcircled{Π}}_S \mathcal{O}_s$ let $\alpha_0 : \mathop{\textcircled{Π}}_{s \in S} O_s \to B_0$ be universal H-multi-equivariant map. For $i = (i_s) \in \mathop{\textcircled{Π}}_S I_s$ define $O(i) = (O_s(i))_s \in \mathop{\textcircled{Π}}_S \mathcal{O}_s$ by $i_s \in O_s(i) \in \mathcal{O}_s$. Define

$$
\alpha : \mathop{\textcircled{Π}}_S I_s \to \biguplus \{ B_0 \mid O \in \mathop{\textcircled{Π}}_S \mathcal{O}_s, i \to \alpha_{O(i)}(i)
$$

Then it is readily verified that α is universal H-multi-equivariant. □

Lemma 1.2.9 [**regular balanced**] *Suppose A is an abelian group, $(I_s, s \in S)$ a finite family of transitive A-sets. Put $C = \langle C_G(I_s) \mid s \in S \rangle$.*

(a) [**a**] *Let $i = (i_s) \in \mathop{\textcircled{Π}}_S I_s$ and $(a_s) \in \mathop{\textcircled{Π}}_S A$. Then the map $\mathop{\textcircled{$\Pi$}}_S I_s \to A/C, (a_s i_s) \to \mathop{\textcircled{Π}}_{s \in S} a_s C$ is welldefined and universal A-multi-equivariant.*

(b) [**b**] *A acts transitively on ${}_A\textcircled{$\Pi$}_S I_s$ and $C = C_G(I)$.*

Proof: (a) Since A is tranisitive each $(j_s)_\in \textcircled{$\Pi$}_S I_s$ is of the form $(a_s i_s)$. Also if $(a_s i_s) = (b_s i_s)$ then $a_s b_s^{-1} \in C_A(I_s)$ and so $\prod a_s \cdot (\prod b_s)^{-1} \in C$. Thus α is well defined. Clearly α is A-multi-equivariant. Let $\beta : \textcircled{$\Pi$}_i I_s \to J$ be A-multiequivariant. Pick a fixed $t \in S$ and define

$$\gamma : A/C \to I \prod a_s C \to \beta((a_s i_s)_s)$$

This clearly has all the required properties, but we must verify that it is well defined. So suppose $\prod a_s C = \prod b_s C$. Since $C = \langle C_A(I_s) \rangle = \prod_S C_A(I_s)$, the exists $c_s \in C_G(I_s)$ with $a := \prod a_s = \textcircled{Π}\, b_s c_s$ and since β is A-equivariant we get $\beta((a_s i_s)_s) = \beta((b_s c_s i_s)_s) = \beta((b_s)_s))$ and so γ is well-defined. □

Definition 1.2.10 [**def:g-i-sets**] *Let G be a group and I a G-set. A $(G\text{-}I, H)$-biset is a family $(M_i, i \in I)$ of right H-sets together with a G-action on the disjoint union $\biguplus_{i \in I} M_i$ such*

(a) [**a**] *$gM_i = M_{ig}$*

(b) [**b**] *$\rho_i(g) : M_i \to M_{gi}$, $m \to gm$ is H-equivariant for all $i \in I$.*

A G-I-set is a $(G\text{-}I, 1)$-biset.

Note here that condition (b) ensures that $\biguplus_{i \in I} M_i$ is a (G, H)-biset.

Some examples: If G acts trivially on I (that is $gi = i$ for all $g \in G, i \in I$), then an $(G\text{-}I, H)$-set is just a family $(M_i, i \in I)$ of (G, H)-bisets.

Let M be (G, H)-biset and $K \leq G$ and W a (K, H)-subset of M. Then $(TW \mid T \in G/K)$ is an $(G\text{-}G/K, H)$-biset. Here for $T \in G/H$, $TW = \{tw \mid t \in T, w \in T\} = tW$ for all $t \in T$.

Let $(M_i, i \in I)$ be a system of imprimitivity of H-invariant subsets for G on M. Then $(M_i, i \in I)$ is an $(G\text{-}I, H)$-biset.

Lemma 1.2.11 [**g-i-set**] *Let G and H be a groups with H-abelian, I a G-set and $(M_i, i \in I)$ a $(G\text{-}I, H)$-set.*

(a) [**a**] *$(M_i, i \in I)$ is an H-invariant system of imprimitivity for G on $\biguplus_{i \in I} M_i$.*

(b) [**b**] *${}_H\textcircled{$\Pi$}_I M_i$ is a (G, H)-biset via $g \cdot_H m = {}_H(g \cdot m \circ g^{-1})$. Moreover, $(g \cdot_H m)_i = {}_H(g m_{g^{-1}i})$ for all $g \in G$ and $m = (m_i)_i \in \textcircled{Π}_I M_i$.*

Proof: (a) is obvious.

(b) Let $f, g \in G$ and $m = (m_i) \in I$. Put $n_i = g m_{g^{-1}i}$ and so $g \cdot m = n$. Then

$$f \cdot (g \cdot m) = f \cdot n = (f n_{g^{-1}i})_i = (f \cdot (g m_{g^{-1}f^{-1}i})_i = (f \cdot m_{(fg)^{-1}i})_i = fg \cdot m.$$

So G acts on $\textcircled{$\Pi$}_I M_i$. Moreover, for fixed $g \in G$ the map $\textcircled{$\Pi$}_I M_i \to {}_H\textcircled{Π}_I M_i, m \to {}_H gm$ is clearly H-multi-equivariant and so (b) holds. □

Definition 1.2.12 [**def:product action**] *The action of G on ${}_H\textcircled{\Pi}_I M_i$ as in 1.2.11(b) is called the* product action *of G on ${}_H\textcircled{\Pi}_I M_i$.*

Consider the case $H = 1$ in 1.2.11(b). Let $\mathcal{T}$ be the set of all transversal to $(M_i, i \in I)$. Then map $\textcircled{\Pi}_I M_i \to \mathcal{T}, m \to \operatorname{Im} m$ is a G-isomorphism, where $\Im m = \{m_i \mid i \in I\}$.

Lemma 1.2.13 [**transfer map**] *Let G be a group and $H \leq G$ with $|G/H|$ finite.*

(a) [**a**] *$(K/H' \mid K \in K \in G/H)$ is a $(G\text{-}G/H, H/H')$-set.*

(b) [**b**] *H/H' acts regularly on $I := {}_{H/H'}\textcircled{\Pi}_{G/H} K/H'$.*

(c) [**c**] *For $g \in G$ there exists a unique $h(g) \in H/H'$ with $gi = ih(g)$ for all $i \in I$.*

(d) [**d**] *Then map $\tau_{G \to H} : G \to H/H', g \to h(g)$ is a homomorphism.*

(e) [**e**] *Let $K \in G/H$ pick $t_K \in K$ and for $K \in K$ and $g \in G$ define $h_K(g) \in G$ by $gt_K = t_{gK}h(g, K)$. Then*

$$\tau_{(}G \to H) = \textcircled{\Pi}_{K \in G/H)} h(g, K))H'$$

Proof: (a) Clear H/H' acts G/H' by right multiplication, $(K/H' \mid K \in K \in G/H)$ is the set of orbits for H/H' on G/H' and so an $(G\text{-}G/H, H/H')$-set.

(b) H/H' acts regularly on K/H' for all $K \in G/H$. So (b) follows from 1.2.9

(c) Follows from the fact that I is a $G, H/H')$-biset and H/H' acts regulary on I.

(d) Obvious, since G acts on I.

(e) We have

$$\begin{array}{rclcl} g \cdot {}_H(t_K) & = & {}_H(gt_{g^{-1}K} & = & {}_H(t_K h(g, g^{-1}K)) \\ & = & {}_H(t_K) \cdot \prod_{K \in G/H} h(g, g^{-1}K) & = & {}_H(t_K) \cdot \prod_{K \in G/H} h(g, K) \end{array}$$

and so $\tau_{G \to H}(g) = h(g) = \textcircled{\Pi}_{K \in G/H} h(g, K)$. □

Definition 1.2.14 [**def:transfer**] *Let G be a group and H a subgroup. Then* $\operatorname{Der}_H(G) = \langle {}^g h h^{-1} \mid h \in H, g \in G, {}^g h \in H \rangle$

Lemma 1.2.15 [**transfer**] *Let G be a group and H a subgroup of finite index n. Let $g \in G$.*

(a) [**a**] *Let $\mathcal{B}$ be the set of orbits for $\langle g \rangle$ on G/H. For $B \in \mathcal{B}$ pick $T_B \in B$ and $r_B \in T_B$. Then*

$$\tau_{G \to H}(g) = (\prod_{B \in \mathcal{B}} r_B^{-1} g^{|B|} r_B)H'$$

(b) [**b**] *Put* $D = \mathrm{Der}_H(G)$. *If* $g \in H$, *then* $\tau_{G\to H}(g)D = g^n D$.

(c) [**c**] *If* $H \leq Z(G)$ *then* $\tau(g) = g^n$.

Proof: (a) Observe that $(g^i r_B \mid B \in \mathcal{B}, 0 \leq i < |B|)$ is a transversal to H. Define $h(g, K)$ for $g \in g$ and G/H as in **??**(**??**). We have $g \cdot g^i r_B = g^{i+1} r_B$. So $h(g, g^i T_B) = 1$ for all $0 \leq i < |B| - 1$ and $h(g, g^{|B|-1} T_B) = r_B^{-1} g_B^{|B|} r_B$. So (a) follows from the definition of $\tau_{G\to H}$.

(b) Since $r_B^{-1} g^{|B|} r_B \in H$ and $g^{|B|} \in H$ we get

$$r_B^{-1} g^{|B|} r_B g^{-|B|} \in D$$

and so

$$r_B^{-1} g^{|B|} r_B g^{-|B|} D = g^{|B|} D.$$

Hence by (a)

$$\tau_{G\to H}(g)D = (\prod_{B\in\mathcal{B}} r_B^{-1} g^{|B|} r_B)D = \prod_{B\in\mathcal{B}} g^{|B|} D = g^{\sum_{B\in\mathcal{B}} |B|} D$$

But $\sum_{B\in\mathcal{B}} |B| = |G/H| = n$ and so (b) holds.

(c) We have $r_B^{-1} g^{|B|} r_B \in H \leq Z(G)$ and so $r_B^{-1} g^{|B|} r_B = g^{|B|}$. Also $H' = 1$ and $\sum_{B\in\mathcal{B}} |B| = n$. So (c) follows from (a). □

1.3 Central by finite groups

Lemma 1.3.1 (Reidemeister-Schreier) [**rs**] *Let* G *be a group and* N *subgroup of* G.

Let I *be a transversal to* N *and* $J \subseteq G$ *with* $G = \langle J \rangle$ *and* $J = J^{-1}$. *For* $i \in I, j \in J$ *pick* $n(i,j) \in N$ *and* $k(i,j) \in I$ *with* $ji = k(i,j)n(i,j)$. *Then* $N = \langle n(i,j) \mid i \in I, j \in J \rangle$.

In particular, N *can be generated by* $|J||G/N|$ *elements.*

Proof: Let $A = \langle n(i,j) \mid i \in I, j \in J \rangle$. Let $i \in I, j \in J$. Then $jiA = k(i,j)n(i,j)A = k(i,j)A$. Thus $JIA \subseteq IA$. Since $J = J^{-1}$ we get $JIA = IA$. Since the set of all $g \in G$ with $gIA = IA$ is a subgroup group of G, we get $G = GIA = IA$. Hence $N = A(N \cap I)$ and since $|N \cap I| = 1$, $N = A$.

Definition 1.3.2 [**def:commutators**] *Let* G *be a group.*

(a) [**a**] *For* $x, y \in G$, $[x,y] = xyx^{-1}y^{-1}$. $[x,y]$ *is called the* commutator *of* x *and* y.

(b) [**b**] *For* $A, B \subseteq G$, $[A,B] = \langle [a,b] \mid a \in A, b \in B \rangle$.

(c) [**c**] $G' = [G,G]$. G' *is called the commutator or* derived *group of* G.

Lemma 1.3.3 [**commutators**] *Let* G *be a group and* $x, y, z \in G$. *Then* *(a)* [**a**] $xy = [x,y]yx$.

(b) [**b**] $[x,y]^{-1} = [y,x]$.

(c) [**c**] $[xy,z] = {}^{x}[y,z][x,z]$ *and* $[z,xy] = [z,x]\,{}^{x}[z,y]$

(d) [**d**] $[A,B] = [B,A]$ *for all* $A, B \subseteq G$.

Proof: (a) $[x,y]yx = xyx^{-1} \cdot y^{-1}y \cdot x = xy \cdot x^{-1}x = xy$.
(b) $[x,y]^{-1} = (xyx^{-1}y^{-1})^{-1} = yxy^{-1}x^{-1} = [y,x]$.
(c)

$$\begin{aligned} [xy,z] &= xyzy^{-1}x^{-1}z^{-1} &&= x \cdot yzy^{-1}z^{-1} \cdot zx^{-1}z^{-1} \\ &= x \cdot [y,z] \cdot x^{-1} \cdot xzx^{-1}z^{-1} &&= {}^{x}[y,z][x,z] \end{aligned}$$

and so using (b)

$$[z,xy] = [xy,z]^{-1} = ({}^{x}[y,z][x,z])^{-1} = [z,x]\,{}^{x}[z,y]$$

(d) follows from (b). □

Proposition 1.3.4 [**center of finite index**] *Let G be a group with $Z(G)$ of finite index n . Then $|G'|$ is finite of order bounded in terms of n. Moroever, G has exponent dividing n.*

Proof: Let $n = |G/Z(G)|$. By 1.2.15(c), the map $\tau : G \to Z(G), g \to g^n$ is homomorphism. Since $Z(G)$ is abelian, $G' \leq \ker\tau$ and G' has exponent dividing n. Since $[g_1z_1, g_2z_2] = [g_1, g_2]$ for all $g_1, g_2 \in G$ and $z_1, z_1 \in Z(G)$, there exists at most n^2 commutators. So by 1.3.1 $G' \cap Z(G)$ can be generated by n^3 elements. So $G' \cap Z(G)$ is abelian of exponent dividing n, $|G' \cap Z(G)| \leq n^{n^3}$ and so $|G'| \leq n^{n^3+1}$. □

1.4 Finite p-Groups

Lemma 1.4.1 [**aut cylic**] *Let $n \in \mathbb{Z}^+$ and let $n = \prod_{i=1}^m p_i^{k_i}$ be the prime factorization of n. Let P be a cyclic group of order n. Then $|\mathrm{Aut}(P)| = \prod_{i=1}^m (p_i - 1)p_i^{k_i-1}$.*

Proof: Let P_i be the Sylow p_i subgroup of P. Then $P = \bigoplus_{i=1}^m P_i$ and each P_i is invariant under $\mathrm{Aut}(P)$. So $\mathrm{Aut}(P) = \mathop{\textcircled{Π}}_{i=1}^m \mathrm{Aut}(P_i)$ and we may assume $n = p^k$ for some prime p and some $k \in \mathbb{Z}^+$. Let Q be the cyclic subgroup of order p^{k-1} in P. If $x \in P$ then $P = \langle x \rangle$ iff $x \notin Q$. Fix $x \in P \setminus Q$. Then for each $y \in P \setminus Q$ there exists unique $\alpha \in \mathrm{Aut}(P)$ with $\alpha(x) = y$. Thus $\mathrm{Aut}(P) = |P \setminus Q| = p^k - p^{k-1} = p^{k-1}(p-1)$. □

Lemma 1.4.2 [**central commutator**] *Let G be a group with $G' \leq Z(G)$.*

(a) [**a**] *The commutator map $G/Z(G) \times G/Z(G) \to G', (xZ(G), yZ(G)) \to [x,y]$ is well defined and $\mathbb{Z}$-bilinear.*

(b) [**b**] $[x^i, y^j] = [x,y]^{ij}$ *for* $x, y \in G, i, j \in \mathbb{Z}$.

(c) [**c**] $(xy)^i = [y,x]^{\binom{i}{2}} x^i y^i$ *for all* $x, y \in G, i \in \mathbb{N}$.

Proof: (a) By 1.3.3(c), $[xy, z] = {}^x[y,z][x,z]$. Since $G' \leq Z(G)$ we conclude $[xy,z] = [x,z][y,z]$. Similary $[x,yz] = [x,y][x,z]$ and so (a) holds.

(b) follows immediately from (a).

(c) Let $z = [y,x]$. For $i = 0$, both sides in (c) are 1. For $i = 1$ both sides are xy. Suppose (c) is true for i. By (b), $[y^i, x] = z^i$ and so $y^i x = z^i x y^i$. Hence

$$(xy)^{i+1} = (xy)^i \cdot xy = z^{\binom{i}{2}} x^i \cdot y^i x \cdot y = z^{\binom{i}{2}} x^i \cdot z^i x y^i \cdot y = z^{\binom{i}{2}+i} x^{i+1} y^{i+1} = z^{\binom{i+1}{2}} y^{i+1} x^{i+1}$$

□

Definition 1.4.3 [**def:frattini**] *Let G be a group.*

(a) [**a**] *$\Phi(G)$ is the intersection of the maximal subgroups of G, with $\Phi(G) = G$ if G has no maximal subgroups. $\Phi(G)$ is called the* Frattini subgroup *of G.*

(b) [**b**] *Let p be a prime or $p = \infty$. Then G is an* elementary abelian *p group if G is abelian and $|g| = p$ for all $g \in G^\sharp$.*

(c) [**c**] *$Z_0(G) = 1$ and inductively $Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$. $Z_i(G)$ is called the i-th center of G.*

(d) [**d**] *G is called* nilpotent *if $G = Z_n(G)$ for some $n \in mnN$. The smallest such n is called the nilpotency* class *of G.*

Lemma 1.4.4 [**p groups nilpotent**] *All finite p-groups are nilpotent.*

Proof: Let P be a non-trivial finite p-group and T a transversal to the conjugacy classes of P. By the orbit equation 1.1.15

$$|P| = \sum_{t \in T} |P/C_P(t)| = 1 + \sum_{1 \neq t \in T} |P/C_P(t)|$$

Since $p \mid |P|$ we conclude that $p \nmid |P/C_P(t)|$ for some $1 \neq t \in T$. Hence $P = C_P(t)$, $t \in Z(P)$ and so $Z(P) \neq 1$. By induction $P/Z(P)$ is nilpotent. So $P/Z(P) = Z_k(P/Z(P))$ for some k and thus $P = Z_{k+1}(P)$. □

Lemma 1.4.5 [**nilpotent**] *Let G be a nilpotent group.*

(a) [**a**] *If $1 \neq H \trianglelefteq G$, then $H \cap Z(G) \neq 1$.*

(b) [**b**] *If $1 \neq H \trianglelefteq G$, then $[H, G] < H$.*

(c) [**c**] *If $H < G$, then $H < N_G(H)$.*

(d) [**d**] *If H is maximal in G, then $H \trianglelefteq G$ and $|G/H|$ is a prime.*

Proof: (a) Let k be minimal with $H \cap Z_k(G) \neq 1$. Then $[H \cap Z_k(G), G] \leq H \cap Z_{k-1}(G) = 1$ and so $H \cap Z_k(G) \leq Z(G)$.

(b) Since $H \not\leq 1 = Z_0(G)$ but $H \leq G = Z_n(G)$ for some n, there exists a maximal k with $H \not\leq Z_k(G)$. Then $H \leq Z_{k+1}(G)$ and $[H, G] \leq H \cap Z_k(G) < H$.

(c) Since $G \not\leq H$, there exists a maximal k with $Z_k(G) \leq H$. Then $Z_{k+1}(G) \not\leq H$ and $[Z_{k+1}(G), H] \leq Z_k(G) \leq H$. Thus $Z_{k+1}(G) \leq N_G(H)$ and $H < N_G(H)$.

(d) By (c), $H < N_G(H)$ and so by maximality of H, $G = N_G(H)$. So $H \trianglelefteq G$. By maximality of H, G/H has no proper subgroups and so G/H has prime order.

Lemma 1.4.6 [**char nilpotent**] *Let G be a finite group. The the following are equivalent*

(a) [**a**] *G is nilpotent.*

(b) [**b**] *For all $H < G$, $H < N_G(H)$.*

(c) [**c**] *All maximal subgroups of G are normal in G.*

(d) [**d**] *For all primes p, G has a unique Sylow p-subgroup.*

(e) [**e**] *G is a direct product of p-groups.*

Proof: (a)$\Longrightarrow$ (b): See 1.4.5(c).

(b)$\Longrightarrow$ (c): Let M be a maximal subgroups of G. Then $M < N_G(M) \leq G$ and by maximality of G, $M \trianglelefteq G$.

(c)$\Longrightarrow$ (d): Let S be a Sylow p-subgroup of G. If $G = N_G(S)$, (c) holds. So suppose $N_G(S) \neq G$ and let M be a maximal subgroup of G with $N_G(S) \leq M$. By assumption $M \trianglelefteq G$ and so by the Frattini argumment, $G = N_G(S)M \leq M$, a contradiction.

(d)$\Longrightarrow$ (e): Let S and T be Sylow subgroups for distinct primes. Then by (c) S and T are normal in G and so $[S, T] = 1$. It follows that G is the direct product of irs Sylow subgroups.

(e)$\Longrightarrow$ (a): Since finite direct products of nilpotent groups are clearly nilpotent, this follows from 1.4.4. □

Lemma 1.4.7 [**frattini**] *Let p be a prime and P a finite p-group. Then $\Phi(P) = P'\langle g^p \mid g \in P\rangle$ and $\Phi(P)$ is the smallest normal subgroup of P with elementary abelian quotient.*

Proof: Let $H = P'\langle g^p \mid g \in P\rangle$ and let $N \trianglelefteq G$. Then P/N is elementary abelian iff $H \leq N$. So it remains to show that $H = \Phi(P)$.

If M is a maximal subgroup of P, then by 1.4.5(d), P/M is cylic of order p and so $H \leq M$. Thus $H \leq \Phi(P)$.

Let $\overline{P} = P/H$. Then $\overline{P}$ is elementary abelian and so a vector space over $\mathbb{Z}/p\mathbb{Z}$. Let $a \in P \setminus H$. It follows that $\overline{P} = \langle \overline{a} \rangle \oplus \overline{A}$ for some $H \leq A < P$. Then A is a maximal subgroup of P and $a \notin A$. Thus $a \notin \Phi(P)$ and so $\Phi(P) \leq H$. □

1.5 A p-complement Theorem

Definition 1.5.1 [**def:hall**] *Let π be a set of primes and G a finite group.*

(a) [**z**] *Let n be an integer then $\pi(n)$ is the set of positive prime divisors of n. n_π is the largest divsor of n, with $\pi(n_\pi) \subseteq \pi$.*

(b) [**y**] *$\pi(G) = \pi(|G|)$, G is a π-group if $\pi(G) \subseteq \pi$.*

(c) [**a**] *A π-Hall subgroup of H is a subgroup H with $|H| = |G|_\pi$*

(d) [**b**] *$O_\pi(G)$ is the largest normal π-sibgroup of G.*

(e) [**c**] *$O^\pi(G)$ is the smallest normal subgroup of G such that $G/O^\pi(G)$ is a π-group.*

(f) [**d**] *π' is the set all primes not in π.*

(g) [**e**] *G is called a π-group if $|G| = |G|_\pi$.*

(h) [**f**] *$g \in G$ is called a π-element if $|g| = |g|_\pi$.*

Lemma 1.5.2 [**decompose x**] *Let G be a group and $x \in G$ with finite order. Let π be a set of prime. Then there exists unique $y, z \in \langle x \rangle$ with $x = yz$, x a π and y a pi'-element. We denote y by x_π and z by $x_{\pi'}$.*

Proof: Let $n = |g|$. Since n_π and $n_{\pi'}$ are relative prime, there exists $m_\pi, m_{\pi'} \in \mathbb{Z}$ with $1 = n_\pi m_\pi + m_{\pi'} m_{\pi'}$. Put $y = x^{m_{\pi'}} m_{\pi'}$ and $z = x^{n_\pi m_\pi}$. The lemma is now easy to verify.□

Lemma 1.5.3 [**easy hall**] *Let π be a set of primes, G a finite group and $N \trianglelefteq G$.*

(a) [**a**] *$O^\pi(G)$ is the subgroup of G generated by all the π'-elements.*

(b) [**b**] *If G is nilpotent, $G = O_\pi(G) \times O_{\pi'}(G)$ and $O_\pi(G) = O^{\pi'}(G)$.*

(c) [**c**] *$O^\pi(G/N) = O^\pi(G)N/N$.*

(d) [**d**] *$O_\pi(H) = H \cap O_\pi(G)$ for all subnormal subgroups H of G.*

(e) [**e**] *Let H be a π-Hall subgroup of G. Then HN/N is a π-Hall subgroup of G/N. In particular, $G = HO^{\pi}(G)$.*

(f) [**f**] *$O^{\pi'}(G)G' \cap O^{\pi}(G)G' = G'$.*

(g) [**g**] *$H \cap O^{\pi}(G) \leq G'$ for all π-subgroups H of G.*

(h) [**h**] *$O^{\pi}(H) \leq O^{\pi}(G)$ for all $H \leq G$.*

Proof:

(a) Let H be the subgroup generated by all the π'-elements in G. Let $g \in G$, then $g = xy$ where x is a π and y is a π'-element. $|yO^{\pi}(G)/O^{\pi}(G)$ is a $\pi-$ and a π'-element and so $y \in O^{\pi}(G)$. In partculcar, $H \leq O^{\pi}(G)$. Now $gH = xH$ and so G/H is a π-group and $O^{\pi}(G) \leq H$.

(b) Follows from 1.4.6(d).

(c) $G/O^{\pi}(G)N$ is a π-group and so $O^{\pi}(G/N) \leq O^{\pi}(G)N/N$. $O^{\pi}(G)N/N$ is generated by π'-elements and so $O^{\pi}(G)N/N \leq O^{\pi}(G/N)$.

(d) Let $H \trianglelefteq\trianglelefteq M \triangleleft G$. By induction on $|G|$, $O_{\pi}(H) = O_{\pi}(M) \cap H$. $O_{\pi}(M)$ is characteristic in M and so normal in G. So $O_{\pi}(M) \leq O_{\pi}(G)$. $O_{\pi}(G) \cap M$ is a normal π-subgroup of M and so $O_{\pi}(G) \cap M \leq O_{\pi}(M)$. Thus $O_{\pi}(M) = O_{\pi}(G) \cap M$ and

$$O_{\pi}(H) = O_{\pi}(M) \cap H = (O_{\pi}(G) \cap M) \cap H = O_{\pi}(G) \cap H.$$

(e) $|HN/N|$ divides $|H|$ and $|G/HN|$ divides $|G/H|$.

(f) Follows from (c) (with $N = G'$) and (b).

(g) Follows from (a) and (f).

(h) Follows from (a). □

Proposition 1.5.4 [**focal**] *Let π be a set of primes, G be a finite group and H a π- Hall-subgroup of G. Then*

$$H \cap G' = \mathrm{Der}_H(G) \text{ and } O_{\pi}(G/G') \cong H/\mathrm{Der}_H(G)$$

Proof: Let $D = \mathrm{Der}_H(G)$ and $\tau = \tau_{G \to H}$. Clearly $D \leq H \cap G'$. Since τ is a homomorphism and $\tau(G) \leq H/H'$ is abelian, $G' \leq \ker \tau$. Let $g \in H \cap G'$ and put $n = |G/H|$. Then by 1.2.15(b) $g^n D = \tau(g)D = D$. So $g^n \in D$. Since $|H/D|$ is relatively prime to n we get $g \in D$. Thus $H \cap G' = D$.

by 1.5.3(e) HG'/G' is a π-Hall subgroup of G/G' and so by 1.5.3(b), $HG'/G' = O_{\pi}(G/G')$. Also $HG'/G' \cong H/H \cap G' = H/D$ and so the proposition is proved. □

Lemma 1.5.5 (Burnside lemma) [**central fusion**] *Let G be a finite group, p a prime and $S \in \mathrm{Syl}_p(G)$. Let A, B be normal subsets S. Then A and B are conjugate in G iff they are conjugate in $N_G(S)$.*

Proof: Let $g \in G$ with ${}^gA = B$. Then both ${}^gS$ and S are Sylow p-subgroups of $N_G(B)$ and so ${}^{hg}S = S$ for some $h \in N_G(A)$. Thus $hg \in N_G(S)$ and ${}^{hg}A = {}^hB = B$.

Lemma 1.5.6 [**focal burnside**] *Let G be a finite group, p a prime and $S \in \mathrm{Syl}_p(G)$. Suppose that S is abelian.*

(a) [**a**] $S \cap G' = \mathrm{Der}_S(G) = [N_G(S), S] = [O^p(N_G(S)), S] = S \cap O^p(G)$.

(b) [**c**] *If $S \leq Z(N_G(S))$, then $S \cap O^p(G) = 1$ and $SO^p(G) = G$.*

(c) [**d**] *If $G = O^p(G)$ then $[N_G(S), S] = S$.*

Proof: (a) By 1.5.4

$$S \cap G' = \mathrm{Der}_S(G) \tag{1}$$

By 1.5.5

$$\mathrm{Der}_S(G) = \langle {}^gss^{-1} \mid g \in G, s \in S, {}^gs \in S\rangle = \langle {}^gss^{-1} \mid g \in N_G(S), s \in S\rangle = [N_G(S), S]$$

That is

$$\mathrm{Der}_S(G) = [N_G(S), S]. \tag{2}$$

Put $H = N_G(S)$. By 1.5.3(e), $H = O^p(H)S$ and since $[S, S] = 1$

$$[N_G(S), S] = [O^p(H), S] \leq O^p(G) \cap S. \tag{3}$$

By 1.5.3(g),

$$S \cap O^p(G) \leq S \cap G'. \tag{4}$$

(1)-(4) imply (a).

(b) By (a) $S \cap O^p(G) = [N_G(S), S] = 1$ and by 1.5.3(e), $G = SO^p(G)$.

(c) By (a) $S = S \cap O^p(G) = [N_G(S), S]$. □

Corollary 1.5.7 [**cyclic sylows**] *Let G be a finite group.*

(a) [**a**] *Let p be the positive prime dividing $|G|$. If the Sylow p-subgroups of G are cyclic, $O^p(G)$ is a p'-group.*

(b) [**b**] *Suppose all Sylow subgroups of G are cyclic. Let $p_1 > p_2 > p_3 > \dots p_n$ be the prime divisors of $|G|$ and let $S_i \in \mathrm{Syl}_{p_i}(G)$. Put $T_i = S_1 S_2 \dots S_i$ and $\pi_i = \{p_1, \dots, p_i\}$. Then*

(a) [**a**] $T_0 = 1 \lhd T_1 \lhd T_2 \lhd T_3 \dots \lhd T_{n-1} \lhd T_n = G$.

(b) [**b**] $T_i/T_{i-1} \cong S_i$ *for all* $1 \leq i \leq n$.

(c) [**c**] $T_i = O_{\pi_i}(G) \trianglelefteq G$ *and* T_i *is the unique* π_i*-Hall subgroup of* G.

(d) [**d**] G *is solvable.*

Proof: (a) Let S be a Sylow p-subgroup of G. Since S is abelian $S \leq C_G(S)$ and so $N_G(S)/C_G(S)$ is a p'-group. Thus $|N_G(S)/C_G(S)|$ divides $|\mathrm{Aut}(S)_{p'}|$. By 1.4.1 $|\mathrm{Aut}(S)|_{p'} = p-1$. Since $|N_G(S)|$ is not divisible by any prime smaller than p, $N_G(S)/C_G(S) = 1$ and so $[N_G(S), S] = 1$. Thus (a) follows from 1.5.6(b).

(b) Let $p = p_n$. Then by (a), $H := O^p(G)$ is p'-group. So $p_1, \dots, p_{n-1}$ are exactly the prime divsiors of $|H|$. Thus $O_{\pi_{n-1}}(G) \leq H \leq O_{\pi_{n-1}}(G)$. So $H = O_{\pi_{n-1}}(G)$. Moreover, $S_i \leq H$ and so by induction on n,

1° [**1**]

(a) [**1:a**] $T_0 = 1 \lhd T_1 \lhd T_2 \lhd T_3 \dots \lhd T_{n-1} = H$.

(b) [**1:b**] $T_i/T_{i-1} \cong S_i$ *for all* $1 \leq i \leq n-1$.

(c) [**1:c**] $T_i = O_{\pi_i}(H)$ *and* T_i *is the unique* π_i*-Hall subgroup of* H *for all* $1 \leq i \leq n-1$.

We have $G = S_n H = S_n T_{n-1} = T_n$ and so (a) implies (b:a).

We have $S_n \cap H = 1$ and so $G/T_{n-1} \cong S_n$ and so (b) implies (b:b).

Clearly $O_{\pi_n}(G) = G = T_n$ and T_n is the unique π_n-Hall subgroup of G.

Let $i < n$. Then $O_{\pi_i}(H)$ is a π_{n-1}-subgroup and so contained in H. So by 1.5.3(d) and (c) gives

$$O_{\pi_i}(G) = O_{\pi_i}(G) \cap H = O_{\pi_i}(H) = T_i$$

Also any π_i-Hall subgroups of G is contained in H and so (c) implies (b:c).

(b:d) follows from (a) and (b). □

Chapter 2

General Representation Theory

2.1 Basic Definitions

With ring we always mean a ring with 1 and all ring homomorphisms send 1 to 1.

Definition 2.1.1 [**def:r-module**] *Let R be a ring and M an abelian group. An R-*module structure *on M is a binary operation*

$$\cdot : R \times M \to M, (r, m) \to rm$$

such that

(a) [**a**] $r(m + \tilde{m}) = rm + r\tilde{m}$

(b) [**b**] $(r + \tilde{r})m = rm + r\tilde{m}$

(c) [**c**] $(r\tilde{r})m = r(\tilde{r}m)$

(d) [**d**] $1m = m.$

for all $r, \tilde{r} \in R$ and $m, \tilde{m} \in M$.
*An R-*module *is an abelian group M together with an R-module structure $\cdot$ on M.*

Let M be an abelian group. $\mathrm{End}(M)$ denotes the endomorphism ring on M. So, as a set, $\mathrm{End}(M)$ consists of all homomorphisms from M to M. For $\alpha, \beta \in \mathrm{End}(M)$, $\alpha + \beta$ and $\alpha\beta$ are defined by $(\alpha + \beta)(m) = \alpha(m) + \beta(m)$ and $(\alpha\beta)(m) = \alpha(\beta(m))$. Note that M is an $\mathrm{End}(M)$ module via $\alpha m = \alpha(m)$ for all $\alpha \in \mathrm{End}(M)$, $m \in M$.

Definition 2.1.2 [**def:r-linear**] *Let R be a ring and let M, N be R-modules. A homomorphism $\alpha : M \to N$ is called R-*linear *provided that $\alpha(rm) = r\alpha(m)$ for all $r \in R$ and $m \in M$.* $\mathrm{Hom}_R(M, N)$ *denotes the set of all R-linear homomorphisms.* $\mathrm{End}_R(M)$ *consists of all R-linear endomorphisms of M. $GL_R(M)$ consists of all R-linear isomorphisms of M. M and N are called* isomorphic *R-modules provided that there exists an R-linear isomorphism from M to N.*

Note that $\mathrm{End}_R(M)$ is a subring of $\mathrm{End}(M)$ and $GL_R(M)$ is a subgroup of $\mathrm{Aut}(M)$.

For every abelian group M there exists a unique $\mathbb{Z}$-module structure on M. Indeed $1m = m$, $2m = (1+1)m = m+m$ and so inductively

$$nm = \underbrace{m + \ldots + m}_{n \text{ times}}$$

for all $n \in \mathbb{Z}^+$ and $m \in M$. Also $0m = 0$ and $(-n)m = -(nm)$. So there exists at most one $\mathbb{Z}$-module structure on M. Conversely, it is easy to see that the above actually defines a $\mathbb{Z}$-module structure on M. Note also that $\mathrm{End}(M) = \mathrm{End}_{\mathbb{Z}}(M)$.

If $\mathbb{K}$ is a field, then a $\mathbb{K}$-module is called a *vector space* over $\mathbb{K}$ or a $\mathbb{K}$-*space*.

Lemma 2.1.3 [**hom and r-modules**] *Let R be a ring and M an abelian group. Then there exists a natural 1-1 correspondence between* $\mathrm{Hom}_{ring}(R, \mathrm{End}(M))$ *and the set of R-module structure on M.*

Proof: Let $\phi : R \to \mathrm{End}(M)$ be a ring homomorphism. Define

$$\cdot : R \times M \to M, (r, m) \to \phi(r)(m)$$

Then it is readily verified that $\cdot$ is an R-module structure on M.

Conversely, suppose that $\cdot : R \times M \to M$ is an R-module structure. For $r \in R$ define $\phi(r) : M \to M, m \to rm$. Then it is easy to verify that $\phi(r) \in \mathrm{End}(M)$ and $\phi : R \to \mathrm{End}(M), r \to \phi(r)$ is a ring homomorphism. □

The preceding lemma gives a second proof that there exists a unique $\mathbb{Z}$ structure on a given abelian group M. Indeed, there exists a unique ring homomorphism from $\mathbb{Z}$ to $\mathrm{End}(M)$.

If R is a ring and M an R-module, then $GL_R(M)$ acts on M via $\alpha m = \alpha(m)$ for all $\alpha \in GL_R(M)$ and $m \in M$.

Definition 2.1.4 [**def:rg-module**] *Let R be a ring, M an R-module and G a group. Then an RG-*module structure *on M is a binary operation*

$$\cdot : G \times M \to M$$

such that

(a) [**a**] $(g\tilde{g})m = g(\tilde{g}m)$

(b) [**b**] $1m = m$

(c) [**c**] $g(rm) = r(gm)$

(d) [**d**] $g(m + \tilde{m}) = gm + g\tilde{m}$

*for all $g, \tilde{g} \in G$, $m, \tilde{m} \in M$ and $r \in R$. An RG-*module *is an abelian group M together with an RG-module structure on M.*

Note that (a) and (b) in the preceding definition just say that G acts on M, while (c) and (d) say that the action is R-linear.

Let $\mathbb{K}$ be a field, V a $\mathbb{K}$ space with basis $\mathcal{V}$. Let G be a group acting on $\mathcal{V}$. Then

$$G \times V \to V, (g, \sum_{v \in \mathcal{V}} k_v v) \to \sum_{v \in \mathcal{V}} k_v gv$$

is a $\mathbb{K}G$-module structure on V. In particular, V can be viewed as a $\mathbb{K}\mathrm{Sym}(\mathcal{V})$-module such that $\alpha v = \alpha(v)$ for all $\alpha \in \mathrm{Sym}(\mathcal{V})$ and $v \in \mathcal{V}$.

Definition 2.1.5 [**def:rep**] *Let R be a field, M an R-module and G a group. A* representation *of G on M over R is a group homomorphism $\rho : G \to GL_R(M)$.*

Lemma 2.1.6 [**reps and modules**] *Let R be a ring, M an R-module and G a group. Then there exists a natural $1-1$-correspondence between representations of G on M over R and RG-module structures on M.*

Proof: If $\rho : G \to GL_R(M)$ is a homomorphism, then $G \times M \to M, (g, m) \to \rho(g)(m)$ is an R-module structure. Conversely if $G \times M \to M, (g, m) \to gm$ is an R-module structure, define $\rho(g) \in GL_R(M)$ by $\rho(g)(m) = gm$. Then $\rho : G \to GL_R(M)$ is a representation of G on M over R. □

Definition 2.1.7 [**direct sums**]

(a) [**a**] *Let $(A_i, i \in I)$ be a family of sets. Then*

$$\mathop{\textcircled{$\scriptstyle\Pi$}}_{I} A_i := \mathop{\textcircled{$\scriptstyle\Pi$}}_{i \in I} A_i := \{f : I \to \bigcup_{i \in I} A_i \mid f(i) \in A_i, \forall i \in I\}.$$

We denote $f \in \mathop{\textcircled{$\scriptstyle\Pi$}}_I A_i$ by $(f(i))_{i \in I}$. $\mathop{\textcircled{$\scriptstyle\Pi$}}_I A_i$ is called the direct product of $(A_i, i \in I)$.

(b) [**b**] *If $(A_i, i \in I)$ is a family of groups, then*

$$\bigoplus_{i \in I} A_i = \{(a_i)_{i \in I} \in \mathop{\textcircled{$\scriptstyle\Pi$}}_{I} A_i \mid |\{i \in I \mid a_i \neq 1\}| < \infty\}$$

$\bigoplus_I A_i$ is called the direct sum of $(A_i, i \in I)$.

We often will write $\mathop{\textcircled{$\scriptstyle\Pi$}}_I A_i$ for $\mathop{\textcircled{$\scriptstyle\Pi$}}_{i \in I} A_i$ and $(a_i)_I$ or (a_i) for $(a_i)_{i \in I}$.

If $(A_i, i \in I)$ is a family of groups, then both $\mathop{\textcircled{$\scriptstyle\Pi$}}_I A_i$ and $\bigoplus_I A_i$ are groups via $(a_i)(b_i) = (a_i b_i)$. Similarly if $(A_i, \mid i \in I)$ is a family of rings, then $\mathop{\textcircled{$\scriptstyle\Pi$}}_I A_i$ is a ring. If I is finite, then also $\bigoplus_I A_i$ is a ring, but if I is infinite, $\bigoplus_I A_i$ might not have a multiplicative identity.

If $(M_i, i \in I)$ is a family of R-modules then both $\mathop{\textcircled{$\scriptstyle\Pi$}}_I M_i$ and $\bigoplus_I M_i$ are R-modules via $r \cdot (m_i) = (rm_i)$.

Definition 2.1.8 [**def:group ring**] *R be a ring and G a group. Then the* group ring *RG for G over R is the ring defined as follows: $RG = \bigoplus_G R$ as an abelian group and multiplication*

$$(r_i)_i \cdot (s_j)_j = (\sum (r_i s_j \mid i,j \in G, ij = k, r_i \neq 0, s_j \neq 0)_k\,)_k.$$

We identify $r \in R$ with $(\delta_{1g} r)_g$ in RG and $h \in G$ with $(\delta_{gh})_g$ in RG. So we view R as a subring of RG and G as a subgroup of the R^*, the group of multiplicative units in R. With this identification, $(r_g) = \sum_{g\in G} r_g g$ and

$$(\sum_{i\in G} r_i i) \cdot (\sum_{j\in G} s_j j) = \sum_{i,j\in G} r_i s_j ij.$$

Note also the $rg = gr$ in RG. One might view RG as the largest ring generated by the subring R and multiplicative subgroup G subject two the relations $rg = gr$ for all $r \in R$, $g \in G$. More precisely we have:

Lemma 2.1.9 [**universal group ring**] *Let R and S be rings and G a group. Let $\alpha : R \to S$ be a ring homomorphism and $\beta : G \to R^*$ a multiplicative homomorphism. Suppose that $\alpha(r)\beta(g) = \beta(g)\alpha(r)$ for all $r \in R$ and $g \in G$. Then*

$$\gamma : RG \to S, \sum r_g g \to \sum \alpha(r_g)\beta(g)$$

is the unique ring homomorphism $\gamma : RG \to S$ with $\gamma(r) = \alpha(r)$ and $\gamma(g) = \beta(g)$ for all $r \in R$, $g \in G$.

Proof: Define $\gamma(\sum r_g g) = \sum \alpha(r_g)\beta(g)$. Then $\gamma(g) = \gamma(1g) = \alpha(1)\beta(g) = 1\beta(g) = \beta(g)$ for all $g \in G$. Similarly $\gamma(r) = \alpha(r)$. Since α is an additive homomorphism, γ is an additive homomorphism as well. To check that γ is a multiplicative homomorphism we compute

$$\begin{aligned}
\gamma\left(\sum_h r_h h) \cdot (\sum_i s_i i)\right) &= \gamma(\sum_{h,i} r_h s_i hi) \\
&= \sum_{h,i} \alpha(r_h s_i)\beta(hi) \\
&= \sum_{h,i} \alpha(r_h)\alpha(s_i)\beta(h)\beta(i) \\
&= \sum_{h,i} \alpha(r_h)\beta(h)\alpha(s_i)\beta(i) \\
&= (\sum_h \alpha(r_h)\beta(h)) \cdot (\sum_i \alpha(s_i)\beta(i)) \\
&= \gamma(\sum_h r_h h) \cdot \gamma(\sum_i s_i i)
\end{aligned}$$

Thus γ is a ring homomorphism.

Now suppose that $\gamma : RG \to S$ is a ring homomorphism with $\gamma(r) = \alpha(r)$ and $\gamma(g) = \beta(g)$. Then

$$\gamma(\sum r_g g) = \sum \gamma(r_g)\gamma(g) = \sum \alpha(r)\beta(g)$$

and so γ is unique. □

We reader should notice that with the introduction of the group ring RG the term "RG-module" now has been defined twice. Namely by 2.1.1 applied to the ring RG and also in 2.1.4. Luckily these two definitions are the same:

Suppose first that $RG \times M \to M, (d, m) \to dm$ is an RG–module structure in the sense of 2.1.1. Then M is an R-module via $(r, m) \to rm$. Moreover, since $rg = rg$ in RG one easily verifies that $G \times M \to M, (g, m) \to gm$ is an RG-module structure for G on M over R in the sense of 2.1.4.

Conversely, if M is an R-module and $G \times M \to M$ is an RG-module structure on M in the sense of 2.1.4, then

$$RG \times M \to M, (\sum_g r_g g, m) \to \sum_g r_g gm$$

is an RG-module structure in the sense of 2.1.1. Indeed, this can be verified by direct calculation. Alternatively, one can apply 2.1.9 to $\alpha : R \to \mathrm{End}(M), \alpha(r)(m) = rm$ and $\beta : G \to \mathrm{End}(M), \beta(g)(m) = gm$ to obtain a homomorphism $\gamma : RG \to \mathrm{End}(M)$. According to 2.1.6, γ gives an RG-module structure on M.

Definition 2.1.10 [**submodules**] *Let R be a ring and M an R-module.*

(a) [**a**] *An R-submodule of M is a subgroup N of M with $rn \in N$ for all $r \in R$, $n \in N$.*

(b) [**b**] *M is a* simple *R-module $M \neq 0$ and if 0 and M are the only R-submodules of M.*

Let R be a ring and $\mathcal{M}_n(R)$ the ring of $n \times n$ matrices over R. Identify R^n with the $n \times 1$-matrices over R. Then matrix multiplication $\mathcal{M}_n(R) \times R^n \to R^n(A, b) \to Ab$, is an $\mathcal{M}_n(R)$-module structure on R^n. Let $1 \leq m < n$ and let S be consist of all matrices of the form

$$\begin{pmatrix} A & B \\ 0 & D \end{pmatrix},$$

where A, B, D are $m \times m, m \times n - m$ and $(n - m) \times (n - m)$ matrices, respectively. Let $W = \{(r_1, \ldots, r_m, 0, \ldots, 0) \mid r_i \in R\}$.

Then S is a subring of $\mathcal{M}_n(R)$ and R^m is an S-submodule of R^n.

Definition 2.1.11 [**generation**] *Let R be a ring and M an R-module.*

(a) [**a**] *$N \leq_R M$ means that N is an R-submodule of M.*

(b) [**b**] *For $I \subseteq M$ define $\langle I\rangle_R = \bigcap\{N \mid I \subseteq N \leq_R M\}$.*

(c) [**c**] *For a family $(N_i, i \in I)$ of R-submodules in M, let*

$$\sum_I N_i = \{\sum_{i\in I} n_i \mid (n_i) \in \bigoplus_I N_i\}.$$

(d) [**d**] *We say that M is the* internal direct sum *of the family $(N_i, i \in I)$ of R-submodules in M if for each $m \in M$ there exists a unique $(n_i) \in \bigoplus_I N_i$ with $m = \sum_{i\in I} n_i$.*

(e) [**e**] *We say that a family $(N_i, i \in I)$ of R-submodules in M is* linearly independent *if $N_i \neq 0$ for all $i \in I$ and if $(n_i) \in \bigoplus_I N_i$ with $\sum_{i\in I} n_i = 0$ implies $n_i = 0$ for all $i \in I$.*

Note that $\langle I\rangle_R$ is an R-submodule of M containing I. So loosely speaking $\langle I\rangle_R$ is the smallest R-submodule of M containing I. Observe that $\sum_I N_i = \langle\bigcup_{i\in I} N_i\rangle_R$.

Lemma 2.1.12 [**easy independent**] *Let $(N_i, i \in I)$ be a family of R-submodules of the R-module M. Then $(N_i, i \in I)$ is linearly independent iff $(N_j, j \in J)$ is linearly independent for all finite subsets J of I.*

Proof: Obvious. □

Lemma 2.1.13 [**sums of submodules**] *Let M be an R-module $(M_i, i \in I)$ a family of non-zero R-submodules of M. Let $W = \sum_{i\in I} M_i$. Then the following are equivalent.*

(a) [**a**] *W is the internal direct sum of $(M_i, i \in I)$.*

(b) [**z**] *$(M_i, i \in I)$ is linearly independent.*

(c) [**b**] *The map $\phi : \bigoplus_I M_i \to W$, $(m_i) \to \sum_{\in I} m_i$ is an R-linear isomorphism.*

(d) [**c**] *For each $k \in I$, $M_k \cap \sum_{k\neq j\in I} M_j = 0$.*

Proof: ϕ is clearly R-linear and onto. The definitions imply that ϕ is a bijection if and only if W is the internal direct sum of the $(M_i, i \in I)$. Also $(M_i \mid i \in I)$ is linearly independent iff $\ker\phi = 0$. So (a), (b) and (c) are equivalent.

Suppose (c) holds and let $m \in M_k \cap \sum_{k\neq j\in I} M_j$. Then there exists $(m_j) \in \bigoplus_{k\neq j\in I} M_j$ with $\sum m_j = m$. Put $m_k = -m$. Then $\phi((m_i)) = 0$. Thus $m_i = 0$ for all i and so $m = -m_k = 0$. Thus (d) holds.

Suppose that (d) holds and let $(m_i) \in \bigoplus_{i\in I} M_i$ with $\phi((m_i)) = 0$. Let $k \in I$. Then

$$-m_k = \sum_{k\neq j\in I} m_j \in M_k \cap \sum_{k\neq j\in I} M_k = 0.$$

Thus $m_k = 0$, $(m_i) = 0$ and ϕ is one to one. So (c) holds. □

By the previous lemma, if $\sum M_i$ is the internal direct sum of $(M_i, i \in I)$, then $\sum M_i \cong \bigoplus_{i\in I} M_i$. In this case we usually identify $\sum_I M_i$ with $\bigoplus_I M_i$. In particular, we will write $\sum M_i = \bigoplus M_i$ to indicate that $\sum M_i$ is the internal direct sum of $(M_i, i \in I)$. We will also write just "direct sum" instead of "internal direct sum".

Definition 2.1.14 [**def:free module**] *, Let R a ring and I a set.*

(a) [**a**] *A function $f : I \to M$, where M is an R-module is called R-free and M is called a free R-module of rank I if for all R-modules N and all functions $g : I \to N$, there exists a unique R-linear map $h : M \to N$ with $g = h \circ f$.*

(b) [**b**] *Let M be an R-module and $b = (b_i) \in \textcircled{\Pi}_I M$. Then b is called a basis for M if for all $m \in M$ there exists a unique $(r_i) \in \bigoplus_I R$ with $m = \sum_{i\in I} r_i m_i$.*

Lemma 2.1.15 [**free module**] *Let I be a set, R an R-module and $b = (b_i) \in \textcircled{\Pi}_I M$. Then the following are equivalent.*

(a) [**a**] *The function $\alpha : \bigoplus_I R \to M, (r_i) \to \sum r_i m_i$ is an isomorphisms.*

(b) [**b**] *b is a basis for M.*

(c) [**c**] *$f : I \to M, i \to m_i$ is R-free.*

Proof: Clearly (a) and (b) are equivalent.

Suppose (b) holds. Let N be an R-module and $g : I \to N$ be a function. If $h : M \to M$ is linear with $g = h \circ f$, then $h(m_i) = g(i)$ and so for all $(r_i) \in \bigoplus_I R$,

$$(*) \qquad h(\sum r_i b_i) = \sum r_i g(i)$$

So such an h is unique. Conversely, since b is a basis for M, (*) defines an R-linear map $M \to N$ with $h(m_i) = g(i)$. Thus f is R-free and (c) holds.

Suppose now that (c) holds. Let $a_i = (\delta_{ij})_{j\in I} \in \bigoplus_I R$. Then $(a_i, i \in I)$ is a basis for $\bigoplus_I R$. Since (b) implies (c), $g : I \to a_i$ is a free map. Since a free map is unique up to isomorphism, we conclude that there exists an isomorphism $\alpha : \bigoplus_I R \to M$ with $\alpha(a_i) = m_i$. So (a) holds. □

Definition 2.1.16 [**def:semisimple**] *Let R be a ring and M an R-module.*

(a) [**a**] *We say that M is* semisimple *if M is the direct sum of simple R-submodules.*

(b) [**b**] *M is* indecomposable *if M is not the direct sum of two proper R-submodules.*

(c) [**c**] *Let N be an R-submodule of M. Then we say that N is a* direct summand *of M or that M splits over N as an R-module if there exists an R-submodule K of M with $M = N \oplus K$.*

Lemma 2.1.17 [**sum to direct sum**] *Let $\mathcal{S}$ a set of simple R-submodules of the R-module M. Also let N be a R-submodule of M and suppose that $M = \sum \mathcal{S}$.*

(a) [**a**] *There exists a subset $\mathcal{M}$ of $\mathcal{S}$ with $M = N \oplus \bigoplus \mathcal{M}$.*

(b) [**b**] *N is a direct summand of M.*

(c) [**c**] *$M = \bigoplus \mathcal{T}$ for some $\mathcal{T} \subseteq \mathcal{S}$.*

(d) [**d**] *$M/N \cong \bigoplus \mathcal{M}$ for some linearly independent subset $\mathcal{M}$ of $\mathcal{S}$.*

(e) [**e**] *M/N is semisimple.*

(f) [**f**] *$N \cong \bigoplus \mathcal{N}$ for some linearly independent subset $\mathcal{N}$ of $\mathcal{S}$.*

(g) [**g**] *N is semisimple.*

(h) [**h**] *If N is simple then $N \cong S$ for some $S \in \mathcal{S}$.*

Proof:

Let $\mathcal{B}$ consists of all the linearly independent subsets $\mathcal{T}$ of $\mathcal{S}$ with $N \cap \sum \mathcal{T} = 0$. Since $\emptyset \in \mathcal{B}$, $\mathcal{B} \neq \emptyset$. Order $\mathcal{B}$ by inclusion and let $\mathcal{C}$ be a chain in $\mathcal{B}$. Let $\mathcal{D} = \bigcup \mathcal{C}$. By 2.1.12 $\mathcal{D}$ is a linearly independent subset of $\mathcal{S}$. Let $m \in M \cap \sum \mathcal{D}$. Then there exists $D_i \in \mathcal{D}$, $1 \leq i \leq n$ and $d_i \in D_i$ with $m = \sum_{i=1}^{n} d_i$. For each D_i there exists $C_i \in \mathcal{C}$ with $D_i \in C_i$. As $\mathcal{C}$ is a chain we may assume that $C_1 \subseteq C_2 \subseteq \ldots C_n$. Then $D_i \in C_n$ for all $1 \leq i \leq n$ and so $m \in N \cap \sum C_n = 0$.

Therefore $N \cap \sum \mathcal{D} = 0$ and $\mathcal{D} \in \mathcal{B}$. So we can apply Zorn's lemma to obtain a maximal element $\mathcal{M}$ in $\mathcal{B}$. Put $W = \sum \mathcal{M}$. Suppose that $M \neq N + W$. Then there exists $S \in \mathcal{S}$ with $S \not\leq N + W$. Since S is simple, $(N + W) \cap S = 0$. So $(N + W) \cap (S + W) = W + ((N + W) \cap S) = W$ and so $N \cap (S + W) \leq N \cap W = 0$. Also $W \cap S = 0$ implies that $\sum \mathcal{S} \cup \{M\} = W \oplus S = \bigoplus \mathcal{M} \cup \{S\}$. Thus $\mathcal{M} \cup \{S\}$ is linearly independent and so $\mathcal{M} \cup \{S\} \in \mathcal{B}$, a contradiction to the maximality of $\mathcal{M}$.

Thus $M = N \oplus W$. So (a) and (b) hold.

(c) follows from (a) applied with $N = 0$. (d) follows from (a). (e) follows from (d). Note that $N \cong M/W$. So (f) follows from (d) applied to W in place of N. (g) follows from (f). Suppose N is simple. Then the set $\mathcal{N}$ from (e) only contains one element, say S. So $N \cong S$ and (h) is proved. □

Lemma 2.1.18 [**semisimple**] *Let R be a ring and M an R-module. Then the following are equivalent*

(a) [**c**] *M is a sum of simple R-modules.*

(b) [**a**] *Every R-submodule of M is semisimple.*

(c) [**b**] *M is a semisimple R-module.*

(d) [**d**] *Every non-zero R-submodule of M is a direct summand of M and contains a simple R-submodule.*

(e) [**e**] *If N is an R-submodule of M with $N \neq M$, then there exists simple R-submodule S with $S \nleq N$.*

Proof: By 2.1.17(g), (a) implies (b). Clearly (b) implies (c).

Suppose that (c) holds and let N be a non-zero R-submodule of M. By 2.1.17(b) N is a direct summand of M and by 2.1.17(g) N is semisimple. So since $N \neq 0$, N has a simple submodule.

Suppose now that (d) holds and let $N \neq M$ be an R-submodule of M. By (d) $M = N \oplus W$ for some R-submodule W. Since $N \neq M$, $W \neq 0$. Thus (d) implies W has a simple R-submodule S. Since $N \cap W = 0$, $S \nleq N$ and (e) holds.

Suppose (e) holds. Let N be the sum of all the simple R-submodules in M. If $N \neq M$, then (e) implies the existence of a simple R-submodule S of M with $S \nleq N$. But this contradicts the definition of N. So $N = M$ and (a) holds. □

Corollary 2.1.19 [**sections of semisimple**] *Let M semisimple R-module. Then all R-sections of M are semisimple.*

Proof: Let $A \leq B \leq M$ be R-submodule of M. 2.1.17(g) implies that B is semisimple. Then 2.1.17(e) applied to (A, B) in place of (N, M) shows that B/A is semisimple. □

2.2 Krull-Schmidt Theorem

Definition 2.2.1 [**def:local ring**] *A ring with a unique maximal left ideal is called a local ring.*

Lemma 2.2.2 [**inverses**] *Let G be a monoid and $a, r, l \in G$. If $la = ar = 1$, then a is unit and $r = l$ is the inverse of a.*

Proof: $l = l1 = l(ar) = (la)r = 1r = 1$. □

Lemma 2.2.3 [**splitting**] *Let $\alpha : A \to B$ be an R-linear map and D an R-submodule of A*

(a) [**a**] *If $\alpha\mid_D$ is 1-1 then $D \cap \ker \alpha = 0$.*

(b) [**b**] *If $\alpha\mid_D$ is onto then $A = D + \ker \alpha$.*

(c) [**c**] *If $\alpha\mid_D$ is an isomorphism, $A = D \oplus \ker\alpha$.*

Proof: (a) is obvious. For (b) let $a \in A$ and pick $d \in D$ with $\alpha(a) = \alpha(d)$. Then $a - d \in \ker\alpha$ and so $a = d + (a - d) \in D + \ker\alpha$. (c) follows from (a) and (b). □

Lemma 2.2.4 [**easy local ring**] *Let $R \neq 0$ be ring. R is local if and only if the set of non-units $I = R \setminus R^*$ is an ideal. In this case I is the unique maximal left ideal in R and the unique maximal right ideal in R.*

Proof: Suppose first that I is an ideal and let J be a right ideal in R. If $J \nleq I$ there exits $j \in J \setminus I$. Thus j is a unit and so $R = Rj \subseteq J$ and $R = J$. Thus I is the unique maximal left ideal in R. By symmetry I is also the unique maximal right ideal in R.

Suppose next that R has a unique maximal left ideal J. We will first show that J is also a right ideal in R. Let $r \in R$. Then Jr is a left ideal in R. So either $Jr \subseteq J$ or $Jr = R$. Suppose that $Jr = R$. Let $\alpha : R \to R, t \to tr$ and note that α is R-linear if we view R as an R-module by left multiplication. In particular, $\ker\alpha$ is a left ideal in R. Also $\alpha\mid_J$ is onto and so by 2.2.3(b), $R = J + \ker\alpha$. Thus $\ker\alpha \leq J$, $R = \ker\alpha$ and $R = Rr = 0$, a contradiction. Thus $Jr \subseteq J$ and J is a right ideal.

Let $r \in R \setminus J$. Then $Rr \nleq J$ and so $Rr = R$ and there exists $s \in R$ with $sr = 1$. If $s \in J$, then, since J is a right ideal, also $1 = sr \in J$, a contradiction. Thus $s \notin J$ and so $ks = 1$ for some $k \in R$. Thus by 2.2.2, $k = r$ is the inverse of s. Thus $r \notin I$.

If $i \notin I$, then $Ri = R$ and so $i \notin J$. Thus $I = J$ is an ideal in R. □

Lemma 2.2.5 [**sum invertible**] *Let R be a local ring and $r_1, \ldots r_n \in R$ such that $r_1 + r_2 + \ldots + r_n$ is a unit. Then r_i is a unit for some $1 \leq i \leq n$.*

Proof: By 2.2.4 the set I of non-units is an ideal in R. If $r_i \in I$ for all $1 \leq i \leq n$, then also $r_1 + r_2 + \ldots + r_n \in I$, a contradiction. □

Lemma 2.2.6 [**composition invertible**] *Let $\alpha : A \to B$ and $\beta : B \to C$ be R-linear maps such that $\beta \circ \alpha$ is invertible.*

(a) [**a**] *$\alpha : A \to \operatorname{Im}\alpha$ is an isomorphism.*

(b) [**b**] *$\beta\mid_{\operatorname{Im} A}$ is an isomorphism.*

(c) [**c**] *$B = \operatorname{Im}\alpha \oplus \ker\beta$.*

(d) [**d**] *If, in addition, B is indecomposable and $A \neq 0$, then both α and β are isomorphisms.*

Proof: (a) and (b) are readily verified.

(c) follows from (b) and 2.2.3(c).

(d) Suppose now that B is indecomposable. Then either $\operatorname{Im}\alpha = 0$ or $\operatorname{Im}\alpha = B$. In the first case (a) gives $A = 0$. In the second case (a) and (b) give that both α and β are isomorphisms. □

Definition 2.2.7 [**def:acc**] *Let M be an R-module.*

(a) [**a**] *We say that M fulfills the ascending chain condition (ACC) if each ascending chain*

$$M_1 \leq M_2 \leq \ldots \leq M_n \leq M_{n+1} \leq \ldots$$

terminates, that is there exists $m \in \mathbb{Z}^+$ with $M_k = M_m$ for all $k \geq m$.

(b) [**b**] *We say that M fulfills the descending chain condition (DCC) if each descending chain*

$$M_1 \geq M_2 \geq \ldots \geq M_n \geq M_{n+1} \geq \ldots$$

terminates.

Lemma 2.2.8 [**char dcc**] *Let M be an R-module. Then the following are equivalent.*

(a) [**a**] *M fulfills DCC.*

(b) [**b**] *Every nonempty set of R-submodules of M has a minimal element.*

(c) [**c**] *If $\mathcal{M}$ is a set of R-submodules, then there exists a finite subset $\mathcal{N}$ of $\mathcal{M}$ with $\bigcap \mathcal{M} = \bigcap \mathcal{N}$.*

Proof: (a)$\Longrightarrow$ (b): Let $\mathcal{M}$ be a non empty set of R-submodules of M and suppose $\mathcal{M}$ has no minimal element. Let $M_1 \in \mathcal{M}$ and inductively assume we already found $M_1, M_2, \ldots, M_k \in \mathcal{M}$ with

$$M_1 > M_2 > \ldots > M_k$$

Since M_k is not a minimal element, there exists $M_{k+1} \in \mathcal{M}$ with $M_k > M_{k+1}$. Hence $\{M_k \mid k \in \mathbb{Z}^+\}$ is a non-terminating descending chain of R-submodules, a contradiction to *DCC*.

(b)$\Longrightarrow$ (c): Let $\mathcal{M}$ be a set of R-submodules and let

$$\mathcal{F} = \{\bigcap \mathcal{N} \mid \mathcal{N} \text{ finite subset of } \mathcal{M}\}.$$

By (b), $\mathcal{F}$ has a minimal element W. Then $W = \bigcap \mathcal{N}$ for some finite $\mathcal{N} \subseteq \mathcal{M}$. Let $N \in \mathcal{M}$. Then $W \cap N = \bigcap(\mathcal{N} \cup \{N\}) \in \mathcal{F}$ and so by minimality of W, $W = W \cap N \leq N$. Thus $W = \bigcap \mathcal{M}$ and (b) holds.

(c)$\Longrightarrow$ (a): Let $M_1 \geq M_2 \geq M_3 \ldots$ be an descending chain of R-submodules of M. By (c) applied to $\mathcal{M} = \{M_i \mid 1 \leq i < \infty\}$ there exists a finite subset $\mathcal{N}$ of $\mathcal{M}$ with $\bigcap \mathcal{N} = \bigcap \mathcal{M}$. Since $\mathcal{N}$ is finite and total ordered $\bigcap \mathcal{N} = M_i$, where M_i is the minimal element of $\mathcal{N}$. If follows that $M_i \leq M_j$ for all j and so $M_i = M_j$ for all $j \geq i$. □

Lemma 2.2.9 (Fitting) [**fitting**] *Let M be an R-module and $f \in \mathrm{End}_R(M)$.*

(a) [**a**] *If f is onto and M fulfills ACC, then f is an isomorphism.*

(b) [**b**] *If M fulfills DCC, there exists $n \in \mathbb{Z}^+$ with $\mathrm{Im}\, f^n = \mathrm{Im}\, f^{n+1}$.*

(c) [**c**] *If M fulfills ACC and DCC then there exists $n \in \mathbb{Z}^+$ such that $M = \ker f^n \oplus \mathrm{Im}\, f^n$.*

(d) [**d**] *If M is indecomposable and fulfills ACC and DCC, then f is either invertible or nilpotent.*

Proof: (a) Let $n \in \mathbb{Z}^+$ and $a \in M$. Then $f^n(a) \in \ker f$ if and only if $a \in \ker f^{n+1}$. Since f^n is onto, this implies $f^n(\ker f^{n+1}) = \ker f$ and $\ker f^n \leq \ker f^{n+1}$. The isomorphism theorem applied to the R-linear map $f^n : \ker f^{n+1} \to \ker f$ gives

$$(*) \qquad \ker f^{n+1}/\ker f^n \cong \ker f.$$

Now $0 \leq \ker f \leq \ker f^2 \leq \ldots$ is an ascending chain of R modules and so by ACC there exists n with $\ker f^{n+1} = \ker f^n$. Thus (*) implies that $\ker f = 0$ and so f is one to one.

(b) Just observe that $M \geq \mathrm{Im}\, f \geq \mathrm{Im}\, f^2 \geq \mathrm{Im}\, f^3 \geq \ldots$, is an descending chain of R-submodules in M.

(c) Choose n as in (b). Then $f : \mathrm{Im}\, f^n \to \mathrm{Im}\, f^n$ is onto. Hence also $f^n : \mathrm{Im}\, f^n \to \mathrm{Im}\, f^n$ is onto. By (b) we conclude that $f^n : \mathrm{Im}\, f^n \to \mathrm{Im}\, f^n$ is an isomorphism. So we can apply 2.2.3(c) to $f^n : M \to \mathrm{Im}\, f^n$ in place of α and $\mathrm{Im}\, f^n$ in place of D. Therefore $M = \mathrm{Im}\, f^n \oplus \ker f^n$.

(d) Since M is indecomposable, (c) implies that either $\ker f^n = M$ and $\mathrm{Im}\, f^n = 0$, or $\ker f^n = 0$ and $\mathrm{Im}\, f^n = M$. In the first case $f^n = 0$ and so f is nilpotent. In the second case f^n is an isomorphism and so invertible. But then also f is invertible. □

Lemma 2.2.10 [**local and indecomposable**] *Let M be an R-module.*

(a) [**a**] *If $\mathrm{End}_R(M)$ is a local ring, M is indecomposable.*

(b) [**b**] *If M fulfills ACC and DCC, then M is indecomposable iff $\mathrm{End}_R(M)$ is a local ring.*

Proof: Let $A = \mathrm{End}_R(M)$.

(a) Suppose for a contradiction that A is a local ring and M is decomposable. Let $M = X \oplus Y$ for some proper R-submodules X and Y. Let $\pi_X : M \to M$ be the projection map defined by, $\pi_X(x+y) = x$ for all $x \in X$ and $y \in Y$. Similarly define π_Y. Then π_X and π_Y are in A and $\pi_X + \pi_Y = \mathrm{id}_M$. Since $X = \ker \pi_Y$, π_Y is not invertible. Similarly π_X is not invertible. But this contradicts 2.2.5

(b) By (a) it remains to show that if M is indecomposable then A is a local ring. So suppose M is indecomposable and let I be a maximal left ideal in A. Let $f \in A \setminus I$. We will show that f is invertible. Since I is a maximal left ideal in A, $A = Af + I$. Hence $1 = af + i$ for some $a \in A$, $i \in I$. Since $Ai \leq I$, i is not invertible and so by 2.2.9(d), $i^n = 0$ for some $n \in \mathbb{Z}^+$. Thus $1 - i$ has an inverse j, namely $j = \sum_{k=0}^{n-1} i^k$. From $af = 1 - i$ we conclude that $jaf = 1$. Thus $Af = A$, f is not contained in any proper left ideal in A and so I is the unique maximal ideal in A. Hence A is a local ring and (b) holds.. □

Proposition 2.2.11 [**exchange lemma**] *Let M be an R-module, $\mathcal{B}$ a finite set of indecomposable R-submodules of M with $M = \bigoplus \mathcal{B}$. If A is a direct summand of M such that* $\mathrm{End}_R(A)$ *is a local ring, then there exists $B \in \mathcal{B}$ such that*

$$M = A \oplus \bigoplus \mathcal{B}^*, \quad \textit{where } \mathcal{B}^* = \mathcal{B} \setminus \{B\}.$$

In particular, $A \cong M/\bigoplus \mathcal{B}^* \cong B$ and $M/A \cong \bigoplus \mathcal{B}^* \cong M/B$ as R-modules.

Proof: Let X be an R-submodule of M with $M = A \oplus X$. Let $\iota_A : A \to M, a \to a$ and $\pi_A : M \to A, a + x \to a$ be the associate inclusion and projection maps. For $D \in \mathcal{B}$, let $\iota_D : D \to M, d \to d$ and $\pi_D : M \to D, \sum_{B \in \mathcal{B}} m_B \to m_D$ be the inclusion and projection map associated to the direct sum decomposition $M = \bigoplus \mathcal{B}$. Then $\pi_A \iota_A = \mathrm{id}_A$ and $\sum_{B \in \mathcal{B}} \iota_B \pi_B = \mathrm{id}_M$. Hence

$$\sum_{B \in \mathcal{B}} \pi_A \iota_B \pi_B \iota_A = \pi_A \cdot (\sum_{B \in \mathcal{B}} \iota_B \pi_B) \cdot \iota_A = \pi_A \iota_A = \mathrm{id}_A$$

By assumption, $\mathrm{End}_R(A)$ is a local ring and so 2.2.5 implies that that there exists $B \in \mathcal{B}$ such that $\pi_A \iota_B \pi_B \iota_A$ is invertible. As B is indecomposable 2.2.6 gives that $\pi_B \iota_A$ is invertible. As $\pi_B \iota_A = \pi_B \mid_A$ we conclude from 2.2.3 that $M = A \oplus \ker \pi_B$. Now $\ker \mathcal{B} = \bigoplus \mathcal{B}^*$ and so the first statement of the lemma is proved. The remaining statements follow easily from the first. □

Definition 2.2.12 [**def:isomorphic sets of modules**] *Let $\mathcal{A}$ and $\mathcal{B}$ be sets of $\mathcal{R}$ modules. We say that $\mathcal{A}$ and $\mathcal{B}$ are* isomorphic *as R-modules and write $\mathcal{A} \cong \mathcal{B}$ or $\mathcal{A} \cong_R \mathcal{B}$ if there exists a bijection $\alpha : \mathcal{A} \to \mathcal{B}, A \to A'$ with $A \cong_R A'$ for all $A \in \mathcal{A}$.*

Theorem 2.2.13 (Krull-Schmidt) [**krull-schmidt**] *Let $\mathcal{A}$ and $\mathcal{B}$ be sets of indecomposable R-modules. Suppose that $\mathcal{B}$ is finite and that for each $A \in \mathcal{A}$,* $\mathrm{End}_R(A)$ *is a local ring. If $\bigoplus \mathcal{A} \cong_R \bigoplus \mathcal{B}$ then $\mathcal{A} \cong_R \mathcal{B}$.*

Proof: Note that the theorem holds if $\mathcal{B} = \emptyset$. We proceed by induction on $|\mathcal{B}|$. We may assume that $M := \bigoplus \mathcal{A} = \bigoplus \mathcal{B}$. Let $A \in \mathcal{A}$. Then by 2.2.11 there exists $B \in \mathcal{B}$ such that $A \cong B$ and $M/A \cong M/B$. Let $\mathcal{A}^* = \mathcal{A} \setminus \{A\}$ and $\mathcal{B}^* = \mathcal{B} \setminus \{B\}$. Then $M/A \cong \bigoplus \mathcal{A}^*$ and $M/B \cong \bigoplus \mathcal{B}^*$. Thus $\bigoplus \mathcal{A}^* \cong \bigoplus \mathcal{B}^*$. By induction $\mathcal{A}^* \cong \mathcal{B}^*$ and since $A \cong B$, also $\mathcal{A} \cong \mathcal{B}$. □

2.3 Maschke's Theorem

Lemma 2.3.1 [**semisimple is local**] *Let R be a ring and M an R-module. Then M is semisimple if and only if Rm is semisimple for all $m \in M$.*

Proof: If M is semisimple, then by 2.1.18 also the submodule Rm is semisimple. So suppose that Rm is semisimple for all $m \in M$. Let $m \in M$. Then Rm is a sum of simple modules and so m is contained in the sum W of all the simple R-submodules of M. Thus $m \in W$, $W = M$ and W is semisimple.

Theorem 2.3.2 (Mascke) [**maschke**] *Let $\mathbb{K}$ be a field and G a finite group with such that* $\operatorname{char} \mathbb{K}$ *does not divide $|G|$. Then every $\mathbb{K}G$-module is semisimple.*

Proof: Let V be a $\mathbb{K}G$ module. By 2.1.18 we may assume that $V = \mathbb{K}Gv$ for some $v \in V$. In particular, V is finite dimensional over $\mathbb{K}$. Let W be a $\mathbb{K}G$ submodule of V. We will show that W is a direct summand of V as a $\mathbb{K}G$ module. Note that there exists a $\mathbb{K}$- subspace Z of V with $V = W \oplus Z$. Define $\pi : V \to W$ by $\pi(w + z) = w$ for all $w \in W, z \in Z$. Since $\operatorname{char} \mathbb{K}$ does not divide $|G|$, $\frac{1}{|G|}$ is a well defined element of $\mathbb{K}$ and we can define

$$\rho : V \to V, v \to \frac{1}{|G|} \sum_{g \in G} g^{-1}\pi(gv)$$

Since $\pi(gv) \in W$ and W is a $\mathbb{K}G$-submodule, $g^{-1}\pi(gv) \in W$ and so $\rho(V) \leq W$. For $w \in W$, $gw \in W$ and so $\pi(gw) = gw$, $g^{-1}\pi(gw) = w$ and $\rho(w) = w$. Let $Y = \ker \rho$. Since $\rho \mid_W = \mathrm{id}_W$, $Y \cap W = 0$. Also if $v \in V$, then $\rho(v - \rho(v)) = \rho(v) - \rho(v) = 0$, $v - \rho(v) \in Y$ and so $v = \rho(v) + (v - \rho(v)) \in W + Y$. Thus $V = W \oplus Y$.

We claim that ρ is $\mathbb{K}G$-linear. ρ is a sum of compositions of $\mathbb{K}$-linear maps and so $\mathbb{K}$-linear. Let $h \in G$ and $v \in V$. Then

$$\begin{aligned}
\rho(hv) &= \sum_{g\in G} g^{-1}\pi(ghv) \\
&= \sum_{g\in G} h(gh)^{-1}\pi(ghv) \\
&= h\sum_{g\in G}(gh)^{-1}\pi((gh)v \\
&= h\sum_{g\in G} g^{-1}\pi(gv) \\
&= h\rho(v)
\end{aligned}$$

Thus ρ is indeed $\mathbb{K}G$-linear and so $Y = \ker \rho$ is a $\mathbb{K}G$-submodule of V. Hence any submodule of V is a direct summand of V. Suppose $W \neq 0$. Since W is finite dimensional, we can choose a $\mathbb{K}G$ submodule U in W of minimal dimension. Then U is simple. 2.1.18 now implies that V is semisimple. □

As an example let $G = \langle g \rangle$ be a cyclic group of order 2 and $\mathbb{K}$ any field. Let $M = \mathbb{K}^2$ and define an action of G on M by $g(a,b) = (b,a)$. Then M is a $\mathbb{K}G$-module. Let $M_+ = \{(a,a) \mid a \in \mathbb{K}\}$ and $M_- = \{(a,-a) \mid a \in \mathbb{K}\}$. Then M_+ and M_- are $\mathbb{K}G$-submodules of M. Since they are 1-dimensional over $\mathbb{K}$ both M_+ and M_- are simple $\mathbb{K}G$-modules.

If $\operatorname{char}\mathbb{K} \neq 2$, then $M_+ \neq M_-$ and so $M = M_+ \oplus M_-$. So M is a semisimple $\mathbb{K}G$-module.

Suppose now that $\operatorname{char}\mathbb{K} = 2$ and let U be a 1-dimensional $\mathbb{K}G$-submodule in M. Let $0 \neq u \in U$. Then $gu = ku$ for some $k \in \mathbb{K}$. Since $g^2 = 1$ we get $u = k^2u$ and so $(k-1)^2 = k^2 - 1 = 0$. Thus $k = 1$. Hence $gu = u$ and so $u \in M_+$. It follows that M_+ is the unique simple $\mathbb{K}G$ submodule of M and so M is not semisimple. This shows that the assumption $\operatorname{char}\mathbb{K} \nmid |G|$ in Maschke's theorem is necessary.

For a second example let $\mathbb{K}$ be a field of characteristic p. Define $\phi \in GL_{\mathbb{K}}(\mathbb{K}^2)$ by $\phi(a,b) = (a+b,b)$. Then $\phi^n(a+nb,b)$ and so $\phi^p = 1$ Thus $G = \langle\phi\rangle$ has order p if $p \neq 0$ and G has infinite order if $p = 0$. Observe that $(\phi - 1)^2 = 0$. Let W be a simple $\mathbb{K}G$-submodule in $\mathbb{K}^2$. Since also $[W,\phi]$ is a $\mathbb{K}G$ submodule and $[W,\phi,\phi] = 0$, the simplicity implies that $[W,\phi] = 0$. Hence $W = \{(a,0) \mid a \in \mathbb{K}\}$ and so $\mathbb{K}^2$ has a unique simple $\mathbb{K}G$-submodule. Thus $\mathbb{K}^2$ is not semisimple. For $p = 0$ this shows 2.3.2 is false for infinite groups. □

2.4 Jacobson Radical

Definition 2.4.1 [**def:arm**] *Let M be an R-module, $S \subseteq R$ and $N \subseteq M$.*

(a) [**a**] *SN is the additive subgroup of M generated by $\{sn \mid s \in S, n \in N\}$*

(b) [**b**] $\mathrm{A}_S(N) := \{s \in S \mid sN = 0\}$. *$\mathrm{A}_S(N)$ is called the annihilator of N in S.*

(c) [**c**] $\mathrm{A}_N(S) = \{n \in N \mid Sn = 0\}$

(d) [**d**] *M is called a* faithful *R-module if* $\mathrm{A}_R(M) = 0$.

(e) [**e**] *M is* cyclic *R-module if $M = Rm$ for some $m \in M$.*

(f) [**f**] *M is called a* finitely generated *R-module if $M = RN$ for a finite subset N of M.*

(g) [**g**] *N is called S invariant if $sn \in N$ for all $s \in S$, $n \in N$.*

Lemma 2.4.2 [**generating set**] *Let M be an R-module and $N \subseteq M$ with $M = RN$. Then*

$$\phi : \bigoplus_{n \in N} R/\,\mathrm{A}_R(n) \to M, (r_n + \mathrm{A}_R(n)) \to \sum_{n \in N} r_n \cdot n$$

is a well defined onto R-linear map. If $|N| = 1$, then ϕ is a isomorphism.

Proof: Readily verified. □

Let R be a ring. We view R as a R-module via left multiplication. Note that a submodule of R in R is an ideal. If I is an ideal in R, then also R/I is an R-module. For $a \in R$ let $\overline{a} = a + I \in A/I$. Then

$$\mathrm{A}_R(\overline{1}) = \{r \in R \mid r\overline{1} = 0\} = \{r \in R \mid \overline{r} = 0\} = I.$$

Definition 2.4.3 [**def:closed**] *Let M be an R-module,$N \subseteq M$ and $I \subseteq R$.*

(a) [**a**] *N is called* closed *in M if $N = \mathrm{A}_M(J)$ for some $I \subseteq R$.*

(b) [**b**] *$N^\circ := \mathrm{A}_M(\mathrm{A}_R(N))$ is called the closure of N in M.*

(c) [**c**] *I is called closed in R with respect to M if $I = \mathrm{A}_R(U)$ for some $U \subseteq M$.*

(d) [**d**] *$I^\circ := \mathrm{A}_R(\mathrm{A}_M(I))$ is called that closure of I in R with respect to M.*

Lemma 2.4.4 [**arm**] *Let M be an R-module, $I \subseteq R$ and $N \subseteq M$.*

(a) [**z**] *0 and M are closed in M.*

(b) [**y**] *R is closed and $0^\circ = \mathrm{A}_R(M)$.*

(c) [**a**] *$\mathrm{A}_R(N)$ is a left ideal in R.*

(d) [**b**] *If N is R-invariant, then $\mathrm{A}_R(N)$ is an ideal in R.*

(e) [**c**] *$\mathrm{A}_M(I)$ is an a $\mathrm{End}_R(M)$-submodule of M.*

(f) [**d**] *If I is right ideal, then $\mathrm{A}_M(I)$ is an R-submodule of M*

(g) [**e**] $\mathrm{A}_R(N) = \mathrm{A}_R(N^\circ)$ *and* $N^{\circ\circ} = N^\circ$.

(h) [**f**] $\mathrm{A}_M(I) = \mathrm{A}_M(I^\circ)$ *and* $I^{\circ\circ} = I^\circ$.

(i) [**g**] N° *is a smallest closed subset of* M *containing* N.

(j) [**h**] I° *is the smallest closed subset of* R *containing* I.

(k) [**i**] $\mathrm{A}_R(RN)$ *is the largest right ideal of* R *contained in* $\mathrm{A}_R(N)$.

(l) [**j**] M *is faithful module for* $R/\mathrm{A}_R(M)$ *via* $(r + \mathrm{A}_R(M)) \cdot m = rm$.

Proof: Let $s, \tilde{s} \in \mathrm{A}_R(N)$, $m, \tilde{m} \in \mathrm{A}_M(I)$, $r \in R$ and $a \in End_R(M)$.

(a) $0 = \mathrm{A}_M(1)$ and $M = \mathrm{A}_M(0)$.

(b) $R = \mathrm{A}_R(0)$ and since $\mathrm{A}_M(0) = M$, $0^\circ = \mathrm{A}_R(M)$.

(c) Since $(s \pm \tilde{s})N \leq sN + \tilde{s}N = 0$, $\mathrm{A}_R(N)$ is closed under addition and additive inverses. Moreover, $(rs)N = r(sN) = r0 = 0$ and so $\mathrm{A}_R(N)$ is a left ideal.

(d) If N is R invariant we have $(sr)N = s(rN) \subseteq aN = 0$ and so (d) holds.

(e) $I(m \pm \tilde{m}) \subseteq Im + I\tilde{m} = 0$. Also $0 \in \mathrm{A}_M(I)$. Moreover, $I(am) = a(Im) = 0$ and so (e) holds.

(f) $I(rm) = (Ir)m \subseteq Im = 0$.

(g) Put $J = \mathrm{A}_R(N)$. Then $N^\circ = \mathrm{A}_M(J)$, $N \subseteq N^\circ$ and $J \subseteq \mathrm{A}_R(N^\circ)$. Thus

$$J \subseteq \mathrm{A}_R(N^\circ) \subseteq \mathrm{A}_R(N) = J$$

Thus $J = \mathrm{A}_R(N^\circ) = \mathrm{A}_R(N)$. Hence $N^{\circ\circ} = \mathrm{A}_M(J) = N^\circ$.

(h) Let $D = \mathrm{A}_M(I)$. Then $I^\circ = \mathrm{A}_R(D)$, $I \subseteq I^\circ$ and $D \subseteq \mathrm{A}_M(I^\circ)$. Thus

$$D \subseteq \mathrm{A}_M(I^\circ) \subseteq \mathrm{A}_M(I) = D$$

Hence $D = \mathrm{A}_M(I^\circ) = \mathrm{A}_M(I)$ and so $I^{\circ\circ} = \mathrm{A}_R(D) = I^\circ$.

(i) By (g) $N^\circ = N^{\circ\circ}$ and so N° is closed. If $N \subseteq \mathrm{A}_M(J)$ for some $J \subseteq R$, then $J \subseteq \mathrm{A}_R(N)$ and so $N^\circ = \mathrm{A}_M(\mathrm{A}_R(N)) \subseteq \mathrm{A}_M(J))$.

(j) By (h) $I^\circ = I^{\circ\circ}$ and so I° is closed. If $I \subseteq \mathrm{A}_R(D)$ for some $D \subseteq M$, then $D \subseteq \mathrm{A}_M(I)$ and so $I^\circ = \mathrm{A}_R(\mathrm{A}_M(I)) \subseteq \mathrm{A}_R(D)$.

(k) Since RN is an R-submodule, (d) implies that $\mathrm{A}_R(RN)$ is an ideal in R. Now let J be a right ideal of R with $J \subseteq \mathrm{A}_R(N)$. Then $N \subseteq \mathrm{A}_R(J)$. By (f) $\mathrm{A}_M(J)$ is an R-submodule of M and so $RN \subseteq \mathrm{A}_M(J)$. Thus $J \subseteq \mathrm{A}_R(RN)$

(l) Readily verified. □

Corollary 2.4.5 [**closed correspondence**] *Let* M *be an* R*-module. Then*

(a) [**a**] *The map* $N \to \mathrm{A}_R(N)$ *is a bijection between the closed subsets of* M *and the closed subsets of* R.

(b) [**b**] *Its inverse of the map in (a) is $I \to \mathrm{A}_M(I)$.*

(c) [**c**] *If N is closed in M, then N is an R-submodule iff $\mathrm{A}_R(N)$ is an ideal.*

(d) [**d**] *If I is closed in R then I is an ideal iff $\mathrm{A}_M(I)$ is an R-submodule of M.*

Proof: Let $N \subseteq M$ and $I \subseteq R$ be closed. By 2.4.4 i $N = N^\circ = \mathrm{A}_M(\mathrm{A}_R(N))$ and $I = I^\circ = \mathrm{A}_R(\mathrm{A}_M(I))$. So the maps given in the corollary are inverse to each other. If N is an R-submodule, $\mathrm{A}_R(N)$ is an ideal. If I is an ideal, when $\mathrm{A}_M(I)$ is an R-submodule. □

Lemma 2.4.6 [**simple and maximal ideal**] *Let M be an R-module and $0 \neq m \in M$.*

(a) [**a**] *If M is simple, then $M = Rm$.*

(b) [**b**] *If $M = Rm$, then $M \cong R/\mathrm{A}_R(m)$. Moreover, M is simple if and only if $\mathrm{A}_R(m)$ is a maximal left ideal in R.*

Proof: (a) Just observe that Rm is a non-zero R-submodule of M.

(b) By 2.4.2, $M \cong R/\mathrm{A}_R(m)$. The second statement holds since the submodule of $R/\mathrm{A}_R(M)$ are exactly the $J/\mathrm{A}_R(m)$ with J a left ideal of R containing $\mathrm{A}_r(m)$. □

Theorem 2.4.7 [**jacobson radical**] *Let R be a ring, $\mathcal{I}$ the set of maximal left ideal in R and $\mathcal{S}$ the class of simple R-modules. Then*

$$\bigcap_{I \in \mathcal{I}} I = \bigcap_{S \in \mathcal{S}} \mathrm{A}_R(S).$$

Proof: For $S \in \mathcal{S}$ let $\mathcal{I}(S) = \{\mathrm{A}_R(s) \mid 0 \neq s \in S\}$. Then by 2.4.6 $\mathcal{I}(S) \subseteq \mathcal{I}$. Also $\mathrm{A}_R(M) = \bigcap \mathcal{I}(S)$.

Let $I \in \mathcal{I}$. Then $R/I \in \mathcal{S}$ and $\mathrm{A}_R(R/I) \leq \mathrm{A}_R(1 + I/I) = I$. Thus

$$\bigcap_{I \in \mathcal{I}} I \supseteq \bigcap_{I \in \mathcal{I}} \mathrm{A}_R(R/I) \supseteq \bigcap_{S \in \mathcal{S}} \mathrm{A}_R(S) = \bigcap_{S \in \mathcal{S}} \bigcap_{I \in \mathcal{I}(S)} I \supseteq \bigcap_{I \in \mathcal{I}} I.$$

Thus equality holds everywhere and the lemma is proved. (We remark that instead of defining $\mathcal{S}$ to be the class of all simple R-modules we really should have define $\mathcal{S}$ to be the set of isomorphism classes of simple R-modules, since otherwise some of the above intersection would not be defined. Since $\mathrm{A}_R(S)$ only depends on the isomorphism class of S some minor modification of the above will give a formally correct proof.) □

Definition 2.4.8 [**def:jacobson radical**] *Let R be a ring, then $J(R)$ is the intersection of the maximal left ideals in R. $J(R)$ is called the* Jacobson radical *of R. If M is an R-module, let $J_M(R)$ be the intersection of the maximal R-submodules of M.*

Note that $J_R(R) = R$.

Lemma 2.4.9 [**jacobson for semisimple**] *Suppose that M is a semisimple R-module, then $J_M(R) = 0$.*

Proof: Let $\mathcal{S}$ be a set of simple R-submodules with $M = \bigoplus \mathcal{S}$. For $S \in \mathcal{S}$ let $S^* = \sum\{S \neq T \in \mathcal{S}\}$. Then $M/S^* \cong S$ and so S^* is a maximal R-submodule of M. Clearly $\bigcap_{S\in\mathcal{S}} S^* = 0$ and so $J_M(R) = 0$. □

Lemma 2.4.10 [**semisimple for jacobson**] *Let M and R-module and $\mathcal{M}$ a finite set of maximal R-submodules of M with $\bigcap \mathcal{M} = 0$. Choose $\mathcal{N} \subseteq \mathcal{M}$ with $\bigcap \mathcal{N} = 0$. Then the map*

$$\phi : M \to \bigoplus_{N\in\mathcal{M}} M/N, m \to (m+N)_N$$

is an R-isomorphism. In particular, M is semisimple.

Proof: Clearly ϕ is R-linear. Let $m \in \ker \phi$. Then $m + N = 0_{M/N} = N$ and so $m \in N$ for all $N \in \mathcal{N}$. Thus $m \in \bigcap \mathcal{N} = 0$ and ϕ is $1-1$.Let $L \in \mathcal{N}$. Let $L^* = \bigcap\{L \neq T \in \mathcal{N}\}$. The b minimality of $\mathcal{N}$, $L^* \neq 0$. Since ϕ is $1-1$, also $\phi(L^*) \neq 0$. Let $W = \bigoplus_{N\in\mathcal{N}} M/N$ and let W_L be the image of M/L in W. Then $W_L \cong M/L$ is simple. Note that $0 \neq \phi(L^*) \leq W_L$ and the simplicity of W_L implies $W_L = \phi(L^*) \leq \operatorname{Im}\phi$. Thus $W = \sum_{N\in\mathcal{N}} W_N \leq \operatorname{Im}\phi$ and so ϕ is onto. □

Corollary 2.4.11 [**semisimple = jacobson**] *Let M be an R-module with DCC. Then M is semisimple iff $J_M(R) = 0$.*

Proof: If M is semisimple, $J_M(R) = 0$ by 2.4.9. Suppose now that $J_M(R) = 0$ and let $\mathcal{S}$ be the set of maximal R-submodules of M. Then $\bigcap \mathcal{S} = J_M(R) = 0$. Since M fulfills DCC, 2.2.8 implies that there exists a finite subset $\mathcal{M}$ of $\mathcal{S}$ with $\bigcap \mathcal{M} = \bigcap \mathcal{M} = 0$. So by 2.4.10, M is semisimple. □

2.5 Simple modules for algebras

Lemma 2.5.1 (Schur I) [**schur i**] *Let M, N be simple R-modules and $f \in \operatorname{Hom}_R(M,N)$. If $f \neq 0$, then f is R-isomorphism. In particular, $\operatorname{End}_R(M)$ is a division ring.*

Proof: Since $f \neq 0$, $\ker f \neq M$. Also $\ker f$ is an R-submodule and so $\ker f = 0$ and f is 1-1. Similarly, $\operatorname{Im} f \neq 0$, $\operatorname{Im} f = N$ and so f is onto. So f is a bijection and has an inverse f^{-1}. An easy computation shows that $f^{-1} \in \operatorname{Hom}_R(N,M))$. Choosing $N = M$ we see that $\operatorname{End}_R(M)$ is a division ring. □

Definition 2.5.2 [**def:k-algebra**] *Let R be commutative ring. A R-algebra A is a ring A with $R \leq Z(A)$.*

Let $\mathbb{K}$ be a field and V a non-zero $\mathbb{K}$-space. We identify $k \in \mathbb{K}$ with the endomorphism $v \to kv$ of V. Then $\mathrm{End}_{\mathbb{K}}(V)$ is a $\mathbb{K}$-algebra. If $\dim_{\mathbb{K}} V = n < \infty$, then $\dim_{\mathbb{K}} \mathrm{End}_{\mathbb{K}}(V) = n^2$.

Lemma 2.5.3 (Schur II) [**schur ii**] *Let $\mathbb{K}$ be a a field, A a $\mathbb{K}$-algebra and M a simple A-module with $\dim_{\mathbb{K}} M$ finite. Let $\mathbb{D} = \mathrm{End}_A(M)$. Then $\mathbb{D}$ is a $\mathbb{K}$-algebra and $\dim_{\mathbb{K}} \mathbb{D}\infty$. If $|\mathbb{K}|$ is finite, then $\mathbb{D}$ is a field. If $\mathbb{K}$ is algebraically closed, then $\mathbb{D} = \mathbb{K}$.*

Proof: Clearly $\mathbb{D}$ is a $\mathbb{K}$-subalgebra of $\mathrm{End}_{\mathbb{K}}(M)$. Since $\mathrm{End}_{\mathbb{K}}(M)$ is finite dimensional over $\mathbb{K}$, so is $\mathbb{D}$. By 2.5.1 $\mathbb{D}$ is a division ring. If V is finite, so is $\mathbb{D}$ and Wedderburn's Theorem implies that D is a field. Let $d \in \mathbb{D}$. Then $\mathbb{K}(d)$ is a finite field extension of $\mathbb{K}$. If $\mathbb{K}$ is algebraically closed, we conclude that $d \in \mathbb{K}$ and so $\mathbb{K} = \mathbb{D}$.

Lemma 2.5.4 [**closed in simple**]. *Let M be a simple R-module, A a closed subset of M, $J = \mathrm{A}_R(A)$ and $m \in M \setminus A$. Then $M = Jm$ and the map $J/\mathrm{A}_J(m) \to M, j + \mathrm{A}_J(m) \to jm$ is a well defined R-linear isomorphism.*

Proof: Since A is closed, $A = \mathrm{A}_R(J)$ and so $Jm \neq 0$. By 2.4.4 J is a left ideal in R and so Jm is an R-submodule of M. Since M is simple, $M = Jm$. Then map $J \to M, j \to jm$ exhibits $J/\mathrm{A}_J(m) \cong M$. □

Lemma 2.5.5 [**finite extension**] *Let M be simple R-module and $\mathbb{D} = \mathrm{End}_R(M)$. Let $V \leq W$ be $\mathbb{D}$ submodules of M with $\dim_{\mathbb{D}}(W/V)$ finite. If V is closed in M so is W. In particular all finite dimensional $\mathbb{D}$ subspaces of M are closed.*

Proof: By induction on $\dim_{\mathbb{D}} W/V$ we may assume that $W = V + \mathbb{D}w$ for some $w \in W \setminus V$. Let $I = \mathrm{A}_R(V)$ and $J = \mathrm{A}_I(w)$. We will show that $W = \mathrm{A}_R(J)$. So let $m \in \mathrm{A}_M(J)$. Then $J \subseteq \mathrm{A}_I(m)$ and hence the map $\alpha : I/J \to M, i + J \to im$ is well defined and R-linear. By 2.5.4 the map $\beta : I/J \to M, i + J \to iw$ is an R-isomorphism. Put $\delta = \alpha\beta^{-1}$. Then $\delta : M \to M$ is R-linear and $\delta(iw) = im$ for all $i \in I$. Hence $\delta \in \mathbb{D}$ and

$$i(\delta(w) - m) = i\delta(w) - im = \delta(iw) - im = 0$$

for all $i \in I$. Since V is closed, $V = \mathrm{A}_M(I)$ and so $\delta(w) - m \in V$. Thus $m \in \delta(w) + V \leq W$. Clearly $W \leq \mathrm{A}_M(J)$ and so indeed, $W = \mathrm{A}_W(J)$ is closed. □

Definition 2.5.6 [**def:dense**] *Let M be an R-module and $\mathbb{D} \leq \mathrm{End}_R(M)$ a division ring. Then we say that R is dense on M with respect to $\mathbb{D}$ if for each tuple $\mathbb{D}$-linear independent tuple $(m_i)_{i=1}^n \in M^n$ and each $(w_i)_{i=1}^n \in M^n$, there exists $r \in R$ with $rm_i = w_i$ for all $1 \leq i \leq n$.*

Theorem 2.5.7 (Jacobson's Density Theorem) [**density**] *Let M be an R-module and put $\mathbb{D} = \mathrm{End}_R(M)$. If M is simple, then R is dense on M with respect to $\mathbb{D}$.*

Proof: Let $(m_i)_{i=1}^n \in M^n$ be $\mathbb{D}$-linear independent and $(w_i)_{i=1}^n \in M^n$. By induction on n we will show that there exists $r \in R$ with $rm_i = w_i$ for all $1 \leq i \leq n$. For $n = 0$, there is nothing to prove. By induction there exists $s \in R$ with $sm_i = w_i$ for all $1 \leq i < n$. Let $V = \sum_{i=1}^{n-1} \mathbb{D}m_i$. Then by 2.5.5 V is closed and so by 2.5.4 there exists $t \in \mathrm{A}_R(V)$ with $tm_n = w_n - sm_n$. Put $r = s + t$. For $1 \leq i < n$, $tm_i = 0 =$ and so $rm_i = sm_i = w_i$. Also $rm_i = sm_i + tm_i = sm_n + (w_n - sm_n) = w_n$ and the theorem is proved. □

Corollary 2.5.8 [**more density**] *Let M be a simple R-module, $\mathbb{D} = \mathrm{End}_R(M)$ and W a finite dimensional $\mathbb{D}$-submodule of M. Put $N_R(W) = \{r \in R \mid rW \subseteq W\}$. Then $N_R(W)$ is a subring of W, W is a $N_R(W)$-submodule of M, $\mathrm{A}_R(W)$ is an ideal in $N_R(W)$ and if R^W denotes the image of $N_R(W)$ in $\mathrm{End}(W)$, then*

$$N_R(W)/\,\mathrm{A}_R(W) \cong R^W = \mathrm{End}_{\mathrm{D}}(W)$$

Proof: All but the very last statement in are readily verified. Clearly R_W is contained in $\mathrm{End}_{\mathrm{D}}(W)$. Let $\phi \in \mathrm{End}_{\mathrm{D}}(W)$ and choose a basis $(v_i, 1 \leq i \leq n)$ for W over $\mathbb{D}$. By 2.5.7 there exists $r \in R$ with $rv_i = \phi v_i$. Then $rW \leq W$ and so $r \in N_R(W)$. The image of r in $\mathrm{End}(W)$ is ϕ. Thus $\phi \in R^W$ and so $R^W = \mathrm{End}_{\mathbb{D}}(W)$. □

Definition 2.5.9 [**def:simple**] *A ring with no proper ideals is called* simple. *A direct sum of simple ring is called* semisimple.

Corollary 2.5.10 [**char simple rings**] *Let R be a simple ring. Then there exists a simple R-module M. Moreover, if M is a simple R-module and $\mathbb{D} = \mathrm{End}_R(M)$, then R is isomorphic to a dense subring of* $\mathrm{End}_{\mathrm{D}}(M)$.

Proof: Let I be a maximal left ideal, then R/I is a simple R-module. Now let M be any simple R-module. Since R is simple, $\mathrm{A}_R(M) = 0$. Thus $R \cong R^M$ and by 2.5.7, R and so also R^M is dense on M. □

Proposition 2.5.11 [**unique simple**] *Let M be faithful, simple R-module and put $\mathbb{D} = \mathrm{End}_R(M)$. Suppose that* $\dim_{\mathrm{D}} M$ *is finite.*

(a) [**z**] $R \cong R^M = \mathrm{End}_{\mathrm{D}}(M)$.

(b) [**a**] *As a left R-module $R \cong M^n$, where $n = \dim_R$.*

(c) [**b**] *Let I be a maximal left ideal in R Then $I = \mathrm{A}_R(m)$ for some $0 \in m \in M$ and $R/I \cong M$*

(d) [**c**] *Each left ideal in R is closed with respect to M.*

(e) [**d**] *The map $I \to \mathrm{A}_R(I)$ is a bijection between the left ideals in R and the $\mathbb{D}$-subspaces in M. Its inverse is $M \to \mathrm{A}_M(I)$.*

(f) [**e**] *Each simple R-module is isomorphic to M.*

(g) [**f**] *R is a simple ring.*

Proof: (a) Note that $N_R(M) = R$ and so (a) follows from 2.5.8

(b) Observe first that M is a simple R-module. Let $\mathcal{B}$ be a basis for M over $\mathbb{D}$ and let $b \in \mathcal{B}$. Then by 2.4.6, $\mathrm{A}_R(b)$ is a maximal ideal in R and $R/\mathrm{A}_R(b) \cong M$. Let $\mathcal{D}$ be a subset of $\mathcal{B}$. Then

$\bigcap_{b\in\mathcal{D}} \mathrm{A}_R(b) = \mathrm{A}_R(\mathbb{D}\mathcal{D})$. Moreover, by 2.5.5 $\mathbb{D}\mathcal{D}$ is closed in M. Also $\mathrm{A}_R(M) = 0$ since M is faithful and so $\mathrm{A}_R(\mathbb{D}\mathcal{D}) = 0$ iff $\mathbb{D}\mathcal{D} = M$ iff $\mathcal{B} = \mathcal{D}$. Thus 2.4.10 implies

$$R \cong \bigoplus_{b\in\mathcal{B}} R/\mathrm{A}_R(b) \cong M^n.$$

(c) By (b) there exists a simple R-submodule S of R with $S \cong M$ and $I \cap S = 0$. By maximality of I and simplicity of S, $R = I + S$ and $I \cap S = 0$. Hence $R/I \cong S \cong M$. Let $\psi : R/I \to M$ be an R-isomorphism and put $m = \phi(1 + I/I)$. Then

$$I = \mathrm{A}_R(1 + I/I) = \mathrm{A}_R(m)$$

(d) Let I be an left ideal in R and $\mathcal{J}$ the set of maximal ideals in R containing I. Since R is a semisimple R-module, so is R/I. Thus 2.4.9 implies that $J_{R/I}(R) = 0$. Thus $\bigcap \mathcal{J} = I$. By (c), for each $J \in \mathcal{J}$ there exists $m_J \in M$ with $J = \mathrm{A}_R(m_J)$. Put $N = \{m_J \mid J \in \mathcal{J}\}$. Then

$$\mathrm{A}_R(N) = \bigcap_{J\in\mathcal{J}} \mathrm{A}_R(m_J) = \bigcap J \in \mathcal{J}J = I.$$

So I is closed.

(e) follows from (c), 2.5.5 and 2.4.5.

(f) Follows from (c) and 2.4.6.

(g) Since M is simple, 0 and M are the only R-submodules in M. So by (c), 2.5.5 and 2.4.5 $M = \mathrm{A}_R(O)$ and $0 = \mathrm{A}_R(M)$ are the only ideals in M. □

Lemma 2.5.12 [**endend**] *Let $\mathbb{D}$ be a division ring and M a vector space over $\mathbb{D}$. Then*

(a) [**a**] $\mathrm{End}_{\mathrm{End}_{\mathbb{D}}(M)}(M) = \mathbb{D}$.

(b) [**b**] *If* $\dim \mathbb{D}W$ *is finite dimensional then* $\mathrm{End}_{\mathbb{D}}(M)$ *is simple.*

Proof: (a) Let $\mathbb{F} = \mathrm{End}_{\mathrm{End}_{\mathbb{D}}(M)}(M)$. Then clearly $\mathbb{D} \leq \mathbb{F}$. By 2.5.1, $\mathbb{F}$ is a division ring. Let $\mathcal{B}$ be a $\mathbb{D}$ basis for $\mathcal{M}$. Pick $m \in \mathcal{B}$ and define $\phi \in \mathrm{End}_{\mathrm{D}}(M)$ by $\phi(b) = \delta_{bm}m$ for all $b \in \mathcal{B}$. Then $\phi(M) = \mathbb{D}m$. Let $f \in \mathbb{F}$. Then

$$f(\phi(M)) = \phi(f(M)) \leq \phi(M)$$

Thus $fm = dm$ for some $d \in \mathcal{F}$. Since $f - d \in \mathcal{F}$, $(f - d)m = 0$ an d$\mathcal{F}$ is a division ring, $f - d = 0$. Thus $f = d$ and $\mathbb{F} = \mathbb{D}$.

(b) Note that M is a simple $\mathrm{End}_{\mathbb{D}}(M)$-module. By (a) we can apply 2.5.11 to $R = \mathrm{End}_{\mathbb{D}}(M)$. So (b) follows from 2.5.11(g). □

Definition 2.5.13 [**def:artinian**] *A ring R is called* Artinian *if it fulfills the DCC on left ideals.*

Lemma 2.5.14 [**simple for artin**] *Let R be an Artinian ring and M a simple R-module. Then M is finite dimensional over $\mathbb{D} = \mathrm{End}_R(M)$.*

Proof: . Suppose that $\dim_{\mathbb{D}} M\infty$. Then there exists an infinite strictly ascending series

$$M_1 < M_2 < M_3 < \ldots$$

of finite dimensional $\mathbb{D}$-subspaces. By 2.5.5 each M_i is closed. Thus

$$\mathrm{A}_R(M_1) > \mathrm{A}_R(M_2) > \mathrm{A}_R(M_3) > \ldots$$

is a strictly descending chain of left ideals in R, contradicting the *DCC* conditions of Artinian rings. □

Lemma 2.5.15 (Chinese Remainder Theorem) [**chinese**] *Let R be ring and $\mathcal{I}$ a finite set of ideals in R. Suppose that $\bigcap \mathcal{I} = 0$ and $I + J = R$ for all $I \neq J \in \mathcal{I}$. Let $I \in \mathcal{I}$ and put $R_I = \bigcap\{J \mid I \neq J \in \mathcal{I}\}$. Then*

(a) [**a**] $R = I \bigoplus R_I$.

(b) [**b**] $I = \bigoplus\{R_J \mid I \neq J \in \mathcal{I}\}$.

(c) [**c**] $R = \bigoplus_{I \in \mathcal{I}} R_I$.

(d) [**d**] *The map $R_I \to R/I$, $r \to r + I$ is an isomorphism.*

(e) [**e**] *The map $R \to \bigoplus_{I \in \mathcal{I}} R/I, r \to (r + I)_{I \in \mathcal{I}}$ is an isomorphism of rings.*

Proof: Let $\mathcal{J} = \mathcal{I} \setminus \{I\}$ and let $\emptyset \neq \mathcal{N} \subseteq \mathcal{J}$. We claim that $R = I + \bigcap \mathcal{N}$. If $|\mathcal{N}| = 1$, this holds by assumption. Let $J \in \mathcal{N}$ and but $S = \bigcap\{K \in \mathcal{N} \mid K \neq J\}$. By induction $R = I + S = I + J$. Since R has a one,

$$R = R^2 = (I+S)(I+J) = I^2 + SI + IJ + SJ$$

Since I is an ideal, $I^2 + SI + IJ \leq I$. Since S and J are ideals $SJ \leq S \cap J = \bigcap \mathcal{N}$. So $R = I + \bigcap \mathcal{N}$, proving the claim.

For $\mathcal{N} = \mathcal{J}$ we conclude that $R = I + R_I$. Since $I \cap R_I = \bigcap \mathcal{I} = 0$ we have $R = I \oplus R_I$. Thus (a) holds. In particular, I has a one element and so is a is a ring. Note that $\bigcap_{j \in J}(I \cap J) = \bigcap \mathcal{I} = 0$ and $R_J = \bigcap\{I \cap K \mid J \neq K \in \mathcal{J}\}$.

By induction (c) holds for R replaced by I and $\mathcal{I}$ by $\{I \cap J \mid J \in \mathcal{J}\}$. This gives (b).

(c) follows from (a) and (b). (d) follows from (a). (e) follows easily from (b), (c) and (d). □

Lemma 2.5.16 [**basic direct sum of rings**] *Let $\mathcal{S}$ be a finite set rings and $R = \bigoplus \mathcal{S}$. For $S \in \mathcal{S}$ let $S^* = \bigoplus\{S \neq T \in \mathcal{S}\}$ and $\mathcal{S}^* = \{S^* \mid S \in \mathcal{S}\}$.*

(a) [**a**] *Let I be left ideal in R. Then $I = \bigoplus_{S \in \mathcal{S}} I \cap S$.*

(b) [**e**] *If I is a minimal left ideal of R, then $I \leq S$ for some $S \in \mathcal{S}$. Moreover, I is a minimal left ideal of S*

(c) [**f**] *If I is a maximal left ideal of R, then $S^* \leq I$ for some I. Moreover, $I = (I \cap S) \oplus S^*$ and $I \cap S$ is a maximal ideal in S.*

(d) [**g**] *Let M be a simple R-module, then $S^* \leq \mathrm{A}_R(M)$ for some $S \in \mathcal{S}$.*

(e) [**h**] *$J(R) = \bigoplus_{S \in \mathcal{A}} J(R)$.*

Proof: (a) Let I be an left ideal and $i \in I$. Then $i = 1_R i = \sum_{S \in \mathcal{S}} 1_S i$. Since I is left ideal, $1_S i \in I$ and since S is an ideal in R, $1_S i \in S \cap I$. Thus $i \in \bigoplus_{S \in \mathcal{S}} I \cap S$ and (a) holds.

(b) and (c) follows immediately form (a).

(d) By 2.4.6, $M \cong R/I$ for some maximal left ideal I in R. By (c), $S^* \leq I$ for some $S \in \mathcal{S}$ and so $S^* \leq \mathrm{A}_R(R/I) = \mathrm{A}_R(M)$.

(e) Follows from (c). □

Corollary 2.5.17 [**basic semisimple rings**] *Let R be a semisimple ring and let $\mathcal{S}$ be a (finite) set of simple rings with $R = \bigoplus \mathcal{S}$. For $S \in \mathcal{S}$ let $S^* = \bigoplus\{S \neq T \in \mathcal{S}\}$ and $\mathcal{S}^* = \{S^* \mid S \in \mathcal{S}\}$. Then*

(a) [**b**] *Let I be an ideal in R. Then $I = \bigoplus\{S \mid S \in \mathcal{S}, S \leq I\}$.*

(b) [**c**] *$\mathcal{S}$ is the set of minimal ideals of R.*

(c) [**d**] *$\mathcal{S}^*$ is the set of maximal ideals of R.*

(d) [**g**] *Let M be a simple R-module, then $S^* = \mathrm{A}_R(M)$ for some $S \in \mathcal{S}$.*

(e) [**h**] $J(R) = 0$.

(a) Let I be an ideal in R and $S \in \mathcal{S}$. Then $S \cap I$ is an ideal in the simple ring S. Thus either $S \cap I = 0$ or $S \cap I = S$. So (a) follows from 2.5.16(a).

(b) and (c) follows immediately from (a).

(d) By 2.5.16(d) $S^* \leq \mathrm{A}_R(M)$ for some $S \in \mathcal{S}$. Since S^* is a maximal ideal, $\mathrm{A}_R(M) = S^*$.

(e) Let $S \in \mathcal{S}$. Since $J(S) < S$ and S is simple, $J(S) = 0$. So (e) follows from 2.5.16(e). □

Theorem 2.5.18 [**classification of artin**] *Let R be an Artinian ring with $J(R) = 0$. Let $\mathcal{M}$ be a set of representatives for the isomorphism classes of simple R-modules and let $M \in \mathcal{M}$. Put $R_M = \bigcap\{\mathrm{A}_R(P) \mid M \neq P \in \mathcal{M}\}$. Then*

(a) [**a**] *$\mathcal{M}$ is finite.*

(b) [**b**] *M is finite dimensional over $\mathrm{D}_M := \mathrm{End}_R(M)$.*

(c) [**c**] $R_M \cong R^M = \mathrm{End}_{\mathbb{D}_M}(M)$.

(d) [**d**] $R = \bigoplus_{M \in \mathcal{M}} R_M \cong \bigoplus_{M \in \mathcal{M}} \mathrm{End}_{\mathbb{D}_M}(M)$

(e) [**e**] $\mathrm{A}_R(M) = \bigoplus\{R_P \mid M \neq P \in \mathcal{M}\}$.

(f) [**f**] *R is semisimple.*

Proof: By 2.4.7 $\bigcap_{M \in \mathcal{M}} \mathrm{A}_R(M) = J(R) = 0$. By 2.2.8 there exists a finite subset $\mathcal{N}$ of $\mathcal{M}$ with $\bigcap_{N \in \mathcal{N}} \mathrm{A}_R(N) = 0$. By 2.5.14 M is finite dimensional and so by 2.5.11, $R^M = \mathrm{End}_{\mathbb{D}_M}(M)$ is simple, and M is up to isomorphism the unique simple $R/\mathrm{A}_R(M)$-module. In particular, if $M \neq N \in \mathcal{M}$ then $\mathrm{A}_R(M) \nleq \mathrm{A}_R(N)$. Since $R/\mathrm{A}_R(N) \cong R^N$ is simple , $R = \mathrm{A}_R(M) + \mathrm{A}_R(N)$. For $N \in \mathcal{N}$ put $R^*_N = \bigcap\{P \in \mathcal{N} \mid P \neq N\}$. Then by 2.5.15,

$$R = \bigoplus_{N \in \mathcal{N}} R^*_N$$
$$R^*_N \cong R/\mathrm{A}_R(N) \cong R^N = \mathrm{End}_{\mathbb{D}_N}(N)$$
$$N^* := \bigoplus\{R^*_P \mid N \neq P \in \mathcal{N}\} = \mathrm{A}_R(N)$$

Let $M \in \mathcal{M}$. 2.5.17(d) implies $N^* \leq \mathrm{A}_R(M)$ for some $N \in \mathcal{N}$. Hence $\mathrm{A}_R(N) \leq \mathrm{A}_R(M)$ and so $M \cong N$ and $M = N$. Thus $\mathcal{M} = \mathcal{N}$ and $R_N = R^*_N$. □

Lemma 2.5.19 [**all modules semisimple**] *Let R be a ring. Then R is semisimple as a left R-modules iff all R-modules are semisimple.*

Proof: Suppose R is semisimple as a left R-module and let M be an R-module. Let $m \in M$. Then $Rm \cong R/\operatorname{A}_R(m)$. Since R is semisimple as an R-module, so is $R/\operatorname{A}_R(m)$ and hence Rm. Thus by 2.3.1, M is semisimple.

The other direct is obvious . □

Proposition 2.5.20 [**char semisimple artin**] *Let R be an Artinian ring. The the following are equivalent.*

(a) [**a**] *Every R-module is semisimple.*

(b) [**b**] *R is semisimple as left R-module.*

(c) [**c**] $J(R) = 0$.

(d) [**d**] *R is a semisimple ring.*

Proof: (a)$\iff$ (b): Thus is 2.5.19.

(b)$\iff$ (c): Follows from 2.4.11 applied to $M = R$.

(c)$\Longrightarrow$ (d): Follows from 2.5.18

(d)$\Longrightarrow$ (c): See 2.5.17(e). □

Corollary 2.5.21 [**semisimple implies artin**] *Let R be a ring and suppose that R is semisimple as a left R-module. Then R is Artinian and so semisimple as a ring.*

Proof: Since R is the sum of simple R-submodules, there exists a finite set $\mathcal{I}$ of simple R-submodules with $1 \in \sum caI$. But then $R = R \leq \sum \mathcal{I}$ and $R = \sum \mathcal{I}$. So by 2.1.17(f) every R submodule W of R is the direct sum of finitely many simple R-submodule. By 2.2.13 the number d_W of simple direct summands is independent from the choice of the direct sum decomposition of W. If $V < W$ are R-submodules of R, then 2.1.17(a) implies that $d_V < d_W$. Thus R fulfills DCC on left ideals, that is R is Artinian. The second statement now follows from 2.5.20. □

Corollary 2.5.22 [**simple rings and artin**] *Let R be a simple ring. Then the following are equivalent.*

(a) [**a**] *R is Artinian.*

(b) [**b**] $R \cong \operatorname{End}_{\mathbb{D}}(M)$ *for some division ring and some finite dimensional $\mathbb{D}$-module M.*

(c) [**c**] *R has a minimal left ideal.*

(d) [**d**] *R is semisimple as a left R-module.*

Proof: (a)$\Longrightarrow$ (b): follows from 2.5.18.

(b)c Since $\dim_{\mathbb{D}} M$ is finite there exists an $\mathbb{D}$-subspace in M. By 2.5.12 a we can apply 2.5.11(f) and conclude that $\mathrm{End}_{\mathbb{D}}(M)$ has a minimal left ideal.

(c)d Let I be a minimal left ideal in R. For each $r \in R$, the map $I \to R, i \to ir$ is R-linear. Thus either $Ir = 0$ or Ir is a simple R-submodule of R. Thus by 2.1.17 IR is a semisimple R-module. Note that IR is an ideal in R and since R is simple $IR = R$.

(d)a follows from 2.5.21. □

Since there do exists non Artinian simple rings, we conclude that there exists simple rings without minimal left ideals and in particular that semisimple rings do not need to me semisimple as a left R-module.

Corollary 2.5.23 [**group rings semisimple**] *Let $\mathbb{K}$ be a field and G a finite group. If* $\mathrm{char}\,\mathbb{K} \nmid |G|$ *then $J(\mathbb{K}G) = 0$ and $\mathbb{K}G$ is a semisimple ring.*

Proof: Since $\mathbb{K}G$ is finite dimensional over $\mathbb{K}$, $\mathbb{K}G$ is Artinian. By 2.3.2 all $\mathbb{K}G$-modules are finite dimensional and so the Corollary follows from 2.5.20. □

Corollary 2.5.24 [**fd k algebras**] *Let $\mathbb{K}$ be an algebraically closed field and A a finite dimensional $\mathbb{K}$-algebra with $J(A) = 0$. Let $\mathcal{M}$ be a set of representatives for the isomorphism classes of simple R-modules. Then $\mathcal{M}$ is finite, each $M \in \mathcal{M}$ is finite dimensional over $\mathbb{K}$ and*

$$A \cong \bigoplus_{M \in \mathcal{M}} \mathrm{End}_{\mathbb{K}}(M)$$

Proof: Since $\dim_{\mathbb{K}} A$ is finite, A is Artinian. Let $M \in \mathcal{M}$ and $0 \neq m \in M$. Then $M \cong A/\,\mathrm{A}_A(m)$. Thus $\dim_{\mathbb{K}} M \leq \dim_{\mathbb{K}} A < \infty$. By 2.5.3, $\mathrm{End}_A(M) = \mathbb{K}$. So the Corollary follows from 2.5.18.

2.6 Tensor Products

Definition 2.6.1 [**def:multilinear**] *Let R be a commutative ring and M an R-module. Furthermore let $(M_i, i \in I)$ a family of R-modules and $f : \mathop{\textcircled{Π}}_I M_i \to M$ a function. Let J and K be subset of I with $I = J \cup K$ and $J \cap K = \emptyset$.*

(a) [**b**] $\iota_{J,K} : \mathop{\textcircled{Π}}_{j \in J} M_j \times \mathop{\textcircled{Π}}_{k \in K} M_k \to \mathop{\textcircled{Π}}_{i \in I} M_i, ((m_j), (m_k)) \to (m_i)$

(b) [**c**] *For $m \in \mathop{\textcircled{Π}}_{k \in K} M_k$ define $f_m : \mathop{\textcircled{Π}}_{j \in J} M_j \to M, n \to f(\iota_{J,K}(n, m))$.*

(c) [**d**] *f is called R-multilinear if for all $i \in I$ and all $m \in M_{I\setminus i}$, $f_m : M_i \to M$ is R-linear.*

We usually will identify $(n,m) \in \mathop{\text{\textcircled{Π}}}_{j\in J} M_j \times \mathop{\text{\textcircled{Π}}}_{k\in K} M_k$ with $\iota_{J,K}(n,m)$. In particular, we will write $f(n,m)$ for $f(\iota_{J,K}(n,m))$ and so $f_m(n) = f(n,m)$.

Definition 2.6.2 [**def:multilinear tensor**] *Let R be a commutative ring and $f : \mathop{\text{\textcircled{Π}}}_I M_i \to M$ be R-multilinear map. Suppose that for all R-multilinear maps $g : \mathop{\text{\textcircled{Π}}}_I M_i \to N$ there exists unique R-linear map $h : M \to N$ with $g = h \circ f$. Then f is called a* tensor map *for $(M_i, i \in I)$ and M a* tensor product *of $(M_i, i \in I)$.*

Lemma 2.6.3 [**multilinear tensor**] *Let R be a commutative ring and $(M_i, i \in I)$ a family of R-modules. Then there exists a tensor map $f : \mathop{\text{\textcircled{Π}}}_I M_i \to M$ and f is unique up to isomorphism.*

Proof: Let F be a free R-module with basis $(a(m) \mid m \in \mathop{\text{\textcircled{Π}}}_{i\in I} M_i)$. Let W be the R-submodule generated by all the $a(ru+sv,n) - ra(u,n) - sa(v,n)$, $r,s \in R, i \in I$, $u,v \in M_i$ and $n \in M_{I\setminus i}$. Put $M = F/W$ and define $f(m) = a(m)+W$ for all $m \in M_I$. Then clearly f is R-multilinear. Now let $g : \mathop{\text{\textcircled{Π}}}_I M_i \to N$ be R-multilinear. Then there exists an R-linear map $\tilde{h} : F \to N$ with $\tilde{h}(a(m)) = g(m)$ for all $m \in M_I$. Since g is R-multilinear, $W \leq \ker \tilde{h}$ and so there exists an R-linear $h : M \to N$ with $h(a(m)+W) = g(m)$ for all $m \in M_I$. So $g = h \circ f$. The uniqueness of h is readily verified. So f is a tensor map of $(M_i, i \in I)$.

That f is unique up to isomorphism is obvious. □

Let $f : \mathop{\text{\textcircled{Π}}}_I M_i \to M$ be a tensor map for $(M_i, i \in I)$. We will denote M by $\bigotimes_I M_i$, f by $\otimes_I$ and write $\otimes_{i\in I} m_i$ for $f((m_i))$ and if $m \in \mathop{\text{\textcircled{Π}}}_{i\in I} M_i$, $\otimes m = \otimes_I m = f(m)$. If $g : \mathop{\text{\textcircled{Π}}}_{i\in I} M_i \to N$ is R-multilinear $\otimes g$ denotes the unique R-linear map $\bigotimes_{i\in I} M_i \to N$ with $g = (\otimes g) \circ f$. So $(\otimes g)(\otimes m) = g(m)$ for all $m \in \mathop{\text{\textcircled{Π}}}_{i\in I} M_i$.

Lemma 2.6.4 [**basic multilinear tensor**] *Let R be a commutative ring and a $(M_i, i \in I)$ a finite family of R-modules.*

(a) [**a**] *If $M_i = R$ for all $i \in I$, then $\mathop{\text{\textcircled{Π}}}_{i\in I} R \to R, (r_i) \to \prod_{i\in I} r_i$ is a tensor product of $(M_i, i \in I)$.*

(b) [**b**] *Suppose for each $i \in I$, $M_i = \bigoplus \mathcal{W}_i$ for some set $\mathcal{W}_i$ of R-submodules of M_i.*

$$\mathop{\text{\textcircled{Π}}}_{i\in I} M_i \cong_R \bigoplus \left\{ \bigotimes_{i\in I} W_i \mid (W_i) \in \mathop{\text{\textcircled{Π}}}_{i\in I} \mathcal{W}_i \right\}.$$

(c) [**c**] *Suppose that for each $i \in I$, M_i is a free R-module with basis $\mathcal{B}_i$. Then $\bigotimes_{i\in I} M_i$ is a free R-module with basis*

$$\otimes_{i\in I}\mathcal{B}_i := (\otimes b \mid b \in \mathop{\text{\textcircled{Π}}}_{i\in I} \mathcal{B}_i).$$

(d) [**d**] *If $I = \emptyset$, then $f : \mathop{\textcircled{Π}}_{\emptyset} \to R, () \to 1$ is a tensor product of $()$.*

(e) [**e**] *If $I = \{i\}$, then id_{M_i} is a tensor product for $(M_i, i \in I)$ over R.*

Proof: (a) Let $f((r_i)) = \mathop{\textcircled{Π}}_{i\in I} r_i$. Then clearly f is R-multilinear. Let $g : \mathop{\textcircled{Π}}_{i\in I} R \to N$ be R-multilinear. Define $n = g((1)_{i\in I})$ and $R \to N, r \to rn$. Then clearly $g = h \circ f$ and h is unique with this property. So (a) holds.

(b) For $i \in I$ and $W \in \mathcal{W}_i$ let $\pi_W : M_i \to W$ be the projection according to $M_i = \bigoplus \mathcal{W}_i$. Define

$$f : \mathop{\textcircled{Π}}_{i\in I} M_i \to \bigoplus\{\bigotimes_{i\in I} W_i \mid (W_i) \in \mathop{\textcircled{Π}}_{i\in I} \mathcal{W}_i\}, (m_i) \to (\otimes_{i\in I}\pi_{W_i}(m_i)) \mid (W_i) \in \mathop{\textcircled{Π}}_{i\in I} \mathcal{W}_i\}$$

Note that for given $i \in I$ and $m_i \in M_i$, $\pi_W(m_i) = 0$ for almost all $W \in \mathcal{W}_i$. Hence also $\otimes_{i\in I}\pi_{W_i}(m_i) = 0$ for almost all $(W_i) \in \mathop{\textcircled{Π}}_I \mathcal{W}_i$. Thus f is a well defined R-multilinear map.

Now let $g : \mathop{\textcircled{Π}}_{i\in I} R \to N$ be R-multilinear. For $W = (W_i) \in \mathop{\textcircled{Π}}_I \mathcal{W}_i$ let g_W be the restriction of g to $\mathop{\textcircled{$\Pi$}}_{i\in I} W_i$. Then there exists $h_W : \bigotimes_{i\in I} W_i \to N$ with $g_W(w) = h_W(\otimes w)$ for all $w \in \mathop{\textcircled{Π}}_{i\in I} W_i$. Define

$$h : \bigoplus \left\{ \bigotimes_{i\in I} W \mid W \in \mathop{\textcircled{Π}}_{i\in I} \mathcal{W}_i \right\} \to N, \quad (a_W)_{W\in \mathop{\textcircled{Π}} \mathcal{W}_i} \to \sum\{h_W(a_W) \mid W \in \mathop{\textcircled{Π}} \mathcal{W}_i\}$$

Then it is easy to check that $g = h \circ f$ and h is unique with this property. So (b) holds.

(c) Let $b_i \in \mathcal{B}_i$, then by (a) $\bigotimes_{i\in I} Rb_i$ is free with basis $\otimes_{i\in I} b_i$. Moreover, $M_i = \bigoplus_{b\in\mathcal{B}_i} Rb$ and so (c) follows from (b).

(d) Note here that the direct product $\mathop{\textcircled{$\Pi$}}_{\emptyset}$ of the empty family of sets is a set with one element. We call this element the empty tuple and denote it by $()$. Given an R-module N and $g : \mathop{\textcircled{Π}}_{\emptyset} \to N, () \to n$. Define $h : R \to N, r \to rn$. Then $g = h \circ f$.

(e) is readily verified. □

Lemma 2.6.5 [**tensor associative**] *Let R be a commutative ring, $(M_i, i \in I)$ a family of R-modules and $(I_d, d \in \Delta)$ a partition of I. Then there exists a unique R-linear map*

$$\rho : \bigotimes_{i\in I} M_i \to \bigotimes_{d\in\Delta} \left(\bigotimes_{i\in I_d} M_i \right) \text{ with } \otimes\, i \in Im_i) \to \otimes_{d\in\Delta}(\otimes_{i\in I_d} m_i)$$

Moreover, if Δ is finite, then ρ is an isomorphism.

Proof: Observe that the map $\mathop{\textcircled{$\Pi$}}_{i\in I} M_i, (m_i) \to \otimes_{d\in\Delta}(\otimes_{i\in I_d} m_i)$ is R-multilinear. Thus the uniqueness and existence of ρ follows from the definition of the tensor product.

If Δ is finite, we may assume by induction that $|\Delta| = 2$. It is now easy to define an inverse to ρ. □

For finite Δ we will usually identify $\bigotimes_{d\in\Delta}\left(\bigotimes_{i\in I_d} M_i\right)$ with $\bigotimes_{i\in I} M_i$ via the map ρ of the preceding lemma. In particular, if $I = J\cup K$ with $J\cap K = \emptyset$ and $p = (m_j)_{j\in J} \in \bigoplus_{j\in J} M_j$ and $q = (m_k)_{k\in K} \in \bigoplus_{k\in K} M_k$ then

$$(\otimes p) \otimes (\otimes q) = \otimes(p, q) = \otimes_{i\in I} m_i.$$

Definition 2.6.6 [**def:balanced**] *Let R be a ring, X a right R module and Y a left R-module, Z a $\mathbb{Z}$-module and $f : X \times Y \to Z$ a function.*

(a) [**a**] *f is called R-*balanced *if it is $\mathbb{Z}$-multilinear and for all $x \in X, y \in Y$ and $r \in R$, $f(xr, y) = f(x, ry)$.*

(b) [**b**] *Suppose that f is balanced and that for each R-balanced map $g : X \times Y \to N$, there exists a unique $\mathbb{Z}$-linear map, $h : Z \to N$ with $g = h \circ f$. Then f is called a* tensor map *of X and Y over R and Z is called a* tensor product *of X and Y over R.*

Lemma 2.6.7 [**balanced tensor**] *Let X be a right- and Y a left R-module. Then there exists a tensor product for X and Y over R. Moreover, any two such tensor products are isomorphic.*

Proof: Let $F = X \otimes_{\mathbb{Z}} Y$ and W the $\mathbb{Z}$-subspace generated by the $(xr) \otimes y - x \otimes (ry)$, $x \in X, y \in Y$ and $r \in R$. Put $Z = F/W$ and define $f : X \times Y \to X, (x, y) \to x \otimes y + W$. □

We denote the tensor product of X and Y over R by $X \otimes_R Y$. We reader might convince themselves that in the case of a commutative ring our two notation of tensor product agree. More precisely suppose that X and and Y are left R-modules. Let $\tilde{X}$ be a the right R-module, define by $\tilde{X} = X$ as abelian groups and $xr = rx$ for all $x \in X, r \in R$. Then the tensor product for X and Y over R is also the tensor product for $\tilde{X}$ and Y over R.

Definition 2.6.8 [**def:directed set**] *Let $(I, \leq)$ be a partially ordered set.*

(a) [**a**] *$(I, \leq)$ is called a* directed set *if for each $i, j \in I$ there exists $k \in I$ with $i \leq j$ and $i \leq k$.*

(b) [**b**] *A* directed system *consists of a directed set $(I, \leq)$, a family of sets $(M_i, i \in I)$ and family of functions $(\alpha_{ij} \mid M_i \to M_j \mid i \leq j \in I)$ such that $\alpha_{ii} = \mathrm{id}_{M_i}$ and $\alpha_{jk} \circ \alpha_{ij} = \alpha_{ik}$ for all $i \leq j \leq k \in I$.*

(c) [**c**] *Let $\mathcal{L} = (\alpha_{ij} \mid i \leq j \in I)$ be a direct system. A* direct limit *for $\mathcal{L}$ is a set L (denoted by $\varinjlim \mathcal{L}$ together with a family of functions $(\alpha_i : M_i \to L)$ such that*

(a) [**a**] *$\alpha_i = \alpha_j \circ \alpha_{ij}$ for all $i \leq j \in I$; and*

(b) [**b**] *whenever* $(\beta_i : M_i \to N$ *is a family of functions with* $\beta_i = \beta_j \circ \alpha_{ij}$ *for all* $i \leq j \in I$*, then there exists a unique function* $\beta : L \to N$ *with* $\beta_i = \beta \circ \alpha_i$ *for all* $i \in I$*.*

Lemma 2.6.9 [**basic direct limit**] *Let* $\mathcal{L} = (\alpha_{ij} \mid i \leq j \in I)$ *be a direct system. Then*

(a) [**a**] $\mathcal{L}$ *has a direct limit*

(b) [**b**] *Any two direct limits are isomorphic.*

(c) [**c**] *Let* $(\alpha_i : M_i \to M; i \in I)$ *be a direct limit of* $\mathcal{L}$*. Then* $M = \bigcup_{i\in I} \operatorname{Im} \alpha_i$*.*

Proof: (a) Let $F = \{(i, m) \mid i \in I, m \in M_i\}$ be the disjoint union of the $M_i, i \in I$. Define a relation $\sim$ on F by $(i, m) \sim (j, n)$ if there exists $k \in I$ with $i, j \leq k$ and $\alpha_{ik}(m) = \alpha_{jk}(n)$. It is readily verified that $\sim$ is an equivalence relation. Let $L = F/\sim$ and define $\alpha_i : M_i \to L, m \to [(i, m)]$. Clearly 2.6.8(c:a) holds. Let $(\beta_i : M_i \to N)$ be as in 2.6.8(c:b). Define $\beta : L \to N$ by $\beta([(i, m)]) = \beta_i(m)$. Then clearly $\beta_i = \beta \circ \alpha_i$, but we need to verify that β is well defined. So let $(i, m) \sim (j, n)$ and choose k with $i, j \leq k$ with $p := \alpha_{ik}(m) = \alpha_{jk}(n)$. Then $\beta_i(m) = (\beta_k \circ \alpha_{ik})(m) = \beta_k(p)$ and by symmetry, $\beta_j(n) = \beta_k(p)$. So β is well defined.

(b) Follows easily from the definition of a direct limit.

(c) By construction this holds for the direct limit found in (a). So (c) follows from (b).

□

Lemma 2.6.10 [**easy direct limits**] *Let* $\mathcal{L} = (\alpha_{ij} \mid i \leq j \in I)$ *be a direct system,* L *a set and* $(\alpha_i : M_i \to L)$ *be a family of functions with* $\alpha_i = \alpha_j \circ \alpha_{ij}$ *for all* $i \leq j \in I$*. Suppose that each* α_{ij} *is one to one. Then the following are equivalent:*

1. [**a**] $(\alpha_i, i \in I)$ *is a direct limit of* $\mathcal{L}$*.*

2. [**b**] *Each* $\alpha_i, i \in I$ *is* $1 - 1$ *and* $L = \bigcup_{i\in I} \operatorname{Im} \alpha_i$*.*

Proof: (1)$\Longrightarrow$ (2): Since any two direct limits are isomorphic we may assume that $(\alpha_i, i \in I)$ is the direct limit constructed in 2.6.9. Since $[(i, m)] = \alpha_i(m)$, $L = \bigcup_{i\in I} \operatorname{Im} \alpha_i$. Suppose that $\alpha_i(m) = \alpha_i(n)$. Then $[(i, m)] = [(i, n)]$ and so there exists $i \leq k \in I$ with $\alpha_{ik}(m) = \alpha_{ik}(n)$. Since α_{ik} is $1 - 1$ by assumption we get $n = m$. So α_i is $1 - 1$ and (2) holds.

(2)$\Longrightarrow$ (1): We will verify that $(\alpha_i; i \in I)$ fulfills the definition of a direct limit. Let $(\beta_i : M_i \to K, i \in I)$ be a family of function with $\beta_i = \beta_j \circ \alpha_{ij}$ for all $i \leq j \in I$. Suppose that $\alpha : L \to K$ is a function with $\beta_i = \alpha \circ \alpha_i$ for all $i \in I$. Then

$$(*) \qquad \alpha(l) = \beta_i(m) \quad \forall l \in L, i \in I, m \in M_i \text{ with } l = \alpha_i(m)$$

Since $L = \bigcup_{i\in I} \operatorname{Im} \alpha_i$, this uniquely determines α. To show the existence we define α via (*), but need to verify that this is well defined. So suppose that $i, j \in I, m_i \in M_i$

and $m_j \in M_j$ with $\alpha_i(m_i) = \alpha_j(m_j)$, Choose k with $i, j \leq k$ and put $n_i = \alpha_{ik}(m_i)$ and $n_j = \alpha_{jk}(m_j)$. Then

$$\alpha_k(n_i) = \alpha_k(\alpha_{ik}(m_i)) = \alpha_i(m_i) = \alpha_j(m_j) = \alpha_k(\alpha_{jk}(m_j)) = \alpha_k(n_k)$$

Since α_k is one to one we conclude $n_i = n_j$. Thus

$$\beta_i(m_i) = \beta_k(\alpha_{ik}(m_i)) = \beta_k(n_i) = \beta_k(n_j) = \beta_k(\alpha_{jk}(m_j) = \beta_j(m_j)$$

So α is well defined.

□

Example 2.6.11 [**direct limits of z**] *Let $(n_i, i \in I)$ be a family of positive integers. Let $\mathcal{F}(I)$ be the set of finite subsets of I. For $J \in \mathcal{F}(I)$ put $M_J = \mathbb{Z}$ and $n_J = \prod_{j \in J} n_j$. For $J \subseteq K \in \mathcal{F}(I)$, define $\alpha_{JK} : M_J \to M_k, m \to n_{K \setminus J} \cdot m$. Then $\mathcal{L} = (\alpha_{JK})$ is a directed system. Let $L = \{\frac{n}{n_J} \mid J \in \mathcal{F}(I), n \in \mathbb{Z}\}$. Then L is an additive subgroup of $\mathbb{Q}$. Define $\alpha_J : M_J \to L, m \to \frac{m}{n_J}$. Then $L = \varinjlim M_J$.*

Proof: Let $J \subseteq K \in \mathcal{F}(I)$ and $m \in M_J$. Then $n_K = n_J \cdot n_{K \setminus I}$ and so

$$\alpha_K(\alpha_{JK}(m)) = \alpha_K(n_{K \setminus J} m) = \frac{n_{K \setminus J} \cdot m}{n_K} = \frac{m}{n_J} = \alpha_J(m)$$

So 2.6.8(c:a) holds. Clearly $L = \bigcup \operatorname{Im} \alpha_K$ and each α_J and α_{JK} is $1-1$. So by 2.6.10, L is the direct limit of the M_J. □

Lemma 2.6.12 [**direct limit of modules**] *Let R be a ring and $\mathcal{L} = (\alpha_{i,j} : M_i \to M_J)$ a directed system of R-linear maps. Let $(\alpha_i : M_i \to L)$ be a direct limit for $\mathcal{L}$. Then there exists a unique R-module structure on L such that each α_i is R-linear.*

Proof: Let $a, b \in L \in L$ and $r \in R$. By 2.6.9(c) there exists $i, j \in I$ and $a_i \in M_i$ and $b_j \in M_j$ with $\alpha_i(a_i) = a$ and $\alpha_j(b_j) = b$. Choose $k \in I$ with $i \leq k$ and $j \leq k$ and put $a_k = \alpha_{ik}(a_i)$ and $b_k = \alpha_{jk}(b_j)$. Then $a = \alpha_k(a_k)$ and $b = \alpha_j(b_k)$. If L is an R-module and α_k is R-linear, then $ra = r\alpha_k(a_k) = \alpha_k(ra_k)$ and $a + b = \alpha_k(a_k) + \alpha_k(b_k) = \alpha_k(a_k + b_k)$. So there exists at most one R-module structure on L which makes each α_i R-linear.

Conversely define $ra = \alpha_k(ra_k)$ and $a + b = \alpha_l(a_k + b_k)$. Since the α_{ij} are R-linear this turns out to be well defined and gives an R-module structure on L which makes each each α_i R-linear. □

Lemma 2.6.13 [**infinite tensor**] *Let $(M_i, i \in I)$ be a family of R-modules. For $n, m \in \textcircled{\small$\Pi$}_I M_i$ define $n \sim m$ if $n_i = m_i$ for almost all $i \in I$. For $J \subseteq I$, let $J' = I \setminus J$. For $m \in \textcircled{\small$\Pi$}_{i \in I} M_i$ and $\overline{m}$ be the equivalence class of m with respect to $\sim$ (and so $\overline{m} = m + \bigoplus_{i \in I} M_i$). Let $x \in \overline{\textcircled{\small$\Pi$}_I M_i}$.*

(a) [**b**] *Let $\mathcal{P}_f(I)$ be the set of finite subsets of I. Put*

$$\mathcal{F} = \{(n, J) \mid J \in \mathcal{P}_f(I), n \in \mathop{\textcircled{$\scriptstyle\Pi$}}_{i\in J'} M_i\}$$

and define $(n, J) \leq (p, K)$ if $J \subset K$ and $n \mid_{K'} = p$. For $e = (p, J)$ and $f = (q, K) \in \mathcal{F}$ with $e \leq f$ define

$$\alpha_{ef} : \bigotimes_{j\in J} M_j \to \bigotimes_{k\in K} M_k, w \to w \otimes (\otimes p \mid_{K\setminus J})$$

also put

$$\mathcal{F}(x) = \{(n, J) \mid n = m \mid_{J'} \text{ for some } m \in x\}.$$

Then $\mathcal{F}(x)$ is a direct set and $(\alpha_{e,f} \mid e \leq f \in \mathcal{F}(x))$ is a direct system.

(b) [**c**] *Put $F(x) = \varinjlim \mathcal{F}(x)$. Then*

$$\bigotimes_{i\in I} M_i \cong \bigoplus_{x\in\overline{\mathop{\textcircled{$\scriptstyle\Pi$}}_I M_i}} F(x).$$

Proof:

(a) is readily verified.

(b) For $x \in \overline{\mathop{\textcircled{$\scriptstyle\Pi$}}_{i\in I} M_I}$ let $\big(\beta_{(n,J)} : \bigotimes_J M_j \to F(x) \mid (n, J) \in \mathcal{F}(x)\big)$ be the direct limit of $(\alpha_{ef} \mid e \leq f \in \mathcal{F}(x)\}$. Define

$$f_x : \mathop{\textcircled{$\scriptstyle\Pi$}}_I M_i \to F(x), \quad m \to \begin{cases} f_x(m) = \beta_{(m,\emptyset)}(\otimes()) & \text{if } m \in x \\ 0 & \text{if } m \notin x \end{cases}$$

Define

$$f : \mathop{\textcircled{$\scriptstyle\Pi$}}_I M_i \to \bigoplus_{x\in\overline{\mathop{\textcircled{$\scriptstyle\Pi$}}_I M_i}} F(x), \quad m \to (f_x(m))_x$$

To show that f is R-multilinear we need to show that each f_x is R-multilinear. Let $j \in I$, $u \in M_j$, $J = \{j\}$ and $n \in \mathop{\textcircled{$\scriptstyle\Pi$}}_{k\in J'} M_k$. Put $m = (u, n) \in \mathop{\textcircled{$\scriptstyle\Pi$}}_{i\in I} M_i$. Note that $(m, \emptyset) \leq (n, J)$. Also

$$\alpha_{(m,\emptyset)(n,J)}(\otimes()) = (\otimes()) \otimes (\otimes\, m \mid_J) = \otimes u = u$$

where we did identify $\bigotimes_{j\in J} M_j$ with M_j. Thus

$$\beta_{(m,\emptyset)}(\otimes()) = \beta_{(n,J)}(\alpha_{(m,\emptyset)(n,J)}(\otimes())) = \beta_{(n,J)}(u)$$

Note that $\overline{m}$ only depends on n but not on u. If $x \neq \overline{m}$ we have $f_x(u) = 0$ and so f_x is linear in the j-coordinate. If $x = \overline{m}$ the above calculations show that $f_x(u, n) = \beta_{n,J}(u)$. Since $\beta_{n,J}$ is R-linear, we see that f_x is R-linear in the j-coordinate.

So f is indeed R-multilinear. Now let $g : \mathop{\textcircled{Π}}_{i\in I} M_i \to N$ be any R-multilinear map. Let $x \in \overline{\mathop{\textcircled{Π}}_I M_i}$. For $e = (p, J) \in \mathcal{F}(x)$ define $h_e = \otimes g_p$, so

$$h_e : \bigotimes_{j\in J} M_j \to N \text{ with } \otimes q \to g(q, p)$$

for all $q \in \mathop{\textcircled{Π}}_{j\in J} M_j$

If $e = (p, J) \leq f = (q, K) \in \mathcal{F}(x)$, then for all $w \in \mathop{\textcircled{Π}}_{j\in J} M_j$,

$$\begin{array}{rclcl} h_e(\otimes w) & = & g(w, p) & = & g(w, p\,|_{K\setminus J}, p\,|_{K'}) \quad = \quad g(w, p\,|_{K\setminus J}, q) \\ & & & = & h_f((\otimes w) \otimes (p\,|_{K\setminus J})) \quad = \quad h_f(\alpha_{ef}(\otimes w)) \end{array}$$

Thus $h_e = h_f \circ \alpha_{ef}$ and by definition of the direct limit there exists a unique $h_x : F(x) \to N$ with $h_x \circ \beta_f = h_f$ for all $f \in \mathcal{F}(x)$. Define

$$h : \bigoplus_{x\in\overline{\mathop{\textcircled{Π}}_I M_i}} F(x) \to N, (f_x)_x \to \sum_x h_x(w_x).$$

Let $m \in \mathop{\textcircled{Π}}_I M_i$. If $x \neq \overline{m}$, then $f_x(m) = 0$. Thus

$$\begin{array}{rclclcl} h(f(m)) & = & h_{\overline{m}}(f_{\overline{m}}(m)) & = & h_{\overline{m}}(\beta_{(m,\emptyset)})(\otimes()) & = & h_{m,\emptyset}(()) \\ & & & = & g(m, ()) & = & g(m) \end{array} .$$

The uniqueness of h is readily verified. □

Corollary 2.6.14 [**infinite tensor ii**] *Let $(M_i, i \in I)$ be a family of R-modules. For $x \in \overline{\mathop{\textcircled{Π}}_I M_i}$ let $M_x = \langle \overline{m} \mid m \in x\rangle_{\mathbb{Z}}$. Then*

(a) [**a**] $\bigotimes_I M_i = \bigoplus_x M_x$.

(b) [**b**] *For $e = (p, J) \in \mathcal{F}(x)$ define $\alpha_e : \bigotimes_J M_j \to M_x, w \to w \otimes (\otimes p))$. Then $(\alpha_e, e \in \mathcal{F}(x))$ is a direct limit for $(\alpha_{ef}; e \leq f \in \mathcal{F}(x))$.*

Proof: Since any two tensor products of $(M_i, i \in I)$ are isomorphic we may use the tensor product constructed in 2.6.13. Also we identify $F(x)$ with its image in $\bigotimes_I M_i = \bigoplus_x F(x)$. Since $f_x(m) = 0$ for $x \neq \overline{m}$ we then have $\otimes m = f(m) = f_{\overline{m}}(m) = \beta_{(m,\emptyset)}(\otimes())$. So

$$\otimes m = \beta_{(m,\emptyset)}(\otimes())$$

and $\otimes m \in F(\overline{m})$. Thus

$$\bigotimes_I M_i = \langle \overline{m} \mid m \in \mathop{\textcircled{Π}}_I M_i\rangle = \sum_x M_x \leq \sum_x F(x) = \bigoplus_x F(x).$$

So $M_x = F(x)$ and (a) holds.

Also for $e = (p, J) \in \mathcal{F}(x)$ and $w \in \textcircled{$\Pi$}_J M_j$,

$$\alpha_e(\otimes w) = (\otimes w) \otimes (\otimes p) = \otimes(w, p) = \beta_{((w,p),\emptyset)}(\otimes())$$

Since $(w, p), \emptyset) \leq e = (p, J)$, we have $\beta_e \circ \alpha_{(w,p),e)} = \beta_(w, p)$. Also $\alpha_{((w,p),\emptyset)(p,J)}(\otimes()) = (\otimes()) \otimes (\otimes w) = \otimes w$ and so

$$\alpha_e(\otimes w) = \beta_{((w,p),\emptyset)}(\otimes()) = \beta_e(\alpha(w, p)(\otimes()) = \beta_e(\otimes w)$$

Hence $\alpha_e = \beta_e$ and so (b) holds. □

As an exercise the reader might prove 2.6.14 without referring and to 2.6.13 and thereby giving an alternative proof for 2.6.13.

Definition 2.6.15 [**def:cofinal**] *A subset J of a directed set I is called cofinal if for all $i \in I$ there exists $j \in J$ with $i \leq j$.*

Lemma 2.6.16 [**cofinal**] *Let I be a direct set and J a cofinal subset. Then J is directed. Let $(\alpha_{ik} : M_i \to M_k$ be a direct system and $(\alpha_j : M_j \to L)$ a family of functions with $\alpha_j = \alpha_k \circ \alpha_{jk}$ for all $j, k \in J$ with $i \leq k$. Then $(\alpha_j; j \in J$ can be uniquely extended to a family $(\alpha_k : M_k \to L)$ a family of functions with $\alpha_i = \alpha_k \circ \alpha_{jk}$ for all $i, k \in I$ with $i \leq k$. In particular $\lim\limits_{\rightarrow}{}_{i \in I} M_i \cong \lim\limits_{\rightarrow}{}_{j \in J} M_j$.*

Proof: Let $j, k \in J$. Then there exists $n \in I$ with $j, k \leq n$ and $m \in J$ with $n \leq m$. So $j, k \leq m$ and J is directed.

Suppose that $(\alpha_i; i \in I)$ is an extension of $(\alpha_j; j \in J)$. let $i \in I$ and $m_i \in M_i$. Pick $j \in J$ with $i \leq j$. Then

$$(*) \qquad \alpha_i(m_i) = \alpha_j(\alpha_{ij}(m_j))$$

and so α_i is uniquely determined. To show existence we define α_i via $(*)$. This is well defined: Let $j, k \in J$ with $i \leq j, k$ and choose $m \in J$ with $j, k \leq n$. Then

$$\begin{aligned} \alpha_j(\alpha_{ij}(m_i)) &= \alpha_n(\alpha_{jn}(\alpha_{ij}(m_i))) &= \alpha_n(\alpha_{in}(m_i)) \\ &= \alpha_n(\alpha_{kn}(\alpha_{ik}(m_i))) &= \alpha_k(\alpha_{ik}(m_i)) \end{aligned}$$

So α_i is well defined. Now let $i \leq k \in I$ and pick $j \in J$ with $k \leq j$. Then

$$\alpha_k(\alpha_i(m_i)) = \alpha_j(\alpha_{jk}(\alpha_i(m_i))) = \alpha_j(\alpha_{ij}(m_i)) = \alpha_i(m_i)$$

so $\alpha_i = \alpha_k \circ \alpha_{ik}$. □

Lemma 2.6.17 [**easy f(x)**] *Let $(M_i, i \in I)$ be a family of R-modules and $m \in \text{\textcircled{Π}}_{i\in I} M_i$. For $J \subseteq K \subseteq I$ define*

$$\alpha_{JKm} : \bigotimes_{j\in J} M_j \to \bigotimes_{k\in K} M_k, w \to w \otimes (\otimes_{k\in K\setminus J} m_k)$$

Also put $\mathcal{F}(m) = (\alpha_{JKm} \mid J \subseteq K \in \mathcal{P}_f(I))$.

Then $\mathcal{F}(m)$ is a directed system and $F(m) := \varinjlim \mathcal{F}(m) \cong F(\overline{m})$.

Proof: Let $J \subseteq K \in \mathcal{P}_f(I)$. Then $\tilde{J} := (m\mid_{J'}, J) \in \mathcal{F}(\overline{m})$. Moreover, $\tilde{J} \leq \tilde{K}$ and $\alpha_{JKm} = \alpha_{\tilde{J}\tilde{K}}$. Let $(p, J) \in \mathcal{F}(\overline{m})$. Then there exists $n \in \overline{m}$ with $n\mid_J = p$. Since $n \sim m$, there exists a $K \in \mathcal{P}_f(I)$ with $J \subseteq K$ and $m_{K'} = n_{K'} = p_{K'}$. Thus $(p, J) \leq \tilde{K}$. So $\mathcal{F}(m)$ is isomorphic to the cofinal subsystem $(\alpha_{\tilde{I}\tilde{J}} \mid J \subseteq K \in \mathcal{F}(I)\}$ of $\mathcal{F}(\overline{m})$. Thus the lemma holds.

Lemma 2.6.18 [**structure of f(m)**] *Let $(M_i, i \in I)$ be a family of R-modules and $m \in \text{\textcircled{Π}}_{i\in I} M_i$. Suppose that for each $i \in I$, M_i is free R-module. Let J be a finite subset of I.*

(a) [**a**] *Let $k \in J'$ and $K = J \cup \{k\}$. Then*

$$\ker \alpha_{JKm} = \mathrm{A}_R(m_k) \cdot \bigotimes_J M_j$$

(b) [**b**] *Suppose that R is an integral domain and $m_i \neq 0$ for all $i \in I$. Then for all $K \in \mathcal{P}_f(I)$ with $J \leq K$, α_{JKm} is $1-1$. Moreover, α_{JIm} is $1-1$.*

Proof: (a) For $x \in \bigotimes_{j\in J} M_j$ we have $\alpha_{JKm}(x) = x \otimes m_k$. By 2.6.4(c), $\otimes_{j\in J} M_j$ is free with basis say $\mathcal{D}$. Let $\mathcal{B}$ be a basis for M_k and let $m_k = \sum_{b\in\mathcal{B}} r_b b$. Then

$$\alpha_{JKM}(\sum_{d\in\mathcal{D}} s_d d) = \sum_{d\in\mathcal{D}, b\in\mathcal{B}} r_b s_d \cdot d \otimes b.$$

Since $(d \otimes b \mid d \in \mathcal{D}, b \in \mathcal{B})$ is a basis for $\bigotimes_{i\in K} M_i$ we conclude that

$$w = \sum_{d\in\mathcal{D}} s_d d \in \ker \alpha_{JKm}$$

iff $r_b s_d = 0$ for all $b \in \mathcal{B}, d \in \mathcal{D}$. Note that this is the case iff $s_d m_k = 0$ for all $d \in \mathcal{D}$ and iff $w \in \mathrm{A}_R(m_k) \cdot \bigotimes_{j\in J} M_j$. □

(b) Let $J \subseteq X \subseteq K$ with $|K \setminus X| = 1$. By induction we may assume that α_{JXm} is $1-1$. By (a) also α_{XKm} is $1-1$. Hence $\alpha_{JKm} = \alpha_{XKm} \circ \alpha_{JX}$ is $1-1$. 2.6.10 implies that also α_{JIm} is $1-1$. □

Lemma 2.6.19 [**more structure of f(m)**] *Let $\mathbb{K}$ be a field, $(M_i, i \in I)$ a family of $\mathbb{K}$-spaces. Let $m = (m_i) \in \bigoplus_{i\in I} M_i$ with $m_i \neq 0$ for all $i \in I$. For each $i \in I$ choose a basis $\mathcal{B}_i$ of M_i with $m_i \in \mathcal{B}_i$. Then*

$$\mathcal{D} := (\otimes n \mid n \in \bigoplus_{i\in I} \mathcal{B}_i, n \sim m).$$

is a basis for $F(m)$.

Proof: Let $w \in F(m)$. Then $w \in \mathrm{Im}_{\alpha_{JIm}}$ for a finite subset J of I. Since $\otimes_J \mathcal{B}_j$ spans $\bigotimes_J M_j$ we conclude that w is in $\mathbb{K}\mathcal{D}$.

Next let $n_1, n_2, \ldots, n_t \in \bigoplus_{i\in I} \mathcal{B}_i$ be pairwise distinct with $n_s \sim m$ for all s. Then there exists a finite subset J of I with $n_s \mid_{J'} = m_{|'_J}$ for all s. Let $u_s = n_s \mid_J$. Then $\otimes n_s = \alpha_{JIm}(\otimes u_s$. Since $\otimes_J \mathcal{B}_j$ is linearly independent in $\bigotimes_J M_j$, $(\otimes u_1, \ldots, \otimes u_t)$ is linearly independent. Since α_{JIm} is 1-1 also $(\otimes n_1, \ldots, \otimes n_t)$ is linearly independent. Thus $\mathcal{D}$ is linearly independent, proving the lemma. □

Lemma 2.6.20 [**tensor of algebras**] *Let R be a commutative ring and let A and B be R-algebras. Then there exits a unique R-multilinear binary operation*

$$A \otimes_R B \times (A \otimes_R B) \to A \otimes_R B \textit{ with } (a \otimes b) \cdot (c \otimes d) = (ac) \otimes (bd)$$

for all $a, c \in A, b, d \in B$. Moreover, $A \otimes B$ is a $Z(A) \otimes Z(B)$-algebra.

Proof: For a fixed $(c, d) \in A \times B$, the map

$$A \times B \to A \otimes B, (a, b) \to (ac) \otimes (bd)$$

is R-multilinear and we obtain a uniquely determined R-linear map

$$f_{cd} : A \otimes B \to A \otimes B, a \otimes b \to (ac) \otimes (bd)$$

The map $A \times B \to \mathrm{Hom}_R(A \otimes B, A \otimes B), (c, d) \to f_{cd}$ is R-multilinear and so we obtain a uniquely determined R-linear map

$$f : A \otimes B \to \mathrm{Hom}_R(A \otimes B, A \otimes B), \quad c \otimes d \to f_{cd}$$

For $x, y \in A \otimes B$ define $xy = f(y)(x)$. The lemma is now readily verified. □

Lemma 2.6.21 [**extension of scalars**] *Let R and S be commutative fields with $R \leq S$. Let A be an R-algebra and M an A-module. Then there exists a unique R-multilinear module structure*

$$S \otimes_R A \times S \otimes_R M \to S \otimes_R M \textit{ with } (s \otimes a) \cdot (t \otimes m) = st \otimes am.$$

for all $s, t \in S, a \in A, m \in M$.

Proof: Readily verified. □

Definition 2.6.22 [**def:absolutely simple**] *Let $\mathbb{K}$ be a field, A an $\mathbb{K}$-algebra and M an A-module. Then M is called absolutely simple over $\mathbb{K}$ if for all fields $\mathbb{F}$ with $\mathbb{K} \leq \mathbb{F}$, $\mathbb{F} \otimes_{\mathbb{K}} M$ is simple $\mathbb{F} \otimes_{\mathbb{K}} A$-module.*

Lemma 2.6.23 [**absolute and end**] *Let $\mathbb{K}$ be a field, A an $\mathbb{K}$-algebra and M an simple A-module. Then M is absolutely simple iff* $\mathrm{End}_A(M) = \mathbb{K}$.

Proof: Let $\mathbb{F}$ be a subfield of $\mathrm{End}_A(M)$ with $\mathbb{K} \leq \mathbb{F}$. Since $\mathbb{F}\otimes_M \to M, (f,m) \to f(m)$ is $\mathbb{K}$-multilinear and so we obtain a unique $\mathbb{K}$-linear map

$$\alpha : F \otimes_{\mathbb{K}} M \to M, f \otimes m \to f(m).$$

Also observe that M is a $F \otimes_K A$ module via $(f \otimes a) \cdot m = f(am)$ for all $f \in F, a \in A, m \in M$.

Let $f, g \in \mathbb{F}, a \in A$ and $m \in M$. Then

$$\begin{aligned} \alpha((f \otimes a)(g \otimes m)) &= \alpha(fg \otimes am) = (fg)(am) = f(g(am)) \\ &= f(ag(m)) = f(a\alpha(g \otimes m)) = (f \otimes a) \cdot \alpha(g \otimes m) \end{aligned}$$

Thus α is $F \otimes A$-linear. Since $f \mid 1 \otimes M$ is onto we have $F \otimes M = 1 \otimes M + \ker \alpha$.

If M is absolutely simple over R, we get $\ker \alpha = 0$ and $F \otimes M = 1 \otimes M$. Let $\mathcal{B}$ be a $\mathbb{F}$-basis for M. Then $1 \otimes \mathcal{B}$ is an $\mathbb{F}$-basis for $\mathbb{F} \otimes_{\mathbb{K}} M$ and spans $1 \otimes M$ as a $\mathbb{K}$-space. Hence $\mathbb{F} = \mathbb{K}$. Let $d \in \mathbb{D} := \mathrm{End}_A(M)$ and put $\mathbb{F} = \mathbb{K}(d)$. Since $\mathbb{K} \leq Z(\mathbb{D})$, $\mathbb{F}$ is a field. So $d \in \mathbb{F} = \mathbb{K}$ and so $\mathbb{D} = \mathbb{K}$.

Conversely suppose that $\mathrm{End}_A(M) = \mathbb{K}$. The by the Jacobson's Density Theorem, A is dense on M with respect to $\mathbb{K}$. Let $\mathbb{F}$ be a field extension of $\mathbb{K}$ and let $v, w \in \mathbb{F} \otimes_{\mathbb{K}} M$ with $v \neq 0$. Then there exists $e_1, \ldots e_n, f_1, \ldots f_m$ in $\mathbb{F}$ and $v_1, v_2, v_n, w_1, \ldots, w_m \in m$ with

$$v = \sum_{i=1}^{n} e_i \otimes v_i \text{ and } w = \sum_{i=1}^{m} f_i \otimes w_i$$

We may assume without loss that the v_i are linearly independent over $\mathbb{K}$ and that $e_1 \neq 0$. Since A is dense on M with respect to $\mathbb{K}$, there exists $a_i \in A$ for $1 \leq i \leq m$ with $a_i v_1 = w_i$ and $a_i v_i = 0$ for all $2 \leq i \leq n$. Put $d := \sum_{i=1}^{m} \frac{f_i}{e_1} \otimes a_i \in \mathbb{F} \otimes A$. Then $dv = w$.

We conclude that $(\mathbb{F} \otimes_{\mathbb{K}} A)v = \mathbb{F} \otimes_{\mathbb{K}} M$ and so $\mathbb{F} \otimes_{\mathbb{K}} M$ is a simple $\mathbb{F} \otimes_{\mathbb{K}} A$-module. □

Corollary 2.6.24 [**splitting field of a module**] *Let $\mathbb{K}$ be a field, A a $\mathbb{K}$-algebra and M a simple A-module. Let $\mathbb{F}$ be a maximal subfield of* $\mathrm{End}_A(M)$. *Then M is an absolutely simple $\mathbb{F} \otimes_{\mathbb{K}} A$-module.*

Proof: Let $\mathbb{D} = \mathrm{End}_A(M)$. We have $\mathrm{End}_{\mathbb{F}\otimes_{\mathbb{K}}A}(M) = \mathrm{End}_A(M) \cap \mathrm{End}_{\mathbb{F}}(M) = C_{\mathrm{D}}(\mathbb{F})$. By maximality of $\mathbb{F}$, $C_{\mathbb{D}}(\mathbb{F}) = \mathbb{F}$. Thus 2.6.23 implies that M is an absolutely simple $\mathbb{F} \otimes_{\mathbb{K}} A$-module. □

Corollary 2.6.25 [**algebraically to absolute**] *Let $\mathbb{K}$ be a algebraically closed field, A a $\mathbb{K}$-algebra and M a simple A-module. If M is finite dimensional over $\mathbb{K}$, then M is an absolutely simple A-module over $\mathbb{K}$.*

Proof: By 2.5.3 $\mathrm{End}_A(M) = \mathbb{K}$ and so 2.6.23 implies that M is absolutely simple over $\mathbb{K}$. □

2.7 Induced and Coinduced Modules

Definition 2.7.1 [**def:induced**] *Let R be a ring, S a subring of R and W an S module, M an R-module.*

(a) [**a**] *Let $f : W \to M$ be S-linear. We say that f is induced from W to R provided that whenever N is an R-module and $g : W \to N$ is S-linear, then there exists a unique R-linear map $h : M \to N$ with $g = h \circ f$. In this case M is called the R-module induced from W to R and is denoted by $W{\uparrow}^R_S$. f is denoted by $\iota^S_R(W)$ and h by $h{\uparrow}^S_R$.*

(b) [**b**] *Let $f : M \to W$ be S-linear. We say that f is coinduced from W to R provided that whenever N is an R-module and $g : N \to W$ is S-linear, then there exists a unique R-linear map $h : N \to M$ with $g = f \circ h$. In this case M is called the R-module coinduced from W to R and is denoted by $W{\Uparrow}^R_S$. f is denoted by $\pi^S_R(W)$ and h by $h{\Uparrow}^S_R$.*

Lemma 2.7.2 [**induced**] *Let R be a ring, S a subring of R and W an S module. View R as a right S module via right multiplication.*

(a) [**a**] *There exists a unique R-module structure*

$$R \times R \otimes_S W \to R \otimes_S W \text{ with } r(t \otimes w) = rt \otimes w$$

for all $r, t \in R, w \in W$.

(b) [**b**] *The map $f : W \to R \otimes_S W, w \to 1 \otimes w$ is induced from W to R.*

(c) [**c**] *Any map induced from W to R is isomorphic to f.*

Proof: (a) Let $r, t \in R, s \in S$ and w in W. Then $t(rs) \otimes w = (tr)s \otimes w = tr \otimes sw$ and so the map $\alpha_t : R \times W \to R \otimes_S W, (r, w) \to tr \otimes w$ is S balanced. The universal property of the tensor product implies that (a) holds.

(b) Let N be an R-module and $g : W \to N$ an S-linear map. Then the map $R \times W \to N, (r, w) \to rg(w)$ is S balanced. So by definition of the tensor product there exists a $\mathbb{Z}$-linear map $h : R \otimes_S W \to N$ with $r \otimes w \to rg(w)$. Then $h(f(w)) = h(1 \otimes w) = 1g(w) = g(w)$ and so $h \circ f = g$. Moreover $th(r \otimes w) = t(rg(w)) = (tr)g(w) = h(tr \otimes w) = h(t \cdot r \otimes w)$ and so h is R-linear. Thus (b) holds.

(c) is obvious. □

Lemma 2.7.3 [**coinduced**] *Let R be a ring, S a subring of R and W an S module. View R as S-module via left multiplication.*

(a) [**a**] $\mathrm{Hom}_S(R, W)$ *is an R-module via $(t\alpha)(r) = \alpha(rt)$ for all $r, t \in R, \alpha \in \mathrm{Hom}_S(R, W)$.*

(b) [**b**] *The map $f : \mathrm{Hom}_S(R, W) \to W, \alpha \to \alpha(1)$ is S-linear and coinduced from W to R.*

(c) [**c**] *Any map coinduced from W to R is isomorphic to f.*

Proof: (a) We first need to verify that $t\alpha$ is S-linear. Let $s \in S$ and $r \in R$. Then

$$(t\alpha)(sr) = \alpha((sr)t) = \alpha(s(rt)) = s\alpha(rt) = s \cdot (t\alpha)(r)$$

So indeed $t\alpha \in \mathrm{Hom}_S(R, W)$. To check that this is an R-module structure let also $u \in R$. Then

$$((ut)\alpha)(r) = \alpha(r(ut)) = \alpha((ru)t) = (t\alpha)(ru) = (u \cdot (t\alpha))(r)$$

So $(ut)\alpha = u(t\alpha)$ and (a) is proved.

(b) We have $f(s\alpha) = (s\alpha)(1) = \alpha(s1) = s \cdot \alpha(1) = s \cdot f(\alpha)$ and so f is S-linear. Let N be an R-module and $g : N \to W$ be S-linear. Define $h : N \to \mathrm{Hom}_S(R, W)$ by $h(n)(r) = r \cdot g(n)$. We have

$$h(n)(sr) = (sr) \cdot g(n) = s \cdot (r \cdot g(n)) = s \cdot h(n)(r)$$

and so $h(n)$ is indeed S-linear. Also

$$f(h(n)) = h(n)(1) = 1 \cdot g(n) = g(n)$$

and so $f \circ h = g$.

(c) Obvious. □

Proposition 2.7.4 (Frobenius Reciprocity) [**frobenius rec**] *Let R and S be rings with $S \leq R$, W an S- and V an R-module.*

(a) [**a**] *The map* $\mathrm{Hom}_R(W{\uparrow}_R^S, V) \to \mathrm{Hom}_S(W, V), \alpha \to \alpha \circ \iota_R^S(W)$ *is a $\mathbb{Z}$-isomorphism with inverse $\beta \to \beta{\uparrow}_R^S$.*

(b) [**b**] *The map* $\mathrm{Hom}_R(V, W\uparrow_R^S) \to \mathrm{Hom}_S(V, W), \alpha \to \pi_R^S(W) \circ \alpha$ *is a mbZ-isomorphism with inverse* $\beta \to \beta\Uparrow_R^S$.

Proof: This proposition merely rephrases the definitions of induced and coinduced maps. □

Lemma 2.7.5 [**induced for r free over s**] *Let R and S be rings with $S \leq R$ and let W be an R-module.*

(a) [**a**] *Suppose that R is a free right S-module with basis $\mathcal{B}$. Then the map*

$$\bigoplus_{\mathcal{B}} W \to W\uparrow_R^S, \quad (w_b) \to \sum_{b\in\mathcal{B}} b \otimes w_b$$

is a $\mathbb{Z}$-isomorphism.

(b) [**b**] *Suppose that R is a free S-module with basis $\mathcal{B}$. Then the map*

$$W\Uparrow_R^S \to \mathop{\text{\textcircled{Π}}}\limits_{\mathcal{B}} W, \quad \alpha \to \alpha \mid \mathcal{B}$$

is a $\mathbb{Z}$-isomorphism.

Proof: (a) We have $R = \bigoplus_{b\in\mathcal{B}} bS$ and $bS \otimes_S W \cong W$.

(b) Follows immediately from the definition of an S-basis. □

Definition 2.7.6 [**def:imprimitive**] *Let R be a ring, G a group and M an RG-module.*

(a) [**a**] *A* system of imprimitivity *for RG on M is a tuple $(M_b \mid b \in \mathcal{B})$ such that*

- *(a)* [**a**] *$\mathcal{B}$ is a G-set.*
- *(b)* [**b**] *For $b \in \mathcal{B}$, M_b is a non-zero R-submodules of M.*
- *(c)* [**c**] *$gM_b = M_{gb}$ for all $g \in G, b \in \mathcal{B}$*
- *(d)* [**d**] *$M = \bigoplus_{b\in\mathcal{B}} M_b$.*

(b) [**b**] *A system of imprimitivity is called* proper *if $|\mathcal{B}| > 1$.*

(c) [**c**] *An RG- module with a proper system of imprimitivity is called* imprimitive.

(d) [**d**] *A RG- module M is called* primitive *if M is simple and not imprimitive.*

Suppose that $(M_b \mid b \in \mathcal{B})$ fulfills (a:a)-(a:c) of 2.7.6. Then $\mathcal{M} = \{M_b \mid b \in \mathcal{B}\}$ is a G-invariant set of non-zero R-submodules of M. Moreover $M = \bigoplus_{b\in\mathcal{B}} M_b$ iff $M = \bigoplus \mathcal{M}$ and $M_a \neq M_b$ for all $a, b \in \mathcal{B}$.

In particular, if $\mathcal{M}$ is G-invariant set of R-submodules of M, then $(W \mid W \in \mathcal{M})$ is a system of imprimitivity for RG on M.

Lemma 2.7.7 [**submodules of induced**] *Let R be a ring, G a group, M an RG-module and $(M_b \mid b \in \mathcal{B})$ a system of imprimitive for RG on M. Fix $a \in B$ and let W_a be non-zero $C_G(a)$ submodule of M_a. Put $W = RGW_a$. Then $W \cap M_a = W_a$, $W \leq \sum_{b \in Ga} M_a$ and $(W \cap M_a \mid b \in Ga)$ is a system of imprimitivity for G on W.*

Proof: For $g \in G$ put $W_{ga} = gW_a$. Since $C_G(a)W_a = W_a$, this is well defined. Then for all $b \in Ga$, $W_b \leq M_b$ and so

$$W = GW_a = \sum_{g \in G} gW_a = \sum_{b \in Ga} W_b = \bigoplus_{b \in Ga} W_b$$

Hence $W \cap M_b = W_b$ for all $b \in \mathcal{B}$ and the lemma is proved. □

Lemma 2.7.8 [**imprimitive and induced**] *Let R be ring, G a group and V an RG-module.*

(a) [**a**] *If $H \leq G$ and W is a non zero RH-module with $V = W{\uparrow}_H^G$, then $\iota_H^G(W)$ is $1-1$ and $(T \otimes W \mid T \in G/H)$ is a system of imprimitivity for G on V.*

(b) [**b**] *Let $(V_b, b \in \mathcal{B})$ be a system of imprimitivity for RG on V. Let $b \in \mathcal{B}$. Then V_b is an $RC_G(b)$-submodule and there exists a unique RG-linear map*

$$\rho : V_b{\uparrow}_{C_G(b)}^G \to V \text{ with } \iota(v) = v$$

for all $v \in V_b$, where $\iota = \iota_{C_G(b)}^G(V_b)$.

Moreover, ρ is $1-1$ and $\operatorname{Im}\rho = \sum_{a \in Gb} V_a$. In particular, if G is transitive on $\mathcal{B}$, then ρ is an isomorphisms.

Proof: (a) Let $\mathcal{T}$ be a left transversal for H on G (that is $(tH \mid t \in \mathcal{T})$ is a partition of G) with $1 \in \mathcal{T}$. Clearly $\mathcal{T}$ is a basis for RG as a right RH-module. Then by 2.7.5(a), $\alpha : \bigoplus_{\mathcal{T}} W \to V, (w_t) \to \sum t \otimes w_t$ is a $\mathbb{Z}$-isomorphism. In particular, $\iota_H^G(W) : W \to V, w \to 1 \otimes w$ is $1-1$ and $V = \bigoplus_{t \in \mathcal{T}} t \otimes W$. Since $th \otimes W = t \otimes hW = t \otimes W$ for all $h \in H$ we have $t \otimes W = tH \otimes W = (tH)(1 \otimes W)$ and so

$$V = \bigoplus (T \otimes W) \mid T \in G/H)$$

Also $g(T \otimes W) = gT \otimes W$ and so (a) holds.

(b) Put $H = C_G(b)$ and $W = V_b$. Then for all $h \in H$, $hb = b$ and so $hV_b = V_b$. So W is an RH-submodule of V. Let $j : W \to V$ be the inclusion map. The uniqueness and existence of ρ follows from the definition of the induced module, namely $\rho = j{\uparrow}_H^G$. Let $\mathcal{T}$ be as in (a). Let $u \in W{\uparrow}_H^G$. Then $u = \sum_{t \in \mathcal{T}} t \otimes w_t$ for some $w_t \in W$ and so

$$0 = \rho(u) = \rho(\sum_{t \in \mathcal{T}} t \otimes w_t) = \sum_{t \in \mathcal{T}} t\rho(1 \otimes w_t) = \sum_{t \in \mathcal{T}} tw_t$$

Since $w_t \in V_b$, $tw_t \in V_{tb}$. Conversely if $a \in Gb$ and $m \in V_b$, then $a = tb$ for some $t \in \mathcal{T}$ and $t^{-1}m \in V_b$. Thus $\operatorname{Im}\rho = \sum_{a\in Gb} V_a$.

Suppose that $u \in \ker\rho$. Since $\mathcal{T}$ is transversal to $H = C_G(b)$ we have $tb \neq sb$ for all $t, s \in \mathcal{T}$. Thus $V = \bigoplus_{d\in\mathcal{B}} V_b$ implies $tw_t = 0$ for all $t \in \mathcal{T}$. Hence also $w_t = 0$ and $u = 0$. So ρ is 1-1. □

2.8 Tensor Induction and Transfer

Definition 2.8.1 [**def:rgi-module**] *G a group and I a G-set. Let R be a ring. A $G-I$-set $(M_i, i \in I)$ is called an $RG-I$-module provided that each M_i is an R-module and each $\rho_g(i), g \in G, i \in I$ is R-linear.*

Let M be an RG-module and $H \leq G$ and W an RH-submodule. Then $(TW \mid T \in G/H)$ is an $RG - G/H$-module. Here for $T \in G/H$, $TW = \{tw \mid t \in T, w \in T\} = tW$ for all $t \in T$.

Let $(M_i, i \in I)$ be a system of imprimitivity for G on M with respect to R.. Then $(M_i, i \in I)$ is an $RG - I$-module

Lemma 2.8.2 [**rg-i-module**] *Let R be a ring, G a group I a G-set and $(M_i, i \in I)$ an $RG - I$-module.*

(a) [**a**] *$\textcircled{$\Pi$}_I M_i$ is an RG-module via $g \cdot (m_i)_i = (gm_{g^{-1}i})$ for all $g \in G$ and $m = (m_i)_i \in \textcircled{Π}_I M_i$. Moreover, the action of G on $\bigcap_I M_i$ view as a subset of M is the same as the action of G on ${}_JM_i$.*

(b) [**b**] *$M := \bigoplus_I M_i$ is an RG-submodule of $\textcircled{$\Pi$}_I M_i$ and $(M_i, i \in I)$ is a system of imprimitivity for G on M with respect to R.*

(c) [**c**] *Suppose R is commutative, then $\bigotimes_I M_i$ is an RG-module via $g \otimes m = \otimes gm$ for all $g \in G, m \in \textcircled{Π}_{m_i}$.*

Proof: (a) By 1.2.11 G acts on $\textcircled{$\Pi$}_I M_i$ in the given way. This action is clearly R-linear. Let $\sigma_j : M_i \to \textcircled{Π}_I M_i$ be natural monomorphism, that is $\sigma_j(m_j) = (\delta_{ij}m_j$. Then $(g\cdot\sigma_j(m_j))_{gi} = g\delta_{ij}m_j$ and so $g \cdot \sigma = (\delta_{gi,j}gm_i) = \sigma_{gj}(gm_i)$, proving the last statement in (a).

(b) follows directly from (a).

(c) For $g \in G$ define $\alpha_g : \textcircled{$\Pi$}_I M_i \to \bigotimes_I^R M_i m \to \otimes gm$. This is R-multilnear and we obtain an R-linear map $\beta_g : \bigotimes_I M_i \to \bigotimes_I M_i, \otimes m \to \otimes gm$. Then $\beta_g(beta_h(\otimes m)) = \otimes ghm = \beta_{gh}(\otimes m)$ and so $\beta_{gh} = \beta_g\beta_h$. Thus G acts R-linearly on $\bigotimes_I M_i$. □

Lemma 2.8.3 [**basis for rg-i-module**] *Let R be a ring, G a group, I a G-set and $(M_i, i \in I)$ an $RG-I$-module. Suppose that G acts transitively on I and fix $k \in I$. Let $H = C_G(k)$. Let $i \in I$ and choose $r_i \in H$ with $i = r_ik$. Suppose that M_k is a free R-module with basis $\mathcal{A}$ and that for $h \in H$, $(h_{ab})_{(a,b)}$ is the matrix of $\rho_k(h)$ with respect to $\mathcal{A}$. Put $\mathcal{A}_i = r_i\mathcal{A}$. For $g \in G$ define $h(g,i) \in H$ by $gr_i = r_{gi}h(g,i)$*

(a) [**a**] *$\mathcal{A}_i$ is an R-basis for M_i.*

(b) [**b**] *Let $j = gi$. The matrix of $\rho_i(g)$ with respect to $\mathcal{A}_i$ and $\mathcal{A}_j$ is $(h(g,i)_{ab})_{(r_ia,r_jb)}$.*

(c) [**c**] *$\mathcal{A}_I := \biguplus_{i\in I}\mathcal{A}_i$ is an R-basis for $M = \bigoplus_I M_i$.*

(d) [**d**] *The matrix for g on M with respect to $\mathcal{A}_I$ is $(\delta_{gi,j}\, h(g,i)_{ab})_{(r_ia,r_jb)}$.*

(e) [**e**] *Suppose I is finite and R is commutative. Then $\otimes_I\mathcal{A}_i$ is an R- basis for $N := \bigotimes_I M_i$.*

(f) [**f**] *Suppose I is finite and R is commutative. Then the matrix for g on M with respect to $\otimes_{i\in I}A_i$ is $(\,\prod_{j\in I} h(g,j)_{a_jb_{gj}}\,)_{(\otimes r_ia_i,\otimes r_ib_i)}$.*

Proof: Recall first that if V, W are free R-modules with R basis $\mathcal{C}$ and $\mathcal{D}$ respectively, then the matrix $(k_{cd})_(c,d)$ of $f \in \mathrm{Hom}_R(V,W)$ is define by $f(c) = \sum_{d\in\mathcal{D}} k_{cd}d$.

(a), (c) and (e) are obvious.

(b) Since $gr_i = r_jh(g,i)$,

$$g\cdot r_ia = r_hh(g,i)a = r_h\sum_{b\in\mathcal{A}} h(g,i)_{ab}b = \sum_{b\in\mathcal{A}} h(g,i)_{ab}r_jb$$

(d) Follows from (b).

(f) Let $a\otimes_I A_i$. Then $a = \otimes r_ia_i$ for some $a_i \in \mathcal{A}$.

$$\begin{array}{rclcl} ga & = & g\otimes a_i & = & \otimes g r_{g^{-1}i}a_{g^{-1}i} \\ & = & \otimes\sum_{b_i\in\mathcal{A}} h(g,g^{-1}i)_{(a_{g^{-1}i},b_i)}r_ib_i & = & \sum_{(b_i)\in\textcircled{Π}_I\mathcal{A}}\left(\prod_{i\in I} h(g,g^{-1}i)_(a_{g^{-1}i},b_i)\right)\otimes r_ib_i \\ & & & = & \sum_{(b_i)\in\textcircled{Π}_I\mathcal{A}}\Big(\prod_{j\in I} h(g,j)_(a_j,b_{gj})\Big)\otimes r_ib_i \end{array}$$

and so (e) holds. □

Definition 2.8.4 [**def:tensor induction**] *Let R be a commutative ring, G a group, $H \leq G$ and W an RH-module. For $T \in G/H$ let $T\otimes W = \{t\otimes w \mid t\in T, w\in W\} \leq RG\otimes_{RH} W$. The RG-module $\bigotimes_{T\in G/H} T\otimes W$ is called the tensor induced RG-module of W and is denoted by $W{\uparrow}_H^{\otimes G}$.*

Lemma 2.8.5 [**transfer hom**] *Let R be a commutative ring, G a group, $H \leq G$ with G/H finite. Let $\lambda : H \to R$ a multiplicative homomorphism. Let $(r_T, \mid T \in G/H)$ be a transversal and define*

$$\lambda^{\otimes G} : G \to R, g \to \prod_{T\in G/H}\lambda(h(g,T))$$

Let R_λ be the RH module with $R_\lambda = R$ as R-module and $hr = \lambda(h)r$ for all $r\in R, h\in H$.

(a) [**a**] $\det_{R_\lambda\uparrow_H^G}(g) = \lambda^{\otimes G}(g)\,\mathrm{sgn}_{G/H}(g)$.

(b) [**b**] $R_\lambda\uparrow_H^{\otimes G} \cong R_{\lambda^{\otimes G}}$ *as an RG-module.*

(c) [**c**] $\lambda^{\otimes G}$ *is a multiplicative homomorphism.*

Proof: (a) and (b) follow from 2.8.3. (c) follows from (a) and equally well from (b). □

2.9 Clifford Theory

Definition 2.9.1 [**def:homogeneous**] *Let R be a ring and M an R-module. Then M is called R-*homogeneous *if M is the direct sum of isomorphic simple R-modules. For S an isomorphism class of simple R-modules, M_S denotes the sum of all simple R-submodules contained in S. M_S is called a* homogeneous components *for R on M. Also let $S_M(R)$ be the sum of all simple R-submodules in M.*

Lemma 2.9.2 [**basic homogeneous**] *Let $\mathcal{S}$ the set of isomorphism classes of simple R-submodules of M.*

(a) [**a**] *$S_M(R)$ is the largest semisimple R-submodule if M.*

(b) [**b**] *Each $M_S, S \in \mathcal{S}$, is a maximal homogeneous R-submodule of M.*

(c) [**c**] $S_M(R) = \bigoplus_{S\in\mathcal{S}} M_S$.

Proof: (a) and (b) are fairly obvious. For (c) let $S \in \mathcal{S}$ and put $W = \sum\{M_T \mid S \neq T \in \mathcal{S}\}$. By 2.1.17(h) any simple submodule of M_S is contained in S and any simple submodule of W is contained in a member of $\mathcal{S} \setminus \{S\}$. Thus $W \cap M_S$ contains no simple R-submodule. By 2.1.18 $W \cap M_S$ is semisimple. So $W \cap M_S = 0$ and so (c) holds. □

Definition 2.9.3 [**def:conjugate modules**] *Let N be a group, R a ring and W and RN-module. For $\alpha \in \mathrm{Aut}(N)$, ${}^{\alpha}W$ denotes the RN-module with $W = {}^{\alpha}W$ as R-module and $n \cdot_\alpha w = \alpha^{-1}(n)w$ for all $n \in N, w \in W$. If G is a group with $N \trianglelefteq G$ and $g \in G$ we write ${}^{g}N$ for ${}^{\alpha}N$, where $\alpha : N \to N, n \to gng^{-1}$. So $n \cdot_g w = (g^{-1}ng)w$.*

Lemma 2.9.4 [**basic conjugate modules**] *Let R be an ring.*

(a) [**a**] *Let N a group, $\alpha \in \mathrm{Aut}(N)$ and V and W are RN-modules. Then $V \cong W$ iff ${}^{\alpha}V \cong {}^{\alpha}W$.*

(b) [**b**] *Let N a group, $\alpha, \beta \in \mathrm{Aut}(N)$ and V an RN-module. Then ${}^{\alpha}({}^{\beta}V) = {}^{\alpha\beta}V$.*

(c) [**c**] *Let G be a group, $N \trianglelefteq G$, V an RG-module, W an RN-submodule of V and $g \in G$. Then gW is an RN-submodule and $gW \cong {}^{g}W$.*

(a) and (b) Readily verified.

(c) Define $\rho : {}^gW \to V, w \to gw$. Then clearly ρ is 1-1, $\operatorname{Im}\rho = gW$ and ρ is R-linear. Now let $n \in N$ and w in W. Then

$$\rho(n \cdot_g w) = \rho((g^{-1}ng)w) = gg^{-1}ngw = ngw = n\rho(w)$$

Thus ρ is RN-linear. In particular, $gW = \operatorname{Im}\rho$ is an RN-submodule and (c) is proved. □

Definition 2.9.5 [**iso classes**] *Let R be a ring and M an R-module.*

(a) [**a**] *$[M]$ denotes the isomorphism class of M that is the class of all R-modules isomorphic to M.*

(b) [**b**] *If $R = K[N]$ for some ring K and some group N, and $\alpha \in \operatorname{Aut}(N)$, then ${}^\alpha[M] = [{}^\alpha M]$.*

Theorem 2.9.6 (Clifford) [**clifford**] *Let R be a ring, G a group, $N \trianglelefteq G$ and M and RG-module. Let $\mathcal{I}$ be the set of simple RN-submodules in $\mathcal{I}$. For $I \in \mathcal{I}$ let $[I]$ be the isomorphism class of I. Put $\mathcal{S} = \{[I] \mid I \in \mathcal{I}\}$.*

(a) [**a**] *$gM_S = M_{{}^gS}$ for all $S \in \mathcal{S}$ and $g \in G$.*

(b) [**b**] *$(g, S) \to {}^gS$ is an action of G on $\mathcal{S}$.*

(c) [**c**] *$(M_S \mid S \in \mathcal{S})$ is a system of imprimitivity for G on $S_M(RN)$.*

(d) [**d**] *$N_G(M_S) = N_G(S)$ for all $S \in \mathcal{S}$.*

(e) [**e**] *Suppose that $\mathcal{S} \neq \emptyset$ and let $S \in \mathcal{S}$. Then M is a simple RG-module iff each of the following holds:*

(a) [**a**] *$M = S_M(RN)$.*

(b) [**b**] *G acts transitively on $\mathcal{S}$.*

(c) [**c**] *M_S is a simple $RN_G(S)$-module.*

(f) [**f**] *If M is a simple RG-module and there exists $S \in \mathcal{S}$, then $M \cong M_S{\uparrow}^G_{N_G(S)}$.*

Proof: (a) $I \in \mathcal{I}$ with $I \in S$ and $g \in G$. Then by 2.9.4(c), $gI \in [{}^gI] = {}^gS$. Thus $gI \leq M_{{}^gS}$ and so $M_S \leq M_{{}^gS}$. Since g is invertible in G. By 2.9.4(b), ${}^{g^{-1}}({}^gS) = S$ and so also $M_{{}^gS} \leq M_S$ and so (a) holds.

(b) If T is an isomorphism class of RN-modules, then $T \in \mathcal{S}$ iff $M_T \neq 0$. So (a) implies, ${}^gS \in \mathcal{S}$ for all $g, S \in S$. (b) now follows from 2.9.4(b).

(c) Follows from (a), (b) and 2.9.2(c).

(d) By (a), $N_G(S) \leq N_G(M_S)$. Let $g \in N_G(M_S)$ and $I \in \mathcal{I}$ with $I \in S$. Thus gI is a simple RN-submodule isomorphic to ^{Ig}. Also $gI \leq M_S$ and so $[I^g] = S$ and $g \in N_G(S)$.

(e) Suppose first that M is a simple RG-module. By assumption $S_M(N) \neq 0$ and since M is simple for RG, $S_M(N) \neq 0$ and so $S_M(N) = M$. Let $S \in \mathcal{S}$ and W_S a nonzero $N_G(S)$-submodule of M_S. Put $W = RGW_S$. Since M is simple, $W = M$. By 2.7.7, $M = W \leq \sum_{T \in {}^GS} M_T$ and so G is transitive on $\mathcal{S}$. Also $W_S = W \cap M_S = M_S$ and so M_S is a simple $RN_G(S)$-module.

Suppose now that (e:a)-(e:c) hold. Let W be a non-zero RG-submodule of M. By (e:a), M and so also W is semisimple for RN. In particular there exists $I \in \mathcal{I}$ with $I \leq W$. By (e:b), ${}^g[I] = S$ for some $g \in G$. Thus $gI \leq W \cap M_S$. Hence $W \cap M_S \neq 0$ and (e:c) implies $M_S = M_S \cap W \leq W$. (e:a) and 2.7.7 imply that $M = RGM_S = W$. Thus M is a simple RG-module.

(f) Follows from (c), (e) and 2.7.8 □

Lemma 2.9.7 [**interwining numbers**] *Let $\mathbb{K}$ be am algebraicly closed field and R a finite dimensional K-algebra. Let $\mathcal{S}$ be a set of representatives for isomorphism classes of simple A-modules. For R-modules M, N define $i(N, M) = \dim_{\mathbb{K}} \mathrm{Hom}_R(N, M)$. Let $S \in \mathcal{S}$ and M an R-module.*

(a) [**a**] $i(S, M) = i(N, \mathrm{S}_M(R)) = i(S, M_{[S]})$.

(b) [**b**] *If M is finite dimensional (over $\mathbb{K}$), then $M_{[S]} \cong S^{i(S,M)}$ as an R-module.*

(c) [**c**] *If M is semisimple and finite dimensional, $M \cong \bigoplus_{S \in \mathcal{S}} S^{i(S,M)}$.*

(d) [**d**] *If N and M are semisimple, then $i(N, M) = \sum_{S \in \mathcal{S}} i(S, N) i(S, M)$.*

Proof: (a) Let $0 \neq f \in Hom_S(M)$. Then $\Im f \cong S$ and so $\Im f \leq M_{[S]} \leq \mathrm{S}_M(R)$. Thus $\mathrm{Hom}_R(S, M) = \mathrm{Hom}_R(S, \mathrm{S}_M(R) = \mathrm{Hom}_R(S, M_{[S]}$. So (a) holds.

(b) Note that $M_{[S]} \cong S^n$ for some $n \in \mathbb{N}$. Thus $\mathrm{Hom}_R(S, M_{[S]}) \cong Hom_R(S, S)^n$ and by 2.5.3, $Hom_R(S, M_{[S]}) \cong \mathbb{K}^n$.

(c) Since $M = \bigoplus_{S \in \mathcal{S}} M_{[S]}$, this follows from (c).

(d) Follows from (c) and (b).

□

Chapter 3

Character Theory

3.1 Semisimple Group Algebra

Definition 3.1.1 [**def:splitting field**] *Let G be a finite group. Then a splitting field for G is a field $\mathbb{K}$ such that all simple $\mathbb{K}G$-modules are absolutely simple.*

Lemma 3.1.2 [**existence of splitting fields**] *Let G be a finite group.*

(a) [**a**] *Let $\mathbb{K}$ be a field, then there exists a finite extension $\mathbb{F}$ of G such that $\mathbb{F}$ is a splitting field for $\mathfrak{G}$.*

(b) [**b**] *Every algebraicly closed field is a splitting field for G.*

Proof:

(a) Let $\mathcal{S}$ be a set of representatives for the isomorphism classes of $\mathbb{K}G$-modules. Since $\mathbb{K}G$ is Artinian, $\mathcal{S}$ is finite and all $S \in \mathcal{S}$ are finite dimensional. Let $\overline{\mathbb{K}}$ be an algebraic closure of $\mathbb{K}$. For $S \in \mathcal{S}$ choose a subfield $\mathbb{K}_S$ in $\mathrm{End}_{\mathbb{K}G}(S)$ and $\mathbb{K}$-linear monomorphism $\sigma_S : \mathbb{K}_S \to \overline{\mathbb{K}}$. Let $\mathbb{F}$ be the subfield of $\mathbb{K}$ generated by all the $\Im\sigma_S, S \in \mathcal{S}$. Then by 2.6.24 $\mathbb{F}$ is a splitting field for G.

(b) Follows from (a) and equally well from 2.6.25.

In this section we assume that G is a finite group, and $\mathbb{K}$ is a splitting field for G with $\mathrm{char}\,\mathbb{K} \nmid |G|$. Let $\mathcal{S} = \mathcal{S}(\mathbb{K}G)$ be a set of representatives for the isomorphism classes of simple $R := \mathbb{K}G$ modules. For $S \in \mathcal{S}$ let $d_S = \dim_{\mathbb{K}} S$ and $R_S = \bigcap\{\mathrm{A}_R(T) \mid S \neq T \in \mathcal{S}\}$. Let $\mathcal{C}$ be the set of conjugacy classes of G, that is the set of orbits of G acting on G by conjugation. For $H \subseteq G$ put $a_H = \sum H \in \mathbb{K}G$. For $C \in \mathcal{C}$ choose $g_C \in C$.

Theorem 3.1.3 [**structure of group algebra**] *Let $S \in \mathcal{S}$.*

(a) [**a**] $R = \bigoplus_{S\in\mathcal{S}} R_S$.

(b) [**b**] $R_S \cong R^S = \mathrm{End}_{\mathbb{K}}(S)$ *is simple and* $\dim_{\mathbb{K}} I_S = d_S^2$.

(c) [**c**] $|G| = \sum_{S\in\mathcal{S}} d_S^2$.

(d) [**d**] *Let e_S be the multiplicative identity in I_S. Then $Z(R_S) = \mathbb{K}e_S$ and $(e_S, S \in \mathcal{S})$ is a basis for for $Z(R)$.*

(e) [**e**] *$(a_C \mid C \in \mathcal{C})$ is a basis for $Z(R)$.*

(f) [**f**] $|\mathcal{S}| = \dim_{\mathbb{K}} Z(R) = |\mathcal{C}|$.

Proof: (a) and (b) By 2.5.23 $J(R) = 0$. Thus (a) and (b) follows from 2.5.18.

(c) Follows immediately from (a) and (b).

(d) By 2.5.12 $\mathrm{End}_{\mathrm{End}_{\mathbb{K}}(S)}(S) = \mathbb{K}$. Hence $Z(\mathrm{End}_{\mathbb{K}}(S)) = \mathbb{K}$ and so $Z(R_S) = \mathbb{K}e_S$. By (a) $Z(R) = \bigoplus_{S \in \mathcal{S}} Z(R_S)$ and so (d) holds.

(e) Let $a = \sum_{g \in G} k_g g \in R$. Then the following are equivalent:

$$\begin{array}{rl}
a \in Z(R) & \\
ah = ha & \forall h \in G \\
hah^{-1} = a & \forall h \in G \\
\sum_{g \in G} k_g hah^{-1} = \sum_{g \in G} k_g g & \forall h \in G \\
\sum_{g \in G} k_{h^{-1}gh} g = \sum_{g \in G} k_g g & \forall h \in G \\
k_{h^{-1}gh} = k_g & \forall h \in G \\
k_g = k_h & \forall C \in \mathcal{C}, g, h \in C \\
a = \sum_{C \in \mathbb{C}} k_C a_c & \text{for some}(k_C) \in \underset{\mathbb{C}}{\textcircled{Π}} \mathbb{K}
\end{array}$$

So (e) holds.

(f) follows immediately from (d) and (e). □

Lemma 3.1.4 [**class algebra constant**] *There exists integers k_{CDE}, $C, D, E \in \mathcal{C}$ with*

$$a_C a_D = \sum_{E \in \mathcal{C}} k_{CDE} a_E.$$

for all C, D, E.

Proof: This follows from $a_C a_D \in Z(\mathbb{Z}G)$. □

Definition 3.1.5 [**def:class algebra constant**] *The integers k_{CDE} in 3.1.4 are called the* class algebra constants *of G.*

3.2 Characters

From now an $\mathbb{K}$ is a splitting field of G contained in $\mathbb{C}$ and all $\mathbb{K}G$-modules are assumed to be finite dimensional over $\mathbb{K}$.

Definition 3.2.1 [**def:character**] *Let M be a R-module of finite dimension d_M and $r \in R$. $\rho_M : R \to \mathrm{End}_{\mathbb{K}}(M)$ is the corresponding homomorphism defined by $\rho_M(r)(m) = rm$ for all $r \in R, m \in M$. $\eta_M(r)$ is the characteristic polynomial $\rho_M(r)$. $tr_M(r)$ is the trace of $\rho_M(r)$. χ_M is the restricton of* ttr_M *to G. χ_M*

Definition 3.2.2 [**def:class function**]

(a) [**a**] *A class function is a function $\tau : G \to \mathbb{K}$ which is constant on every conjugacy class.*

(b) [**b**] *$\mathcal{F}(G, \mathbb{K})$ denotes the set of all class function.*

(c) [**c**] *For any funtion $\tau : G \to K$, $\tilde{\tau}$ denotes the unique $\mathbb{K}$-linear extension of τ to $\mathbb{K}G$, that is $\tilde{\tau}(\sum_{k_g} g)) = \sum k_g \tau(g)$.*

Observe that for an $\mathbb{K}G$-module M, $\tilde{\chi}_M = \mathrm{tr}_M$.

Lemma 3.2.3 [**class functions**] *Let $\tau \in \mathcal{F}(G, \mathbb{K})$. Then $\tau = \sum_{g \in G} \tau(g) g \in Z(\mathbb{K}(G))$. In particular, $\mathcal{F}(G, \mathbb{K}) = Z(\mathcal{KG})$.*

Proof: Just recall that by definition $\mathbb{K}G$ is the set of all functions $f : G \to \mathbb{K}$ and we identified g with the functions $h \to \delta_{hg}$. □

Lemma 3.2.4 [**characters are class functions**] *Let M be a $\mathbb{K}G$-module.*

(a) [**a**] *χ_M is a class function.*

(b) [**b**] *If N is an $\mathbb{K}G$-module isomorphic to M, then $\chi_N = \chi_M$.*

(c) [**c**] *If $\mathcal{N}$ is a set of R-submodules with $M \cong \bigoplus \mathcal{N}$ then $\tilde{\chi}_M = \sum_{N \in \mathcal{N}} \tilde{\chi}_N$.*

Proof: (a) and (b) follow from the fact that $\mathrm{tr}(\alpha) = \mathrm{tr}(\beta)$ for any two equivalent K-endomorphism α and β.

(b) is obvious. □

Definition 3.2.5 [**def:algebraic integers**] *Let $a \in \mathbb{C}$.*

(a) [**a**] *a is called an algebraic integer if $f(a) = 0$ for some monic $f \in \mathbb{Z}[x]$. $\mathbb{A}$ denotes the set of all algebraic integers.*

(b) [**b**] *$\overline{a}$ is the commplex conjugate of a and $|a| = \sqrt{a\overline{a}}$.*

Lemma 3.2.6 [**algebraic integers**]

(a) [**a**] *$\mathbb{A}$ is a subring of $\mathbb{Z}$*

(b) [**b**] *$\mathbb{A} \cap \mathbb{Q} = \mathbb{Z}$.*

(c) [**c**] *If $a \in \mathbb{A}$ and let f_a be the minimal polynomial of a over $\mathbb{Q}$. Then $f \in \mathbb{Z}[x]$.*

(d) [**d**] *Let $\lambda \in \mathbb{K}$ be a root of unity (that is $\lambda^n = 1$ for some $n \in \mathbb{Z}^+$. Then $|\lambda| = 1$ and $\overline{\lambda} = \lambda^{-1}$.*

(e) [**e**] *Let $a \in \mathbb{K}$ and suppose $a = \sum_{i=1}^d \lambda_i$, where each λ_i is a root of unity.*

  (a) [**a**] *a is an algebraic integer.*

  (b) [**b**] *$|a| \leq d$.*

  (c) [**c**] *$|a| = d$ iff $\lambda_1 = \lambda_2 = \ldots = \lambda_d$.*

  (d) [**d**] *$a = d$ iff $\lambda_1 = \lambda_2 = \ldots = \lambda_d = 1$.*

  (e) [**e**] *If $\frac{a}{d} \in \mathbb{A}$, then either $a = 0$ or $|a| = d$.*

Proof: (a) See any graduate algebra book. For example [Gr, VI.4.4].

(b) Let $a = \mathbb{A} \cap mbQ$. Then $a = \frac{n}{m}$ for some $n, m \in \mathbb{Z}$ with $\gcd(n, m) = 1$ and $f(a) = 0$ for some monic $f = \sum_{i=0}^d a_i x^i \in \mathbb{Z}[x]$. So $n^d = -\sum_{i=0}^{d-1} a_i n^i m^{d-i}$. Thus $m \mid n$ and since $\gcd(n, m) = 1$, $m = \pm 1$. So $a \in \mathbb{Z}$.

(c) Let $\mathbb{F}$ be the splitting field of a over $\mathbb{Q}$ and $H = \mathrm{Aut}_{\mathbb{Q}}(\mathbb{F})$. By Galois theory $f = \prod_{h \in H}(x - h(a))$. Clearly each $h(a) \in \mathbb{A}$ and so by (a), $f \in \mathbb{A}[x]$. Thus (c) follos from (b).

(d) $\lambda^n = 1$ implies $(\lambda\overline{\lambda})^n = 1$. Since $\lambda\overline{\lambda}$ is a positive real number, $\lambda\overline{\lambda} = 1$. So $|\lambda = 1|$ and $\overline{\lambda} = -\lambda^{-1}$. Also λ is a root of $x^n - 1$ and so $\lambda \in \mathbb{A}$.

(e:a) (d) each $\lambda_i \in \mathbb{A}$ and so by (a), $a \in \mathbb{A}$.

(e:b) By the tringualar inequality,

$$(*) \qquad |a| \leq \sum_{i=1}^d |\lambda_i| = d$$

(e:c) Equality holds in (*) iff exists there exists $\lambda \in \mathbb{K}$ and $r_i \in \mathbb{R}^{\geq 0}$ with $\lambda_i = r_i \lambda$. Since $|\lambda_i| = 1$ we get $r_i = 1$ and the λ_i are all equal.

(e:d) Follows from (e:d).

(e:e) Let f be the minimal polynomial of $\frac{a}{d}$ over $\mathbb{Q}$, $\mathbb{F} = \mathbb{Q}(\lambda_1, \ldots, \lambda_d)$ and $h \in H := \mathrm{Aut}_{\mathbb{Q}}(\mathbb{F})$. Then

$$h(a) = sum_{i=1}^d h(\lambda_i)$$

Each $h(\lambda_i$ is a root of unity and so by (e:c), $|h(a)| \leq d$. Thus $|h(\frac{a}{d}| \leq 1$. Put $e := \prod_{h\in H} h(\frac{a}{d}$. Then $|e| \leq |\frac{a}{n}| \leq 1$. But $e = \pm f(0)$ and so by (b), $e \in \mathbb{Z}$. Thus $e = 0, \pm 1$. In the first case we get $a = 0$ and in the second $|e| = 1$ and so also $|fracad = 1$ and $|a| = d$. □

Definition 3.2.7 [**dual**] *Let F be a commutative ring, A an F-algebra and M an A-module.*

(a) [**a**] *Then $M^* = Hom(M, A)$ is called the* dual *of M. We view M^* as a right R-module via $(\alpha b)(m) = \alpha(bm)$ for all $\alpha \in M^*, b \in A$ and $m \in M$.*

(b) [**b**] *If $A = F[H]$ for a group H, let $\circ : A \to A$ be F-linear anti-automorphism with $g^\circ = g^{-1}$ for all $g \in G$. Then we view M^* has a left R-module via $b\alpha = \alpha b^\circ$ for all $b \in A$, $\alpha \in M^*$.*

Lemma 3.2.8 [**basic character**] *Let M be an R-module and $g \in G$.*

(a) [**a**] $\chi_M(1) = d_M := \dim_{\mathbb{K}} M$.

(b) [**b**] *$\chi_M(g)$ is the sum of the eigenvalues for g on M over $\mathbb{C}$, counting multiplicities. In particular, $\chi_M(g)$ is an algebraic integer.*

(c) [**c**] *$\chi_M(g^-1) = \overline{\chi_M(g)}$, where $\overline{k}$ denotes the complex conjugate of $k \in \mathbb{K}$.*

(d) [**d**] $\overline{\chi_M} = \chi_{M^*}$

(e) [**e**] $|\chi_M(g)| \leq d_M$.

(f) [**f**] *$|\chi_M(g)| = d_M$ iff g acts as a scalar on M.*

(g) [**g**] *$\chi_M(g) = d_M$ iff $g \in C_G(M)$.*

Proof: (a) is obvious.

(b) For example by Maschke's Theorem and Schur's Lemma there exists a basis $\mathcal{B}$ of eigenvectors for g on m. For $b \in \mathcal{B}$ let λ_b the the corresponding eigenvector. Let $n = |g|$. Then $b = g^n b = \lambda_b^n b$ and so $\lambda_b^n = 1$. Moreover $\chi_M(g) = \sum_{b\in\mathcal{B}} \lambda_b \in \mathbb{A}$ and so (b) follows from 3.2.6(e).

(c) Since $\overline{\lambda} = \lambda^{-1}$ we have $g^{-1}b = \overline{\lambda}g$ and so (c) holds.

(d) Let $b^* \in M^*$ be define by $\beta^*(a) = \delta_{ab}$ for all $a \in \mathcal{B}$. Then $\mathcal{B}^*$ is a basis of M^*. From $(gb^*)(a) = b^*(g^{-1}a)) = b^*(\overline{\lambda}_a)a) = \delta_{ab}\overline{\lambda}_a$, we see that $\mathcal{B}^*$ is a basis of eigenvectors form g on M^* with eigenvalues $\overline{\lambda}_b$. Thus (d) holds.

(e), (f) and (g) follow from (b) and 3.2.6(e).

Definition 3.2.9 [**trivial module**]

(a) [**a**] *$\mathbb{K}_G$ is the $\mathbb{K}G$-module defined by $\mathbb{K}_G = \mathbb{K}$ has a $\mathbb{K}$-space and $gk = k$ for all $g \in G$ and $k \in K$. Any module isomorphic to $\mathbb{K}_G$ is called a trivial $\mathbb{K}G$-module. $\chi_1 = \chi_{\mathbb{K}_G}$ is the character of the trivial module and so $\chi_1(g) = 1$ for all $g \in G$.*

(b) [**b**] *Let Ω be a G-set. Then $\mathbb{K}\Omega$ is the $\mathbb{K}G$ module with $\mathbb{K}$-basis Ω and $g \cdot \sum_{\omega \in \Omega} k_\omega \omega = \sum_{\omega\in\Omega} k_w gw$.*

Note that for $\Omega = G$ with G acting by left multiplication the just defined $\mathbb{K}G$ module $\mathbb{K}\Omega$ is the same as $\mathbb{K}G$- view as a $\mathbb{K}G$-module by left multiplication.

Lemma 3.2.10 [**permutation character**] *Let Ω be a G-set.*

(a) [**a**] *$(\mathbb{K}\omega \mid \omega \in \Omega)$ is a system of imprimitvity for G on $\mathbb{K}\Omega$.*

(b) [**b**] *$\chi_{\mathbb{K}\Omega}(g) = |C_\Omega(g)|$ for all $g \in G$.*

(c) [**c**] *Suppose G acts transitively on Ω and let $\omega \in \Omega$. Put $H = C_G(b)$. Then then $\mathbb{K}H =\cong \mathbb{K}_H \uparrow_H^G$.*

Proof: (a) We have $g\mathbb{K}\omega = \mathbb{K}(g\omega)$ and $K\Omega = \oplus_{\omega\in\Omega}\mathbb{K}\Omega$. So (a) holds.

(b) For $i \in \Omega$, $gi = \sum_{j \in Omega} \delta_{gi,j} j$ So the matrix for g on $\mathbb{K}\Omega$ with respect to the basis Ω is $(\delta_{gi,j}$. Hence $\chi_{\mathcal{KG}}(g) = \sum_{i\in\Omega} \delta_{gi,i} = \sum_{i \in C_\Omega}(g) 1 = |C_\Omega(g)|$.

(c) Observe that $\mathbb{K}\omega$ is a trivial $\mathbb{K}H$ module. So (c) follows from (a) and 2.7.8(b). □

Lemma 3.2.11 [**reg char**] *Let $g \in G$.*

(a) [**a**] *$R \cong \sum_{S \in \mathcal{S}} S^{d_S}$ as an left R-module.*

(b) [**b**] *$\tilde{\chi}_R = \sum_{S\in\mathcal{S}} d_S \tilde{\chi}_S$.*

(c) [**c**] *$\chi_R(g) = \sum_{S\in\mathcal{S}} d_S \chi_S(g)$.*

(d) [**d**] *$\chi_R(1) = \sum_{S\in\mathcal{S}} d_S^2 = |G|$.*

(e) [**e**] *If $g \neq 1$, then $\chi_R(g) = \sum_{S\in\mathcal{S}} d_S\chi_S(g) = 0$.*

Proof: (a) By 3.1.3(a), $R \cong \bigoplus_{S\in\mathcal{S}} R_S$ as a ring and by By 2.5.11(b), $R_S \cong S^{D_S}$ as a left R_S-module. So (a) holds.

(b) follows from (a) and 3.2.4(c).

(c) follows from (b).

Let $\Omega = G$ view as a G-set by left multiplication. Then $C_\Omega(g) = \emptyset$ if $g \neq 1$ and $C_\Omega(1) = \Omega$. So by 3.2.10 $\chi_R(1) = |G|$ and $\chi_R(g) = 0$ for $1 \neq g \in G$. (d) and (c) now follow from (c) and $\chi_S(1) = D_S$. □

Lemma 3.2.12 [**change of basis**] *Let $S \in \mathcal{S}$ and $C \in \mathcal{C}$.*

(a) [**a**] *$e_S = \frac{d_S}{|G|}\sum_{g\in G} \overline{\chi}_S(g) g = \frac{d_S}{|G|}\sum_{C\in\mathcal{C}} \overline{\chi}_S(g_C)a_C$.*

(b) [**b**] *$a_C = \sum_{S\in\mathcal{S}} \frac{|C|}{d_S}\chi_S(g_C)e_S$.*

Proof: (a) Let $e_S = \sum_{g\in G} k_g g$ with $k_g \in \mathbb{K}$. Let $h \in G$. Then $he_S = \sum_{ginG} k_g hg$. By 3.2.11(d), (e), $\chi_R(hg) = |G|$ if $h = g^{-1}$ and 0 otherwise. So

$$\chi_R(he_S) = k_{h^{-1}}|G|. \tag{1}$$

On the otherhand $\rho_T(e_S) = 0$ for all $S \neq T \in \mathcal{S}$ and $\rho_S(e_S) = \mathrm{id}_S$. Thus $\chi_T(he_S) = 0$ and $\chi_S(he_S) = \chi_S(h)$. So 3.2.11(b) $\chi_R(he_S) = d_S\chi_S(h)$. So by (1) $k_{h^-1} = \frac{d_S}{|G|}\chi_S(h)$ and so $k_h = \frac{d_S}{|G|}\chi_S(h^{-1}) = \frac{d_S}{|G|}\overline{\chi}_S(h)$. Thus (a) holds.

(b) By 3.1.3 $a_C = \sum_{S\in\mathcal{S}} k_S e_S$ for some $k_S \in \mathbb{K}$. Also $\chi_T(e_S) = \delta_{ST}d_S$ and so

$$k_T d_T = \chi_T(a_C) = \sum_{g\in C}\chi_T(g) = |C|\chi_T(g_C)$$

So $k_T = |C|\frac{\chi_T(g_C)}{d_T}$. □

Lemma 3.2.13 [**eigenvalue**] *Let $C \in C$ and $S \in \mathcal{S}$. Then $\rho_S(a_C) = \frac{|C|}{d_S}\chi_S(g_C)\mathrm{id}_S$ and $\frac{|C|}{d_S}\chi_S(g_C)$ is an algebraic integer.*

The first statement follows immediately 3.2.12(b). In particular, e_S is an eigenvector with eigenvalues $\frac{|C|}{d_S}\chi_S(g_C)$ for a_C on $Z(\mathbb{K}G)$. By 3.1.4 the matrix of a_C with respects to the basis $(a_D, D \in \mathcal{C})$ of $Z(\mathbb{K}G)$ is integral. Thus the characteristic polynomial for a_C on $Z(\mathbb{K}G)$ is monic integral. Thus all the eigenvalues are algebraic integers. □

Theorem 3.2.14 (Orthogonality Relations) [**orthogonality**]

(I) [**a**] *For all $S, T \in \mathcal{S}$,*

$$\frac{1}{|G|}\sum_{g\in G}\chi_S(g)\overline{\chi}_T(g) = \delta_{ST}$$

(II) [**b**] *For all $C, D \in \mathcal{C}$,*

$$\sum_{S\in\mathcal{S}}\chi_S(g_C)\overline{\chi}_S(g_D) = |C_G(g_C)|\delta_{CD}.$$

Proof: Let A be the matrix for the change of bases for $Z(\mathbb{K}G)$ from $(a_C, C \in \mathcal{C})$ to $(e_S \mid S \in \mathcal{S})$. Then by 3.2.12(a), $A = (\frac{|d_S}{|G|}\overline{\chi}_S(g_C))_{SC}$. Also let B be the matrix for the change of basis for $Z(\mathbb{K}G)$ from $(e_S \mid S \in \mathcal{S})$ to $(a_C, C \in \mathcal{C})$. Then by 3.2.12(a), $B = (\frac{|C|}{d_S}\chi_S(g_C))_{CS}$.

Since $AB = \mathrm{I}_{\mathcal{S}}$ we get for all $T, S \in \mathcal{S}$ that

$$\sum_{C\in\mathcal{C}} \frac{|d_T}{|G|}\overline{\chi}_T(g_C)\frac{|C|}{d_S}\chi_S(g_C)) = \delta_{ST}$$

and so

$$sum_{g\in G}\chi_S(g_C)\overline{\chi}_T(g_C) = \frac{d_S}{d_T}\delta_{ST} = \delta_{ST}$$

So (I) hold.

Since $BA = \mathrm{I}_{\mathcal{C}}$ we get for all $C, D \in \mathcal{C}$

$$\sum_{S\in\mathcal{S}} \frac{|C|}{d_S}\chi_S(g_C)\frac{|d_S}{|G|}\overline{\chi}_S(g_D) = \delta_{CD}$$

and so

$$\sum_{S\in\mathcal{S}} \chi_S(g_C)\overline{\chi}_S(g_D) = \frac{|G|}{|C|}\delta_{CD}$$

Since $|C| = |G/C_G(g_C)|$ we see that (II) holds. □

Proposition 3.2.15 [**ds divides g**] *d_S divides $|G|$ for all $S \in \mathcal{S}$.*

Proof: By the first orthogonality relation 3.2.14(I) applied with $S = T$,

$$\frac{1}{|G|}\sum_{C\in\mathcal{C}} |C|\chi_S(g_C)\overline{\chi}_S(g_C) = 1$$

Multiplication with $\frac{|G|}{d_S}$ gives:

$$\sum_{C\in\mathcal{S}} \frac{|C|\chi_S(g_c)}{|d_S|}\chi_S(g_C) = \frac{|G|}{d_S}$$

By 3.2.13 $\frac{|C|\chi_S(g_c)}{|d_S|}$ is an algebraic intgeger, by 3.2.8(b), $\chi_S(g_C)$ is an algebraic integer and so by 3.2.6(a), also $\frac{|G|}{d_S}$ is an algebraic integer. So by 3.2.6(b), $\frac{|G|}{d_S}$ is an integer. □

Definition 3.2.16 [**def:char table**] *The $\mathcal{S}\times\mathcal{C}$ matrix $(\chi_S(g_C))_{SC}$ is called the character table of G.*

The next lemma shows how the class algebra constants can be computed from the character table.

Lemma 3.2.17 [**compute constants**] *(a)* [**a**] *For all $C, D, E \in \mathcal{C}$:*

$$k_{CDE} = \frac{|G|}{|C_G(g_C)||C_G(g_D)|} \sum_{S \in \mathcal{S}} \frac{1}{d_S} \chi_S(g_c)\chi_S(g_D)\overline{\chi}_S(g_E)$$

(b) [**b**] *For all $C, D \in \mathcal{C}$*

$$a_C a_D = \frac{|G|}{|C_G(g_C)||C_G(g_D)|} \sum_{S \in \mathcal{S}} \frac{\overline{\chi}_S(g_c)\overline{\chi}_S(g_D)}{d_S} \chi_S$$

Proof: (a) By definition of the k_{CDF},

$$a_C a_D = \sum_{F \in \mathcal{C}} k_{CDF} a_F$$

and so also

$$\rho_S(a_C)\rho_S(a_D) = \sum_{F \in \mathcal{C}} k_{CDF} \rho(a_F)$$

Thus 3.2.13 gives

$$\frac{|C|\chi_S(g_C)}{d_S} \frac{|D|\chi_S(g_D)}{d_S} = \sum_{F \in \mathcal{C}} k_{CDF} \frac{|F|\chi_S(g_F)}{d_S}$$

Thus

$$\frac{|C||D|}{d_S} \chi_S(g_C)\chi_S(g_D) = \sum_{F \in \mathcal{C}} |F| k_{CDF}$$

Multiplying with $\overline{\chi}_S(g_E)$ and summing over all $S \in \mathcal{S}$ gives

$$\begin{aligned} |C||D| \sum_{S \in \mathcal{S}} \frac{1}{d_S} \chi_S(g_C)\chi_S(g_D)\overline{\chi}_S(g_E) &= \sum_{F \in \mathcal{C}} |F| k_{CDF} \sum_{S \in \mathcal{S}} \chi_S(g_F)\overline{\chi}_S(g_E) \\ \text{(2nd Orthogonality relation)} &= \sum_{F \in \mathcal{C}} |F| k_{CDF} |C_G(g_E)\delta_{EF} \\ &= |E| k_{CDE} |C_G(g_E)| \end{aligned}$$

Since $|X| = \frac{|G|}{|C_G(g_X)|}$ for $X = C, D$ and E, (a) holds.
(b) Note that k_{CDE} is real valued. So (b) follows from (a). □

3.3 Burnside's p^aq^b Theorem

In this short section we will show that all groups of order p^aq^b, where p and q are primes are solvable.

Definition 3.3.1 [**def:zchi**] *Let χ be a character of G. Then*

$$\begin{aligned} \ker\chi &= \{g\in G \mid \chi(g)=\chi(1)\} \\ Z(\chi) &= \{g\in G \mid |\chi(g)|=\chi(1)\} \end{aligned}$$

Lemma 3.3.2 [**zchi**] *Let $S\in\mathcal{S}$. Then*

(a) [**a**] $\ker\chi_S=\ker_G(\rho_S)=C_G(S)$.

(b) [**b**] *$Z(\chi_S)$ consists of all $g\in G$ which act as scalars on G. Moreover, $Z(\chi_S)/\ker\chi_S = Z(G/\ker\chi_S)$.*

Proof: (a) follows from 3.2.8(g) and the first part of (b) from 3.2.8(f). For the second statment since $G/\ker\chi_S\cong\rho_S(G)$ we may assume that $G\leq GL_{\mathbb{K}}(S)$. The $Z(G)=G\cap \mathrm{End}_{\mathbb{K}G}(S)$ and by Schur's Lemma 2.5.3, $\mathrm{End}_{\mathbb{K}G}(S)=\mathbb{K}$. So $Z(G)=G\cap\mathbb{K}$ and so the second statement in (b) holds. □

Lemma 3.3.3 [**gcd=1**] *Let $S\in\mathcal{S}$ and $C\in\mathcal{S}$ with $\gcd(d_S,|C|)=1$. Then either $\chi(g_C)=0$ or $C\subseteq Z(\chi_M)$.*

Proof: Choose integers a,b with $ad_S+b|C|=1$. Multiplying with $\frac{\chi_S(g_C)}{d_S}$ gives

$$a\chi_S(g_C)+b\frac{|C|\chi_S(g_C)}{d_S}=\frac{\chi_S(g_C)}{d_S}$$

By 3.2.13,3.2.8(b) and 3.2.6(a) the left side of this equation is an algebraic integer. The right side is the sum of d_S roots of unity devided by d_S. So by 3.2.6(e), $\chi_S(g_C)=0$ or $|\chi_S(g_C)=d_S$. □

Proposition 3.3.4 [**towards paqb**] *Suppose that $C\in\mathcal{C}$ with $|C|=p^t$ for some prime p and some $t\in\mathbb{N}$. If $G\neq 1$, then there exists a non-trivial simple character χ with $C\subseteq Z(\chi)$.*

Proof: If $C=\{1\}$, this is true for any non-trivial simple character χ. So suppose $C\neq\{1\}$. By the second orthogonal Relation applies with $D=1$:

$$\sum_{S\in\mathcal{S}}\chi_S(g_C)\chi_S(1)=0$$

and so

$$1 + \sum_{\mathbb{K}_G \neq S \in \mathcal{S}} \chi_S(G_C) d_S = 0$$

By 3.2.6(b), $\frac{1}{p} \notin \mathbb{A}$. Thus $1 \notin p\mathbb{A}$ and by the preceeding equation there exists $\mathbb{K}_G \neq S \in \mathcal{S}$ with $\chi_S(g_C)d_S \notin p\mathbb{A}$. Since $\chi_S(g_C) \in \mathbb{A}$ this implies $p \nmid d_S$ and $\chi_S(g_C)$. Since $|C| = p^t$ we get $\gcd(d_S, |C|) = 1$ and the proposition follows from 3.3.3. □

Theorem 3.3.5 (Burnside's p^ap^b-Theorem) [**paqb**] *Let p and q be primes, $a, b \in \mathbb{N}$ and G a finite group of order p^aq^p. Then G is solvable.*

Proof: By induction on $|G|$. The Theorem is clearly true for $|G| = 1$. So suppose $|G| \neq 1$ and say $q^b \neq 1$. Let Q be a Sylow q-subgroup of G and $1 \neq g \in Z(Q)$. Then $q^b \mid |C_G(g)$ and so $|G/C_G(g)| = p^t$ for some $0 \leq t \leq a$. Put $C = {}^Gg$. Then $|C| = p^t$ and by 3.3.4 $C \subseteq Z(\chi)$ for some non-trivial simple character χ. Since χ is non-trivial simple, $\ker \chi \neq G$. So by induction $\ker \chi$ is solvable. By 3.3.2, $Z(\chi)/\ker \chi$ is abelian and so solvable. Since $C \subseteq Z(\chi)$, $Z(\chi) \neq 1$ and so by induction also $G/Z(\chi)$ is solvable. Since extensions of solvable groups are solvable, G is solvable. □

3.4 An hermitian form

Recall that $r \in \mathbb{K}[G]$ is a function from $G \to \mathbb{K}G$ and $\tilde{r}$ is linear extension of r to $\mathbb{K}[G]$.

Definition 3.4.1 [**def:inner product**] *Let $r, s \in \mathbb{K}G$.*

(a) [**a**] *$\overline{r}$ is defined by $\overline{r}(g) = \overline{r(g)}$, in other words if $r = \sum_{g \in G} r_g g$, then $\overline{r} = \sum_{g \in G} \overline{r}_g g$.*

(b) [**b**] $(r \mid s) = \frac{1}{|G|}\tilde{r}(\overline{s}) = \frac{1}{|G|}\sum_{g \in G} r_g \overline{s}_g$.

Lemma 3.4.2 [**inner product**]

(a) [**a**] *G is a positive orthogonal basis for $\mathbb{K}G$ with respect to $(\cdot \mid \cdot)$.*

(b) [**b**] *$(\cdot \mid \cdot)$ is a positive definite hermitian form on $\mathbb{K}G$.*

(c) [**c**] *$(rt \mid s) = (r \mid s\overline{t}^\circ)$ and $(tr \mid s) = (r \mid \overline{t}^\circ s)$ for all $r, s, t \in \mathbb{K}G$.*

(d) [**d**] *$r \circ \mathrm{inn}(g) = g^{-1}rg$ for all $r \in \mathbb{K}G$, $g \in G$.*

Proof: (a) Let $g, h \in G$. Then by defintion $(g \mid h) = \frac{1}{|G|}\delta_{gh}$.

(b) Clearly $(\cdot \mid \cdot)$ is $\mathbb{K}$-linear in the first coordinate and $(\mathbb{K}, \bar{\cdot})$-similinear in the second. Also by (b), $(\cdot \mid \cdot)$ is symmetric and real valued then restricted by the basis G. So by sesquilinearity $(r \mid s) = \overline{(s \mid r)}$ for all r, s. Thus $(\cdot \mid \cdot)$ is an hermitian form. So by (a), $(\cdot \mid \cdot)$ is positive definite.

(c) Let $g, h, l \in G$. Then $gl = h$ iff $g = hl^{-1}$ and so

$$(gl \mid h) = \frac{1}{|G|}\delta_{gl,h} = \frac{1}{|G|}\delta_{g,hl^{-1}} = (g \mid hl^{-1}) = (g \mid hl^{\circ})$$

Sesquilinearity now implies the first statement in (c). The second follows similarly (or by applying the first to the opposite group of G.)

(d) By $\mathbb{K}$-linearity we may assume $r = h \in G$. Let $l \in G$. Then

$$(h \circ \operatorname{inn}(g))(l) = h(glg^{-1}) = \delta_{h,glg^{-1}} = \delta_{g^{-1}hg,l} = (g^{-1}hg)(l)$$

So $h \circ \operatorname{inn}(g) = g^{-1}hg$. □

Lemma 3.4.3 [**orthonormal basis**] *$(\chi_S \mid S \in \mathcal{S})$ is an orthonormal basis for $Z(\mathbb{K}G)$.*

Proof: By the First Orthogonality Relation, $s\chi_S\chi_T = \delta_{ST}$. In particular,$(\chi_S \mid S \in \mathcal{S})$ is lineraly independent and since $\dim Z(\mathcal{KG}) = |\mathcal{S}|$, $(\chi_S \mid S \in \mathcal{S})$ is a basis for $Z(\mathbb{K}G)$. □

Corollary 3.4.4 [**i=s**] *Let N, M be $\mathbb{K}G$-modules. Then*

(a) [**a**] *For any $\alpha \in \mathrm{Z}(\mathbb{K}G)$, $\alpha = \sum_{S\in\mathcal{S}}(\chi_S \mid \alpha)\chi_S$.*

(b) [**b**] *Let $M \cong \sum_{S\in\mathcal{S}} S^{i_S}$ and $N \cong \sum_{S\in\mathcal{S}} S^{j_S}$. Then $(\chi_M \mid \chi_N) = \sum_{S\in\mathcal{S}} i_S j_S = i(N, M)$.*

(c) [**c**] *$N \cong \sum_{S\in\mathcal{S}} S^{(\chi_S|\chi_N)}$.*

(d) [**d**] *$M \cong_{KG} N$ if and only if $\chi_M = \chi_N$.*

(a) Follow from 3.4.3.

(b) Note that $\chi_M = \sum_{S\in\mathcal{S}} i_S\chi_S$ and $\chi_N = \sum_{S\in\mathcal{S}} j_S\chi_S$. Thus (b) folloes from 3.4.3 and 2.9.7.

(c) By (b) applies with $M = S$, $i_S = (\chi_S \mid \chi_N)$.

(d) follows from (c). □

Definition 3.4.5 [**def:gen char**] *Let U be an additive subgroup of $\mathbb{K}$. A U-linear combination of characters ic called a U-*generalized character*. $\mathcal{F}_U(G, \mathbb{K})$ denotes the set of all U-generalized character. A generalized character is a $\mathbb{Z}$-generalized character.*

Note that a chacter is the same as a $\mathbb{N}$-generalized character. And a generalized character is just the difference of two characters.

Corollary 3.4.6 [**gen char**] *Let U be an additive subgroup of $\mathbb{K}$ and $a \in \mathcal{F}(G, \mathbb{K})$. Then $a \in \mathcal{F}_U(G, \mathbb{K})$ iff $(a \mid \chi) \in U$ for all charaters χ of G over $\mathbb{K}$ and iff $sa\chi \in U$ for all irreducible characters χ of G over $\mathbb{K}$.*

Proof: This follows immediately from 3.4.4(a).

Lemma 3.4.7 [**products of char**] *Let N, M be $\mathbb{K}G$-modules. Then $\chi_N\chi_M = \chi_{N\otimes_{\mathbb{K}}M}$. In particular, the product of two charcters is a character and if U is a subring of $\mathbb{K}$, $\mathcal{F}_U(G,\mathbb{K})$ is a subring of $\mathcal{F}_U(G,\mathbb{K})$.*

Proof: Recall first by 2.8.2 $N\otimes M$ is a $\mathbb{K}G$-module via $g(n\otimes m) = gn\otimes gm$. If $\mathcal{A}$ and $\mathcal{B}$ is $\mathbb{K}$-basis for N and M respectively and $A = (a_{ij})_{(i,j)}$ and $B = b_{kl})_{(k,l)}$ are the corresponding matrices for g, then $(a_{ij}b_{kl})_{(i\otimes k, j\otimes l)}$ is the matrix for g with respect to the matrix $\mathcal{A}\otimes\mathcal{B}$. So

$$\chi_{N\otimes M}(g) = \sum_{i\in\mathcal{A},k\in\mathcal{B}} a_{ii}b_{kk} = (\sum_i a_{ii})\sum_k b_{kk} = \chi_N(g)\chi_M(g)$$

□

Definition 3.4.8 [**def:induced class**] *Let $H \leq G$ and $\alpha \in \mathcal{F}(H,\mathbb{K})$. Then $\alpha\uparrow_H^G$ is the unique element of $\mathcal{F}(H,\mathbb{K})$ with*

$$(\alpha^G \mid \beta)_G = (\alpha \mid \beta\mid_H)_H$$

for all $\beta \in \mathcal{F}(G,H)$. In other words, the map $\alpha \to \alpha\uparrow_H^G$ is the adjoint of the restrictions map $\beta \to \beta_H$.

Lemma 3.4.9 [**induced gen char**] *Let U be a an additive subring of $\mathbb{K}$ and $a \in \mathcal{F}_U(H,\mathbb{K})$. Then $a\uparrow_H^G \in \mathcal{F}_U(G,\mathbb{K})$.*

Proof: Thus follows from 3.4.6 and definition of the induced character. □

Lemma 3.4.10 [**induced=induced**] *Let $H \leq G$, W and $\mathbb{K}G$-module and V a $\mathbb{K}H$-module. Then $(\chi_V)\mid_H = \chi_{V\mid_H}$ and $\chi_W\uparrow_H^G = \chi_{W\uparrow_H^G}$.*

The first statement is obvious. For the second note that by 2.7.4 $\mathrm{Hom}_{\mathbb{K}G}(W\uparrow_H^G, V) \cong \mathrm{Hom}_{\mathbb{K}H}(W,V)$. Hence also $i(W\uparrow_H^G, V) = i(W, V\mid_H)$ and so by 3.4.4(b),

$$(\chi_{W\uparrow_H^G} \mid \chi_V)_G = (\chi_W W \mid (\chi_V)\mid_H).$$

By 3.4.3 any $\alpha\mathcal{F}(G,\mathbb{K})$ is the $\mathbb{K}$ linear combinations of χ_V's and so

$$(\chi_{W\uparrow_H^G} \mid \alpha)_G = (\chi_W W \mid \alpha\mid_H).$$

Thus $\chi_W\uparrow_H^G = \chi_{W\uparrow_H^G}$. □

Lemma 3.4.11 [**induced class function**] *Let $H \leq G$ and $z \in \mathcal{Z}(\mathbb{K}H)$. Let $\mathcal{T}$ be a left transversal to H in G. Then Then*

$$a\uparrow_H^G = \frac{1}{|H} \sum_{g \in G} gzg^{-1} = \sum_{t \in \mathcal{T}} tzt^{-1}$$

Proof: Let $u \in Z(\mathbb{K}G)$ and put $v = \frac{1}{|H|} \sum_{g \in G} gzg^{-1}$. Then cleary $v \in Z(\mathbb{K}G)$ and

$$(v \mid u)_G = \frac{1}{|H|} \sum_{g \in G} (gzg^{-1} \mid u)_G = \frac{1}{|H|} \sum_{g \in G} (z \mid g^{-1}ug^{-1})_G = \frac{1}{|H|} \sum_{g \in G} (z \mid u)_G = \frac{|G|}{|H|} (z \mid u)_G.$$

Also $|G|(z \mid u) = |H|(z \mid u \mid_H)$ and thus

$$svu_G = (z \mid u \mid_H).$$

Thus $v = z\uparrow_H^G$. □

Using 3.4.2(d) and that $\mathcal{F}(H, \mathbb{K}) = Z(\mathbb{K}G)$, we can rephrase the preceeding theorem as

Lemma 3.4.12 [**induced class function ii**] *Let $H \leq G$ and $\alpha \in \mathcal{F}(H, \mathbb{K})$ and define $\alpha_0 \in \mathcal{F}(G, \mathbb{K})$ by $\alpha_0 \mid H = f$ and $\alpha_0 \mid_{G-H} = 0$. Then $\alpha^G = \frac{1}{|H|} \sum_{l \in G} \alpha_0 \circ \operatorname{inn}(l)$, that is*

$$\alpha^G(g) = \frac{1}{|H|} \sum_{l \in G} \alpha_0(lgl^{-1})$$

□

3.5 Frobenius' Theorem

Theorem 3.5.1 (Frobenius) [**frobenius**] *Let H be a subgroup of G and suppose that*

$$(*) \quad H \cap {}^gH = 1 \textit{ for all } g \in G \setminus H.$$

Then $N := G \setminus \{ {}^gh \mid h \in H^\sharp, g \in G\}$ is a normal subgroup of G. Moreover, $H \cap N = 1$ and $G = HN$.

Proof: Let $\mathcal{H} = \{ {}^gh \mid h \in H^\sharp, g \in G\}$ and $\mathcal{N} = N \setminus \{1\}$. Then G is the disjoint union of $\{1\}$, $\mathcal{H}$ and $\mathcal{N}$. Let $\mathcal{R}$ be a left transversal to H in G. We claim that

1° [**1**] *For each $l \in \mathcal{H}$ there exist a unique $h \in H^\sharp$ and $r \in \mathcal{R}$ with $l = {}^rh$.*

Let $l \in \mathcal{H}$. Then by definition of $\mathcal{H}$, $l = {}^gm$ for some $m \in H^\sharp$. Moreover $g = rm$ for some $r \in \mathcal{R}$ and $m \in H$. Put $h = {}^mn$. Then $h \in H^\sharp$ and $l = {}^rh$. Suppose also $l = {}^{\tilde{r}}\tilde{h}$ for some $\tilde{h} \in H$ and $\tilde{r} \in \mathcal{R}$. The ${}^{\tilde{r}^{-1}r}h = {}^{\tilde{r}^{-1}}l = \tilde{h} \in H \cap {}^{\tilde{r}^{-1}r}H$. Thus (*) implies that $\tilde{r}^{-1}r \in H$. Thus $\tilde{r}H = rH$ and since $\mathcal{R}$ is a transversal $r = \tilde{r}$. Hence also $h = \tilde{h}$ and (1°) holds.

2° [**2**] *Let $a = \sum_{h\in H} a_h h \in Z(\mathbb{K}H)$ Then*

$$a^G = |G/H|a_1 + \sum_{h\in H^\sharp}\sum_{r\in\mathcal{R}} a_h {}^r h$$

Since ${}^r1 = r$ for all $r \in \mathcal{R}$ and $|\mathcal{R}| = |G/H$, (2°) follow from 3.4.11.

3° [**3**] *If $a, b \in Z(\mathbb{K}H)$ with $a_1 = 0$, then $(a^G \mid b^G)_G = (a \mid b)_H$.*

From (1°) and (2°) and $a_1 = 0$:
$(a^G \mid b^G)_G = \frac{1}{G}\sum_{h\in H^\sharp}\sum_{r\in\mathcal{R}} a_h\bar{b}_h = \frac{1}{G}\frac{|G|}{|H|}\sum_{h\in H^\sharp} a_h\bar{b}_h = (a \mid b)_H$.

4° [**4**] *Let S be non-trivial simple H-character and put $\alpha_S = \chi_S - d_S 1_H$. Then $\alpha_S^G = \beta_S - d_S 1_G$ for some simple G-character β_S of dimension d_S.*

By Frobenius Reciprocity

$$(\alpha_S^G \mid \chi_{\mathbb{K}_G})_G = (\chi_S \mid 1_H) - d_S(\chi_{\mathbb{K}_H} \mid 1_G) = -d_S$$

.

Put $\beta_S = \alpha_S^G + d_S 1_G$. Then $(b_S \mid 1_G) = 0$ and so

$$(\alpha_S^G \mid \alpha_S^G) = (\beta_S \mid \beta_S) + d_S^2$$

On the otherhand (3°) implies

$$(\alpha_S^G \mid \alpha_S^G) = (\chi_S - d_S 1_H \mid \chi_S - d_S 1_H) = 1 + d_S^2$$

So $(b_S \mid \beta_S) = 1$. Hence β_S or $-b_S$ is a simple character. But $\beta_S(1) = \alpha_S(1) + d_S = d_S$ and so β_S is a simple character.

5° [**5**] $\beta_S = \sum_{n\in N} d_S n + \sum_{h\in H^\sharp}\sum_{r\in\mathcal{R}} \chi_S(h){}^r h$.

Let $M = \bigcap\{\ker\beta_S \mid 1_S \neq S \in \mathcal{S}(H)\}$. Then by $N \subseteq M$. Suppose there exists $hinH^\sharp$ and $r \in \mathcal{R}$ with ${}^r h \in M$. Then $h \in \ker\chi_S$ for all $1 \neq S \in \mathcal{S}(H)$. So $h \in C_H(S)$ for all $S \in \mathcal{S}(H)$. But $\mathbb{K}H \cong \sum_{S\in\mathcal{S}(H)} S^{d_S}$ and so h acts trvialy on $\mathbb{K}H$ by left multiplication. Hence $h = h1 = 1$, a contradiction. Thus $M \cap \mathcal{H} = \emptyset$ and so $M = N$. Thus $N \trianglelefteq G$. Clearly $H \cap N = 1$. By (1°), $|\mathcal{H}| = |\mathcal{R}||H^\sharp| = \frac{|G|}{|H|}(|H| - 1) = |G| - \frac{|G|}{|H|}$ and so $|N| = \frac{|G|}{|H|}$ and $|HN| = |H||N| = |G|$. Thus $G = NH$ and all parts of the Theorem are proved. □

Corollary 3.5.2 [**frobenius ii**] *Suppose G acts transitively on set Ω and every non-trivial element fixes at most one element in Ω. Let $\mathcal{N}$ be the set of elements in G acting fixed-point freely on Ω. Then $N = \mathcal{N} \cup \{1\}$ is a normal subgroup of G.*

Proof: Fix $\omega \in \Omega$ and put $H = C_G(\omega)$. If $g \in G \setminus H$, then $\omega \neq g\omega$ and so every element of $H \cap {}^g h$ as at leat two fixed-points, namely ω and $g\omega$. So by assumption $H \cap {}^g H = 1$. Moreover, if $\mu \in \Omega$ then $\mu = g\omega$ for some $g \in G$ and so $C_G(\mu) = {}^g H$. Thus $N = G \setminus \{g^h \mid g \in G, h \in H^\sharp\}$ and by 3.5.1, $N \trianglelefteq G$.

3.6 Quaternion Groups

Lemma 3.6.1 [**unique p**] *Let p be a prime and Q a non-cyclic p-group. Suppose that Q has a unique subgroup of order p. Then*

(a) [**a**] $|Q| \geq 8$.

(b) [**b**] *Q has a cylic subgroup of M of index p.*

(c) [**c**] $p = 2$.

(d) [**d**] *$|g| = 4$ for all $g \in Q \setminus M$.*

(e) [**e**] *${}^g h = h^{-1}$ for all $g \in Q \setminus M$ and $h \in M$.*

(f) [**f**] $|Z(Q)| = 2$.

Proof: Any abelian group is the product of cylic p groups. So Q is not abelian and $|G| \geq p^3$. So (a) holds. Let Z be the unique subgroup of order p in Q. Then $Z \trianglelefteq Q$ and so $Z \leq Z(Q)$. The $Z(Q/Z) \neq 1$ and so there exists $Z \leq F \trianglelefteq Q$ with $|F/Z| = p$. Then F is cylic of order p^2.

By **??** $|\mathrm{Aut}(F)|_p = p$ and so $|Q/C_Q(F)| \leq p$. Hence there exists a maximal subgroup M of Q with $F \leq M \leq C_Q(F)$. Then $F \leq Z(M)$ and so by induction and (f), M is cylic. So (b) holds.

Now let M be any cylic subgroup of $|Q|$ with $|M/Q| = p$ and let $x \in M$ with $M = \langle x \rangle$.

Let $y \in Q \setminus M$ and let $\tilde{M}$ be maximal subgroup of Q with $g \in \tilde{M}$. Put $D = M \cap \tilde{M}$. Then $Q = M\tilde{M}$, $Q' = [M, \tilde{M}] \leq D$ and $|M/D| = |\tilde{M}/D| = p$. Then $D = \langle x^p \rangle$. Put $i := |D|$.

Suppose first that $\tilde{M}$ is abelian. Then also $\tilde{M}$ is cyclic, $\tilde{M} = \langle y \rangle$ and $D \leq Z(M\tilde{M}) = Z(Q)$. Moreover $|x| = |y| = pi$ and so x^i and y^i both have order p. Hence $Z = \langle x^i \rangle = \langle y^i \rangle$ and replacing y^j for some $1 \leq j < p$ we may assume $x^i y^i = 1$. Let $z = [x, y]$. The by 1.4.2(b), $z^p = [x^p, y] \in [D, \tilde{M}] = 1$. Thus by 1.4.2(c), $(xy)^i = z^{\binom{i}{2}} x^i y^i = z^{\binom{i}{2}}$.

If $|i| > 2$, then $p \mid \binom{i}{2}$. So $(xy)^i =$. But then $D\langle xy \rangle$ abelian, but not cyclic, a contradiction.

Thus $i = 2$, $p = 2$, $|Q| = 8$ and $|x| = |y| = |xy| = 4$. Also ${}^y x \neq x$ and ${}^y x = x^{-1}$. So the lemma holds in this case.

Suppose next that $\tilde{M}$ is not abelian. Then by induction (a)-(d) hold for $\tilde{M}$. In particular, either $|D| = 4$ and $\tilde{M}| = 8$ and or D is the unique cyclic subgroup of order i in $\tilde{M}$. In either case y has order 4 and y inverts D. In particular (d) holds and $({}^y x)^2 = x^{-2}$. There are only two elements in M whose square is x^{-2} namely x^{-1} and zx^{-1}, where $1 \neq z \in Z$.

Suppose that ${}^y x = x^{-1}z$. Since $|y| = 4$, $|y^2| = 2$ and $y^2 = z$ and $y = y^{-1}z$. So $yxy^-1 = x^{-1}z$ implies $xyxy^{-1}x^{-1} = 1$ and $|xy|^2 = 1$, a contradiction.

Thus ${}^y x = x^{-1}$ and so (e) holds. Let $a \in Z(Q)$. By (e), $a \in M$ and again (e), $a = a^-1$ and so $a^2 = 1$. Thus $a \in Z$ and $Z(Q) = Z$. So (f) holds.

Let Q be as in the preceeding lemma and $n = |Q|$. Then Q is called a quaternion group of order n.

Lemma 3.6.2 [**char table q2n**] *Let $n \geq 2$, Q a quaternion group of order 2^{n+1}, $x \in Q$ with $|x| = 2^n$ and $y \in Q \setminus \langle x \rangle$. Put $z = x^{2^{n-1}}$.*

(a) [**a**] *Let Q has $2^{n-1} + 3$ conjugacy classes namely $\{1\}, \{z\}$, $\{x^{2i}y \mid 0 \leq i < 2^{n-1}\}$, $\{x^{2i+1}y \mid 0 \leq i < 2^{n-1}\}$ and $\{x^i, x^{-i}\}, 1 < i < 2^{n-1}$.*

(b) [**b**] *$1, z, y, xy, x^i, 1 \leq i < 2^{n-1}$ is transversal to conjuagacy classes of Q.*

(c) [**c**] *$C_Q(1) = C_Q(z) = Q$, $C_Q(y) = \langle y \rangle$, $C_Q(xy) = \langle xy \rangle$ and $C_Q(\langle x^i \rangle = \langle x \rangle$ for $1 \leq i < 2^{n-1}$.*

(d) [**d**] *$Q' = \langle x^2 \rangle$.*

(e) [**e**] *Up to isomorphism there are four 1-dimensional $\mathbb{K}Q$ module $S_{\epsilon_x, \epsilon_y} = \mathbb{K}$, $(\epsilon_x, \epsilon_y) \in \{pm\} \times \{\pm\}$ with basis $xk = \epsilon_x k$ and $yk = \epsilon_y k$ for all $k \in \mathbb{K}$.*

(f) [**f**] *Let ξ be a primitive 2^n-root of unity in $\mathbb{K}$. Up to isomorphism there are $2^{n-1} - 1$ 2-dimensional $\mathbb{K}Q$ module $S_{\xi^j}, 1 \leq i < 2^{n-1}$ with basis u, v such that the matrices of x and y are*

$$x \leftrightarrow \begin{pmatrix} \xi^j & 0 \\ 0\xi^{-j} & \end{pmatrix} \quad y \leftrightarrow \begin{pmatrix} 0 & 1 \\ (-1)^j & 0 \end{pmatrix}$$

(g) [**g**] *The character table of $\mathbb{K}Q$ is*

	1	z	y	xy	x^i
S_{++}	1	1	1	1	1
S_{+-}	1	1	-1	-1	1
S_{-+}	1	1	1	-1	$(-1)^i$
S_{--}	1	1	-1	1	$(-1)^i$
S_{ξ^j}	2	$(-1)^j \cdot 2$	0	0	$\xi^{ij} + \overline{\xi}^{ij}$

Proof: (a) Let $M = \langle x \rangle$ and $h \in M$. Then by 3.6.1 $yhy^{-1} = h^{-1}$. Since $Q = M \cup yM$ and M centralizes h, we conclude that ${}^Q h = \{h, {}^y h\} = \{h, h^{-1}\}$. If $h = 1, z$ we have $h = h^{-1}$. Otherwise $h \neq h^{-1}$ and $\{h, h^{-1}\} = \{x^i, x^{-i}\} = \{x^i, x^{2n-i}\}$ for some $1 \leq i < 2^{n-1}$.

Next let $g \in Q \setminus M$. Then $Q = M \cup Mg$ and so ${}^Q g = {}^M g$. We have

$$x^i g x^{-i} = x^i g x^{-1} g^{-1} g = x^i x^i g = x^{2i} g.$$

Hence

$$^{Q}y = \{x^{2i}y \mid 0 \leq i < 2^{n-1}\} \text{ and } ^{Q}xy = \{x^{2i+1}y \mid 0 \leq i < 2^{n-1}\}$$

So (a) holds.

(b) follows immediately from (a).

(c) Cleary $C_Q(1) = Q = C_Q(z)$, If $1 \leq i < 2^{n-1} - 1$, then $[y, x^i] \neq 1$ and so $C_Q(x^i) = M$. For $g \in Q \setminus H$ we have $C_M(g) = \langle z \rangle \in \langle g \rangle$ and so $C_Q(g) = \langle g \rangle C_M(\langle g \rangle = \langle g \rangle$.

(d) $[x, y] = x^y x{-}1 = xx = x^2$.

(e) Let S be 1-dimensional $\mathbb{K}Q$-module. Then $Q/C_S(Q)$ is abelian and so $Q' \leq C_S(Q)$. Hence both x^2 and $z = y^2$ are in $C_S(Q)$ and so both x and y acts as $\pm \mathrm{id}_S$ on S.

(f) Let S be a simple module $\mathbb{K}Q$-module with $\dim_{\mathbb{K}} S \geq 2$. Let u be an eigenvector with eigenvalue λ for x on S. Since $|x| = 2^n$, $\lambda = \xi^j$ for some $0 \leq j < 2^n$. Let $v = yu$. Then $xv = xyu = y \cdot y^{-1}xy \cdot u = yx^{-1}u = y\lambda^{-1}u = \lambda^{-1}u$. So v is an eigenvector with eigenvalue $\xi^{-j} = \xi 2^n - j$. Replacing u by v if necessary we may assume that $0 \leq j \leq 2^{n-1}$. Note also that $yv = y^2u = zu = \xi^{2^{n-1}j}u$. Since $\xi^{2^{n-1}}$ has order two, $\xi^{2^{n-1}} = -1$ and so $yv = (-1)^j$. In particular, $\mathbb{K}u + \mathbb{K}v$ is a $\mathbb{K}Q$-submodule and since S is simple $S = \mathbb{K}u + \mathbb{K}v$. So (u, v) is a $\mathbb{K}$-basis for S.

Suppose that $i = 0$ or $i = 2^{n-1}$. Then $x^2u = u$ and $x^2v = v$. Hence $Q' \leq C_Q(S)$. But simple modules for abelian groups are 1-dimensional, a contradiction. Thus $1 \leq j < 2^{n-1}$ and so (f) holds.

(g) From (f) the matrices for elements in (c) on S_{ξ^j} are

$$x^i \leftrightarrow \begin{pmatrix} \xi^{ij} & 0 \\ 0 & \xi^{-ij} \end{pmatrix} \qquad y \leftrightarrow \begin{pmatrix} 0 & 1 \\ (-1)^j & 0 \end{pmatrix}$$
$$z \leftrightarrow \begin{pmatrix} (-1)^j & 0 \\ 0 & (-1)^j \end{pmatrix} \quad xy \leftrightarrow \begin{pmatrix} 0 & \xi^j \\ (-\xi)^{-j} & 0 \end{pmatrix}$$

Also $\xi^{-1} = \overline{\xi}$ and (g) is readily verified. □

Lemma 3.6.3 [**quaternion**] *Let n be an integer of with $n \geq 2$. Then there exists a quaternion group of order 2^{n+1} and any quaternion group of order 2^{n+1} isomorphic to the group with generators and relations*

$$\langle x, y \mid x^{2^n} = 1, y^2 = x^{2^{n-1}}, yxy^{-1} = x^{-1} \rangle.$$

Proof: Let $P = \langle x, y \mid x^{2^n} = 1, y^2 = x^{2^{n-1}}, yxy^{-1} = x^{-1} \rangle$. We first show

1° [**1**] *$|x| = 2^n$ and $y \notin \langle x \rangle$.*

For this let $\mathbb{F}$ be any field containing an element λ of multiplicative order 2^n. Put

$$a = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \quad b = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

Then $|a| = 2^n$, $b^2 = -\mathrm{id} = a^{2^{n-1}}$, $bab^{-1} = a^{-1}$ and $b \notin \langle a \rangle$. Hence there exists a homomorphism $\alpha : P \to \langle a, b \rangle$ with $\alpha(x) = a$ and $\alpha(y) = b$ and so (1°) holds.

2° [**2**] $|P| = 2^{n+1}$.

Since y normalizes $< x\rangle$, $P = \langle x, y \rangle = \langle x \rangle \langle y \rangle$. Since $y^2 \in \langle x \rangle$, (1°) gives $|\langle y \rangle \langle x \rangle / \langle x \rangle| = 2$ and $\langle x \rangle = 2^n$. So (2°) holds.

3° [**3**] *P is quaternion group.*

P is not abelian and so not cyclic. If $u \in P \setminus \langle x \rangle$ then $u = x^i y$ for some i. So

$$u^2 = x^i y x^i y = x^i y x^i y^{-1} y^2 = x^i x^{-i} y^2 = y^2 \neq 1.$$

Moreover $\langle x \rangle$ contains a unique involution and so (3°) holds.

4° [**4**] *Let Q be a quaternion group of order 2^{n+1}. Then $Q \cong P$.*

By 3.6.1 Q fulfills the relations for P and so is a quotient of P. Since $|P| = |Q|$, $P \cong Q$. □

3.7 Groups with quaternion Sylow 2-subgroup

Definition 3.7.1 [**def:ti-set**] *Let G be a group and $T \subseteq G$. Then T is called a* TI-set *in G if for all $A \neq B \in {}^G T$, $A \cap B \subseteq 1$.*

Lemma 3.7.2 [**trivial ti**] *Let T be a TI-set in G. Then $T \leq N_G(T)$.*

Proof: Let $t \in T$. Then $t = {}^t t \in T \cap {}^t T$ and so $T = {}^t T$. □

Lemma 3.7.3 [**induced ti**] *Let T be TI sets in G and put $N = N_G(T)$. Let $a, b \in Z(\mathbb{K}N) \cap \mathbb{K}T$.*

(a) [**a**] $a^G \mid_{T^\sharp} = a$

(b) [**b**] *If $a_1 = 0$, then $(a^G \mid b^G)_G = (a \mid b)_N$.*

Proof:

Let $\mathcal{R}$ be a transversal to N with $1 \in \mathcal{R}$.

(a) Then $a^G = \sum_{r \in \mathcal{R}} rar^{-1} = \sum_{t \in T} \sum_{r \in \mathcal{R}} a_t {}^r t$. If $t \in T^\sharp$, then $t \notin {}^r T$ for all $1 \neq r \in \mathcal{R}$. Thus the coefficent of t in a^G is a_t and so (a) holds.

(b) By Frobenius reciprocity, $(a^G \mid b^G)_G = (a^G \mid_N \mid b)_N$.

Since $b_n = 0$ for $n \in N \setminus X$ and $a_1 = 0$ we have conclude that from (a)

$$(a^G \mid_N \mid b)_N = \frac{1}{|N|} \sum_{t \in T^\sharp} a_t b_t = (a \mid b)_N.$$

□

Theorem 3.7.4 (Brauer-Suzuki) [**brauer-suzuki**] *Let G be a finite group, p a prime and $S \in \mathrm{Syl}_p(G)$. Suppose S contains a unique subgroup Z of order p and that $N_G(S) = SC_G(S)$. Then $[Z, G] \leq O_{p'}(G)$.*

Proof:

Suppose first that S is abelian. Then $S \leq Z(N_G(S))$. So by 1.5.6, $G = SO_{p'}(G)$ and so the theorem holds in this case.

Suppose next that S is not abelian. Then by 3.6.1 $p = 2$ and S is a quaternion group of order 2^n, $n|geq3$.

1° [**0**] *Let M be the subgroup generated by all the elements of order p in G. Then M acts transitively on the cyclic subgroups of order p in G and $M = \langle M^Z \rangle$.*

Let $T \leq G$, $|T| = p$. Since $S \cap M$ is a Sylow p-subgroup of G, $T^m \leq S \cap M$ for some $m \in M$. So $T^m = Z$ and so $M = \langle M^Z \rangle$.

If the theorem holds for any subgroup of G containing M we conclude that $|M/O_{p'}(M) = 2$ and the theorem holds.

We may assume that $G = MS$. Suppose that $M \cap S$ is cylic. Since $p = 2$, $\mathrm{Aut}(M \cap S)$ is a 2-group and we are done by the cylic case.

So $M \cap S$ is not cylic and so has order at least 8. Note that the assumption $N_G(S) = SC_G(S)$ is automatically fulfilled if $|S| \geq 16$. So we may assume that $|G/M| \leq 2$.

Suppose that $|S| = 8$. Put $D = \mathrm{Der}_S(G)$. We claim that $D = S'$.. Let $s \in S$ and $g \in G$ with ${}^g s \in S$. If $|s| \leq 2$ we get ${}^g s \leq S'$. So suppose that $|s| = 4$. Then both $\langle s \rangle$ and ${}^g\langle s \rangle$ are normal in S and so by 1.5.5, ${}^g < s\rangle = {}^h s$ for some $h \in N_G(S)$. Since $N_G(S) = C_G(S)S$ we may choose $h \in S$ and so ${}^g\langle s \rangle = \langle s \rangle$ and $[g, s] \in S'$. So indeed $D = S'$. Hence $S \cap G' = S'$ and $M \cap S$ is cylic a contradiction.

Thus $|S| \leq 16$ and S has a unique cyclic subgroup H of order index two. Let P and U be the subgroups of H of index 2 and 4 respectively. Then $|P| \geq 4$, $P \not\leq Z(S)$ and so $C_S(P) = H$. Let $C = C_G(P)$ and $N = N_G(P)$. Then $S \in \mathrm{Syl}_2(N)$ and since $\mathrm{Aut}(P)$ is a 2-group, $N = CS$. In particular, $H = S \cap C \in \mathrm{Syl}_2(C)$ and so $C = HK$ and $H \cap K = 1$, where $K = O^2(C)$. Let

$$X = \{g \in C \mid |P| \mid |g|\} = C \setminus UK$$

We will show that

2° [**1**] *X is a TI-set on G and $N_G(X) = N$.*

Let $x \in X$ and $g \in G$ with $y = {}^g x \in X$. Then $|P| \mid |y|$ and so $\langle y \rangle$ contains a subgroup T of order $|P|$. Then $T \leq PK$. But $[P, K] = 1$ and so P is the unique Sylow 2-subgroup of PK. Thus $T = P$ and $g^P = P$. So $g \in N$ and ${}^g X = X$. So (2°) holds.

Let λ be a linear (that is 1-dimensional) character of C with $\ker \lambda = UK$. Put $\theta = \lambda^N - 1_C^N$.

3° [**2**] *$\theta \leq \mathbb{K}X$ and $(\theta \mid \theta)_N = 3$.*

For $g \in UK = \ker \lambda$ we have $\lambda(1) = 1_C(g)$. Thus $\lambda \in \mathbb{K}X$. Since X is normal subset of N we het $\theta \in \mathbb{K}X$.

Since $1_C^N(1) = 2$ and $(1_C \mid 1_N) = (1_C \mid 1_C) = 1$, $1_C^N = 1_N + \mu$ for some linear character $\mu \neq 1_N$. Since $P = S' \nleq \ker \lambda$, $P \nleq \ker \lambda^N$. Thus the 2-dimensional character λ^G is not the sum of linear characters and so λ^N is simple. $\theta = \lambda^G - 1_N - \mu$ now implies $(\theta \mid \theta) = 3$.

4° [**3**] *$\theta^G \mid X = \theta \mid_X$ and $\theta^G = \chi_1 - \chi_2 - 1_G$ for simple characters χ_1, χ_2 of G.*

By (3°) and 3.7.3, the first statement holds and $(\theta^G \mid \theta^G) = 3$. Also $(\theta^G \mid 1_G) = (\theta \mid 1_N) = -1$ and so

$$\theta^G = \pm\chi_1 \pm \chi_2 - 1_G$$

for some simple characters χ_i. Since $\theta^G(1) = \theta(1) = 0$ we have $\pm\chi_1 \pm \chi_2(1) = 1 > 0$ we may assume $\pm\chi_1(1) \geq 1$ and so $\pm\chi_2(1) \leq 0$. So (4°) holds.

5° [**4**] *K be the set on involutions in G. Then K is a conjugacy class and $|ab|$ is odd for $a, b \in \mathcal{K}$.*

The first statement follows from (1°). Suppose $|ab|$ is even and let u be the involution in $\langle ab \rangle$. Then $\langle u, a \rangle$ is a 2-group containing two different involutions, a contradiction.

6° [**5**] *Let $a = a_K^2$. Then $a(g)\theta_G(g) = 0$ for all $g \in G$. In particular $(a \mid \theta^G) = 0$.*

Let $g \in G$ with $a(g) \neq 0$. Then $g = de$ for some $d, e \in d, e \in \mathcal{K}$. Thus by (5°), g has odd order and so is not conjugate to an element of X. Thus (3°) implies $\theta(g) = 0$.

7° [**6**] *$ka = \sum_{S \in \mathcal{S}} \frac{\chi_S(z)^2}{d_S} \chi_S$ for $1 \neq z \in Z$ and some $0 \neq k \in \mathbb{Q}$.*

Let $k = \frac{|C_G(z)|^2}{|G|}$. Note that $z \in \mathcal{K}$. $z^2 = 1$ implies that any eigen value for z is ± 1 and so $\chi_S(z) = \overline{\chi}_S(z)$ for all $S \in \mathcal{S}$. Thus (7°) follows from 3.2.17(b) applied with $C = D = K$.

8° [**7**] $z \in \ker \chi_1$ *and* $d_1 > 1$.

From (6°) and (5°) $(ka \mid \chi_1 - \chi_2 - 1_G)$. So from (7°) and $(\chi_S \mid \chi_T) = \delta_{ST}$

$$(*) \qquad \frac{\chi_1(z)^2}{d_1} - \frac{\chi_2(z)^2}{d_2} - 1 = 0$$

where $d_i = \chi_i(1)$. For $u \in \{1, z\}$ (3°) and (4°) imply $\theta^G(u) = 0$ and so $\chi_2(u) = \chi_1(u) - 1$. Let $x = \chi_1(z)$ and $d = d_1$. Substitution into (*) gives:

$$\begin{array}{rcl} \frac{x^2}{d+1} - \frac{(x-1)^2}{d-1} - 1 & = & 0 \\ x^2(d-1) - (x-1)^2 d - d(d-1) & = & 0 \\ x^2 d - x^2 - x^2 d + 2xd - d - d^2 + d & = & 0 \\ -(x^2 - 2xd + d^2) & = & 0 \\ (x-d)^2 & = & 0 \end{array}$$

So $x = d$. That is $\chi_1(1) = d_1$ and so (8°) holds.

From $z \in \ker \chi_1$ we get $M \le \ker \chi_1$ and so $|G/\ker \chi_1| \le 2$. But a group of order at most 2 does not not have a non-linear character. Thus contradiction completes the proof.□

Chapter 4

Linear Algebra

4.1 Bilinear Forms

Definition 4.1.1 [**def:bilinear form**] *Let R be a ring, V an R-module and W a right R-module and $s : V \times W \to R, (v, w) \to (v \mid w)$ a function. Let $A \subseteq V$ and $B \subseteq W$. Suppose that s is R-bilinear, that is $(\sum_{i=1}^{n} r_i v_i \mid \sum_{j=1}^{m} w_j s_j) = \sum_{i=1}^{n} \sum_{j=1}^{m} r_i (v_i \mid w_j) s_j$ for all $v_i \in V, w_j \in W$ and $r_i, s_j \in R$. Then*

(a) [**a**] *s is called a* bilinear form.

(b) [**b**] *s is called* symmetric *if $V = W$ and $(v \mid w) = (w \mid v)$ for all $v, w \in V$.*

(c) [**z**] *s is called* symplectic *if $V = W$ and $(v \mid v) = 0$ for all $v \in V$.*

(d) [**c**] *Let $v \in V$ and $w \in W$ we say that v and w are* perpendicular *and write $v \perp w$ if $(v \mid w) = 0$.*

(e) [**d**] *We say that A and B are perpendicular and write $A \perp B$ if $a \perp b$ for all $a \in A$, $b \in B$.*

(f) [**e**] *$A^\perp = \{w \in W \mid A \perp w\}$ and ${}^\perp B = \{v \in V \mid v \perp B\}$. $A^\perp$ is called the right* perp *of A and ${}^\perp B$ the left perp of B.*

(g) [**f**] *If A is an R-submodule of V, define $s_A : W \to A^*$ by $s_A(w)(a) = (a \mid w)$ for all $a \in A, w \in W$.*

(h) [**g**] *If B is an R-submodule of W, define $s_B : V \to B^*$ by $s_B(v)(b) = (v \mid b)$ for all $v \in V, b \in B$.*

(i) [**h**] *s is called non-degenerate if $V^\perp = 0$ and ${}^\perp W = 0$.*

(j) [**i**] *If V is free with basis $\mathcal{V}$ and W is free with basis $\mathcal{W}$, then the $\mathcal{V} \times \mathcal{W}$ matrix $M_{\mathcal{V}}^{\mathcal{W}}(s) = (\,(v \mid w)\,)_{v \in \mathcal{V}, w \in \mathcal{W}}$ is called the* Gram Matrix *of s with respect to $\mathcal{V}$ and $\mathcal{W}$. Observe that the Gram Matrix is just the restriction of s to $\mathcal{V} \times \mathcal{W}$.*

Let I be a set, R a ring, $W = \textcircled{$\Pi$}_I R$ and $V = \bigoplus_I R$. Define $s : V \times W \to R$, $(v \mid w) = \sum_{i \in I} v_i w_i$. Note that this is well defined since almost all v_i are zero. Note also that if we view v and w as $I \times 1$ matrices we have $(v \mid w) = v^{\mathrm{T}} w$.

As a second example let V be any R-module and $W = V^*$ and define $(v \mid w) = w(v)$. If V is a free R-module this example is essentially the same as the previous:

Lemma 4.1.2 [**dual basis**] *Let V be a free R module with basis $\mathcal{V}$. For $u \in V$ define $u^* \in V^*$ by $u^*(v) = \delta_{uv}$. Define*

$$\phi_{\mathcal{V}} : V \to \bigoplus_{\mathcal{V}} R, v \to (w^*(v))_{w \in \mathcal{V}}$$

and

$$\phi_{\mathcal{V}*} : V^* \to \textcircled{Π}_{\mathcal{V}} R, \alpha \to (\alpha(v))_{v \in \mathcal{V}}$$

(a) [**a**] *Both $\phi_{\mathcal{V}}$ and $\phi_{\mathcal{V}*}$ are R-isomorphisms.*

(b) [**b**] *Let $w \in V^*$ and $v \in V$ and put $\tilde{v} = \phi_{\mathcal{V}}(v)$ and $\tilde{w} = \phi_{\mathcal{V}*}(w)$. Then $w(v) = \tilde{v}^{\mathrm{T}} \tilde{w}$.*

Proof: (a) Since V is free with basis $\mathcal{V}$, the map $\oplus_{\mathcal{V}} R \to V, (r_v) \to \sum_{v \in \mathcal{V}} r_v v$ is an R-isomorphism. Clearly $\phi_{\mathcal{V}}$ is the inverse of this map and so $\phi_{\mathcal{V}}$ is an R-isomorphism. To check that $\phi_{\mathcal{V}*}$ is an R-linear map of right R-modules recall first that V^* is a right R-module via $(wr)(v) = w(v)r$. Also $\textcircled{$\Pi$}_{\mathcal{V}} R$ is a right R-module via $(r_v)_v r = (r_v r)_v$. We compute

$$\phi_{\mathcal{V}*}(wr) = ((wr)(v))_v = (w(v)r)_v = (w(v))_v r$$

and so $\phi_{\mathcal{V}*}$ is R-linear. Given $(r_v)_v \in \textcircled{Π}_{\mathcal{V}} R$, then $w : V \to R, \sum_{v \in \mathcal{V}} s_v v \to \sum_{v \in \mathcal{V}} s_v r_v$ is the unique element of V^* with $w(v) = r_w$ for all $v \in \mathcal{V}$, that is with $\phi_{\mathcal{V}*}(w) = (r_v)_v$. So $\phi_{\mathcal{V}*}$ is a bijection.

(b) For $u \in \mathcal{V}$ let $s_u = u^*(v)$ and $r_u = w(u)$. Then $v = \sum_{u \in \mathcal{V}} s_u u$ and so $w(v) = \sum_{u \in \mathcal{V}} s_u w(u) = \sum_{u \in \mathcal{V}} s_u r_u = \tilde{v}^{\mathrm{T}} \tilde{w}$. □

Definition 4.1.3 [**dual map**] *Let R be a ring and $\alpha : V \to W$ an R-linear map. Then the R-linear map $\alpha^* : W^* \to V^*, \phi \to \phi \circ \alpha$ is called the* dual *of α.*

Lemma 4.1.4 [**matrix of dual**] *Let R be a ring and V and W free R modules with basis $\mathcal{V}$ and $\mathcal{W}$, respectively. Let $\alpha : V \to W$ be an R-linear map and M its matrix with respect to $\mathcal{V}$ and $\mathcal{W}$. Let $\delta \in W^*$. Then*

$$\phi_{\mathcal{V}*}(\alpha^*(\delta)) = M^{\mathrm{T}} \phi_{\mathcal{W}*}(\delta)$$

Proof: Let $v \in \mathcal{V}$. Then the v-coordinate of $\phi_{\mathcal{V}*}(\alpha^*(\delta))$ is $\alpha^*(\delta)(v) = (\delta \circ \alpha)(v) = \delta(\alpha(v))$. By definition of $M = (m_{wv})_{w \in \mathcal{W}, v \in \mathcal{V}}$, $\alpha(v) = \sum_{w \in \mathcal{W}} m_{wv} w$ and so

$$\phi_{\mathcal{V}*}(\alpha^*(\delta)) = (\delta(\alpha(v)))_v = (\sum_{w \in \mathcal{W}} m_{wv}\delta(w)) = M^{\mathrm{T}}\phi_{\mathcal{W}*}(\delta)$$

□

Lemma 4.1.5 [**associated non-deg form**] *Let R be a ring and $s : V \times W \to R$ an R-bilinear form. Let A be an R-subspace of V and B an R-subspace of W. Then*

$$\overline{s}_{AB} : A/A \cap {}^{\perp}B \times B/B \cap A^{\perp}, (a + (A \cap {}^{\perp}B), b + (B \cap A^{\perp}) \to (a \mid b)$$

is a well-defined non-degenerate R-bilinear form.

Proof: Readily verified. □

Lemma 4.1.6 [**basic bilinear**] *Let R be a ring and let $s : V \times W \to R$ be an R-bilinear form.*

(a) [**a**] *Let A be an R-subspace of V, then $A^{\perp} = \ker s_A$.*

(b) [**b**] *Let B be an R-subspace of W then ${}^{\perp}B = \ker s_B$.*

(c) [**c**] *s is non-degenerate if and only if s_V and s_W are 1-1.*

Proof: (a) and (b) are obvious and (c) follows from (a) and (b). □

Lemma 4.1.7 [**finite dim non-deg**] *Let $\mathbb{F}$ be a division ring and $s : V \times W \to \mathbb{F}$ a non-degenerate $\mathbb{F}$-bilinear form. Suppose that one of V or W is finite dimensional. Then both V and W are finite dimensional, both s_V and s_W are isomorphisms and $\dim_{\mathbb{F}} V = \dim_{\mathbb{F}} W$.*

Proof: Without loss $\dim_{\mathbb{F}} V < \infty$ and so $\dim V = \dim V^*$. By 4.1.6(c), s_V and s_W are 1-1 and so $\dim W \leq \dim V^* = \dim V$. So also $\dim W$ is finite and $\dim V \leq \dim W^* = \dim W$. Hence $\dim V = \dim W = \dim W^* = \dim V^*$. Since s_V and s_W are 1-1 this implies that s_V and s_W are isomorphisms. □

Corollary 4.1.8 [**dual s-basis**] *Let $\mathbb{F}$ be a division ring, $s : V \times W \to \mathbb{F}$ a non-degenerate $\mathbb{F}$-bilinear form, $\mathcal{B}$ a basis for V. Suppose that $\mathcal{B}$ is finite. Then for each $b \in \mathcal{B}$ there exists a unique $\tilde{b} \in W$ with $s(a, \tilde{b}) = \delta_{ab}$ for all $a, b \in B$. Moreover, $(\tilde{b} \mid b \in \mathcal{B})$ is an $\mathbb{F}$-basis for W.*

Proof: By 4.1.7 $s_V : W \to V^*$ is an isomorphism. Let $b^* \in V^*$ with $b^*(a) = \delta_{ab}$ and define $\tilde{b} = s_V^{-1}(b^*)$. □

Definition 4.1.9 [**def:s-dual basis**] *Let $\mathbb{F}$ be a division ring, $s : V \times W \to \mathbb{F}$ a non-degenerate $\mathbb{F}$-bilinear form, $\mathcal{B}$ a basis for V. A tuple $(\tilde{b} \mid b \in \mathcal{B})$ such that for all $a, b \in \mathcal{B}$, $\tilde{b} \in W$ $(a \mid \tilde{b}) = \delta_{ab}$ and $(\tilde{b} \mid b \in \mathcal{B})$ is basis for W is called the basis for W dual to $\mathcal{B}$ with respect to s.*

Definition 4.1.10 [**def:adjoint**] *Let R be ring , $s_i, V_i \times W_i \to R$ $(i = 1, 2)$ R-bilinear forms and $\alpha : V_1 \to V_2$ and $\beta : W_2 \to W_1$ R-linear maps. We say that α and β are adjoint (with respect to s_1 and s_2) or that β is an adjoint of α provided that*

$$(\alpha(v_1) \mid w_2)_2 = (v_1 \mid \beta(w_2))_1$$

for all $v_1 \in V_1$, $w_2 \in W_2$.

Lemma 4.1.11 [**basic adjoint**] *Let R be a ring , $s_i : V_i \times W_i \to R, (v, w) \to (v \mid w)_i$ $(i = 1, 2)$ R-bilinear forms and $\alpha : V_1 \to V_2$ and $\beta : W_2 \to W_1$ R-linear maps. Then α and β are adjoint iff $s_{1V_1} \circ \beta = \alpha^* \circ s_{2V_2}$.*

Proof: Let $v_1 \in V_1$ and $w_2 \in W_2$. Then

$$(\alpha v_1 \mid w_2)_2 = s_{2V_2}(w_2)(\alpha)(v_1) = (\alpha^*(s_{2V_2}(w_2))(v_1) = (\alpha^* \circ s_{2V_2})(w_2)(v_1)$$

and

$$(v_1 \mid \beta(w_2))_1 = s_{1V_1}(\beta(w_2))(v_1) = (s_{1V_1} \circ \beta)(w_2)(v_1)$$

and the lemma holds. □

Lemma 4.1.12 [**kernel of adjoint**] *Let R be a ring , $s_i : V_i \times W_i \to R$ $(i = 1, 2)$ R-bilinear forms and $\alpha : V_1 \to V_2$ and $\beta : W_2 \to W_1$ R-linear maps. Suppose α and β are adjoint. Then $\ker \alpha \leq {}^{\perp} \operatorname{Im} \beta$ with equality if ${}^{\perp}W_2 = 0$.*

Proof: Let $v_1 \in V_1$. Then

$$\begin{array}{cc}
 & v_1 \in \ker \alpha \\
\iff & \alpha(v_1) = 0 \\
\implies (\iff \text{ if } W_2^{\perp} = 0) & (\alpha(v_1) \mid w_2) = 0 \, \forall w_2 \in W_2 \\
\iff & (v_1 \mid \beta(w_2)) = 0 \, \forall w_2 \in W_2 \\
\iff & v_1 \in {}^{\perp} \operatorname{Im} \beta
\end{array}$$

□

Lemma 4.1.13 [**unique adjoint**] *Let R be a division ring, $s_i : V_i \times W_i \to R$ $(i = 1, 2)$ R-bilinear forms and $\alpha : V_1 \to V_2$ and $\beta : W_2 \to W_1$ R-linear maps. Suppose s_1 is non-degenerate and V_1 is finite dimensional over R.*

(a) [**a**] *There exists a unique adjoint α^{ad} of α with respect to s_1 and s_2.*

(b) [**b**] *Suppose that also s_2 is non-degenerate and V_2 is finite dimensional. Let $\mathcal{V}_i$ be a basis for V_i and $\tilde{\mathcal{V}}_i = (\tilde{v} \mid v \in \mathcal{V}_i)$ the basis W_i dual to $\mathcal{V}_i$ with respect to s_i. If M is the matrix of α with respect to $\mathcal{V}_1$ and $\mathcal{V}_2$, then M^{T} is the matrix for α^{ad} with respect to $\tilde{\mathcal{V}}_2$ and $\tilde{\mathcal{V}}_1$.*

Proof: (a) By 4.1.7 s_{1V_1} is an isomorphism and so by 4.1.11 $s_{1V_1}^{-1} \circ \alpha^* \circ s_{2V_2}$ is the unique adjoint of α. □

(b) Let $v_i \in \mathcal{V}_i$. Then the (v_1, v_2)-coefficient of M is $(\alpha(v_1) \mid \tilde{v}_2)_2$. By definition of the adjoint $(\alpha(v_1) \mid \tilde{v}_2)_2 = (v_1 \mid \alpha^{\mathrm{ad}}(\tilde{v}_2))_1$ and so (b) holds.

Corollary 4.1.14 [**dual basis for subspace**] *Let $\mathbb{F}$ be a field, V a finite dimensional $\mathbb{F}$-space and $s : V \times V \to \mathbb{F}$ an non-degenerate symmetric $\mathbb{F}$-bilinear form on V. Let W be an s-non-degenerate $\mathbb{F}$-subspace of V. Let $\mathcal{V}$ be an $\mathbb{F}$-basis for V and $\mathcal{W}$ an $\mathcal{W}$-basis for W. Let $\tilde{\mathcal{V}} = (\tilde{v} \mid v \in \mathcal{V}$ and $\tilde{\mathcal{W}} = (\tilde{w} \mid w \in \mathcal{W})$ be the corresponding dual basis for W and V, respectively. Let $M = (m_{vw})$ be the $\mathcal{V} \times \mathcal{W}$ matrix over $\mathbb{F}$ defined by*

$$v + W^{\perp} = \sum_{w \in \mathcal{W}} m_{vw} w + W^{\perp}$$

for all $v \in \mathcal{V}$. Then

$$\tilde{w} = \sum_{v \in \mathcal{V}} m_{vw} \tilde{w}$$

Proof: Since W is non-degenerate, $V = W \oplus W^{\perp}$. Let $\alpha : V \to W$ be the orthogonal projection onto W, that is if $v = w + y$ with $w \in W$ and $y \in W^{\perp}$, then $w = \alpha(v)$. Observe that the matrix of α with respect to $\mathcal{V}$ and $\mathcal{W}$ is M^{T}. Let $\beta : W \to V, w \to w$, be the inclusion map. Then for all $v \in V, w \in W$:

$$(\alpha(v) \mid w) = (v \mid w) = (v \mid \beta w)$$

and so β is the adjoint of α. Thus by 4.1.13(b) the matrix for β with respect to $\tilde{\mathcal{W}}$ and $\tilde{\mathcal{V}}$ is $M^{\mathrm{TT}} = M$. So

$$\tilde{w} = \beta(\tilde{w}) = \sum_{v \in \mathcal{V}} m_{vw} \tilde{w}.$$

□

Lemma 4.1.15 [**gram matrix**] *Let R be a ring, V a free R-module with basis $\mathcal{V}$ and W a free right R-module with basis $\mathcal{W}$. Let $\phi_{\mathcal{V}} : V \to \bigoplus_{\mathcal{V}} R$, $\phi_{\mathcal{W}} : V \to \bigoplus_{\mathcal{W}} R$, $\phi_{\mathcal{V}*} V^* \to \textcircled{Π}_{\mathcal{V}} R$ and $\phi_{\mathcal{W}*} W^* \to \textcircled{Π}_{\mathcal{V}} R$ be the associated isomorphisms. Let $s : V \times W \to R$ be bilinear form and M its Gram Matrix with respect to $\mathcal{V}$ and $\mathcal{W}$. Let $v \in V$, $w \in W$, $\tilde{v} = \phi_{\mathcal{V}}(v)$ and $\tilde{w} = \phi_{\mathcal{W}}(w)$,* *(a)* [**a**] $(v \mid w) = \tilde{v}^{\mathrm{T}} M \tilde{w}$.

(b) [**b**] $\phi_{\mathcal{V}}(V^{\perp}) = \mathrm{Null}(M)$, *the Null space of* M.

(c) [**c**] $\phi_{\mathcal{V}}(^{\perp}W) = \mathrm{Null}\, M^{\mathrm{T}}$

(d) [**d**] $\phi_{\mathcal{W}*}(s_W(v)) = M^{\mathrm{T}}\tilde{v}$.

(e) [**e**] $\phi_{\mathcal{V}*}(s_V(w)) = M\tilde{w}$.

Proof: (a) We have $v = \sum_{a \in \mathcal{V}} \tilde{v}_a a$, $w = \sum_{b \in \mathcal{W}} b\tilde{w}_b$ and $M = ((a \mid b))_{ab}$. Since s is R-bilinear,

$$(v \mid w) = \sum_{a \in \mathcal{V}, b \in \mathcal{W}} \tilde{v}_a (a \mid b) \tilde{w}_b = \tilde{v}^{\mathrm{T}} M \tilde{w}$$

(b) By (a) $w \in V^{\perp}$ iff $\tilde{v}^{\mathrm{T}} M \tilde{w} = 0$ for all $\tilde{v}$, iff $M\tilde{w} = 0$ and iff $\tilde{w} \in \mathrm{Null}(M)$.
(c) $v \in {}^{\perp}W$ iff $\tilde{v}^{\mathrm{T}} M = 0$, iff $M^{\mathrm{T}}\tilde{v} = 0$ iff $\tilde{v} \in \mathrm{Null}\, M^{\mathrm{T}}$.
(d) Let $u = s_W(v)$ and $\tilde{u} = \Phi_{\mathcal{W}*}(v)$. Then by "right-module" version of 4.1.2

$$u(w) = \tilde{w}^{\mathrm{T}} \cdot_{\mathrm{op}} \tilde{u} = \tilde{u}^{\mathrm{T}} \cdot \tilde{w}.$$

On the other hand

$$u(w) = s_W(v)(w) = (v \mid w) = \tilde{v}^{\mathrm{T}} M \cdot \tilde{w} =$$

Thus $\tilde{u}^{\mathrm{T}} = \tilde{v}^{\mathrm{T}} M$ and so $\tilde{u} = M^{\mathrm{T}} v$ and (d) holds.
(e) Let $u = s_V(w)$ and $\tilde{u} = \Phi_{\mathcal{V}*}(u)$. Then by 4.1.2

$$u(v) = \tilde{v}^{\mathrm{T}} \cdot \tilde{u}.$$

On the otherhand

$$u(v) = s_V(w)(v) = (v \mid w) = \tilde{v}^{\mathrm{T}} \cdot M\tilde{w}.$$

So $\tilde{u} = M\tilde{w}$ and (e) holds. □

Lemma 4.1.16 [**gram matrix of dual basis**] *Let* $\mathbb{F}$ *be a division ring and* $s : V \times W \to \mathbb{F}$ *a non-degenerate* $\mathbb{F}$*-bilinear form. Let* $\mathcal{V}$ *and* $\mathcal{W}$ *be* $\mathbb{F}$*-basis for* V *and* W *respectively and* $\tilde{\mathcal{V}}$ *and* $\tilde{\mathcal{W}}$*, the corresponding dual basis for* W *and* V*. Let* M *be the Gram matrix for* s *with respect to* $\mathcal{V}$ *and* $\mathcal{W}$*. Let* N *the Gram matrix for* s *with respect to* $\tilde{\mathcal{W}}$ *and* $\tilde{\mathcal{V}}$*. Then*

(a) [**a**] M^{T} *is the matrix for* id_V *with respect to* $\mathcal{V}$ *and* $\tilde{\mathcal{W}}$.

(b) [**b**] N *is the matrix for* id_W *with respect to* $\mathcal{W}$ *and* $\tilde{\mathcal{V}}$

(c) [**c**] M *and* N *are inverse to each other.*

Proof: (a) We have $\mathrm{id}_V : V \overset{s_W}{\to} W^* \overset{s_W^{-1}}{\to} V$. By 4.1.15(d), the matrix of s_W with respect to $\mathcal{V}$ and $\mathcal{W}^*$ is M. By definiton of $\tilde{\mathcal{W}}$ the matrix of s_W^{-1} with respect to $\mathcal{W}^*$ and $\tilde{\mathcal{W}}$ is the identity matrix. So (a) holds.

(b) Similar to (a), use s_V and 4.1.15(e).

(c) By (b) N^{-1} is the matrix of id_W with respect to $\tilde{\mathcal{V}}$ and $\mathcal{W}$. Note that id_V is the adjoint of id_W. So by (a) and 4.1.13(b), $N^{-1} = M^{\mathrm{TT}} = M$. □

Lemma 4.1.17 [**circ and bilinear**] *Let R be a commutative ring, G a group and let V and W be RG-modules. Let $s : V \times W \to R$ be R-bilinear form.*

(a) [**a**] *s is G-invariant iff $(a^\circ v \mid w) = (v \mid aw)$ for all $a \in inRG$.*

(b) [**b**] *Let $a \in RG$. Then $\mathrm{A}_W(a) \leq (a^\circ V)^\perp$ with equality if $V^\perp = 0$.*

Proof: (a) Recall first for $a = \sum_{g\in G} a_g g \in Rg$, $a^\circ = \sum_{g \in G} a_g g^{-1}$. Thus

$$\begin{array}{rcl} & & s \text{ is } G \text{ invariant} \\ & \iff & (gu \mid gw) = (u \mid w) \quad \forall g \in G, u \in V, w \in W \\ (u \to v = gu \text{ is a bijection}) & \iff & (v \mid gw) = (g^{-1}v \mid w) \;\; \forall g \in G, v \in V, w \in W \\ (s \text{ is } R \text{ bilinear}) & \iff & (v \mid aw) = (a^\circ v \mid w) \;\; \forall a \in RG, v \in V, w \in W \end{array}$$

(b) By (a) a and a° are adjoints. So (b) follows from 4.1.12 □

Lemma 4.1.18 [**extending scalars and bilinear**] *Let $R \leq \tilde{R}$ be an extensions of rings and $s : V \times W \to R$ an R-bilinear form. There exists a unique $\tilde{R}$-bilinear form*

$$\tilde{s} : \tilde{R} \otimes_R V \times W \otimes_R \tilde{R} \to \tilde{R}, (a \otimes v, w \otimes b) = a((\mid v), w)b$$

for all $a, b \in \tilde{R}, v \in V, w \in V$.

Proof: Observe that the map

$$\tilde{R} \times V \times W \times \tilde{R}\ to \tilde{R}, (a, v, b, w) \to a((\mid v), w)b$$

is R-balanced in (a, v) and (b, w). The universal property of the tensor product now shows the existence of the map $\tilde{s}$. A simple calculation shows that $\tilde{s}$ is $\tilde{R}$-bilinear. □

Lemma 4.1.19 [**extending scalars and intersections**] *Let $\mathbb{F} \leq \mathbb{K}$ be an extension of division rings and V an $\mathbb{F}$ space.*

(a) [**a**] *Let $\mathcal{W}$ be a set of $\mathbb{F}$-subspaces of V. Then*

$$\bigcap_{W \in \mathcal{W}} \mathbb{K} \otimes W = \mathbb{K} \otimes \bigcap_{W \in \mathcal{W}} W$$

(b) [**b**] *Let $s : V \otimes W \to \mathbb{F}$ be an $\mathbb{F}$-bilinear form and extend s to a bilinear form $\tilde{s} : \mathbb{K} \otimes_{\mathbb{F}} V \times W \otimes_{\mathbb{F}} \mathbb{K} \to \mathbb{K}$ (see 4.1.18). Let X an $\mathbb{F}$-subspace of V. Then $\mathbb{K} \otimes_{\mathbb{F}} X^\perp = (\mathbb{K} \otimes X)^\perp$.*

Proof: (a) Suppose first that $\mathcal{W} = \{W_1, W_2\}$. Then there exists $\mathbb{F}$-subspaces X_i of W_i with $W_i = X_i \oplus (W_1 \cap W_2)$. Observe that $W_1 + W_2 = (W_1 \cap W_2) \oplus X_1 \oplus X_2$. For X an $\mathbb{F}$-subspace of V let $\overline{X} = \mathbb{K} \otimes_{\mathbb{F}} X \leq \mathbb{K} \otimes_{\mathbb{F}} V$. Then $\overline{W_i} = \overline{W_1 \cap W_2} \oplus \overline{X_i}$ and $\overline{W_1 + W_2} = \overline{W_1 \cap W_2} \oplus \overline{X_1} \oplus \overline{X_2}$ and so $\overline{W_1} \cap \overline{W_2} = \overline{W_1 \cap W_2}$. So (a) holds if $|\mathcal{W}| = 2$. By induction it holds if $\mathcal{W}$ is finite.

In the general case let $\overline{v} \in \overline{V}$. Then there exists a finite dimensional $U \leq V$ with $\overline{v} \in \overline{U}$ Moreover, there exists a finite subset $\mathcal{X}$ of $\mathcal{W}$ with $\overline{U} \cap \bigcap_{X \in \mathcal{X}} \overline{X} = \overline{U} \cap \bigcap_{X \in \mathcal{W}} \overline{X}$. By the finite case, $\overline{U} \cap \bigcap_{X \in \mathcal{X}} \overline{X} = \overline{U \cap \bigcap_{X \in \mathcal{X}} X}$ and so (a) is proved.

(b) Note that $X^\perp = \bigcap_{x \in X} x^\perp$. So by (a) we may assume that $X = \mathbb{F}x$ for some $x \in X$. If $X \perp V$, then also $\overline{X} \perp \overline{V}$ and we are done. Otherwise $\dim V/X^\perp = 1$ and so also $\dim \overline{V}/\overline{X^\perp} = 1$. From $\overline{X^\perp} \leq \overline{X}^\perp < \overline{V}$ we conclude that $\overline{X^\perp} = \overline{X}^\perp$. □

Lemma 4.1.20 [**symmetric form for p=2**] *Let $\mathbb{F}$ be a field with* $\operatorname{char} \mathbb{F} = 2$. *Define $\sigma : \mathbb{F} \to \mathbb{F}, f \to f^2$ and let $\mathbb{F}^\sigma$ by the $\mathbb{F}$-space with $\mathbb{F}^\sigma = \mathbb{F}$ as abelian group scalar multiplication $f \cdot_\sigma k = f^2 l$. Let s a symmetric form on V and define $\alpha : V \to \mathbb{F}^\sigma : v \to (v \mid v)$. Then α is $\mathbb{F}$-linear, $W := \ker \alpha = \{v \in V \mid (v \mid v) = 0\}$ is an $\mathbb{F}$-subspace, $s \mid_W$ is a symplectic form and* $\dim_{\mathbb{F}} V/W \leq \dim_{\mathbb{F}} \mathbb{F}^\sigma = \dim_{\mathbb{F}^2} \mathbb{F}$.

Proof: Since $(v+w \mid v+w) = (v \mid v) + (v \mid w) + (w \mid v) + (w \mid w) = (v \mid v) + 2(v \mid w) + (w \mid w) = (v \mid v) + (w \mid w)$ and $(fv \mid fv) = f^2(v \mid v) = f \cdot_\sigma (v \mid v)$ conclude that α is $\mathbb{F}$-linear. Thus $W = \ker \alpha$ is an $\mathbb{F}$-subspace of V and $V/W \cong \operatorname{Im} \alpha$. Also $\dim_{\mathbb{F}} \operatorname{Im} \alpha \leq \dim_{\mathbb{F}} \mathbb{F}^\sigma$. The map $(\sigma, \mathrm{id}_{\mathbb{F}} : \mathbb{F} \times \mathbb{F}^\sigma \to \mathbb{F}^2 \times \mathbb{F}, (f, k) \to (f^2, k)$ provides an isomorphism of the $\mathbb{F}$ space $\mathbb{F}^\sigma$ and the $\mathbb{F}^2$-space $\mathbb{F}$. So $\dim_{\mathbb{F}} \mathbb{F}^\sigma = \dim_{\mathbb{F}^2} \mathbb{F}$.

Cleary $s \mid_W$ is a symplectic form. □

Lemma 4.1.21 [**symplectic forms are even dimensional**] *Let $\mathbb{F}$ be a field, V a finite dimensional $\mathbb{F}$-space and s a non-degenerate symplectic $\mathbb{F}$-form on V. Then there exists an $\mathbb{F}$-basis $v_i, i \in \{\pm 1, \pm 2, \ldots \pm n\}$ for V with $(v_i \mid v_j) = \delta_{i,-j} \cdot \operatorname{sgn}(i)$. In particular* $\dim_{\mathbb{F}} V$ *is even.*

Proof: Let $0 \neq v_1 \in V$. Since $v_1 \notin 0 = V^\perp$, there exists $v \in V$ with $(v_1 \mid v) \neq 0$. Let $v_{-1} = (v_1 \mid v)^{-1} v$. Then $(v_1 \mid v_{-1}) = 1 = -(v_{-1} \mid v_1)$. Let $W = \mathbb{F}\langle v_1, v_{-1} \rangle$. The Gram Matrix of s on W with respect to (v_1, v_{-1}) is $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. So the Gram matrix has determinant $1 \neq 0$. Thus W is non-degenerate and so $V = W \oplus W^\perp$. Hence also $W^\perp$ is non-degenerate and the theorem follows by induction on $\dim_{\mathbb{F}} V$. □

Lemma 4.1.22 [**selfdual and forms**] *Let $\mathbb{F}$ be field, G a group and V simple $\mathbb{F}G$ module. Suppose that V is self-dual (that is $V^* \cong V$ as $\mathbb{F}G$-module).*

(a) [**a**] *There exists a non-degenerate G-invariant symplectic or symmetric form s on V.*

(b) [**b**] *Suppose that* $\operatorname{char}\mathbb{F} = 2$ *and* $\mathbb{F}$ *is perfect. Then either* $V \cong \mathbb{F}_G$ *or* s *is symplectic.*

(a) Let $\alpha : V \to V^*$ be an $\mathbb{F}G$-isomorphism and $t : V \times V \to \mathbb{F}, (v, w) \to \alpha(v)(w)$, the corresponding G-invariant $\mathbb{F}$-bilinear form. Since V is a simple $\mathbb{F}G$-module any non-zero G-invariant bilinear form on V is non-degenerate.

Define $r(v, w) = t(v, w) + t(w, v)$. Then r is a symmetric form. If $r \neq 0$, then (a) holds with $s = r$. If $r = 0$ then $t(v, w) = -t(w, v)$ for all $v, w \in V$. If $\operatorname{char}\mathbb{F} = 2$, then t is symmetric and (a) holds with $s = t$. If $\operatorname{char}\mathbb{F} \neq 2$, then $t(v, v) = -t(v, v)$ implies that t is symplectic. So again (a) holds with $s = t$.

(b) Let s be as in (a) and observe that in either case of (a), s is symmetric. Let $\alpha : V \to \mathbb{F}\sigma$ be as in 4.1.20. View $\mathbb{F}^\sigma$ as an $\mathbb{F}G$-module with G acting trivially. Then by 4.1.20 α is $\mathbb{F}$ linear and since S is G-invariant also $\mathbb{F}G$-linear. Since $\mathbb{F}$ is perfect, $\dim_{\mathbb{F}} F^\sigma = 1$. So $\mathbb{F}^\sigma \cong \mathbb{F}_G$ has $\mathbb{F}G$-modulo and either $\alpha = 0$ or α is onto. If $\alpha = 0$, s is symplectic. If α is onto $\ker\alpha \neq V$ is an $\mathbb{F}G$-submodule of V. Since V is simple, $\ker\alpha = 0$ and so $V \cong \operatorname{Im}\alpha = F^\sigma \cong \mathbb{F}_G$. □

Chapter 5

Representations of the Symmetric Groups

5.1 The Symmetric Groups

For $n \in \mathbb{Z}^+$ let $\Omega_n = \{1, 2, 3 \ldots, n\}$ and $\mathrm{Sym}(n) = \mathrm{Sym}(\Omega_n)$. Let $g \in \mathrm{Sym}(n)$ and let $O(g) = \{O_1, \ldots 0_k\}$ be the sets of orbits for g on Ω_n. Let $|O_i| = n_i$ and choose notation such that $n_1 \geq n_2 \geq n_3 \geq \ldots n_k$. Define $n_i = 0$ for all $i > 1$. Then the sequence $(n_i)_{i=1}^{\infty}$ is called the cycle type of g. Pick $a_{i0} \in O_i$ and define $a_{ij} = g^j(a_{i0})$ for all $j \in \mathbb{Z}$. Then $a_{ij} = a_{ik}$ if and only if $j \equiv k \pmod{n)_i}$. The denote the element g by

$$g = (a_{11}, a_{12}, \ldots a_{1n_1})(a_{21}, a_{22}, \ldots, a_{2n_2}) \ldots (a_{k1}, a_{k2}, \ldots a_{kn_k}).$$

Lemma 5.1.1 [**conjugacy classes in sym(n)**] *Two elements in $Sym(n)$ are conjugate if and only if they have the same cycle type.*

Proof: Let g be as above and $h \in Sym(n)$. Then

$$hgh^{-1} = \\ (h(a_{11}), h(a_{12}), \ldots h(a_{1n_1}))(h(a_{21}), h(a_{22}), \ldots, h(a_{2n_2})) \ldots (h(a_{k1}), h(a_{k2}), \ldots h(a_{kn_k}))$$

and the lemma is now easily proved. □

Definition 5.1.2 [**def:partition of n**] *A* partition *of $n \in \mathbb{N}$ is a non decreasing sequence $\lambda = (\lambda_i)_{i=1}^{\infty}$ of non-negative intergers with $n = \sum_{i=1}^{\infty} \lambda_i$.*

Note that if λ is a partion of n the necessarily $\lambda_i = 0$ for almost all i. For example $(4, 4, 4, 3, 3, 1, 1, 1, 1, 0, 0, 0, \ldots)$ is a partition of 22. We denote such a partition by $(4^3, 3^2, 1^4)$.

Observe that the cycle type of $g \in \mathrm{Sym}(n)$ is a partition of n. Together with 3.1.3(f) we conclude

Lemma 5.1.3 [**number of partitions**] *Let $n \in \mathbb{Z}^+$. The follwing numbers are equal:*

(a) [**a**] *The numbers of partitions of n.*

(b) [**b**] *The numbers of conjugacy classes of* $\mathrm{Sym}(n)$*.*

(c) [**c**] *The number of isomorphism classes of simple* $\mathbb{C}\mathrm{Sym}(n)$*-modules.* □

Our goal now is to find an explicit 1-1 correspondence between the set of partions of n and the simple $\mathbb{C}\mathrm{Sym}(n)$-modules. We start by associating a $\mathrm{Sym}(n)$-module M^λ to each partition λ of n. But this modules is not simple. In later section we will determine a simple section of M^λ.

Definition 5.1.4 [**def:lambda partition**] *Let I be a set of size n and λ a partition of n. A λ-partition of I is a sequence $\Delta = (\Delta_i)_{i=1}^\infty$ of subsets of Δ such that*

(a) [**a**] $I = \bigcup_{i=1}^\infty \Delta_i$

(b) [**b**] $\Delta_i \cap \Delta_j = \emptyset$ *for all* $1 \leq i < j < \infty$*.*

(c) [**c**] $|\Delta_i| = \lambda_i$*.*

For example $(\{1,3,5\},\{2,4\},\{6\},\emptyset,\emptyset,\ldots)$ is a $(3,2,1)$ partition of I_6 where $I_n = \{1,2,3,\ldots n\}$. we will write such a partition as

$$\begin{array}{l}\hline 1\,3\,5\\ \hline 2\,4\\ \hline 1\\ \hline\end{array}$$

The lines in this array are a remainder that the order of the elements in the row does not matter. On the otherhand since sequences are ordered

$$\begin{array}{l}\hline 1\,3\,5\\ \hline 2\,4\,6\\ \hline\end{array} \neq \begin{array}{l}\hline 2\,4\,6\\ \hline 1\,3\,5\\ \hline\end{array}$$

Let $\mathcal{M}^\lambda$ be the set of all λ-partions of I_n. Note that $\mathrm{Sym}(n)$ acts on λ via $\pi\Delta = (\pi(\Delta_i))_{i=1}^\infty)$. Let $\mathbb{F}$ be a fixed field and let $M^\lambda = M^\lambda_\mathbb{F} = \mathbb{F}\mathcal{M}(\lambda)$. Then M^λ is an $\mathbb{F}\mathrm{Sym}(n)$-module. Note that for $M^{(n-1,1)} \cong \mathbb{F}I_n$. Let $(\cdot \mid \cdot)$ the unique bilinear form on M^λ with orthonormal basis $\mathcal{M}^\lambda$. Then by $(\cdot \mid \cdot)$ is $\mathrm{Sym}(n)$-invariant and non-degenerate.

5.2 Diagrams,Tableaux and Tabloids

Definition 5.2.1 [**def:diagram**] *Let $D \subseteq \mathbb{Z}_+ \times \mathbb{Z}_+$*

(a) [**z**] *Let $(i,j),(k,l) \in \mathbb{Z}^+ \times \mathbb{Z}^+$. Then $(i,j) \leq (k,l)$ provided that $i \leq k$ and $j \leq l$*

(b) [**a**] *D is called a* diagram *i if for all $d \in D$ and $e \in \mathbb{Z}_+ \times \mathbb{Z}_+$ with $e \leq d$ one has $e \in D$.*

(c) [**b**] *The elements of diagram are called the* nodes *of the diagram.*

(d) [**c**] *$r : \mathbb{Z}^+ \times \mathbb{Z}^+ \times (i, j) \to i$ and $c : \mathbb{Z}^+ \times \mathbb{Z}^+ \times (i, j) \to j$.*

(e) [**e**] *The i-th* row *of D is $D_i := D \cap \{i\} \times \mathbb{Z}^+$ and the j*-column *of D is $D^j := \mathbb{Z}^+ \times \{j\}$.*

(f) [**d**] *$\lambda(D) = (|D_i|)_{i=1}^{\infty}$ and $\lambda'(D) = (|D^j|)_j^{\infty}$*

Definition 5.2.2 [**def:diagram2**] *$\lambda \in \mathbb{Z}_+^{\infty}$ define*

$$[\lambda] = \{(i, j) \in \mathbb{Z}_+ \times \mathbb{Z}_+ \mid 1 \leq j \leq \lambda_i\}.$$

Lemma 5.2.3 [**basic diagram**] *Let $n \in \mathbb{N}$. Then the map $D \to \lambda_D$ is a bijection between the Diagram of size n and the partitions of n. The inverse is is by $\lambda \to [\lambda]$.*

Proof: Let D be a diagram of size n and put $\lambda = \lambda(D)$. Let $i \in \mathbb{N}$ and let j be maximal with $(i, j) \in D$. By maximality of j and the definition of a diagram, $(i, k) \in D$ iff $k \leq j$. Thus $j = |D_i| = \lambda_i$ and $D = [\lambda]$. Let $k \leq i$. Since $(i, \lambda_i) \in D$, the defintion of a diagram implies (k, λ_i) and so $\lambda_i \leq \lambda_k$. Thus λ is non-increasing. Clearly $\sum_{i=1}^{\infty} \lambda_i = |D| = n$ and so λ is a partition of n.

Conversely suppose that λ is a partition of n. Let $(i, j) \in D$ and $(a, b) \in \mathbb{Z}_+ \times \mathbb{Z}_+$ with $a \leq i$ and $b \leq j$. Then $a \leq i \leq \lambda_j \leq \lambda_b$ and so $(a, b) \in [\lambda]$. Thus $[\lambda]$ is a diagram. Clearly $|[\lambda]_i| = \lambda_i$, that is $\lambda([\lambda]) = \lambda$. □

We draw diagams as in the following example:

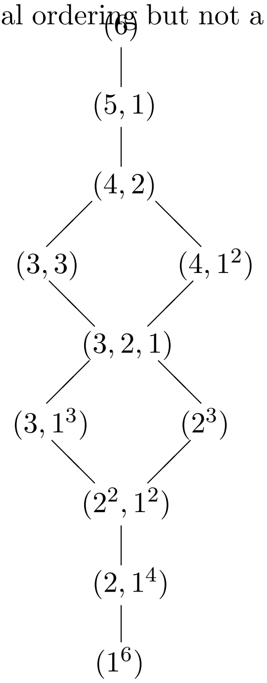
$$[5, 3^3, 2^2, 1] = \begin{array}{l} x\,x\,x\,x\,x \\ x\,x\,x \\ x\,x\,x \\ x\,x\,x \\ x\,x \\ x\,x \\ x \end{array}$$

Definition 5.2.4 [**def:dominates**] *Let λ and μ be partitions of $n \in \mathbb{Z}^+$. We say that λ dominates μ and write $\lambda \trianglerighteq \mu$ if*

$$\sum_{i=1}^{j} \lambda_i \geq \sum_{i=1}^{j} \mu_i$$

for all $j \in \mathbb{Z}^+$.

Note that “dominates” is a partial ordering but not a total ordering. For $n = 6$ we have



On rare occasions it will be useful to have a total ordering on the partition.

Definition 5.2.5 [**def:lexiographic ordering**] *Let λ and μ be partitions of $n \in \mathbb{Z}^+$. We write $\lambda > \mu$ provided that there exists $i \in \mathbb{Z}^+$ with $\lambda_i > \mu_i$ and $\lambda_j = \mu_j$ for all $1 \leq j < i$.*

Observe that $'' <''$ is a total ordering on the partitions of n, called the *lexiographic* ordering. If $\lambda \rhd \mu$ and i is minimal with $\lambda_i \neq mu_i$, then $\sum_{j=1}^{i-1} \lambda_j = \sum_{j=1}^{i-1} \mu_i$ and $\sum_{j=1}^{i} \lambda_j \geq \sum_{j=1}^{i} \mu_i$. Thus $\lambda_i \geq \mu_i$ and so $\lambda > \mu$.

Definition 5.2.6 [**def:conjugate partition**]

(a) [**a**] *Let $D \subseteq \mathbb{Z}^+ \times \mathbb{Z}^+$. Then $D' = \{(j, i) \mid (i, j) \in D\}$. D' is called the* conjugate *of D.*

(b) [**b**] *Let λ be a partition of n. Then $\lambda' = (|[\lambda]^i|)$ is the number of nodes in the i'th column of $[\lambda]$.*

Lemma 5.2.7 [**basic conjugate**]

(a) [**a**] *The conjugate of a diagram is a diagram.*

(b) [**b**] *Let D be a diagram. Then the rows of D' are the conjugates of the columns of D: $D'_i = (D^i)'$.*

(c) [**c**] *Let λ be a partition of n. Then λ' is a partition of n and $[\lambda]' = [\lambda']$.*

Proof: (a) follows immediately from the definition of a diagram.

(b) is obvious.

(c) By (b) $|[\lambda]'_i| = |[\lambda^i] = \lambda'_i$. Thus $\lambda' = \lambda([\lambda]')$. So (c) follows from 5.2.3. □

Lemma 5.2.8 [**reverse ordering**] *Let λ and μ be partitions of n. Then $\lambda \trianglerighteq \mu$ if and only if $\lambda' \trianglelefteq \mu'$.*

Proof: Let $j \in \mathbb{Z}^+$ and put $i = \mu'_j$.Define the following subsets of $\mathbb{Z}^+ \times \mathbb{Z}^+$

$$\begin{array}{c} Top = \{(a,b) \mid a \leq i\} \;\; Bottom = \{(a,b) \mid a > i\} \\ Left = \{(a,b) \mid b \leq j\} \;\; Right = \{(a,b) \mid b > i\} \end{array}$$

Since λ dominates μ:

$$|Top \cap [\lambda]| \geq |Top \cap [\mu]| \tag{1}$$

By definition of $i = \mu'_j$, $\lambda_i \geq j$ and $\lambda_{i+1} > j$. Thus

$$Top \cap Left \subseteq [\mu] \text{ and } Bottom \cap Right \cap [\mu] = \emptyset$$

Hence

$$|Top \cap Left \cap [\lambda]| \leq |Top \cap Left \cap [\mu]| \tag{2}$$

and

$$|Bottom \cap Right \cap [\lambda]| \geq |Bottom \cap Right \cap [\mu] \tag{3}$$

From (1) and (2) we conclude

$$|Top \cap Right \cap [\lambda]| \geq |Top \cap Right \cap [\mu]| \tag{4}$$

(3) and (4) imply:

$$|Right \cap [\lambda]| \geq |Bottom \cap [\mu]$$

Since $|[\lambda]| = n = |[\mu]|$ we conclude

$$|Left \cap [\lambda]| \geq Left \cap [\mu]$$

Thus $\sum_{c=1}^{j} \lambda'_c \leq \sum_{c=1}^{j} \mu'_c$ and $\lambda' \trianglelefteq \mu'$. □

Definition 5.2.9 [**def:tableau**] *Let λ be a partition of n. A* λ-tableau *is a function $t : [\lambda] \to I_n$.*

We denote tableaux as in the following example

$$\begin{array}{l} 5\,1\,4 \\ 2\,3 \end{array}$$

denotes the $[3,2]$-tableau $t : (1,1) \to 4, (1,2) \to 1, (1,3) \to 4, (2,1) \to 2, (2,2) \to 3$.

Definition 5.2.10 [**def:partition of tableau**] *Let $t : D \to I_n$ be a tableau. Then $\Delta(t) = (t(D_i))_{i=1}^{\infty})$ and $\Delta'(t) = (t(D^i))_{i=1}^{\infty}$. $\Delta(t)$ is called the* row partition *of t and $\Delta'(t)$ the* column partition *of t.*

Note that if t is a λ-tableau, then $\Delta(t)$ is a λ partition of I_n and $\Delta'(t)$ is a λ-partition of I_n. For example

$$\text{if } t = \begin{array}{l} 2\,4\,3 \\ 6\,1 \\ 5 \end{array} \quad \text{then } \Delta(t) = \begin{array}{l} \hline 2\,4\,3 \\ \hline 6\,1 \\ \hline 5 \\ \hline \end{array}$$

Definition 5.2.11 [**def:tabloids**] *Let s, t be λ-tableaux.*

(a) [**a**] *s and t are called* row-equivalent *if $\Delta(t) = \Delta(s)$. An equivalence class of this relations is called a* tabloid *and the tabloid containing t is denoted by $\overline{\underline{t}}$.*

(b) [**b**] *s and t are called* column-equivalent *if $\Delta'(t) = \Delta'(s)$. The equivalence class of this relations containing t is denoted by $|t|$.*

For example if $t = \begin{array}{l} 1\,4 \\ 2\,3 \end{array}$ then

$$\overline{\underline{t}} = \left\{ \begin{array}{c} \hline 1\,4 \\ \hline 2\,3 \\ \hline \end{array} \;,\; \begin{array}{c} \hline 4\,1 \\ \hline 2\,3 \\ \hline \end{array} \;,\; \begin{array}{c} \hline 1\,4 \\ \hline 3\,2 \\ \hline \end{array} \;,\; \begin{array}{c} \hline 4\,1 \\ \hline 3\,2 \\ \hline \end{array} \right\}$$

Lemma 5.2.12 [**action on tableaux**] *Let λ be partition of n. Let $\pi \in \mathrm{Sym}(n)$ and s, t be λ tableaux.*

(a) [**a**] $\mathrm{Sym}(n)$ *acts transitively on the set of λ-tableaux via $\pi t = \pi \circ t$.*

(b) [**b**] $\pi\Delta(t) = \Delta(\pi t))$.

(c) [**c**] *s and t are row equivalent iff πs and πt are row equivalent. In particular,* $\mathrm{Sym}(n)$ *acts on the set of λ-tabloids via $\pi\overline{\underline{t}} = \overline{\underline{\pi t}}$.*

Proof: (a) Clearly $\pi t = \pi \circ t$ defines an action of $\mathrm{Sym}(n)$ on the set of λ tableaux. Since s, t a bijections from $[\lambda] \to I_n$, $\rho := s \circ t^{-1} \in \mathrm{Sym}(n)$. Then $\rho \circ t = s$ and so the action is transitive.

(b) Let $D = [\lambda]$. Then $\Delta(t) = (D_i)_{i=1}^{\infty})$ and so

$$\pi\Delta(t) = \pi(t(D_i)_{i=1}^{\infty}) = (\pi(t(D_i)_{i=1}^{\infty}) = ((\pi t)(D_i))_{i=1}^{\infty} = \Delta(\pi t)$$

(c) s is row-equivalent to t iff $\Delta(s) = \Delta(t)$ and so iff $\pi\Delta(s) = \pi\Delta(t)$. So by (b) iff $\Delta(\pi s) = \Delta(\pi t)$ and iff πt and πs are row-equivalent. □

Let $\Delta = (\Delta_i)_{i=1}^{\infty}$ be λ-partition of I_n. Let $\pi \in \mathrm{Sym}(n)$. Recall that $\pi \in C_G(\Delta)$ means $\pi\Delta = \Delta$ and so $\pi(\Delta_i) = \Delta_i$ for all i.

$C_{\mathrm{Sym}(n)}(\Delta) = \bigcap_{i=1}^{\infty} N_{\mathrm{Sym}(n)}(\Delta_i)) = \textcircled{T}_{i=1}^{\infty} \mathrm{Sym}(\Delta_i)$. So $C_{\mathrm{Sym}(n)}(\Delta)$ has order $\lambda! := \prod_{i=1}^{\infty} \lambda_i!$.

Definition 5.2.13 [**def: row stabilizer**] *Let t be a tableau. The $R_t = C_{\mathrm{Sym}(n)}(\Delta(t)$ and $C_t = C_{\mathrm{Sym}}(t)(\Delta'(t)$. R_t is called the* row stabilzer *and C_t the* column stablizer *of t.*

Lemma 5.2.14 [**char row equiv**] *Let s and t be λ-tableaux. The s and t are row equivalent iff $s = \pi t$ for some $\pi \in R_t$.*

Proof: Then by 5.2.12(a), $s = \pi t$ for some $\pi \in \mathrm{Sym}(n)$. Then s is row-equivalent to t if and only if $\Delta(t) = \Delta(\pi t)$. By 5.2.12(b), $\Delta(\pi)t) = \pi\Delta(t)$ and so s and t are row equivalent iff $\pi \in R_t$. □

Lemma 5.2.15 [**basic combinatorical lemma**] *Let λ and μ be partions of n, t a λ-tableau and s a μ-tableau. Suppose that for all i, j, $|\Delta(t)_i \cap |\Delta'(s)_j| \leq 1$ (That is no two entrees from the same row of t lie in the same column of s). Then $\lambda \trianglelefteq \mu$. Moreover if $\lambda = \mu$, then there exists λ-tableau r such that r is row equivalent to t and r is column equivalent to s.*

Proof: Fix a column C of Changing the order the entrees of C neither effects the assumptions nor the conclusions of the lemma. So we may assume that if i appears before j in C, then i also lies earlier row than j in the tableau t. We do this for all the columns of s. It follows that an entree in the k-row of t must lie in one of the first k-rows of s. Thus $\sum_{r=1}^{k} \lambda_i \leq \sum_{r=1}^{l} \mu_i$ and μ dominates λ.

Suppose now that $\lambda = \mu$. Since $\lambda_1 = \mu_1$ and the firs row of t is contained in the first row of s, the first row of $\Delta(t)_1 = \Delta(s)_1$. Proceeding by induction we see that $\Delta_(t)_k = \Delta(s)_t$ for all s and t. So s and t are row equivalent. □

5.3 The Specht Module

Definition 5.3.1 [**def:fh**] *Let G be a group, $H \subseteq G$, R a ring and $f \in RG$. Then $f_H = \sum_{h \in H} f_h h$.*

Lemma 5.3.2 [**basic fh**] *Let G be a group, R a ring and $f \in RG$. Suppose that f view as a function is a multiplicative homomorphism.*

(a) [**a**] *Let $A, B \subseteq G$ such that the maps $A \times B \to G, (a,b) \to G$ is $1-1$, then $f_{AB} = f_A f_B$.*

(b) [**b**] *Let $A \leq B \leq G$ and T a left-transversal to A in B. Then $f_B = f_T f_A$.*

(c) [**c**] *Let $A_1, A_2, A_n \leq G$ and $A = \langle A_i \mid 1 \leq i \leq n\rangle$ Suppose $A = \mathop{\text{\textcircled{Π}}}_{i=1}^{n} A_i$, then $f_A = f_{A_1} f_{A_2} \dots f_{A_n}$.*

(d) [**d**] *Suppose f is a class function, then for all $g \in G$ and $H \subseteq G$, $g f_H g^{-1} = f_{gHg^{-1}}$.*

Proof: (a) Since the map $(a,b) \to ab$ is $1-1$, every element in AB can be uniquely written has ab with $a \in A$ and $b \in B$. Thus

$$\begin{aligned} f_A f_B = \quad & \textstyle\sum_{a \in A} f_a a \cdot \sum_{b \in B} f_b b & = \textstyle\sum a \in A, b \in B f_a f_b ab \\ = \textstyle\sum_{a \in A, b \in B} f_{ab} ab = & \textstyle\sum_{c \in AB} f_c c & \\ & = & f_{AB} \end{aligned}$$

(b) is a special case of (a).
(c) follows from (a) and induction on n.
(d) Readily verified.

Since the map $\underline{\overline{t}} \to \Delta(t)$ is a well defined bijection between the λ tabloids and the the λ partitions of I_n we will often identify $\underline{\overline{t}}$ with $\Delta(t)$. In particular, we have $\underline{\overline{t}} \in M^\lambda$.

Definition 5.3.3 [**polytabloid**] *Let t be λ-tableau.*

(a) [**a**] $k_t = \mathrm{sgn}_{C_t} = \sum_{\pi \in C_t} \mathrm{sgn}\pi\pi \in F\mathrm{Sym}(n)$.

(b) [**b**] $e_t = k_t \underline{\overline{t}} = \sum_{\pi \in C_t} \mathrm{sgn}\pi \underline{\overline{\pi t}} \in M^\lambda$. *$e_t$ is called a* polytabloid.

(c) [**c**] *S^λ is the F-subspace of M^λ spanned by the λ-polytabloids. S^λ is called a* Specht module.

(d) [**d**] *F^λ is the left ideal in $F\mathrm{Sym}(n)$ generated by the k_t, t a λ-tableau.*

As a first example consider $t = \begin{array}{l} 3\,2\,5 \\ 1\,4 \end{array}$.
The $C_t = \mathrm{Sym}(\{1,3\}) \times \mathrm{Sym}(\{\{2,4\}$,
$k_t = (1 - (13) \cdot (1 - (24)) = 1 - (13) - (24) + (13)(24)$ and
$e_t = \begin{array}{l} \hline 3\,2\,5 \\ \hline 1\,4 \\ \hline \end{array} - \begin{array}{l} \hline 1\,2\,5 \\ \hline 3\,4 \\ \hline \end{array} - \begin{array}{l} \hline 3\,4\,5 \\ \hline 1\,2 \\ \hline \end{array} + \begin{array}{l} \hline 1\,4\,5 \\ \hline 3\,2 \\ \hline \end{array}$

As a second example consider $\lambda = (n-1,1)$ and $t = \begin{matrix} i \cdots \\ j \end{matrix}$. Then $C_i = \mathrm{Sym}(\{i,j\} = \{1,(i,j)\}$ $k_t = 1-(i,j)$ and

$$e_t = \begin{array}{l}\hline i \dots \\ \hline j \\ \hline \end{array} - \begin{array}{l}\hline j \dots \\ \hline i \\ \hline \end{array}$$

For $i \in I_n$ put $x_i := (I_n \setminus, \{i\}) = \begin{array}{l}\hline 1\,2 \dots i-1\, i+1 \dots n \\ \hline i \\ \hline \end{array}$

Then $M^{(n-1,1)}$ is the $\mathbb{F}$ space with basis $(x_i, i \in I_n)$ and $e_t = x_j - x_i$. Thus

$$S^{(n-1,1)} = F\langle x_j - x_i \mid i \neq j \in I_n\rangle = \{\sum_{i=1}^n f_i x_i \mid f_i \in F \mid \sum_{i=1}^n f_i = 0\} = (x_1 + x_2 + \ldots + x_n)^\perp$$

The reader should convince herself that if $\mathrm{char}\,\mathbb{F} \nmid n$, then $S^{(n-1,1)}$ is a simple $\mathbb{F}\mathrm{Sym}(n)$-module and if $\mathrm{char}\,\mathbb{F} \mid n$, then $x := \sum_{i=1}^n x_i \in S^{(n-1,1)}$ and $S^{(n-1,1)}/\mathbb{F}x$ is a simple $\mathbb{F}\mathrm{Sym}(n)$-module.

Lemma 5.3.4 [**transitive on polytabloids**] *Let $\pi \in \mathrm{Sym}(n)$ and t a tableau.*

(a) [**z**] $\pi k_t \pi^{-1} = k_{\pi t}$

(b) [**a**] $\pi e_t = e_{\pi t}$.

(c) [**b**] $\mathrm{Sym}(n)$ *acts transitively on the set of λ-polytabloids.*

(d) [**c**] S^λ *is a $F\mathrm{Sym}(n)$-submodule of M^λ.*

(e) [**d**] *If $\pi \in C_t$, then $k_{\pi t} = k_t = \mathrm{sgn}\pi k_t$ and $e_{\pi t} = \mathrm{sgn}\pi e_t$.*

Proof:

(a) We have $C_{\pi t} = \pi C_t \pi^{-1}$ and so by 5.3.2(d) applied to the class function sgn on $\mathrm{Sym}(n)$,

$$k_{\pi t} = \mathrm{sgn}_{C_{\pi t}} = \mathrm{sgn}_{\pi C_t \pi^{-1}} = \pi \mathrm{sgn}_{C_t} \pi^{-1} = \pi k_t \pi^{-1}$$

(b) Using (b), $e_{\pi t} = k_{\pi t}\overline{\underline{\pi t}} = \pi k_t \pi^{-1} \pi \overline{\underline{t}} = \pi k_t \overline{\underline{t}} = \pi e_t$

(c) and (d) follow from (b).

(e) Since $\pi \in C_t$, $C_{\pi t} = C_t = C_t \pi$. Thus $k_t = k_{\pi t}$ and

$$\begin{array}{rcl} k_t = & \sum_{\alpha \in C_t} \mathrm{sgn}\alpha \cdot \alpha & = \sum_{\beta \in C_t} \mathrm{sgn}(\beta\pi) \cdot (\beta\pi) \\ = \mathrm{sgn}\pi \sum_{\beta \in C_{\pi t}} \mathrm{sgn}\beta \cdot \beta = & & \mathrm{sgn}\pi k_t \pi \end{array}$$

The second statement follows from the first and $\pi\overline{\underline{t}} = \overline{\underline{\pi t}}$. □

Lemma 5.3.5 [**action of es on ml**] *Let λ and μ be partitions of n.*

(a) [**a**] *If $F^\mu M^\lambda \neq 0$, then $\lambda \trianglelefteq \mu$.*

(b) [**b**] *If t and s are λ-tableau with $k_s\overline{\underline{t}} \neq 0$, then then $k_s\overline{\underline{t}} = \pm e_s$.*

Proof: Let s be a μ tableau and t and λ-tableau with $k_s\overline{\underline{t}} \neq 0$.

Suppose first that there exists a $i \neq j \in I_n$ such that i and j are on the same row of t and in the same column of s. Let $H = \mathrm{Sym}(\{i,j\} = \{1,(i,j)\}$. Then

$$\mathrm{sgn}_H\overline{\underline{t}} = \overline{\underline{t}} + \mathrm{sgn}((i,j))(i,j)\overline{\underline{t}} = \overline{\underline{t}} = \overline{\underline{b}} = 0.$$

Since i,j are in the same column of s, $H \leq C_s$ and we can choose a transversal $\mathcal{T}$ to H in C_s. Then

$$k_s\overline{\underline{t}} = (\mathrm{sgn}\mathcal{T})\mathrm{sgn}H\overline{\underline{t}} = 0,$$

contrary to our assumption. Thus no such i,j exists. So by 5.2.15 $\lambda \trianglelefteq \mu$. Moreover, if $\lambda = \mu$, there exists a λ tableau r which is row equivalent to t an columns equivalent to s. Hence $k_r = k_s$ and $\overline{\underline{r}} = \overline{\underline{s}}$. Moreover $\pi s = r$ for some $\pi \in C_s$ and so by 5.3.4(e),

$$k_s\overline{\underline{t}} = e_r = \mathrm{sgn}\pi e_s$$

□

Lemma 5.3.6 [**es self dual**] *Let λ and μ be partitions of n and s an μ-tableau. Then*

(a) [**a**] $k_S = k_S^\circ$

(b) [**b**] $(k_S M^\lambda)^\perp = \mathrm{A}_{M^\lambda}(k_s)$.

(c) [**c**] *$k_s M^\mu = Fe_s$ and $\mathrm{A}_{M^\mu}(k_s) = e_s^\perp$.*

(d) [**d**] *$k_s v = (v \mid e_s)e_s$ for all $v \in M^\mu$.*

Proof: (a) If $\pi \in C_s$ then also $\pi^{-1} \in C_s$. Moreover $\mathrm{sgn}\pi = \mathrm{sgn}\pi^{-1}$ and (a) holds.

(b) Follows from (a) and 4.1.17

(c) By 5.3.5 $e_S M^\lambda = Fe_s$ and so by (b) $\mathrm{A}_{M^\lambda}(k_s) = e_s^\perp$.

(d) By (c) $k_s v = fe_s$ for some $f \in F$. Hence

$$(v \mid e_s) = (v \mid k_s\overline{\underline{t}}) = (k_s v \mid \overline{\underline{t}}) = (fe_t \mid \overline{\underline{t}}) = f$$

□

Lemma 5.3.7 [**fl and ml**] *$F^\lambda M^\lambda = S^\lambda$ and $\mathrm{A}_{M^\Lambda}(F^\lambda) = S^{\lambda\perp}$.*

Proof: This follows immediately from 5.3.6(b) and 5.3.6(c). □

Lemma 5.3.8 [**submodules of ml**] *Supp F is a field and let λ be a partition of n and V be an $F\mathrm{Sym}(n)$-submodule of M^λ. Then either $F^\lambda V = S^\mu$ and $S^\mu \leq V$ or$F^\lambda V = 0$ and $S^\lambda \leq V$.*

Proof: If $F^\lambda V = 0$, then by 5.3.7, $V \leq S^{\lambda\perp}$.

So suppose $F^\lambda V \neq 0$. Then $k_sV \neq 0$ for some λ-tableau s. So 5.3.6 implies $k_sV = Fe_s = k_sM^\lambda$. Since by 5.3.4(a) implies $k_sV = k_sM^\lambda$ for all λ-tableaux s. Thus $F^\lambda V = F^\lambda M^\lambda = S^\lambda$ and $S^\lambda \leq V$. □

If $\mathbb{F} \leq \mathbb{K}$ is a field extensions we view $M^\lambda = M^\lambda_\mathbb{F}$ has a subset of S^μ. Note also that $M^\lambda_\mathbb{K}$ is canonically isomorphic to $\mathbb{K} \otimes_\mathbb{F} M^\lambda$. Put $D\lambda = S^\lambda/(S^\lambda \cap S^{\lambda\perp})$.

Lemma 5.3.9 [**dl=fldl**] *Let λ be a partition of n. If F is a field then $F^\lambda D^\lambda = D^\lambda$.*

Proof: By 5.3.8 either $F^\lambda S\lambda = S^\lambda$ or $S^\lambda \leq S^{\lambda\perp}$. In the first case $F^\lambda D^\lambda = D^\lambda$ and in the second $D^\lambda = 0$ and again $F^\lambda D^\lambda = D^\lambda$.

Proposition 5.3.10 [**dl=du**] *Let λ and μ be partitions of n with $D^\lambda = 0$. Suppose F is a field. If D^λ is isomorphic to an $F\mathrm{Sym}(n)$-section of M^μ, then $\lambda \trianglelefteq \mu$. In particular, $D^\lambda \cong D^\mu$ then $\lambda = \mu$.*

Proof: By 5.3.9 $F^\lambda D^\lambda = D^\lambda \neq 0$. Hence also $F^\lambda D^\mu \neq 0$ and $F^\lambda M^\mu \neq 0$. So by 5.3.5(a), $\lambda \trianglelefteq \mu$. If $D^\lambda \cong D^\mu$, the D^μ is a section of M^λ and so $\mu \trianglelefteq \lambda$ and $\mu = \lambda$. □

Lemma 5.3.11 [**scalar extensions of ml**] *Let λ be a partition of n and $\mathbb{F} \leq \mathbb{K}$ a field extension.*

(a) [**a**] $S^\lambda_\mathbb{K} = \mathbb{K}S^\lambda \cong K \otimes_\mathbb{F} S^\lambda$.

(b) [**b**] $S^{\lambda\perp}_\mathbb{K} = \mathbb{K}(S^{\lambda\perp}) \cong \mathbb{K} \otimes_\mathbb{F} S^{\lambda\perp}$.

(c) [**d**] $S^\lambda_\mathbb{K} \cap S^{\lambda\perp}_\mathbb{K} = \mathbb{K}(S^\lambda \cap S^{\lambda\perp}) = \mathbb{K} \otimes_\mathbb{F} S^\lambda \cap S^{\lambda\perp})$.

(d) [**c**] $D^\lambda_\mathbb{K} \cong \mathbb{K} \otimes_\mathbb{F} D^\lambda$.

Proof: (a) is obvious.

(b) follows from (a) and 4.1.19(b)

(a) follows from (a), (b) and 4.1.19(a).

(d) follows from (a) and (c). □

Lemma 5.3.12 [**dl absolutely simple**] *Let λ be a partition of n and suppose $D^\lambda \neq 0$. Then D^λ is an absolutely simple $\mathbb{F}Sym(n)$-module.*

Proof: By 5.3.11(d) it suffices to show that D^λ is simple. So let V be an $\mathbb{F}Sym(n)$-submodule of S^λ with $S^\lambda \cap S^{\lambda\perp} \leq V$. By 5.3.8 either $S^\lambda \leq V$ or $V \leq S^{\lambda\perp}$. In the first case $V = S^\lambda$ and in the second $V \leq S^\lambda \cap S^{\lambda\perp}$ and $V = S \cap S^{\lambda\perp}$. Thus $D^\lambda = S^\lambda/(S^\lambda \cap S^{\lambda\perp})$ is simple. □

5.4 Standard basis for the Specht module

Proposition 5.4.1 [**garnir relations**] *Let t be a λ-tableau, $i < j \in \mathbb{Z}^+$, $X \subseteq \Delta'(t)_i$ and $Y \subseteq \Delta'(t)_j$. Let $\mathcal{T}$ be any transversal to* $\mathrm{Sym}(X) \times \mathrm{Sym}(Y)$ *in* $\mathrm{Sym}(X \cup Y)$.

(a) [**a**] $\mathrm{sgn}_{\mathcal{T}}\, e_t$ *is independent from the choice of the tranversal $\mathcal{T}$.*

(b) [**b**] *If $|X \cup Y| > \lambda'_i$. Then*

$$\mathrm{sgn}_{\mathcal{T}} e_t = 0$$

Proof: (a) Let $\pi \in \mathrm{Sym}(X \cup Y)$ and $\rho \in \mathrm{Sym}(X) \times \mathrm{Sym}(Y) \leq C_t$. Then

$$\mathrm{sgn}(\pi\rho) \cdot \pi\rho \cdot e_t = \mathrm{sgn}(\pi)\pi \cdot \mathrm{sgn}(\rho)\rho e_t \overset{5.3.4(e)}{=} \mathrm{sgn}(\pi)\pi e_t$$

and so (a) holds.

(b) Since $|X \cap Y| > \lambda'_i \geq \lambda'_j$, there exists $i \in X$ and j in Y such that i and j are in the same row of t. So $(1 - (ij))\overline{\pi t} = 0$. If $\pi \in \mathrm{Sym}(X \cup Y)$, then π and $\pi \cdot (ij)$ lie in differen cosets of $\mathrm{Sym}(X) \times \mathrm{Sym}(Y)$. Hence we can choose $\mathcal{R} \subseteq \mathrm{Sym}(X \cup Y)$ such that $\mathcal{R} \cap \mathcal{R} \cdot (i,j) = \emptyset$ and $\mathcal{R} \cup \mathcal{R} \cdot (ij)$ is a transversal to $\mathrm{Sym}(X) \cup \mathrm{Sym}(Y)$. By (a) we may assume $\mathcal{T} = \mathcal{R} \cup \mathcal{R} \cdot (ij)$ and so

$$\mathrm{sgn}_{\mathcal{T}} = \mathrm{sgn}_{\mathcal{R}}\mathrm{sgn}_{\{1,(ij)\}} = \mathrm{sgn}_{\mathcal{R}} \cdot (1 - (ij))$$

and

$$\mathrm{sgn}_{\mathcal{T}} e_t = \mathrm{sgn}_{\mathcal{R}} \cdot (1 - (ij))e_t = 0.$$

□

Definition 5.4.2 [**def:garnir**] *Let t be a λ-tableau, $i < j \in \mathbb{Z}^+$, $X \subseteq \Delta'(t)_i$ and $Y \subseteq \Delta'(t)_j$.*

(a) [**a**] *$\mathcal{T}_{XY}$ is the set of all $\pi \in$ $\mathrm{Sym}(X \cup \mathrm{Sym}Y)$ such that the restrictions of $\pi \circ t$ to $\pi^{-1}(X)$ and $\pi^{-1}(Y)$ are increasing.*

(b) [**b**] *$G_{XYt} = \mathrm{sgn}_{\mathcal{T}_{XY}}$. G_{XYt} is called a* Garnir element *in* $F\mathrm{Sym}(n)$.

Lemma 5.4.3 [**basic garnir**] *Let t be a λ-tableau, $i < j \in \mathbb{Z}^+$, $X \subseteq \Delta'(t)_i$ and $Y \subseteq \Delta'(t)_j$.*

(a) [**a**] *$\mathcal{T}_{XY}$ is a transvsersal to $Sym(X)$* $\times \mathrm{Sym}(Y)$ *in* $\mathrm{Sym}(X \cup Y)$.

(b) [**b**] *If* $|X \cup Y| > \lambda'_i$. *Then*

$$G_{XYt}e_t = 0.$$

Proof: (a) Just observe that if $\pi \in \mathrm{Sym}(X \cup \mathrm{Sym}(Y)$, then there exists a unique element $\rho \in \mathrm{Sym}(X) \cup \mathrm{Sym}(Y)$ such that the restriction of $\pi\rho$ to $t^{-1}(X)$ and to $t^{-1}(Y)$ are increasing. (b) follows from (a) and 5.4.1(b). □

Consider $n = 5$, $\lambda = (3,2)$, $t = \begin{array}{c}\hline 1\,2\,3\\ \hline 4\,5\\ \hline\end{array}$, $X = \{2,5\}, Y = \{3\}$

Then $G_{XY}e_t = 0$ gives

$$\begin{array}{c}\hline 1\,2\,3\\ \hline 4\,5\\ \hline\end{array} - \begin{array}{c}\hline 1\,3\,2\\ \hline 4\,5\\ \hline\end{array} - \begin{array}{c}\hline 1\,2\,5\\ \hline 4\,3\\ \hline\end{array} = 0$$

Definition 5.4.4 [**def:increasing tableau**] *Let λ be a partion of n and t a λ-tableau.*

(a) [**a**] $r_t = r \circ t^{-1}$ *and* $c_t = s \circ t^{-1}$. *So $i \in I_n$ lies in row $r_t(i)$ and column $c_t(i)$ of t.*

(b) [**b**] *We say that t is row-increasing c_t is increasing on each row $\Delta_i(t)$ of t*

(c) [**c**] *We say that t is column-increasing if r_t is increasing on column $\Delta'_i(t)$.*

Note that r_t only depends on $\overline{\underline{T}}$ and so we will also write $r_{\overline{\underline{t}}}$ for r_t. Indeed $\overline{\underline{r}} = \overline{\underline{s}}$ iff $r_t = r_s$.

Lemma 5.4.5 [**basic increasing**] *Let λ be a partion of n and t a λ-tableau.*

(a) [**a**] *$\overline{\underline{t}}$ contains a unique row-increasing tableau.*

(b) [**b**] *$|t|$ contains a unique column-increasing tableau.*

(c) [**c**] *Let $\pi \in \mathrm{Sym}(n)$ and $i \in I$. Then $r_t(i)) = r_{\pi t}(\pi i)$.*

Proof: (a) and (b) are readily verfied.
(c) $r_{\pi t} \circ \pi = r \circ (\pi \circ t)^{-1} \circ \pi = r \circ t^{-1} = r_t$. □

Definition 5.4.6 [**def:standart tableau**] *Let λ be a partition of n and t a λ-tableau. A* standard tableau *is row- and column-increasing tableau. A tabloid is called standard if it contains a standard tableau. If t is a standard tableau, then e_t is called* standard polytabloid.

By 5.4.5(a), a standard tabloid contains a unique standard tableau.
We will show that the standard polytabloids form a basis of S^λ for any ring F.
For this we need to introduce a total order on the tabloids

Definition 5.4.7 [**def:order tabloids**] *Let $\overline{\underline{t}}$ and $\overline{\underline{s}}$ be the distinct λ-tabloids. Let $i \in I_n$ be maximal with $r_{\overline{\underline{t}}}(i) \neq r_{\overline{\underline{s}}}(i)$. Then $\overline{\underline{t}} < \overline{\underline{s}}$ provided that $r_{\overline{\underline{t}}}(i) < r_{\overline{\underline{s}}}(i)$.*

Lemma 5.4.8 [**basic order tabloids**] *$<$ is a total ordering on the set of λ tabloids.*

Proof: Any tabloid $\underline{\overline{t}}$ is uniquely determined by the tuple $(r_{\underline{\overline{t}}}(i))_{i=1}^n$. Moreover the ordering is just a lexiographic ordering in terms of it associated tuple. □

Lemma 5.4.9 [**proving maximal I**] *Let A and B be totally ordered sets amd $f : A \to B$ be a function. Suppose A is finite and $\pi \in \mathrm{Sym}(A)$ with $f \neq f \circ pi$. Let $a \in A$ be maximal with $f(a) \neq f(\pi(a))$. If f is non-decreasing then $f(a) > f(\pi(a))$ and if f is non-increasing then $f(a) < f(\pi(a))$.*

Proof: Reversing the ordering on F if necessary we may assume that f is non-decreasing. Let $J = \{j \in J \mid f(j) > f(a)\}$ and let $j \in J$. Since f is non-decreasing, $j > a$ and so by maximality of f, $f(\pi j) = f(j) > f(a)$. Hence $\pi(J) \subseteq J$. Since J is finite this implies $\pi(J) = J$ andso since π is $1-1$, $\pi(I \setminus J) \subseteq I \setminus J$. Thus $\pi(a) \notin J$, $f(\pi(a) \leq f(a)$ and since $f(\pi(a)) \neq f(a)$, $f(\pi(a)) < f(a)$. □

The above lemma is false if I is not finite (even if there exists a maximal a): Define $f : \mathbb{Z}^+ \to \{0, 1\}$ by $f(i) = 0$ if $i \leq 0$ and $f(i) = 1$ otherwise. Define $\pi : \mathbb{Z}^+\mathbb{Z}^+, i \to i + 1$. Then f is non-decreasing and $a = 0$ is the unique element with $f(a) \neq f(\pi(a))$. But $f(a) = 0 < 1 = f(\pi(a))$.

Allthough the lemma stays true if there exists a maximal a and f is increasing (decreasing). Indeed in thus case $J = C_I(\pi)$ and so $\pi(I \setminus J) = I \setminus J$.

Lemma 5.4.10 [**proving maximal**] *Let t be a λ-tableau and $X \subseteq I_n$.*

(a) [**a**] *Suppose that r_t is non-decreasing on X. Then $\underline{\overline{\pi t}} \leq \underline{\overline{t}}$ for all $\pi \in \mathrm{Sym}(X)$.*

(b) [**b**] *Suppose that r_t is non-increasing on X. Then $\underline{\overline{\pi t}} > \underline{\overline{t}}$ for all $\pi \in \mathrm{Sym}(X)$.*

Proof: (a) Suppose that $\underline{\overline{\pi t}} \neq \underline{\overline{t}}$. Let i be maximal in I_n with $r_t(i) \neq r_{\pi t}(i)$. Note that $r_{\pi t}(i) = r_t(\pi^{-1}(i)$ Since r_t is non-decreasing 5.4.9 gives $r_t(i) < r_t(\pi^{-1}i) = r_{\pi t}(i)$. Thus $\underline{\overline{t}} < \underline{\overline{\pi}} t$.

(b) Similar to (a). □

Lemma 5.4.11 [**maximal in et**] *Let t be column-increasing λ tableau. Then $\underline{\overline{t}}$ is the maximal tabloid involved in e_t.*

Proof: Any tabloid involved in e_t is of the form $\underline{\overline{\pi t}}$ with $\pi \in C_t$. Since r_t is increasing on each column, we can apply 5.4.10 to the restriction of π to each of the columns. So the result holds. □

Lemma 5.4.12 [**linear independent and order**] *Let $\mathbb{F}$ be ring, V a vector space with a totally ordered basis $\mathcal{B}$ and $\mathcal{L}$ a subset of V. Let $b \in \mathcal{B}$ and $v \in V$. We say that b is involved in v if the b-coordinate of v is non-zero. Let b_v be maximal element of $\mathcal{V}$ involved in v. Suppose that the $b_l, l \in \mathcal{L}$ are pair wise distinct and the coefficient f_l of b_l in l is not a left zero divisor.*

(a) [**a**] *$\mathcal{L}$ is linearly independent.*

(b) [**b**] *Suppose in addition that each $f_l, l \in \mathcal{L}$ is a unit and $\mathcal{L}$ is finite. Put $\mathcal{C} = \{b_l \mid l \in \mathcal{L}\}$ and $\mathcal{D} = \mathcal{B} \setminus \mathcal{C}$.*

  - *(a)* [**a**] *$\mathcal{L} \cup \mathcal{D}$ is an R-basis for M.*
  - *(b)* [**b**] *Suppose R is commutative and $(\cdot \mid \cdot)$ be the unique R bilinar form on M with orthormal basis $\mathcal{B}$. Then*
    - *(a)* [**a**] *For each $d \in \mathcal{D}$ there exists a unique $e_d \in d + R\mathcal{C}$ with $e_d \in \mathcal{L}^\perp$.*
    - *(b)* [**b**] *$(e_d \mid d \in \mathbb{D}$ is an R-basis for $\mathcal{L}^\perp$.*
    - *(c)* [**c**] *$\mathcal{L}^{\perp\perp} = R\mathcal{L}$.*

Proof: (a) Let $0 \neq (f_l) \in \bigoplus_{\mathcal{L}} F$. Choose $l \in \mathcal{L}$ with b_l maximal with respect to $f_l \neq 0$. Then $b_l > b_k$ for $l \neq k \in \mathcal{L}$ with $f_k \neq 0$. So b_l is involved in $f_l l$, but in not other $f_k k$. Thus $\sum_{l \in \mathcal{L}} f_l l \neq 0$ and $\mathcal{L}$ is linearly independent.

(b) We assume without loss that $f_l = 1$ for all $l \in \mathcal{L}$.

(b:a) Let $m = \sum_{b \in \mathcal{B}} m_b b \in M$. We need to show that $m \in R(\mathcal{D} \cup \mathcal{L}$. If $m_b = 0$ for all $b \in \mathcal{B}_{\mathcal{L}}$, this is obvious. Otherwise pick $b \in \mathcal{B}_{\mathcal{L}}$ maximal with $m_b \neq 0$ and let $l \in \mathcal{L}$ with $b = b_l$. Then by induction on b, $m - m_b l \in R(\mathcal{D} \cup \mathcal{L})$.

(b:b) We will first show that

$$(*) \qquad R \cap C \cap \mathcal{L}^\perp = 0$$

Let $0 \neq m = \sum_{l \in \mathcal{L}} m_l b_l$ and choose l with $m_l \neq 0$ and b_l minimal. Then $(m \mid l) = m_l \neq 0$ and $m \notin \mathcal{L}^\perp$.

(b:b:a) This is just the Gram Schmidt process. For completeness here are the details. Let $\mathcal{L} = \{l_1, l_2, \ldots l_n\}$ and $b_i = b_{l_i}$ with $b_1 < b_2 < \ldots b_n\}$. Put $e_0 = d$ and suppose inductively that we have found $e_i \in d + Rb_1 + \ldots + Re_i$ with $e_i \perp l_j$ for all $1 \leq j \leq e_i$. If $i < n$ put $e_{i+1} = e_i - (e_i \mid l_{i+1}) b_{l+1}$. Then $(e_{i+1} \mid l_{i+1} = 1$ and since $b_{i+1} \perp l_j$ for all $j \leq i$. Put $e_d = e_n$. By (*), e_d is unique.

(b:b:b)) Clearly $(e_d \mid d \in \mathcal{D})$ is R-linearly independent. Moreover if $m = \sum_{b \in caB} m_b b \in \mathcal{L}^\perp$, then $\tilde{m} := m - \sum_{d \in \mathcal{D}} m_d e_d \in R\mathcal{C} \cap \mathcal{L}^\perp$. So (*) implies $\tilde{m} = 0$ and (b:b:b) holds.

(b:b:c) $m = \sum_{b \in caB} m_b b \in \mathcal{L}^{\perp\perp}$. By (b:a) there exists $\tilde{m} \in R\mathcal{L}$ with $m = \tilde{m} \in R\mathcal{D}$ and so we may assume that $m_c = 0$ for all $c \in \mathcal{C}$. Then $0 = (m \mid e_d) = m_d$ for all $d \in \mathcal{D}$ and so $m = 0$. □

Theorem 5.4.13 [**standard basis**] *Let F be a ring and λ a partition of n. The standard polytabloids form a basis of S^λ. Moreover, $S^{\lambda\perp\perp} = S^\lambda$ and there exists an R-basis for S^λ indexed by the nonstandard λ-polytabloids.*

By 5.4.10(a) and 5.4.12 the standard polytabloids are linearly independent. Let t be λ-tableau. Let $|t|$ be the column equivalence class of t. Total order the column euqivalence classes analog to 5.4.7 We show by downwards induction that e_t is a F-linear combination of the standard polytableaux. Since $e_t = \pm e_s$ for any s column-equivalent to t we may assume that t is column increasing. If t is also row-increasing, t is standard tableaux and we are done. So suppose t is not row-increasing so there exists $(i,j) \in \mathbb{Z}^+\times$ such that $t(i,j) > t(i,j+1)$. Let $X = \{t(k,j) \mid i \leq k \leq \lambda'_i$ and $Y = \{t(k,j+1) \mid 1 \leq k \leq j$. Then $|X \cup Y| = \lambda'_j + 1$ and so by 5.4.1

$$\sum_{\pi \in \mathcal{T}_{XY}} \mathrm{sgn}\pi e_{\pi t} = 0$$

Since c_t is increasing on X and on Y and since $t(i,j) > t(i,j+1)$, r_t is non-increasing on $X \cup Y$. So by 5.4.10 $|\pi t| > |$— for all $1 \neq \pi \in Sym(X\cup)$. Thus by downwards induction $e_{\pi t}$ is an R-linear combination of the standard polytabloids. Hence the same is true for $e_t = -\sum_{1\neq\pi\mathcal{T}} \mathrm{sgn}\pi e_{\pi t}$.

The remaining statements now follow from 5.4.12. □

5.5 The number of simple modules

Definition 5.5.1 [**def:p-regular class**] *Let p be an integer. An element g in a group G is called p-singular if p divides $|g|$. Otherwise g is called p-regular. A conjugacy class is called p-regular if its elements are p-regular.*

The goal of this section is to show that if $\mathbb{K}$ is an algebraicly closed field, G is a finite group and $p = \operatorname{char} K$ then the number of isomorpism classes of simle $\mathbb{K}G$-modules equals the number of p-regular conjugacy classes.

Lemma 5.5.2 [**cyclic permutation**]

(a) [**a**] *Let G be a group, $n \in \mathbb{Z}^+$ and $a_1, \dots a_n \in G$. Then for all $i \in \mathbb{N}$ $a_{i+1}a_{i+2}\dots a_{i+n}$ is conjugate $a_1a_2\dots a_n$ in G.*

(b) [**b**] *Let R be a group, $n \in \mathbb{Z}^+$ and $a_1, \dots a_n \in R$. Then for all $i \in \mathbb{N}$, $a_{i+1}a_{i+2}\dots a_{i+n} \equiv a_1a_2\dots a_n \pmod{} S(R)$*

Proof: (a) We have $a_1^{-1} \cdot a_1a_2\dots a_n \dots a_1 = a_2 \dots a_n a_1$. So (a) follows by induction on n.

(b) $a_1 \cdot a_2 \dots a_n - a_2 \dots a_n \cdot a_1 \in \mathrm{S}(R)$ So (b) follows by induction on n. □

Definition 5.5.3 [**def: sr**] *Let R be ring and $p = \operatorname{char} R$. Then* $\mathrm{S}(R) = \langle xy - yx \mid x, y \in R\rangle_{\mathbb{Z}}$*. Let $\tilde{p} = p$ if $p \neq 0$ and $\tilde{p} = 1$ if $p = 0$.* $\mathrm{T}(R) = \{r \in R \mid r^{\tilde{p}^m} \in \mathrm{S}(R)$ *for some* $m \in \mathbb{N}\}$.

Lemma 5.5.4 [**sr for group rings**] *Let R be a commutative ring and G a group. Then* $\mathrm{S}(RG)$ *consists of all $a = \sum_{r_g g} \in RG$ with $\sum_{g\in\mathbb{C}} r_g = 0$ for all conjugacy classes C of G.*

Proof: Let U consists of $a = \sum_{r_g g} \in RG$ with $\sum_{g\in\mathbb{C}} r_g = 0$ for all conjuagacy classes C of G. Note that both $\mathrm{S}(R)$ and U are R-submodules. As an R-modules $\mathrm{S}(R)$ is spaned by the $gh - hg$ wth $g, h \in G$. By 5.5.2 gh and hg are conjugate in G. Thus $gh = hg \in U$ and $\mathrm{S}(R) \subseteq U$. U is spanned by the $g - h$ where g, h in G are conjuagte. Then $h = aga^{-1}$ and $g - h = a^{-1} \cdot ag = ag \cdot a^{-1}$ and so $g - h \in \mathrm{S}(R)$ and $U \subseteq \mathrm{S}(R)$. □

Lemma 5.5.5 [**basic sr**] *Let R be a ring with $p := \operatorname{char} R$ a prime.*

(a) [**a**] $(a+b)^{p^m} \equiv a^{p^m} + b^{p^m} \mod \mathrm{S}(R)$ *for all $a, b \in R$ and $m \in \mathbb{N}$.*

(b) [**b**] $\mathrm{T}(R)$ *is an additive subgroup of R.*

(c) [**c**] *Suppose that $R = \bigoplus_{i=1}^{s} R_i$. Then $S(R) = \bigoplus_{i=1}^{r} S_i$ and $T(R) = \bigoplus T(R_i)$.*

(d) [**d**] *Let I be an ideal in R. Then $S(R/I) = S(R) + I/I$.*

(e) [**e**] *Let I be a nilpotent ideal in R. Then $I \leq T(R)$, $T(R/I) = T(R)/I$ and $R/T(R) \cong (R/I)/T(R/I)$.*

Proof: (a) Let $A = \{a, b\}^p$ and let $H = \langle h\rangle$ be a cyclic group of order p acting on A via $h(a_i) = (a_{i+1})$. Then H has two fixed points on A namely the constant sequence (a) and (b). Since the length of any orbit of H divises $|H|$, all other orbits have lenghth p. Let C be an orbit of length p for H on A. For $a = (a_1, a_2, \ldots a_p) \in A$ puy $\prod a = a_1 a_2 \ldots a_p/$ Then by 5.5.2 $\prod a \equiv \prod b \pmod{} S(R)$ for all $a, b \in C$ and so $\sum_{b\in C} \prod b \equiv p \prod a = 0 \mod \mathrm{S}(R)$. Hence for $(a+b)^p = \sum_{\alpha in A} \prod a \equiv a^p + b^p \mod \mathrm{S}(R)$. (a) now follows by induction on m.

(b) Follows from (a).

(c) Obvious.

(d) Obvious.

(e) Since I is nilpotent, $I^k = 0$ for some integer k. Choose m with $p^m \geq k$. Then for all $i \in I$, $i^{p^m} = 0 \in \mathrm{S}(R)$ and so $i \in \mathrm{T}(R)$. Thus $I \leq \mathrm{T}(R)$. Since $S(R) + I/I = S(T/I)$ we have $T(R)/I \leq T(R/I)$. Conversely if $t + I \in T(R/I)$, then $t^{p^l} \in S(R) + I$. Since bith $\mathrm{S}(R)$ and I are in $T(R)$, (b) implies $t^{p^l} \in T(R)$ and so also $t \in T(R)$. □

Lemma 5.5.6 [**tr for group rings**] *Let $\mathbb{F}$ be an integral domain with $\operatorname{char} \mathbb{F} = p$. Let G be a periodic group and let $\mathcal{C}_p$ be the set of p-regular conjugacy classes of G. For $C \in \mathcal{C}_p$ let $g_C \in C$. Then $(g_C + \mathrm{S}(\mathbb{F}G) \mid C \in \mathcal{C}_p)$ is a F-basis for $\mathbb{F}G/\mathrm{S}(\mathbb{F}G)$.*

Proof: Let $g \in G$ and write $g = ab$ with $[a,b] = 1$, $a^{p^m} = 1$ and b, p-regular. Then $g^{p^m} - b^{p^m} = 0$ and so by 5.5.5(b), $g \equiv \quad \mod \mathrm{T}(\mathbb{F}G)$. Also by 5.5.4 $b \equiv g_C$ where $C = {}^G b$. $(g_C + (\ \mathbb{F}G) \mid C \in \mathcal{C}_p)$ is a spanning set for $\mathbb{F}G/\,\mathrm{S}(\mathbb{F}G)$. Now let $r_C \in R$ with

$$\sum_{C \in \mathcal{C}_r} r_c g_C \in \mathrm{T}(\mathbb{F}G)$$

Then there exists $m \in \mathbb{N}$ with $(\sum_{C \in \mathcal{C}_p} r_c g_C)^{p^m} \in \mathrm{S}(\mathbb{F}G)$. Since g_C is p-regular, $p \nmid g_C$ and so p is invertible in $\mathbb{Z}/|g_C|\mathbb{Z}$. Hence there exists $m_C \in \mathbb{Z}$ with $|g_C| \mid p^{m_C} - 1$. Put $k = m \prod_{C \in \mathcal{C}_p} m_C$. Then $g_C^{p^k} = g_C$ and $(\sum_{C \in \mathcal{C}_p} r_c g_C)^{p^k} \in \mathrm{S}(\mathbb{F}G)$. By 5.5.5(b),

$$\sum_{C \in \mathcal{C}_p} r_C^{p^k} g_C = \sum_{C \in \mathcal{C}_p} r_C^{p^k} g_C^p \in \mathrm{S}(\mathbb{F}G)$$

Thus 5.5.4 shows that $r_C^{p^k} = 0$ for all $C \in \mathcal{C}_p$. So also $r_C = 0$ and $(g_C + (\ \mathbb{F}G) \mid C \in \mathcal{C}_p)$ is a linearly independent. □

Lemma 5.5.7 [**sr for matrix ring**] *Let R be a commutative ring and $p = \operatorname{char} R$.*

(a) [**a**] $\mathrm{S}(\mathrm{M}_n(R))$ *consists of the trace zero matrices and* $M_n(R)/\,\mathrm{S}(M_n(R)) \cong R$.

(b) [**b**] $p = \operatorname{char} \mathbb{K}$ *is a prime, then* $\mathrm{T}(\mathrm{M}_n(R)) = \{a \in \mathrm{M}_n(R) \mid \mathrm{tr}(a)^{\tilde{p}^m} = 0 \textit{for somem} \in \mathbb{N}\}\}$.

(c) [**c**] *If R is a field, then* $\mathrm{S}(\mathrm{M}_n(R)) = \mathrm{T}(\mathrm{M}_n(R))$ *and* $M_n(R)/\,\mathrm{T}(M_n(R)) \cong R$.

Proof: Since $\mathrm{tr}(xy) = \mathrm{tr}(yx)$ and so $\mathrm{S}(\mathrm{M}_n(R)) \leq \ker \mathrm{tr}$. $\ker \mathrm{tr}$ is generted by the matrices E_{ij} and $E_{ii} - E_{jj}$ with $i \neq j$. $E_{ij} = E_{ii}E_{ij} - E_{ij}E_{ii}$ and so $E_{ij} \in \mathrm{S}(\mathrm{M}_n(R)$. $E_{ii} - E_{jj} = E_{ij}E_{ji} - E_{ji}E_{ij}$ and so $E_{ii} - E_{jj} \in \ker \mathrm{tr}$.

Suppose now that p is a prime and let $a \in M_n(R)$. Let $b = \mathrm{tr}(a)E_1 1$ and $c = a - b$. Then $\mathrm{tr} c = 0$, $c \in \mathrm{S}(\mathrm{M}_n(R))$ and so by 5.5.5 $a \in T(M_n(R)0$ if and only if $b \in \mathrm{T}(\mathrm{M}_n(R))$. Since $\mathrm{tr}(b^{p^m}) = \mathrm{tr}(a)^{p^m}$ the lemma is proved. □

Theorem 5.5.8 [**pmodular simple**] *Let G be a finite group, $\mathbb{F}$ an algebraicly closed field and $p = \operatorname{char} F$. Then the number of isomorphism classes of simple $\mathbb{F}G$-modules equals the number of p-regular conjugacy classes.*

Proof: By 5.5.6 the number of p' conjugacy classes is $\dim_{\mathbb{F}} \mathbb{F}G/\,\mathrm{T}(\mathbb{F}G)$.

Let $A = \mathbb{F}G/\mathrm{J}(\mathbb{F}G)$. By 6.3.4 $\mathrm{J}(\mathbb{F}G)$ is nilpotent and so by 5.5.5(e), $\mathbb{F}G/\,\mathrm{T}(\mathbb{F}G) \cong A/\,\mathrm{T}(A)$.

By 2.5.24 $R \cong \bigoplus_{i=1}^n \mathrm{M}_{d_i}(\mathbb{F})$, where n is the number of isomorphism classes of simple $\mathbb{F}G$-modules.

Thus by 5.5.5(c) and 5.5.7(c), $R/T(R) \cong \mathbb{F}^n$. So $\dim_{\mathbb{F}} \mathbb{F}G/\,\mathrm{T}(\mathbb{F}G)$ is the number of isomorphism classes of simple $\mathbb{F}G$-modules. □

5.6 p-regular partitions

Definition 5.6.1 [**def:p-regular partition**] *Let p and n be positive integers with p being a prime. A partition λ of n is called* p-singular, *if there eixsts $i \in \mathbb{N}$ with $\lambda_{i+1} = \lambda_{i+2} = \ldots = \lambda_{i+p}$. Otherwise λ is called* p-regular.

Lemma 5.6.2 [**p-regular=p-regular**] *Let p, n be positive integers with p beieng a prime. The number of p-regular conjugacy classes of* $\mathrm{Sym}(n)$ *equals the number of p-regular partitions of* $\mathrm{Sym}(n)$.

Proof: Let $g \in G$ and μ its cycle-type. Then g is p-regular iff none of the μ_i is divisible by p. Any such partions we can uniquely determined by a sequence $(z_i)_{p \nmid i}$ of non-negative integers with $\sum iz_i = n$, where j_i is the number of $k's$ with $\mu_k = i$. Any p-regular partion we can write as a sequence $(z_i)_{i=1}^{\infty}$ with $0 \leq j_i < p$.

Let $f = \frac{\prod_{i=1}^{\infty}(1-x^{pi})}{\prod_{i=1}^{\infty}(1-x^{i})}$ viewed as an element of $\mathbb{Z}(x))$, the ring of formal integral power series.

We compute f in two different ways:

(i) [**1**] Let $A = \mathbb{N} \setminus p\mathbb{N}$. For each i cancel the factor $1 - x^{pi}$ in the numerator and denumerator of f to obtain:

$$\begin{array}{rcccc} f & = & \prod_{p\in A} \frac{1}{1-x^i} & = & \prod_{p\in A} \sum_{j=0}^{\infty} x^{ij} \\ & = & \sum_{(j_i)\in\oplus_A\mathbb{N}} \prod_{i\in A} x^{ij_i} & = & \sum_{(j_i)\in\oplus_A\mathbb{N}} x^{\sum_{i\in A} ij_i} \end{array}$$

Thus the coefficent of x^n is the number of partions of n, none of whose parts is divisible by p. So the coefficent of x^n is the number of p-regular conjugacy classes in $\mathrm{Sym}(n)$.

(ii) [**2**] Let $B = \{0, 1, \ldots p - 1\}$.

$$\begin{array}{rcccc} f & = & \prod_{i=1}^{\infty} \frac{1-x^{pi}}{1-x^i} & = & \prod_{i=1}^{\infty} \sum_{j=0} p - 1x^j \\ & = & \sum_{(j_i)\in\oplus_\infty B} \prod x^{j_i} & = & \sum_{(j_i)\in\oplus_\infty B} x^{\sum_{i=1}^{\infty} ij_i} \end{array}$$

So the coefficient of x^n in f is the number of p-regular partitions.

□

Definition 5.6.3 [**def:glambda**] *Let λ be a partition of n and $F = \mathbb{Z}$. Then*

$$g^{\lambda} = \gcd\{(e_t \mid e_s) \mid t, s\lambda - \textit{tableaux}\}$$

Lemma 5.6.4 [**glambda and dlambda**] *Let λ be a partition of n. Then $D^{\lambda} = 0$ iff* $\operatorname{char} F \mid g^{\lambda}$.

Proof: Since S^λ is spanned by the λ-polytabloid we have

$$\begin{array}{rcl} & D^\lambda = 0 & \\ \iff & S^\lambda = S^\lambda \cap S^{\lambda\perp} & \\ \iff & S^\lambda \perp S^\lambda & \\ \iff & e_t \perp e_s & \forall \lambda - \text{tableaux} s, t \\ \iff & (e_t \mid e_s) & \forall \lambda\text{-tableaux} s, t \\ \iff & \operatorname{char} F \mid (e_t \mid e_s)_{\mathbb{Z}} & \forall \lambda\text{-tableaux} s, t \\ \iff & \operatorname{char} F \mid g^\lambda & \end{array}$$

□

Lemma 5.6.5 **[glambda]** *Let λ be a partition of n and for $F = \mathbb{Z}$ define*

$$g^\lambda = \gcd\{(e_t \mid e_s) \mid t, s\lambda - \textit{tableaux}\}$$

Let $z_j = |\{i \mid \lambda_i = j|\}$. Then g^λ divides $\prod_{j=1}^\infty (z_j!)^j$ and $\prod_{j=1}^\infty z_j!$ divides g^λ.

Define two λ-tabloids $\underline{\overline{s}}$ and $\underline{\overline{t}}$ to be equivalent $\{\Delta_i(t) \mid i \in \mathbb{Z}^+ = \{\Delta_i(s) \mid i \in \mathbb{Z}\}$, that is if $\underline{\overline{t}}$ and $\underline{\overline{s}}$ have the rows but in possible different orders. Define $Z_j = \{i \in \mathbb{Z}^+ \mid \lambda_i = j$ and $Z = (Z_j)_{j=1}^\infty$. Then Z is partition of $\mathbb{Z}^+$. Note that $\underline{\overline{t}}$ and $\underline{\overline{s}}$ $\underline{\overline{s}}$ are this is the case if and only if there exists $\pi = \pi(\underline{\overline{r}}, \underline{\overline{s}}) \in \operatorname{Sym}(\mathbb{Z}^+)$ with $\Delta_{\pi i}(t) = \Delta_i(s)$. Then $\lambda_{\pi t} = |\Delta_{\pi t}| = |\Delta_i(s)| = \lambda_i$ and so $\pi Z = Z$. Conversely if $\pi \in \operatorname{Sym}(Z) := C_{\operatorname{Sym}(\mathbb{Z}^+)}(Z) = \textcircled{T}_{j \in \mathbb{Z}^+} \operatorname{Sym}(Z_j)$, then there exists a unique tabloid $\underline{\overline{s}}$ with $\Delta_i(s) = \Delta_{\pi i}(t)$ and $\underline{\overline{s}}$ is equivalent to $\underline{\overline{s}}$.

Hence

1° **[1]** *Each equivalence class contains $|Sym(Z) = z! := \prod_{j=1}^\infty z_j!$ tabloids.*

For a tabloid $\underline{\overline{r}}$ and a tableau t let $\epsilon_t(\underline{\overline{r}})$ be the coefficient of $\underline{\overline{r}}$ in e_t. So $e_t = \sum \epsilon_t(\underline{\overline{r}})\underline{\overline{r}}$.

2° **[2]** *Let $\underline{\overline{r}}$ and $\underline{\overline{s}}$ are equivalent λ-tableaux. Then there exists $\epsilon = \epsilon(\underline{\overline{r}}, \underline{\overline{s}}) \in \{\pm 1\}$ such that for any λ-tableaux t, $\epsilon_t(\underline{\overline{s}}) = \epsilon \cdot \epsilon_t(\underline{\overline{r}})$.*

Let $\pi = \pi(\underline{\overline{r}}, \underline{\overline{s}})$. Let π_j be the restriction of π to Z_j and define $\epsilon = \prod_j \operatorname{sgn}\pi^j$. We may assume that $\underline{\overline{r}}$ is involved in e_t and so $\underline{\overline{r}} = \underline{\overline{\rho t}}$ for some $\rho \in C_t$. Without loss $r = \rho t$. Define $\pi^* \in \operatorname{Sym}(n$ by $\pi^*(r(i,j) = r(\pi(i), j)$. Then $\pi^* \in C_t$, $\operatorname{sgn}\pi^* = \epsilon$ and $\underline{\overline{\pi^* r}} = \underline{\overline{s}}$. Thus $\underline{\overline{s}} = \underline{\overline{\pi^* \rho}}$, the coefficent of $\underline{\overline{r}}$ in e_t is $\operatorname{sgn}\rho$ and the coefficent of $\underline{\overline{s}}$ is $\operatorname{sgn}(\pi * \operatorname{sgn}\rho) = \epsilon \operatorname{sgn}\rho$.

3° **[3]** *$z!$ divides g^λ.*

Let t, u be λ tableaux. Let A be an equivalence class of tabloids and $\overline{\underline{r}} \in A$. Let $\overline{\underline{s}} \in A$ and choose ϵ as in (2°). Then

$$\epsilon_t(\overline{\underline{s}})\epsilon_u(\overline{\underline{s}}) = \epsilon \cdot \epsilon_t(\overline{\underline{s}}) \cdot \epsilon \cdot \epsilon_s(\overline{\underline{r}}) = \epsilon_t(\overline{\underline{r}})\epsilon_t(\overline{\underline{s}})$$

Thus $\sum_{s\in\mathcal{A}} \epsilon_t(\overline{\underline{s}})\epsilon_u(\overline{\underline{s}}) = |A|\epsilon_t(\overline{\underline{r}})\epsilon_u(\overline{\underline{r}})$

By (1°), $|A| = z!$. Summing over all the A's we conclude that $z!$ divides $(e_t \mid e_s)$. Thus (3°) holds.

Let t be λ-tableau. Define $\sigma \in \mathrm{Sym}(n)$ by $\sigma(t(i,j)) = t(i, \lambda_i + 1 - j)$ and put $\tilde{t} = \sigma t$. So $\tilde{t}$ is the tableaux obtained by reversing the rows of t. We will show that $(e_t \mid () \mid e_{\tilde{t}}) = \prod_{i=1}^{\infty}(z_i!)^j$.

Put $U_i := U_i(t) := \bigcup_{k\in Z_i} \Delta_k(t)$, the union of the rows of t of size i. Note that $U_i = U_i(\tilde{t})$ and $U = (U_i)$ is partion of I_n. Also put $U_i^j := U_i^j(t) = U_i \cap \Delta'_j$, the part of column j of t lying in U_i. Then $U_i^j(\tilde{t}) = U_i^{i+1-j} = \sigma(U_i^j)$. Let $P = (U_i^j) \mid i, j \in \mathbb{Z})$. Then P is a partition of I_n refining both U and column partition. $\Delta'(t)$. Hence $\mathrm{Sym}(U) \leq C_t$. Also σ permutes the U_{ij} and so σ normalizes $\mathrm{Sym}(U)$ and so $\mathrm{Sym}(U) \leq \sigma C_t \sigma^{-1} = C_{\tilde{t}}$. Observe $|U_i^j(t)| = z_j$ if $j \leq i$ and $U_i^j(t) = \emptyset$ otherwise. Thus

4° [**4**] $|\mathrm{Sym}(U)| = \prod_{i,j} |U_i^j(t)|! = \prod_{i=1}^{\infty}(z_i!)^i$.

We show next

5° [**5**] *Let $\pi \in \mathrm{Sym}(U)$. Then $\epsilon_t(\overline{\underline{\pi t}}) = \epsilon_{\tilde{t}}(\overline{\underline{\pi t}}) = \mathrm{sgn}\pi$.*

Since $\pi \in C_t$ we have $\epsilon_t(\overline{\underline{\pi t}}) = \mathrm{sgn}\pi$.
Since $\pi \in C_{\tilde{t}}$ we have $\epsilon_t(\overline{\underline{\pi \tilde{t}}}) = \mathrm{sgn}\pi$.
Since σ fixes the rows of t, $\pi\sigma\pi^{-1}$ fixes the rows of πt. Thus

$$\overline{\underline{\pi t}} = \overline{\underline{\pi\sigma\pi^{-}1\pi t}} = \overline{\underline{\pi\sigma t}} = \overline{\underline{\pi\tilde{t}}}$$

and so (5°) holds.

6° [**6**] *Let $\pi \in C_t$ such that $\overline{\underline{\pi t}}$ is involved in $e_{\tilde{t}}$. Then $\pi \in \mathrm{Sym}(U)$.*

Since $\overline{\underline{\pi t}}$ is involved in $e_{\tilde{t}}$ there exists $\tilde{\pi} \in C_{\tilde{t}}$ with $\overline{\underline{\pi t}} = \overline{\underline{\tilde{\pi}\tilde{t}}}$. Hence for all $k \in I_n$, $r_{\pi t)}(k) = r_{\tilde{\pi}\tilde{t}}(k)$ and so $r_t(\pi^{-1}k) = r_{\tilde{t}}(\tilde{\pi}{-}1k)$. Put $\alpha = \pi^{-1}$ and $\tilde{\alpha} = \pi^{*-1}$. Then for all $k \in I$.

$$(*) \qquad \alpha \in C_t, \quad \tilde{\alpha} \in C_{\tilde{t}} \quad \text{and} \quad r_t(\alpha(k)) = r_{\tilde{t}}(\tilde{\alpha}(k))$$

We need to show that $\alpha(U_i^j) = U_i^j = \tilde{\alpha}(U_i^j)$ for all i, j. The proof uses double induction. First on j and then downwards on i.

For $I, J \subset \mathbb{Z}^+$ let $U_I^J = \bigcup\{U_i^j \mid i \in I, j \in J\}$. If $I = \mathbb{Z}^+$ or $J = \mathbb{Z}^+$ we drop the subscript I, respectively superscript. For example $U^{\leq j} = \bigcup U_i^k \mid i, k \in \mathbb{Z}^+ \mid k \leq j\}$ consists ofthe first j columns of t.

Suppose that $\alpha(U_k^l) = U_k^l = \tilde{\alpha}(U_k^l)$ whenever $l < j$ or $l = j$ and $k > i$. Then $\alpha(U_{>i}^j) = \alpha(U_{>i}^j)$ and $\alpha(U^j) = U^j$ implies $\alpha(U_i^j) \subseteq U_{\leq i}^j$. Hence by (*) also

$$(**) \qquad \tilde{a}lpha(U_i^j) \subseteq U_{\leq i}$$

Let $c = i + 1 - j$. Then $U_i^j = \tilde{U}_i^c$ and

$$\tilde{U}_{<i}^c = \bigcup_{k<i} U_k^{c+1-k}$$

and so by induction $\tilde{\alpha}\tilde{U}_{<i}^c = U_{<i}^c$. Hence $\tilde{\alpha}(U_i^j) \subseteq \tilde{\alpha}(\tilde{U}_{\geq i}^c) = \tilde{U}_{\geq i}^c \subseteq \tilde{U}_{\geq i} = U_{\geq i}$. So by (**) $\tilde{\alpha}(U_i^j) \subseteq U_i \cap \tilde{U}^c = \tilde{U}_i^c = U_i^j$ and $\tilde{a}(U_i^j) = U_{i^j}$. Hence by (*) also $\alpha(U_i^J \leq U_i \cap U^j = U_i^j$ and $\alpha(U_i^j) = U_i^j$.

So (6°) is proved.

From (5°) and (6°) we conclude that $(e_t \mid e_{\tilde{t}}) = |\mathrm{Sym}(U)| = \prod_{i=1}^{\infty}(z_i!)^i$. Since g^λ divides $(e_t \mid e_{\tilde{t}})$ the lemma is proved. □

Proposition 5.6.6 [**dlambda not zero**] *Suppose F is an integral domain and λ is a partition of n. Let $p = \mathrm{char}\, F$. Then $D^\lambda \neq 0$ iff λ is p-regular.*

Proof: Since F is an integral domain, $p = 0$ or p is a prime. Let $\lambda = (i_i^z)_{i=1}$. Then $p \mid \prod_i z_i!$ iff $p \leq z_i$ for some i, iff $p \mid \prod_i (z_i!)^i$ and iff λ is p-singular.

So 5.6.5 implies that $p \mid g_\lambda$ iff λ is p-singular. And so by 5.6.4, $D_\lambda = 0$ iff λ is p-singular. □

Theorem 5.6.7 [**all simple sym(n)-modules**] *Let F be a field, n a postive integer and $p = \mathrm{char}\, F$.*

(a) [**a**] *Let λ be a p-regular partition of n. Then D_λ is an absolutely simple, selfdual $F\mathrm{Sym}(n)$-module.*

(b) [**b**] *Let I be a simple $F\mathrm{Sym}(n)$-module. Then there exists a unique p-regular partition λ of n with $I \cong D^\lambda$.*

Proof: (a) By 5.6.6 $D^\lambda \neq 0$. By 4.1.5, s induces a non-degenerate G-invariant form on D^λ and so by 4.1.6(c), D^λ is isomorphic to its dual. By 5.3.12, D^λ is absolutely simple.

(b) If λ and μ are distinct p-regular partition then by 5.3.10 and (a), D^λ and D^μ are non-isomorphic simple $F\mathrm{Sym}(n)$-modules. The number of simple $F\mathrm{Sym}(n)$-modules is less or equal to the number simple $Sym(n)$-modules over the algebraic closure of $\mathbb{F}$. The latter number is by 5.5.8 equal to to the number of p'-conjuagacy classes and so by 5.6.2 equal to the number of p-regular partitions of n. So (b) holds. □

5.7 Series of R-modules

Definition 5.7.1 [**def:series**] *Let R be a ring and M and R-module. Let $\mathcal{S}$ be a set of R-submodules of M. Then $\mathcal{S}$ is called an* R-series *on M provided that:*

(a) [**a**] $0 \in \mathcal{S}$ *and* $M \in \mathcal{S}$.

(b) [**b**] $\mathcal{S}$ *is totally ordered with respect to inclusion.*

(c) [**c**] *For all* $\emptyset \neq T \subset \mathcal{S}$, $\bigcap \mathcal{T} \in \mathcal{S}$ *and* $\bigcup \mathcal{T} \in \mathcal{S}$.

For example $\mathbb{Z} > 2\mathbb{Z} > 6\mathbb{Z} > 30\mathbb{Z} > 210\mathbb{Z} > \ldots > 0$ is an $\mathbb{Z}$-series on $\mathbb{Z}$.

Definition 5.7.2 [**def:jumps**] *Let R be a ring, M an R-module and $\mathcal{S}$ an R-series on M. For $0 \neq A \in \mathcal{S}$ put $A^- = \bigcup\{B \in \mathcal{S} \mid B \subset A\}$. If $A \neq A^-$ then (A^-, A) is called a* jump *of $\mathcal{S}$ and A/A^- a* factor *of $\mathcal{S}$. $\mathcal{S}$ is called a composition series for R on $\mathcal{S}$ provided that all its factors are simple R-modules.*

The above example is composition series and its sets of factors is isomorphic to $\mathbb{Z}/p\mathbb{Z}$, p a prime.

Lemma 5.7.3 [**basic series**] *Let R be a ring, M an R-module, $\mathcal{S}$ an R-series on M.*

(a) [**a**] *Let $A, B \in \mathcal{S}$ with $B \subset A$. Then (B, A) is a jump iff $A = C$ or $B = C$ for all $C \in \mathcal{S}$ with $B \subseteq C \subseteq A$.*

(b) [**b**] *Let $U \subset M$. Then there exists a unique $A \in \mathcal{U}$ minimal with $U \subseteq A$. If U is finite and contains a non-zero element then $A^- \neq A$ and $A \cup U \nsubseteq A^-$.*

(c) [**c**] *Let $0 \neq m \in M$. Then there exists a unique jump (B, A) if $\mathcal{S}$ with $v \in A$ and $v \notin B$.*

Proof: (a) Suppose first that (B, A) is a jump. Then $B = A^-$. Let $C \in \mathcal{S}$ with $B \subseteq C \subseteq A$ Suppose $C \subset A$. Then $C \subseteq A^- = B$ and $C = B$.

Suppose next that $A = C$ or $B = C$ for all $C \in \mathcal{S}$ with $B \subseteq C \subseteq A$. Since $B \subseteq A$, $B \subseteq A^-$. Let $C \in \mathcal{S}$ with $C \subset A$. Since $\mathcal{S}$ is totally ordered, $C \subseteq B$ or $B \subseteq C$. In the latter case, $B \subseteq C \subset A$ and so by assumption $B = C$. So in any case $C \subseteq B$ and thus $A^- \subseteq B$. We conclude that $B = A^-$ and so (B, A) is a jump.

(b) Put $A = \bigcup\{S \in \mathcal{S} \mid U \subseteq S\}$. By $A \in \mathcal{S}$ and so clearly is minimal with respect to $U \subseteq A$ and is unique with respect to this property. Suppose now that U is finite and contains a non-zero element. Then $A \neq 0$. Suppose that $A = A^-$. Then for each $u \in U$ we can choose $B_u \in \mathcal{S}$ with $u \in B_u$ and $B_u \subset A$. Since U is finite $\{B_u, u \in U\}$ has a maximal elemeent B. Then $U \subseteq B \subset A$, contradicting the minimality of A

Thus $A \neq A^-$ and by minimality of A, $U \nsubseteq A$.

(c) Follows from (b) applied to $U = \{m\}$. □

Lemma 5.7.4 [**series and basis**] *Let R be a ring, M a free R-module with basis $\mathcal{B}$ and $\mathcal{S}$ be an R-series on M. Then the following four statements are equivalent. one of the follwing holds:*

(a) [**a**] *For each $A \in \mathcal{S}$, $A \cap \mathcal{B}$ spans A over R.*

(b) [**b**] *For each $B \in \mathcal{S}$, $(a + B \mid a \in \mathcal{B} \setminus B\}$ is R-linear independent in V/B. Then*

(c) [**c**] *For each jump (B, A) of $\mathcal{S}$, $(a+B \mid a \in \mathcal{B} \cap A \setminus B\}$ is R-linear independent in A/B.*

(d) [**d**] *For all $A, B \in \mathcal{S}$ with $B \subseteq A$, $(a + B \mid a \in \mathcal{B} \cap A \setminus B\}$ is an basis R-basis for A/B.*

Proof: (a)$\Longrightarrow$ (b): $(r_a) \in \bigoplus_{a \in \mathcal{B} \setminus A} R$ with $\sum_{a \in \mathcal{B} \setminus A} r_a a \in B$. Then by (a) applied to B there exists $(r_a) \in \bigoplus_{a \in \mathcal{B} \cap A}$ with

$$\sum_{a \in \mathcal{B} \setminus A} r_a a = \sum_{a \in \mathcal{B} \cap A} r_a a$$

Since $\mathcal{B}$ is linearly independent over R this implies $r_a = 0$ for all $a \in \mathcal{B}$ and so (b) holds.
(b)$\Longrightarrow$ (c): Obvious.

(c)$\Longrightarrow$ (a): Let $a \in A$. Since $\mathcal{B}$ spans M over R there exists afinite subset $\mathcal{C}$ of $\mathcal{B}$ and $(r_c) \in \bigoplus_{\mathcal{C}} R^\sharp$ with $a = \sum_{c \in \mathcal{C}} r_c c$. Let $D \in \mathcal{S}$ by minimal with $\mathcal{C} \subseteq D$. Then (D^-, D) is a jump and $\mathcal{C} \setminus D^- \neq \emptyset$. Suppose that $D \not\subseteq A$. Since $\mathcal{S}$ is totally ordered, $A \subseteq D^-$. Thus

$$0_{D/D^-} = a + D^- = \sum_{c \in \mathcal{C}} r_c c + D^- = \sum_{c \in \mathcal{C} \setminus D^-} r_c c + D^-$$

a contradiction to (c).
(a)$\Longrightarrow$ (d): (a) implies that $(a + B \mid a \in \mathcal{A}\}$ and so also $(a + B \mid a \in \mathcal{A}\}$ spans A/B. Since (a) implies (b), $(a + B \mid a \in \mathcal{B} \setminus B\}$ and so also $(a + B \mid a \in \mathcal{B} \cap A \setminus B\}$ is R-linear independent. So (d) holds.
(d)$\Longrightarrow$ (a): Just apply (d) with $B = 0$. □

5.8 The Branching Theorem

Definition 5.8.1 [**def:removable node**] *Let λ be partion of n*

(a) [**a**] *A node $d \in [\lambda]$ is called* removable *if $[\lambda] \setminus \{d\}$ is a Ferrers diagram.*

(b) [**b**] *$d_i = (r_i, c_i), 1 \leq i \leq k$ are the the removable nodes of $[\lambda]$ ordered such that $r_1 < r_2 < \ldots < r_k$. $\lambda^{(i)} = \lambda([\lambda] \setminus \{d_i\}$ and $\lambda \downarrow = \{\lambda^{(i)} \mid 1 \leq i \leq k\}$*

(c) [**c**] *$e \in \mathbb{Z}^+ \to \mathbb{Z}^+$ is called an* exterior node *of $[\lambda$ if $D \cup \{e\}$ is a Ferrers diagram . $\lambda \uparrow$ is the set of partions of n obtained by extending $[\lambda]$ by an exterior node.*

Lemma 5.8.2 [**basic removable**] *Let λ be a partition of n and $(i,j) \in D$. Then the following are equivalent*

(a) [**a**] *(i,j) is a removable node of $[\lambda]$.*

(b) [**b**] *$j = \lambda_i$ and $\lambda_i > \lambda_{i+1}$.*

(c) [**c**] *$i = \lambda'_j$ and $\lambda'_j > \lambda'_{j+1}$.*

(d) [**d**] *$j = \lambda_i$ and $i = \lambda'_j$.*

Proof: Obvious. $\square$

Definition 5.8.3 [**def:restrictable**] *Let λ be partition of n and t be a λ-tableau. We say that t is restrictable if $t^{-1}(n)$ is a removable node of $[\lambda]$. In this case $t \mid_{t^{-1}(I_{n-1})}$ is denoted by $t\downarrow$. $\overline{\underline{t}}$ is called restrictable if $\overline{\underline{t}}$ contains a restrictable tableau s. In this case we define $\overline{\underline{t}}\downarrow = \overline{\underline{s\downarrow}}$*

Lemma 5.8.4 [**basic restrictable**] *Let λ be a partion of t. If t is restricable then $t\downarrow$ is a tableau. If t is standard then t is restrictable and $t\downarrow$ is standard. Let $\pi \in \mathrm{Sym}(n-1)$. Then t is restrictable iff πt is restrictible. In this case $(\pi t)\downarrow = \pi(t\downarrow)$. $\overline{\underline{t}}$ is restrictable iff $\pi\overline{\underline{t}}$ is restrictable In this case $(\pi\overline{\underline{t}})\downarrow = \pi(\overline{\underline{t}}t\downarrow)$.*

Proof: Obvious.

Theorem 5.8.5 [**restricting specht**] *Let λ be a partition of n. For $0 \leq i \leq k$ let V_i be the F-submodule of S^λ spanned by all e_t where t is a restrictable λ-tableau with n in one of the rows $r_1, r_2, \dots r_i$. Then*

$$0 = V_0 < V_1 \ldots < V_{k-1} < V_k = S^\lambda$$

as a series of $F\mathrm{Sym}(n-1)$-submodules with factors $V_i/V_{i-1} \cong S^{\lambda^{(i)}}$.

Proof: Clearly the the set of restrictable λ tableaux with n in row r_i is invariant under the action of $\mathrm{Sym}(n-1)$. Thus each V_i is an $FSym(n-1)$ submodule of S^λ. Also clearly $V_{i-1} \leq V_i$ and it remains to show that $V_i/V_{i-1} \cong S^{\lambda^{(i)}}$. For this define and F-linear map

$$\theta_i : M^\lambda \to M^{\lambda^{(i)}}, \quad \overline{\underline{t}} \to \begin{cases} \overline{\underline{t}}\downarrow & \text{if } n \text{ is in row } r_i \text{ of } t \\ 0 & \text{otherwise} \end{cases} \tag{1}$$

Clearly θ_i commutes with the action of $\mathrm{Sym}(n-1)$ and so θ_i is $F\mathrm{Sym}(n-1)$ linear. Let n be a restrictable tableau with n in row r_j. Then for all $\pi \in C_t$ n is in a row less or equal to r_i, with equality iff π fixes n, that is if $\pi \in C_{t\downarrow}$. Thus

$$\theta_i(e_t) = \begin{cases} e_{t\downarrow} & \text{if } j = i \\ 0 & \text{if } j < i \end{cases} \tag{2}$$

If s is a $\lambda^{(i)}$-tableau, then $s = t\downarrow$ for a (unique) restrictable λ tableau t with n in row r_i. Hence

$$V_{i-1} \leq V_i \cap \ker\theta_i \quad \text{and} \quad V_i/V_i \cap \ker\theta_i \cong \operatorname{Im}\theta_i = S^{\lambda^{(i)}} \tag{3}$$

Let $\mathcal{B}$ be the set of standard λ-polytabloids and $\mathcal{B}_i$ the e_t with t standard and n in row r_i. Then by (1) $\theta_i(\mathcal{B}_i)$ is the standard basis for $S^{\lambda^(i)}$ and so is linear independently. Thus also the image of $\mathcal{B}_i$ in $V_i/V_i\ker\theta_i$ is linearly independent. Consider the series of F-modules

$$0 = V_0 \leq V_1 \cap \ker\theta_1 \leq V_1 \leq V_2 \cap \ker\theta_2 < V_2 < \ldots < V_{k-1} \leq V_k \cap \ker\theta_k < V_k < S^\lambda$$

Each $e_t \in \mathcal{B}$ lies in a unique $\mathcal{B}_i$ and so in $V_i \setminus (V_i \cap \ker\pi_i)$. Thus $\mathcal{B} \cap V_i \cap \ker\theta_i \subseteq V_{i-1}$. So we can apply 5.7.4 to the series of F-modules and conlcude that $V_i \cap \ker\theta_i/V_{i-1}$ is as the emptyset as an R-basis. Hence $V_{i-1} = V_i \cap \ker\theta_i$. For the same reason $V_k = S^\lambda$ and theorem now follows from (3). □

Theorem 5.8.6 (Branching Theorem) [**branching theorem**] *Let F be a field with* $\operatorname{char} F = 0$ *and λ a partition of n.*

(a) [**a**]

$$S^\lambda\downarrow_{\mathrm{Sym}(n-1)} = \bigoplus_{\mu\in\lambda\downarrow} S^\mu$$

(b) [**b**]

$$S^\lambda\uparrow^{\mathrm{Sym}(n-1)} = \bigoplus_{\mu\in\lambda\uparrow} S^\mu$$

Proof: (a) Follows from 5.8.5 and Maschke's Theorem 2.3.2

(b) Follows from (a) and Frobenius Reprocity 2.7.4.

5.9 $S^{(n-2,2)}$

In this section we investigate the Specht modules $S^{(n)}$, $S^{(n-1,1)}$ and $S^{n-2,2}$.

Lemma 5.9.1 [**s(n)**] *$M^{(n)} = S^{(n)} \cong D^{(n)} \cong F$.*

Proof: There there a unique (n)-tabloid $\underline{t}$ and $\pi\underline{t} = \underline{t}$ for all $\pi \in Sym(n)$. Moreover $e_t = \underline{t}$ and so $S^{(n)} = M^{(n)}$. Also $S^{(n)\perp} = 0$ and the lemma is proved. □

Lemma 5.9.2 [**s(n-1)**] *Let x_i the unique $(n-1,1)$-tabloid with i in row 2. Let $z = \sum_{i=1}^n x_i$ be the sum of all λ-tabloids. Then*

(a) [**a**] $S^{(n-1,1)} = \{\sum_{i=1}^n f_i x_i \mid f_i \in F, \sum_{i=1}^n f_i = 0.$

(b) [**b**] $S^{(n-1,1)\perp} = Fz.$

(c) [**c**] $S^{(n-1,1)\perp} \cap S^{(n-1,1)} = \{fx \mid f \in F, nf = 0\}.$

Proof: (a) If t is tableau with $t(1,1) = i$ and $t(2,1) = j$, then $e_t = x_i - x_j$. This easily implies (a).

(b) $\sum_{f_i z_i} \perp x_i - x_j$ iff $f_i = f_j$.

(c) Follows from (a) and (b). □

Corollary 5.9.3 [**dim d(n-1)**] *Let F be a field and $p = \mathrm{char}\,\mathbb{F}$.*

(a) [**a**] *If $p \nmid n$, then $S^{(n-1,1)} \cong D^{(n-1,1)}$ has dimension $n-1$ over D.*

(b) [**b**] *If $p \mid n$, then $D^{(n-1,1)}$ has dimension $n-2$ over F.*

Proof: Follows immediately from 5.9.2. □

To analyze $S^(n-2,2)$ we introduce the follwing notation: Let $n \in \mathbb{N}$ with $n \geq 4$ and $\lambda = (n-2,2)$. Let $\mathcal{P}$ be the set for subsets of size two in I_n. For $P \in P_n$ let x_P be the λ-partition $(P, I_n \setminus P)$. Then $(x_P \mid P \in \mathcal{P})$ is an F-basis for M^λ. For a, b, c, d pairwise distinct elements in I_n put $e_{ab|cd} = x_{ac} + x_{bd} - x_{ad} - x_{bc}$. So $e_{ab|cd} = e_t$ for any λ tableau of the form $\frac{\overline{a\,c\ldots}}{\underline{b\,d}}$.

For $i \in I_n$ define $x_i := \sum_{i \in P \in \mathcal{P}} x_P$ and $y_i = \sum_{i \notin P \in \mathcal{P}} x_P$. Also let $z = \sum_{P \in \mathcal{P}} x_P$ and observe that $x_i + y_i = z$ for all $i \in I$.

Lemma 5.9.4 [**basis for s(n-2,2)perp**]

(a) [**a**] $x_1, x_2, \ldots x_{n-1}, y_n$ *is an F-basis for $S^{\lambda\perp}$.*

(b) [**b**] $x_1, x_2, \ldots x_{n-1}, z$ *is an F-basis for $S^{\lambda\perp}$.*

(c) [**c**] $y_1, y_2, \ldots y_{n-1}, z$ *is an F-basis for $S^{\lambda\perp}$.*

(d) [**d**] *If 2 is invertible in F then $x_1, x_2, \ldots x_n$ is an F-basis for $S^{\lambda\perp}$.*

(e) [**e**] *If $n-2$ is invertible in F, then $y_1, y_2, \ldots y_n$ is an F-basis for $S^{\lambda\perp}$.*

Proof: (a) We will first show that $x_i \perp e_{ab|cd}$ for all appropriate i, a, b, c, d. If $i \notin \{a, b, c, d\}$, x_i and $e_{ab|cd}$ have do not share a tabloid and so $(x_i \mid e_{ab|cd}) = 0$. So suppose $i = a$, then x_i and $e_{ab|cd}$ share x_{ac} and x_{ad} with opposite signs and so again $x_i \perp e_{ab|cd}$. Clearly $z \perp e_{ab|cd}$ and so also $y_i \perp e_{ab|cd}$. Thus x_i, y_i and z are all contained in $S^{\lambda\perp}$.

Now let $a = \sum_{P\in\mathcal{P}} r_P x_P \in S^{\lambda\perp}$. We need to show that a is a unique F-linear combination of $x_1, x_2, \dots x_{n-1}, y_n$. For $n \neq i \in I_n$, x_i is the only one involving x_{in}. So replacing a by $a - \sum_{i=1}^{n-1} r_{in} x_i$ we assume that $r_{in} = 0$ for all $i \neq n$. And we need to show that a is scalar multiple of y_n. That is we need to show that $r_{ij} = r_{kl}$ whenever $\{i, j\}, \{k, l\} \in \mathcal{P}$ with $n \notin \{i, j, k, l\}$. Suppose first that $P \cap Q \neq \emptyset$ and say $i = k$ and withoutloss $j \neq l$. Since $a \in S^{\lambda\perp}$, $a \perp e_{in|jl}$. Thus $r_{ij} + r_{nl} - r_{il} - r_{nj} = 0$. By assumption $r_{nl} = r_{nj} = 0$ and so $r_{ij} = r_{il} = r_{kl}$. In the geneal case we conclude $r_{ij} = r_{ik} = r_{kl}$ and (a) is proved.

(b) Observe that $z = \sum_{i=1}^{n-1} x_i - y_n$. Thus (b) follows from (a).

(c) Since $y_i = z - x_i$ this follows from (b).

(d) Observe that $\sum_{i=1}^{n} x_i = 2z$ and so $x_n = -\sum_{i=1}^{n-1} x_i + 2z$. So (d) follows from (b).

(e) We have $\sum_{i=1}^{n} y_i = \sum_{i=1}^{n}(z - x_i) = nz - \sum_{i=1}^{n} x_i = (n-2)z$. So $y_n = -\sum_{i=1}^{n-1} y_i + (n-2)z$ and (e) follows from (c). □

It might be interesting to observe that $y_1, \dots, y_{n-1}, x_n$ is only a basis if $n-2$ is invertible. Indeed $x_n = -\sum_{i=1}^{n-1} x_i + 2z = \sum_{i=1}^{n-1}(y_i - z) + 2z = \sum_{i=1} y_i + (n-2)z$.

We know proceed to compute $S^\lambda \cap S^{\lambda\perp}$ if F is a field.

Lemma 5.9.5 [**s(n-2) cap s(n-2)perp**] *Suppose F is field and put $p = \operatorname{char} F$.*

(a) [**a**] *Suppose $p = 0$ or p is odd and $n \not\equiv 1, 2 \mod p$ or $p = 2$ and $n \equiv 3 \mod 4$. Then n $S^\lambda \cap S^{\lambda\perp} = 0$.*

(b) [**b**] *Suppose p is odd and $n \equiv 1 \mod p$ or $p = 2$, $n \equiv 1 \mod 4$. Then $S^\lambda \cap S^{\lambda\perp} = Fz$.*

(c) [**c**] *Suppose p is odd and $n \equiv 2 \mod p$ or $p = 2$ and $n \equiv 2 \mod 4$, then $S^\lambda \cap S^{\lambda\perp} = \langle Fy_i \mid 1 \leq i \leq n\rangle$ and $\sum_{i=1}^{n} y_i = 0$.*

(d) [**d**] *Suppose $p = 2$ and $n \equiv 0 \mod 4$. Then $S^\lambda \cap S^{\lambda\perp} = \langle Fy_i y_j \mid 1 \leq i < j \leq n\rangle$ and $\sum_{i=1}^{n} y_n = 0$.*

Proof: Since F is a field and $(\cdot \mid \cdot)$ is non-degenerate, $S^{\lambda\perp\perp} = S^\lambda$ and so $S^\lambda \cap S^{\lambda\perp} = S^{\lambda\perp\perp} \cap S^{\lambda\perp}$ is the radical of the restriction of $(\cdot \mid \cdot)$ to S^λ.

By 5.9.4 $y_1, y_2 \dots y_{n-1} z$ is basis for $S^{\lambda\perp}$. Let $a = r_0 z + \sum_{i=1}^{n-1} r_i y_i$. Then

Observe that

$$\begin{aligned}(y_i \mid y_i) &= \tbinom{n-1}{2}\\ (y_i \mid y_j) &= \tbinom{n-2}{2}\ i \neq j\\ (y_i \mid z) &= \tbinom{n-1}{2}\\ (z \mid z) &= \tbinom{n}{2}\end{aligned}$$

So $(a \mid y_j) = r_0\binom{n-1}{2}+r_j\binom{n-1}{2}+\sum_{i\neq j=1}^{n-1} r_i\binom{n-2}{2}$. Put $r = \sum_{i=1}^{n-1} r_i$. Since $\binom{n-1}{2}-\binom{n-2}{2} = \binom{n-2}{1} = n-1$ we conclude $a \in S^\lambda$ if and only if

$$(a \mid y_j) = \binom{n-1}{2} r_0 + (n-2)r_j + \binom{n-2}{2} r = 0 \forall 1 \leq j < n \tag{1}$$

and

$$(a \mid z) = r_0\binom{n}{2} + r\binom{n-1}{2} = 0 \tag{2}$$

.

Sustracting (1) for two diffrent values of for j gives

$$(n-2)r_j = (n-2)r_k \forall 1 \leq j < k \leq n-1 \tag{3}$$

and so

$$(n-2)r = (n-1)(n-2)r_j \tag{4}$$

Substracting (2) from (1) gives

$$(n-1)r_0 + (n-2)r_j = (n-2)r \tag{5}$$

and using (4)

$$(n-1)r_0 = (n-2)^2 r_j \tag{6}$$

Note also that (1) and (2) are equivalent to (2),(3) and (6).

Suppose first that $n-2 = 0$ in F. Then $\sum_{i=1}^n y_n = (n-2)z = 0$ and $\langle y_i \mid 1 \leq i \leq n\rangle_F = \langle y_i \mid 1 \leq i \leq n-1\rangle_F$ and

Also $n-1 \neq 0$. So (3) and (6) hold if and only if $r_0 = 0$. If $p \neq 2$ or $p = 2$ and $n \equiv 2 \mod 4$, then also $\binom{n-1}{2} = 0$ in F and so also (6) holds. Thus (c) holds in this case. If $p = 2$ and $n \equiv 0 \mod 4$, then $\binom{n-1}{2} = 1$ and so (6) holds if and only if $r = 0$. Observe also that $\sum_{i=1}^n y_i = 0$ and n even implies $\langle y_i + y_j \mid 1 \leq i < j \leq n\rangle_F = \langle y_i + y_j \mid 1 \leq i < j \leq n-1\rangle_F$ and so (d) holds.

Suppose next that $n-2 \neq 0$ in F. Then (3) just says $r_j = r_k$. Assume that $n-1 = 0$ in $\mathbb{F}$. Then (6) holds iff $r_j = 0$ for all j. Hence (2) says $r_0\binom{n}{2}r = 0$. If $p \neq 2$ or $p = 2$ and $n \equiv 1 \mod 4$, $\binom{n}{2} = 0$ and (b) holds. If $p = 2$ and $n \equiv 3 \pmod 4$, then $\binom{n}{2} = 1$. So $r_0 = 1$ and (a) holds.

Assume next that $n-1 \neq 0$ and so $p \neq 2$. Multipying (2) with $\frac{2}{n-1}$ gives $nr_0 = -(n-2)r$. Adding to (5) gives $r_0 = 0$. So also $0 = (n-2)r = (n-2)(n-1)r_j$ and $r_j = 0$. Thus (a) holds. □

Corollary 5.9.6 [**dimension of d(n-2,2)**] *Suppose F is a field, then* $\dim_F S^{(n-2,2)} = \frac{n(n-3)}{2}$ *Moreover,*

(a) [**a**] *Suppose $p = 0$ or p is odd and $n \not\equiv 1, 2 \mod p$ or $p = 2$ and $n \equiv 3 \mod 4$. Then* $\dim_F D^{(n-2,2)} = \frac{n(n-3)}{2}$.

(b) [**b**] *Suppose p is odd and $n \equiv 1 \mod p$ or $p = 2$, $n \equiv 1 \mod 4$. Then* $\dim_F D^{(n-2,2)} = \frac{n(n-3)}{2} - 1$

(c) [**c**] *Suppose p is odd and $n \equiv 2 \mod p$ or $p = 2$ and $n \equiv 2 \mod 4$. Then* $\dim_F D^{(n-2,2)} = \frac{(n-1)(n-4)}{2} - 1$.

(d) [**d**] *Suppose $p = 2$ and $n \equiv 0 \mod 4$. Then* $\dim_F D^{(n-2,2)} = \frac{(n-1)(n-4)}{2}$.

Proof: Since $\dim D^\lambda = \dim S^\lambda - \dim(S^\lambda \cap S^{\lambda\perp})$, this follows from 5.9.5 and some simple calculations. □

Definition 5.9.7 [**def:shape**] *Let M be an R-module.*

(a) [**a**] *A shape of height n of M is inductively defined as follows:*

(i) [**i**] *A shape of height 1 of M is any R-module isomorphic to M.*

(ii) [**ii**] *A shape of height h of M is one of the following.*

(a) [**1**] *A triple $(A, \oplus, B)$ such that there exists R-submodules X, Y of M with $M = X \oplus Y$ such that A is a shape of height i of X, B is a shape of height j of Y and $k = i + j$.*

(b) [**2**] *A triple $(A, |, B)$ such that there exists R-submodules X of Y such that A is shape of height i of X, B is a shape of height j of M/X and $k = i + j$.*

(b) [**b**] *If $M \sim S$ means that S is a shape of M. A shape $(A, \oplus, B)$ as in (a:ii:a) is denoted by $A \oplus B$. A shape $(A, |, B)$ as in (a:ii:a) is denoted by $A \mid B$ or $\dfrac{A}{B}$.*

(c) [**c**] *A factor of a S shape of M is incuctively defined as follows: If S has height 1, then S itseld the only fcator of S. If $S = A \mid B$ or $S = A \oplus B$, then any factor of A or B is a factor of S.*

(d) [**d**] *A simple shape of M is a shape all of its factors are simple.*

Observe that if $M \sim A \mid (B \mid C$ then also $M \sim (A \mid B) \mid C$ and we just write $M \mid A \mid B \mid C$. Similar $M \sim (A \oplus B \oplus C)$ means $M \sim (A \oplus B) \oplus C$ and equally well $A \oplus B(\oplus C)$. We also have $M \sim A \oplus B$ iff $M \sim B \oplus A$. But $M \sim A \mid B$ does not imply $M \sim B \mid A$. We have $M \sim A \oplus (B \mid C)$ implies $M \mid (A \oplus B) \mid C$ and $M \sim B \mid (A \oplus C)$. But $M \sim (A \oplus B) \mid C$ does not imply $M \sim A \oplus (B \sim C)$.

For example if F is a field with char $F = p$ then by 5.9.2 $M^{(n-1,1)} \sim D^{(n)} \oplus D^{(n-1,1)}$ if $p \nmid n$ and $M^{(n-1,1) \sim D^{(n}} \mid D^{(n-1,1)} \mid D(n)$ if $p \mid n$.

If might also be worthwhile to define the following binary operation on classes of R-modules. If A, B are classes of R-modules, then $A \oplus B$ denotes the set of all R-modules M such that $M \cong X \oplus Y$ with $X \in A$ and $Y \in B$. $A \mid B$ is the class of all R-modules M such that M has an R-submodule X with $X \in A$ and $M/X \in B$. A shape of M then can be interpreted as a class of R-modules containing M obtained form the isomorphism classes of R modules and repeated application of the operations $\oplus$ and $|$.

To improve readabilty we write $D(a, b, c \ldots)$ for $D^{(a,b,c,\ldots)}$ in the next lemma.

Corollary 5.9.8 [**shape of m(n-2,2)**] *Suppose F is a field. Then $D^{(n-2,2)}$ has simply shapes as follows:*

(a) [**a**] *Suppose $p = 0$ or p is odd and $n \not\equiv 0, 1, 2 \mod p$ or $p = 2$ and $n \equiv 3 \mod 4$. Then*

$$M^{(n-2,2)} \sim D(n-2,2) \oplus D(n-1,1) \oplus D(n)$$

(b) [**b**] *Supose $p \neq 0, 2$ and $n \equiv 0 \mod p$. Then*

$$M^{(n-2,2)} \sim D(n-2,2) \quad \oplus \quad \begin{array}{c} D(n) \\ \hline D(n-1,1) \\ \hline D(n) \end{array}$$

(c) [**c**] *Suppose p is odd and $n \equiv 1 \mod p$ or $p = 2$, $n \equiv 1 \mod 4$. Then*

$$M^{(n-2,2)} \sim \begin{array}{c} D(n) \\ \hline D(n-2,2) \\ \hline D(n) \end{array} \quad \oplus \quad D(n-1,1)$$

(d) [**d**] *Suppose p is odd and $n \equiv 2 \mod p$. Then*

$$M^{(n-2,2)} \sim \begin{array}{c} D(n-1,1) \\ \hline D(n-2,2) \\ \hline D(n-1,1) \end{array} \quad \oplus \quad D(1)$$

(e) [**e**] *Suppose $p = 2$ and $n \equiv 2 \mod 4$. Then*

$$M^{(n-2,2)} \sim \begin{array}{c} D(n-1,1) \\ \hline D(n) \\ \hline D(n-2,2) \\ \hline D(n) \\ \hline D(n-1,1) \end{array} \quad \oplus \quad D(1)$$

(f) [**f**] *Suppose $p = 2$ and $n \equiv 0 \mod 4$. Then*

$$M^{(n-2,2)} \sim \begin{array}{c} D(n-1,1) \oplus D(n) \\ \hline D(n-2,2) \\ \hline D(n-1,1) \oplus D(n) \end{array}$$

Proof: This is straighforward from 5.9.5. As an example we consider the case $p = 2$ and $n \equiv 2 \pmod 4$. Observe that $(z \mid z) = \binom{n}{2} \neq 0$ and so $M^\lambda = \mathbb{F}z$. Thus $M^\lambda \sim D(n) \oplus z \perp$, and the restrition of $(\cdot \mid \cdot)$ to $z^\perp$ is a non-degenerate.

5.9.5 $B := S^\lambda \cap S^{\lambda\perp} = \langle y_i \mid 1 \leq 1 \leq n \rangle$. So B has the submodule, $A = \langle y_i y_j \mid 1 \leq u < j \leq n \rangle$. Since $\sum_{i=1}^n y_i = 0$, $B \cong D(n-1,1)$. Since n is even, $A/B \neq 1$ and $A/B \cong D(n)$. $S^\lambda/A = D^\lambda = D(n-2,2)$. Since $S^{\lambda\perp} = A + Fz$, $S^\lambda = z^\perp \cap A^\perp$. So $z^\perp \cap B^\perp / S^\lambda \cong (A/B)^* \cong D(n)^* \cong D(n)$. Moreover, $z^\perp / z^\perp \cap A^\perp \cong A^* \cong D(n-1,1)^* \cong D(n-1,1)$. Thus (e) holds. □

5.10 The dual of a Specht module

Definition 5.10.1 [**def:twisted module**] *Let R be a ring, G a group , M an RG-module and $\epsilon : G \to Z(R)^\sharp$ a multiplicative homomoprhism. Then M_ϵ is the RG-module which is equal to M as an R-module and $g \cdot_\epsilon m = \epsilon(g)gm$ for all $g \in G, m \in M$.*

Note that this definition is consistent with our definition of the RG-module R_ϵ.

Proposition 5.10.2 [**slambdaprime**] *Let λ be a partion of n. Then*

$$S^{\lambda *} \cong M^\lambda / S^{\lambda\perp} \cong S^{\lambda'}_{\text{sgn}}$$

as $F\mathrm{Sym}(n)$-module.

Proof: Fix a λ tableau s. Let $\pi \in R_s = C_G(\underline{\overline{s}})$. Since $R_s = C_{s'}$, 5.3.4(e) gives $\pi e_{s'} = \text{sgn}\pi e_{s'} = \pi \cdot_{\text{sgn}} e_{s'}$. Hence there exists a unique $F\mathrm{Sym}(n)$-linear homorphism

$$\alpha_s : M^\lambda \to M^{\lambda'} \text{ with } \underline{\overline{s}} \to e_{s'} \tag{1}$$

Let t be any λ-tabloids. Then the exists $\pi \in \mathrm{Sym}n$ with $\pi s = t$ (namely $\pi = ts^{-1}$) and so

$$\alpha_s(\underline{\overline{t}})\alpha_s(\underline{\overline{\pi s}}) = \pi \cdot_{\text{sgn}} e_{s'} = \text{sgn}(\pi) e_{\pi s'} = \text{sgn}(ts^{-1}) e_{t'}$$

that is

$$\alpha_s(\underline{\overline{t}}) = \text{sgn}(ts^{-1}) e_{t'} \tag{2}$$

Observe that (2) implies

$$\operatorname{Im}\alpha_s = S^{\lambda'} \tag{3}$$

Since $\lambda'' = \lambda$ we also obtain a unique $F\mathrm{Sym}(n-1)$ linear map

$$\alpha_{s'} : M^\lambda \to M^\lambda, \overline{\underline{t'}} \to \mathrm{sgn}(ts^{-1})e_t \tag{4}$$

Then

$$\operatorname{Im}\alpha_{s'} = S^{\lambda} \tag{5}$$

We claim that $\alpha_{s'}$ is the adjoint of α_s. That is

$$(\alpha_s(\overline{\underline{t}}) \mid \overline{\underline{r'}}) = (\overline{\underline{t}} \mid \alpha_{s'}(t))\overline{\underline{r}} \tag{6}$$

for all λ-tableaux t, r.

Indeed suppose that $\overline{\underline{r'}}$ is involved in involved in $\alpha_s(\overline{\underline{t}}) = \mathrm{sgn} ts^{-1}e_{t'}$. Then there exists $\beta \in C_{t'}$ with $\overline{\underline{r'}} = \overline{\underline{\beta t'}}$ and so there exists $\delta \in R_{r'}$ with $\delta r' = \beta t'$. Moreover

$$(\alpha_s(\overline{\underline{t}}) \mid \overline{\underline{r'}}) = \mathrm{sgn}(ts^{-1})\mathrm{sgn}\beta$$

Observe that $\delta \in C_r$ and $\beta \in R_t$. Thus $\overline{\underline{t}} = \overline{\underline{\beta t}} = \overline{\underline{\delta r}}$ and so $\overline{\underline{t}}$ is involved in e_r and

$$(\overline{\underline{t}} \mid \alpha_{s'}(\overline{\underline{r'}})) = \mathrm{sgn}(rs^{-1})\mathrm{sgn}\delta$$

$\delta r = \beta t$ implies $\delta rs^{-1} = \beta ts^{-1}$ and so

$$\mathrm{sgn}(rs^{-1})\mathrm{sgn}\delta = \mathrm{sgn}(ts^{-1})\mathrm{sgn}\beta$$

and so (6) holds.

Let $m \in M^\lambda$. $(\cdot \mid \cdot)$ is non-degenereate, (6) implies $\alpha_s(m) = 0$ iff $(\alpha_s(m) \mid m') = 0$ for all $m' \in M^{\lambda'}$ iff $(m \mid \alpha_{s'}(m')) = 0$ and iff $m \in (\operatorname{Im}\alpha_{s'})^\perp$. So by (5) $\ker\alpha_s = S^{\lambda\perp}$ and so

$$M^\lambda / S^{\lambda\perp} \cong M^\lambda / \ker\alpha_s \cong \operatorname{Im}\alpha_s = S^\lambda$$

□

Lemma 5.10.3 [**tensor and twist**] *Let R be a ring, G a group , M an RG-module and $\epsilon : G \to Z(R)^\sharp$ a multiplicative homomoprhism. Then*

$$M_\epsilon \cong R_\epsilon \otimes_R M$$

as an RG-module.

Proof: Observe first that there exists an R-isomorphism $\alpha : R_\epsilon \otimes_R M \to M$ with $r \otimes m \to rm$. Moreover, if $g \in G, r \in R$ and $m \in M$ then

$$\begin{array}{rcccl} \alpha(g(r \otimes m) = \alpha(g \cdot_\epsilon r \otimes gm) & = & \alpha(\epsilon(g)r) \otimes gm \\ = \ \epsilon(g)rgm = & \epsilon(g)grm \\ = \quad g \cdot_\epsilon rm & = & g \cdot_\epsilon \alpha(r \otimes m) \end{array}$$

and so α is an RG-ismomorphism. □

Corollary 5.10.4 [**slambdaprime II**]

(a) [**a**] $S^{(1^n)} \cong F_{\text{sgn}}$.

(b) [**b**] *Let λ be a partition of n. Then $S^{\lambda *} \cong S(1^n) \otimes S^{\lambda'}$*

Proof: (a) By 5.9.1 $S^{(n)} \cong F$ and so by 5.10.2 $F \cong F^* \cong S^{(n)*} \cong S_{\text{sgn}}^{(n)'} = S_{\text{sgn}}^{(1^n)}$.

(b) $S^{\lambda *} \cong S_{\text{sgn}}^{\lambda'} \cong F_\epsilon \otimes S^{\lambda'} \cong S^{(1^n)} \otimes S^{\lambda'}$. □

Chapter 6

Brauer Characters

6.1 Brauer Characters

Let p be a fixed prime. Let $\mathbb{A}$ be the ring of algebraic integers in $\mathbb{C}$. Let I be an maximal ideal in $\mathbb{A}$ containing $p\mathbb{A}$ and put $\mathbb{F} = \mathbb{A}/I$. Then $\mathbb{F}$ is a field with with $\operatorname{char} \mathbb{F} = p$.

$$^* : \mathbb{A} \to \mathbb{F}, a \to a + I$$

be the correspoding ring homorphism.

Let $\tilde{\mathbb{A}}$ be the localization of $\mathbb{A}$ with respect to the maximal ideal I, that is $\tilde{\mathbb{A}} = \{\frac{a}{b} \mid a \in \mathbb{A}, b \in \mathbb{A} \setminus I$. Observe that * extends to a homomorphism

$$^* : \tilde{\mathbb{A}} \to \mathbb{F}, \frac{a}{b} \to a^*(b^*)^{-1}$$

In particular $\tilde{I} := \ker * = \{\frac{a}{b} \mid a \in I, b \in \mathbb{A} \setminus I\}$ is an maximal ideal in $\tilde{\mathbb{A}}$, $\tilde{\mathbb{A}}/\tilde{I} \cong \mathbb{F}$ and is the kernel of the homomorphism $\tilde{I} \cap \mathbb{A} = I$. Let U be the set of elements of finite p'-order in $\mathbb{A}^\sharp$.

Lemma 6.1.1 [**f=fpbar**]

(a) [**a**] *The restriction $U \to \mathbb{F}^\sharp, u \to u^*$ is an isomorphism of multiplicative groups.*

(b) [**b**] *$\mathbb{F}$ is an algebraic closure of its prime field $\mathbb{Z}^* \cong \mathbb{F}_p$.*

Proof: Let $u \in U$ and m the multiplicative order of u. Then

$$\sum_{i=0}^{m-1} x^i = \frac{x^m - 1}{x - 1} = \prod_{i=1}^{m-1} (x - u^i)$$

Substituting 1 for x we see that $1 - u$ divided m in $\mathbb{A}$. Thus $1 - u^*$ divides m^* in $\mathbb{F}$. Since $p \nmid 0$ and $\operatorname{char} F = p$, $m^* \neq 0$ and so also $1 - u^* \neq 0$. Thus * is 1-1 on U.

If $a \in \mathbb{A}$ then $f(a) = 0$ for some monic $f \in \mathbb{Z}[x]$. Then also $f^*(a) = 0$ and $f^* \neq 0$. So a^* is algebraic over $\mathbb{Z}^*$. Let $\mathbb{K}$ be an algebraic closure of $\mathbb{F}$ and so of $\mathbb{Z}^*$. Let $0 \neq k \in \mathbb{K}$. Then $k^m = 1$ where $m = |\mathbb{Z}^*[k]| - 1$ is coprime to p. Since U^* contains all m roots of $x^m - 1$ we get $k \in U^*$. Thus $\mathbb{K}^* \subseteq U^* \subseteq \mathbb{F}^* \subseteq \mathbb{K}^*$ and the lemma is proved. □

Definition 6.1.2 [**def:brauer character**] *Let G be a finite group and M an $\mathbb{F}G$-module. $\tilde{G}$ is the set of p-regular elements in G. Let $g \in \tilde{G}$ and choose $\xi_1, \ldots \xi_n \in U$ such that $\eta_M(g) = \prod_{i=1}^n (x - \xi_i^*)$, where $\eta_M(g)$ is the characteristic polynomial of g on M. Put $\phi_M(g) = \sum_{i=1}^n \xi_i$. Then the function*

$$\phi_M : \tilde{G} \to \mathbb{A}, g \to \phi_M(g)$$

is called the Brauer character *of G with respect to M.*

Recall that if $H \subseteq G$ then we view RH as R an an R-submodule of RG. Also note that $\phi_M = \sum_{g \in \tilde{G}} \phi_M(g) g \in \mathbb{A}\tilde{G} \subseteq \mathbb{A}G$. Observe also that 1_{G° is the Brauer character of the trivial module $\mathbb{F}_G$.

Lemma 6.1.3 [**basic brauer**] *Let M be a G-module.*

(a) [**a**] *ϕ_M is a class function.*

(b) [**b**] *$\overline{\phi}_M(g) = \phi_M(g^{-1})$.*

(c) [**c**] *$\overline{\phi}_M = \phi_{M^*}$.*

(d) [**d**] *If $H \leq G$ then $\phi \mid_H = \phi_{M|_H}$.*

(e) [**e**] *$\mathcal{F}$ be the sets of factors of some $\mathbb{F}G$-series on M. Then*

$$\phi_M = \sum_{F \in \mathcal{F}} \phi_F$$

Proof: Readily verified. See 3.2.8. □

Definition 6.1.4 [**def tilde a**]

(a) [**a**] *For $g \in G$ let $g_p, g_{p'}$ be defined by $g_p, g_{p'} \in \langle g \rangle$, $g = g_p g_{p'}$, g_p is a p- and $g_{p'}$ is a p'-element.*

(b) [**b**] *For $a = \sum_{g \in G} a_g g \in \mathbb{C}G$, $\tilde{a} = a \mid_{\tilde{G}} = \sum_{g \in \tilde{G}} a_g g$.*

(c) [**c**] *For $a = \mathbb{C}\tilde{G}$ define $\check{a} \in \mathbb{C}G$ by $\check{a}(g) = a(g_{p'}$.*

Recall that $\chi_M(g) = \mathrm{tr}_M(g)$ is the trace of g on M.

Lemma 6.1.5 [**brauer and trace**] *Let M be a $\mathbb{F}G$-module. Then $(\check{\phi}_M)^* = \chi_M$.*

Proof: Let $W_i, 1 \leq i \leq n$ be the factors of an $\mathbb{F}\langle g \rangle$ composition series on M. Then since $\mathbb{F}$ is algebraically closed, W_i is 1-dimensionaly and g acts as a scalar μ_i on W_i. Since $\mathbb{F}$ contains no non-trivially p-root of unity g_p acts trivially on W_i and so also $g_{p'}$ acts as μ_i on W_i. Pick $\xi_i \in U$ with $\xi_i^* = \mu_i$. Then

$$\check{\phi}_M(g) = \phi_M(g_{p'}) = \sum_{i=1}^{n} \xi_i$$

and so

$$(\check{\phi}_M(g))^* = \sum_{i=1}^{n} \mu_i = \chi_M(g)$$

□

Let $\mathcal{S}_p$ be a set of representatives for the simple $\mathbb{F}G$-modules.

6.2 Algebraic integers

Definition 6.2.1 [**def:tracekf**] *Let $\mathbb{F} : \mathbb{K}$ be a finite separable field extension and $\mathbb{E}$ a splitting field of $\mathbb{F}$ over $\mathbb{K}$. Let Σ be set of $\mathbb{F}$-linear monomorphism from $\mathbb{F}$ to $\mathbb{K}$.*

$$\mathrm{tr} = \mathrm{tr}_{\mathbb{K}}^{\mathbb{F}} : \mathbb{F} \to \mathbb{K} \mid f \to \sum_{\sigma \in \Sigma} \sigma(f)$$

Lemma 6.2.2 [**basic tracekf**] *Let $\mathbb{F} : \mathbb{K}$ be a finite separable field extension. Then $s : \mathbb{F} \times \mathbb{F} \to \mathbb{K}, (a, b) \to \mathrm{tr}(ab)$ is a non-degenerate symmetric $\mathbb{K}$-bilinear form.*

Proof: Clearly s is$\mathbb{K}$-bilinear and symmetric. Suppose that $a \neq f \in \mathbb{F}^{\perp}$. Then $\mathrm{tr}(ab) = 0$ for all $b \in \mathbb{F}$ and since $a \neq o$, $\mathrm{tr}(f) = 0$ for all $f \in F$. Thus $\sum_{\sigma \in \Sigma} \sigma$, contradiction the linear idependence of filed monomorphism [Gr, III.2.4].

Corollary 6.2.3 [**trace dual basis**] *Let $\mathbb{F} : \mathbb{K}$ be a finite separable field extension and $\mathcal{B}$ a $\mathbb{K}$ basis for $\mathbb{F}$. Then $b \in \mathcal{B}$ there exists a unique $\tilde{b} \in \mathbb{F}$ with $\mathrm{tr}(a\tilde{b}) = \delta_{ab}$ for all $ab \in \mathbb{F}$.*

Proof: 6.2.2 and 4.1.8. □

Definition 6.2.4 [**def:integral**] *Let S be a commutative ring and R a subring.*

(a) [**a**] *$a \in R$ is called* integral *over S if there exists a monic $f \in S[x]$ with $f(a) = 0$.*

(b) [**b**] *$\overline{Int}_S(R)$ is the set of elements in S intgeral over R.*

(c) [**c**] *R is* integrally closed *in S if* $\mathrm{Int}_R(S)$.

(d) [**d**] *If Ris an integral domain, then R is called integrall closed if R is integraly closed in its field of fractions $\mathbb{F}_R$.*

Lemma 6.2.5 [**basic integral**] *Let S be a commutative ring, R a subring and $a \in S$. Then the following are equivalent:*

(a) [**a**] *a is integral over S.*

(b) [**b**] *$R[a]$ is finitely generated S-submodule of R.*

(c) [**c**] *There exists a faithful, finitely R-generated $R[a]$ module M*

Proof: (a)$\Longrightarrow$ (b): Let $f \in R[x]$ be monic with $f(a) = 0$. Then $a^n \in R\langle 1, \ldots, a^{n-1}\rangle$ and so $R[a] = R\langle 1, a, \ldots, a^{n-1}\rangle$ is finitely R-generated.

(a)$\Longrightarrow$ (b): Take $M = R[a]$.

(b)$\Longrightarrow$ (c): Let $\mathcal{B} \subseteq M$ be finite with $M = R\mathcal{B}$. Choose a matrix $D = (d_{ij}) \in \mathrm{M}_{\mathcal{B}}(R)$ with $ai = \sum_{i\in\mathcal{B}} d_{ij}j$ for all $i \in \mathcal{B}$. Let f be the characteristic polynomial of D. Then $f \in R[x]$ and f is monic. By Cayley-Hamilton [La, XV Theorem 8] $f(D) = 0$. Since $f(a)i = \sum_{j\in\mathcal{B}} f(D)_{ij}j$ for all $i \in I$ we get $f(a)M = 0$. Since $\mathrm{A}_R(M) = 0$ we have $f(a) = 0$. □

Lemma 6.2.6 [**integral closure**] *Let S be a commutative ring and R a subring of S.*

(a) [**a**] *Let $a \in S$. If a is integral over R, then also $R[a]$ is integral over R.*

(b) [**b**] *Let T be a subring of S with $R \subseteq T$. Then S is integral over R iff T is integral over R and S is integral over T.*

(c) [**c**] $\mathrm{Int}_S(R)$ *is a subring of R and* $\mathrm{Int}_R(S)$ *is integrally closed in S.*

Proof: (a) Let $b \in R[a]$. By 6.2.5(b), $R[a]$ is finitely R-generated. Since $R[a]$ is a faithful $R[b]$-module, 6.2.5(c) implies that b is integral over R.

(b) One direction is obvious. So suppose $S : T$ and $T : R$ are integral and let $a \in S$. Let $f = sum_{i=1}^n t_i x^i \in T[x]$ be monic with $f(a) = 0$. Put $R_0 = R$ and inductively $R_i = R_{i-1}[a_i]$. Then a_i is integral over R_{i-1}, R_i is finitely R_{i-1}-generated. Also $f \in R_n[x]$ and so $R_n[a]$ is finitely R_n-generated. It follows that $R_n[a]$ is finitely R-generated and so by 6.2.5(c), a is integral over R.

(c) Let $a, b \in \mathrm{Int}_S(R)$. By (a) $R[a] : R$ and $R[a, b] : R[a]$ are integral. So by (b) $R[a, b] : R$ is integral and so $R[a, b] \subseteq \mathrm{Int}_S(R)$ and $\mathrm{Int}_S(R)$ is a subring. Since both $\mathrm{Int}_S(\mathrm{Int}_S(R) : \mathrm{Int}_S(R)$ and $\mathrm{Int}_S(R)$ are integral, (b) implies that $\mathrm{Int}_S(R)$ is integrally closed in R. □

Lemma 6.2.7 [**f integral**] *Let R be a integral domain with field of fraction F and let K be a field extension of F. Let $a \in F$ be integral over R and f the minimal polynomial of a over $\mathbb{F}$.*

(a) [**a**] *All coefficents of f are integral over R.*

(b) [**b**] *If $\mathbb{K} : \mathbb{F}$ is finite seperable, then* $\mathrm{tr}(a)$ *is integral over R.*

Proof: (a) Let $\mathcal{A}$ be the set of roots of f in some splitting of f over $\mathbb{K}$. Alos let $g \in R[x]$ be monic with $f(a) = 0$. Then $f \mid g$ in $\mathbb{F}[x]$ and so $f(b) = 0$ for all $b \in \mathcal{A}$. Thus $\mathcal{A}$ is integral over R. Since $f \in R[\mathcal{A}][x]$, (a) holds.

(b) Let Σ be the set of monomorphism from $\mathbb{K}$ to the splitting field of $\mathbb{K}$ over $0\mathbb{F}$. Then each $\sigma(a), \sigma \in \Sigma$ is a root of f. Thus $\mathrm{tr} a = \prod_{\sigma \in \Sigma} \sigma(a) \in R[\mathcal{A}]$. □

Lemma 6.2.8 [**k=int/r**]*Suppose R is an integral domain with field of fraction $\mathbb{F}$. Let $\mathbb{K}$ be an algebraic field extension of $\mathbb{F}$. Then $\mathbb{K} = \{\frac{i}{r} \mid i \in \mathrm{Int}_{\mathbb{K}}(R), r \in R^\sharp\}$. In particular, $\mathbb{K}$ is the field of fraction of $\mathrm{Int}_R(S)$.*

Proof: Let $k \in \mathbb{K}$. Then ther exists a non-zero $f \in \mathbb{F}[x]$ with $f(k) = 0$. Multitiplying f with the product of the denominatos of its coeeficents we may assume that $f \in R[x]$. Let $f = \sum_{i=0}^n a_i x_i$ with $a_n \neq 0$. Put $g(x) = a_n^{n-1} f(\frac{x}{a_n}) = \sum_{i=0}^n a_i a^{n-1-i} x^i$. Then $g \in R[x]$, g is monic and $g(a_n k) = a_n^{n-1} f(k) = 0$. Thus $a_n k \in \mathrm{Int}_{\mathbb{K}}(R)$ and $k = \frac{a_n k}{k}$. □

Definition 6.2.9 [**def:lattice**] *Let R be a ring, S a subring of R, M an R-module and L an S-module of M. Then L is called a $R : S$-lattice for M provided that there exists an S-basis $\mathcal{B}$ for L such that $\mathcal{B}$ is also an R-basis for M.*

Lemma 6.2.10 [**intfr noetherian**] *Suppose R is an integral domain with field of fraction $\mathbb{F}$. Let $\mathbb{K}$ be a finite seperable extension of $\mathbb{F}$.*

(a) [**a**] *There exists an $\mathbb{F} : R$-lattice in $\mathbb{K}$ containing* $\mathrm{Int}_{\mathbb{K}}(R)$.

(b) [**b**] *If R is Noetherian, so is* $\mathrm{Int}_{\mathbb{K}}(R)$.

(c) [**c**] *If R is a PID,* $\mathrm{Int}_{\mathbb{K}}(R)$ *is an $\mathbb{F} : R$-lattice in $\mathbb{K}$.*

(a) Let $\mathcal{B}$ be a $\mathbb{F}$ basis for $\mathbb{K}$. For each $b \in \mathcal{B}$ there exisst $i_b \in \mathrm{Int}_{\mathbb{K}}(R)$ and $r_b \in R^\sharp$ with $b = \frac{i_B}{r_b}$. So replacing $\mathcal{B}$ by $b \prod_{d \in \mathcal{B}} r_b$ we may assume that $\mathcal{B} \subseteq \mathrm{Int}_{\mathbb{K}}(R)$. By 6.2.2 and 4.1.8 there exists $b^* \in\in \mathbb{K}$ with $\mathrm{tr}(b^* d) = \delta_{bd}$ for all $b, d \in \mathcal{B}$ and $(b^* \mid b \in \mathcal{B})$ is a $\mathbb{F}$-basis for $\mathbb{K}$. Thus $L = \mathrm{Int}_{\mathbb{K}}(R)\langle b^* \mid b \in \mathcal{B}\rangle$ is an $\mathrm{Int}_{\mathbb{K}}(R)$-lattice in $\mathbb{K}$. Let $i \in \mathrm{Int}_{\mathbb{K}}(R)$. Then $i = \sum_{b \in \mathcal{T}} \mathrm{tr}(bi) b^*$. Since $\mathrm{Int}_{\mathbb{K}}(R)$ is a subring $bi \in \mathrm{Int}_{\mathbb{K}}(R)$. So by 6.2.7(b) $\mathrm{tr}(bi) \in \mathrm{Int}_{\mathbb{K}}(R)$ and so $i \in L$.

(b) By (a) $\mathrm{Int}_{\mathbb{K}}(R)$ is contained in a finitely generated R-module. Since R is Noetherian we conclude that $\mathrm{Int}_{\mathbb{K}}(R)$ is a Noetherian R- and so also a Neotherian $\mathrm{Int}_{\mathbb{K}}(R)$-module.

(c) By (a) $\mathrm{Int}_{\mathbb{K}}(S)$ ia a finitely generated, torsion free R-module and so is free with R- basis say $\mathcal{D}$. It is easy to see that $\mathcal{D}$ is also linearly independent over $\mathbb{F}$. From 6.2.8, $\mathbb{K} = \mathbb{F}\mathrm{Int}_K(S)$ and so $\mathbb{F}\mathcal{D} = \mathbb{K}$ and $\mathcal{D}$ is also an $\mathbb{F}$ basis. □

Definition 6.2.11 [**def:algebraic number field**] *An* algebraic number field *is a finite field extension of* $\mathbb{Q}$.

Lemma 6.2.12 [**primes are maximal**] *Let* $\mathbb{K}$ *be an algebraic number field and* J *a non-zero prime ideal in* $R := \mathrm{Int}_{\mathbb{K}}(\mathbb{Z})$. R/J *is a finite field and in particular* J *is a maximal ideal in* R.

Proof: Let $0 \neq j \in J$ and let $f \in \mathbb{Z}[x]$ monic of minimal degree with $f(j)$. Let $f(x) = g(x)x + a$ with $a \in \mathbb{Z}$. Then $f(j) = 0$ gives $a = -g(j)j \in J$. By minimality of $\deg f$, $g(j) \neq 0$ and so also $a \neq 0$. Thus $J \cap \mathbb{Z} \neq 0$ and so $\mathbb{Z} + J/J$ is finite. By 6.2.10(a) R is a finite generate $\mathbb{Z}$-module. Thus R/J is a finitely generated $\mathbb{Z} + J/J$-module and so R/J is a finite. Since J is prime, R/J is an integral domain and so R/J is a finite field. □

Definition 6.2.13 [**def:dedekind domain**] *A* Dedekind domain *is an integrally closed Noetherian domain in which every which every non-zero prime ideal is maximal.*

Corollary 6.2.14 [**algebraic integers are dedekind**] *The set of algebriac integers in an algebraic number field form a Dedekind domain.*

Proof: Let $\mathbb{K}$ be an algebraic number field and $R := \mathrm{Int}_{\mathbb{K}}(\mathbb{Z})$. By 6.2.8 $\mathbb{K}$ is the field of fraction of R. So by 6.2.6(c) R is integrally closed. By 6.2.10 R is Noetherian and by 6.2.12 all prime ideals in R are maximal. □

Lemma 6.2.15 (Noetherian Induction) [**noetherian induction**] *R be a ring and M be an Noetherian R-module and $\mathcal{A}$ and $\mathcal{B}$ sets of R-submodules of M. Suppose that for all $A \in \mathcal{A}$ such that $D \in \mathcal{B}$ for all $A < D \in \mathcal{A}$, then $\mathcal{A} \subseteq \mathcal{B}$.*

Proof: Suppose not. Then $\mathcal{A} \setminus \mathcal{B}$ has a maximal element element A. But then $D \in \mathcal{B}$ for all $A < D \in \mathcal{A}$ and so by assumption $A \in \mathcal{B}$, a contradiction. □

Lemma 6.2.16 [**contains product of prime**] *Let R be a commutative Noetherian ring and J an ideal in R. Then there exist prime ideals $P_1, P_2 \ldots P_n \in R$ with $J \subseteq P_i$ and $\prod_{i=1}^n P_i \in J$.*

Proof: If J is is a prime ideal the lemma holds with $n = 1$ and $P_1 = J$. So suppose J is not a prime ideal. The there exists ideal $J < J_k < R$, $k = 1, 1$ with $J_1 J_2 \subseteq R$. By Notherian induction we may assume that there exists prime ideals $J_k \subseteq P_{ik}$ in R with $\prod_{i=1}^{n_k} P_{ik} \subseteq J_k$. Thus $\prod_{k=1}^2 \prod_{i=1}^{n_k} P_{ik} \leq J_1 J_2 \subseteq J$. □

Definition 6.2.17 [**def:division**] *Let M be an R module and $N \subseteq M$ and $J \subseteq R$. Then $N \div_M J =: \{m \in M \mid Jm \subseteq N\}$.*

For example $0 \div_M J = \mathrm{A}_M(J)$ and if N is an R-submodule of M, then $N \leq N \div_M J$ and $N \div_M J/N = \mathrm{A}_{M/N}(J)$. If R is an integral domain with field of fraction $\mathbb{K}$ and $a, b \in \mathbb{K}$ with $b \neq 0$, then $Ra \div_{\mathbb{K}} Rb = R\frac{a}{b}$.

Definition 6.2.18 [**def:fractional ideal**] *Let R be a integral domain with field of fraction $\mathbb{K}$. A* fractional ideal *of R is a non-zero R-submodule J of R such that $kJ \subseteq R$ for some $k \in K^\sharp$. $\mathcal{FI}(R)$ is the set of fractional ideals of R. Observe that $\mathcal{FI}(R)$ is an abelian monoid under multiplication with identity element R. A fractional ideal is called* invertible *if its invertible in the monoid $\mathcal{FI}(R)$. $\mathcal{FI}^*(R)$ is the group of invertible elements in $\mathcal{FI}(R)$.*

Lemma 6.2.19 [**basic monoid**] *Let H be a monoid.*

(a) [**a**] *Every h has at most one inverse.*

(b) [**b**] *Let $a, b \in H$. If H is abelian and ab is invertible, then a and b are invertible. invertible.*

Proof: (a) If $ah = 1$ and $hb = 1$, then $b = (ah)b = a(hb) = a$.

(b) Let h be an inverse of a. Then $1 = h(ab) = (ha)b$ and so since H is abelian, ha is an inverse of b. By symmetry hb is an inverse for a. □

Lemma 6.2.20 [**basic invertible**] *Let R be a integral domain with field of fraction $\mathbb{K}$ and let J be a fractional ideal of R.*

(a) [**a**] *If $T \neq 0$ is an R-submodule of J, then T is a fraction ideal of R and $R \div_{\mathbb{K}} J \subseteq R \div_{\mathbb{K}} T$.*

(b) [**b**] *$R \div_{\mathbb{K}} J$ is a fractional ideal of I.*

(c) [**c**] *J is invertible iff and only if $(R \div_{\mathbb{K}} J)J = R$. In this case its inverse is $(R \div_{\mathbb{K}} J)J$.*

Proof: By defintion of a fractiona ideal there exists $k \in \mathbb{K}\sharp$ with $kJ \subseteq R$.

(a) Note that $kT \subseteq R$ and so T is a fractional ideal. If $lK \subseteq R$ then also $lT \subseteq R$ and (a) is proved.

(b) Since $k \in R \div_{\mathbb{K}} J$, $R \div_{\mathbb{K}} J \neq 0$. Let $t \in J^\sharp$. Then by (a) applied to $T = Rt$,

$$R \div_{\mathbb{K}} J \subseteq R \div_{\mathbb{K}} Rrt = R\frac{1}{t}$$

and so $t(R \div_{\mathbb{K}} J) \subseteq R$ and $R \div_{\mathbb{K}} J$ is a fractional ideal.

(c) If $(R \div_{\mathbb{K}} J)J = R$, then $R \div_{\mathbb{K}} J$ is an inverse for J in $\mathcal{FI}(R)$. Suppose now that $T \in \mathcal{FI}(R)$ with $TJ = R$. Then clearly $T \subseteq R \div_{\mathbb{F}} J$. Thus

$$R = TJ \subseteq (R \div_{\mathbb{F}} J)J \subseteq R$$

Thus both T and $R \div_{\mathbb{K}} F$ are inverse of J and so $T = R \div_{\mathbb{K}} F$. □

Lemma 6.2.21 [**partial inverse**] *Let R be an Dedekind domain with field of fraction $\mathbb{K}$ and J proper ideal in R. Then $R < R \div_{\mathbb{K}} J$.*

Proof: Let P be a maximal ideal in R with $J \leq P$. Let $a \in J^\sharp$. By 6.2.16 there exists non-zero prime ideals $P_1, P_2, \ldots P_n$ with $\prod_{i=1}^n P_i \leq Ra$. We also assume that n is minimal with with property. Since $Ra \leq P$ and P is a prime ideal we must have $P_i \leq P$ for some i. By definition of a Dekind domain, P_i is a maximal ideal and so $P_i = P$. Let $Q = \prod_{i \neq j=1}^n P_j$. Then $PQ \leq Ra$ and by minimality of n, $Q \nleq Ra$. Thus $Ja^{-1}Q \leq PQa^{-1} \leq R$ and and $a^{-1}Q \nleq R$. So $a^{-1}Q \leq R \div_{\mathbb{K}} J$ and hence $R \div_{\mathbb{K}} J \nleq R$. Clearly $R \leq R \div_{\mathbb{K}} J$ and the lemma is proved.

Proposition 6.2.22 [**fi for dekind**] *et R be an Dedekind domain with field of fraction $\mathbb{K}$. Let P be a nonzero prime ideal in the Dedekind domain R and J a non-zero ideal with $J \subseteq P$. Then P invertible and $J < JP^{-1} \leq R$.*

Proof: Put $Q := R \div_{\mathbb{K}}$. Then $R \leq Q$ and $J \subseteq JQ \subseteq R$. Suppose that $J = JQ$. Since R is Noetherian, J is finitely R-generated. Since $\mathbb{K}$ is an integral domain and $J \neq 0$, J is a faithful Q-module. Thus 6.2.5(c) implies that Q is integral over R. By defintition of a Dekind domain, R is integrally closed in $\mathbb{K}$ and so $Q \leq R$. But this contradicts 6.2.21

Thus $J < JQ^{-1}$ and inparticular $P < PQ \leq R$. By definition of a Dekind Domain P is a maximal ideal in R and so $PQ = P$. Thus $Q = P^{-1}$ and the proposition is proved. □

Theorem 6.2.23 [**structure of dedekind**] *Let R be a Dedekind domain and let $\mathcal{P}$ be the set of non-zero prime ideals in R. Then the map*

$$\tau : \oplus_{\mathcal{P}} \mathbb{Z} \to \mathcal{FI}(R) \mid (z_P) \to \prod_{P \in \mathcal{P}} P^{z_P}$$

is an isomorphism of monoids. In particular, $\mathcal{FI}(R)$ is a group. Moreover $\tau(z) \leq R$ if and only if $z \in \oplus_{\mathcal{P}} \mathbb{N}$.

Proof: Clearly τ is an homomorphism. Suppose there exists $0 \neq z \in \ker \tau$. Let $X = \{P \in \mathcal{P} \mid z_P < 0$ and $Y = \{P \in \mathcal{P} \mid z_P > 00$. Then $X \cap Y = \emptyset$ and $X \cup Y \neq \emptyset$. Moreover, $\tau(z) = R$ implies

$$\prod_{P \in X} P^{-z_p} = \prod_{P \in Y} P^{z_P}$$

In particular both X and not empty. Let $Q \in X$. Then

$$\prod_{P \in Y} P^{z_P} \leq Q$$

a contrdiction since $P \nleq Q$ for all $P \in Y$ and sinceR/Q is a prime ideal.

Thus τ is $1-1$.

Next let J be a proper ideal in R and P a maximal ideal in R with $J \leq P$. By 6.2.22 $J < JP^{-1} \leq R$. By Noetherian induction $JP^{-1} = P_1 \dots P_n$ for some prime ideals $P_1, \dots P_n$ and so $J = PP_1 \dots P_n$, that is $J = \tau(z)$ for some $z \in \oplus_{\mathcal{P}}\mathbb{N}$.

Finally let J be an arbitray fraction ideal in $\mathbb{K}$. Then by definition ther exists $kJ \subseteq R$ for some $k \in \mathbb{K}^\sharp$. Then $k = \frac{r}{s}$ with $r, s \in R^\sharp$ and so $rJ = skJ \subseteq R$. Let $u, v \in \bigoplus_{\mathcal{P}} \mathbb{N}$ with $\tau(u) = Rr$ and $\tau(v) = rJ$. Then

$\tau(v - u) = (Rr)^{-1}(rJ) = Rr{-}1rJ = J$ and so τ is onto. □

The next proposition shows that Dedekind domains are not far away from being principal domains.

Proposition 6.2.24 [**nearly principal**] *Let R be a Dedekind domain.*

(a) [**a**] *Let A and B be a fractional ideals of R with $B \leq A$. Then A/B is a cyclic R-module.*

(b) [**b**] *Let A be a fractional ideal of R. Then there exists $a, b \in A$ with $A = Ra + Rb$.*

Proof: (a) Replacing A and B by kA and kB for a suitable $k \in R$ we may assume that $B \leq A \leq R$, Let $\mathcal{Q}$ be a finite set of prime ideals in R with $A = \prod_{P \in \mathcal{Q}} P^{a_P}$ and $B = \prod_{P \in \mathcal{Q}} P^{b_P}$ for some $a_p, b_P \in \mathbb{N}$. Choose $x_P \in P^{a_p} \setminus P^{a_p+1}$. Observe that $P^{a_p+1} + Q^{a_Q+1} = R$ for disctinct $P, Q \in \mathcal{Q}$. So by the Chinese Remainder Theorem 2.5.15(e) the exists $x \in R$ with $x + P^{a_p+1} = x_p + P^{a_p+1}$ for all $P \in \mathcal{Q}$. Thus $x \in \bigcap_{P \in \mathcal{Q}} P^{a_p} = A$ and $x \notin P^{a_P+1}$. Since $B \leq Rx + B$, $Rx + B = \prod_{P \in \mathcal{Q}} P^{c_P}$ for some $c_P \in \mathbb{N}$. Since $Rx + B \leq A$, $c_P \geq a_P$. Since $x \notin P^{a_P+1}$, $c_P \leq a_p$. Thus $a_P = c_P$ for all $P \in \mathcal{Q}$ and so $A = Rx + B$.

(b) Let $0 \neq b \in A$ and put $B = Ra$. By (a) $A/B = Ra + B/B$ for some $a \in A$. Thus $A = Ra + Rb$. □

6.3 The Jacobson Radical II

Lemma 6.3.1 (Nakayama) [**nakayama**] *Let R be a ring and M a non zero finitely generated R-module then* $\mathrm{J}(R)M \neq 0$.

Let $\mathcal{B} \subseteq M$ be minimal with $R\mathcal{B} = M$. Let $b \in \mathcal{B}$, then $M \neq R(\mathcal{B} \setminus \{b\}$ and repplacing M be $M/R(\mathcal{B} \setminus \{b\}$ we mau assume that $M = Rb$. Then $M \cong R/\mathrm{A}_R(b)$. Let J be maximal left ideal of R with $A_R(b) \leq J$. Then $\mathrm{J}(R) + A_R(b) \leq J < R$ and so also $\mathrm{J}(R) < M$. □

Lemma 6.3.2 [**jr and inverses**] *Let R be a ring and $x \in R$.*

(a) [**a**] *$x \in \mathrm{J}(R)$ iff $rx - 1$ has a left inverse for all $x \in R$.*

(b) [**b**] *x is left invertible in R iff $x + \mathrm{J}(R)$ is left invertible in $R/\mathrm{J}(R)$.*

(c) [**c**] *The $J(R)$ is equal to the right Jacobson radical* $\mathrm{J}(R^{\mathrm{op}}$.

(d) [**d**] *x is invertible in R iff $x + \mathrm{J}(R)$ is invertible in $R/\mathrm{J}(R)$.*

Proof: (a) Let $x \in R$ and let $\mathcal{M}$ be the set of maximal left ideals in R. The the follwing are equivalent

$$\begin{array}{cc}
x \notin \mathrm{J}(R) & \\
x \notin M & \text{for some}M \in \mathcal{M} \\
Rx + M = R & \text{for some}M \in \mathcal{M} \\
rx + m = 1 & \text{for some}M \in \mathcal{M}, m \in \mathcal{M}, r \in R \\
rx - 1 \in \mathcal{M} & \text{for some } r \in R, M \in \mathcal{M} \\
R(rx-1) \neq R & \text{for some}r \in R \\
(rx-1) \text{ is not left invertible} & \text{for some}r \in R
\end{array}$$

(b) If x is left invertible, then $x + \mathrm{J}(R)$ is left invertible. Suppose now that $x + \mathrm{J}(R)$ is left invertible. Then $1 - yx \in \mathrm{J}(R)$ for some $y \in R$. By (a) $yx = 1 - (1 - yx)$ has a left inverse. Hence also x as a left inverse.

As a step towards (c) and (d) we prove next:

1° [**1**] *If $x - 1 \in \mathrm{J}(R)$. Then x is invertible.*

By (b) there exists $k \in R$ with $kx = 1$. Thus $k - 1 = k - kx = k(1 - x) \in \mathrm{J}(R)$ and so by (b) again k has a left inverse l. So by 2.2.2 $x = l$ and k is an inverse of x.

(c) Let $j \in \mathrm{J}(R)$ and $r \in \mathrm{J}(R)$. Since $\mathrm{J}(R)$ is an ideal, $jr \in \mathrm{J}(R)$. Thus by (1°) $1 + jr$ is invertible. So by (a) applied to R^{op}, $j \in \mathrm{J}(R^{\mathrm{op}}$. Hence $\mathrm{J}(R) \leq \mathrm{J}(R^{\mathrm{op}}$. By symmetry $\mathrm{J}(R) \leq \mathrm{J}(R^{\mathrm{op}}$.

(d) Follows from (b) applied to R and R^{op}. □

Lemma 6.3.3 [**jr cap za**] *Let A be a ring, R a subring and suppose that A is finite generated as an R-module. Then $\mathrm{J}(R) \cap Z(A) \leq \mathrm{J}(A)$.*

Proof: Let M be a simple A-module. Then M is cylcic as an A-module and so finitely generated as an R-module. Thus by 6.3.1, $\mathrm{J}(R)M \neq M$. Hence also $(\mathrm{J}(R) \cap \mathrm{Z}(A))M < M$ and since $(\mathrm{J}(R) \cap \mathrm{Z}(A))M$ is an A-submodule we conclude that $\mathrm{J}(R) \cap \mathrm{Z}(A) \leq \mathrm{A}_A(M)$. Thus $\mathrm{J}(R) \cap \mathrm{Z}(A) \leq J(A)$. □

Proposition 6.3.4 [**jza**] *Let A be a ring.*

(a) [**a**] *If K is a nilpotent left ideal in A, then $K \leq \mathrm{J}(A)$*

(b) [**b**] *If A is artian, $\mathrm{J}(A)$ is the largest nilpotent ideal in A.*

(c) [**c**] *If A is artian and finitely $Z(A)$-generated then* $\mathrm{J}(A) \cap \mathrm{Z}(A) = \mathrm{J}(\mathrm{Z}(A))$.

Proof:

(a) Let $k \in K$. Then rk is nilpotent and so $1 + rk$ is invertible in in R. So by 6.3.2(a), $k \in \mathrm{J}(A)$.

(b) Since A is Artinian we can choose $n \in \mathbb{N}$ with $\mathrm{J}(A)^n$ minimal. Then $\mathrm{J}(A)\mathrm{J}(A)^n = \mathrm{J}(A)^n$. Suppose $\mathrm{J}(A)^n \neq 0$ and choose a left ideal K in A minimal with $\mathrm{J}(A)^n K \neq 0$. Let $k \in K$ with $\mathrm{J}(A)^n k \neq 0$. Then $\mathrm{J}(A)^n \mathrm{J}(A)k = J^(A)^n k \neq 0$ and so by mimimality of K, $K = \mathrm{J}(A)k$. Thus $k = jk$ for some $j \in \mathrm{J}(A)$. Thus $(1 - j)k = 0$. By 6.3.2 $1 - j$ is invertible and so $k = 0$, a contradiction.

(c) By (b) $\mathrm{J}(A) \cap \mathrm{Z}(A)$ is a nilpotent ideal in $\mathrm{Z}(A)$ and so by (a) $\mathrm{J}(A) \cap \mathrm{Z}(A) \leq \mathrm{Z}(\mathrm{J}(A))$. By 6.3.3 $\mathrm{J}(\mathrm{Z}(A)) \leq \mathrm{J}(A) \cap \mathrm{Z}(A)$ and (c) is proved. □

Lemma 6.3.5 [**invertible in ere**] *Let R be a ring, $S \leq \mathrm{Z}(R)$ and suppose that R is a finitely generated S-module. Let $e \in R$ be an idempotent and $x \in eRe$ with $x + \mathrm{J}(S)R = e + \mathrm{J}(S)R$. Then there exists a unique $y \in eRe$ with $xy = yx = e$.*

Proof: Since $(ere)(ete) = e(eter)e$, eRe is a ring with identity e. We need to show that x is invertible in eRe. If $R = ST$ for a finite subset T of R then also $eRe = eS(eTe)$ and so eRe is a finitely geneerated eS-module. Also $eS = eSe \leq \mathrm{Z}(eRe)$ and so by 6.3.3 $\mathrm{J}(eS) \leq \mathrm{J}(eRe)$. Since $e : S \to eS$ is an onto ring homomorphism, $eJ(S) \leq \mathrm{J}(eS) \leq \mathrm{J}(eRe)$. Since $x \in eRe$ and $x - e \in \mathrm{J}(S)R$

$$x - e = e(x - e)e \in e\mathrm{J}(S)Re = e\mathrm{J}(s)eRe \leq \mathrm{J}(eRe)eRe \leq \mathrm{J}(eRe)$$

Thus $x - e \in \mathrm{J}(eRe)$ and by 6.3.2 x has an inverse in eRe. □

6.4 A basis for $\mathbb{C}\tilde{G}$

Lemma 6.4.1 [**from oq to f**] *Let X be non-empty finite subset of $\overline{\mathbb{Q}}^\sharp$. Then there exists $b \in \mathbb{Q}(X)$ with $bX \subseteq \mathbb{A}$ and $bX \nsubseteq I$.*

Proof: By 6.2.22 applied with $\mathbb{K} = \mathbb{Q}(X)$ we have $I^{-1}I = \mathbb{A}$. So there exists $b \in I^{-1}$ with $bX \nsubseteq I$. □

Corollary 6.4.2 [**f linearly independent**] *Let V be an $\overline{\mathbb{Q}}$-space and $(v_i)_{i=1}^n \in V^n$. Let $W = \mathbb{A} < v_i \mid 1 \leq i \leq n$. and suppose that $(v_i + IW)_{i=1}^n$ is $\mathbb{F}$-linearly independent in W/IW. Then $(v_i)_{i=1}^n$ is linearly idenpendet over $\overline{\mathbb{Q}}$.*

Proof: Suppose there exists $a_i \in \overline{\mathbb{Q}}$ not all zero with $\sum_{i=1}^n a_i v_i = 0$. By 6.4.1 there exists $b \in \overline{\mathbb{Q}}$ with $ba_i \in \mathbb{A}$ anf $ba_j \notin I$ for some $1 \leq j \leq n$. Then $\sum_{i=1}^n (ba_i + I)(v_i + IW) = 0$ but $ba_j + I \neq I$, a contradcition. □

Lemma 6.4.3 [**linear independence of characters**]

(a) [**a**] $(\chi_M \mid M \in \mathcal{S}_p)$ *is $\mathbb{F}$-linear independent in $\mathbb{F}G$.*

(b) [**b**] $(\phi_M \mid M \in \mathcal{S}_p)$ *is $\mathbb{C}$-linearly independent in $\mathbb{C}\tilde{G}$.*

Proof: (a) Let $f_M \in \mathbb{F}$ with $\sum f_M \chi_M = 0$. Pick $e_M \in \mathrm{End}_{\mathbb{F}}(M)$ with $\mathrm{tr}_M(e_M) = 1$. 2.5.18 there exists $a_M \in \mathbb{F}G$ such that a_M acts as e_M on N and trivially on N for all $M \neq N \in \mathcal{S}_p$. Then

$$0 = \sum_{N \in \mathcal{S}_p} f_N \chi_N(e_M) = f_M$$

and so (a) holds.

(b) Since all coefficents of ϕ_M are in $\mathbb{A}$, $\phi_M \mid M \in \mathcal{S}_p)$ is $\mathbb{C}$-linearly independent iff $(\phi_M \mid M \in \mathcal{S}_p)$ is $\overline{\mathbb{Q}}$-linearly independent and iff $(\check{\phi}_M \mid M \in \mathcal{S}_p)$ is $\overline{\mathbb{Q}}$-linearly independent. By 6.1.5 $(\check{\phi}_M)^* = \chi_M$ and so by (a) $(\check{\phi}_M)^* \mid M \in \mathcal{S}_p)$ is $\mathbb{F}$-linearly independent. So (b) follows from 6.4.2. □

Lemma 6.4.4 [**existence of a lattice**] *Let V be an $\rtimes Q$-space and W a finitely generated $\mathbb{A}_I$ submodule of V with $V = \mathbb{Q}W$. Then W is an $\mathbb{A}_I$-lattice in V.*

Proof: Note that $W/I_I W$ is a finite dimensional vector space over $\mathbb{A}_I/I_I = \mathbb{F}$ and so has a basis $u_i + I_I W, 1 \leq i \leq n$. By 6.4.2 $(u_i)_{i=1}^n$ is linearly independent over $\overline{\mathbb{Q}}$ and so also over $\mathbb{A}_I$. Let $U = \mathbb{A}_i\langle u_i \, od 1 \leq i \leq n$. Then $W = U + I_I W$. Since I_I is the unique maximal ideal in $\mathbb{A}_I$, $I_I = (\,\mathbb{A}_I)$. Thus by the Nakayama Lemma 6.3.1 applied to W/U gives $W = U$. Hence also $V = \overline{\mathbb{Q}}W = \overline{\mathbb{Q}V}\langle u_i \mid 1 \leq i \leq n\rangle$ □

Lemma 6.4.5 [**existence of oq lattice**] *Let $\mathbb{E} : \mathbb{K}$ be a field extension and M a simple $\mathbb{K}G$-module. If $\mathbb{K}$ is algebraicly closed then there exists an G-invarinant $\mathbb{K}$ lattice L is M. For any such L, L is a simple $\mathbb{K}G$-module and $M \cong \mathbb{E} \otimes_{\mathbb{K}} L$.*

Proof: Since G is finite there exists a simple $\mathbb{K}G$-submodule L in M. Moreover there is a non-zero $\mathbb{E}G$-linear map $\alpha : \mathbb{E} \otimes_{\mathbb{K}} L \to M, e \otimes l \to el$. Since $\mathbb{K}$ is algebraicly closed, $\mathbb{E} \otimes_{\mathbb{K}} L$ is a simple $\mathbb{E}G$-module. The same is true for M and so α is an isomorphism. In particular, any $\mathbb{K}$ basis for L is also a $\mathbb{E}$-basis for M and so L is a K-lattice in M.

Now let L is any $\mathbb{K}$-lattice in G. If $) \neq N \leq L$ is a $\mathbb{K}G$-submodule then $\mathbb{E}N$ is a $\mathbb{E}G$-submodule of M. Thus $\mathbb{E}N = M$ and $\dim_{\mathbb{K}} N = \dim_{\mathbb{E}} \mathbb{E}N = \dim_{\mathbb{E}} M = \dim_{\mathbb{K}} L$ and so $N = L$ and L is a simple $\mathbb{K}G$-module. □

Lemma 6.4.6 [**existence of ai lattice**] *Let M be an $\mathbb{C}G$-module. Then there exists a G-invariant $\mathbb{A}_I$-lattice L in M.*

Proof: By 6.4.5 there exists a G-invariant $\overline{\mathbb{Q}}$-lattice V in M. Let X be a $\overline{\mathbb{Q}}$-basis for V and put $L = \mathbb{A}_I GX$. Since G and X are finite, L is finitely $\mathbb{A}_I$-generated. Thus by 6.4.4, L is an $\mathbb{A}_I$-lattice in V and so also in M. □

Lemma 6.4.7 [**characters are brauer characters**] *Let* M *be an* $\mathbb{C}G$*-module and* L *a* G*-invariant* $\mathbb{A}_I$*-lattice in* M*. Let* M° *be the* $\mathbb{F}G$*-module,* L/I_IL*. Then* $\chi_M^* = \chi_{M^\circ}$ *and* $\tilde{\chi}_M = \phi_{M^\circ}$

Proof: Let $\mathcal{B}$ be an $\mathbb{A}_I$ basis for L, $g \in G$ and D the marix for g with respect to $\mathcal{B}$. Then D^* is the matrix for g with respect to the basis $(b + I_L L)_{b \in \mathcal{B}}$ for M°. Since $\eta_M(g) = \det(x\mathrm{I}\, d_n - D)$ we conclude that $\eta_M(g)^* = \eta_{M^\circ}(g)$. In particular $\chi_M(g)^* = \chi_{M^\circ}(g)$ and if $\eta_M(g) = \prod_{i=1}^n (x - \xi_i)$ then $\eta_{M^\circ}(g) = \prod_{i=1}^n (x - \xi_i^*)$. So if $g \in G^\circ$, then $\chi_M(g) = \phi_{M^\circ}(g)$.□

Definition 6.4.8 [**def:Irr G**]

(a) [**a**] $\mathrm{Irr}(G) = \{\chi_M \mid M \in \mathcal{S}\}$ *is the set of simple characters of* G*.*

(b) [**b**] $\mathrm{IBr}(G) = \{\phi_M \mid M \in \mathcal{S}_p\}$ *is the set of simple Brauer characters of* G*.*

(c) [**c**] $Z\mathbb{C}\tilde{G} := \mathbb{C}\tilde{G} \cap Z(\mathbb{C}G)$ *is the set of complex valued class function on* $\tilde{G}$*.*

(d) [**d**] *If* M *be an* $\mathbb{C}G$*-module and* L *an* G *invariant* $\mathbb{C} : \mathbb{A}_I$ *lattice in* M*, then* $M^\circ = L/I_IL$ *is called a* reduction modulo p *of* M*.*

Theorem 6.4.9 [**ibr basis**]

(a) [**a**] $Z\mathbb{C}(\tilde{G})$ *is the* $\mathbb{C}$*-span of the Brauer characters.*

(b) [**b**] $\mathrm{IBr}(G)$ *is a* $\mathbb{C}$*-basis for*$Z\mathbb{C}(\tilde{G})$

(c) [**c**] $|\mathcal{S}|_p = |\mathrm{IBr}(G)$ *is the number of* p'*-conjugacy classes.*

Proof: (a) Observe that the map $\tilde{}: Z(\mathbb{C}G) \to Z\mathbb{C}(\tilde{G})$ is an orthogonal projection and so onto. On the otherhand since $Z(\mathbb{C}G)$ is an $\mathbb{C}$ -span of the G-characters we conclude from 6.4.7 that the image of $\tilde{}$ is conatained in $\mathbb{C}$-span of the Brauer characters. So (a) holds.

(b) By 6.1.3(e) every Brauer chacter is a sum of simple Brauet charcters. So by (a), $\mathrm{IBr}(G)$ spans $Z\mathbb{C}(\tilde{G})$ By 6.4.3(b) $\mathrm{IBr}(G)$ is linearly independent over $\mathbb{C}$ and so (b) holds.

(c) Both $\mathrm{IBr}(G)$ and $(a_C \mid C a p'$ conjugacy class$\}$ are bases for $Z\mathbb{C}(\tilde{G})$ □

Definition 6.4.10 [**def:decomposition matrix**]

(a) [**a**] $D = D(G) = (d_{phi\chi})$ *is the matrix of* $\tilde{}: Z\mathbb{C}G \to Z\mathbb{C}\tilde{G}$ *with respect to* $\mathrm{Irr}(G)$ *and* $\mathrm{IBr}(G)$*.* D *is called the* decompositon matrix *of* G*.*

(b) [**b**] $C = C(G) = (c_{\phi\psi})$ *is the inverse of Gram matrix of* $(\cdot \mid \cdot)$ *with respect to* $\mathrm{IBr}(G)$. C *is called the* Cartan matrix *of* G.

(c) [**c**] *For* $\phi \in \mathrm{IBr}(G)$, $\Phi_\phi = \sum_{\chi\in\mathrm{Irr}(G)} d_{\phi\chi}\chi$ *is called the* projective indecomposable *character associated to* ϕ. *For* $M \in \mathcal{S}_p$ *put* $\Phi_M = \Phi_{\phi_M}$.

Lemma 6.4.11 [**basic decomposition**]

(a) [**a**] *Let* $\chi \in \mathrm{Irr}(G)$. *Then* $\tilde{\chi} = \sum_{\phi\in\mathrm{IBr}(G)} d_{\phi\chi}\phi$.

(b) [**z**] *Let* $M \in \mathcal{S}(G)$, M° *a* p*-reduction of* M, $N \in \mathcal{S}_p(G)$ *and* $\mathcal{F}$ *a* $\mathbb{F}G$*-composition series on* M. *Then* $d_{\phi_N\chi_M}$ *is the number of factors of |caF isomorphic to* N.

(c) [**b**] *Let* $\phi, \psi \in \mathrm{IBr}(G)$. *Then* $\Phi_\phi \in Z\mathbb{C}\tilde{G}$ *and* $(\Phi_\phi \mid \psi) = \delta_{\phi\psi}$. *So* $(\Phi_\phi \mid \phi \in \mathrm{Irr}(G))$ *is the dual basis for* $Z\mathbb{C}\tilde{G}$.

(d) [**c**] $C^{-1} = ((\phi \mid \psi))_{\phi\psi}$

(e) [**d**] $C = ((\Phi_\phi \mid \Phi_\psi))$ *is Gram matrix of* $(\mathrm{cot} \mid \cdot)$ *with respect to* $(\Phi_\phi \mid \phi \in \mathrm{IBr}(G)$.

(f) [**e**] *Let* $\phi \in \Psi$. *Then* $\Phi_\phi = \tilde{\Phi}_\phi = \sum_{\psi\in\mathrm{IBr}(G)} c_{\phi\psi}\psi$.

(g) [**f**] $C = DD^{\mathrm{T}}$.

Proof: (a) Immediate from the definition of D.

(b) For $N \in \mathcal{S}_p(G)$ Let a_N be the number of compostion factors of G isomorphic to N. Then by 6.1.3(e), $\phi_{M^\circ} = \sum_{N\in\mathcal{S}_p(G)} a_N\phi_N$.

By 6.4.7 $\phi_{M^\circ} = \tilde{\chi}_M$. So (a) and the linearly independence of $\mathrm{IBr}(G)$ implies $d_{\phi_N\chi_M} = a_N$.

(c) Follows from 4.1.14

(d) Immediate from the definition of C.

(e) and (f) follows from 4.1.16

(g) From (d) and the definition of Φ_π:

$$c_{\phi\psi} = (\sum_{\chi\in\mathrm{Irr}(G)} d_{\phi\chi}\chi \mid \sum_{\chi\in\mathrm{Irr}(G)} d_{\psi\chi}\chi) = \sum_{\chi\in\mathrm{Irr}(G)} d_{\phi\chi}d_{\psi\chi}$$

and so (g) holds.

Corollary 6.4.12 [**dphichi not zero**] *For each* $\phi \in \mathrm{IBr}(G)$, *there exists* $\chi \in \mathrm{Irr}(G)$ *with* $d_{\phi\chi\neq 0}$. *In otherwords, for each* $M \in \mathcal{S}_p$ *there exists a* $\check{M} \in \mathcal{S}$ *such that* M *is isomorphic to a composition factor of nay* p*-reduction of* $\check{M}$.

Proof: Follows from the fact that $\tilde{}: Z(\mathbb{C}G) \to Z\mathbb{C}\tilde{G}$ is onto. □

Corollary 6.4.13 [**projective is regular**] *Let* $M \in \mathcal{S}_p$ *and* $P \in \mathrm{Syl}_p(M)$*. Then* $\dim \Phi_M$ *is divisiple* $|P|$*. Moreover,* Φ_M *restricted to* P *is an integral multiple of the regular character for* P*.*

Proof: Since $\Phi_M = \tilde{\Phi}_M$ we have $\Phi_M(g) = 0$ for all $g \in P^\sharp$. Thus $(\Phi_M\ |_P|\ 1_P)_P = \frac{1}{|P|}\Phi_M(1)$ and so $|P|$ divides $\Phi_M(1)$. Therefore

$$\Phi_M(1) = \frac{\Phi_M(1)}{|P|}\chi^P_{\mathrm{reg}}$$

□

Theorem 6.4.14 [**pprime=0**] *Suppose* G *is a* $p\prime$ *group.*

(a) [**a**] $\mathrm{Irr}(G) = \mathrm{IBr}(G)$ *and* $D = (\delta_{\phi\psi})$*.*

(b) [**b**] *For* $M \in \mathcal{S}$ *let* M° *be a reduction modulo p. Then* M° *is a simple* $\mathbb{F}G$*-module and the map* $\mathcal{S} \to \mathcal{S}_p, M \to M^\circ$ *is bijection.*

Proof: By 3.1.3(c) $|G| = \sum_{\phi\in\mathrm{IBr}(G)} \phi(1)^2 = \sum_{\chi\in\mathrm{Irr}(G)} \chi(1)^2$ Thus

$$\begin{array}{rclcl}
|G| & = & \displaystyle\sum_{\chi\in\mathrm{Irr}(G)} \chi(1)^2 & = & \displaystyle\sum_{\chi\in\mathrm{Irr}(G)} \left(\sum_{\phi\in\mathrm{IBr}(G)} d_{\phi\chi}\phi(1)\right)^2 \\
 & \geq & \displaystyle\sum_{\chi\in\mathrm{Irr}(G)}\sum_{\phi\in\mathrm{IBr}(G)} d_{\phi\chi})^2\phi(1)^2 & = & \displaystyle\sum_{\phi\in\mathrm{IBr}(G)} \left(\sum_{\chi\in\mathrm{Irr}(G)} d_{\phi\chi})^2\right)\phi(1)^2 \\
 & \geq & \displaystyle\sum_{\phi\in\mathrm{IBr}(G)} \phi(1)^2 & = & |G|
\end{array}$$

Hence equality holds everythere. In particular $\sum_{\chi\in\mathrm{Irr}(G)} d_{\phi\chi})^2 = 1$ for all $\phi \in \mathrm{IBr}(G)$. So there exists a unique $\chi_\phi \in \mathrm{Irr}(G)$ with $d_{\phi\chi_\phi} \neq 0$. Moreover $d_{\phi\chi_\phi} = 1$.

Also $\left(\sum_{\phi\in\mathrm{IBr}(G)} d_{\phi\chi}\right)^2 = \sum_{\phi\in\mathrm{IBr}(G)}(d_{\phi\chi})^2$ and so for each $\chi \in \mathrm{IBr}(G)$ there exists unique $\phi_\chi \in \mathrm{IBr}(G)$ with $d_{\phi_\chi\chi} \neq 0$. Hence $\chi = \chi_{\phi_\chi}$, $d_{\phi_\chi\chi} = 1$, $\chi = \tilde{\chi} = \phi_\chi = \chi_\chi$ and (a) holds.

(b) follows from (a) and 6.4.11(b). □

Proposition 6.4.15 [**fong**] *Suppose that* $p = 2$ *and* $\phi \in \mathrm{IBr}(G)$*. If* ϕ *is real valued and* $\phi(1)$ *is odd, then* $\phi = 1_{\tilde{G}}$*.*

Proof: Let $M \in \mathcal{S}_p$ with $\phi = \phi_M$. Then $\phi_{M^*} = \overline{\phi}_M = \Phi_M$ and some $M \cong M^*$. Thus the proposition follows from 4.1.22 and 4.1.21. □

Lemma 6.4.16 [**opg trivial**] *Let $M \in \mathcal{S}_p$. Then $O_p(G) \leq C_G(M)$.*

Proof: Let W be a simple $\mathbb{F}O_p(G)$ submodule in M. The number of p' conjugacy classes of $O_p(G) = 1$. So up to isomorphism $O_p(G)$ has a unique simple module, namely $\mathbb{F}_{O_p(G)}$. Thus $0 \neq W \leq C_M(O_p(G))$. Since $C_M(O_p(G))$ is an $\mathbb{F}G$-submodule we conclude $M = C_M(O_p(G))$ and $O_p(G) \leq C_G(M)$. □

6.5 Blocks

Lemma 6.5.1 [**omegam**] *Let $\mathbb{K}$ be an algebraicly closed field and M a simple $\mathfrak{G}G$-moudle.*

(a) [**a**] *$a \in Z(\mathbb{K}G)$ there exists a unique $\omega_M \in \mathbb{K}$ with $\rho_M(a) = \omega_M(a)\mathrm{id}_M$.*

(b) [**b**] *$\omega_M : Z(\mathbb{K}G) \to \mathbb{K}$ is a ring homomorphism.*

(c) [**c**] *$\chi_M(a) = \dim_{\mathbb{K}} M \cdot \omega_M(a) = \chi_M(1)\omega_M(a)$.*

(d) [**d**] *If $\mathbb{K} = \mathbb{C}$ then and $a \in Z(\mathbb{A}G)$, then $\omega_M(a) \in \mathbb{A}$.*

Proof: (a) follows from Schurs Lemma 2.5.3.

(b) and (c) are obvious.

(d) By 3.2.13 $\omega_M(a_C) \in \mathcal{A}$ for all $C \in \mathcal{C}$. Since $(a_C \mid C \in \mathcal{C})$ is a $\mathbb{A}$-basis for $Z(\mathbb{A}G)$, (d) follows from (b). □

Definition 6.5.2 [**def:lambdaphi**]

(a) [**a**] *Let $M \in \mathcal{S}$ and $\chi = \chi_M$. Then $\omega_\chi = \omega_M$.*

(b) [**b**] *Let $M \in \mathcal{S}$ and $\chi = \chi_M$. Then $\lambda_\chi : Z(\mathbb{F}G) \to \mathbb{F}$ is define by $\lambda_\chi(a^*) = \omega_\chi(a)^*$ for all $a \in Z(\mathbb{A}_I G)$.*

(c) [**c**] *Let $M \in \mathcal{S}_p$ and $\phi = \phi_M$. Then $\lambda_\phi = \omega_M$.*

(d) [**d**] *Define the relation $\sim_p$ on $\mathrm{Irr}(G) \cup \mathrm{IBr}(G)$ by $\alpha \sim_p \beta$ if $\lambda_\alpha = \lambda_\beta$. A* block *(or p-block) of G is an equivalence class of $\sim_p$.*

(e) [**e**] *$\mathrm{Bl}(G)$ is the set of blocks of G.*

(f) [**f**] *If B is a block of G then $\mathrm{Irr}(B) = B \cap \mathrm{Irr}(G)$ and $\mathrm{IBr}(B) = B \cap \mathrm{IBr}(G)$.*

(g) [**g**] *For $\mathcal{A} \subseteq \mathrm{Irr}(G)$, put $\mathcal{A}^\dagger = \{\phi \in \mathrm{IBr}(G) \mid d_{\phi\chi\neq 0}$ for some $\chi \in \mathcal{A}\}$.*

(h) [**h**] *For $\mathcal{B} \subseteq \mathrm{IBr}(G)$, put $\mathcal{B}^\dagger = \{\chi \in \mathrm{Irr}(G) \mid d_{\phi\chi\neq 0}$ for some $\phi \in \mathcal{B}\}$.*

Proposition 6.5.3 [**d and lambda**] *(a)* [**a**] *Let* $\chi \in \mathrm{Irr}(G)$ *and* $\phi \in \mathrm{IBr}(G)$*. If* $d_{\phi\chi} \neq 0$ *then* $\lambda_\phi = \lambda_\chi$*.*

(b) [**b**] *Let* B *be a block of* G *then* $\mathrm{IBr}(B) = \mathrm{Irr}(B)^\dagger$ *and* $\mathrm{Irr}(B) = \mathrm{IBr}(B)^\dagger$*.*

Proof: (a) Let $M \in \mathcal{S}$ with $\chi = \chi_M$ and $N \in \mathcal{S}_p$ with $\phi = \phi_N$. Let L be an G-invariant A_I-lattice in M. Since $d_{\phi\chi \neq 0}$, N is isomorphic to $\mathbb{F}G$ composition factor of $M^\circ = L/I_I L$. Let $a \in Z(\mathbb{A}G)$. Then a acts as the scalar $\omega_\chi(a)$ on M and on L. Thus a acts as the scalar $\omega_\chi(a)^* = \lambda_\chi(a^*)$ on M° and on N. Thus $\lambda_\chi(a^*) = \lambda_\phi(a^*)$ and (a) holds.

(b) $\phi \in \mathrm{IBr}(G)$ with $d_{\phi\chi}$ for some $\chi \in \mathrm{Irr}(B)$ then by (a) $\phi \in B$. Thus $\mathrm{Irr}(B)^\dagger \subseteq \mathrm{IBr}(B)$. Conversely if $phi \in \mathrm{IBr}(B)$ we can choose (by 6.4.12) $\chi \in \mathrm{IBr}(G)$ with $d_{\phi\chi} \neq 0$. Then by (a) $\chi \in B$ and so $\mathrm{IBr}(B) \subseteq \mathrm{Irr}(B)^\dagger$. Thus $\mathrm{IBr}(B) = \mathrm{Irr}(B)^\dagger$. Similary $\mathrm{Irr}(B) = \mathrm{IBr}(B)^\dagger$. □

Let $\chi \in \mathrm{Irr}(G)$ and $\phi \in \mathrm{IBr}(G)$. Then λ_χ is defined by **??**(**??**) and λ_ϕ by **??**(**??**). If $\lambda = \phi$ then 6.5.3(a) shows that $\lambda_\chi = \lambda_\phi$.

Definition 6.5.4 [**brauer graph**] *Let* $\chi, \psi \in \mathrm{Irr}(G)$*. We say that* ϕ *and* ψ *are* linked *if there exists* $\phi \in \mathrm{IBr}(G)$ *with* $d_{\phi\chi} \neq 0 \neq d_{\phi\psi}$*. The graph on* $\mathrm{IBr}(G)$ *with edges the linked pairs is called the* Brauer graph *of* G*. We say* χ *and* ψ *are connected if* ϕ *and* ψ *lie in the same connected component of the Brauer graph.*

Corollary 6.5.5 [**blocks and connected component**]

(a) [**a**] *Let* $\mathcal{A} \subseteq \mathrm{Irr}(G)$*. Then* $\mathcal{A}^{\dagger\dagger}$ *consist of all simple characters linked to some element of* $\mathcal{A}$*.*

(b) [**b**] *Let* $\mathcal{A} \subseteq \mathrm{Irr}(G)$*. Then* $\mathcal{A}$ *is union of connected components of the Brauer graph iff and only if* $\mathcal{A} = \mathcal{A}^{\dagger\dagger}$*.*

(c) [**c**] *If* B *is a block then* $\mathrm{Irr}(B)$ *is a union of connected components of the Brauer Graph.*

Proof: (a) Let $\psi \in \mathrm{Irr}(G)$. Then

$$\begin{gathered} \psi \text{ is linked to some element of } \mathcal{A} \\ \text{iff} \\ \text{there exists } \chi \in \mathcal{A} \text{ and } \phi \in \mathrm{IBr}(G) \text{ with } d_{\phi\chi} \neq 0 \neq d_{\phi\psi} \\ \text{iff} \\ \text{there exists } \phi \in \mathcal{A}^\dagger \text{ with } d_{\phi\psi} \neq 0 \\ \text{iff} \\ \psi \in \mathcal{A}^{\dagger\dagger} \end{gathered}$$

So (a) holds.

(b) follows immediately from (a).

(c) By 6.5.3 $\mathrm{Irr}(B)^{\dagger\dagger} = \mathrm{IBr}(B)^\dagger = \mathrm{Irr}(B)$.

Proposition 6.5.6 [**osima**] *Let $\mathcal{A} \subseteq \operatorname{Irr}(G)$ with $\mathcal{A} = \mathcal{A}^{\dagger\dagger}$. Let $x \in \tilde{G}$ and $y \in G$. Then*

$$\sum_{\chi \in \mathcal{A}} \chi(x)\chi(y) = \sum_{\phi \in \mathcal{A}^\dagger} \phi(x)\Phi_\phi(y)$$

Proof: We compute

$$\begin{array}{cccc} & \displaystyle\sum_{\chi\in\mathcal{A}} \chi(x)\chi(y) & = & \displaystyle\sum_{\chi\in\mathcal{A}} \left(\sum_{\phi\in\operatorname{IBr}(G)} d_{\phi\chi}\phi(x) \right) \chi(y) \\ = & \displaystyle\sum_{\chi\in\mathcal{A}} \left(\sum_{\phi\in\mathcal{A}^\dagger} d_{\phi\chi}\phi(x) \right) \chi(y) & = & \displaystyle\sum_{\chi\in\mathcal{A}^\dagger} \left(\sum_{\phi\in\mathcal{A}} d_{\phi\chi}\chi(y) \right) \phi(x) \\ = & \displaystyle\sum_{\chi\in\mathcal{A}^\dagger} \left(\sum_{\phi\in\operatorname{Irr}(G)} d_{\phi\chi}\chi(y) \right) \phi(x) & = & \displaystyle\sum_{\chi\in\mathcal{A}^\dagger} \Phi_\phi(y)\phi(x) \end{array}$$

□

Corollary 6.5.7 (Weak Block Orthogonality) [**weak block orthogonality**] *Let B be block of G, $x \in \tilde{G}$ and $y \in G \setminus \tilde{G}$. Then*

$$\sum_{\chi\in\operatorname{Irr}(B)} \chi(x)\overline{\chi(y)} = 0$$

Since $\operatorname{Irr}(G)^{\dagger\dagger} = \operatorname{Irr}(G)$ we can apply 6.5.6:

$$\sum_{\chi\in\operatorname{Irr}(B)} \chi(x)\overline{\chi(y)} = \sum_{\chi\in\operatorname{Irr}(B)} \chi(x)\chi(y^{-1}) = \sum_{\phi\in\mathcal{A}^\dagger} \phi(x)\Phi_\phi(y^{-1})$$

Since $y^{-1} \not\tilde{G}$ 6.4.11(c) implies $\Phi_\phi(y^{-1} = 0$ and so the Corollary is proved. □

Definition 6.5.8 [**def:ea**]

(a) [**a**] *For $M \in \mathcal{S}$ and $\chi = \chi_M$ put $e_\chi = e_M$(see 3.1.3(d).*

(b) [**b**] *For $\mathcal{A} \subseteq \operatorname{Irr}(G)$, put $e_{\mathcal{A}} = \sum_{\chi\in\mathcal{A}} e_\chi$.*

Corollary 6.5.9 [**ea in ai(tilde g)**] *Let $\mathcal{A} \subseteq \operatorname{Irr}(G)$ with $\mathcal{A} = \mathcal{A}^{\dagger\dagger}$. Then $e_{\mathcal{A}} \in ZA_I\tilde{G}$.*

Proof: Let $\chi \in \mathcal{A}$ and $g \in G$. By 3.2.12(a), g coefficents of e_χ is $\frac{1}{|G|}\chi(1)\overline{\chi}(x)$ Let f_g be the g-coefficent of $e_{\mathcal{A}}$. Then by 6.5.6

$$f_g = \frac{1}{|G|} \sum_{\chi\in\mathcal{A}} \chi(1)\chi(x^{-1}) = \frac{1}{|G|} \sum_{\phi\in\mathcal{A}^\dagger} \phi(1)\Phi_\phi(g^{-1})$$

If $g \notin \tilde{G}$ we conclude that $f_g = 0$ and so

$$(*) \qquad e_{\mathcal{A}} \in \mathbb{C}\tilde{G}$$

Suppose now that $g \in \tilde{G}$. Then using 6.5.6 one more time:

$$f_g = \frac{1}{|G|}\sum_{\chi \in \mathcal{A}} \chi(g^{-1})\chi(1) = \frac{1}{|G|}\sum_{\phi \in \mathcal{A}^\dagger} \phi(g^{-1})\Phi_\phi(1) = \sum_{\phi \in \mathcal{A}^\dagger} \phi(g^{-1})\frac{\Phi_\phi(1)}{|G|}$$

By 6.4.13 $\frac{\Phi_\phi(1)}{|G|} \in \mathbb{A}_I$. Also $\phi(g^{-1} \in \mathbb{A} \in \mathbb{A}_I$ and so $f_g \in \mathbb{A}_i$. Thus $e_{\mathcal{A}} \in \mathbb{A}G$. Together with (*) and the fact that e_χ is class function we see that the Corollary holds. □

Lemma 6.5.10 [**unions of blocks**] *Let $\mathcal{A} \subseteq \mathrm{Irr}(G)$ with $e_{\mathcal{A}} \in Z(\mathbb{A}_I(G))$. Then $\mathcal{A} = \bigcup_{i=1}^k \mathrm{Irr}(B_i)$ for some blocks $B_1, \dots B_k$.*

Proof: Let $\chi, \psi \in \mathrm{Irr}(G)$. Then $\omega_\chi(e_\psi) = \delta_{\chi\psi}$ and so $\omega_\chi(e_{\mathcal{A}}) = 1$ if $\chi \in \mathcal{A}$ and $\omega_\chi(e_{\mathcal{A}}) = 0$ otherwise. By assumption $e_{\mathcal{A}} \in Z(\mathbb{A}_I(G))$ and so $\lambda_\chi(e^*_{\mathcal{A}}) = \omega_\chi(e_{\mathcal{A}})$ and so

$$(*) \qquad \chi \in \mathcal{A} \text{ iff } \lambda_\chi(e^*_{\mathcal{A}}) = 1$$

Let B be the block containg χ and $\psi \in \mathrm{Irr}(B)$. Then $\lambda_\chi(e^*_{\mathcal{A}}) = \lambda_\psi(e^*_{\mathcal{A}})$ and so by (*), $\chi \in \mathcal{A}$ iff $\psi \in \mathcal{A}$. □

Theorem 6.5.11 [**block=connected components**] *If B is block, then $\mathrm{Irr}(B)$ is connected in the Brauer Graph. So the connected components of the Brauer graph are exactly the $\mathrm{Irr}(B)$, B a block.*

Proof: If B is a block then by 6.5.5(c), $\mathrm{Irr}(B)$ is the union of connected components. Connversely if $\mathcal{A}$ is a connected component then by 6.5.9 $e_A \in Z(A_I G)$ and so by 6.5.10 $\mathcal{A}$ is a union of blocks. □

Definition 6.5.12 [**def:fb**]

(a) [**a**] *Let B be a block. Then $e_B = e^*_{\mathrm{Irr}(B)}$ and $f_B = e_{\mathrm{Irr}(B)}$.*

(b) [**b**] *Let $\mathcal{A}$ be set of blocks. Then $e_{\mathcal{A}} = \sum_{B \in \mathcal{A}} e_B$ and $f_{\mathcal{A}} = \sum_{B in \mathcal{B}} f_B$*

(c) [**c**] *Let B be block, then $\mathbb{F}B := \mathbb{F}Ge_B$.*

(d) [**d**] *If $\mathcal{A}$ is a set of blocks, then $\mathbb{F}\mathcal{A} = \mathbb{F}Ge_{\mathcal{A}}$.*

(e) [**e**] *Let B be a block then $\lambda_B = \lambda_\phi$ for any $\phi \in \mathrm{IBr}(G)$.*

(f) [**f**] *Let B be a block, then $\mathcal{S}_p(B) = \{M \in \mathcal{S}_p \mid \phi_M \in B\}$ and $\mathcal{S}(B) = \{M \in \mathcal{S} \mid \chi_M \in B\}$*

Lemma 6.5.13 [**omega chi fy**] *Let X, Y be blocks and $\chi \in X$. Then $\omega_\chi(f_Y) = \delta XY$ and $\lambda_X(e_Y) = \delta_{XY}$*

Proof: This follows from $\omega_\chi(e_\psi) = \delta_{\chi\psi}$ for all $\chi\psi \in \mathrm{Irr}(G)$. □

Theorem 6.5.14 [**structure of fg**]

(a) [**a**] $\sum_{B\in \mathrm{Bl}(G)} e_B = 1$.

(b) [**b**] *$e_B \in Z(\mathbb{F}G)$ for all blocks B*

(c) [**c**] *$e_X e_Y = 0$ for any distinct blocks X and Y.*

(d) [**d**] *$e_B^2 = e_B$ for all blocks b*

(e) [**e**] *$\mathbb{F}G = \bigoplus_{B\in\mathcal{B}} \mathbb{F}B$.*

(f) [**f**] *$Z(\mathbb{F}G) = \bigoplus_{B\in\mathcal{B}} Z(\mathbb{F}B)$.*

(g) [**g**] *$\mathrm{J}(\mathbb{F}G) = \bigoplus_{B\in\mathcal{B}} \mathrm{J}(\mathbb{F}B)$.*

(h) [**h**] *Let X, Y be blocks. Then $\lambda_X(e_Y) = \delta_{XY}$.*

(i) [**i**] *Let X and Y be distincts blocks. Then $\mathbb{F}X$ annihilates all $M \in \mathcal{S}_p(Y)$.*

(j) [**j**] *Let B be a block. Then $\S_p(B)$ is set of representativves for the isomorphism classes classes of simple $\mathbb{F}B$-modules.*

Proof: (a) $\sum_{\chi\in\mathrm{Irr}(G)} e_\chi = 1$ and so also $\sum_{B\in\mathrm{Bl}(G)} e_{\mathrm{Irr}(B)} = 1$. Applying * gives (a).

(b) Since $e_\chi \in \mathrm{Z}(\mathbb{C}G)$, $e_{\mathrm{Irr}G} \in Z(\mathbb{A}_I G)$ and so (b) holds.

(c) $e_\chi e_\psi = 0$ for distinct simple characters. So $e_{Irr(X)} e_{Irr(Y)} = 0$ and so (c) holds.

(d) follows from $e^2_{\mathrm{Irr}(B)} = e_{\mathrm{Irr}(B)}$.

(e) (a) implies $\mathbb{F}G = \sum_{B\in\mathrm{Bl}(G)} \mathbb{F}B$. Let $B \in \mathcal{B}$ and $\mathcal{B} = \mathrm{Bl}(G) \setminus \{B\}$. Then by (c) $\mathbb{F}B \cdot \mathbb{F}\mathcal{B} = 0$. Moreover if $x \in \mathbb{F}B$ then $e_B x = x$ and if $x \in \mathbb{F}\mathcal{B}$ then $e_B x = 0$. Thus $\mathbb{F}B \cap \mathbb{F}\mathcal{B} = 0$ and so (d) holds.

(f) follows from (d).

(g) follows from (d) and 2.5.16(e).

(h) Let $\chi \in \mathrm{Irr}(X)$. Then $\lambda_X(e_Y) = \lambda_X(e^*_{\mathrm{Irr}(Y)}) = \omega_X((e_{\mathrm{Irr}(Y)})^* = \delta^*_{XY} = \delta_{XY}$.

(i) Let $M \in \mathcal{S}_p(Y)$. Then e_X acts as the scalar $\lambda_\phi(e_X) = \lambda_Y(e_X)$ on M. So by (h) e_X annhilates M. Thus also $\mathbb{F}X = \mathbb{F}Ge_X$ annihilates M.

(j) Any simple $\mathbb{F}B$-module is also a simple $\mathbb{F}G$-module. So (j) follows from (i). □

Theorem 6.5.15 [**zfb is local**] *$Z(\mathbb{F}B)$ is a local ring with unique maximal ideal $\mathrm{J}(\mathrm{Z}(\mathbb{F}B)) = \ker \lambda_B \cap Z(\mathbb{F}B)$.*

Proof: Let $M \in \mathcal{S}_p(B)$ and $z \in \mathrm{Z}(\mathbb{F}(B))$. Then z acts as the scalar $\lambda_B(z)$ on M. So z annihilates M if and only if $z \in \ker \lambda_B$. Thus $\mathrm{Z}(\mathbb{F}(B)) \cap \mathrm{A}_{\mathbb{F}B}(M) = \mathrm{Z}(\mathbb{F}B) \cap \ker \lambda_B$ and so

$$\mathrm{J}(\mathrm{Z}(\mathbb{F}B)) \overset{6.3.4}{=} \mathrm{Z}(\mathbb{F}B)) \cap \mathrm{J}(\mathbb{F}(B)) \underset{6.5.14(j)}{\overset{2.4.7}{=}} \mathrm{Z}(\mathbb{F}(B)) \cap \bigcap_{M \in \mathcal{S}_p(B)} \mathrm{A}_{\mathbb{F}B}(M) = Z(\mathbb{F}B) \cap \ker \lambda_B$$

So $\mathrm{J}(\mathrm{Z}(\mathbb{F}B)) = \ker \lambda_B \cap Z(\mathbb{F}B)$. Since $\mathrm{Z}(\mathbb{F}B)/ker\lambda_B \cap Z(\mathbb{F}B) \cong \mathrm{Im}\,\lambda_B = \mathbb{F}$ we conclude that $\mathrm{J}(\mathrm{Z}(\mathbb{F}B))$ is a maximal ideal in $Z(\mathbb{F}(B))$. This clearly implies that $\mathrm{J}(\mathrm{Z}(\mathbb{F}B))$ is the unique maximal ideal in $\mathbb{F}(B)$. □

Corollary 6.5.16 [**blocks indecomposable**] *Let B be a block.*

(a) [**a**] *Then $\mathbb{F}B$ is indecompsable as a ring.*

(b) [**b**] *Let e be an idempotent in $\mathrm{Z}F(G)$ then e_T for some $T \subseteq \mathrm{Bl}(G)$.*

Proof: (a) Suppose $\mathbb{F}B = X \oplus Y$ for some proper ideals X and Y. Then both X and Y have an identity. Thus $Z(X) \neq 0$, $Z(Y) \neq 0$ and $Z(\mathbb{F}(B) = \mathrm{Z}(X) \oplus Z(Y)$, a contradiction to 6.5.15.

(b) Since $e = \sum_{B \in \mathrm{Bl}(B)} ee_B$ and each non-zero ee_B is an idempotent we may assume that $e = ee_B \in \mathbb{F}B$ for some block B. Then $\mathbb{F}B = e\mathbb{F}B \oplus (e - e_B)\mathbb{F}B$ and (a) implies $e - e_B = 0$ and so $e = e_B$. □

Lemma 6.5.17 [**phi fb**] *Let B be a block then*

$$\phi_{\mathbb{F}B} = \sum_{\chi \in \mathrm{Irr}(B)} \chi(1)\tilde{\chi} = \sum_{\phi \in IBr} \Phi_\phi(1)\phi$$

Proof: By 3.2.11(c) $\chi_{\mathbb{C}G} = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)\chi$. So by 6.4.7 applied to the $\mathbb{A}_I$-lattice $\mathbb{A}_I G$ in $\mathbb{C}G$,

(1) $$\phi_{\mathbb{F}G}G = \tilde{\chi}_{\mathbb{C}G} = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)\tilde{\chi} = \sum_{B \in \mathrm{Bl}(G)} \sum_{\chi \in B} \chi(1)\tilde{\chi}$$

Observe that

(2) $$\sum_{\chi \in B} \chi(1)\tilde{\chi} = \sum_{\chi \in \mathrm{Irr}(B)} \chi(1) \left(\sum_{\phi \in \mathrm{Irr}(B)} d_{\phi\chi}\phi \right) = \sum_{\phi \in \mathrm{IBr}(B)} \Phi_\phi(1)\phi$$

and so by (1)

$$\phi_{\mathbb{F}G} = \sum_{B\in \mathrm{Bl}(G)} \sum_{\phi\in \mathrm{IBr}(B)} \Phi_\phi(1)\phi \tag{3}$$

Now let B a block. If M is composition factor for $\mathbb{F}G$ of $\mathbb{F}B$ then e_B acts identity on M. So by 6.5.14 $\phi_M \in B$. It follows that

$$\phi_{\mathbb{F}B} = \sum_{\phi\in \mathrm{IBr}(G)} d_\phi\phi \tag{4}$$

for some $d_\phi \in \mathbb{N}$. Since $\mathbb{F}G = \sum_{B\in \mathrm{Bl}(G)} \mathbb{F}B$ we conclude

$$\phi_{\mathbb{F}G} = \sum_{B\in \mathrm{Bl}(G)} \sum_{\phi\in \mathrm{IBr}(B)} d_\phi\phi \tag{5}$$

From (3) and (5) and the linear independence of $\mathrm{IBr}(G)$ we get $d_\phi = \Phi_\phi(1)$ for all $\phi \in \mathrm{IBr}(G)$. The lemma now follows from (4) and (2). □

6.6 Brauer's Frist Main Theorem

Definition 6.6.1 [**def:defect group c**] *Let C be a conjugacy class of G.*

(a) [**z**] A defect group *of C is a Sylow p-subgroup of $C_G(x)$ for some $x \in C$.*

(b) [**a**] $\mathrm{Syl}(C)$ *is the set of all defect groups of G.*

(c) [**b**] *We fix $g_C \in C$ and $D_C \in \mathrm{Syl}_p(C_G(g_C))$.*

(d) [**d**] *Let $\mathcal{A}$ and $\mathcal{B}$ be set of subgroups of G. We write $\mathcal{A} \prec \mathcal{B}$ if for all $A \in \mathcal{A}$ there exists $B \in \mathcal{B}$ with $A \leq B$.*

(e) [**e**] *Let $\mathcal{A}$ be a set subgroups of G. Then $\mathcal{C}_{\mathcal{A}} = \{C \in \mathcal{C} \mid \mathrm{Syl}(C) \prec \mathcal{A}\}\}$ and $\mathrm{Z}_{\mathcal{A}}(\mathbb{F}G) = \mathbb{F}\langle a_C \mid C \in \mathcal{C}_{\mathcal{A}}\rangle$.*

(f) [**f**] *For $A \subseteq \mathrm{Z}(\mathbb{F}G)$ set $\mathcal{C}_A = \{C \in \mathcal{C}(G) \mid a(g_C) \neq 0$ for some $a \in A\}$.*

(g) [**g**] *For $A, B, C \in \mathcal{C}$ put $K_{ABC} = \{(a, b) \in A \times B \mid ab = g_C\}$.*

Lemma 6.6.2 [**trivial zdfg**] *Let $z \in \mathrm{Z}(\mathbb{F}G)$ and $\mathcal{D}$ a set of subgroups of G. Then $z \in \mathrm{Z}_{\mathcal{D}}(\mathbb{F}G)$ iff $a_C \in \mathrm{Z}_{\mathcal{D}}(\mathbb{F}G)$ for all $C \in \mathcal{C}_z$ and iff $\mathrm{Syl}(C) \prec \mathcal{D}$ for all $C \in \mathcal{C}_z$.*

Proof: Since $z = \sum_{C \in \mathcal{C}(G)} z(g_C)a_C$ and $(a_C \mid C \in \mathcal{C}(G))$ is linearly independent this follows immediately from the definition of $\mathrm{Z}_{\mathcal{D}}(\mathbb{F}G)$. □

Lemma 6.6.3 [**syl c prec syl a**] *Let $A, B, C \in \mathcal{C}$*

(a) [**a**] $|K_{ABC}| \equiv |\{(a, b) \in \mathcal{A} \times \mathcal{B} \mid a, b \in C_G(D_C), ab = g_C\}|$ (mod p)*.*

(b) [**b**] *If $p \nmid |K_{ABC}|$ then* $\mathrm{Syl}(C) \prec \mathrm{Syl}(A)$*.*

Proof: (a) Observe that $C_G(g_C)$ acts on K_{ABC} by coordinate wise conjugation. All non-trivial orbits of D_C on K_{ABC} have length divisble by p and so (a) holds.

(b) By (a) there exists $a \in \mathcal{A}$ with $D_C \in C_G(a)$ and so $D_C \leq D$ for some $D \in \mathrm{Syl}_p(C_G(a)$. Since G acts transitively on $\mathrm{Syl}(C)$, $\mathrm{Syl}(C) \prec \mathrm{Syl}(A)$. □

Proposition 6.6.4 [**zdfg ideal**] *Let $\mathcal{D}$ be set of subgroups of G. Then $\mathrm{Z}_{\mathcal{D}}(\mathbb{F}G)$ is an ideal in G.*

Proof: Let $A, B \in \mathcal{C}$ with $\mathrm{Syl}(A) \prec \mathcal{D}$. Then in $\mathbb{F}G$:

$$a_A a_B = \sum_{C \in \mathcal{C}} |K_{ABC}| a_C = \sum_{C \in \mathcal{C}, \phi \nmid |K_{ABC}|} |K_{ABC} a_C$$

By 6.6.3 $\mathrm{Syl}(C) \prec \mathrm{Syl}(A) \prec \mathcal{D}$ whenever $p \nmid |K_{ABC}|$. Then $a_C \in \mathrm{Z}_{\mathcal{D}}(\mathbb{F}G)$ and so $a_A a_B \in \mathrm{Z}_{\mathcal{D}}(\mathbb{F}G)$. □

Definition 6.6.5 [**def:fa**]

(a) [**a**] *$\mathfrak{G}$ be the set of sets of of subgroups of G. $\mathfrak{G}_\circ$ consist of all $\mathcal{A} \in \mathfrak{G}$ such that $A, B \in \mathcal{A}$ with $A \subseteq B$ implies $A = B$.*

(b) [**b**] *If $\mathcal{A} \in \mathfrak{G}$, then* $\max(\mathcal{A})$ *is the set maximal elements of $\mathcal{A}$ with respect to inclusion.*

(c) [**c**] *Let $\mathcal{A}, \mathcal{B} \in \mathfrak{G}$. Then $\mathcal{A} \wedge \mathcal{B} := \max(\{A \cap B \mid A \in \mathcal{A}, B \in \mathcal{B}\})$.*

(d) [**d**] *Let $\mathcal{A}, \alpha B \in \mathfrak{G}$. The $\mathcal{A} \vee \mathcal{B} = \max(\mathcal{A} \cup \mathcal{B})$.*

Lemma 6.6.6 [**basis fa**] *Let $\mathcal{A}, \mathcal{B}, \mathcal{D} \in \mathfrak{G}$.*

(a) [**a**] *$\prec$ is reflexive and transitive.*

(b) [**b**] $\mathcal{A} \prec \max \mathcal{A}$ *and* $\max \mathcal{A} \prec \mathcal{A}$*.*

(c) [**c**] $\max(A) \in \mathfrak{G}_\circ$ *and if $\mathcal{A}$ is G-invariant so is* $\max \mathcal{A}$*.*

(d) [**d**] $\mathcal{A} \prec \mathcal{B}$ *iff* $\max(\mathcal{A}) \prec \max(\mathcal{B})$*.*

(e) [**e**] *If all elements in $\mathcal{A}$ have the same size, $\mathcal{A} \in \mathfrak{G}_\circ$.*

(f) [**f**] *If $\mathcal{A}$ is conjugacy class of subgroups of G, then $\mathcal{A} \in \mathfrak{G}_\circ$.*

(g) [**g**] $\mathcal{C}_\mathcal{A} = \mathcal{C}_{\max(\mathcal{A})}$ *and* $\mathrm{Z}_\mathcal{A}(\mathbb{F}G) = \mathrm{Z}_{\max(\mathcal{A})}(\mathbb{F}G)$.

(h) [**h**] *Restricted to $\mathfrak{G}_\circ$, $\prec$ is a partial ordering.*

(i) [**i**] $(\mathcal{A} \vee \mathcal{B}) \prec \mathcal{D}$ *iff* $\mathcal{A} \prec \mathcal{D}$ *and* $\mathcal{B} \prec \mathcal{D}$.

(j) [**j**] $\mathcal{D} \prec (\mathcal{A} \wedge \mathcal{B})$ *iff* $\mathcal{D} \prec \mathcal{A}$ *and* $\mathcal{D} \prec \mathcal{B}$.

Proof:

(a) Obvious.

(b) Clearly $\max \mathcal{A} \prec \mathcal{A}$. Let $A \in \mathcal{A}$ since G is finite we can choose $B \in \mathcal{A}$ of maxial size with $A \subseteq B$. Then $B \in \max(\mathcal{A}0$ and so $\mathcal{A} \prec \max \mathcal{A}$.

(c) If $A, B \in \max(\mathcal{A})$ with $A \subseteq B$, then $A = B$ by maximalty of A.

(d) Follows from (a) and (b).

(e) is obvious.

(f) follows from (e).

(g) The first statement follows from (d) and the second from the first.

(h) Let $\mathcal{A}, \mathcal{B} \in \mathfrak{A}(G)$ with $\mathcal{A} \prec \mathcal{B}$. Let $A \in \mathcal{A}$ and choose $B \in \mathcal{B}$ with $A \leq B$. Then choose $D \in \mathcal{A}$ with $B \leq D$. Then $A \leq D$ and so $A = D$ and $A = B$. Thus $\mathcal{A} \subseteq \mathcal{B}$. By symmetry $\mathcal{B} \subseteq \mathcal{A}$. So $\mathcal{A} = \mathcal{B}$. (h) now follows from (a).

(i) By (d) $(\mathcal{A} \vee \mathcal{B}) \prec \mathcal{D}$ iff $(\mathcal{A} \cup \mathcal{B}) \prec \mathcal{D}$ and so iff $\mathcal{A} \prec \mathcal{D}$ and $\mathcal{B} \prec \mathcal{D}$.

(j) By (d) $\mathcal{D} \prec (\mathcal{A} \wedge \mathcal{B})$ iff $\mathcal{D} \prec \{A \cap B \mid A \in \mathcal{A}, B \in \mathcal{B}\}$ and so iff $\mathcal{D} \prec \mathcal{A}$ and $\mathcal{D} \prec \mathcal{B}$. □

Lemma 6.6.7 [**basic zdfg**] *Let $\mathcal{D}, \mathcal{E} \in \mathfrak{D}_\circ$.*

(a) [**a**] *If $\mathcal{D} \prec \mathcal{E}$, then $\mathcal{C}_\mathcal{D} \subseteq \mathcal{C}_\mathcal{E}$ and $\mathrm{Z}_\mathcal{D}(\mathbb{F}G) \leq \mathrm{Z}_\mathcal{E}(\mathbb{F}G)$.*

(b) [**b**] $(\mathcal{D} \wedge \mathcal{E}) \prec \mathcal{D}$.

(c) [**c**] $\mathcal{C}_\mathcal{D} \cap \mathcal{C}_\mathcal{E} = \mathcal{C}_{\mathcal{D} \wedge \mathcal{E}}$ *and* $\mathrm{Z}_\mathcal{D}(\mathbb{F}G) \cap \mathrm{Z}_\mathcal{E}(\mathbb{F}G) = \mathrm{Z}_{\mathcal{D} \wedge \mathcal{E}}(\mathbb{F}G)$

(d) [**d**] *Let $A \subseteq \mathrm{Z}(\mathbb{F}(G))$. Let $\mathfrak{G}_\circ(A) := \{\mathcal{A} \in \mathfrak{G}_\circ \mid \mathrm{Z}_\mathcal{D}(\mathbb{F}G)$. Then there exists a unique $\mathcal{E} \in \mathfrak{G}_\circ(A)$ with $\mathcal{E} \prec \mathcal{D}$ for all $\mathcal{D} \in \mathfrak{G}_\circ(A)$. We denote this $\mathcal{E}$ by* $\mathrm{Syl}(A)$.

(e) [**e**] *If $A \subseteq B \subseteq \mathrm{Z}(\mathbb{F}(G))$, then* $\mathrm{Syl}(A) \prec \mathrm{Syl}(B)$.

(f) [**f**] *For all $C \in \mathcal{C}$,* $\mathrm{Syl}(a_C) = \mathrm{Syl}(C)$

(g) [**g**] $\mathrm{Syl}(\mathrm{Z}(\mathbb{F}G)) = \mathrm{Syl}(G)$

(h) [**h**] *For all $A \subseteq \mathrm{Z}(\mathbb{F}(G))$,* $\mathrm{Syl}(A) \prec \mathrm{Syl}(G)$, *that is* $\mathrm{Syl}(A)$ *is a set of p subgroups of G.*

(i) [**i**] *Let $A, B \subseteq \mathrm{Z}(\mathbb{F}G)$. Then* $\mathrm{Syl}(A \cup B) = \mathrm{Syl}(A) \vee \mathrm{Syl}(B)$.

(j) [**j**] *Let* $A \subset \mathrm{Z}(\mathbb{F}G)$ *then* $\mathrm{Syl}(A) = \mathrm{Syl}(\{a_C \mid C \in \mathcal{A}\}) = \bigvee_{C \in \mathcal{C}_A} \mathrm{Syl}(C)$.

Proof: (a) and (b) are obvious.

(c) Let $C \in \mathcal{C}$. Then $C \in \mathcal{C}_{\mathcal{D}} \cap \mathcal{C}_{\mathcal{E}}$ iff $\mathrm{Syl}(C) \prec \mathcal{D}$ and $\mathrm{Syl}(C) \prec \mathcal{E}$. Thus by **??** iff $\mathrm{Syl}(C) \prec \mathcal{D} \wedge \mathcal{E}$ and iff $C \in \mathcal{C}_{D \wedge \mathcal{E}}$. So the first statement in (b) holds.

Since $\{a_C \mid C \in \mathcal{C}\}$ is $\mathbb{F}$-linearly independent

$$\mathrm{Z}_{\mathcal{D}}(\mathbb{F}G) \cap \mathrm{Z}_{\mathcal{E}}(\mathbb{F}G) = \mathbb{F}\{a_C \mid C \in \mathcal{C}_{\mathcal{D}} \cap \mathcal{C}_{\mathcal{E}}\}$$

So the second statement in (c) follows from the first.

(d) Put $\mathcal{E} = \bigwedge_{\mathcal{D} \in \mathfrak{G}_\circ(A)} \mathcal{D}$. By (c), $A \leq \mathrm{Z}_{\mathcal{E}}(\mathbb{F}G)$ and by (b) $\mathcal{E} \prec \mathcal{D}$ for all $\mathcal{D} \in \mathfrak{A}$. Since $\prec$ is antisymmetric on $\mathfrak{G}_\circ$, $\mathcal{E}$ is unique.

(e) Observe that $\mathrm{Syl}(B) \in \mathfrak{G}_\circ$ and so (e) follows from (d).

(f) Since $\mathrm{Syl}(C) \prec \mathrm{Syl}(C)$, $C \in \mathcal{C}_{\mathrm{Syl}C}$ and so $a_C \in \mathrm{Z}_{\mathrm{Syl}(C)}(\mathbb{F}G)$. Since $a_C \in \mathrm{Z}_{\mathrm{Syl}(a_C)}(\mathbb{F}G)$ we conclude from 6.6.2 that $C \in \mathcal{C}_{\mathrm{Syl}(a_c)}$ and so $\mathrm{Syl}(C) \prec \mathrm{Syl}(a_C)$. Since $\prec$ is anti-symmetric (f) holds.

(g) Let $S \in \mathrm{Syl}(G)$, $1 \neq x \in Z(S)$ and $C = {}^G x$. Then clearly $\mathrm{Syl}(C) = \mathrm{Syl}(G)$ and so by (e) and (f), $\mathrm{Syl}(\mathrm{Z}(\mathbb{F}G)) \prec \mathrm{Syl}(G)$. Clearly $\mathrm{Syl}(C) \prec \mathrm{Syl}(G)$ for all $C \in \mathcal{C}$. So $\mathcal{C}_{\mathrm{Syl}(G)} = \mathcal{C}$ and $\mathrm{Z}_{\mathrm{Syl}(G)}(\mathbb{F}G) = \mathrm{Z}(\mathbb{F}G)$. (d) implies $\mathrm{Syl}(\mathrm{Z}(\mathbb{F}G)) \subseteq \mathrm{Syl}(G)$ and so (g) holds.

(h) follows from (e) and (g).

(i) We have $\mathrm{Z}_{\mathrm{Syl}(A) \vee \mathrm{Syl}(B)}(\mathbb{F}G) = \mathrm{Z}_{\mathrm{Syl}(A) \cup \mathrm{Syl}(B)}(\mathbb{F}G) = \mathrm{Z}_{\mathrm{Syl}(A)}(\mathbb{F}G) + \mathrm{Z}_{\mathrm{Syl}(B)}(\mathbb{F}G)$ and so $A \cup B \subseteq \mathrm{Z}_{\mathrm{Syl}(A) \vee \mathrm{Syl}(B)}(\mathbb{F}G)$. Thus $\mathrm{Syl}(A \cup B) \prec \mathrm{Syl}(A) \vee \mathrm{Syl}(B)$. Since $A \leq Z_{\mathrm{Syl}(A \cup B)}(\mathbb{F}G,$ $\mathrm{Syl}(A) \prec \mathrm{Syl}(A \cup B)$ and by symmetry $\mathrm{Syl}(B) \prec \mathrm{Syl}(A \cup B)$. Thus $\mathrm{Syl}(A) \vee \mathrm{Syl}(B) \prec \mathrm{Syl}(A \cup B)$ and (i) holds.

(j) By 6.6.2 $\mathrm{Syl}(A) = \mathrm{Syl}(\{a_C \mid C \in \mathcal{C}_A\}$. By (i) and (f) $\mathrm{Syl}(\{a_C \mid C \in \mathcal{C}_A\} = \bigvee_{C \in \mathcal{C}_A} \mathrm{Syl}(a_C)$. □

Lemma 6.6.8 [**eb in sum k**] *Let* B *be a block and* $\mathcal{K}$ *a set of ideals in* $\mathrm{Z}(\mathbb{F}G)$ *with* $e_B \in \sum \mathcal{K}$. *Then* $Z(\mathbb{F}B) \leq K$ *for some* $K \in \mathcal{K}$.

Proof: Since $e_B = e_B^2 \in \sum_{K \in \mathcal{K}} e_B K$ there exists $K \in \mathcal{K}$ with $e_B K \not\leq \mathrm{J}(\mathrm{Z}(\mathbb{F}B))$. Since by 2.2.4 all elements in $\mathrm{Z}(\mathbb{F}B)) \setminus \mathrm{J}(\mathrm{Z}(\mathbb{F}B))$ are invertible, $\mathrm{Z}(\mathbb{F}B) = e_B K \leq K$. □

Definition 6.6.9 [**sylb**] *Let* B *be a block. Then* $\mathrm{Syl}(B) := \mathrm{Syl}(e_B)$. *The members of* $\mathrm{Syl}(B)$ *are called the* defect groups *of* B.

Proposition 6.6.10 [**sylow theorem for blocks**] *Let* B *be block of* G. *Then* G *acts transitively on* $\mathrm{Syl}(B)$.

Proof: Let $\mathfrak{D}$ be the set of orbits for G on $\mathrm{Syl}(B)$. Then clearly $\mathcal{C}_{\mathrm{Syl}(B)} = \bigcup_{\mathcal{D} \in \mathfrak{D}} C_{\mathcal{D}}$ and so

$$e_B \in \mathrm{Z}_{\mathrm{Syl}(B)}(\mathbb{F}G) = \sum_{\mathcal{D}\in\mathfrak{D}} \mathrm{Z}_{\mathcal{D}}(\mathbb{F}G)$$

So by 6.6.8 $e_B \in \mathrm{Z}_{\mathcal{D}}(\mathbb{F}G)$ for some $\mathcal{D} \in \mathfrak{D}$. Thus by 6.6.7(d) implies $\mathrm{Syl}(B) = \mathrm{Syl}(e_B) \prec \mathcal{D}$. Since $\mathcal{D} \subseteq \mathrm{Syl}(e_B)$ we get $\mathrm{Syl}(e_B) = \mathcal{D}$. □

Definition 6.6.11 [**def:defect class**] *Let B be a block and $C \in \mathcal{C}(G)$. Then C is called a* defect class *of B provided that $\lambda_B(a_C) \neq 0 \neq \epsilon_B(g_C)$.*

Lemma 6.6.12 [**existence of defect class**] *Every block has at least one defect class.*

Proof: We have $e_B = \sum_{C\in\mathcal{C}(G)} e_B(g_C)a_C$ and so

$$1 = \lambda_B(e_B) = \sum_{C\in\mathcal{C}(G)} e_B(g_C)\lambda(a_C).$$

Proposition 6.6.13 [**min-max**] *Let B be a block of G and C a conjuagacy class.*

(a) [**a**] *If $\lambda_B(a_C) \neq 0$, then* $\mathrm{Syl}(B) \prec \mathrm{Syl}(C)$.

(b) [**b**] *If $\epsilon_B(a_C) \neq 0$ then* $\mathrm{Syl}(C) \prec Syl(B)$

(c) [**c**] *If C is a defect class of B, then* $\mathrm{Syl}(C) = \mathrm{Syl}(B)$.

Proof: (a) Since $\lambda_B(a_C) \neq 0$ and $a_C \in Z_{\mathrm{Syl}(C)}(\mathbb{F}G)$ we have $Z_{\mathrm{Syl}(C)}(\mathbb{F}G) \not\leq \ker\lambda_B$. Since λ_B has codimension 1 on $\mathrm{Z}(\mathbb{F}G)$ we conclude

$$\mathrm{Z}(\mathbb{F}G) = \ker\lambda_B + \mathrm{Z}_{\mathrm{Syl}(C)}(\mathbb{F}G)$$

Since $e_B \notin \ker\lambda_B$ 6.6.8 implies $e_B \in \mathrm{Z}_{\mathrm{Syl}(C)}(\mathbb{F}G)$. Thus by 6.6.7(d), $\mathrm{Syl}(B) \prec \mathrm{Syl}(C)$.
(b) This follows from 6.6.7(j).
(c) Follows from (a) and (b). □

Lemma 6.6.14 [**ac in jzfg**] *Let $C \in \mathcal{C}(G)$ with $C \cap C_G(O_p(G)) = 1$, then $a_C \in \mathrm{J}(\mathrm{Z}(\mathbb{F}(G))$ and so $\lambda_B(a_C) = 0$ for all blocks B.*

Proof: Let $M \in \mathcal{S}_p(G)$ and let P be an orbit for $O_p(G)$ on C and $g \in P$. By assumption $|P| \neq 1$ and so $p \mid |P|$. By 6.4.16 $\rho_M(O_p(G)) = 1$ and so $\rho_M({}^q g) = \rho_M(g)$ for all $g \in O_p(G)$. Thus $\rho_M(a_P) = |P|\rho_M(g) = 0$ and so also $\rho_M(a_C) = 0$. Thus $a_C \in \mathrm{J}(\mathbb{F}(G))$. 6.3.4 completes the proof. □

Lemma 6.6.15 [**defect classes**] *All defect class of G are contained in $C_G(O_p(G))$.*

Proof: Let C be a defect class of the block B. Then $\lambda_B(a_C) \neq 0$ and so $a_C \notin \mathrm{J}(\mathrm{Z}(\mathbb{F}B))$. Thus by 6.6.14 $C \cap C_G(O_p(G)) \neq \emptyset$. Since G is transitive on C, $C \subseteq C_G(O_p(G))$. □

Proposition 6.6.16 [**opg in defect group**]

(a) [**a**] *$O_p(G)$ is contained in any defect group of any block of G.*

(b) [**b**] *If P is a defect group of some block of G and $P \trianglelefteq G$ then $P = O_p(G)$*

(a)Let B be a block, C a defect class of B. By 6.6.15 $O_p(G) \leq C_G(g_C)$ and so $O_p(G) \leq D_C$.
(b) Follows immediateley from (a) □

Definition 6.6.17 [**def:brauer map**] *Let P be a p-subgroup. Then* $\mathrm{Br}_P : \mathrm{Z}(\mathbb{F}G) \to \mathrm{Z}(\mathbb{F}C_G(P)), a \to a \mid_{C_G(P)}$ *is called the* Brauer map *of P.*

Proposition 6.6.18 [**basic brauer map**]

(a) [**a**] *Let $K \subseteq G$. Then* $\mathrm{Br}_P(a_K) = a_{K \cap C_G(P)}$.

(b) [**b**] Br_P *is an algebra homomophism.*

(c) [**c**] *If $C_G(P) \leq H \leq N_G(P)$ then* $\mathrm{Im}\,\mathrm{Br}_P \leq \mathrm{Z}(\mathbb{F}H)$ *and so we obtain algebra homomorphism*

$$\mathrm{Br}_P^H : \mathrm{Z}(\mathbb{F}G) \to \mathrm{Z}(\mathbb{F}H), a \in \mathrm{Br}_P(H)$$

Proof: (a) is obvious.

(b) Let $A, B \in \mathcal{C}(G)$. We need to show that $\mathrm{Br}_P(a_A a_B) = \mathrm{Br}_P(a_A)\mathrm{Br}_P(a_B)$. Let $g \in C_G(P)$. Then the coeficient of g in $\mathrm{Br}_P(a_A a_B)$ is the order of the set

$$\{(a,b) \in A \times B \mid ab = g\}$$

The coefficient of g in $\mathrm{Br}_P(a_A a_B)$ is the order of

$$\{(a,b) \in A \times B \mid a \in C_G(P), b \in C_G(P), ab = g\}$$

Since P centralizes g, P acts on the first set and the second set consists of the fixedpoints of P. So the size of the two sets are equal modulo p and (b) holds.

(c) Let $\alpha : \mathbb{F}G \to \mathbb{F}C_G(P)$ be the restriction map. Since $C_G(P) \trianglelefteq H$, $\alpha(hah^{-1}) = \alpha(hah^{-1})$ for all $a \in G$ and all $h \in H$. Hence the same is true for all $a \in \mathbb{F}G$, $h \in H$. Thus $\mathrm{Im}\, Br_P = \alpha(\mathrm{Z}(\mathbb{F}G)) \leq Z(\mathbb{F}H)$. □

Lemma 6.6.19 [**kernel of brauer map**] *Let P be a p-subgroup of G.*

(a) [**a**] *Let $C \in \mathcal{C}(G)$. Then $C \cap C_G(P) \neq \emptyset$ iff $P \prec \mathrm{Syl}(C)$.*

(b) [**b**]

$$\ker \mathrm{Br}_P = \mathbb{F}\langle a_C \mid C \in \mathcal{C}(G), P \not\prec \mathrm{Syl}(C)\rangle$$

Proof: (a) $C \cap C_G(P) \neq \emptyset$ iff $P \leq C_G(g)$ for some $g \in C$ and so iff $P \leq D$ for some $D \in \mathrm{Syl}(C)$, that is iff $P \prec \mathrm{Syl}(C)$.

(b) Let $z = \sum_{g\in G} z(g)g = \sum_{C\in\mathcal{C}(G)} z(g_c)a_C \in \mathrm{Z}(\mathbb{F}(G))$. Then $\mathrm{Br}_P(z) = 0$ iff $z(g) = 0$ for all $g \in P$, iff $z(g_c) = 0$ for all $C \in \mathcal{C}$ with $C \cap P \neq \emptyset$ and iff $z \in \mathbb{F}\langle a_C \mid C \cap P = \emptyset\rangle$. So (a) implies (b). □

Proposition 6.6.20 [**defect and brauer map**] *Let B be a block of G and P be a p-subgroup of G.*

(a) [**a**] $\mathrm{Br}_P(e_B) \neq 0$ *iff $P \prec \mathrm{Syl}(B)$.*

(b) [**b**] *$P \in \mathrm{Syl}(B)$ iff P is p-subgroup maximal with respect to* $\mathrm{Br}_P(e_B) \neq 0$.

Proof: (a) By 6.6.19(b), $\mathrm{Br}_P(e_P) \neq 0$ iff $e_B \notin \mathbb{F}\langle a_C \mid C \in \mathcal{C}(G), P \not\prec \mathrm{Syl}(C)\rangle$ and so iff $P \prec \mathrm{Syl}(C)$ for some $C \in \mathcal{C}(G)$ with $e_B(g_C) \neq 0$.

If $P \prec \mathrm{Syl}(B)$, then by 6.6.13(c), $P \prec \mathrm{Syl}(C)$ for amy defect class C of B. Thus $\mathrm{Br}_P(e_B) \neq 0$.

Conversely suppose $\mathrm{Br}_P(e_P) \neq 0$ and let $C \in \mathcal{C}(G)$ with $e_B(g_C) \neq 0$ and $P \prec \mathrm{Syl}(C)$. By 6.6.13(b), $\mathrm{Syl}(C) \prec Syl(B)$ and so (a) is proved.

(b) follows immediately from (a). □

Definition 6.6.21 [**def:lbg**] *Let $H \leq G$ and b a block of H.*

(a) [**a**] $\lambda_b^G : \mathrm{Z}(\mathbb{F}G) \to \mathbb{F}, a \to \lambda_b(a\mid_H)$.

(b) [**b**] *If λ_b^G is an algebra homomorphsim, the b^G is the unique block of G with $\lambda_{b^G} = \lambda_b^G$.*

Lemma 6.6.22 [**syl(b) in syl(bg)**] *Let b be a block of $H \leq G$. If b^G is defined then* $\mathrm{Syl}(b) \prec \mathrm{Syl}(b^G)$.

Proof: Let C be a defect class of B. Then $0 \neq \lambda_{b^G}(a_C) = \lambda_b^G(a_C) = \lambda_b(a_{C\cap H})$. Ot follows that there exists $c \in \mathcal{C}(H)$ with $c \subseteq C$ and $\lambda_b(a_c) \neq 0$. Hence by 6.6.13(a), $\mathrm{Syl}(b) \prec \mathrm{Syl}(c)$. Clearly $\mathrm{Syl}(c) \prec \mathrm{Syl}(C) = \mathrm{Syl}(B)$ and the lemma is proved. □

Proposition 6.6.23 [**lbg=brplb**] *Suppose that P is a p-subgroup of G and $PC_G(P) \leq H \leq N_G(P)$.*

(a) [**a**] $\lambda_b^G = \lambda_b \circ \mathrm{Br}_P$ *for all blocks b of H.*

(b) [**b**] *b^G is defined for all blocks b of H.*

(c) [**c**] *Let B be a block if G and b a block of H. Then $B = b^G$ iff $\lambda_b(\mathrm{Br}_P(e_B)) = 1$.*

(d) [**d**] *Let B be a block. Then $\mathrm{Br}_P(e_B) = \sum\{e_b \mid b \in \mathrm{Bl}(H), b^G = B\}$.*

(e) [**e**] *Let B be a block of G. Then $B = b^G$ for some block b of H iff $P \prec \mathrm{Syl}(B)$.*

Proof: (a) Let $C \in (G)$ we have to show that

$$(*) \qquad \lambda_b(a_{C\cap H}) = \lambda_b(a_{C\cap C_G(P)})$$

Since H nomrmalizes $C \cap H$ and $C \cap C_G(P)$. $C \cap H \setminus C_G(P)$ is a union of conjugacy classes of H. Let $c \in \mathcal{C}(H)$ with $c \subseteq C$ and $c \cap C_G(P)\emptyset$. Since $P \leq O_p(H)$, $C_H(O_p(H)) \leq C_G(P)$ and thus $c \cap C_H(O_p(H)) = 1$. 6.6.14 implies $a_c \in \mathrm{J}(\mathrm{Z}(\mathbb{F}H))$ and so $\lambda_b(a_c) = 0$. This implies (*) and so (a) holds.

(b) Since both Br_P and λ_b are homomorphism this follows from (a).

(c) By (b) $\lambda_b(\mathrm{Br}_B(e_B) = \lambda_{b^G}(e_B) = \delta_{B,b^G}$.

(d) Since Br_P is a homomorphism, $\mathrm{Br}_P(e_B)$ is either zero or an idempotent in $\mathrm{Z}(\mathbb{F}H)$. Hence by 6.5.16(b) (applied to H $\mathrm{Br}(e_B) = e_T$ for some (possible empty) $T \subseteq \mathrm{Bl}(H)$. Let $b \in \mathrm{Bl}(H)$. The $\lambda_b(e_T) = 1$ if $b \in T$ and 0 otherwise. So by (c), $T = \{b \in \mathrm{Bl}(G) \mid B = b^G\}$.

(e) By (d) $\mathrm{Br}_P(e_B) \neq 0$ iff ther exists $b \in \mathrm{Bl}(G)$ with $B = b^G$. Thus (e) follows from 6.6.20(a). □

Definition 6.6.24 [**def:G—P**] *Let P be a p-sugbroups of G. Then $\mathcal{C}(G|P) = \{C \in \mathcal{C}(G) \mid P \in \mathrm{Syl}(C)\}$ and $\mathrm{Bl}(G|P) = \{B \in \mathrm{Bl}(G) mid P \in \mathrm{Syl}(G)\}$.*

Proposition 6.6.25 [**defect opg**] *Let B be a block of G with defect group $O_p(G)$. Then $\mathrm{Syl}(C) = \{O_p(G)\}$ for all $C \in \mathcal{C}(G)$ with $e_B(g_C) \neq 0$ and so $e_B \in \mathbb{C}\langle a_C \mid C \in \mathcal{C}(G|O_p(G))\rangle$*

Proof: Let $C \in \mathcal{C}(G)$ with $e_B(g_C) \neq 0$. Then by 6.6.13(b), $\mathrm{Syl}(C) \prec \mathrm{Syl}(B) = \{O_p(G)\}$. On the otherhand $b = B$ is the unique block of G with $B = b^G$ and so by 6.6.23(d), $\mathrm{Br}_{O_p(G)} = e_B$. It follows that $C \leq C_G(O_p(G))$ and so $O_p(G) \prec \mathrm{Syl}(C)$. □

Lemma 6.6.26 [**first for classes**] *Let P be a p-subgroup of G. Then the map*

$$\mathcal{C}(G|P) \to \mathcal{C}(N_G(P)|P), C \to C \cap C_G(P)$$

is a well defined bijection.

Proof: Let $C \in \mathcal{C}(G|P)$. To show that out map us well defined we have to show that $C \cap C_G(P)$ is a conjugacy class for $N_G(P)$. Since $N_G(P)$ normalizes C and $C_G(P)$ it normalizes $C \cap C_G(P)$. Note that Gacst on the set $\{(x,Q) \mid x \in C, Q \in \mathrm{Syl}_p(G) = \{(x,Q) \mid x \in C, Q \in\cong GP, [x,Q] = 1\}$. Let $x \in C$. Then $C_G(x)$ acts tranistively on $Syl_p(C_G(x))$ and so by 1.1.10 $N_G(P)$ is tranistive on $C \cap C_G(P)$. So $C \cap C_G(P)$ is a conjugacy class of $N_G(P)$.

Since distinct conjugacy clases are disjoint, our map is injective. Let $L \in \mathcal{C}(N_G(P)|P)$ and let C be the unique conjugacy class of G containing L. Let $x \in L$. Since $P \in \mathrm{Syl}(L)$ and $P \trianglelefteq N_G(P)$, $\mathrm{Syl}(L) = \{P\}$ and so $P \in \mathrm{Syl}_p(N_G(P) \cap C_G(x))$. Let $P \leq Q \in \mathrm{Syl}_p(C_G(x))$. Then $PleqN_Q(P) \in N_G(P) \cap C_G(x)$ and so $P = N_Q(P)$. 1.4.5(c) implies $P = Q$ and so $P \in \mathrm{Syl}(C)$ and $C \in \mathcal{C}(G \mid P)$. Since $C \cap C_G(P)$ is a conjugacy class of $N_G(P)$, $C \cap C_G(P) = L$ and so our map is onto. □

Theorem 6.6.27 (Brauer's First Main Theorem) [**first**] *Let P be a p-subgroup of G.*

(a) [**a**] *The map $\mathrm{Bl}(N_G(P)|P) \to \mathrm{Bl}(G|P), b \to b^G$ is well defined bijection.*

(b) [**b**] *Let $B \in \mathrm{Bl}(G|P)$ and $b = \mathrm{Bl}(N_G(P)|P)$, then $B = b^G$ iff $\mathrm{Br}_P(e_B) = e_b$.*

Proof: Let b be a block of $N_G(P)$ with defect group P. Since $P \trianglelefteq N_G(P)$, $\mathrm{Syl}(b) = \{P\}$. By 6.6.23 b^G is defined and $\lambda_{b^G} = \lambda_b^G = \lambda_b \circ \mathrm{Br}_P$.To show that our map is well defiend we need to show P is a defect group of b^G. Let L be a defect class of b. Then by 6.6.13(c), $\mathrm{Syl}(L) = \mathrm{Syl}(b) = \{P\}$ and thus $L \in \mathcal{C}(N_G(P)|P)$. Let C be the unique conjugacy class of G containin L. By 6.6.26 $P \in \mathrm{Syl}(C)$ and $C \cap C_G(P) = L$. Hence

$$\lambda(b^G)(a_C) = \lambda_{(}\mathrm{Br}_P(a_C)) = \lambda_b(a_{C \cap C_G(P)}) = \lambda_b(a_L) \neq 0$$

Thus by 6.6.13(a), $\mathrm{Syl}(b^G) \prec \mathrm{Syl}(C)$ and so P contains a defect group of $\mathrm{Syl}(b^G)$. By 6.6.22, $\{P\} = \mathrm{Syl}(b) \prec \mathrm{Syl}(b^G)$. Thus P is contained in a defect group of b^G. Hence P is a defect group of b^G.

To show that $b \to b^G$ is onto let $B \in Bl(G|P)$. Let T be the set of blocks of $N_G(P)$ with $B = b^G$. Then by By 6.6.23(d), $e_B = e_T$ and by 6.6.23(e), $T \neq 0$. Let $b \in T$. Since $P \leq O_p(N_G(P))$, 6.6.16 implies that P is contained in any defect group of b. By 6.6.22 any defect groups of b is contained in a defect group of $B = b^G$. Thus P is a defect group of b.

Finally assume that $b^G = d^G$ for some $b, d \in \mathrm{Bl}(N_G(P)|P)$. Then $\lambda_b \circ \mathrm{Br}_P = \lambda_{b^G} = \lambda_d \circ \mathrm{Br}_P$. Thus $\lambda_b(a_{C \cap C_G(P)}) = \lambda_d(a_{C \cap C_G(P)}$ for all $C \in \mathcal{C}(G)$. Hence by 6.6.26, $\lambda_b(a_L) = \lambda_d(a_L)$ for all $L \in \mathcal{C}(N_G(P) \mid P)$. Observe that by 6.6.16(b), $P = O_p(N_G(P))$ and so by 6.6.25 e_b is a $\mathbb{C}$-linear combination of the $a_L, L \in \mathcal{C}(N_G(P)|P$. Thus

$$1 = \lambda_b(e_b) = \lambda_d(e_b) = \delta_{bd}$$

and $b = d$. So our map is 1-1. □

Corollary 6.6.28 [**p=opng**] *Let P be the defect group of some block of G. Then $P = O_p(N_G(P))$.*

Proof: By 6.6.27 P is a defect group of some block of $N_G(P)$. So by 6.6.16(b), $P = O_p(N_G(P))$. □

6.7 Brauer's Second Main Theorem

Lemma 6.7.1 [**x invertible in zag**] *Let B be block of G and $x \in \mathrm{Z}(\mathbb{A}_I G)$ with $\lambda_B(x^*) = 1$. Then there exists $y \in f_B \mathrm{Z}(\mathbb{A}_I G)$ with $yx = f_B$.*

Proof: Since $\lambda_B((f_B x)^*) = \lambda_B(e_B)\lambda_B(x) = 1$ we may replace x by $f_B x$ and assume that $x \in f_B \mathrm{Z}(\mathbb{A}_I G))$. Then $f_B x = x$, $e_B x^* = x^*$ and $x^* \in \mathbb{F}B$. Since $\lambda_B(x^*) = 1\lambda_B(e_B)$ and $\ker \lambda_B \cap \mathrm{Z}(\mathbb{F}B) = \mathrm{J}(\mathrm{Z}(\mathbb{F}B))$ we conclude for 6.7.1 that x^* is invertible in $\mathrm{Z}(\mathbb{F}B)) = e_B \mathrm{Z}(\mathbb{F}G) = (f_B \mathrm{Z}(\mathbb{A}_I G))^*$. So there exists $u \in f_B \mathrm{Z}(\mathbb{A}_I G))$ with $(ux)^* = e_B$. Observe that $\ker(^*\colon \mathbb{A}_I H \to \mathbb{F}G) = I_I G = \mathrm{J}(A_I) \cdot \mathbb{A}_I G$ and $ux \in f_B \cdot \mathbb{A}_I G \cdot f_B$. Thus 6.3.5 shows that there exists a unique $v \in f_B \cdot \mathbb{A}_I G \cdot f_B$ with $vux = f_B$. Let $g \in G$. Then $t \cong gv \cdot ux = {}^g(vux) = {}^g f_B = f_B$ and so by uniqueness of v, ${}^g v = v$ and $v \in \mathrm{Z}(\mathbb{A}_I G)$. So the lemma holds with $y = vu$. □

Lemma 6.7.2 [**fb on fbprime**] *Let $H \leq G$, b a block of H. Suppose that b^G is define and put $B = b^G$. Then there exists $w \in \mathbb{A}_I(G \setminus H)$ such that*

(a) [**a**] $f_b f_{B'} = w f_{B'}$.

(b) [**b**] $f_b w = w = w f_b$.

(c) [**c**] *H centralizes.*

Proof: Let $x = f_B \mid_H$ and $z = f_B \mid_{H \setminus H}$. Then $f_B = a + c$. By defintion of $B = B^G$, $\lambda_B = \lambda_b^G$ and so

$$1 = \lambda_B(e_B) = \lambda_n(e_B \mid H) = \lambda_B((f_B \mid_H)^*) = \lambda_B(x^*).$$

Hence by 6.7.1 applied to H in place of G there exists $y \in f_B \mathrm{Z}(\mathbb{A}_I H)$ with $yx = f_B$. Put $w = -yz$ and note that H centralizes w. Since $H \cdot (G \setminus H) \subseteq G \setminus H$, $w \in \mathbb{A}_I(G \setminus H)$. Since $f_b y = f_b$ also $f_b w = w$. It remains to prove (a).

$$y f_B = y(x + z) = yx + yz = f_B - w$$

Hence

$$(f_b - w) f_{B'} = y f_B f_{B'} = 0$$

This (a) holds.

Lemma 6.7.3 [**p partition**]

(a) [**a**] *Let $\langle h\rangle$ be a finite cyclic group acting on a set Ω. Suppose h_p acts fixed-point freely on Ω. Then there exists there exists an $< h >$-invariant partion of $(\Omega_i)_{i\in\mathbb{F}_p}$ of Ω with $h\Omega_i = \Omega_{i+1}$.*

(b) [**b**] *If $h \leq H \leq G$ with $C_H(h_p) \leq H$, S a ring and $w \in S[G \setminus H]$. If h centralizes w, then there exists $w_i \in S[G \setminus H], i \in F_p$ with $hw_ih^{-1} = w_{i+1}$ and $\sum_{i\in\mathbb{F}_p} w_i = w$.*

(a) Put $H = \langle h\rangle$ act transitively on Ω. Let Ω_0 be an orbit for H^p on Ω. Suppose that $\Omega_0 = \Omega$. Then by the Frattinargument, $H = H^pC_H(\omega)$ and so $H/C_H(\omega)$ is a p' group. Thus $h_p \in C_H(\omega)$ contrary to the assumptions. Thus $\Omega_0 \neq \Omega$ Since $H^p \trianglelefteq H$, $H/H^p \cong C_p$ acts tranistively on the set of orbits of H^p on Ω. So (a) holds with $\Omega_i = h^i\Omega_0$, for $i \in \mathbb{F}_p$.

(b) Since $C_G(h_p) \leq H$, h_p acts fixed-point freely on $G \setminus H$ via conjuagtion. Let Ω_i be as in (a) with $\Omega = G \setminus H$ and put $w_i = w \mid_{\Omega_i}$. Then clearly $w = \sum_{i\in\mathbb{F}_p} w_i$. Now

$$ {}^hw_i = {}^h(w \mid \Omega_i) = {}^hw \mid_{{}^h\Omega_i} = w \mid_{\Omega_{i+1}} = w_{i+1} $$

and (b) is proved.

Lemma 6.7.4 [**eigenvector for h**] *Let $H \leq G$ and b a block for G. Suppose that $B = b^G$ us defined and that $h \in H$ with $C_G(h_p) \in H$.*

(a) [**a**] *Let $\omega \in \mathbb{C}$ with $\omega^p = 1$. If $f_{B'}f_b \neq 0$, then the exists a unit t in the ring $f_{B'}f_b \cdot \mathbb{A}_IG \cdot f_{B'}f_b$ with ${}^ht = \omega t$.*

(b) [**b**] *If $\chi \in \mathrm{Irr}(G)$ with $\chi \notin B$. Then $\chi(hf_b) = 0$.*

Proof: (a) Let w be a as in 6.7.2. By 6.7.3(b) theer exists $w_i \in \mathbb{A}_IG$ with $w = s\sum_{i\in\mathbb{F}_p} w_i$ and ${}^hw_i = w_{i+1}$. By 6.7.2(b), $w = f_bwf_b$ and so replacing w_i by $f_bw_if_b$ we may assume that $w_i \in f_b \cdot \mathbb{A}_IG \cdot f_b$. Put $s = \sum_{i\in\mathbb{F}_p} \omega^iw_i$. Then clearly ${}^hs = \omega s$ and $s \in f_b \cdot \mathbb{A}_IG \cdot f_b$. Put $t = f_{B'}s$. $f_{B'} \in \mathrm{Z}(\mathbb{A}_IG)$ is a central idempotent, $t \in f_{B'}f_b \cdot \mathbb{A}_IG \cdot f_{B'}f_b$ and ${}^ht = \omega t$. To complete the proof of (a) we need to show that t is unit in the ring $f_{B'}f_b \cdot \mathbb{A}_IG \cdot f_{B'}f_b$.

Since $\mathbb{F}$ has no element of multiplicative order p, $\omega^* = 1$ and so $s^* = \sum_{i\in\mathbb{F}_p} w_i^* = w^*$ and so by 6.7.2(a),

$$ f_{B'}f_b)^* = (f_{B'}w)^* = (f_{B'}s)^* = t^* $$

So 6.3.5 applied with the idempotent $f = f_{B'}f_b$ yields that t is a unit in $f_{B'}f_b \cdot \mathbb{A}_IG \cdot f_{B'}f_b$.

(b) Let $M \in \mathcal{S}(G)$ with $\chi = \chi_M$. Put $V = f_bM$. Observe that V that $\mathbb{C}H$ submodule of M. Moreover, $M = \mathbb{A}_M(f_b) \oplus V$ and f_b acts as id_V on V. Thus $\chi_M(hf_b) = \chi_V(f_b)$. Since $\chi \notin B$, $f_BM = 0$ and so $f_{B'}$ act as identity on M and on V. So also $f_{\mathrm{B}'}f_b$ acts as indentity on V. The $V = f_{B'}f_bM$ is a module for the ring $f_{B'}f_b \cdot \mathbb{A}_IG \cdot f_{B'}f_b$

If $V = 0$ clearly (b) holds. So suppose $V \neq 0$ and so also $f_{B'}f_b \neq 0$.

For L be the set of eigenvalues for h on V and for $l \in L$ let V_l be the corresponding eigenspace. Then $V = \bigoplus_{l \in L} V_l$. Let ω be a primitive p-root of unity in U and choose t as in (a). Then t is invertible on V. Moreover, if $l \in L$ and $v \in V_l$, then $htv = hth^{-1}hv = \omega tlv = (\omega l)tv$. Thus $tV_l \leq V_{tl}$. In particular $t^pV_l = V_{t^pL} = V_l$ and since t^p is invertible, $t^pV_l = V_l$ and so also $tV_l = V_{tl}$. T Inparticular $< \omega\rangle$ acts an L be left multiplication and $\dim V_l = \dim V_{\omega l}$. Let L_0 be a set of representatoves for the orbits of $\langle \omega \rangle$ in L. Then

$$\begin{array}{rcccc} \chi_V(h) & = & \sum_{l \in L} \chi_{V_l}(h) & = & \sum_{l \in L} l \dim_{V_l} \\ = \sum_{l \in L_0} \sum_{i=0}^{p-1} \omega^i l \dim V_{\omega^i l} & = & \sum_{l \in L_0} \left(\sum_{i=0}^{p-1} \omega^i \right) l \dim V_l & = & 0 \end{array}$$

□

Definition 6.7.5 [**def:p-section**] *Let $x \in G$ be a p-element. Then $\mathrm{S}_G(x) = \mathrm{S}(x) = \{y \in G \mid y_p \in {}^Gx\}$ is called the* p-section *if x in G.*

Lemma 6.7.6 [**basic p-section**] *Let $x \in G$ be a p-elemenent and Y a set of representatives for the p'-conjugact classes in $C_G(x)$. Then $\{xy \mid y \in Y\}$ is a set of representaives for the conjugacy classes of G in $\mathrm{S}(x)$.*

Proof: Any $s \in \mathrm{S}(x)$ is uniquely determined by the pair $(s_p, s_{p'})$. So the lemma follows from 1.1.10 □

Definition 6.7.7 [**def:bx**] *Let $x \in G$ be a p-element and B a block p-block and $\theta \in \mathbb{C}G)$.*

(a) [**a**] *Let T a block or a set of blocks. Then $\theta_T : G \to \mathbb{C} \mid g \to \theta(f_T g)$.*

(b) [**b**] $\theta^x : G \to \mathbb{C},\ x \to \theta(xh)$.

(c) [**c**] $B^x = \{b \in \mathrm{Bl}(C_G(x))\} \mid b^G = B\}$.

Lemma 6.7.8 [**fchi selfadjoint**] *Let $T \subseteq \mathrm{Irr}(G)$. Then*

(a) [**a**] $f_{T^\circ} = \overline{f}_T$

(b) [**b**] $(af_T \mid b) = (a \mid bf_T)$ *for all* $a, b \in \mathbb{C}G$.

Proof: By linearity we may assume $T = \{\chi\}$ for some $\chi \in \mathrm{Irr}(G)$.

(a) Since $\chi^\circ = \bar{c}hi$ and $f_\chi = \frac{\chi(1)}{|G|}\overline{\chi}$ we have $f_{\chi^\circ} = \overline{f}_\chi$.

(b) By (a) $\overline{f}_\chi^\circ = f_\chi$ and 3.4.2(c) implies $(af_\chi \mid b) = (a \mid bf_\chi)$.

Lemma 6.7.9 [**dual of a block**] *Let B be a block.*

(a) [**a**] $\overline{B} = \{\psi \mid \psi \in B\}$ *is a block.*

(b) [**b**] $\lambda_{\overline{B}}(a) = \lambda_B(a^\circ)$.

(c) [**c**] $f_{\overline{B}} = \overline{f}_B = f^\circ_B$.

(d) [**d**] $e_{\overline{B}} = e^\circ_B$.

Proof: (a) and (b): Let $\psi \in B$ and M the correspoding module. Then $\overline{\psi}$ corresponse to M^*. By the definition of the action of a group ring on the dual $\rho_{M^*}(a) = \rho_M(a^\circ)^{\mathrm{dual}}$. It follows that $\lambda_{\overline{\psi}}(a) = \lambda_\psi(a^\circ)$. Thus $\lambda_\alpha = \lambda_\beta$ iff $\lambda_{\overline{\alpha}} = \lambda_{\overline{b}}$ and so (a) and (b) hold.

(c): Clearly $f_{\overline{B}} = \overline{f}_B$. By 6.7.8, $\overline{f}_B = f^\circ_T$ and so (c) holds.

(d): Apply * to (c). □

Lemma 6.7.10 [**theta b**] *Let T be a block or or a set of blocks and $\theta \in \mathbb{C}G$. Then $\theta_B = \theta f_{\overline{B}}$.*

Proof: Let $b \in G$. Then by 6.7.8

$$\theta_T(b) = \theta(f_B b) = |G|(\theta \mid \overline{f_T b}) = |G|(\theta \overline{f_T} \mid \overline{b}) = (\theta f_{\overline{B}})(b).$$

□

Lemma 6.7.11 [**theta fb**] *Let B be a block.*

(a) [**a**] $\mathrm{Irr}(B)$ *is a basis for* $\mathbb{C}\overline{B} := \mathbb{C}G f_B$.

(b) [**b**] *Both* $\mathrm{IBr}(G)$ *and* $(\Phi_\phi \mid \phi \in \mathrm{IBr}(G)$ *are a basis for* $\mathbb{C}\tilde{\overline{B}}$, *where* $\mathbb{C}\tilde{B} := \mathbb{C}\tilde{G} \cap \mathbb{C}B$.

(c) [**c**] *If* $\chi \in \mathrm{Irr}(B)$, *then* $\tilde{\chi} \in \mathbb{F}\overline{B}$.

(d) [**d**] *For all* $\theta \in \mathrm{Z}(\mathbb{C}G)$, $\widetilde{\theta f_B} = \tilde{\theta} f_B$ *and* $\tilde{\theta_B} = \tilde{\theta}_B$.

(e) [**e**] *Let* $\theta \in \mathrm{Z}(\mathbb{C}G)$ *and* B *a block of* G. *Then* $\theta f_B = \sum_{\chi \in \mathrm{Irr}(\overline{B})} (\theta \mid \chi)\chi$.

Proof: (a): Let $\chi \in \mathrm{Irr}(B)$. Then $\chi = \frac{|G|}{\phi(1)} f_{\overline{\chi}} \in \mathbb{C}G\overline{B}$ and so (a) holds.

(b) Let $\phi \in \mathrm{IBr}(B)$. Then by (a)

$$\Phi_\psi = \sum_{\chi \in \mathrm{Irr}(B)} d_{\phi\chi}\chi \in \mathbb{C}\overline{B}$$

and so $(\Phi_\phi \mid \phi \in \mathrm{IBr}(G)$ is a basis for $\mathbb{C}\tilde{\overline{B}}$. Moreover,

$$\phi = \sum_{\psi \in \mathrm{IBr}(B)} (\phi \mid \psi)\Phi_\psi \in \mathbb{C}\overline{B}$$

and so (b) holds.

(c) $\tilde{\chi} = \sum_{\phi \in \mathrm{IBr}(B)} d_{\phi\chi}\phi$. So (c) follows from (b).

(d) By linearity we may assume that $\theta \in \mathrm{Irr}(G)$. If $\theta \in \overline{B}$ then by (b) and (c)

$$\tilde{\theta} f_B = \tilde{\theta} = \widetilde{\theta f_B}$$

and if $\theta \notin \overline{B}$, then

$$\tilde{\theta} f_B = 0 = \tilde{0} = \widetilde{\theta f_B}$$

So the first statement holds. The second now follows from 6.7.10

(e) follows from $\theta = \sum_{\chi \in \mathrm{Irr}(G)} (\theta \mid \chi)$ and (a). □

Lemma 6.7.12 [**decomposing theta x**] *Let $x \in G$ be a p-element, B a block of G.*

(a) [**a**] *If $\chi \in \mathrm{Irr}(B)$, then $\widetilde{\chi^x} = \widetilde{\chi^x}_{B^x}$.*

(b) [**b**] *Let $\theta \in \mathrm{Z}(\mathbb{C}G)$, then $((\tilde{\theta_B})^x) = (\tilde{\theta^x})_{B^x}$.*

Proof: (a) Let $b \in \mathrm{Bl}(C_G(x)) \setminus B^x$ and $y \in \widetilde{C_G(x))}$. Then

$$\widetilde{\chi^x}_b(y) = \widetilde{\chi^x}(f_b y) \overset{6.7.11(d)}{=} \chi^x(f_b y) = \chi(f_b x y) \overset{6.7.4(b)}{=} 0$$

Thus $\widetilde{\chi^x}_b = 0$ and so $\widetilde{\chi^x} = \sum_{b \in \mathrm{IBr}(C_G(x))} \widetilde{\chi^x}_b = \sum_{b \in \mathrm{IBr}(B^x)} \widetilde{\chi^x}_b = \widetilde{\chi^x}_{B^x}$.

(b) By linearity we may assume $\theta \in Irr(G)$ and say $\theta \in A \in \mathrm{Bl}(G)$. So (b) follows from (a). □

□

Theorem 6.7.13 [**my second**] *Let $\mathcal{X}$ a set of representatives for the p-element classes. Define*

$$\mu : \mathrm{Z}(\mathbb{C}G) \to \bigoplus_{x \in X} \mathrm{Z}\mathbb{C}\widetilde{C_G(x)}, \theta \to (\tilde{\theta}^x)_x$$

and

$$\nu : \bigoplus_{x \in X} \mathrm{Z}\mathbb{C}\widetilde{C_G(x)} \to \mathrm{Z}(\mathbb{C}G), (\tau_x)_x \to \theta$$

where $\theta(g) = \tau_x(y)$ for $x \in \mathcal{X}$ and $y \in \widetilde{C_G(x)}$ with $xy \in {}^G x$.

(a) [**a**] *μ and ν are inverse to each other and so both are $\mathbb{C}$-isomorphism*

(b) [**b**] *$\mu(\mathrm{Z}\mathbb{C}\widetilde{C_G(x)}) = \mathrm{Z}\mathbb{C}\,\mathrm{S}(x)$.*

(c) [**c**] *μ and ν are isometries.*

(d) [**d**] *$\mathrm{Z}(\mathbb{C}G) = \bigoplus_{x \in \mathcal{X}} \mathrm{Z}\mathbb{C}\,\mathrm{S}(x)$.*

(e) [**e**] *For each block B of G,* $\Xi(\mathrm{Z}(\mathbb{C}B)) = \bigoplus_{x\in X}\mathrm{Z}\mathbb{C}\widetilde{B^x}$

(f) [**f**] $\mathrm{Z}(\mathbb{C}B) = \bigoplus_{x\in\mathcal{X}}\nu(\mathrm{Z}\mathbb{C}\widetilde{B^x}))$

Proof: Observe that by 6.7.6 ν is well defined. Also we view $\mathrm{Z}\mathbb{C}\widetilde{C_G(x)}$ has subring of $\bigoplus_{x\in X}\mathrm{Z}\mathbb{C}\widetilde{C_G(x)}$.

(a) and (b) are obvious.

(c) Let $r, x \in \mathcal{X}$, $s \in \widetilde{C_G(r)}$ and $y \in \widetilde{C_G(x)}$. Let $C \neq D \in \mathcal{C}(G)$, $E \in (C_G(x)$ and $F \in C_G(r)$ with $rs \in C, xy \in D$, $s \in E$ and $y \in F$. Then $\mu(a_C) = a_E$ and $\mu(a_D) = F$. Since $C \neq D$ either $x \neq y$ or $E \neq F$ and in both cases $a_E \perp a_F$ in $\bigoplus_{x\in X}\mathrm{Z}\mathbb{C}\widetilde{C_G(x)}$. Note that also $a_C \perp a_D$ in $\mathrm{Z}(\mathbb{C}G)$. Moreover

$$(a_D \mid a_D)_G = \frac{|D|}{|G|} = \frac{1}{|C_G(xy)|} = \frac{1}{|C_{C_x}(y)|} = \frac{|F|}{|C_G(x)|} = (a_F \mid a_F)_{C_G(x)}$$

and so (c) holds.

(d) Follows since G is the disjoint union of the $opS(x), x \in \mathcal{X}$. Alternaively it folloes from (a) -(c).

(e) Follows from 6.7.12.

(f) follows from (e) and and (c). □

Lemma 6.7.14 [**x decomposition**] *Let $x \in G$. Define the complex* $\mathrm{IBr}(C_G(x)) \times \mathrm{Irr}(G)$-*matrix $D^x = (d^x_{\phi\chi})$ by*

$$\tilde{\chi^x} = \sum_{\phi\in\mathrm{Irr}(\mathcal{G})} \delta^x_{\phi\chi}\phi$$

any $\chi \in \mathrm{Irr}(G)$ Then

$$d^x_{\phi\chi} = \sum_{\psi\in\mathrm{Irr}(C_G(x))} (\chi\,|_H|\,\psi)_H \frac{\psi(x)}{\psi(1)}\phi(y)$$

Proof:

Let $\chi = \chi_M$ with $M \in \mathcal{S}(G)$ an d$y \in \widetilde{C_G(x)}$. Then as an $C_G(x)$-module, $M \cong \sum_{N\in\mathcal{S}(H)} N^{d_N}$ for some $d_N \in \mathbb{N}$. Since $x \in Z(C_G(x))$, x acts as a scalar λ^x_N on N. Then $\chi_N(f_{\mathcal{B}}xy) = \lambda^x_N\chi_N(f_{\mathcal{B}}y)$. Moreover $f_{\mathcal{B}}$ annhilates N if $N \notin \mathcal{S}(\mathcal{B})$ and acts as identiity on N if $N \in \mathcal{S}(\mathcal{B})$. Hence

$$(*) \qquad \chi(f_{\mathcal{B}}xy) = \sum_{N\in\mathcal{S}(C_g(x))} d_N\lambda^x_N\chi_N(f_{\mathcal{B}}y) = \sum_{N\in\mathcal{S}(\mathcal{B})} \chi_N(y)$$

Observe that $\delta_N = (\chi \mid H \mid \chi_N)$, $\lambda^x_N = \frac{\chi_N(x)}{\chi_N(1)}$ and $\tilde{\chi}_N = \sum_{\phi\in\mathrm{IBr}(C_G(x))} d_{\phi\chi_N}\phi_N$. Substitution into (*) gives the lemma. □

Theorem 6.7.15 (Brauer's Second Main Theorem) [**second**] *Let x be a p-element in G and $b \in \mathrm{Bl}(C_G(x))$. If $\chi \in \mathrm{Irr}(G)$ but $\chi \notin \mathrm{Irr}(b^G)$, then $d^x_{\phi\chi} = 0$ for all $\phi \in \mathrm{IBr}(G)$.*

Proof: Follows from 6.7.12(a).

Corollary 6.7.16 [**chixy**] *Let x be a p-element in G, $y \in C_G(x)$ a p'-element, B a block of B and $\chi \in \mathrm{Irr}(B)$. Then*

$$\chi(xy) = \sum\{d^x_{\phi\chi} \mid b \in \mathrm{Bl}(C_G(x)), B = b^G\}$$

Proof: This just rephrases 6.7.12(a).

Corollary 6.7.17 [**gp in defect group**] *Let B be a block of G, $\chi \in \mathrm{Irr}(B)$ and $g \in G$. If $\chi(g) \neq 0$ then g_p is contained in a defect group of B,*

Proof: Let $x = g_p, y = g_{p'}$. Since $\chi(g) = \chi(xy) \neq 0$, 6.7.16 implies tat there exists $b \in IBr(G)$ with $B = b^G$. Since $x \in O_p(C_G(x)$ is contained in any defect group of b, 6.6.22 implies that x is contained a defect group of B. □

Bibliography

[Co] M.J. Collins, *Representations and characters of finite groups*, Cambridge studies in advanced mathematics **22**, Cambridge University Press, New York (1990)

[Go] D.M. Goldschmidt, *Group Characters, Symmetric Functions and the Hecke Algebra*, University Lectures Series Volume **4**, American Mathematical Society, Providence (1993)

[Gr] L.C. Grove, *Algebra*, Academic Press, New York (1983)

[Is] I.M. Isaacs, *Character Theory Of Finite Groups*, Dover Publications, New York (1994)

[Ja] G.D. James *The Reprentation Theory of the Symmetric Groups* Lecture Notes in Mathematics **682**, Springer, New York (1978).

[La] S.Lang *Algebra* ....

[Na] G. Navarro *Characters and Blocks of Finite Groups* London Mathematical Society Lecture Notes Series **250** Cambridge University Press, Cambridge (1998)

[Sa] B.E. Sagan *The Symmetric Group Representations,Combinatorial Algorithms and Symmetric Functions* 2nd Edition, Graduate Text in Mathematics **203** Springer, New York, 2000

Index

$A_S(N)$, 17
$J(R)$, 20
$J_M(R)$, 20
End(M), 5

closed, 18
cylic, 18

direct summand, 11

faithful, 18
finitely generated, 18

group ring, 8

indecomposable, 11
internal direct sum, 10
isomorphic, 5, 15

Jacobson radical, 20

linear, 5
linear independent, 10

module, 5, 7
module structure, 5, 7

represention, 7

semisimple, 11
simple, 10
space, 6

vector space, 6