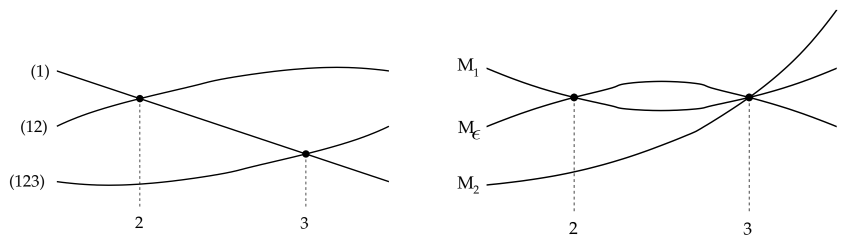
The representation ring and the center of the group ring

Brakenhoff, J.F.

The representation ring and the center of the group ring



Master's thesis
Jos Brakenhoff

supervisor
Bart de Smit

Mathematisch instituut
Universiteit Leiden

February 28, 2005

Contents

Chapter 1

Introduction

Let G be a finite group of order g. For this group we will construct two commutative rings, which we will compare in this thesis. One of these rings, the representation ring, is built up from the representations of G. A representation of the group G is a finite dimensional $\mathbb{C}$-vector space M together with a linear action of G, that is a homomorphism $G \to \mathrm{GL}(M)$. With this action M becomes a $\mathbb{C}[G]$-module.

For each representation M of G and an element $\sigma \in G$ we look at the trace of the map $M \to M : m \mapsto \sigma m$, which we will denote by $\mathrm{Tr}_M(\sigma)$ If σ and τ are conjugate elements of G, then $\mathrm{Tr}_M(\sigma) = \mathrm{Tr}_M(\tau)$. Let $G/{\sim}$ be the set of conjugacy classes of G. We obtain a map

$$\begin{array}{rcl} \chi_M : G/{\sim} & \to & \mathbb{C} \\ x & \mapsto & \mathrm{Tr}_M(\sigma), \end{array}$$

with $\sigma \in x$. This map is called the character of M. So we have a map

$$\begin{array}{rcl} \{\text{representations of } G\} & \to & \mathbb{C}^{G/\sim} \\ M & \mapsto & \chi_M. \end{array}$$

The representation ring $R(G)$ is the subring of $\mathbb{C}^{G/\sim}$ generated by χ_M for all representations M. Two representations are isomorphic if they have the same image in $\mathbb{C}^{G/\sim}$. We have two identities one for addition: $\chi_M + \chi_N = \chi_{M\oplus N}$ and the other for multiplication: $\chi_M \cdot \chi_N = \chi_{M\otimes N}$.

We can write every $\mathbb{C}[G]$-module in a unique way as a direct sum of simple modules, that is, non-zero modules without proper submodules. The representation ring is a free $\mathbb{Z}$-module, with a basis $\mathcal{S}$ consisting of the isomorphism classes of the simple modules, we have

$$R(G) \cong \bigoplus_{S\in\mathcal{S}} \mathbb{Z} \cdot \chi_S.$$

The number of simple modules is $\#(G/{\sim})$, so $R(G) \otimes \mathbb{C}$ is isomorphic to $\mathbb{C}^{G/\sim}$.

The other ring is the center of the group ring $\mathbb{Z}[G]$, which we will call $\Lambda(G)$. This ring is free with basis $\left\{\sum_{\sigma\in x} \sigma : x \in G/{\sim}\right\}$. For this ring we have an embedding into $\mathbb{C}^{\mathcal{S}}$:

$$\begin{array}{rcl} \Lambda(G) & \to & \mathbb{C}^{\mathcal{S}} \\ \displaystyle\sum_{\sigma\in x} \sigma & \mapsto & \displaystyle\left(\frac{\#x}{\dim_{\mathbb{C}} S}\chi_S(x)\right)_{S\in\mathcal{S}}, \end{array}$$

where $\left(\frac{\#x}{\dim_{\mathbb{C}} S}\chi_S(\sigma)\right)$ is the scalar with which $\sum_{\sigma\in x} \sigma$ acts on S.

For an abelian group G these two rings are isomorphic. The ring $\Lambda(G)$ is equal to $\mathbb{Z}[G]$ and the representation ring can be identified with $\mathbb{Z}[\hat{G}]$, where $\hat{G}$ is $\mathrm{Hom}(G, \mathbb{C}^*)$, the dual of G. For other groups they are not always isomorphic, but they have some similarities, for example, they are both a free $\mathbb{Z}$-module of rank $n = \#(G/\sim)$. In this thesis we will compare these two rings on several aspects. We will compare their discriminants, their spectra and the $\mathbb{Q}$-algebra they generate.

In the second chapter we compare the discriminants of these rings. The only primes which divide the discriminant of $R(G)$ are the primes which divide the order of G. The same is true for the discriminant of $\Lambda(G)$. For groups of order less than 512 the quotient $\frac{\Delta(\Lambda(G))}{\Delta(R(G))}$ is in $\mathbb{Z}$. We ask whether this is true for all groups. and shall prove this for groups of order p^k and pq, where p and q are primes and $k \leq 4$.

In the third chapter we will give a description of the spectra of $R(G)$ and $\Lambda(G)$ over A, the subring of $\mathbb{C}$ generated by the g-roots of unity. Since all characters have images in A, the spectra of $R(G) \otimes A$ and $\Lambda(G) \otimes A$ are easier to compute than the spectra of $R(G)$ and $\Lambda(G)$. We will get surjective maps $\mathrm{Spec}(A^n) \to \mathrm{Spec}(R(G) \otimes A) \to \mathrm{Spec}(A)$ and $\mathrm{Spec}(A^n) \to \mathrm{Spec}(\Lambda(G) \otimes A) \to \mathrm{Spec}(A)$, such that for all primes $\mathfrak{p}$ of A not dividing $\#G$ there are n points of $\mathrm{Spec}(R(G) \otimes A)$ respectively $\mathrm{Spec}(\Lambda(G) \otimes A)$ which map to $\mathfrak{p}$. For $R(G) \otimes A$ we will calculate the spectrum and show that it is connected. For $\Lambda(G) \otimes A$ we will give a description of a spectrum between $\mathrm{Spec}(A^n)$ and $\mathrm{Spec}(\Lambda(G) \otimes A)$; it remains a question whether this spectrum is in fact equal to $\mathrm{Spec}(\Lambda(G) \otimes A)$. The spectrum of $\Lambda(G)$ is also connected.

The rings $R(G)$ and $\Lambda(G)$ are connected by the pairing

$$\begin{array}{rcl} R(G) \times \Lambda(G) & \to & \mathbb{C} \\ \left(\chi_S, \sum_{\sigma \in x} \sigma\right) & \mapsto & \dfrac{\chi_S(\sigma)}{\dim_{\mathbb{C}} S} \quad S \in \mathcal{S}, x \in G/\sim . \end{array}$$

If we view $R(G)$ and $\Lambda(G)$ over $\mathbb{Q}$, we see that they are the row span respectively the column span of the matrix

$$\left(\frac{1}{\dim_{\mathbb{C}} S} \chi_S(\sigma)\right)_{S \in \mathcal{S}, [\sigma] \in G/\sim} .$$

In the last chapter we will generalize this setting and make an equivalence between two categories. For the first category the objects are matrices with entries in $\mathbb{C}$ of which both the row and column span over $\mathbb{Q}$ are rings. For the other category the objects are two abelian finite étale algebras, that is, finite étale algebras for which the Galois group is abelian, with a pairing. From this we will derive that $R(G) \otimes \mathbb{Q}$ and $\Lambda(G) \otimes \mathbb{Q}$ are abelian finite étale algebras which are Brauer equivalent; see section 4.5 for the definition. Furthermore, we have an action of $\Gamma = \mathrm{Gal}\ (\mathbb{Q}^{ab}/Q)$ on them, which satisfies $\langle \gamma M, c \rangle = \gamma \langle M, c \rangle = \langle M, \gamma c \rangle$ for all $M \in R(G) \otimes Q, c \in \Lambda(G) \otimes \mathbb{Q}$ and $\gamma \in \Gamma$, where $\langle \cdot, \cdot \rangle$ is the $\mathbb{Q}$-bilinear pairing

$$\begin{array}{rcl} R(G) \otimes \mathbb{Q} \times \Lambda(G) \otimes \mathbb{Q} & \to & \mathbb{C} \\ \left(\chi_S \otimes 1, \sum_{\sigma \in x} \sigma \otimes 1\right) & \mapsto & \dfrac{\chi_S(\sigma)}{\dim_{\mathbb{C}} S} \quad S \in \mathcal{S}, x \in G/\sim . \end{array}$$

Chapter 2

Comparison of discriminants

In this chapter we will introduce the representation ring $R(G)$ and the center of the group ring $\Lambda(G)$ of a finite group G. Using the characters, we will give an ring embedding into $\mathbb{C}^n$, where n is the number of conjugacy classes of G. With this embedding we can calculate the discriminant of these rings. The question we want to answer, is whether these discriminants divide each other. We will prove for groups of order p^k or pq, with p and q prime and $k \leq 4$ that this indeed the case.

2.1 The representation ring and the center of the group ring

First we define the representation ring and center of the group ring and describe their ring structure.

Let G be a finite group of order g.

Let $X = G/\sim$ be the set of conjugacy classes of G.

Let $\mathcal{S}$ be a set of representatives for the isomorphism classes of simple $\mathbb{C}[G]$-modules.

For each finitely generated $\mathbb{C}[G]$-module M we have $\chi_M : G \to \mathbb{C}$, the character of M, defined by $\chi_M(\sigma) = \mathrm{Tr}(M \to M : m \mapsto \sigma m)$. If σ and τ are conjugate elements of G, then $\chi_M(\sigma) = \chi_M(\tau)$. We define $\chi_M(x) = \chi_M(\sigma)$ for $x \in X$, where σ is an element of x. Furthermore, if M and N are isomorphic modules, then $\chi_M = \chi_N$.

Let $R(G)$ be the Grothendieck group of finitely generated $\mathbb{C}[G]$-modules, that is, the abelian group given by generators the set of isomorphism classes of finitely generated $\mathbb{C}[G]$-modules and relations $\{[M_2] = [M_1] + [M_3] : 0 \to M_1 \to M_2 \to M_3 \to 0$ a short exact sequence$\}$. We will write $[M]$ for the isomorphism class of M. One can prove that $[M] = [N]$ if and only if M and N are isomorphic

The group $R(G)$ becomes a ring with the multiplication $[M] \cdot [N] = [M \otimes_{\mathbb{C}} N]$ for M and N finitely generated $\mathbb{C}[G]$-modules [4, sect. 1.5]. As a group $R(G)$ is a free $\mathbb{Z}$-module on $\{[S] : S \in \mathcal{S}\}$.

Let $\Lambda(G)$ be the center of the group ring $\mathbb{Z}[G]$. As a group it is a free $\mathbb{Z}$-module on $\{c_x = \sum_{\sigma \in x} \sigma : x \in X\}$.

Example 2.1.1.
If G is an abelian group, then $X = G$ and we can take $\mathcal{S} = \{S_\chi : \chi \in \mathrm{Hom}(G, \mathbb{C}^*)\}$, where S_χ is $\mathbb{C}$ with G-action $gz = \chi(g)z$ for $g \in G$ and $z \in \mathbb{C}$.

Now, $R(G)$ as a group is $\oplus_{S\in\mathcal{S}}\mathbb{Z}[S]$ and for the multiplication we have $[S_{\chi_1}]\cdot[S_{\chi_2}] = [S_{\chi_1}\otimes_{\mathbb{C}} S_{\chi_2}] = [S_{\chi_1\cdot\chi_2}]$. So, We obtain the ring isomorphism $R(G)\cong\mathbb{Z}[\mathrm{Hom}(G,\mathbb{C}^*)]$.

Furthermore, $\Lambda(G)=\mathbb{Z}[G]$. Since G and $\mathrm{Hom}(G,\mathbb{C}^*)$ are isomorphic groups, $R(G)$ and $\Lambda(G)$ are isomorphic rings.

We will see that in general $R(G)$ and $\Lambda(G)$ are non-isomorphic. To better understand these rings, we are going to give an explicit description of their structure. To do this, we first define the ring homomorphism

$$\begin{array}{rcl} \phi:\mathbb{C}[G] & \to & \Pi_{S\in\mathcal{S}}\mathrm{End}_{\mathbb{C}}(S) \\ \sigma & \mapsto & (s\mapsto\sigma s)_{S\in\mathcal{S}}, \end{array}$$

which sends an element of $\mathbb{C}[G]$ to all its actions on the simple modules. From representation theory we know that ϕ is an isomorphism [3, chap. XVIII, sect. 4]. So, the centers of $\mathbb{C}[G]$ and $\Pi_{S\in\mathcal{S}}\mathrm{End}_{\mathbb{C}}(S)$ are isomorphic. Using the notation $Z(R)$ for the center of the ring R, we have

$$\begin{array}{rcl} Z(\mathbb{C}[G]) & = & \bigoplus_{x\in X} c_x\mathbb{C} \qquad \text{and} \\ Z(\Pi_{S\in\mathcal{S}}\mathrm{End}_{\mathbb{C}}(S)) & = & \Pi_{S\in\mathcal{S}}Z(\mathrm{End}_{\mathbb{C}}(S))=\Pi_{S\in\mathcal{S}}I_S\mathbb{C}, \end{array}$$

with I_S the identity on S.

On the center, we can write

$$\begin{array}{rcl} \phi(c_x) & = & (\alpha_S I_S)_S, \quad \text{where} \\ \alpha_S & = & \dfrac{1}{\dim_{\mathbb{C}} S}\mathrm{Tr}(\text{action of } c_x \text{ on } S) \\ & = & \dfrac{1}{\dim_{\mathbb{C}} S}\displaystyle\sum_{\sigma\in x}\chi_S(\sigma)=\dfrac{\#x}{\dim_{\mathbb{C}} S}\chi_S(x). \end{array}$$

The isomorphism of the centers $\bigoplus_{x\in X} c_x\mathbb{C}\to\Pi_{S\in\mathcal{S}}I_S\mathbb{C}$ is given by the matrix

$$\left(\frac{\#x}{\dim_{\mathbb{C}} S}\chi_S(x)\right)_{S\in\mathcal{S},x\in X}. \tag{2.1}$$

It follows that this matrix is invertible. By restricting the isomorphism of the centers on the left side to $\Lambda(G)$, we have proved the following lemma.

Lemma 2.1.2. *The map*

$$\begin{array}{rcl} \Lambda(G) & \to & \mathbb{C}^{\mathcal{S}} \\ c_x & \mapsto & \left(\dfrac{\#x}{\dim_{\mathbb{C}} S}\chi_S(x)\right)_{S\in\mathcal{S}}. \end{array} \tag{2.2}$$

is an injective ring homomorphism.

A similar description for $R(G)$ is given by the following lemma.

Lemma 2.1.3. *The map*

$$\begin{array}{rcl} R(G) & \to & \mathbb{C}^X \\ [S] & \mapsto & (\chi_S(x))_{x\in X}. \end{array} \tag{2.3}$$

is an injective ring homomorphism.

Proof. First note that if M and N are isomorphic modules, then $\chi_M = \chi_N$. So this map is independent of the choice of $\mathcal{S}$.

Furthermore, for all finitely generated $\mathbb{C}[G]$-modules M, N, we have $\chi_M + \chi_N = \chi_{M\oplus N}$ and $\chi_M \cdot \chi_N = \chi_{M\otimes_{\mathbb{C}} N}$, which can be seen by writing down the corresponding matrices or looking at [4, sect. 2.1, prop, 2].

Finally, since the matrix (2.1) is invertible, the matrix $(\chi_S(x))_{S\in\mathcal{S},x\in X}$ is invertible, so the $\mathbb{C}$-linear map

$$\begin{array}{rcl} R(G)\otimes\mathbb{C} & \to & \mathbb{C}^X \\ [S] & \mapsto & (\chi_S(x))_{x\in X}. \end{array}$$

is a bijection. After restricting the left side to $R(G)$, we obtain an injection. □

The matrix $(\chi_S(x))_{S\in\mathcal{S},x\in X}$ is called the character table of G.

Example 2.1.4.

Take $G = S_3$, the symmetric group on three elements. Then $X = \{\overline{(1)}, \overline{(1\,2)}, \overline{(1\,2\,3)}\}$ and $\mathcal{S} = M_1, M_\epsilon, M_2$, where M_1 and M_ϵ are 1-dimensional $\mathbb{C}$-modules, with the following actions

$$\begin{array}{rcl} G\times M_1 & \to & M_1 \\ (\sigma, m) & \mapsto & m \end{array}$$

$$\begin{array}{rcll} G\times M_\epsilon & \to & M_\epsilon & \\ (\sigma, m) & \mapsto & \epsilon(\sigma)m & \qquad \text{where } \epsilon(\sigma) \text{ is the sign of } \sigma. \end{array}$$

Let S_3 act on $\mathbb{C}^3 = v_1\mathbb{C}\oplus v_2\mathbb{C}\oplus v_3\mathbb{C}$ by permuting the coordinates. Now, S_3 acts trivially on the vector space $(v_1+v_2+v_3)\mathbb{C}$. The module M_2 is $\mathbb{C}^3/(v_1+v_2+v_3)\mathbb{C}$.

Now we can calculate the character table:

$$\begin{array}{rcl} \chi_{M_1}(\sigma) & = & 1 \\ \chi_{M_\epsilon}(\sigma) & = & \epsilon(\sigma) \\ \chi_{M_2}(1) & = & \mathrm{Tr}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 2 \\ \chi_{M_2}(1\,2) & = & \mathrm{Tr}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = 0 \\ \chi_{M_2}(1\,2\,3) & = & \mathrm{Tr}\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} = -1 \end{array}$$

So

$$(\chi_S(\sigma))_{S\in\mathcal{S},[\sigma]\in X} = \begin{array}{c} \\ M_1 \\ M_\epsilon \\ M_2 \end{array} \begin{array}{c} \begin{array}{ccc} \overline{(1)} & \overline{(1\,2)} & \overline{(1\,2\,3)} \end{array} \\ \begin{pmatrix} 1 & 1 & 1 \\ 1 & -1 & 1 \\ 2 & 0 & -1 \end{pmatrix} \end{array}.$$

We obtain the following ring isomorphism

$$R(S_3) \cong \mathbb{Z}(1,1,1)\oplus\mathbb{Z}(1,-1,1)\oplus\mathbb{Z}(2,0,-1)\subset\mathbb{Z}^3.$$

Furthermore,

$$\left(\frac{\#x}{\dim_{\mathbb{C}} S}\chi_S(x)\right)_{S\in\mathcal{S},x\in X} = \begin{array}{c} \\ M_1 \\ M_\epsilon \\ M_2 \end{array} \begin{array}{c} \begin{array}{ccc} \overline{(1)} & \overline{(1\,2)} & \overline{(1\,2\,3)} \end{array} \\ \begin{pmatrix} 1 & 3 & 2 \\ 1 & -3 & 2 \\ 1 & 0 & -1 \end{pmatrix} \end{array}.$$

Which gives the ring isomorphism

$$\Lambda(S_3) \cong \mathbb{Z}\begin{pmatrix}1\\1\\1\end{pmatrix} \oplus \mathbb{Z}\begin{pmatrix}3\\-3\\0\end{pmatrix} \oplus \mathbb{Z}\begin{pmatrix}2\\2\\-1\end{pmatrix} \subset \mathbb{Z}^3.$$

2.2 Discriminants

In this section we calculate the discriminants of $R(G)$ and $\Lambda(G)$. First the definition of discriminant.

Definition 2.2.1. *Suppose $R = \oplus_{i=1}^n \mathbb{Z}\cdot\omega_i$ is a ring, then the discriminant $\Delta(R)$ is defined as the $\mathbb{Z}$-ideal generated by $\det(\mathrm{Tr}_{R/\mathbb{Z}}(\omega_i\omega_j))_{i,j=1\ldots n}$.*

In this section we will prove the following two propositions.

Proposition 2.2.2. *Let G be a finite group of order g. The discriminant of $R(G)$ is generated by $\frac{g^{\#X}}{\prod_{x\in X}\#x}$.*

Proposition 2.2.3. *Let G be a finite group of order g. The discriminant of $\Lambda(G)$ is generated by $\frac{g^{\#X}\cdot\prod_{x\in X}\#x}{\left(\prod_{S\in\mathcal{S}}\dim_{\mathbb{C}} S\right)^2}$.*

For the proof of these propositions we first give some lemmas.

Lemma 2.2.4. *Suppose $R = \oplus_{i=1}^n \mathbb{Z}\cdot\omega_i$ is a ring, then $\#\mathrm{Hom}_{\mathrm{ring}}(R,\mathbb{C}) \leq n$ and $\#\mathrm{Hom}_{\mathrm{ring}}(R,\mathbb{C}) = n$ if and only if R is a reduced ring, that is, a ring without nilpotent elements.*

Proof. By extending every morphism of R to $R\otimes\mathbb{Q}$, we see that $\mathrm{Hom}_{\mathrm{ring}}(R,\mathbb{C}) \cong \mathrm{Hom}_{\mathrm{ring}}(R\otimes\mathbb{Q},\mathbb{C})$. The ring $R\otimes\mathbb{Q} = \oplus_{i=1}^n \mathbb{Q}\cdot\omega_i$ is artinian and therefore it is a finite product of artinian local rings [1, thm. 8.7]. Write $R\otimes\mathbb{Q} = \prod_j R_j$, where the R_j are artinian local rings. Let $\mathfrak{m}_j$ be the maximal ideal of R_j. From [3, chap. X, cor. 2.2] we know that $\mathfrak{m}_j$ consists of all the nilpotent elements of R_j. So we have $\mathrm{Hom}_{\mathrm{ring}}(R\otimes\mathbb{Q},\mathbb{C}) = \coprod_j \mathrm{Hom}_{\mathrm{ring}}(R_j,\mathbb{C}) \cong \coprod_j \mathrm{Hom}_{\mathrm{ring}}(R_j/\mathfrak{m}_j,\mathbb{C})$. Therefore

$$\begin{aligned}\#\mathrm{Hom}_{\mathrm{ring}}(R,\mathbb{C}) &= \sum_j \#\mathrm{Hom}_{\mathrm{ring}}(R_j/\mathfrak{m}_j,\mathbb{C})\\ &= \sum_j \#\dim_{\mathbb{Q}} R_j/\mathfrak{m}_j \leq \#\dim_{\mathbb{Q}} R_j = n,\end{aligned}$$

where the second equality come from the fact that $R_j/\mathfrak{m}_j$ is separable over $\mathbb{Q}$ [3, chap. V, sect. 4]. Equality holds if and only if $\mathfrak{m}_j = 0$ for all j, that is, R has no nilpotent elements. □

Lemma 2.2.5. *Suppose $R = \oplus_{i=1}^n \mathbb{Z}\cdot\omega_i$ is a reduced ring. Then $\Delta(R)$ is generated by $\det(f\omega_i)^2_{i,f}$, where i ranges from 1 to n and f over $F = \mathrm{Hom}_{\mathrm{ring}}(R,\mathbb{C})$.*

Proof. Since R is reduced, we have the following ring isomorphism

$$\begin{aligned} R\otimes\mathbb{C} &\to \mathbb{C}^F\\ \omega &\mapsto (f(\omega))_f\,. \end{aligned}$$

Restricting this morphism to R and taking the trace on both sides, we obtain $\mathrm{Tr}_{R/\mathbb{Z}}(\omega) = \sum_f f(\omega)$ for all $\omega\in R$.

So we have $(\mathrm{Tr}_{R/\mathbb{Z}}(\omega_i\omega_j))_{i,j} = (\sum_f f(\omega_i\omega_j))_{i,j} = (f(\omega_i))_{i,f}\cdot(f(\omega_j))_{f,j}$.

Therefore $\Delta(R)$ is generated by $\det(f(\omega_i))_{i,f}\cdot\det(f(\omega_j))_{f,j} = \det(f\omega_i)^2_{i,f}$. □

Lemma 2.2.6. *For all $x, y \in X$ we have*

$$\sum_{S\in\mathcal{S}} \chi_S(x)^*\chi_S(y) = \begin{cases} g/\#x & \text{if } x = y \\ 0 & \text{if } x \neq y \end{cases}.$$

where $\chi_S(x)^*$ is the complex conjugate of $\chi_S(x)$.

Proof. [4, sect. 2.5, prop. 7] $\square$

Proof of proposition 2.2.2. The representation ring $R(G) = \oplus_{S\in\mathcal{S}}\mathbb{Z}[S]$ satisfies $\#\mathrm{Hom}_{\mathrm{ring}}(R(G), \mathbb{C}) = \#\mathcal{S}$, since we have the following distinct ring homomorphisms from lemma 2.1.3

$$\begin{array}{rcll} R(G) & \to & \mathbb{C} & \\ [S] & \mapsto & \chi_S(x) & \text{for all } x \in X. \end{array}$$

So $R(G)$ is reduced and we can apply lemma 2.2.5. Its discriminant is generated by $\det(\chi_S(x))^2_{S\in\mathcal{S},x\in X}$. For some number k we have

$$\det(\chi_S(x))^2_{S\in\mathcal{S},x\in X} = (-1)^k \det\left((\chi_S(x)^*)^T_{S\in\mathcal{S},x\in X}(\chi_S(x))_{S\in\mathcal{S},y\in X}\right).$$

Using lemma 2.2.6, the generator of $\Delta(R(G))$ is

$$\begin{aligned} & \det\left((\chi_S(x)^*)^T_{S\in\mathcal{S},x\in X}(\chi_S(x))_{S\in\mathcal{S},y\in X}\right) \\ = \ & \det\left(\sum_{S\in\mathcal{S}}\chi_S(x)^*\chi_S(y)\right)_{x,y\in X} \\ = \ & \det\begin{pmatrix} \frac{g}{\#x_1} & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \frac{g}{\#x_n} \end{pmatrix} \text{where the } x_i \text{ run over } X \\ = \ & \frac{g^{\#X}}{\prod_{x\in X}\#x}. \end{aligned}$$

$\square$

Proof of proposition 2.2.3. The center of the group ring $\Lambda(G) = \oplus_{x\in X}\mathbb{Z}\cdot c_x$ satisfies $\#\mathrm{Hom}_{\mathrm{ring}}(\Lambda(G), \mathbb{C}) = \#X$, since we have the following distinct ring homomorphisms from lemma 2.1.2

$$\begin{array}{rcll} \Lambda(G) & \to & \mathbb{C} & \\ c_x & \mapsto & \frac{\#x}{\dim_{\mathbb{C}} S}\chi_S(x) & \text{for all } S \in \mathcal{S}. \end{array}$$

So $\Lambda(G)$ is reduced and we can apply lemma 2.2.5. The discriminant of $\Lambda(G)$ is

$$\Delta(\Lambda(G)) = \det\left(\frac{\#x}{\dim_{\mathbb{C}} S}\chi_S(x)\right)^2_{S\in\mathcal{S},x\in X}.$$

It follows that $\frac{\Delta(\Lambda(G))}{\Delta(R(G))}$ is generated by

$$\frac{\det\left(\frac{\#x}{\dim_{\mathbb{C}} S}\chi_S(\sigma)\right)^2_{S\in\mathcal{S},x\in X}}{\det(\chi_S(\sigma))^2_{S\in\mathcal{S},[\sigma]\in X}} = \left(\frac{\Pi_{x\in X}\#x}{\Pi_{S\in\mathcal{S}}\dim_{\mathbb{C}} S}\right)^2$$

and $\Delta(\Lambda(G))$ by

$$\left(\frac{\Pi_{x\in X}\#x}{\Pi_{S\in\mathcal{S}}\dim_{\mathbb{C}} S}\right)^2 \cdot \frac{g^{\#X}}{\prod_{x\in X}\#x} = \frac{g^{\#X}\cdot\prod_{x\in X}\#x}{\left(\prod_{S\in\mathcal{S}}\dim_{\mathbb{C}} S\right)^2}.$$

$\square$

Example 2.2.7.

Take $G = S_3$, then $\Delta(R(G)) = \left(\frac{6^3}{1\cdot 2\cdot 3}\right) = (36)$ and $\frac{\Delta(\Lambda(G))}{\Delta(R(G))} = \left(\frac{1\cdot 2\cdot 3}{1\cdot 1\cdot 2}\right)^2 = (9)$, so $\Delta(\Lambda(G)) = (324)$.

We see that $\Lambda(G)$ and $R(G)$ are not isomorphic as rings, since they have different discriminants. The quotient $\frac{\Delta(\Lambda(G))}{\Delta(R(G))}$ is an integer ideal and we can ask ourselves whether this is always the case.

2.3 Divisibility of discriminants

To ease the notation we will use $\Delta(R) = r$ for "$\Delta(R)$ is generated by r".

For every $g \in \mathbb{N}$ we consider the following statement

Statement 2.3.1. *For each finite group G of order g, we have $\frac{\Delta_{\Lambda(G)/\mathbb{Z}}}{\Delta_{R(G)/\mathbb{Z}}} \in \mathbb{Z}$.*

In this section we will prove the following theorems

Theorem 2.3.2. *Let p be a prime. If $g = p^k$ with $k \leq 4$ then statement 2.3.1 is true.*

Theorem 2.3.3. *Let p, q be primes. If $g = pq$ then statement 2.3.1 is true.*

To show this we will prove the following statement, which is a sufficient condition for statement 2.3.1 to be true, for $g = p^k$ and $g = pq$.

Statement 2.3.4. *For all $c_1, \ldots c_s, d_1, \ldots d_t \in \mathbb{N}$ such that*

1. $s = t$,
2. $\sum c_i = \sum d_j^2 = g$,
3. $c_i \mid g$ *for all* i,
4. $d_j \mid g$ *for all* j,
5. $\#\{i \mid c_i = 1\} \mid g$,
6. $\frac{g}{\#\{i \mid c_i = 1\}}$ *is not prime,*
7. $\#\{i \mid d_i = 1\} \mid g$,

we have $\frac{\prod_i c_i}{\prod_j d_j} \in \mathbb{Z}$

Theorem 2.3.5. *For every $g \in \mathbb{N}$ statement 2.3.4 implies statement 2.3.1.*

For the proof we need the following lemma.

Lemma 2.3.6. *Let G be a finite group and $Z(G)$ its center. The index $[G : Z(G)]$ is not prime.*

Proof. If $[G : Z(G)]$ is prime, then $G/Z(G)$ is cyclic. We will prove that if $G/Z(G)$ is cyclic, then $G/Z(G)$ is trivial.

Let $\sigma \in G$ such that $\overline{\sigma}$ generates $G/Z(G)$. Let $h \in G$ be an element, then we can write $h = \sigma^k h'$ for some $k \in \mathbb{N}$ and $h' \in Z(G)$. Now, $\sigma h = \sigma\sigma^k h' = \sigma^k h' \sigma = h\sigma$, so $\sigma \in Z(G)$ and $G/Z(G)$ is trivial. □

Proof of theorem 2.3.5. Let G be a group of order g. Denote by c_i the number of elements of the i-th conjugacy class of G and by d_j the $\mathbb{C}$-dimension of the j-th simple $\mathbb{C}[G]$-module.

Then we have

1. $s = \#X = \#\mathcal{S} = t$,
2. $\sum c_i = \sum_{x \in X} \#x = g$ and
   $g = \dim_{\mathbb{C}} \mathbb{C}[G] = \dim_{\mathbb{C}} \Pi_{S \in \mathcal{S}} \mathrm{End}_{\mathbb{C}}(S) = \sum_{S \in \mathcal{S}} \dim_{\mathbb{C}}^2 S = \sum d_j^2$,
3. $c_i \mid g$, since for the corresponding $x \in X$ we have $\#x \mid g$,
4. $d_j \mid g$, since for the corresponding $S \in \mathcal{S}$ we have $\dim_{\mathbb{C}} S \mid g$ [3, chap. XVIII, cor. 4.8],
5. $\#\{i \mid c_i = 1\} = \#Z(G) \mid g$, where $Z(G)$ is the center of G,
6. $\frac{g}{\#\{i \mid c_i = 1\}} = \frac{g}{\#Z(G)}$ is not prime, see lemma 2.3.6,
7. $\#\{i \mid d_i = 1\} = \#G^{ab} \mid g$, where G^{ab} is the abelianized G.

According to statement 2.3.4, we have $\frac{\prod_i c_i}{\prod_j d_j} \in \mathbb{Z}$. Therefore

$$\frac{\Delta_{\Lambda(G)/\mathbb{Z}}}{\Delta_{R(G)/\mathbb{Z}}} = \left(\frac{\prod_i c_i}{\prod_j d_j} \right)^2 \in \mathbb{Z}.$$

□

We shall now prove theorem 2.3.2 and 2.3.3 by proving statement 2.3.4 for $g = p^k$ and $g = pq$.

Theorem 2.3.7. *Let p be a prime. If $g = p^k$ with $k \leq 4$ then statement 2.3.4 is true.*

Proof. Let $C_m = \#\{i \mid c_i = m\}$ and $D_m = \#\{i \mid d_i = m\}$ for all $m \in \mathbb{N}$.

Suppose statement 2.3.4 is not true for $g = p^k$, then

1. $\sum_l C_{p^l} = \sum_l D_{p^l}$,
2. $p^k = \sum_l C_{p^l} \cdot p^l$,
3. $p^k = \sum_l D_{p^l} \cdot p^{2l}$,
4. $C_1 = p^{l_c}$ with $l_c \leq k$ and $l_c \neq k - 1$,
5. $D_1 = p^{l_d}$ with $l_d \leq k$,
6. $\sum_l l \cdot C_{p^l} < \sum_l l \cdot D_{p^l}$.

If l_c or l_d is equal to k, then both of them are, because of equation (1), (2) and (3), then inequality (6) becomes an equality, contradiction. So $l_c \leq k - 2$ and $l_d \leq k - 1$. Therefore $k \geq l_c + 2 \geq 2$.

Taking equation (2) modulo p, we get $C_1 = 0 \bmod p$, so $l_c \geq 1$. Taking equation (3) modulo p^2, we get $D_1 = 0 \bmod p^2$, so $l_d \geq 2$. Therefore $k \geq l_c + 2 \geq 3$.

When we subtract equation (1) from inequality (6), we get

$$\sum_{l=2}^{k} (l-1) \cdot C_{p^l} < p^{l_c} - p^{l_d} + \sum_{l=2}^{\lfloor \frac{k-1}{2} \rfloor} (l-1) \cdot D_{p^l}. \tag{2.4}$$

The left hand side of 2.4 is non-negative, so the right hand side needs to be greater than 0. For $k \leq 4$ the right hand side is equal to $p^{l_c} - p^{l_d}$, so we need $l_c > l_d$, so $2 \leq l_d < l_c \leq k - 2 \leq 2$. This is a contradiction, so there are no solutions for $k \leq 4$.

□

Theorem 2.3.8. *Let p, q be primes. If $g = pq$ then statement 2.3.4 is true.*

Proof. Let $C_m = \#\{i \mid c_i = m\}$ and $D_m = \#\{i \mid d_i = m\}$ for all $m \in \mathbb{N}$.

If $p = q$, then 2.3.7 tells us this theorem is true, so without loss of generality we can assume $p < q$.

Suppose statement 2.3.4 is not true for $g = pq$, then

1. $C_1 + C_p + C_q = D_1 + D_p + D_q$,
2. $pq = C_1 + pC_p + qC_q$,
3. $pq = D_1 + p^2 D_p + q^2 D_q$,
4. $C_1 \mid pq$ and $C_1 \neq p, q$,
5. $D_1 \mid pq$,
6. $p^{D_p} q^{D_q} \nmid p^{C_p} q^{C_q}$, which means $D_p > C_p$ or $D_q > C_q$.

If C_1 or D_1 is equal to pq, then both of them are, because of equation (1), (2) and (3) then inequality (6) becomes an equality, so $C_1 = 1$ and $D_1 \neq pq$.

Since $pq < q^2$ we have $D_q = 0$, because of equation (3), and therefore $D_p > C_p$. Taking equation (3) modulo p, we get $D_1 = 0 \bmod p$, so $D_1 = p$ and $D_p = \frac{q-1}{p}$.

We are left with the following equations

$$\begin{aligned} C_p + C_q &= p + \frac{q-1}{p} - 1 \\ pC_p + qC_q &= pq - 1. \end{aligned}$$

For which the solution is $C_p = \frac{q-1}{p} = D_p$ and $C_q = p - 1$.

We needed $D_p > C_p$, so there are no solutions. □

For $g = 12$ is statement 2.3.4 not true. We can take $(c_1 \dots c_6) = (1,1,1,3,3,3)$ and $(d_1 \dots d_6) = (1,1,1,1,2,2)$. Then all the conditions are satisfied, but $\frac{\prod_i c_i}{\prod_j d_j} = \frac{3^3}{2^2} \notin \mathbb{Z}$. Through exhaustive search, we can prove that this is the only counterexample for $g = 12$ for statement 2.3.4. Statement 2.3.4 is also false for $g = 18$ and for $g = 3^5$. The following tables give all counterexamples for $g = 18$ and for $g = 3^5$, where we use the same notation as in the proof of theorem 2.3.8.

$g = 18$							
C_1	C_2	C_3	C_6	C_9	D_1	D_2	D_3
1	1	3	1	0	2	4	0
2	2	1	0	1	2	4	0
2	8	0	0	0	9	0	1
3	0	1	2	0	2	4	0
3	0	2	0	1	2	4	0

$g = 3^5$							
C_1	C_3	C_9	C_{27}	C_{81}	D_1	D_3	D_9
27	0	0	8	0	9	26	0
27	0	3	4	1	9	26	0
27	0	6	0	2	9	26	0
27	3	2	1	2	9	26	0

A computer program has checked statement 2.3.1 for $g < 512$, so for the above examples, the c_i and d_j are not the conjugacy class sizes respectively dimensions of simple modules of existing groups.

The way to improve this method would be to give more or better conditions for the c_i and d_j in statement 2.3.4.

Chapter 3

Comparison of spectra

In this chapter we are going to calculate the spectra of $R(G)$ and $\Lambda(G)$. We view the rings over the subring of $\mathbb{C}$ generated by the g-th roots of unity, with g the order of G. We will this ring A. Since all characters of representations of G have images in A, the spectra of $R(G) \otimes A$ and $\Lambda(G) \otimes A$ are easier to compute than the spectra of $R(G)$ and $\Lambda(G)$. After some general notions about spectra we will calculate the spectrum of $R(G) \otimes A$. For the spectrum of $\Lambda(G) \otimes A$ we will give an 'approximation'.

3.1 Spectra

First some general theory about spectra.

Definition 3.1.1. *Let R be a commutative ring. The spectrum of R, denoted by* $\mathrm{Spec}(R)$*, is the topological space consisting of all prime ideals of R, with topology defined by the closed sets $C(I) = \{\mathfrak{p} \text{ prime} : \mathfrak{p} \supset I\}$, for each ideal I of R. This topology is called the Zariski topology.*

Proposition 3.1.2. *If*

$$\phi : R_1 \to R_2$$

is a ring homomorphism, then we have an induced continuous map

$$\begin{array}{rcl} \phi^* : \mathrm{Spec}(R_2) & \to & \mathrm{Spec}(R_1) \\ \mathfrak{p} & \mapsto & \phi^{-1}(\mathfrak{p}). \end{array}$$

Proof. We need to prove that $\phi^{-1}(\mathfrak{p})$ is a prime ideal of R_1. The map

$$\phi' : R_1 \to R_2 \to R_2/\mathfrak{p}$$

gives to following injection into the domain $R_2/\mathfrak{p}$

$$R_1/\ker(\phi') \hookrightarrow R_2/\mathfrak{p}.$$

So $R_1/\ker(\phi')$ is also a domain and $\ker(\phi') = \phi^{-1}(\mathfrak{p})$ is a prime ideal.

Furthermore, to see that ϕ_* is continuous, let $V_f = \{\mathfrak{p} \in \mathrm{Spec}(R_1) : f \notin \mathfrak{p}\}$ for every element $f \in R_1$. These sets are open in $\mathrm{Spec}(R_1)$, since $V_f^c = C(fR)$, where V^c is the complement of the set V. They also form a basis for the topology of $\mathrm{Spec}(R_1)$, since $C(I)^c = \bigcup_{f \in I} V_f$ for every ideal I. Let $W_g = \{\mathfrak{p} \in \mathrm{Spec}(R_2) : g \notin \mathfrak{p}\}$ for every element $g \in R_2$.

Now we have

$$\phi_*^{-1}(V_f) \quad = \quad \{\mathfrak{p} \in \mathrm{Spec}(R_2) : \phi_*(\mathfrak{p}) \in V_f\}$$

$$
\begin{aligned}
&= \{\mathfrak{p} : f \notin \phi^{-1}(\mathfrak{p})\} \\
&= \{\mathfrak{p} : \phi^{-1}\phi f \notin \phi^{-1}(\mathfrak{p})\} \\
&= \{\mathfrak{p} : \phi f \notin (\mathfrak{p})\} = W_{\phi(f)}.
\end{aligned}
$$

So, ϕ_* is continuous. □

Proposition 3.1.3. *If R_1 and R_2 are commutative rings, then* $\mathrm{Spec}(R_1 \times R_2) = \mathrm{Spec}(R_1) \coprod \mathrm{Spec}(R_2)$.

Proof. If $\mathfrak{p}_1$ is a prime ideal of R_1, then $(R_1 \times R_2)/(\mathfrak{p}_1 \times R_2) = R_1/\mathfrak{p}_1$ is a domain. So $(\mathfrak{p}_1 \times R_2)$ is a prime ideal of $(R_1 \times R_2)$. In the same way, if $\mathfrak{p}_2$ is a prime ideal of R_2, then $R_1 \times (\mathfrak{p}_2)$ is a prime ideal of $(R_1 \times R_2)$.

If $\mathfrak{p}$ is a prime ideal of $R_1 \times R_2$, then $(R_1 \times R_2)/\mathfrak{p}$ is a domain. In this domain we have $\overline{(1,0)} \cdot \overline{(0,1)} = \overline{(0,0)}$, so $\overline{(1,0)} = \overline{(0,0)}$ or $\overline{(0,1)} = \overline{(0,0)}$. If $\overline{(1,0)} = \overline{(0,0)}$, then $R_1 \times 0 \subset \mathfrak{p}$, so $\mathfrak{p} = R_1 \times \mathfrak{p}_2$, where $\mathfrak{p}_2$ is a prime ideal of R_2. Since $(R_1 \times R_2)/(R_1 \times \mathfrak{p}_2)$ is a domain, $\mathfrak{p}_2$ is a prime ideal of R_2. In the same way if $\overline{(0,1)} = \overline{(0,0)}$, then $\mathfrak{p} = \mathfrak{p}_1 \times R_2$, where $\mathfrak{p}_1$ is a prime ideal of R_1. □

Definition 3.1.4. *Let R be a commutative ring. Let $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_k$ be a chain of prime ideals of R. We call k the length of such a chain. Define the dimension of R to be the maximal length of all such chains.*

Now, let A be an order in a number field and let B be a ring such that we have a finite set V and injective A-algebra morphisms $A \hookrightarrow B \hookrightarrow A^V$, such that the index $[A^V : B]$ is finite.

Since each non-zero prime ideal of A is maximal, the dimension of A is 1. We can think of $\mathrm{Spec}(A)$ as a line. Furthermore, by proposition 3.1.3, we have $\mathrm{Spec}(A^V) = V \times \mathrm{Spec}(A)$, so we can think of $\mathrm{Spec}(A^V)$ as $\#V$ lines.

We want to determine $\mathrm{Spec}(B)$. We have ring homomorphisms $A \to B \to A^V$, so according to proposition 3.1.2, we have continuous maps $\mathrm{Spec}(A^V) \to \mathrm{Spec}(B) \to \mathrm{Spec}(A)$. Let π be the map $\mathrm{Spec}(A)^V \to \mathrm{Spec}(B)$.

Proposition 3.1.5. *The map* $\mathrm{Spec}(A^V) \to \mathrm{Spec}(B)$ *is surjective.*

Proof. Examine the extension

$$
\begin{array}{ccc}
A & \subset & A^V \\
a & \mapsto & (a, a, \ldots, a).
\end{array}
$$

Let $\alpha = (a_1, a_2, \ldots, a_n) \in A^V$ and $f = \Pi_i(X - a_i) \in A[X]$, then $f(\alpha) = 0$. So $A \subset A^V$ is integral. So A^V is also integral over B. According to the going-up-theorem [1, thm. 5.10] $\mathrm{Spec}(A^V) \to \mathrm{Spec}(B)$ is surjective. □

We now know that $\mathrm{Spec}(B)$ is a quotient set of $\mathrm{Spec}(A^V)$. If two elements $(v_1, \mathfrak{p}_1), (v_2, \mathfrak{p}_2) \in \mathrm{Spec}(A^V)$ are in the same equivalence class, then $\mathfrak{p}_1 = \mathfrak{p}_2$.

The following proposition tells us for which primes $\mathfrak{p}$ the equivalence class $(v, \mathfrak{p})$ consists of one point, for all $v \in V$.

Proposition 3.1.6. *Let $\mathfrak{p}$ be a non-zero prime ideal of A and p the characteristic of $A/\mathfrak{p}$. Suppose $p \nmid [A^V : B] = t$, then B is totally split at $\mathfrak{p}$, which means that the equivalence class $(v, \mathfrak{p})$ consists of one point, for all $v \in V$.*

Proof. We have $tA^V \subset B \subset A^V$ and since localisation is exact, we have $tA^V_{\mathfrak{p}} \subset B_{\mathfrak{p}} \subset A^V_{\mathfrak{p}}$. Now, since $p \nmid t$, we have $t \in (A^V_{\mathfrak{p}})^*$, so $B_{\mathfrak{p}} = A^V_{\mathfrak{p}}$. Therefore we have the following ring isomorphisms

$$B_{\mathfrak{p}} \otimes (A_{\mathfrak{p}}/\mathfrak{p}_{\mathfrak{p}}) = A^V_{\mathfrak{p}} \otimes (A_{\mathfrak{p}}/\mathfrak{p}_{\mathfrak{p}}).$$

So, we have

$$B/\mathfrak{p} = B_\mathfrak{p}/\mathfrak{p}_\mathfrak{p} = B_\mathfrak{p} \otimes (A_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}) = A_\mathfrak{p}^V \otimes (A_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}) = (A_\mathfrak{p}/\mathfrak{p}_\mathfrak{p})^V = (A/\mathfrak{p})^V.$$

Therefore is the number of primes of B which map to the prime $\mathfrak{p}$ of A equal to $\#V$. □

The following proposition gives us a way of computing $\mathrm{Spec}(B)$ in case we have an explicit description.

Proposition 3.1.7. *Suppose B can be written as $B = \bigoplus_{i=1}^{\#V} c_i \cdot A$, with $c_i = (c_{vi})_v \in A^V$. The points $(v_1, \mathfrak{p}), (v_2, \mathfrak{p}) \in \mathrm{Spec}(A^V)$ have the same image in $\mathrm{Spec}(B)$ if and only if we have $c_{v_1 i} \equiv c_{v_2 i} \bmod \mathfrak{p}$ for all i.*

Proof. Suppose $c_{v_1 i} \equiv c_{v_2 i} \bmod \mathfrak{p}$ for all i. Let $b \in \pi(v_1, \mathfrak{p})$ be an element, we can write $b = \sum_i a_i c_i = \left(\sum_i a_i c_{vi}\right)_v$ with $a_i \in A$ and $\sum_i a_i c_{v_1 i} \in \mathfrak{p}$. Since $\sum_i a_i c_{v_1 i} \equiv \sum_i a_i c_{v_2 i} \bmod \mathfrak{p}$, we have $\sum_i a_i c_{v_2 i} \in \mathfrak{p}$. Therefore $b \in \pi(v_2, \mathfrak{p})$ and $\pi(v_1, \mathfrak{p}) = \pi(v_2, \mathfrak{p})$.

On the other hand, if $\pi(v_1, \mathfrak{p}) = \pi(v_2, \mathfrak{p})$, then $c_i - c_{v_1 i} \cdot 1 = (c_{vi} - c_{v_1 i})_v \in \pi(v_1, \mathfrak{p}) = \pi(v_2, \mathfrak{p})$ for all i, so $c_{v_2 i} - c_{v_1 i} \in \mathfrak{p}$ for all i. □

Example 3.1.8.

Let G be S_3, the symmetric group on three elements. From example 2.1.4 we have the following ring isomorphism

$$\Lambda(G) \cong \mathbb{Z}\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \oplus \mathbb{Z}\begin{pmatrix} 3 \\ -3 \\ 0 \end{pmatrix} \oplus \mathbb{Z}\begin{pmatrix} 2 \\ 2 \\ -1 \end{pmatrix} \subset \mathbb{Z}^3.$$

The points $(M_1, \mathfrak{p})$ and $(M_\epsilon, \mathfrak{p})$ are in the same equivalence class if and only if $(1, 3, 2) = (1, -3, 2)$ in $(\mathbb{Z}/\mathfrak{p}\mathbb{Z})^3$, that is, when $\mathfrak{p}$ is 2 or 3.

The points $(M_1, \mathfrak{p})$ and $(M_2, \mathfrak{p})$ are in the same equivalence class if and only if $(1, 3, 2) = (1, 0, -1)$ in $(\mathbb{Z}/\mathfrak{p}\mathbb{Z})^3$, that is, when $\mathfrak{p}$ is 3.

The points $(M_\epsilon, \mathfrak{p})$ and $(M_2, \mathfrak{p})$ are in the same equivalence class if and only if $(1, -3, 2) = (1, 0, -1)$ in $(\mathbb{Z}/\mathfrak{p}\mathbb{Z})^3$, that is, when $\mathfrak{p}$ is 3.

3.2 The spectrum of the representation ring

Let G be a finite group of order g and A the subring of $\mathbb{C}$ generated by the g-th roots of unity.

First we calculate the spectrum of $R(G) \otimes A$. We are going to embed $R(G) \otimes A$ in A^X, for this we use the following lemma.

Lemma 3.2.1. *Let M be a representation of G and $\sigma \in G$, then $\chi_M(\sigma) \in A$.*

Proof. We have $\chi_M(\sigma) = \mathrm{Tr}(M \to M : m \mapsto \sigma m)$, which is the sum of the eigenvalues counted with their multiplicity. Since $(M \to M : m \mapsto \sigma m)$ has order a divisor of g, all its eigenvalues have order a divisor of g. So all eigenvalues are a g-th root of unity. □

So, we can embed $R(G) \otimes A$ in A^X by the injective A-algebra morphisms

$$\begin{array}{rcl} A \to & R(G) \otimes A & \to A^X \\ a \mapsto & 1 \otimes a & \\ & [M] \otimes 1 & \mapsto (\chi_M(x))_{x \in X}. \end{array}$$

So we have continuous maps

$$\mathrm{Spec}(A^X) = X \times \mathrm{Spec}(A) \xrightarrow{\pi} \mathrm{Spec}(R(G) \otimes A) \to \mathrm{Spec}(A)$$

and $\mathrm{Spec}(R(G) \otimes A)$ is a quotient space of $\mathrm{Spec}(A^X)$. We want to know which equivalence classes of $\mathrm{Spec}(R(G) \otimes A)$ consist of more than one point.

First a lemma which restricts the primes we need to look at.

Lemma 3.2.2. *If a prime p divides $[A^X : R(G) \otimes A]$, then it divides $g = \#G$.*

Proof. For this proof we use the generalized notion of discriminant from a book by Serre, which defines the discriminant and index for lattices over a Dedekind domain [5, chap. III, sect. 2]. We will denote the discriminant of a lattice L over the Dedekind domain A as $\Delta_A(L)$ and the index of lattice L and L' as $[L : L']_A$.

From [5, chap. III, sect. 2, prop. 5] we have the following formula for lattices $L' \subset L$ over A

$$\Delta_A(L') = \Delta_A(L)[L : L']_A^2. \tag{3.1}$$

Using this formula for $L = A^X$ and $L' = R(G) \otimes A$ and proposition 2.2.2, we obtain

$$[A^X : R(G) \otimes A]^2 = [A^X : R(G) \otimes A]_A^2 = \frac{\Delta_A(R(G) \otimes A)}{\Delta_A(A^X)} = \left(\frac{g^{\#X}}{\prod_{x\in X} \#x}\right).$$

□

So, according to proposition 3.1.6, if a prime $\mathfrak{p}$ of A does not divide the order of G, then the equivalence classes of $\mathrm{Spec}(R(G) \otimes A)$ above $\mathfrak{p}$ consist of one element.

Next, we will calculate $\mathrm{Spec}(R(G) \otimes A)$ in the same way as [4, sect. 11.4].

Lemma 3.2.3. *Let p be a prime number and G a finite group, then each $x \in G$ can be written in a unique way as $x = x_u x_r$ where x_u is a p-unipotent element, that is, it has order a power of p and x_r is a p-regular element, that is, it has order prime to p.*

Proof. To see that there is a pair x_u and x_r, decompose the cyclic subgroup generated by x as a direct product $H_1 \times H_2$ of two subgroups, where the order of H_1 is a power of p and the order of H_2 is prime to p.

To see this is the only way, suppose $x = x_u x_r$, with x_u a p-unipotent element and x_r a p-regular element. Let H_1 be the subgroup generated by x and let H_2 be the subgroup generated by x_u and x_r. Both H_1 and H_2 are cyclic of order $\mathrm{ord}(x)$. Since $x \in H_2$, we have $H_1 = H_2$, so x_u and x_r are powers of x.

□

The element x_u (respectively x_r) is called the p-component (respectively the p'-component) of x. Note that x_u and x_r commute.

Lemma 3.2.4. *Let $\mathfrak{p}$ be a prime of A with $\mathrm{char}(A/\mathfrak{p}) = p$, let χ be the image of an element of $R(G) \otimes A$ in A^X, let $x \in G$, and let x_r be the p'-component of x. Then $\chi(x) \equiv \chi(x_r) \bmod \mathfrak{p}$.*

Proof. The character χ is also the character of an element of $R(H) \otimes A$ for every subgroup H of G. We will prove the lemma using the subgroup generated by x, which we will call H. Now $\chi = \chi|_H = \sum_i a_i\chi_i$, with $a_i \in A$ and χ_i running over the distinct characters of degree 1 of H. If q is a sufficiently large power of the norm of $\mathfrak{p}$, we have $x^q = x_r^q$ and thus $\chi_i(x)^q = \chi_i(x_r)^q$ for all i. Therefore $\chi(x)^q = (\sum_i a_i\chi_i(x))^q \equiv \sum_i a_i^q\chi_i(x)^q = \sum_i a_i^q\chi_i(x_r)^q \equiv (\sum_i a_i\chi_i(x_r))^q = \chi(x_r)^q \bmod \mathfrak{p}$, hence $\chi(x) = \chi(x_r) \bmod \mathfrak{p}$, since $a^q \equiv a \bmod \mathfrak{p}$ for all $a \in A$. □

Lemma 3.2.5. *Let x be a p'-element of G, that is, an element of order coprime to p. Then there is an element $M \in R(G) \otimes A$ for which the character has the following properties:*

$$\begin{array}{rcl} \chi(x) & \not\equiv & 0 \bmod p \\ \chi(s) & = & 0 \textit{ for each } p'\textit{-element of } G \textit{ which is not conjugate to } x. \end{array}$$

Proof. [4, sect. 10.3, lemma 8] □

Theorem 3.2.6. *Let $\mathfrak{p}$ be a prime ideal of A and p the characteristic of $A/\mathfrak{p}$, furthermore let c_1 and c_2 be conjugacy classes of G. Let c_1' (respectively c_2') be the class consisting of the p'-components of the elements of c_1 (respectively c_2). Let π be that map $X \times \operatorname{Spec}(A) \to \operatorname{Spec}(R(G) \otimes A)$ defined previously. Then we have $\pi(c_1, \mathfrak{p}) = \pi(c_2, \mathfrak{p})$ if and only if $c_1' = c_2'$.*

Proof. According to proposition 3.1.7, the two primes $\pi(c_1, \mathfrak{p})$ and $\pi(c_2, \mathfrak{p})$ are the same if and only if for all simple $\mathbb{C}[G]$-modules S we have $\chi_S(c_1) = \chi_S(c_2) \bmod \mathfrak{p}$.

If $c_1' = c_2'$, lemma 3.2.4 shows that for every $\mathbb{C}[G]$-module M we have $\operatorname{Tr}_M(c_1) = \operatorname{Tr}_M(c_1') = \operatorname{Tr}_M(c_2') = \operatorname{Tr}_M(c_2) \bmod \mathfrak{p}$, hence $\pi(c_1, \mathfrak{p}) = \pi(c_2, \mathfrak{p})$.

If $c_1' \neq c_2'$, then lemma 3.2.5 gives an element $M \in R(G) \otimes A$, such that its character χ satisfies

$$\begin{array}{rcl} \chi(c_1') & \not\equiv & 0 \bmod p \\ \chi(c_2') & = & 0, \end{array}$$

which implies there is a simple module S for which $\chi_S(c_1) \neq \chi_S(c_2) \bmod \mathfrak{p}$, hence $\pi(c_1, \mathfrak{p}) \neq \pi(c_2, \mathfrak{p})$. □

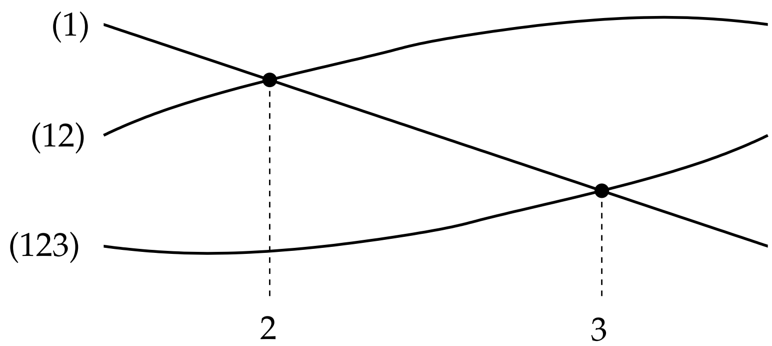
Example 3.2.7.

Let G be S_3, the symmetric group on three elements, then $\#G = 6$, so according to lemma 3.2.2 it suffices to look at primes of residue-characteristic 2 or 3. In the following table are the p'-components for p equal 2 or 3 for all conjugacy classes of G.

conjugacy class	$\overline{(1)}$	$\overline{(1\,2)}$	$\overline{(1\,2\,3)}$
$p = 2$	$\overline{(1)}$	$\overline{(1)}$	$\overline{(1\,2\,3)}$
$p = 3$	$\overline{(1)}$	$\overline{(1\,2)}$	$\overline{(1)}$

So, for all $\mathfrak{p}$ of A of residue-characteristic 2, we have $\pi(\overline{(1)}, \mathfrak{p}) = \pi(\overline{(1\,2)}, \mathfrak{p})$ and for all $\mathfrak{p}$ of A of residue-characteristic 3, we have $\pi(\overline{(1)}, \mathfrak{p}) = \pi(\overline{(1\,2\,3)}, \mathfrak{p})$.

We could also have calculated this spectrum using proposition 3.1.7. Since all the characters of S_3 have image in $\mathbb{Z}^3$, we would have gotten the same result for $R(S_3)$. So the spectrum of $R(S_3)$ looks like



The spectrum of $R(S_3 \otimes A)$ looks the same, with the exception that there are more primes of residue-characteristic 2 or 3.

The spectrum we obtained in the previous example is connected. The following theorem tells us this is the case for all finite groups.

Theorem 3.2.8. *The spectrum* $\mathrm{Spec}(R(G)\otimes A)$ *is connected in the Zariski topology.*

Proof. Let x be an element of G and let $p_1^{k_1} p_2^{k_2} \ldots p_l^{k_l}$ be the prime decomposition of the order of x.

The element x can be written as $x = x_u x_r$, where x_u has order a power of p and x_r has order prime to p. Using this for every prime, we get $x = x_{p_1} x_{p_2} \ldots x_{p_l}$, where x_{p_i} has order $p_i^{k_i}$.

Since x and $x_{p_2} \ldots x_{p_l}$ have the same p'-components, theorem 3.2.6 tells us that $(\overline{x}, \mathfrak{p}_1)$ and $(\overline{x_{p_2} \ldots x_{p_l}}, \mathfrak{p}_1)$ are in the same equivalence class of $R(G) \otimes A$.

Furthermore $\pi(\{y\} \times \mathrm{Spec}(A))$ is connected for all $y \in X$, since it is isomorphic to $\mathrm{Spec}(A)$. So, continuing in the same way, we obtain that $\pi(\overline{x}, \mathrm{Spec}(A))$ is connected to $\pi(\overline{1}, \mathrm{Spec}(A))$. So $\mathrm{Spec}(R(G) \otimes A)$ is connected. □

Corollary 3.2.9. *The spectrum* $\mathrm{Spec}(R(G))$ *is connected in the Zariski topology.*

Proof. From the ring homomorphism $R(G) \to R(G) \otimes A$ we obtain a surjective continuous map $\mathrm{Spec}(R(G) \otimes A) \to \mathrm{Spec}(R(G))$. The spectrum $\mathrm{Spec}(R(G))$ is the image of a connected space under a continuous map and is therefore connected. □

3.3 The spectrum of the center of the group ring

For the spectrum of $\Lambda(G) \otimes A$ we will give a criterion for when an equivalence class certainly consists of more than one element.

We want to embed $\Lambda(G) \otimes A$ in $A^{\mathcal{S}}$, for that we will use the following lemma.

Lemma 3.3.1. *Let* $x \in X$ *be a conjugacy class of* G*, then* $\frac{\#x}{\dim_{\mathbb{C}} S} \chi_S(x) \in A$.

Proof. From lemma 3.2.1 we know that $\chi_S(x) \in A$. Furthermore, the characteristic polynomial of the matrix of the map

$$\begin{array}{ccc} \Lambda(G) & \to & \Lambda(G) \\ c & \mapsto & c_x c. \end{array}$$

is monic and c_x is a zero of it and therefore is c_x integral over $\mathbb{Z}$. Since $\frac{\#x}{\dim_{\mathbb{C}} S} \chi_S(x)$ is the scalar by which c_x acts on S, we have $\frac{\#x}{\dim_{\mathbb{C}} S} \chi_S(x)$ integral over $\mathbb{Z}$ and therefore it is an element of A. □

So, we can embed $\Lambda(G) \otimes A$ in $A^{\mathcal{S}}$ with the A-algebra homomorphisms

$$\begin{array}{rcl} A \to & \Lambda(G) \otimes A & \to A^{\mathcal{S}} \\ a \mapsto & 1 \otimes a & \\ & c_x \otimes 1 & \mapsto \left(\frac{\#x}{\dim_{\mathbb{C}} S} \chi_S(x) \right)_{S \in \mathcal{S}}. \end{array}$$

So we have continuous maps

$$\operatorname{Spec}(A^{\mathcal{S}}) = \mathcal{S} \times \operatorname{Spec}(A) \xrightarrow{\pi} \operatorname{Spec}(\Lambda(G) \otimes A) \to \operatorname{Spec}(A).$$

We want to know for which elements of $\operatorname{Spec}(A^{\mathcal{S}})$ we have $\pi(M_1, \mathfrak{p}) = \pi(M_2, \mathfrak{p})$. First a lemma which restricts the primes we need to look at.

Lemma 3.3.2. *If a prime p divides $[A^X : \Lambda(G) \otimes A]$, then it divides $g = \#G$.*

Proof. Using formula 3.1 for $L = A^X$ and $L' = \Lambda(G) \otimes A$, and proposition 2.2.3 we obtain

$$[A^X : \Lambda(G) \otimes A]^2 = \frac{\Delta_A(\Lambda(G) \otimes A)}{\Delta_A(A^X)} = \frac{g^{\#X} \cdot \prod_{x \in X} \#x}{\left(\prod_{S \in \mathcal{S}} \dim_{\mathbb{C}} S\right)^2}.$$

□

So, according to proposition 3.1.6, if a prime $\mathfrak{p}$ doesn't divide the order of G, then the equivalence classes of $\operatorname{Spec}(\Lambda(G) \otimes A)$ above $\mathfrak{p}$ consist of one element.

Theorem 3.3.3. *Let M and N be two $A[G]$-modules, such that $M \otimes_A \mathbb{C}$ and $N \otimes_A \mathbb{C}$ are simple $\mathbb{C}[G]$-modules and let $\mathfrak{p}$ be a non-zero prime of A. Define $\bar{M} = M \otimes_A A/\mathfrak{p}A$ and $\bar{N} = N \otimes_A A/\mathfrak{p}A$. If $\bar{M}$ and $\bar{N}$ have a common non-trivial $A/\mathfrak{p}A$-subquotient then $\pi(M, \mathfrak{p}) = \pi(N, \mathfrak{p})$.*

Proof. Each element $c \in \Lambda(G) \otimes A$ acts as a scalar of A on M and N, therefore c will act as a scalar of $A/\mathfrak{p}A$ on $\bar{M}$ and $\bar{N}$, say c_M and c_N respectively.

According to proposition 3.1.7, the two primes $\pi(M, \mathfrak{p})$ and $\pi(N, \mathfrak{p})$ are the same if for all $c \in \Lambda(G) \otimes A$ we have $c_M = c_N$.

If $\bar{M}$ and $\bar{N}$ have a non-trivial common subquotient then each c acts as a scalar on that subquotient, say c_S. We get $c_M = c_S = c_N$. □

Note: if $\bar{M}$ and $\bar{N}$ have a non-trivial common subquotient, then they certainly have a common simple subquotient, so it suffices to look at simple subquotients of $\bar{M}$ and $\bar{N}$.

It is proven in [4, section 15.2] that for each simple $\mathbb{C}[G]$-module $M_{\mathbb{C}}$ we can find an $A[G]$-module M_A, such that $M_A \otimes \mathbb{C} = M_{\mathbb{C}}$ and that its simple subquotients do not depend on the choice of M_A. So it is sufficient to construct one $A[G]$-module for each simple $\mathbb{C}[G]$-module and compare only those modules.

Example 3.3.4.

Again, let G be S_3, then $\#G = 6$, so according to lemma 3.3.2 it suffices to look at primes of residue-characteristic 2 or 3.

Recall from section 2.1 the three simple modules M_1, M_ϵ and M_2. The $A[G]$-modules we will use are the module generated by 1 for M_1 and M_ϵ. For M_2 we will use the $A[G]$-module generated by v_1 and v_2.

For primes of residue-characteristic 2 the modules $\bar{M}_1$ and $\bar{M}_\epsilon$ are equal, since $(1, 1, 1) = (1, -1, 1)$ in $(\mathbb{Z}/2\mathbb{Z})^3$. So they certainly have a common non-trivial subquotient.

The module $\bar{M}_2$ does not have a common non-trivial subquotient with $\bar{M}_1$ or $\bar{M}_\epsilon$, since if it would, then there would be a submodule of dimension 1 for which

$(1\,2\,3)$ acts trivially. There is no such submodule, since $\bar{M}_2$ consists of four elements, 0,v_1, v_2 and v_1+v_2, and $(1\,2\,3)$ acts as a cyclic permutation of v_1, v_2 and v_1+v_2.

For primes of residue-characteristic 3, let N be the submodule of $\bar{M}_2$ spanned by v_1+2v_2, then G acts as the sign on N, since $(1\,2)\cdot v_1+2v_2 = v_2+2v_1 = -(v_1+2v_2)$ and $(1\,2\,3)\cdot v_1+2v_2 = v_2+2v_3 = v_2+2(-v_1-v_2) = v_1+2v_2$. So $\bar{M}_2$ and $\bar{M}_\epsilon$ have a common non-trivial subquotient.

Furthermore, G acts on $\bar{M}_2/N$ trivially, since we have $(1\,2)\cdot v_1N = v_2N = (v_2+v_1+2v_2)N = v_1N$ and $(1\,2\,3)\cdot v_1N = v_2N = v_1N$. So $\bar{M}_2$ and $\bar{M}_1$ also have a common non-trivial subquotient.

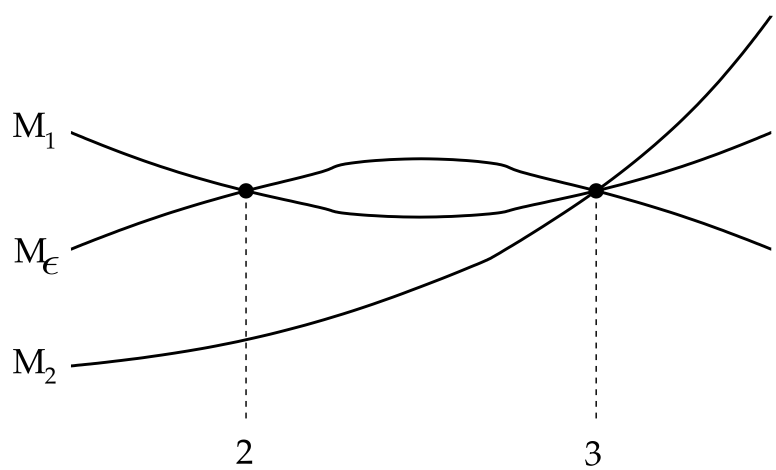
Note that $\bar{M}_1$ and $\bar{M}_\epsilon$ do not have a common non-trivial subquotient, since $(1,1,1)\neq(1,-1,1)$ in $(\mathbb{Z}/3\mathbb{Z})^3$. Still, for primes of residue-characteristic 3, we have $\pi(M_1\mathfrak{p}) = \pi(M_2,\mathfrak{p}) = \pi(M_\epsilon,\mathfrak{p})$.

Apparently, the relation '$\bar{M}$ and $\bar{N}$ have a common non-trivial subquotient' is not transitive, so we need to take the transitive closure to get an quotient space of $\mathrm{Spec}(A^{\mathcal{S}})$. This space is an approximation of $\mathrm{Spec}(\Lambda(G)\otimes A)$.

Let us call the spectrum we just calculated $\mathrm{Spec}(B')$. From theorem 3.3.3 we know we have surjective continuous maps $\mathrm{Spec}(A^{\mathcal{S}}) \twoheadrightarrow \mathrm{Spec}(B') \twoheadrightarrow \mathrm{Spec}(\Lambda(S_3)\otimes A)$.

In fact we have $\mathrm{Spec}(B') = \mathrm{Spec}(\Lambda(S_3)\otimes A)$, since we could also have calculated the spectrum of $\Lambda(S_3)\otimes A$ using proposition 3.1.7. Since we know from example 2.1.4 that $\Lambda(S_3)\otimes A$ has image in $\mathbb{Z}^3$, we would have gotten the same result for $\mathrm{Spec}(\Lambda(S_3))$, which we calculated in example 3.1.8.

Both $\mathrm{Spec}(\Lambda(S_3))$ and $\mathrm{Spec}(B')$ look like



There are more groups for which theorem 3.3.3 gives not only a necessary, but also sufficient condition, but it is not known to the author whether this is true for all groups.

The example tells us that $\mathrm{Spec}(\Lambda(S_3))$ is connected. This is the case for all groups as we shall see from theorem 3.3.8. First some lemmas we need to prove this theorem.

Definition 3.3.5. *A ring R is local if is has a unique maximal left ideal and a unique maximal right ideal and these two ideals coincide [6, thm. 1.3.4].*

Lemma 3.3.6. *Let H be a group of order p^k with p a prime. The ring $\mathbb{F}_p[H]$ is a local ring.*

Proof. Let $\mathfrak{m}$ be a maximal left ideal of $\mathbb{F}_p[H]$. Let I be the ideal generated by

$\{h-1 : h \in H\}$; it is the kernel of the map

$$\begin{array}{rcl} \mathbb{F}_p[H] & \to & \mathbb{F}_p \\ \sum_h a_h h & \mapsto & \sum_h a_h, \end{array}$$

so I is a maximal ideal. Let $\mathfrak{m}$ be a maximal left ideal of $\mathbb{F}_p[H]$. Now, $M = \mathbb{F}_p[H]/\mathfrak{m}$ is a simple left $\mathbb{F}_p[H]$-module. From [3, chap. I, thm 6.5] we know that the center of H contains a non-trivial element c. Since $c^{p^k} = 1$, for some k, we have $(c-1)^{p^k} = 0$ in $\mathbb{F}_p[H]$. So the left module automorphism

$$\begin{array}{rcl} \phi : M & \to & M \\ m & \mapsto & (c-1)m \end{array}$$

is not surjective. Therefore is the image of ϕ equal to 0. So c acts trivially on M and M is a simple $\mathbb{F}_p[H/\langle c\rangle]$-module, where $\langle c\rangle$ is the subgroup of H generated by c.

By induction to the order of H, we get that M is a simple $\mathbb{F}_p$-module and $I = \langle h-1 : h \in H\rangle \subset \mathfrak{m}$. Since I is maximal, we have $I = \mathfrak{m}$.

In the same way we prove that I is the unique maximal right ideal and therefore is $\mathbb{F}_p[H]$ a local ring. □

Lemma 3.3.7. *Let G be a finite group and let P be a finitely generated projective $\mathbb{Z}[G]$-module, then $\#G$ divides the $\mathbb{Z}$-rank of P.*

Proof. Let p be a prime dividing the order of G. Let H be the Sylow-p-group of G, then P is also a $\mathbb{Z}[H]$-module.

The module $P \otimes \mathbb{F}_p$ is a projective $\mathbb{F}_p[H]$-module. From the above lemma we know that $\mathbb{F}_p[H]$ is a local ring, so P is a free module [6, th. 1.3.11] and the rank of P is a multiple of $\#H$. Since this is true for all primes p we have $\#G$ dividing the $\mathbb{Z}$-rank of P. □

Theorem 3.3.8. *Let G be a finite group, then* $\mathrm{Spec}(\Lambda(G))$ *is connected in the Zariski topology.*

Proof. Suppose $\mathrm{Spec}(\Lambda(G))$ is not connected, then we can write $\Lambda(G) = L_1 \oplus L_2$, with L_1 and L_2 proper quotient rings of $\Lambda(G)$. Let e be the unit of L_1, then we can write $\Lambda(G) = e \cdot \Lambda(G) \oplus (1-e)\Lambda(G)$, with e not 0 or 1.

The module $e \cdot \mathbb{Z}[G]$ is a finitely generated projective $\mathbb{Z}[G]$-module of rank which does not divide $\#G$. This is a contradiction with the previous lemma. □

Chapter 4

Comparison of $\mathbb{Q}$-algebras

In this final chapter we view our rings over $\mathbb{Q}$. We will give an equivalence between two categories. The first will generalize the idea of a character table, the second one will consist of a pairing between two abelian finite étale algebras. From this equivalence we will see that $R(G) \otimes \mathbb{Q}$ and $\Lambda(G) \otimes \mathbb{Q}$ are abelian finite étale $\mathbb{Q}$-algebras which are Brauer equivalent. In this chapter we will use several notions from category theory. For definitions, see [2, chap. 2].

4.1 $\mathbb{Q}$-algebras

We are going to examine the rings $R(G) \otimes \mathbb{Q}$ and $\Lambda(G) \otimes \mathbb{Q}$. By tensoring the homomorphism 2.3 with $\mathbb{Q}$, we obtain the following $\mathbb{Q}$-algebra isomorphism

$$R(G) \otimes \mathbb{Q} \xrightarrow{\sim} \mathbb{Q}\text{-span rows} \left(\mathrm{Tr}_S(\sigma)\right)_{S,\sigma} \subset \mathbb{C}^X.$$

Since we are taking the $\mathbb{Q}$-span of the rows, we can multiply a row with a number from $\mathbb{Q}$, without changing the algebra, so we may replace $\left(\mathrm{Tr}_S(\sigma)\right)_{S,\sigma}$ by $\left(\frac{\mathrm{Tr}_S(\sigma)}{\dim_C S}\right)_{S,\sigma}$ to obtain

$$R(G) \otimes \mathbb{Q} \xrightarrow{\sim} \mathbb{Q}\text{-span rows} \left(\frac{\mathrm{Tr}_S(\sigma)}{\dim_C S}\right)_{S,\sigma} \subset \mathbb{C}^X.$$

In the same way, by tensoring the homomorphism 2.2 with $\mathbb{Q}$, we obtain the $\mathbb{Q}$-algebra isomorphism

$$\Lambda(G) \otimes \mathbb{Q} \xrightarrow{\sim} \mathbb{Q}\text{-span columns} \left(\mathrm{Tr}_S(\sigma)\frac{\#[\sigma]}{\dim S}\right)_{S,\sigma} \subset \mathbb{C}^S.$$

We can replace $\left(\mathrm{Tr}_S(\sigma)\frac{\#[\sigma]}{\dim S}\right)_{S,\sigma}$ by $\left(\frac{\mathrm{Tr}_S(\sigma)}{\dim_C S}\right)_{S,\sigma}$ to obtain

$$\Lambda(G) \otimes \mathbb{Q} \xrightarrow{\sim} \mathbb{Q}\text{-span columns} \left(\frac{\mathrm{Tr}_S(\sigma)}{\dim S}\right)_{S,\sigma} \subset \mathbb{C}^S.$$

So the $\mathbb{C}$-valued matrix $\left(\frac{\mathrm{Tr}_S(\sigma)}{\dim S}\right)_{S,\sigma}$ has the property that both the $\mathbb{Q}$-span of the rows and the $\mathbb{Q}$-span of the columns is a ring. We are going the study this kind of matrices and see what we can tell about the $\mathbb{Q}$-spans of rows and columns.

4.2 Finite abelian étale algebras

First we need some new terminology and theory about abelian finite étale algebras.

Let K be a field, $\bar{K}$ an algebraic closure of K. Let K^{sep} be the maximal separable extension of K within $\bar{K}$ and $K^{ab} \subset K^{sep}$ the maximal abelian extension of K within K^{sep}. Let Γ and Γ^{ab} be the Galois groups of K^{sep}/K and K^{ab}/K respectively.

A finite étale K-algebra is a finite product $\prod_i E_i$ where the E_i are finite separable field extensions of K. An abelian finite étale K-algebra is a finite étale K-algebra where the field extensions are abelian over K.

Lemma 4.2.1. *Let E be a abelian finite étale K-algebra.*

1. *There is a unique Γ^{ab}-action on the set E, such that every K-algebra homomorphism $E \to K^{ab}$ is Γ^{ab}-equivariant.*
2. *For this Γ^{ab}-action the map*

$$\begin{array}{rcl} E & \to & E \\ e & \mapsto & \gamma e \end{array}$$

is a K-algebra homomorphism for all $\gamma \in \Gamma^{ab}$.

Proof. Let E_i be a finite abelian extension of K. Let $\sigma_1 : E_i \to K^{ab}$ be a K-algebra homomorphism.

1. The only action of Γ^{ab} on E_i which satisfies the requirements is

$$\begin{array}{rcl} \Gamma^{ab} \times E_i & \to & E_i \\ (\gamma, e) & \mapsto & \sigma_1^{-1}\gamma\sigma_1 e. \end{array}$$

We want to prove that this action is independent of the choice of σ_1. Let $\sigma_2 : E_i \to K^{ab}$ be another K-algebra homomorphism. There is a $\tilde{\gamma} \in \Gamma^{ab}$ such that $\sigma_2 = \tilde{\gamma}\sigma_1$. We now have

$$\begin{array}{rcl} \Gamma^{ab} \times E_i & \to & E_i \\ (\gamma, e) & \mapsto & \sigma_2^{-1}\gamma\sigma_2 e \\ & & = \sigma_1^{-1}\tilde{\gamma}^{-1}\gamma\tilde{\gamma}\sigma_1 e \\ & & = \sigma_1^{-1}\gamma\tilde{\gamma}^{-1}\tilde{\gamma}\sigma_1 e \\ & & = \sigma_1^{-1}\gamma\sigma_1 e. \end{array}$$

So the action on E_i is independent of the choice of σ.

Since every K-algebra homomorphism $E \to K^{ab}$ is composed of a projection $E \to E_i$ and a K-algebra homomorphism $E_i \to K^{ab}$, the only action of Γ^{ab} on E which satisfies the requirements is the componentwise action on the E_i.

2. A projection $E \to E_i$ and the map

$$\begin{array}{rcl} \Gamma^{ab} \times E_i & \to & E_i \\ (\gamma, e) & \mapsto & \sigma_1^{-1}\gamma\sigma_1 e \end{array}$$

are K-algebra homomorphisms.

∎

4.3 Two categories

In this section we define two categories.

Let L be a field, such that $K^{ab} \in L$.

Define the category $\mathcal{C}$ in the following way. The objects of $\mathcal{C}$ are triples (S, T, A) with S and T finite sets and $A = [a_{st}]_{s \in S, t \in T} \in \mathrm{Map}(S \times T, L)$ an invertible matrix such that $\sum_s K(s\text{-th row of } A) \subset L^T$ and $\sum_t K(t\text{-th column of } A) \subset L^S$ are subrings.

A morphism $(S, T, A) \to (S', T', A')$ consists of a map $\phi_S : S' \to S$ and a map $\phi_T : T \to T'$ such that $a_{\phi_S(s')t} = a'_{s'\phi_T(t)}$ for all $s' \in S', t \in T$.

It usually easier to think of a $\mathcal{C}$-morphism as a diagram.

$$\begin{tikzcd}
S & \times & T \arrow[r, "A"] \arrow[d, "\phi_T"] & L \arrow[d, "\mathrm{id}_L"] \\
S' \arrow[u, "\phi_S"] & \times & T' \arrow[r, "A'"] & L
\end{tikzcd}$$

Example 4.3.1.

We take $K = \mathbb{Q}$. Let a and b be non-zero natural numbers. Take for S and T the set $\{1, 2, 3, 4, 5, 6, 7\}$ and

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ \sqrt{a} & \sqrt{a} & -\sqrt{a} & -\sqrt{a} & 1 & 0 & 0 \\ -\sqrt{a} & -\sqrt{a} & \sqrt{a} & \sqrt{a} & 1 & 0 & 0 \\ \sqrt{b} & -\sqrt{b} & \sqrt{b} & -\sqrt{b} & 0 & 1 & 0 \\ -\sqrt{b} & \sqrt{b} & -\sqrt{b} & \sqrt{b} & 0 & 1 & 0 \\ \sqrt{ab} & -\sqrt{ab} & -\sqrt{ab} & \sqrt{ab} & 0 & 0 & 1 \\ -\sqrt{ab} & \sqrt{ab} & \sqrt{ab} & -\sqrt{ab} & 0 & 0 & 1 \end{pmatrix}.$$

Then (S, T, A) is an element of $\mathcal{C}$. To see this we need to show:

1. the element $(1, 1, 1, 1, 1, 1, 1)$ is in the row space.
2. the element $(1, 1, 1, 1, 1, 1, 1)$ is in the column space.
3. if we multiply two rows we get a $\mathbb{Q}$-linear combination of the rows.
4. if we multiply two columns we get a $\mathbb{Q}$-linear combination of the columns.
5. the matrix A is invertible.

Let r_i be the i-th row of A and c_j the j-th column.

1. We have: $(1, 1, 1, 1, 1, 1, 1) = r_1 + \frac{1}{2}\left(r_2 + r_3 + r_4 + r_5 + r_6 + r_7\right).$
2. We have: $(1, 1, 1, 1, 1, 1, 1) = \frac{1}{4}\left(c_1 + c_2 + c_3 + c_4\right) + c_5 + c_6 + c_7.$
3. There are several types of rows. Below is for every combination of types one example.

$$\begin{aligned} r_1 \cdot r_1 &= r_1, \\ r_1 \cdot r_2 &= \frac{1}{2}\left(r_2 - r_3\right), \end{aligned}$$

$$
\begin{aligned}
r_2 \cdot r_2 &= ar_1 + \frac{1}{2}(r_2 + r_3), \\
r_2 \cdot r_6 &= ar_4 - \frac{1}{2}(r_4 + r_5).
\end{aligned}
$$

4. There are several types of columns. Below is for every combination of types one example.

$$
\begin{aligned}
c_1 \cdot c_2 &= \frac{1}{4}(c_1 + c_2 + c_3 + c_4) + ac_5 - bc_6 - abc_7, \\
c_1 \cdot c_5 &= \frac{1}{4}(c_1 + c_2 + c_3 + c_4), \\
c_5 \cdot c_5 &= c_5, \\
c_5 \cdot c_6 &= 0.
\end{aligned}
$$

5. The determinant of A is $128ab$.

Now, define the category $\mathcal{D}$. The objects of $\mathcal{D}$ are triples $(E, F, \langle\cdot,\cdot\rangle)$ where E and F are abelian finite étale K-algebras, and $\langle\cdot,\cdot\rangle$ is a non-degenerate K-bilinear pairing

$$E \times F \xrightarrow{\langle\cdot,\cdot\rangle} K^{ab},$$

which satisfies $\langle \gamma e, f\rangle = \langle e, \gamma f\rangle = \gamma\langle e, f\rangle$ for all $e \in E, f \in F$ and $\gamma \in \Gamma^{ab}$. A morphism $(E, F, \langle\cdot,\cdot\rangle) \to (E', F', \langle\cdot,\cdot\rangle')$ consists of K-algebra homomorphisms $\phi_E : E' \to E$ and $\phi_F : F \to F'$ such that $\langle \phi_E(e'), f\rangle = \langle e', \phi_F(f)\rangle'$ for all $e' \in E'$ and $f \in F$.

It usually easier to think of a $\mathcal{D}$-morphism as a diagram.

$$
\begin{tikzcd}
E & \times & F \arrow[r, "\langle\cdot,\cdot\rangle"] \arrow[d, "\phi_F"] & K^{ab} \arrow[d, "\mathrm{id}_{K^{ab}}"] \\
E' \arrow[u, "\phi_E"] & \times & F' \arrow[r, "\langle\cdot,\cdot\rangle'"] & K^{ab}
\end{tikzcd}
$$

Example 4.3.2.
We take $K = \mathbb{Q}$. Let a and b be two non-square integers. Take

$$E = \mathbb{Q} \times \mathbb{Q}(\sqrt{a}) \times \mathbb{Q}(\sqrt{b}) \times \mathbb{Q}(\sqrt{ab})$$

and

$$F = \mathbb{Q}(\sqrt{a}, \sqrt{b}) \times \mathbb{Q}^3.$$

The pairing will be defined by setting

$$e = (t, u + v\sqrt{a}, w + x\sqrt{b}, y + z\sqrt{ab}) \in E$$

and

$$f = (t' + v'\sqrt{a} + x'\sqrt{b} + z'\sqrt{ab}, u', w', y') \in F$$

and taking

$$
\begin{aligned}
\langle\cdot,\cdot\rangle : E \times F &\to \mathbb{Q}^{ab} \\
(e, f) &\mapsto tt' + uu' + vv'\sqrt{a} + ww' + xx'\sqrt{b} + yy' + zz'\sqrt{ab}.
\end{aligned}
$$

The triple $(E, F, \langle\cdot,\cdot\rangle)$ is an element of $\mathcal{D}$. To see this we need to show that $\langle \gamma e, f\rangle = \langle e, \gamma f\rangle = \gamma\langle e, f\rangle$ for all $\gamma \in \Gamma^{ab}$.

The only elements of Γ^{ab} we need to consider are

$$\begin{array}{ll} \gamma_1 : & (\sqrt{a} \to \sqrt{a}, \sqrt{b} \to -\sqrt{b}), \\ \gamma_2 : & (\sqrt{a} \to -\sqrt{a}, \sqrt{b} \to \sqrt{b}) \text{ and} \\ \gamma_3 : & (\sqrt{a} \to -\sqrt{a}, \sqrt{b} \to -\sqrt{b}). \end{array}$$

We have

$$\begin{aligned} \langle \gamma_1 e, f\rangle = \langle e, \gamma_1 f\rangle = \gamma_1\langle e, f\rangle &= tt' + uu' + vv'\sqrt{a} + ww' - xx'\sqrt{b} + yy' - zz'\sqrt{ab}, \\ \langle \gamma_2 e, f\rangle = \langle e, \gamma_2 f\rangle = \gamma_2\langle e, f\rangle &= tt' + uu' - vv'\sqrt{a} + ww' + xx'\sqrt{b} + yy' - zz'\sqrt{ab}, \\ \langle \gamma_3 e, f\rangle = \langle e, \gamma_3 f\rangle = \gamma_3\langle e, f\rangle &= tt' + uu' - vv'\sqrt{a} + ww' - xx'\sqrt{b} + yy' + zz'\sqrt{ab}. \end{aligned}$$

4.4 An equivalence of categories

We are going to give an equivalence between the categories $\mathcal{C}$ and $\mathcal{D}$, defined in the previous section. First we will construct a functor $\mathcal{C} \to \mathcal{D}$. Theorem 4.4.6 will later tell us this functor is an equivalence.

Lemma 4.4.1. *Let (S, T, A) be an object of $\mathcal{C}$, define $E = \sum_s K(s\text{-th row of } A)$ and $F = \sum_t K(t\text{-th column of } A)$ then $(E, F, \langle\cdot,\cdot\rangle)$, with $\langle\cdot,\cdot\rangle$ defined through*

$$\begin{array}{rcl} E \times F & \xrightarrow{\langle\cdot,\cdot\rangle} & K^{ab} \\ (s\text{-th row of } A, t\text{-th column of } A) & \mapsto & a_{st} \quad \text{for all } s \in S, t \in T \end{array}$$

is an element of $\mathcal{D}$.

Proof. First observe that the rows of A generate a ring of finite dimension over K, therefore, all of the elements of A are algebraic.

Write $e_s = s$-th row of A for $s \in S$, and $f_t = t$-th column of A, for $t \in T$. Write $X = \mathrm{Hom}_{K\text{-alg}}(E, L)$ and $Y = \mathrm{Hom}_{K\text{-alg}}(F, L)$.

Let $t \in T$ and let $\pi_t : L^T \to L$ be the projection on the t-th coordinate. Define a K-algebra morphism $x_t : E \to L$, such that the following diagram of K-algebra morphisms commutes.

$$\begin{tikzcd} E \arrow[r, "\subset"] \arrow[dr, "x_t"] & L^T \arrow[d, "\pi_t"] \\ K \arrow[u] \arrow[r] & L \end{tikzcd}$$

We have $x_t(e_s) = a_{st}$ for all $s \in S$ and $t \in T$. All the x_t are elements of X and since no two columns of A are the same, all these maps are different. We obtain $\#X \geq n = \dim_K E$.

Since E is Artinian, we obtain from [3, chap. X, thm. 7.7] that E is the direct product of local, Artinian rings, $E = \prod_i E_i$. Let $\mathfrak{m}$ be the maximal ideal of E_1. The sequence $\mathfrak{m} \supset \mathfrak{m}^2 \supset \mathfrak{m}^3 \supset \ldots$ has a finite number of ideals, therefore we get from Nakayama's lemma [3, chap. X, lemma 4.1] that $\mathfrak{m}^k = 0$ for some k. We get $\mathfrak{m}$ is nilpotent. Since L^T has no nilpotent elements, E_1 has no nilpotent element. So $\mathfrak{m} = 0$ and E_1 is a field. We obtain E is a finite product of finite field extensions of K.

We now have

$$\begin{aligned}\dim_K E \leq \#X &= \#\mathrm{Hom}_{K\text{-alg}}(E, L)\\ &= \sum_i \#\mathrm{Hom}_{K\text{-alg}}(E_i, L)\\ &\leq \sum_i \#\mathrm{Hom}_K(E_i, \bar{K})\\ &\overset{(*)}{\leq} \sum_i \dim_K E_i = \dim_K E.\end{aligned}$$

So we obtain equality at (*). Therefore all of the E_i are separable [3, chap. V, sect. 4]. We now have $a_{st} \in K^{sep}$ for all $s \in S, t \in T$.

Observe that $X = \{x_t : t \in T\}$. We can let Γ act on X in the following way.

$$\begin{aligned}\Gamma \times X &\to X\\ (\gamma, x) &\mapsto \gamma x.\end{aligned}$$

For all $t \in T$ we have $f_t = (a_{st})_{s\in S} = (x_t(e_s))_{s\in S}$. Let $K[X]$ be the permutation module of X, in other words the $K[\Gamma]$-module with basis X. We have a K-module isomorphism

$$\begin{aligned}i : K[X] &\to F \subset (K^{sep})^S\\ x &\mapsto (x(e_s))_{s\in S}\end{aligned}$$

and since $i(\gamma x) = ((\gamma x)(e_s))_s = (\gamma(x(e_s)))_s = \gamma i x$ for all $\gamma \in \Gamma$, we see that i is a $K[\Gamma]$-module isomorphism. In the same way we can define a $K[\Gamma]$-module isomorphism $K[Y] \to E \subset (K^{sep})^T$.

Now we have $\gamma\langle e_s, f_t\rangle = \gamma(x_t(e_s)) = (\gamma x_t)(e_s) = \langle e_s, \gamma f_t\rangle$ and in the same way $\gamma\langle e_s, f_t\rangle = \langle \gamma e_s, f_t\rangle$ for all $\gamma \in \Gamma, s \in S$ and $t \in T$.

Since $\{e_s : s \in S\}$ and $\{f_t : t \in T\}$ are bases for E and F, we can extend their this property to E and F. So, we have $\langle e, \gamma f\rangle = \gamma\langle e, f\rangle = \langle \gamma e, f\rangle$ for all $\gamma \in \Gamma$, $e \in E$ and $f \in F$.

Now, we have

$$\begin{aligned}\gamma_1\gamma_2\langle e, f\rangle &= \gamma_2\langle \gamma_1 e, f\rangle\\ &= \langle \gamma_1 e, \gamma_2 f\rangle\\ &= \gamma_1\langle e, \gamma_2 f\rangle\\ &= \gamma_2\gamma_1\langle e, f\rangle \qquad \text{for all } \gamma_1, \gamma_2 \in \Gamma, e \in E, f \in F.\end{aligned}$$

The action of Γ factors via its abelian quotient Γ^{ab}. Therefore we can factor all our Γ-actions through Γ^{ab}. The algebras E and F are abelian finite étale algebras. and our constructed Γ^{ab}-action on E satisfies $x(\gamma e) = \gamma(x(e))$ for all $\gamma \in \Gamma^{ab}$, $e \in E$ and $x \in X$. So this action is the unique Γ-action on E from lemma 4.2.1. The same holds for the Γ^{ab}-action on F. □

Given a morphism $(S, T, A) \to (S', T', A')$ of $\mathcal{C}$, let $(E, F, \langle\cdot,\cdot\rangle)$ and $(E', F', \langle\cdot,\cdot\rangle')$ be the objects of $\mathcal{D}$ acquired via the process in lemma 4.4.1.

From the map $\phi_S : S' \to S$ we define an induced map

$$\begin{aligned}\phi_S^* : \left(K^{ab}\right)^S &\to \left(K^{ab}\right)^{S'}\\ (a_s)_{s\in S} &\mapsto (a_{\phi_S(s')})_{s'\in S'}.\end{aligned}$$

For all columns f_t of A we have $\phi_S^*(f_t) = \phi_S^*((ast)_s) = (a\phi_S(s')t)'_s = (a's'\phi_T(t))'_s$, which is the $\phi_T(t)$-th column of A', so we can restrict ϕ_S^* to F. We have a map $\phi_F : F \to F'$.

In the same way, from the map $\phi_T : T \to T'$ we can construct a map $\phi_E : E' \to E$

Lemma 4.4.2. *The maps ϕ_E and ϕ_F are a morphism $(E, F, \langle\cdot,\cdot\rangle) \to (E', F', \langle\cdot,\cdot\rangle')$ of $\mathcal{D}$.*

Proof. First we shall prove that ϕ_F is a K-algebra homomorphism. It is a ring homomorphism, since it is a restriction of ϕ_S^*. So it suffices to show that for all $y' \in \mathrm{Hom}_{K\text{-alg}}(F', K^{ab})$ we have $\phi_F y' \in \mathrm{Hom}_{K\text{-alg}}(F, K^{ab})$.

From the proof of lemma 4.4.1 we know that every $y' \in \mathrm{Hom}_{K\text{-alg}}(F', K^{ab})$ is the restriction of a projection on one of the coordinates of $\left(K^{ab}\right)^{S'}$ So we have the following commutative diagram

$$\begin{tikzcd}
F \arrow[rr, "\subset"] \arrow[d, "\phi_F"'] & & \left(K^{ab}\right)^S \arrow[d, "\phi_S^*"] \\
F' \arrow[rr, "\subset"] \arrow[dr, "y'_s"'] & & \left(K^{ab}\right)^{S'} \arrow[dl, "\pi'_s"] \\
& K^{ab} &
\end{tikzcd}$$

and since the map $\phi_S^*\pi'_s$ is the projection on the $\phi_S(s')$-th coordinate, the map $\phi_F y'_s$ is an element of $\mathrm{Hom}_{K\text{-alg}}(F, K^{ab})$.

In the same way, we prove that ϕ_E is a K-algebra morphism.

It remains to show that $\langle\phi_E(e'), f\rangle = \langle e', \phi_F(f)\rangle'$ for all $e' \in E'$ and $f \in F$.

Let $e_{s'} \in E'$ be the s'-th row of A' and $f_t \in F$ the t-th columns of A. We have seen that $\phi_F(f_t)$ is the $\phi_T(t)$-th column of A' and in the same way is $\phi_E(e_{s'})$ the $\phi_S(s')$-the row of A. So we have

$$\langle\phi_E(e_{s'}), f_t\rangle = a_{\phi_S(s')t} = a_{s'\phi_T(t)} = \langle e_{s'}, \phi_F(f_t)\rangle$$

and since $\{e_{s'} : s' \in S'\}$ are a basis of E and $\{f_t : t \in T\}$ are a basis of F, the identity $\langle\phi_E(e'), f\rangle = \langle e', \phi_F(f)\rangle'$ is true for all $e' \in E'$ and $f \in F$

$\square$

Define the functor $\psi : \mathcal{C} \to \mathcal{D}$ as follows: on objects it applies the process in lemma 4.4.1, on morphisms it applies the process in lemma 4.4.2.

Now we are going to construct a functor $\mathcal{D} \to \mathcal{C}$. This functor will become the inverse of ψ. We first show that E and F have a natural basis. The Gram-matrix $\langle\cdot,\cdot\rangle$ with respect to these bases is the matrix of the associated element of $\mathcal{C}$.

Let $(E, F, \langle\cdot,\cdot\rangle)$ be an object of $\mathcal{D}$.

We can give $X = \mathrm{Hom}_{K\text{-alg}}(E, K^{ab})$ a Γ^{ab}-action by

$$\begin{array}{rcl} \Gamma^{ab} \times X & \to & X \\ (\gamma, x) & \mapsto & \gamma \circ x. \end{array}$$

From the pairing $\langle\cdot,\cdot\rangle$ we can define an isomorphism

$$\begin{array}{rcl} F & \to & \mathrm{Hom}_{K[\Gamma^{ab}]}(E, K^{ab}) \\ f & \mapsto & (e \mapsto \langle e, f\rangle). \end{array}$$

Since the action of Γ on E is the same via every $x \in X$ we have $x(\gamma e) = \gamma x(e)$ for all $x \in X, \gamma \in \Gamma, e \in E$. So $X \subset \mathrm{Hom}_{K[\Gamma^{ab}]}(E, K^{ab})$. For every $x \in X$, let $f_x \in F$ be such that $x(e) = \langle e, f_x \rangle$ for all $e \in E$.

Furthermore, since $\#X = \dim_K E = \dim_K F$ and $\{f_x : x \in X\}$ is K-linearly independent [3, chap. 6, sect. 4], the set $\{f_x : x \in X\}$ is a K-basis of F.

In the same way, for every $y \in Y = \mathrm{Hom}_{K\text{-alg}}(F, K^{ab})$, let $e_y \in E$ be such that $y(f) = \langle e_y, f \rangle$ for all $f \in F$. Then $\{e_y : y \in Y\}$ is a K-basis for E.

Lemma 4.4.3. *The triple* (Y, X, A), *with* $A = (\langle e_y, f_x \rangle)_{y \in Y, x \in X}$ *is an element of* $\mathcal{C}$.

Proof. Since $\{f_x : x \in X\}$ is a basis for F, a linear combination of the rows is 0 if and only if the map $F \to K^{ab}$ it represents, is the zero map. Since $\{e_y : y \in Y\}$ is linearly independent, this can only happen when all coefficients are 0. So A is invertible.

We have a ring isomorphism

$$\begin{array}{rcl} E & \to & \sum_y K(\langle e_y, f_x \rangle)_x \\ e_y & \mapsto & (\langle e_y, f_x \rangle)_x \end{array}$$

So the row span of A is a ring. The column span of A is isomorphic to F, so it is a ring. $\square$

Lemma 4.4.4. *Let* $\phi_E : E' \to E$ *and* $\phi_F : F \to F'$ *be* K*-algebra morphisms, such that* $(E, F, \langle\cdot,\cdot\rangle) \to (E', F', \langle\cdot,\cdot\rangle')$ *is a morphism of* $\mathcal{D}$, *let* (Y, X, A) *and* (Y', X', A') *be the objects of* $\mathcal{C}$ *acquired via the process in lemma 4.4.3.*

The maps

$$\begin{array}{rcl} \phi_Y : Y' & \to & Y \\ y' & \mapsto & y'\phi_F \end{array}$$

and

$$\begin{array}{rcl} \phi_X : X & \to & X' \\ x & \mapsto & x\phi_E \end{array}$$

give a morphism $(Y, X, A) \to (Y', X', A')$ *of* $\mathcal{C}$.

Proof. For all $y' \in Y', x \in X$, we have

$$\begin{array}{rcl} a_{\phi_Y(y')x} & = & \langle e_{\phi_Y(y')}, f_x \rangle = \langle e_{y'\phi_F}, f_x \rangle = y'(\phi_F(f_x)) = \langle e_{y'}, \phi_F(f_x) \rangle' \\ & = & \langle \phi_E(e_{y'}), f_x \rangle = x(\phi_E(e_{y'})) = \langle e_{y'}, f_{x\phi_E} \rangle' = \langle e_{y'}, f_{\phi_X(x)} \rangle' \\ & = & a'_{y'\phi_X(x)}. \end{array}$$

$\square$

Define the functor $\psi' : \mathcal{D} \to \mathcal{C}$ as follows: on objects it applies the process in lemma 4.4.3, on morphisms it applies the process in lemma 4.4.4.

Example 4.4.5.

The triple (S, T, A) from example 4.3.1 is mapped by ψ to an element isomorphic to the triple $(E, F, \langle\cdot,\cdot\rangle)$ from example 4.3.2.

To see this we will first calculate $\mathrm{Hom}(E, \mathbb{Q}^{ab})$. Then, using the isomorphism

$$\begin{array}{rcl} F & \to & \mathrm{Hom}_{K[\Gamma^{ab}]}(E, K^{ab}) \\ f & \mapsto & (e \mapsto \langle e, f \rangle), \end{array}$$

we will find the appropriate basis of F. Using the same notation as example 4.3.2 we have

$\mathrm{Hom}(E, \mathbb{Q}^{ab})$	corresponding element of F
$e \mapsto t$	$(1, 0, 0, 0)$
$e \mapsto u + v\sqrt{a}$	$(\sqrt{a}, 1, 0, 0)$
$e \mapsto u - v\sqrt{a}$	$(-\sqrt{a}, 1, 0, 0)$
$e \mapsto w + x\sqrt{b}$	$(\sqrt{b}, 0, 1, 0)$
$e \mapsto w - x\sqrt{b}$	$(-\sqrt{b}, 0, 1, 0)$
$e \mapsto y + z\sqrt{ab}$	$(\sqrt{ab}, 0, 0, 1)$
$e \mapsto y - z\sqrt{ab}$	$(-\sqrt{ab}, 0, 0, 1)$

The same calculations for $\mathrm{Hom}(F, \mathbb{Q}^{ab})$ and E gives

$\mathrm{Hom}(F, \mathbb{Q}^{ab})$	corresponding element of E
$f \mapsto t' + v'\sqrt{a} + x'\sqrt{b} + z'\sqrt{ab}$	$(1, \sqrt{a}, \sqrt{b}, \sqrt{ab})$
$f \mapsto t' + v'\sqrt{a} - x'\sqrt{b} - z'\sqrt{ab}$	$(1, \sqrt{a}, -\sqrt{b}, -\sqrt{ab})$
$f \mapsto t' - v'\sqrt{a} + x'\sqrt{b} - z'\sqrt{ab}$	$(1, -\sqrt{a}, \sqrt{b}, -\sqrt{ab})$
$f \mapsto t' - v'\sqrt{a} - x'\sqrt{b} + z'\sqrt{ab}$	$(1, -\sqrt{a}, -\sqrt{b}, \sqrt{ab})$
$f \mapsto u'$	$(0, 1, 0, 0)$
$f \mapsto w'$	$(0, 0, 1, 0)$
$f \mapsto y'$	$(0, 0, 0, 1)$

For these two basis the matrix $(\langle e_y, f_x\rangle)$ is A.

Now we have all the ingredients for the following theorem.

Theorem 4.4.6. *The functor ψ is an equivalence between $\mathcal{C}$ and $\mathcal{D}$ and ψ' is its inverse.*

Proof. We need to show the following:

1. The objects (S, T, A) and $\psi'\psi(S, T, A)$ are isomorphic.

2. The objects $(E, F, \langle\cdot,\cdot\rangle)$ and $\psi\psi'(E, F, \langle\cdot,\cdot\rangle)$ are isomorphic.

3. There is a natural isomorphism $\tau : \mathrm{id}_C \to \psi'\psi$, which assigns to every element (S, T, A) of $\mathcal{C}$ a morphism of $\mathcal{C}$, which we will denote by $\tau_{(S,T,A)} : (S, T, A) \to \psi'\psi(S, T, A)$, such that for all $\mathcal{C}$-morphism $g : (S, T, A) \to (S', T', A')$ the following diagram commutes

$$\begin{tikzcd} (S,T,A) \arrow[r, mapsto, "\tau_{(S,T,A)}"] \arrow[d, "g"] & \psi'\psi(S,T,A) \arrow[d, "\psi'\psi(g)"] \\ (S',T',A') \arrow[r, mapsto, "\tau_{(S',T',A')}"] & \psi'\psi(S',T',A') \end{tikzcd}$$

4. There is a natural isomorphism $\tau : \mathrm{id}_D \to \psi\psi'$, which assigns to every element $(E, F, \langle\cdot,\cdot\rangle)$ of $\mathcal{D}$ a morphism of $\mathcal{D}$, which we will denote by $\tau_{(E,F,\langle\cdot,\cdot\rangle)} : (E, F, \langle\cdot,\cdot\rangle) \to \psi'\psi(E, F, \langle\cdot,\cdot\rangle)$, such that for all $\mathcal{D}$-morphism $d : (E, F, \langle\cdot,\cdot\rangle) \to (E', F', \langle\cdot,\cdot\rangle')$ the following diagram commutes

$$\begin{tikzcd}
(E,F,\langle\cdot,\cdot\rangle) \arrow[r, mapsto, "\tau_{(E,F,\langle\cdot,\cdot\rangle)}"] \arrow[d, "d"] & \psi\psi'(E,F,\langle\cdot,\cdot\rangle) \arrow[d, "\psi\psi'(d)"] \\
(E',F',\langle\cdot,\cdot\rangle') \arrow[r, mapsto, "\tau_{(E',F',\langle\cdot,\cdot\rangle')}"] & \psi\psi'(E',F',\langle\cdot,\cdot\rangle')
\end{tikzcd}$$

1. Using notation from lemma 4.4.3, we write $\psi(S,T,A) = (E,F,\langle\cdot,\cdot\rangle)$ and $\psi'(E,F,\langle\cdot,\cdot\rangle) = (Y,X,(\langle e_y,f_x\rangle))$.

   Using the notation from lemma 4.4.1, we define the bijections

$$\begin{array}{rcl} \phi_T : T & \to & X \\ t & \mapsto & x_t \end{array} \tag{4.1}$$

   and

$$\begin{array}{rcl} \phi_S^{-1} : S & \to & Y \\ s & \mapsto & y_s. \end{array} \tag{4.2}$$

   Observe that

$$\begin{array}{rcl} y_s : F & \to & K^{ab} \\ f_t & \mapsto & a_{st} = \langle e_s, f_t\rangle, \end{array}$$

   so $e_{y_s} = e_s = e_{\phi_S(y_s)}$. In the same way we have $f_t = f_{x_t} = f_{\phi_T(t)}$. Therefore we have $\langle e_y, f_{\phi_T(t)}\rangle = \langle e_{\phi_S(y_s)}, f_t\rangle = a_{\phi_S(y_s)t}$ for all $y \in Y$, $t \in T$.

   So (ϕ_S, ϕ_T) is a $\mathcal{C}$-isomorphism.

2. Using notation from lemma 4.4.3, write $\psi'(E,F,\langle\cdot,\cdot\rangle) = (Y,X,(\langle e_y,f_x\rangle))$ and $\psi\left(Y,X,(\langle e_y,f_x\rangle)\right) = (G,H,\langle\cdot,\cdot\rangle_2)$.

   Using the notation from lemmas 4.4.1 and 4.4.3, we define the K-linear maps

$$\begin{array}{rcl} \phi_E : G & \to & E \\ g_y & \mapsto & e_y \end{array} \tag{4.3}$$

   and

$$\begin{array}{rcl} \phi_F : F & \to & H \\ f_x & \mapsto & h_x. \end{array} \tag{4.4}$$

   Remember that g_y is the y-th row of the matrix $(\langle e_y, f_x\rangle)$ and e_y is the element of E such that $y(f) = \langle e_y, f\rangle$ for all $f \in F$.

   Observe that $\langle \phi_E(g_y), f_x\rangle = \langle e_y, f_x\rangle = \langle g_y, h_x\rangle_2 = \langle g_y \phi_F(f_x)\rangle_2$ for all $y \in Y$, $x \in X$. Therefore $\langle \phi_E(g), f\rangle = \langle g, \phi_F(f)\rangle_2$ for all $g \in G$, $f \in F$.

   For all $x \in X, g \in G$, we have $x\phi_E(g) = \langle \phi_E(g), f_x\rangle = \langle g, \phi_F(f_x)\rangle_2 = \langle g, h_x\rangle_2$, so for all $x \in X$ is $x\phi_E \in \mathrm{Hom}(G, K^{ab})$. So ϕ_E is a K-algebra morphism. In the same way we prove that ϕ_F is a K-algebra morphism.

3. Let $\tau_{(S,T,A)} = (\phi_S, \phi_T)$, with ϕ_T from 4.1 and ϕ_S from 4.2, for all $\mathcal{C}$-objects (S,T,A). Write $g = (g_S, g_T)$ and $\psi(g) = (g_E, g_F)$ and $\psi'\psi(g) = ((g_Y, g_X))$. Write $\psi'\psi(S',T',A') = (Y',X',B')$. We need to prove that for all $t \in T$ we have $g_X(\phi_T)(t) = \phi_{T'} g_T(t)$.

   We have $g_X(\phi_T)(t) = g_X(x_t) = x_t g_E$. From the commutative diagram

$$
\begin{tikzcd}
i_{E'} : & E' \arrow[rr, "\subset"] \arrow[d, "g_E"'] & & \left(K^{ab}\right)^{T'} \arrow[d, "g_T^*"] \\
& E \arrow[rr, "\subset"] \arrow[dr, "x_t"'] & & \left(K^{ab}\right)^{T} \arrow[dl, "\pi_t"] \\
& & K^{ab} &
\end{tikzcd}
$$

we see that $x_t g_E = \pi_t g_T^* i_{E'} = \pi_{g_T(t)} i_{E'} = x_{g_T(t)} = \phi_{T'} g_T(t)$.

In the same way we prove that $g_S \phi_{S'}(y') = \phi_S g_Y(y')$ for all $y' \in Y'$.

4. Let $\tau_{(E,F,\langle.,.\rangle)} = (\phi_E, \phi_F)$, with ϕ_E from 4.3 and ϕ_F from 4.4, for all $\mathcal{D}$-objects $(E, F, \langle.,.\rangle)$.Write $d = (g_E, g_F)$ and $\psi'(d) = (d_Y, d_X)$ and $\psi\psi'(d) = ((d_G, d_H))$. Write $\psi\psi'(E', F', \langle.,.\rangle) = (G', H', \langle.,.\rangle_2')$ We need to prove that for all $f \in F$ we have $d_H \phi_F(f) = \phi_{F'} d_F(f)$

   For all $x \in X$ we have $d_H \phi_F(f_x) = d_H(h_x)$. With $i_H : H \to {K^{ab}}^Y$ and $i_{H'} : H' \to {K^{ab}}^{Y'}$ the inclusions from lemma 4.4.3, we get

$$
\begin{array}{rcl}
i_{H'} d_H(h_x) & = & d_Y^* i_H(h_x) = d_Y^*(\langle e_y, f_x \rangle)_y = (\langle e_{d_y(y')}, f_x \rangle)_{y' \in Y'} \\
& = & (\langle e_{y' d_F}, f_x \rangle)_{y'} = (\langle e_{y' d_F}, f_x \rangle)_{y'} = (y' d_F(f_x))_{y'} \\
& = & (\langle e_{y'}, d_F(f_x) \rangle')_{y'} = i_{H'} \phi_{F'} d_F(f_x).
\end{array}
$$

   So, $d_H(h_x) = \phi_{F'} d_F(f_x)$ for all $x \in X$. Therefore $d_H \phi_F(f) = \phi_{F'} d_F(f)$ for all $f \in F$.

   In the same way we prove that $d_E \phi_{E'}(g') = \phi_E d_G(g')$ for all $g' \in G'$.

□

4.5 Brauer equivalence

The category $\mathcal{D}$ is related to Brauer equivalence, as we show in the next section. For this section we require char $K = 0$.

Let E and F be two finite etale K-algebras, then $X = \mathrm{Hom}(E, K^{sep})$ and $Y = \mathrm{Hom}(F, K^{sep})$ are Γ-sets. Define for $\gamma \in \Gamma$ the set $X^{\langle\gamma\rangle} = \{x \in X : \gamma(x) = x\}$.

Definition 4.5.1. *The finite etale algebras E and F are Brauer equivalent if X and Y are linearly equivalent, which means that for all $\gamma \in \Gamma$ we have $\#X^{\langle\gamma\rangle} = \#Y^{\langle\gamma\rangle}$.*

Lemma 4.5.2. *If $K[X] \cong_{K[\Gamma]} K[Y]$ then X and Y are linearly equivalent.*

Proof. For all $\gamma \in \Gamma$ let $\mathrm{Tr}_X(\gamma)$ be the trace of γ on $K[X]$. The action of γ on $K[X]$ is a permutation of X, therefore $\mathrm{Tr}_X(\gamma) = \#X^{\langle\gamma\rangle}$. So $\#X^{\langle\gamma\rangle} = \mathrm{Tr}_X(\gamma) = \mathrm{Tr}_Y(\gamma) = \#Y^{\langle\gamma\rangle}$. □

Theorem 4.5.3. *If $(E, F, \langle\cdot,\cdot\rangle) \in \mathcal{D}$, then E and F are Brauer equivalent.*

Proof. According to lemma 4.5.2 it suffices to prove that $K[X] \cong_{K[\Gamma]} K[Y]$. Since in this case E and F are abelian, we need to prove that $K[X] \cong_{K[\Gamma^{ab}]} K[Y]$.

Write $E = \prod_i E_i$ as a product of fields and define $X_i = \mathrm{Hom}(E_i, K^{ab})$. According to the normal basis theorem [3, chap. VI, thm 13.1] we have

$$E = \prod_i E_i \cong_{K[\Gamma^{ab}]} \prod K[X_i] = K\left[\coprod X_i\right] = K[X].$$

Furthermore, from the proof of lemma 4.4.1, we know that $E \cong_{K[\Gamma^{ab}]} K[Y]$. $\square$

For a finite étale $\mathbb{Q}$-algebra $E = \prod_i E_i$ we define the ring of integers $\mathcal{O}_E$ as $\prod_i \mathcal{O}_{E_i}$, where $\mathcal{O}_{E_i}$ is the ring of integers of E_i. Define the discriminant of $\mathcal{O}_E$ as $\prod_i \Delta\mathcal{O}_{E_i}$.

If E and F are two finite étale algebras which are Brauer equivalent, then the discriminants of their rings of integers are equal [5, chap. VI, sect. 3].

Example 4.5.4.
From example 4.3.2 we get that $\mathbb{Q} \times \mathbb{Q}(\sqrt{a}) \times \mathbb{Q}(\sqrt{b}) \times \mathbb{Q}(\sqrt{ab})$ and $\mathbb{Q}(\sqrt{a}, \sqrt{b}) \times \mathbb{Q}^3$ are Brauer equivalent.

Furthermore, we have $\Delta\left(\mathcal{O}_{\mathbb{Q}(\sqrt{a})}\right) \cdot \Delta\left(\mathcal{O}_{\mathbb{Q}(\sqrt{b})}\right) \cdot \Delta\left(\mathcal{O}_{\mathbb{Q}(\sqrt{ab})}\right) = \Delta\left(\mathcal{O}_{\mathbb{Q}(\sqrt{a},\sqrt{b})}\right)$.

4.6 $\mathbb{Q}$-algebras, continuation

As we have seen in section 4.1, for every finite group G the triple

$$A(G) = \left(\mathcal{S}, X, \left(\frac{\mathrm{Tr}_S(x)}{\dim S}\right)_{S,x}\right)$$

is an element of $\mathcal{C}$. We now have the following corollaries from the theory in sections 4.3–4.5.

Corollary 4.6.1. *The $\mathbb{Q}$-algebras $R(G) \otimes \mathbb{Q}$ and $\Lambda(G) \otimes \mathbb{Q}$ are abelian finite étale $\mathbb{Q}$-algebras with a natural Γ^{ab}-action. The $\mathbb{Q}$-bilinear pairing*

$$\begin{array}{rcl} \langle\cdot,\cdot\rangle_G : R(G) \otimes \mathbb{Q} \times \Lambda(G) \otimes \mathbb{Q} & \to & \mathbb{Q}^{ab} \\ ([S] \otimes 1, c_x \otimes 1) & \mapsto & \dfrac{\mathrm{Tr}_S(x)}{\dim S} \quad \text{for } S \in \mathcal{S}, x \in X. \end{array}$$

satisfies $\gamma\langle M, c\rangle_G = \langle\gamma M, c\rangle_G = \langle M, \gamma c\rangle_G$ for all $\gamma \in \mathrm{Gal}\ (\mathbb{Q}^{ab}/\mathbb{Q}), M \in R(G) \otimes \mathbb{Q}$ and $c \in \Lambda(G) \otimes \mathbb{Q}$.

Proof. The triple $(R(G) \otimes \mathbb{Q}, \Lambda(G) \otimes \mathbb{Q}, \langle\cdot,\cdot\rangle_G)$ is the image of $A(G)$ under ψ. According to lemma 4.4.1 it is an element of $\mathcal{D}$. $\square$

Note that a different scaling of the character table would not have the properties we want, for example, the $\mathbb{Q}$-span of the rows of $(\mathrm{Tr}_S(x))_{S,x}$ is a subring of $\mathbb{C}^X$, but the $\mathbb{Q}$-span of the columns is not in general a subring of $\mathbb{C}^{\mathcal{S}}$. In fact the only scaling we can do which keeps both rows span and column span a subring, is multiplying the entire matrix with a constant from $\mathbb{Q}$.

Corollary 4.6.2. *The $\mathbb{Q}$-algebras $R(G) \otimes \mathbb{Q}$ and $\Lambda(G) \otimes \mathbb{Q}$ are Brauer equivalent.*

Proof. The triple $(R(G) \otimes \mathbb{Q}, \Lambda(G) \otimes \mathbb{Q}, \langle\cdot,\cdot\rangle_G)$ is an element of $\mathcal{D}$. Lemma 4.5.3 tells us that $R(G) \otimes \mathbb{Q}$ and $\Lambda(G) \otimes \mathbb{Q}$ are Brauer equivalent. $\square$

We now also have that the discriminant of the rings of integers of $R(G) \otimes \mathbb{Q}$ and $\Lambda(G) \otimes \mathbb{Q}$ are equal. Remember that the discriminants of $R(G)$ and $\Lambda(G)$ are not always equal, as we have seen in section 2.2.

The rings $R(G) \otimes \mathbb{Q}$ and $\Lambda(G) \otimes \mathbb{Q}$ are not always isomorphic. Counterexamples for 2-groups can be found in [7].

Finally, we give an example of morphisms of $\mathcal{C}$ and $\mathcal{D}$ which occur in representation theory.

Let N be a normal subgroup of G. Let $\mathcal{S}'$ be a set of representatives for the isomorphism classes of simple $\mathbb{C}[G/N]$-modules and let X' be the set of conjugacy classes of G/N.

Lemma 4.6.3. *The maps*

$$\begin{array}{rcl} \phi_S : \mathcal{S}' & \to & \mathcal{S} \\ S' & \mapsto & S, \end{array}$$

where S is the $\mathbb{C}$-module S' with action $G \times S \to S$ defined by $(g, s) \mapsto (gN)s$, and

$$\begin{array}{rcl} \phi_X : X & \to & X' \\ x & \mapsto & xN = \{\sigma N : \sigma \in x\} \end{array}$$

give a morphism $A(G) \to A(G/N)$ in $\mathcal{C}$.

Proof. First we need to show that ϕ_S and ϕ_X are well defined.

Let $S = \phi_S(S')$ for some $S' \in \mathcal{S}'$. A $\mathbb{C}$-vector space with G-action such that N acts trivially, is a $\mathbb{C}[G/N]$-module. So any submodule of S is a submodule of S', since N acts trivially on the submodule. Therefore is S a simple $\mathbb{C}[G]$-module. Let S_2' be the kernel of this morphism. Since $S_2' \cong S_2$ as $\mathbb{C}$-modules and for all $s \in S_2$ we have $gNs \in S_2$, we have $gNs' \in S_2$ for all $s' \in S_2'$. So S_2' is a non-trivial submodule of S'. Since this is a contradiction with S' simple, S is a simple module.

Let σ be an element of x. We have

$$xN = \{\tau\sigma\tau^{-1}N : \tau \in G\} = \{\tau\sigma N\tau^{-1} : \tau \in G/N\}.$$

So xN is a conjugacy class of G/N.

Furthermore, for all $S' \in \mathcal{S}'$ and $x \in X$ we have $\mathrm{Tr}_{\phi_S(S')}(x) = \mathrm{Tr}_{\phi_S(S')}(\sigma) = \mathrm{Tr}(s \mapsto \sigma s) = \mathrm{Tr}(s \mapsto \sigma N s) = \mathrm{Tr}_{S'}(\sigma N) = \mathrm{Tr}_{S'}(xN)$. and $\dim \phi_S(S') = \dim S'$. So

$$\frac{\chi_{\phi_S(S')}(x)}{\dim \phi_S(S')} = \frac{\chi_{S'}(\phi_X(x))}{\dim S'}$$

for all $S' \in \mathcal{S}'$ and $x \in X$.

□

Proposition 4.6.4. *There exist $\mathbb{Q}$-algebra homomorphisms $\phi_R : R(G/N) \otimes \mathbb{Q} \to R(G) \otimes \mathbb{Q}$ and $\phi_\Lambda : \Lambda(G) \otimes \mathbb{Q} \to \Lambda(G/N) \otimes \mathbb{Q}$ such that $\langle \phi_R(M), c \rangle_G = \langle M, \phi_\Lambda(c) \rangle_{G/N}$ for all $M \in R(G/N) \otimes \mathbb{Q}, c \in \Lambda(G) \otimes \mathbb{Q}$.*

Proof. The image under ψ of the map described in lemma 4.6.3, is a map $(R(G) \otimes \mathbb{Q}, \Lambda(G) \otimes \mathbb{Q}, \langle \cdot, \cdot \rangle_G) \to (R(G/N) \otimes \mathbb{Q}, \Lambda(G/N) \otimes \mathbb{Q}, \langle \cdot, \cdot \rangle_{G/N})$. This map consists of the maps ϕ_R and ϕ_Λ. □

Bibliography

[1] M.F. Atiyah, I.G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley, Reading, 1969.

[2] P.J. Hilton, U. Stammbach, *A Course in Homological Algebra*, Springer-Verlag, New York, 1971.

[3] S. Lang, *Algebra, third edition*, Addison-Wesley, Reading, 1993.

[4] J.-P. Serre, *Linear Representations of Finite Groups*, Springer-Verlag, New York, 1977.

[5] J.-P. Serre, *Local Fields*, Springer-Verlag, New York, 1979.

[6] J. Rosenberg, *Algebraic K-theory and its applications*, Springer-Verlag, New York, 1994.

[7] J.G. Thompson, 'A Non-Duality Theorem for Finite Groups', *Journal of Algebra*, **14**, 1970, p. 1–4.