Weil representations associated to finite fields

Parisot Loris

June 21, 2025

Introduction

The main goal of this internship was to formalize some results of the paper "Weil Representation associated to finite fields" by P.Gérardin.

The first section of this report introduces some addenda to mathlib (or other formulations of existing results) that are mandatory to formalize the paper. Those results are about finite group theory, direct sums and tensor products and monoid algebra theory.
The second section aims to add results about the induced representation by the center of a finite group and to provides the formula for its character.
The third section corresponds to some parts of the paper : definition of Heisenberg's group over vector spaces,...

Chapter 1

Addenda to mathlib

This chapter introduces results that weren't in mathlib (or that were in it but needed reformulation to stuck to our situation) and that are mandatory for our goal.

1.1 Group theory

In this section, we fix G group and H a commutative sugroup of G. We denote by $\mathcal{Z}_G$ the center of G and by e_G the neutral of G.

1.1.1 Two lemmas about the center of a group

Proposition 1. *If h is an element of the center of G, it commutes with every element of G.*

Proof. Trivial, just a reformulation in terms of type instead of memebership, useful for the *LEAN* part. □

Proposition 2. *Let $h \in \mathcal{Z}_G$ such that $h = ab$ for some $(a, b) \in G^2$. Then, we also have $h = ba$.*

Proof. Suppose $h = ab$. Then $a = hb^{-1} = b^{-1}h$ because $h \in \mathcal{Z}_G$. Thus $ba = h$. □

1.1.2 Quotient of a group by its center

Definition 3 (Representatives system)**.** We define the system of representatives of $G/\mathcal{Z}_G$ by picking up exactly one element in every classes. We denote it by $\mathcal{S}_{G/\mathcal{Z}_G}$ from now on and denote by C_s the classe of s.

Proof. To do that in *LEAN*, we take the image of G by the map $G \to G/\mathcal{Z}_G \to G$. □

Proposition 4. *If G is finite, then the system of representatives of $G/\mathcal{Z}_G$ is finite too.*

Proof. trivial □

Proposition 5. *Given g and g' in the set of representatives of $G/\mathcal{Z}_G$, if $g \neq g'$ then the classes of g and g' are disjoint.*

Proof. Suppose that the classes aren't disjoints. Then there exists y such that $y \sim g$ and $y \sim g'$. Thus $g \sim g'$ and their classes are equal. But g and g' belongs to the set of representatives. Thus $g = g'$. □

Proposition 6. *We have* $\bigcup_{s \in \mathcal{S}_{G/\mathcal{Z}_G}} C_s = G$.

Proof. If x is in the union, in particular it belongs to G. Let now g be an element of G and let show that it belongs to one of the classes. We apply the map defines in 3 to g and check that g belongs to the class of this element. □

Proposition 7. *We have a bijection between* $\mathcal{S}_{G/\mathcal{Z}_G}$ *and* $\{\bar{g} \in G/\mathcal{Z}_G\}$ *given by the map* $s \to \bar{s}$.

Proof. We check it is a bijection. □

Definition 8. We define a map $\varphi_{G\mathcal{S}} : G \to \mathcal{S}_{G/\mathcal{Z}_G}$ that send every $g \in G$ to its representative.

Proposition 9. *For every* $g \in G$ *and* $h \in \mathbb{Z}_G$, *we have* $\varphi_{G\mathcal{S}}(gh) = \varphi_{G\mathcal{S}}(g)$.

Proof. By definition $g * h$ belongs to the orbit of g, thus they have the same representative. □

Definition 10. We define a map $\psi_{G\mathcal{Z}_G} : G \to \mathcal{Z}_G$ that send every $g \in G$ to the corresponding $h \in \mathcal{Z}_G$ such that $g = sh$ where s is the representative of g.

Proposition 11. *For every* $g \in G$ *the following identity holds :* $g = \varphi_{G\mathcal{S}}(g)\psi_{G\mathcal{Z}_G}(g)$.

Proof. By definition of $G/\mathcal{Z}_G$. □

Proposition 12. *For every* $g \in G$ *the following identity holds :* $\psi_{G\mathcal{Z}_G}(g) = g\varphi_{G\mathcal{S}}(g)^{-1}$.

Proof. Trivial with 11 □

Proposition 13. *For every* $g \in \mathcal{S}_{G/\mathcal{Z}_G}$, *we have* $\psi_{G\mathcal{Z}_G}(g) = e_G$.

Proof. By definition of the map $\psi_{G\mathcal{Z}_G}$. □

Proposition 14. *For every* $g \in \mathcal{S}_{G/\mathcal{Z}_G}$, *we have* $\varphi_{G\mathcal{S}}(g) = g$.

Proof. We have $g = \varphi_{G\mathcal{S}}(g)\psi_{G\mathcal{Z}_G}(g)$ by 11. But $\psi_{G\mathcal{Z}_G}(g) = e_G$ by 13. Thus we get the result. □

Proposition 15. *For every* $g \in G$ *and* $h \in \mathcal{Z}_G$, *we have* $\psi_{G\mathcal{Z}_G}(gh) = h\psi_{G\mathcal{Z}_G}(g)$.

Proof. With 12 we have $\psi_{G\mathcal{Z}_G}(g) = g\varphi_{G\mathcal{S}}(g)^{-1}$ and $\psi_{G\mathcal{Z}_G}(gh) = gh\varphi_{G\mathcal{S}}(gh)^{-1}$. But with 9, we have $\varphi_{G\mathcal{S}}(gh) = \varphi_{G\mathcal{S}}(g)$. Thus, $\psi_{G\mathcal{Z}_G}(gh) = gh\varphi_{G\mathcal{S}}(gh)^{-1} = gh\varphi_{G\mathcal{S}}(g)^{-1} = hg\varphi_{G\mathcal{S}}(g)^{-1} = h\psi_{G\mathcal{Z}_G}(g)$ with the first equality. □

Definition 16. We define a bijection from G to $\mathcal{Z}_G \times \mathcal{S}_{G/\mathcal{Z}_G}$ by $g \mapsto (\psi_{G\mathcal{Z}_G}(g), \varphi_{G\mathcal{S}}(g))$.

Proof. We check the axioms of a bijection. □

Definition 17. The bijection 16 empacked as Sigma type instead of cartesian product. Useful for *LEAN*.

Proposition 18. *We have* $G = \{gh,\ g \in \mathcal{S}_{G/\mathcal{Z}_G},\ h \in \mathcal{Z}_G\}$.

Proof. The inclusion $\{gh,\ g \in \mathcal{S}_{G/\mathcal{Z}_G},\ h \in \mathcal{Z}_G\}$ is trivial. The converse is given by 12. □

1.2 Direct sums and tensor products

1.2.1 Direct sums

Definition 19. If we have two families $(\beta_i)_{i\in I}$ and $(\gamma_i)_{i\in I}$ of additive commutative monoids such that for every $i \in I$, we have an additive bijection φ_i between β_i and γ_i, then we have an additive bijection between $\bigoplus_{i\in I} \beta_i$ and $\bigoplus_{i\in I} \gamma_i$.

Proof. We send $\sum_{i\in I} x_i$ on $\sum_{i\in I} \varphi(x_i)$ and we check that it's an additive bijection. □

Definition 20. Let A be a semiring. If we have two families $(\beta_i)_{i\in I}$ and $(\gamma_i)_{i\in I}$ of additive commutative monoids such that for every $i \in I$, β_i and γ_i are $A-$module and we have a $A-$linear bijection φ_i between β_i and γ_i, then we have a A linear bijection between $\bigoplus_{i\in I} \beta_i$ and $\bigoplus_{i\in I} \gamma_i$.

Proof. We take the map defined in 19 which became $A-$linear by the new properties of the β_i and γ_i. □

Proposition 21. *Let I be a finite set and $(\beta_i)_{i\in I}$ a family of additive commutative monoids. Let Φ be the natural map sending β_{i_0} to $\bigoplus_{i\in I} \beta_i$. Then, for every $x := (x_i)_{i\in I}$ such that $x_i \in \beta_i$ for all $i \in I$, then for every $j \in I$, the following equality holds : $\left(\sum_{i\in I} \Phi(x_i)\right)_j = x_j$.*

Proof. We obvioulsy have $\left(\sum_{i\in I} \Phi(x_i)\right) = \sum_{i\in I} x_i$, which immediately gives the result. □

1.2.2 Tensor products

Definition 22. Let A be ring, B an $A-$algebra, M an $A-$module and N a $B-$module. Then, $\mathrm{Hom}_B((B \otimes_A M), N) \cong \mathrm{Hom}_A(M, N)$.

Proof. We consider the map sending $\varphi \in \mathrm{Hom}_B((B\otimes_A M), N)$ to the $A-$linear map $\Phi_\varphi : M \to N$ defined by $\Phi_\varphi(x) = \varphi(1 \otimes_A x)$ for every $x \in M$. It is injective : if $\Phi_{\varphi_1} = \Phi_{\varphi_2}$, then $\varphi_1(1 \otimes_A x) = \varphi_2(1 \otimes_A x)$ for every $x \in M$. Thus $\varphi_1 = \varphi_2$ by $B-$linearity. It is surjective : let φ be a A-linear map from M to N. Let consider the $B-$linear map ψ from $B \otimes_A M$ to N define by $\psi(b \otimes_A m) = b\varphi(m)$. We have then $\Psi_\psi(x) = \psi(1 \otimes_A x) = \varphi(x)$.

□

1.3 Group algebra

A lot of the results in this section wouldn't really appear in classical mathematics papers, but they are needed to ensure that LEAN understand the operations we will do later.

From now on, $\mathbb{K}$ is a field, G is a group and H is a subgroup of G. We define $mathcal Z_G$ as the center of G.

1.3.1 Setting up operations, coercions and instances in LEAN

Definition 23. Given $\mathbb{K}$ a field, G a group and H a subgroup of G, we have a trivial ring homomorphism φ_{kHkG} from $\mathbb{K}[H]$ to $\mathbb{K}[G]$.

Proof. Trivial. □

Proposition 24. *The map defined in 23 is injective.*

Proof. Trivial. □

Proposition 25. *We have an equality between $h \in H$ seen as an element of $\mathbb{K}[H]$ and h (seen as an element of G) seens as an element of $\mathbb{K}[G]$.*

Proof. Some LEAN stuff. □

Proposition 26. *The map defined in 23 is k linear.*

Proof. Trivial. □

Definition 27. We define a coercion from elements of $\mathbb{K}[H]$ to $\mathbb{K}[G]$ by the map defined in 23.

Proof. Some LEAN stuff. □

Definition 28. We define a coercion from sets of elements of $\mathbb{K}[H]$ to sets of elements of $\mathbb{K}[G]$ by the map defined in 23.

Proof. Some LEAN stuff. □

Definition 29. We define a multiplication between elements of $\mathbb{K}[H]$ and elements of $\mathbb{K}[G]$ by $kH * kG = \varphi_{kHkG}(kH) \times kG$.

Proof. Some LEAN stuff. □

Proposition 30. *$\mathbb{K}[G]$ is a $\mathbb{K}[\mathcal{Z}_G]$ algebra.*

Proof. We check the axiom of an algebra. □

Proposition 31. *If there exists a morphism from H to $\mathcal{Z}_G$, then $\mathbb{K}[G]$ is a $\mathbb{K}[H]$ algebra.*

Proof. We check the axiom of an algebra with the action of $\mathbb{K}[H]$ on $\mathbb{K}[G]$ given by the morphism. □

Proposition 32. *Let $x \in \mathbb{K}[\mathcal{Z}_G]$ and $g \in G$. Then $g \times x = x \times g$.*

Proof. We have $g \times x = g \times \sum_{h \in \mathcal{Z}_g} a_h h = \sum_{h \in \mathcal{Z}_g} a_h gh = \sum_{h \in \mathcal{Z}_g} a_h hg = \left(\sum_{h \in \mathcal{Z}_g} a_h gh \right) \times g.$ □

Definition 33. $\mathbb{K}[\mathcal{Z}_G]$ defines a $\mathbb{K}[G]$ submodule.

Proof. We check the axioms. □

Definition 34. We define the multiplciation of elements $g \in G$ and $kH \in \mathbb{K}[\mathcal{Z}_G]$ in $\mathbb{K}[G]$ by $g \times kH = g \times \varphi_{kHkG}$

Proof. Some LEAN stuff. □

Definition 35. We define the multiplciation of elements $g \in G$ and $kG \in \mathbb{K}[G]$ in $\mathbb{K}[G]$ by $g \times kG$.

Proof. Some LEAN stuff. □

Proposition 36. *Elements of G are distributive over $\mathbb{K}[\mathcal{Z}_G]$*

Proof. Trivial, LEAN stuff. □

1.3.2 Splitting of a group algebra as a direct sum

We use the notation of the section 1 concerning $G/\mathcal{Z}_G$ The main goal of this part is to formalize the following result : $\mathbb{K}[G] \cong \bigoplus_{g \in \mathcal{S}_{G/\mathcal{Z}_G}} g\mathbb{K}[\mathcal{Z}_G]$.

Definition 37. Let $g \in G$ be fixed. The morphism $\varphi_g : \mathcal{Z}_G \to G$ defined by $\varphi_G(x) = gx$ induced a $\mathbb{K}$-linear map Γ_g from $\mathbb{K}[\mathcal{Z}_G]$ to $\mathbb{K}[G]$.

Proof. Trivial. □

Proposition 38. *The map Γ_g defined in 37 is injective.*

Proof. Trivial. □

Proposition 39. *For all $x \in \mathbb{K}[\mathcal{Z}[G]]$, we have $\Gamma_g(x) = g \times x$*

Proof. LEAN stuff to setup a simp lemma. □

Definition 40. We define the set Ω_g to be the image of $\mathbb{K}[\mathcal{Z}_G]$ by Γ_G.

Proof. Nothing useful mathematically, it's just simpler for translating LEAN stuff. □

Definition 41. The map Γ_g defines a k-linear bijection between Ω_g and $\mathbb{K}[\mathcal{Z}_G]$.

Proof. It's injective like we saw before, and $g^{-1} \times x$ is a preimage for x. □

We will now put some structure on Ω_g to makes it understand by LEAN as a $\mathbb{K}[\mathcal{Z}_G]$ module.

Definition 42. We define a multiplication between $x \in \mathbb{K}[\mathcal{Z}_G]$ and $y \in \Omega_g$ by $x \times y$.

Proof. LEAN stuff. □

Definition 43. The multiplication defined in 42 induced an action of $\mathbb{K}[\mathcal{Z}_G]$ on Ω_g.

Proof. We check the axioms. □

Proposition 44. *The action defined in 43 is indeed distributive.*

Proof. We check the axioms. □

Proposition 45. *Ω_g is a $\mathbb{K}[\mathcal{Z}_G]$ module for the action defined in 43.*

Proof. We check the axioms. □

Definition 46. The bijection defined in 41 is indeed a $\mathbb{K}[\mathcal{Z}_G]$-linear map.

Proof. We check the linearity. □

Proposition 47. *Elements of $\mathcal{S}_{G/\mathcal{Z}_G}$ seen as elements of $\mathbb{K}[G]$ defined a basis of $\mathbb{K}[G]$ as a $\mathbb{K}[\mathcal{Z}_G]$ algebra.*

Proof. We show the independence of the family and then that it generates the whole algebra. We suppose that there exists a family $(a_i)_{i\in\mathcal{S}_{G/\mathcal{Z}_G}}$ of elements of $\mathbb{K}[\mathcal{Z}_G]$ such that

$$\sum_{i\in\mathcal{S}_{G/\mathcal{Z}_G}} a_i g_i = 0$$

Using the fact that the family $(h)_{h\in\mathcal{Z}_G}$ seen as a family of elements of $\mathbb{K}[\mathcal{Z}_G]$ is indeed a basis of $\mathbb{K}[\mathcal{Z}_G]$ as a $\mathbb{K}$ vector space we get :

$$\sum_{i\in\mathcal{S}_{G/\mathcal{Z}_G}} \left(\sum_{h\in\mathcal{Z}_G} a_{ih} h\right) g_i = 0$$

where the a_{ih} are elements of $\mathbb{K}$. Those sums are finite, and moreover, the family $(ih)_{(i,h)\in\mathcal{S}_{G/\mathcal{Z}_G}\times\mathcal{Z}_G}$ is a partition of G.
Thus, we get :

$$\begin{aligned}\sum_{i\in\mathcal{S}_{G/\mathcal{Z}_G}} \left(\sum_{h\in\mathcal{Z}_G} a_{ih} h\right) g_i &= \sum_{i\in\mathcal{S}_{G/\mathcal{Z}_G}} \sum_{h\in\mathcal{Z}_G} a_{ih} g_i h \\ &= \sum_{g\in G} a_g g\end{aligned}$$

which is equal to 0. But $(g)_{g\in G}$ seen as a family of elements of $\mathbb{K}[G]$ is a basis of $\mathbb{K}[G]$ as a $\mathbb{K}$ vector space. Finally, $\forall g \in G,\ a_g = 0$ and the family is independent.

Let shows the family generates the whole algebra. Let $x \in \mathbb{K}[G]$. Using the natural basis G of $\mathbb{K}[G]$ and that $(ih)_{(i,h)\in\mathcal{S}_{G/\mathcal{Z}_G}\times\mathcal{Z}_G}$ is a partition of G, we get :

$$\begin{aligned}x &= \sum_{g\in G} a_g g \\ &= \sum_{i\in\mathcal{S}_{G/\mathcal{Z}_G}} \sum_{h\in\mathcal{Z}_G} a_{ih} ih \\ &= \sum_{i\in\mathcal{S}_{G/\mathcal{Z}_G}} \left(\underbrace{\sum_{h\in\mathcal{Z}_G} a_{ih} h}_{\in\mathbb{K}[\mathcal{Z}_G]}\right) i\end{aligned}$$

So it generates the whole algebra and finally we get a basis. □

Definition 48. We define a map on $\mathcal{S}_{G/\mathcal{Z}_G}$ that associates to every elements $g \in \mathcal{S}_{G/\mathcal{Z}_G}$ the natural element of $\bigoplus_{s\in\mathcal{S}_{G/\mathcal{Z}_G}} \mathbb{K}[\mathcal{Z}_G]$, that is 1 of $\mathbb{K}[\mathcal{Z}_G]$ on the $g-$th component and 0 elsewhere.

Definition 49. We construct a $\mathbb{K}[\mathcal{Z}_G]$-linear map on $\bigoplus_{g\in\mathcal{S}_{G/\mathcal{Z}_G}} \mathbb{K}[\mathcal{Z}_G]$ by using the images of the element of the basis 47 by the map 48.

Definition 50. The map defined in 49 is in fact an isomorphism.

Proof. We give an explicit inverse which is $(x_1, \dots, x_g) \mapsto \sum_{g \in \mathcal{S}_{G/\mathcal{Z}_G}} x_g g$. □

Definition 51. We have an isomorphism $\mathbb{K}[G] \cong \bigoplus_{g \in \mathcal{S}_{G/\mathcal{Z}_G}} g\mathbb{K}[\mathcal{Z}_G]$ which is $\mathbb{K}[\mathcal{Z}_G]$-linear.

Proof. We compose the maps defined in 50 and 46 and use the bijection 20. □

1.4 Representation theory

The main goals of this part is to build the representation induced by the center $\mathcal{Z}_G$ of a group G and its basic properties, and to formalize its character.

From now on, $\mathbb{K}$ is a field and G is a group. We denote by $\mathcal{Z}_G$ its center. W is a $\mathbb{K}-$vector space. Finally, θ is a representation of $\mathcal{Z}_G$ in W.

1.4.1 Building the induced representation

Definition 52 (Induced representation as module)**.** Given G a group, $\mathbb{K}$ a field, W a k vector space and θ a representation of $\mathcal{Z}_G$ on W, we define the tensor product $V := \mathbb{K}[G] \otimes_{\mathbb{K}[\mathcal{Z}_G]} V_\theta$, where V_θ is the $\mathbb{K}[\mathcal{Z}_G]$ module associated to θ.

Proposition 53. *The V defined in 52 is an additive commutative monoid.*

Proof. It comes from the fact that $\mathbb{K}[G]$ and $\mathbb{K}[\mathcal{Z}_G]$ are additive commutative monoids. □

Proposition 54. *The V defined in 52 is a $\mathbb{K}[G]$ module.*

Proof. We do *mettre la preuve*. □

Proposition 55. *The V defined in 52 is a $\mathbb{K}[\mathcal{Z}_G]$ module.*

Proof. We do *mettre la preuve*. □

Definition 56 (Induced representation by the center)**.** The V defined in 52 defined a representation of G called the induced representation by $\mathcal{Z}_G$.

Definition 57 (Subrepresentation of the induced)**.** We define the subrepresentation of 56 by $\mathbb{K}[\mathcal{Z}_G] \otimes_{\mathbb{K}[\mathcal{Z}_G]} V_\theta$, where V_θ is the $\mathbb{K}[\mathcal{Z}_G]$ module associated to θ.

Proposition 58. *The tensor product defined in 57 is an additive commutative monoid.*

Proof. It comes from general properties of tensor products. □

Proposition 59. *The tensor product defined in 57 is a $\mathbb{K}[\mathcal{Z}_G]$ module.*

Proof. It comes from general properties of tensor products. □

Proposition 60. *The induced representation defined in 56 is a $\mathbb{K}[\mathcal{Z}_G]$ module.*

Proof. It comes from general properties of tensor products. □

Proposition 61. *We have an isomorphism between $\mathbb{K}[\mathcal{Z}_G] \otimes_{\mathbb{K}[\mathcal{Z}_G]} V_\theta$ and V_θ.*

Proof. It comes from a special case of a theorem *à ajouter*. □

Proposition 62 (Coercion)**.** *We have a coercion from element of type* $\mathbb{K}[\mathcal{Z}_G] \otimes_{\mathbb{K}[\mathcal{Z}_G]} V_\theta$ *to element of type* $\mathbb{K}[G] \otimes_{\mathbb{K}[\mathcal{Z}_G]} V_\theta$*.*

Proof. It comes from 23. □

Proposition 63 (Coercion set)**.** *We have a coercion from element of type* $Set : \mathbb{K}[\mathcal{Z}_G] \otimes_{\mathbb{K}[\mathcal{Z}_G]} V_\theta$ *to element of type* $Set : \mathbb{K}[G] \otimes_{\mathbb{K}[\mathcal{Z}_G]} V_\theta$*.*

Proof. It comes from 23. □

Proposition 64 (V_θ as submodule)**.** *The set of elements of* V_θ *defines a* $\mathbb{K}[\mathcal{Z}_G]$*-submodule of itself.*

Proof. Trivial. □

Proposition 65 (V_θ as submodule isomorphic to V_θ)**.** *The submodule defined in 64 is isomorphic to* V_θ*.*

Proof. Trivial. □

Proposition 66 (Subrepresentation of the induced one as submodule)**.** *The image of the map sending 33 and 65 to their tensor product defines a* $\mathbb{K}[\mathcal{Z}_G]$*-submodule of* $\mathbb{K}[G] \otimes_{\mathbb{K}[\mathcal{Z}_G]} V_\theta$*.*

Proof. Trivial. □

Proposition 67 (Image of V_θ as submodule)**.** *The image of* V_θ *by 61 defines a* $\mathbb{K}[\mathcal{Z}_G]$*-submodule of* $\mathbb{K}[G] \otimes_{\mathbb{K}[\mathcal{Z}_G]} V_\theta$*, ie* V_θ *is a subrepresentation of the induced.*

Proof. Compute the axioms. □

Proposition 68 (Induced reprensentation property)**.** *Let* E *be a* $\mathbb{K}[G]$ *module. We have an isomorphism* $Hom_{\mathbb{K}[G]}\left(\mathbb{K}[G] \otimes_{\mathbb{K}[\mathcal{Z}_G]} V_\theta,\ E\right) \simeq Hom_{\mathbb{K}[\mathcal{Z}_G]}\left(\mathbb{K}[\mathcal{Z}_G] \otimes_{\mathbb{K}[\mathcal{Z}_G]} V_\theta,\ E\right)$*.*

Proof. We use **??** two times. □

1.4.2 Character of the induced representation

Definition 69 (Central function)**.** Given G a group, a function f over G is called central if it is constant on the conjugacy classes of G : $f(g^{-1}xg) = f(x)$ for all $g \in G$ and $x \in G$.

Definition 70 (Induced central function)**.** If H is a subgroup of G a finite group, and if f is a function over H, we define a central function f_G over G (called the induced central function on f) by the formula :

$$f_G(x) = \frac{1}{\mathrm{Card}(H)} \sum_{g \in G \ \wedge \ g^{-1}xg \in H} f(g^{-1}xg)$$

Proof. We check the axiom by reordering the sum with the bijection $x \mapsto g^{-1}x$. □

Definition 71 (Character as central function)**.** A character is of course a central function over G. We empacked this definition in Lean.

Proof. Trivial. □

Proposition 72 (Induced representation is semisimple)**.** *If* $|G| \nmid Char(k)$*, then the module defined in 52 is semisimple.*

Proof. Consequences of . □

Definition 73. We define the $\mathbb{K}[\mathcal{Z}_G]$ module $W_g := g\mathbb{K}[\mathcal{Z}_G] \otimes_{\mathbb{K}[\mathcal{Z}_G]} V_\theta$ for $g \in \mathcal{S}_{G/\mathcal{Z}_G}$.

Definition 74. We have an isomorphism between $\mathbb{K}[G] \otimes_{\mathbb{K}[\mathcal{Z}_G]} V_\theta$ and $\bigoplus_{g \in \mathcal{S}_{G/\mathcal{Z}_G}} W_g = \bigoplus_{g \in \mathcal{S}_{G/\mathcal{Z}_G}} g\mathbb{K}[\mathcal{Z}_G] \otimes_{\mathbb{K}[\mathcal{Z}_G]} V_\theta$.

Proof. We get the resultat with the isomorphism $\mathbb{K}[G] \cong \otimes_{\mathbb{K}[\mathcal{Z}_G]} g\mathbb{K}[\mathcal{Z}_G]$ defined in **??**. □

Chapter 2

Duality and conventions

The article chooses to have a non canonical identification between V and its bidual : $< x, y >= - < y, x >$. Some properties only rely on this identification *(see 86 for an example)*.

2.1 Setting up the conventions

Definition 75 (Bilinear form on $V^{**} \times V$)**.** We define a bilinear form on $V^{**} \times V$ by $(x, y) \mapsto -y(x)$.

Proof. We check the bilinearity. □

We set up also a simp lemma for the evaluation of the bilinear form.

Definition 76 (Map from V to V^{**})**.** We define a linear map from V to V^{**} by $v \mapsto (\varphi \mapsto -\varphi(v))$.

Proof. We check the linearity of the map. □

We set up also a simp lemma for the evaluation of the map.

Proposition 77 (Bijective map from V to V^{**})**.**
If V is reflexive, then the linear map defined in 76 is a bijective linear map from V to V^{**}.

Proof. We check it's a bijective map by giving the explicit inverse map. □

We set up also a simp lemma for the evaluation of the bijective map.

2.2 Some results about the commutator bilinear form

Definition 78 (Commutator form)**.** If V is reflexive, the map $((x_1, y_1), (x_2, y_2)) \mapsto y_1(x_2) - y_2(x_1)$ is a bilinear form on $V \times V^*$.

Proof. We check the bilinearity. □

Proposition 79 (Nondegeneracy)**.**
The bilinear form defined in 78 is a nondegeneracy bilinear form.

Proof. Suppose it is degeneracy. Then there exists $h := (x, y) \in V \times V^*$ such that $h \neq 0$ and $y(x') - y'(x) = 0$ for all $(x', y') \in V \times V^*$. In particular, for $y' = 0$, $y(x') = 0$ for all x', so $y = 0$. Then, for $x' = 0$, $y'(x) = 0$ for all y', so $x = 0$. Thus $h = 0$. Contradiction. □

Chapter 3

Heisenberg's group

3.1 Construction

Definition 80 (Structure of Heisenberg)**.** Given k a field, V a k vector space and V^* its dual vector space, we define the Heisenberg set associated to V by $\mathcal{H}(V) := \{(z, x, y) \in k \times V \times V^*\}$.

Proposition 81 (Trivial bijection)**.** *$\mathcal{H}(V)$ is in bijection with $k \times V \times V^*$.*

Proof. Trivial. □

Definition 82 (Multiplication on Heisenberg)**.**
We define an internal law on Heisenberg by the following formula : $(z_1, x_1, y_1) * (z_2, x_2, y_2) = (z_1 + z_2 + y_1(x_2), x_1 + x_2, y_1 + y_2)$ for every $(z_1, x_1, y_1), (z_2, x_2, y_2) \in \mathcal{H}(V)$.

Definition 83 (Inverse of an element of Heisenberg)**.**
The inverse of $(z, x, y) \in \mathcal{H}(V)$ is given by the formula $(-z - y(-x), -x, -y)$.

Proof. Compute $h * h^{-1}$. □

Proposition 84 (Heisenberg's group)**.** *Heisenberg is a group for the the internal law defined in 82.*

Proof. We check the axioms of a group. □

Definition 85 (Bijectivity with $\mathcal{H}(V*)$)**.**
Under our identification of the bidual, the map $\Phi : (z, x, y) \mapsto (z, y, x)$ defines a bijection between $\mathcal{H}(V)$ and $\mathcal{H}(V^*)$.

Proof. Compute $\Phi \circ \Phi^{-1}$ and $\Phi^{-1} \circ \Phi$. □

Definition 86 (Antiisomorphic with $\mathcal{H}(V*)$)**.**
Under our identification of the bidual, the map define in 85 is a group antiisomorphism from $\mathcal{H}(V)$ to $\mathcal{H}(V^*)$.

Proof. Compute that $\Phi(h_1 * h_2) = \Phi(h_2) * \Phi(h_1)$. □

3.2 Center

Definition 87 (Center of Heisenberg)**.**
We define the center of $\mathcal{H}(V)$ by the set $\mathcal{Z}_{\mathcal{H}(V)} := \{(z,0,0) \in \mathcal{H}(V),\ z \in k\}$

Proposition 88 (The center is a subgroup)**.**
The center of Heisenberg $\mathcal{Z}_{\mathcal{H}(V)}$ is a subgroup of $\mathcal{H}(V)$.

Proof. We check the axioms and compute. □

Proposition 89 (Caracterisation of the center)**.**
The set define in 87 is indeed the center of $\mathcal{H}(V)$.

Proof. By double inclusion. Reciprocity use the fact that the quadratic form 78 is a non degeneracy one *(see 79 for a proof)*. □

3.3 Commutator and nilpotency

Proposition 90 (Commutator)**.**
Let $H_1 := (z_1, x_1, y_1)$ and $H_2 := (z_2, x_2, y_2)$ be two elements of $\mathcal{H}(V)$. The commutator of $[H_1, H_2]$ is $(y_1(x_2) - y_2(x_1), 0, 0)$.

Proof. We compute $H_1 * H_2 * H_1^{-1} * H_2^{-1}$. □

Proposition 91 (Commutator isn't trivial)**.**
If V isn't trivial, the subgroup of $\mathcal{H}(V)$ generates by commutators isn't trivial too.

Proof. By contradiction. If it was trivial, every element of $\mathcal{H}(V)$ would belong to its center. Because V isn't trivial, there exists $x \in V$ such that $x \neq 0$. Thus, $(0, x, 0)$ would belong to the center. But because of the definition of the center, $x = 0$. We get a contradiction. □

Proposition 92 (Caracterisation of the commutator)**.**
If $h := (z, x, y)$ belongs to the commutator subgroup, then $x = 0$ and $y = 0$.

Proof. We compute. □

Theorem 93 (Nilpotency of Heisenberg's group)**.**
If V isn't trivial, $\mathcal{H}(V)$ is a two step nilpotent group.

Proof. We have to show that the commutator isn't trivial and that $[[\mathcal{H}(V), \mathcal{H}(V)], \mathcal{H}(V)]$ is trivial. The first point is done in 91. The second is some computation, using 92. □

3.4 Short exact sequence

Definition 94 (Homomorphism from k to $\mathcal{H}(V)$)**.**
The map $\varphi : z \mapsto (z, 0, 0)$ defines a homomorphism from $(k, +)$ to $\mathcal{H}(V)$.

Proof. Trivial. □

Proposition 95 (Injectivity of φ)**.**
The homomorphism defined in 94 is injective.

Proof. We suppose $\varphi(x) = \varphi(y)$ and we show $x = y$. No difficulties. □

Definition 96 (Homomorphism from $\mathcal{H}(V)$ to $V \times V^*$)**.**
The map $\psi : (z, x, y) \mapsto (x, y)$ defines a homomorphism from $\mathcal{H}(V)$ to $V \times V^*$.

Proof. Trivial. □

Proposition 97 (Surjectivity of ψ)**.**
The homomorphism defined in 96 is surjective.

Proof. Trivial. □

Proposition 98 (Short exact sequence)**.**
We have a short exact sequence $0 \to k \xrightarrow{\varphi} \mathcal{H}(V) \xrightarrow{\psi} V \times V^* \to 0$.

Proof. We check that the kernel of ψ is exactly the image of φ. □

Definition 99 ($\psi^{-1}(V)$)**.**
The pullback $V \times \{0\}$ by ψ defines a subgroup of $\mathcal{H}(V)$.

Proof. We check that it is a subgroup. □

Proposition 100 (Pullback is commutative)**.**
The subgroup defined in 99 is commutative.

Proof. Check that $h_1 * h2 = h2 * h1$. □

Proposition 101 (Pullback is normal)**.**
The subgroup defined in 99 is a normal subgroup of Heisenberg.

Proof. Check that $g * h * g^{-1} \in \psi^{-1}(V)$ for every $g \in \mathcal{H}(V)$ and $h \in \psi^{-1}(V)$. □

Proposition 102 (Maximality of the pullback)**.**
The subgroup defined in 99 is maximal among the commutative subgroups of $\mathcal{H}(V)$.

Proof. By contradiction. If it's not, then there exists Q a commutative subgroup such that $\psi^{-1}(V) \subset Q$ and $Q \neq \psi^{-1}(V)$. Let $q := (z, x, y) \in Q \backslash \psi^{-1}(V)$. In particular, we have for every $h = (a, b, 0) \in \psi^{-1}(V)$ that $x * h = h * x$. We compute this equality and find out that for every $b \in V$, $y(b) = 0$. Thus $y = 0$ and $q \in \psi^{-1}(V)$. Contradiction. □

Definition 103 ($\psi^{-1}(V)$)**.**
The pullback of $\{0\} \times V^*$ by ψ defines a subgroup of $\mathcal{H}(V)$.

Proof. We check the axioms. □

Proposition 104 (Commutativity of the pullback)**.**
The subgroup defined in 103 is commutative.

Proof. Check that $h_1 * h2 = h2 * h1$. □

Proposition 105 (Pullback is normal)**.**
The subgroup defined in 103 is ai normal subgroup of Heisenberg. .

Proof. Check that $g * h * g^{-1} \in \psi^{-1}(V^*)$ for every $g \in \mathcal{H}(V)$ and $h \in \psi^{-1}(V^*)$. □

Proposition 106 (Maximality of the pullback)**.**
The subgroup defined in 103 is maximal among the commutative subgroups of $\mathcal{H}(V)$.

Proof. By contradiction. If it's not, then there exists Q a commutative subgroup such that $\psi^{-1}(V^*) \subset Q$ and $Q \neq \psi^{-1}(V^*)$. Let $q := (z, x, y) \in Q \backslash \psi^{-1}(V^*)$. In particular, we have for every $h = (a, 0, b) \in \psi^{-1}(V^*)$ that $x * h = h * x$. We compute this equality and find out that for every $b \in V^*$, $b(x) = 0$. Thus $x = 0$ and $q \in \psi^{-1}(V^*)$. Contradiction. □

3.5 Specifities of the case $k = \mathbb{F}_q$

Proposition 107 (Cardinality)**.** *If k is a finite field, then $|\mathcal{H}(V)| = |k| \times |V|^2$.*

Proof. With 81 we know $\mathcal{H}(V) \cong k \times V \times V^*$. Because V is finite dimensional, $|V| = |V^*|$, thus we get the result. □

Proposition 108 (Cardinality of the center)**.** *If k is a finite field, then $|\mathcal{Z}_{\mathcal{H}(V)}| = |k|$.*

Proof. Trivial, the center being isomorphic to k. □

Theorem 109 (Index of the center)**.**
If k is a finite field, then $[\mathcal{H}(V) : \mathcal{Z}_{\mathcal{H}(V)}] = |V|^2$.

Proof. We use the fact that $[\mathcal{H}(V) : \mathcal{Z}_{\mathcal{H}(V)}] = \frac{|\mathcal{H}(V)|}{|\mathcal{Z}_{\mathcal{H}(V)}|}$. Given that $|\mathcal{H}(V)| = |k| \times |V|^2$ (because of 107) and $|\mathcal{Z}_{\mathcal{H}(V)}| = |k|$ (because of 108), we get the result. □