Alternate modules are subsymplectic

Clément Guérin*

April 26, 2016

Abstract

In this paper, an alternate module \((A, \phi)\) is a finite abelian group \(A\) with a \(\mathbb{Z}\)-bilinear application \(\phi : A \times A \to \mathbb{Q}/\mathbb{Z}\) which is alternate (i.e. zero on the diagonal). We shall prove that any alternate module is subsymplectic, i.e. if \((A, \phi)\) has a Lagrangian of cardinal \(n\) then there exists an abelian group \(B\) of order \(n\) such that \((A, \phi)\) is a submodule of the standard symplectic module \(B \times B^*\).

Keywords: alternate modules, symplectic modules, Lagrangians, finite abelian groups.
Mathematics Subject Classification: 20K01.

Contents

1 Definitions and statement of the result 2
2 Lagrangians in alternate modules 5
3 Any alternate module is subsymplectic 10
  3.1 Preliminaries ............................................. 11
  3.2 Proof of the fundamental lemma .......................... 15
  3.3 Proof of the theorem ...................................... 20
4 Remarks ..................................................... 20

*IRMA Institut de Recherche Mathématiques avancée, University of Strasbourg, 7 rue René Descartes, F-67084 Strasbourg, France, e-mail: guerin@math.unistra.fr
1 Definitions and statement of the result

Before stating the result, we give some standard definitions along with some properties regarding the alternate modules. The concept is defined by Wall in [Wal64] and by Tignol, Amitsur in [AT86]. Among the results, we will establish here, some might be directly read in those references and also in [TW15].

Let $A$ be an abelian group. If we are given an application $\phi : A \times A \to \mathbb{Q}/\mathbb{Z}$, then we say that $(A, \phi)$ is a bilinear module if $\phi$ is bilinear when $A$ is seen as a $\mathbb{Z}$-module. By definition, the underlying group of the bilinear module $(A, \phi)$ is $A$ and the associated bilinear form to $(A, \phi)$ is $\phi$.

In the sequel, all bilinear modules are assumed to be finite.

Let $(A, \phi)$ a bilinear module, we say that $(A, \phi)$ is an alternate module if $\phi(a, a) = 0$ for all $a \in A$. If $(A, \phi)$ is an alternate module, then for all $a,b \in A$:

\[
0 = \phi(a + b, a + b)
\]

\[
= \phi(a, a) + \phi(a, b) + \phi(b, a) + \phi(b, b)
\]

\[
= \phi(a, b) + \phi(b, a)
\]

since $(A, \phi)$ is alternate

by ”bilinearity”

since $(A, \phi)$ is alternate

Whence for all $a,b \in A$, $\phi(a, b) = -\phi(b, a)$. We will sum up this by saying that if $(A, \phi)$ is an alternate module then, in particular $\phi$ is anti-symmetric.

Let $(A, \phi)$ be an alternate module and $a, b \in A$, we say that $a$ is orthogonal to $b$ if $\phi(a, b) = 0$. Since $A$ is alternate, any element of $A$ is orthogonal to itself and the relation of orthogonality is symmetric by anti-symmetry of the bilinear form $\phi$.

Let $(A, \phi)$ be an alternate module and $S$ a subset of $A$. We define $S^\perp$ the orthogonal of $S$ as the subset of elements in $A$ which are orthogonal to $S$. One can directly check that $S^\perp$ is a subgroup of $A$.

Let $(A, \phi)$ be an alternate module and $B$ a subgroup of $A$ then the bilinear module induced by $A$ on $B : (B, \phi_{B \times B})$ is also an alternate module called the induced submodule on $B$ by $\phi$. 

2
Let \((A_1, \phi_1)\) and \((A_2, \phi_2)\) be two alternate modules, we define the **orthogonal sum** of those modules by :

\[(A_1, \phi_1) \perp \oplus (A_2, \phi_2) := (A, \phi)\]

With \(A := A_1 \oplus A_2\) and \(\phi((a_1, a_2), (b_1, b_2)) := \phi_1(a_1, b_1) + \phi_2(a_2, b_2)\). It is a straightforward verification that \((A, \phi)\) is an alternate module, verifying \(A_1 \leq A_2^\perp, A_2 \leq A_1^\perp\) and the induced submodule by \(\phi\) on \(A_i\) is \((A_i, \phi_i)\).

Conversely, if \((A, \phi)\) is an alternate module and \(B, C\) two subgroups of \(A\) such that \(A = B \oplus C\) with \(B \leq C^\perp\), then \((A, \phi)\) can be written as the orthogonal sum of the two induced modules on \(B\) and \(C\) by \(\phi\).

Let \(A\) be a finite module, we define \(A^*\), the **dual** of \(A\) as the group \(A^* := \text{Mor}(A, \mathbb{Q}/\mathbb{Z})\). A non-trivial result (direct consequence of the classification of finite abelian groups) states that \(A\) is isomorphic to \(A^*\) as a group. Remark that the isomorphism between \(A\) and \(A^*\) is not canonical.

Let \((A, \phi)\) be an alternate module, we define the **dual application** associated to \((A, \phi)\) as :

\[\phi^* : \begin{array}{c|cc}
A & A^* \\
\hline
a & \mapsto & b \mapsto \phi(a, b)
\end{array}\]

The **kernel** \(K_\phi\) of \((A, \phi)\) is, by definition, the kernel \(\text{Ker}(\phi^*)\) of the dual application \(\phi^*\). In other words, \(K_\phi = A^\perp\) i.e. the set of elements in \(A\) which are orthogonal to any element of \(A\).

Let \((A, \phi)\) be an alternate module, we say that \((A, \phi)\) is a **symplectic module** if its kernel \(K_\phi\) is trivial (i.e. the application \(\phi\) is non-degenerate).

To any alternate module \((A, \phi)\), we can associate a symplectic module \((B, \phi_B)\) setting \(B := A/K_\phi\) and :

\[\phi_B(a_1 \text{ mod } K_\phi, a_2 \text{ mod } K_\phi) := \phi(a_1, a_2)\]

The fact that \((B, \phi_B)\) is well defined and is a symplectic module is clear. This symplectic module will always be denoted \((A/K_\phi, \overline{\phi})\) and called the **symplectic module** associated to \((A, \phi)\).

An important example of symplectic module is the following :
Example 1. Let $B$ be an abelian group. We define $A := B \times B^*$ and :

$$
\phi : \begin{array}{c}
A \times A \longrightarrow \mathbb{Q}/\mathbb{Z} \\
((a_1, \psi_1), (a_2, \psi_2)) \longmapsto \psi_2(a_1) - \psi_1(a_2)
\end{array}
$$

Then $(A, \phi)$ is a symplectic module. In the sequel, such symplectic module will always be denoted $B \times B^*$ (the underlying bilinear form being the form $\phi$ as above).

Proof. Clearly $(A, \phi)$ is an alternate module. Let $(a, \psi)$ be in $K_\phi$ then for all $b \in A$ :

$$
\phi((a, \psi), (b, 0)) = 0 \Rightarrow \psi(b) = 0
$$

This implies that $\psi$ is the trivial morphism, i.e. $\psi = 0$. Furthermore for all $\psi' \in Mor(A, \mathbb{Q}/\mathbb{Z})$ :

$$
\phi((a, 0), (0, \psi')) = 0 \Rightarrow \psi'(a) = 0
$$

Since $A$ is isomorphic to $Mor(A, \mathbb{Q}/\mathbb{Z})$ (although the isomorphism is not canonical) this implies that $a = 0$. Therefore $K_\phi$ is trivial and $(A, \phi)$ is a symplectic module.

Let $(A, \phi)$ be an alternate module and $S$ a subset of $A$. We say that $S$ is isotropic if $S \subseteq S^\perp$. Furthermore, if $S = S^\perp$ then $S$ is a subgroup of $A$ and is called a Lagrangian of $(A, \phi)$. In general (see proposition 3) the cardinal of a Lagrangian of $(A, \phi)$ only depends on $|A|$ and $|K_\phi|$. We shall denote $n_{A,\phi} := \sqrt{|A||K_\phi|}$ the cardinal of any Lagrangian of $(A, \phi)$.

In the example the subgroups $B$ and $B^*$ of $A$ are both Lagrangians of the module $(A, \phi)$.

Let $(A, \phi)$ and $(A', \phi')$ be alternate modules, we say that $(A, \phi)$ and $(A', \phi')$ are isometric if there exists a group isomorphism $g : A \rightarrow A'$ verifying $\phi = g^*\phi'$. The isometric relation is clearly an equivalence relation.

Now, we come to the most important definition of this paper. Let $(A, \phi)$ be an alternate module. We say that $(A, \phi)$ is subsymplectic if there exists an abelian group $B$ of order $n_{A,\phi}$ such that $(A, \phi)$ is included in the standard symplectic module $B \times B^*$. The result we are going to prove here is :

Theorem. Any alternate module is subsymplectic.
 Whereas the classification of symplectic modules is easily dealt with, it seems hopeless to do the same thing for alternate modules in general. The statement that alternate modules are subsymplectic appears as the closest possible result to a classification of alternate modules.

In another paper, we will use this result to classify conjugacy classes of centralizers of irreducible subgroups in $PSL(n, \mathbb{C})$.

In the second section, we shall characterize and study the Lagrangians in alternate modules. In the third section we will prove the theorem. In the last section, we make some remarks about this proof and alternate modules in general.

\section{Lagrangians in alternate modules}

Some results in this section have been proven in other papers, we shall only give the references. We begin with an elementary proposition:

**Proposition 1.** Let $(A, \phi)$ be a symplectic module and $B$ a subgroup of $A$ then:

1. $|B||B^\perp| = |A|$ and $(B^\perp)^\perp = B$.

2. If the induced submodule on $B$ by $(A, \phi)$ is a symplectic module then the induced submodule on $B^\perp$ by $(A, \phi)$ is also a symplectic module, furthermore

$$A = B^\perp \oplus B^\perp$$

\textit{Proof.} See proposition 2.2 of [AT86] or lemma 1 in [Wal64].

Whereas, alternate modules are very hard to classify, the following property implies that any symplectic module is isometric to one constructed as in the example\[1\]. In particular, the set of symplectic modules is quite rigid.

**Corollary 1.** Let $(A, \phi)$ be a symplectic module. There exists $B \leq A$ such that $(A, \phi)$ is isomorphic to $B \times B^*$. 

5
Proof. See lemma 7 in [Wal64] or theorem 4.1 in [AT86].

This construction can be seen as the analogous of a symplectic base for \((A, \phi)\) (i.e. a "base" of \(B\) as a finite abelian group and its "dual base" in \(B^*\)). A direct consequence of this corollary is that any two symplectic modules \((A, \phi)\) and \((A', \phi')\) are isometric if and only if \(A\) and \(A'\) are isomorphic as groups.

It is, somehow, surprising that such symplectic base exists for those finite modules (in a similar fashion than for bilinear forms on \(K\)-vector spaces). Whereas \(K\)-vector spaces endowed with an alternate form (not necessarily symplectic) are always the sum of the kernel of the form and a non-degenerate complementary, this is not the case for alternate modules in general. Indeed, one can consider the following counter-example:

**Counter-example 1.** Let \(A := \mathbb{Z}/2 \times \mathbb{Z}/4 \times \mathbb{Z}/8\). We denote \(e_1 := (1, 0, 0), e_2 := (0, 1, 0)\) and \(e_3 := (0, 0, 1)\). Then, on the base \(e_1, e_2, e_3\), we define the alternate bilinear form \(\phi\) on \(A\) with its associated matrix:

\[
M_\phi := \begin{pmatrix}
0 & 1/2 & 1/2 \\
1/2 & 0 & -1/4 \\
1/2 & 1/4 & 0
\end{pmatrix}
\]

Then the kernel \(K_\phi\) of \((A, \phi)\) is not a direct factor of \(A\), in particular, \(A\) is not the sum of a non-degenerate module and its kernel.

Proof. With a straightforward computation, one can check that \(K_\phi = \langle e_1 + 2e_2 + 2e_3 \rangle\) is isomorphic to \(\mathbb{Z}/4\). We remark that \(2(e_1 + 2e_2 + 2e_3) = 4e_3 \in K_\phi\). Furthermore if \((x, y, z) \in A\) then \(4(x, y, z) = (0, 0, 4z)\) so any element \(a \in A\) of order \(8\) will verify that \(4a = 4e_3 \in K_\phi\). In particular, \(K_\phi\) is not a direct factor of \(A\).

This little example shows that the kernel of \((A, \phi)\) is not necessarily a direct factor of \(A\). Furthermore, one can check that \(A\) cannot be written as the orthogonal sum of strictly smaller submodules. In some sense, it is irreducible, this suggests that if there is a classification of alternate modules (in some sense, we would like to have one in the sequel), it should be complicated. Another corollary of the proposition:\

**Corollary 2.** Let \((A, \phi)\) be a symplectic module, then any Lagrangian \(L\) of \(A\) is of cardinal \(\sqrt{|A|}\).
Proof. By definition, $L = L^\perp$, applying the first point of proposition 1, we get $|L|^2 = |A|$.

In their paper, [AT86], J.-P. Tignol and S.A. Amitsur are interested in Lagrangian of symplectic modules, they apply this to division algebra (cf. [AT85]). We need to understand Lagrangians of alternate modules. We recall some results about Lagrangians in this case:

**Proposition 2.** Let $(A, \phi)$ be an alternate module. The Lagrangians of $A$ are exactly the maximal elements for the inclusion within the set of isotropic subsets of $A$. In other words a subset $L$ in $A$ is a Lagrangian of $A$ if and only if for any $K'$ isotropic subset of $A$ containing $L$, $K' = L$.

**Proof.** Let $L$ be an isotropic subset of $A$. Assume that $L$ is a Lagrangian, then if $K'$ is an isotropic subset of $A$ containing $L$, then $L^\perp \supseteq K'$ since $K'$ is orthogonal to $K'$ whence to $L$. Since $L$ is a Lagrangian, $L = L^\perp$ whence $K' \subseteq L$, since $K' \supseteq L$ by assumption $L = K'$ and $L$ is thus maximal among the isotropic subsets of $A$.

Assume that $L$ is not a Lagrangian. Since $L$ is isotropic, $L \subseteq L^\perp$ and there exists $a \in L^\perp$ which does not belong to $L$. We define $K' := \langle L, a \rangle$, clearly $L \subseteq K'$ and $K' \neq L$, furthermore $L$ being isotropic is orthogonal to $a$ by assumption, whence $K'$ is an isotropic subspace of $A$. Whence $L$ is not maximal among the isotropic subsets of $A$.

Let $(A, \phi)$ be an alternate module then the set of isotropic subspaces of $A$ is not empty (it contains the trivial group) and finite (since $A$ is finite). Therefore, there exists a maximal element for the inclusion. Whence any alternate module admits a Lagrangian. Furthermore, if $K$ is any isotropic subset, there will always be a maximal isotropic subset containing it, therefore any isotropic subset is contained in a Lagrangian. In particular, for any $a \in A$, there exists a Lagrangian containing $a$ (applying what we have just done to $K = \langle a \rangle$).

The next proposition is a generalization of corollary 2:

**Proposition 3.** Let $(A, \phi)$ be an alternate module. For any Lagrangian $L$ of $A$, the cardinal of $L$ is $\sqrt{|A||K_\phi|}$.
Proof. We define \((A/K, \phi)\) to be the associated symplectic module to \((A, \phi)\) and \(\pi\) be the projection of \(A\) onto \(A/K\). Clearly the application \(\pi\) leads to a bijective correspondence between isotropic subgroups of \(A\) containing \(K\) and isotropic subgroups of \(A/K\).

Since maximal elements among isotropic subsets of \(A\) are isotropic subgroups of \(A\) containing \(K\), it follows that \(\pi\) induces a bijective correspondence between Lagrangians in \(A\) and Lagrangians in \(A/K\) (by sending \(L\) to \(\pi(L)\)). In particular, any Lagrangian \(L\) of \(A\) is of the form \(\pi^{-1}(\overline{L})\) where \(\overline{L}\) is a Lagrangian in \(A/K\).

\[
|L| = |\pi^{-1}(\overline{L})| \\
= |K| |\overline{L}| \\
= |K| \sqrt{|A|/|K|} \quad \text{by corollary \[2\]} \\
= \sqrt{|A||K|}
\]

We see that the cardinal of Lagrangians is constant in alternate modules. However, the isomorphism class of Lagrangians may vary (see also \[AT86\]).

Example 2. Let \((A, \phi)\) be the alternate module defined in counter-example \[1\]. Then \(A = \mathbb{Z}/2 \times \mathbb{Z}/4 \times \mathbb{Z}/8\), and if we denote \(e_1 := (1, 0, 0)\), \(e_2 = (0, 1, 0)\) and \(e_3 = (0, 0, 1)\) in \(A\) then the subgroups \(L_1 := \langle e_3, e_1 + 2e_2 \rangle\) and \(L_2 := \langle e_1, 2e_2, 2e_3 \rangle\) are Lagrangians in \(A\) and:

- \(L_1\) is isomorphic to \(\mathbb{Z}/2 \times \mathbb{Z}/8\)
- \(L_2\) is isomorphic to \(\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/4\)

In particular, \(L_1\) is not isomorphic to \(L_2\).

Proof. From the counter-example \[1\] \(|K| = 4\), hence the cardinal of a Lagrangian in \((A, \phi)\) is \(\sqrt{2 \cdot 4 \cdot 8 \cdot 4} = 16\) using proposition \[3\].

We directly check that both \(L_1\) and \(L_2\) are isotropic.
Furthermore \( e_1 + 2e_2 \) is of order 2 and not in \( \langle e_3 \rangle \), therefore \( L_1 \) is isomorphic to \( \langle e_1 + 2e_2 \rangle \times \langle e_3 \rangle \). Whence \( L_1 \) is isomorphic to \( \mathbb{Z}/2 \times \mathbb{Z}/8 \). In particular, \( L_1 \) is isotropic and has the cardinal of a Lagrangian, by maximality of Lagrangians (proposition 2) it is Lagrangian.

Finally, \( L_2 \) is clearly isomorphic to \( \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/4 \). Likewise, the \( L_2 \) is isotropic of cardinal 16, by maximality of Lagrangians (proposition 2) it is Lagrangian.

In general, it is much more convenient to work with abelian \( p \)-groups than finite abelian groups. We remark that :

**Proposition 4.** Let \((A, \phi)\) be an alternate module such that \((A, \phi)\) is isometric to the orthogonal sum of \((A_1, \phi_1)\) and \((A_2, \phi_2)\) :

\[
(A, \phi) = (A_1, \phi_1) \perp (A_2, \phi_2)
\]

If both \((A_1, \phi_1)\) and \((A_2, \phi_2)\) are subsymplectic then \((A, \phi)\) is subsymplectic.

**Proof.** We begin by showing that \( K_\phi = K_{\phi_1} \oplus K_{\phi_2} \). Clearly, \( K_\phi \) contains \( K_{\phi_1} \) and \( K_{\phi_2} \) and both are in direct sum. Finally, if \( k = (l_1, l_2) \in K_\phi \leq A_1 \oplus A_2 \) then for all \( a_1 \in A_1 \), we have :

\[
0 = \phi(k, (a_1, 0)) = \phi_1(l_1, a_1) + \phi_2(l_2, 0) = \phi_1(l_1, a_1)
\]

This is true for any \( a_1 \in A_1 \) so \( l_1 \in K_{\phi_1} \). Likewise, \( l_2 \in K_{\phi_2} \), whence \( K_\phi = K_{\phi_1} \oplus K_{\phi_2} \).

It follows that \( |K_\phi| = |K_{\phi_1}||K_{\phi_2}| \), since \( |A| = |A_1||A_2| \), we have :

\[
n_{A,\phi} = n_{A_1,\phi_1}n_{A_2,\phi_2}
\]  

By hypothesis, for \( i = 1, 2 \), there exists \( B_i \), an abelian group of order \( n_{A_i,\phi_i} \) such that \((A_i, \phi_i) \leq B_i \times B_i^* \). Whence :

\[
(A, \phi) = (A_1, \phi_1) \perp (A_2, \phi_2)
\]

\[\leq (B_1 \times B_1^*) \perp (B_2 \times B_2^*)\]

\[\leq B \times B^* \text{ where } B := B_1 \times B_2\]
We have included \((A,\phi)\) (as an alternate module) in \(B \times B^*\), since \(|B| = |B_1||B_2| = n_{A_1,\phi_1}n_{A_2,\phi_2} = n_{A,\phi}\) by equation \(\PageIndex{1}\) it follows, by definition, that \((A,\phi)\) is subsymplectic.

\[\square\]

As a result:

**Corollary 3.** Let \((A,\phi)\) be an alternate module then, we denote, for \(p\) any prime dividing \(|A|\), \(S_p\) the unique \(p\)-Sylow of \(A\). If for all \(p\) dividing \(|A|\), the induced submodule on \(S_p\) by \(\phi\) is subsymplectic then \((A,\phi)\) is subsymplectic.

**Proof.** It is a well known result that if \(p_1,\ldots,p_r\) are the \(r\) distinct primes dividing \(|A|\) then, as a group, \(A\) is isomorphic to the product of its \(p\)-Sylows

\[A = S_{p_1} \oplus \cdots \oplus S_{p_r}\]

Furthermore, if \(1 \leq i \neq j \leq r\) and \(a_i \in S_{p_i}, a_j \in S_{p_j}\) then \(\phi(a_i,a_j)\) is of order dividing some power of \(p_i\) and some power of \(p_j\), it follows that \(\phi(a_i,a_j)\) is of order 1, i.e. is trivial. In particular, for \(i \neq j\), the induced modules \(S_{p_i}\) and \(S_{p_j}\) are orthogonal to each other. It follows that :

\[(A,\phi) = S_{p_1} \perp \cdots \perp S_{p_r}\]

The corollary is a direct consequence of this decomposition and proposition \(\PageIndex{4}\)

\[\square\]

With those classical properties, we will show the theorem.

### 3 Any alternate module is subsymplectic

Basically, the idea is to make an induction on the cardinal of the kernel. The following lemma is the major step of the proof:

**Fundamental lemma.** Let \(p\) be a prime number and \((A,\phi)\) an alternate module which is not symplectic with \(A\) a \(p\)-group. Then there exists an alternate module \((\hat{A},\hat{\phi})\) such that \((A,\phi)\) is a submodule of \((\hat{A},\hat{\phi})\), \(|A| < |\hat{A}|\) and \(n_{A,\phi} = n_{\hat{A},\hat{\phi}}\).
In the sequel, we will say that \((\hat{A}, \hat{\phi})\) is an extension of modules of \((A, \phi)\) via the inclusion \(\iota_A : A \to \hat{A}\) if \(\iota_A\) is an inclusion of alternate modules, i.e. \(\iota_A \hat{\phi} = \phi\) and \(\iota_A\) is an inclusion of modules. The extension will be with constant Lagrangians if \(n_{A,\hat{\phi}} = n_{A,\phi}\).

The first subsection gathers some preliminary results. The second subsection is the proof of the fundamental lemma. For subsections 3.1 and 3.2, \(p\) is a fixed prime number and any alternate module \((A, \phi)\) is assumed to have its underlying group \(A\) to be a \(p\)-group. In the third subsection, we prove the theorem.

### 3.1 Preliminaries

The next lemma is interesting in itself, it generalizes the second point of proposition \(\square\).

**Lemma 1.** Let \((A, \phi)\) be an alternate module. If there exists a submodule \(B\) of \((A, \phi)\) such that \(B\) is a symplectic module then :

\[(A, \phi)\text{ is isometric to } B \oplus B^\perp\]

**Proof.** Let \((A, \phi)\) be an alternate module and \(B\) be a submodule of \(A\) which is symplectic. Then \(B^\perp\) is also a submodule of \((A, \phi)\). Since \(B\) is symplectic, \(B^\perp \cap B\) is trivial. It follows that \(B \oplus B^\perp\) is a subgroup of \(A\). By definition, \(B\) is orthogonal to \(B^\perp\) it follows that :

\(B \oplus B^\perp\) is a submodule of \((A, \phi)\)

Let \(\pi\) be the canonical projection of \(A\) on \(A/K_\phi\). Since \(B\) is symplectic, \(B \cap K_\phi\) is trivial and \(B\) is isomorphic to \(\overline{B} := \pi(B)\). Using the first point of proposition \(\square\) :

\[
\overline{B}^\perp = \frac{|A/K_\phi|}{|\overline{B}|} = \frac{|A|}{|K_\phi||B|}
\]
Clearly, $\pi^{-1}(B^\perp) = B^\perp$, it follows that $|B^\perp| = |K_\phi||B^\perp|$. Finally, we have that:

$$|B \oplus B^\perp| = |B||B^\perp| = |B||K_\phi||B^\perp| = |B||K_\phi||A| = |A|$$

Since $B \oplus B^\perp$ is a submodule of $(A, \phi)$ and both modules have the same cardinal, we have that:

$$(A, \phi) \text{ is isometric to } B \oplus B^\perp$$

The next lemma gives a sufficient condition for an extension of modules to be with constant Lagrangians:

**Lemma 2.** Let $p$ be a prime number, $(\hat{A}, \hat{\phi})$ be an alternate module and $A$ be a subgroup of $\hat{A}$ of index $p$. We denote $(A, \phi)$ the induced submodule on $A$ by $\hat{\phi}$. If $K_\phi$ is not included in $K_{\hat{\phi}}$ then $n_{A,\phi} = n_{\hat{A},\hat{\phi}}$.

**Proof.** Let $\hat{e}$ be an element of $\hat{A}$ which is not in $A$. Since $[\hat{A} : A]$ is of cardinal $p$, any element in $\hat{a} \in \hat{A}$ can uniquely be written as:

$$\hat{a} = \lambda \hat{e} + a \text{ where } 0 \leq \lambda \leq p - 1 \text{ and } a \in A$$

Define:

$$f : \begin{array}{c}
K_\phi \\
\downarrow \\
\hat{K} \\
\downarrow \\
\hat{\phi}(\hat{e}, k)
\end{array}$$

Then for all $k \in K_\phi$:

$$p \cdot f(k) = p \cdot \hat{\phi}(\hat{e}, k) = \hat{\phi}(p\hat{e}, k) = \phi(p\hat{e}, k) \text{ since } p\hat{e} \text{ and } k \text{ are in } A = 0 \text{ since } k \in K_\phi \text{ and } p\hat{e} \in A$$
As a result $\text{Im}(f)$ is a finite subgroup of $\mathbb{Q}/\mathbb{Z}$ of exponent dividing $p$. Whence $\text{Im}(f)$ is either trivial or the unique cyclic subgroup of order $p$ in $\mathbb{Q}/\mathbb{Z}$.

If $\text{Im}(f)$ is trivial, then $K_\phi$ is orthogonal to $\hat{e}$, since $K_\phi$ is orthogonal to $A$ and $\hat{A}$ is generated by $\hat{e}$ and $A$, it follows that $K_\phi$ is orthogonal to $\hat{A}$, whence $K_\phi \leq K_{\hat{\phi}}$. By assumption, this is a contradiction. It follows that $\text{Im}(f)$ is cyclic of cardinal $p$.

Let $x = \lambda \hat{e} + a \in K_{\hat{\phi}}$ where $0 \leq \lambda \leq p - 1$ and $a \in A$. Let $k_0 \in K_\phi$ such that $f(k_0)$ is of order $p$. Since $x \in K_{\hat{\phi}}$, we have $\hat{\phi}(x, k_0) = 0$. On the other hand:

$$\hat{\phi}(x, k_0) = \lambda \hat{\phi}(\hat{e}, k_0) + \hat{\phi}(a, k_0) = \lambda f(k_0) + \phi(a, k_0) = \lambda f(k_0) + 0 \text{ since } k_0 \in K_\phi$$

It follows that $\lambda f(k_0) = 0$. Since $f(k_0)$ is of order $p$, we have that $p$ divides $\lambda$ and since $0 \leq \lambda \leq p - 1$, we end up with $\lambda = 0$ which implies that $x \in A$. As a result, we have shown that $K_{\hat{\phi}} \leq K_{\hat{\phi}}$.

Finally:

$$n_{\hat{A}, \hat{\phi}} = \sqrt{|\hat{A}||K_{\hat{\phi}}|} = \frac{\sqrt{p|A||K_\phi|}}{\sqrt{[K_\phi : K_{\hat{\phi}}]}} = \sqrt{\frac{p}{[K_\phi : K_{\hat{\phi}}]}} n_{A, \phi}$$

Let $L$ be a Lagrangian of $A$, then $L$ is isotropic in $\hat{A}$ and by proposition 2 there exists a Lagrangian $\hat{L}$ of $\hat{A}$ containing $L$. Using Lagrange’s theorem, we have that $|L|$ divides $|\hat{L}|$ and using proposition 3 $n_{A, \phi}$ divides $n_{\hat{A}, \hat{\phi}}$. It follows that $\sqrt{\frac{p}{[K_\phi : K_{\hat{\phi}}]}}$ is a positive integer which cannot but be equal to one (because $p$ is a prime number). In particular, we have that $n_{\hat{A}, \hat{\phi}} = n_{A, \phi}$. \(\blacksquare\)
The last lemma in those preleminaries allows us to construct extension of modules in a fairly simple way.

**Lemma 3.** Let \( p \) be a prime number, \((A, \phi)\) an alternate module where \( A \) is a \( p \) group. Assume that there exist \( r + 1 \) non-trivial elements \( e, e_1, \ldots, e_r \) in \( A \) such that:

\[
A = \langle e \rangle \times \langle e_1 \rangle \times \cdots \times \langle e_r \rangle
\]

Assume furthermore that for any \( 1 \leq i \leq r \) the order of \( \phi(e, e_i) \) is strictly lesser than the order of \( e_i \) then there exists an alternate module \((\hat{A}, \hat{\phi})\) such that \( \hat{A} = \langle \hat{e} \rangle \times \langle e_1 \rangle \times \cdots \times \langle e_r \rangle \) where \( \hat{e} \) is of order \( p \) times the order of \( e \) and the inclusion:

\[
\iota_A : \begin{array}{c|c}
A & \hat{A} \\
\hline
\hat{e} & p\hat{e} \\
e_i & e_i \text{ for } 1 \leq i \leq r \\
\end{array}
\]

is an inclusion of submodules.

**Proof.** Let \( \hat{A} \) be \( \langle \hat{e} \rangle \times \langle e_1 \rangle \times \cdots \times \langle e_r \rangle \) where \( \hat{e} \) is of order \( p \) times the order of \( e \). Clearly, the mapping:

\[
\iota_A : \begin{array}{c|c}
A & \hat{A} \\
\hline
\hat{e} & p\hat{e} \\
e_i & e_i \text{ for } 1 \leq i \leq r \\
\end{array}
\]

defines an injective morphism of groups. In order to define the bilinear form \( \hat{\phi} \), it suffices to define it on a generating set of \( A \times \hat{A} \). Define:

\[
\hat{\phi}(e_i, e_j) := \phi(e_i, e_j) \text{ for all } 1 \leq i, j \leq r
\]

We also define \( \hat{\phi}(\hat{e}, \hat{e}) := 0 \). Finally, remark that the group \( \mathbb{Q}/\mathbb{Z} \) is \( p \)-divisible (i.e. any element admits a \( p \)-th root). Then for any \( 1 \leq i \leq r \), define \( \lambda_i \) to be one element verifying \( p\lambda_i = \phi(e, e_i) \).

Remark that the order of \( \lambda_i \) thus defined divides \( p \) times the order of \( \phi(e, e_i) \). By assumption, this divides the order of \( e_i \) and also divides the order of \( \hat{e} \) which is \( p \) times the order of \( e \). It follows that \( \lambda_i \) divides both the order of \( \hat{e} \) and \( e_i \). Whence the following equations:
\[ \hat{\phi}(e_i, e_j) := \phi(e_i, e_j) \text{ for all } 1 \leq i, j \leq r \]
\[ \hat{\phi}(\hat{e}, \hat{e}) := 0 \]
\[ \hat{\phi}(\hat{e}, e_i) := \lambda_i \]
\[ \hat{\phi}(e_i, \hat{e}) := -\lambda_i \]

allow us to define a group morphism on \( \hat{A} \) which is clearly an alternate module. Let \( \psi \) be the induced module on \( A \) via \( \iota_A \) by \( \hat{\phi} \):

\[ \psi(e_i, e_j) = \hat{\phi}(e_i, e_j) = \phi(e_i, e_j) \text{ for all } 1 \leq i, j \leq r \]
\[ \psi(e, e_j) = \hat{\phi}(p\hat{e}, e_j) = p\lambda_j = \phi(e, e_j) \text{ for all } 1 \leq j \leq r \]

Whence \( \psi = \phi \) on \( A \times A \) (since they are alternate forms). In particular we have shown that \((A, \phi)\) is a submodule of \((\hat{A}, \hat{\phi})\) via \( \iota_A \).

We have the tools to prove the fundamental lemma.

### 3.2 Proof of the fundamental lemma

We recall first the statement of the fundamental lemma:

**Fundamental lemma.** Let \( p \) be a prime number and \((A, \phi)\) an alternate module which is not symplectic with \( A \) a \( p \)-group. Then there exists an alternate module \((\hat{A}, \hat{\phi})\) such that \((A, \phi)\) is a submodule of \((\hat{A}, \hat{\phi})\), \(|A| < |\hat{A}|\) and \( n_{A, \phi} = n_{\hat{A}, \hat{\phi}} \).

**Proof.** We prove the lemma doing a strong induction on the cardinal of the module. Let \( p^k \) be such that the lemma is true for any alternate module \( M \) with \(|M| < p^k\). Let \((A, \phi)\) be an alternate module which is not symplectic and \( A \) be of cardinal \( p^k \). There are two different cases to consider:

**Case 1:** \( K_\phi \) is not included in \( p \cdot A \)
By the classification of abelian $p$-groups, decompose the group $A$ as a product of cyclic subgroups:

$$A = \langle e_0 \rangle \times \langle e_1 \rangle \times \cdots \times \langle e_r \rangle \quad (2)$$

Denote $d_i$ the order of $e_i$, then we may assume that $d_{i-1}$ divides $d_i$ for $1 \leq i \leq r$.

Let $k_0 \in K_\phi$ which is not in $p \cdot A$. By the decomposition 2, we may write

$$k_0 = \sum_{i=0}^{r} \alpha_i e_i \text{ where } \alpha_0, \ldots, \alpha_r \in \mathbb{N}$$

Since $k_0$ is not in $p \cdot A$ there exists at least one coefficient among the $\alpha_0, \ldots, \alpha_r$ which is not divisible by $p$. Denote $i_0$ to be one index such that $\alpha_{i_0}$ is not divisible by $p$.

Define the group $\hat{A} := \mathbb{Z}/p \times A$. Let $\gamma$ be a generator of $\mathbb{Z}/p$. Then we define an alternate form $\hat{\phi}$ on $\hat{A}$ by:

$$\hat{\phi}(e_i, e_j) := \phi(e_i, e_j) \text{ for } 0 \leq i, j \leq r$$
$$\hat{\phi}(\gamma, e_i) := 0 \text{ for } 0 \leq i \leq r \text{ and } i \neq i_0$$
$$\hat{\phi}(e_i, \gamma) := 0 \text{ for } 0 \leq i \leq r \text{ and } i \neq i_0$$
$$\hat{\phi}(\gamma, \gamma) := 0$$
$$\hat{\phi}(\gamma, e_{i_0}) := \frac{1}{p}$$
$$\hat{\phi}(e_{i_0}, \gamma) := -\frac{1}{p}$$

Clearly, $\hat{\phi}$ is an alternate form on $\hat{A}$, furthermore, the inclusion of $A$ in $\hat{A}$ given by $a$ is mapped to $(0, a)$ clearly leads to an inclusion of modules.

Finally:
\[ \hat{\phi}(\gamma, k_0) = \sum_{i=0}^{r} \alpha_i \hat{\phi}(\gamma, e_i) \]

\[ = \alpha_{i_0} \hat{\phi}(\gamma, e_{i_0}) \text{ since } \gamma \text{ is orthogonal to } e_i \text{ where } i \neq i_0 \]

\[ = \frac{\alpha_{i_0}}{p} \neq 0 \text{ in } \mathbb{Q}/\mathbb{Z} \text{ since } p \text{ does not divide } \alpha_{i_0} \]

Hence we found an element in \( K_\phi \) which is not in the kernel of \( K_\hat{\phi} \).

Applying lemma 2, we have \( n_{A,\phi} = n_{A,\hat{\phi}} \), hence \( (\hat{A}, \hat{\phi}) \) contains \( (A, \phi) \), has the same cardinality of Lagrangians and is strictly greater than \( A \). In this case, we have constructed the extension with constant Lagrangians (without using the induction hypothesis).

Case 2 : \( K_\phi \) is included in \( p \cdot A \)

Write:

\[ A = \langle e \rangle \times \langle e_1 \rangle \times \cdots \times \langle e_r \rangle \tag{3} \]

Denote \( d \) the order of \( e \), \( d_i \) the order of \( e_i \), then we may assume that \( d \) divides \( d_1 \) and \( d_i \) divides \( d_{i+1} \) for \( 1 \leq i \leq r - 1 \).

Assume that there exists \( 1 \leq i \leq r \) such that the order of \( \phi(e, e_i) \) is equal to \( d_i \) (the order of \( e_i \)), since the order of \( \phi(e, e_i) \) divides \( d \), the order of \( e \) (by bilinearity), it follows that \( d_i \) divides \( d \). Since we also have \( d \) divides \( d_i \) by definition, we have two elements \( e \) and \( e_i \) in \( A \) whose order is equal to \( d \) and such that \( \phi(e, e_i) \) is of order \( d \). As a result, the submodule \( B \) generated by \( e \) and \( e_i \) is isometric to \( \mathbb{Z}/d \times (\mathbb{Z}/d)^* \). In particular \( B \) is a submodule of \( (A, \phi) \) which is symplectic, by lemma 1, it follows that:

\[ (A, \phi) = B \perp B^\perp \]

Let \( (B^\perp, \psi) \) be the induced submodule on \( B^\perp \) by \( \phi \). By induction hypothesis, there exists a module \( (C, \hat{\psi}) \) such that \( n_{B^\perp, \psi} = n_{C, \hat{\psi}} \) with \( |B^\perp| < |C| \) and \( (B^\perp, \psi) \) is a submodule of \( (C, \hat{\psi}) \). Denote:

\[ (\hat{A}, \hat{\phi}) := B \perp (C, \hat{\psi}) \]
Clearly $A = B \perp B^\perp$ is a submodule of $(\hat{A}, \hat{\phi})$ and $|A| < |\hat{A}|$. Remark that $K_\phi = K_\psi$ and $\hat{K}_\phi = \hat{K}_\psi$ since $B$ is symplectic. Whence :

$$n_{A,\phi} = \sqrt{|A||K_\phi|}$$

$$= \sqrt{|B|\sqrt{|B^\perp||K_\psi|}}$$

$$= \sqrt{|B|n_{B^\perp,\psi}}$$

$$= \sqrt{|B|n_{C,\hat{\psi}} \text{ by construction of } (C, \hat{\psi})}$$

$$= \sqrt{|B|\sqrt{|C||K_{\psi}|}}$$

$$= \sqrt{|\hat{A}||K_{\hat{\phi}}|}$$

$$= n_{\hat{A},\hat{\phi}}$$

In this case we can also construct an extension $(\hat{A}, \hat{\phi})$ of $(A, \phi)$ with constant Lagrangians.

Assume now that for $1 \leq i \leq r$, the order of $\phi(e, e_i)$ strictly divides the order of $d_i$. Then we are in the condition of applications of lemma 3. Define $\hat{A} = \langle \hat{e} \rangle \times \langle e_1 \rangle \times \cdots \times \langle e_r \rangle$ where $\hat{e}$ is of order $p$ times the order of $e$ and the inclusion :

$$\iota_A : \begin{align*}
A & \longrightarrow \hat{A} \\
 e & \longmapsto p\hat{e} \\
 e_i & \longmapsto e_i \text{ for } 1 \leq i \leq r
\end{align*}$$

then we have defined on $\hat{A}$ a bilinear form $\hat{\phi}$ such that $\iota_A \star \hat{\phi} = \phi$.

We recall that we are in the second case where $K_\phi \leq p \cdot A$. Denote $\pi$ the canonical projection of $A$ onto $A/K_\phi$. Since $K_\phi \leq p \cdot A$, it follows that $\pi^{-1}(p \cdot (A/K_\phi)) = p \cdot A$. In particular (since $e$ is clearly not an element of $p \cdot A$) it follows that $\pi(e)$ is not in $p \cdot (A/K_\phi)$.

We know that $A/K_\phi$ is isomorphic to $B \times B^*$ by corollary 1. Denote $g_1, \ldots, g_s$ a ”base” of $B$ and $g_1^*, \ldots, g_s^*$ the corresponding ”dual base” of $B^*$ and write :
\[ \pi(e) = \sum_{i=1}^{r} \gamma_i g_i + \gamma_i^* g_i^* \]

Since \( \pi(e) \) is not in \( p \cdot (A/K_\phi) \), it follows that at least one of the \( \gamma_i \) or \( \gamma_i^* \) is not divisible by \( p \). Up to exchanging \( g_i \) and \( g_i^* \), we may assume that \( \gamma_i^* \) is not divisible by \( p \).

Let \( p^k \) (with \( k \geq 1 \)) be the order of \( g_{i_0} \) and \( a_0 \in A \) such that \( \pi(a_0) = g_{i_0} \). Since \( g_{i_0} \) is of order \( p^k \), \( p^k \cdot a_0 \in K_\phi \). Furthermore:

\[
\phi(e, p^{k-1} \cdot a_0) = \overline{\phi}(\pi(e), p^{k-1} \cdot \pi(a_0)) \text{ by definition of } (A/K_\phi, \overline{\phi}) \\
= p^{k-1} \overline{\phi}(\pi(e), g_{i_0}) \\
= p^{k-1} \sum_{i=1}^{r} \gamma_i \overline{\phi}(g_i, g_{i_0}) + \gamma_i^* \overline{\phi}(g_i^*, g_{i_0}) \\
= p^{k-1} \gamma_{i_0}^* \overline{\phi}(g_{i_0}^*, g_{i_0})
\]

Remark that, by definition \( \overline{\phi}(g_{i_0}^*, g_{i_0}) \) is of order \( p^k \), since \( \gamma_{i_0}^* \) is not divisible by \( p \):

\[
\phi(e, p^{k-1} \cdot a_0) = p^{k-1} \gamma_{i_0}^* \overline{\phi}(g_{i_0}^*, g_{i_0}) \text{ is of order } p, \text{ whence not trivial.}
\]

Remark now that, in \( (\hat{A}, \hat{\phi}) \) we have:

\[
\hat{\phi}(\hat{e}, p^k \cdot a_0) = \hat{\phi}(p \cdot \hat{e}, p^{k-1} \cdot a_0) \text{ by } \mathbb{Z} \text{-bilinearity} \\
= \phi(e, p^{k-1} \cdot a_0) \text{ since } p \cdot \hat{e} = \iota_A(e) \text{ and } \iota_A \circ \hat{\phi} = \phi \\
\neq 0 \text{ in } \mathbb{Q}/\mathbb{Z}
\]

In particular, \( p^k \cdot a_0 \) is an element of \( K_\phi \) which is not in \( K_{\hat{\phi}} \). Applying lemma \( [2] \) we have that \( n_{A,\phi} = n_{\hat{A},\hat{\phi}} \).

Now that the fundamental lemma is proven, we shall see that the theorem follows by an easy induction on the cardinal of the kernel of the alternate module.
3.3 Proof of the theorem

Recalling that the result we want to prove is the following theorem :

**Theorem.** Any alternate module is subsymplectic.

**Proof.** By corollary 3, it suffices to prove it for alternate modules \((A, \phi)\) where \(A\) is a \(p\)-group and \(p\) is a prime number.

Let us show the following by induction on \(k\) : Let \((A, \phi)\) be an alternate module which is a \(p\)-group with \(|K_\phi| = p^k\) then \((A, \phi)\) is subsymplectic.

If \(k = 0\) then \((A, \phi)\) is symplectic. Therefore, by corollary 1, it is isometric to \(B \times B^*\) where \(|B| = \sqrt{|A|} = n_{A,\phi}\). It follows that \((A, \phi)\) is subsymplectic by definition.

If \(k > 0\) then \((A, \phi)\) is an alternate module which is not symplectic (its kernel is not trivial) whence, by the fundamental lemma, there exists an alternate module \((\hat{A}, \hat{\phi})\) such that \((A, \phi)\) is a submodule of \((\hat{A}, \hat{\phi})\), \(|A| < |\hat{A}|\) and \(n_{A,\phi} = n_{\hat{A},\hat{\phi}}\).

We have \(n_{A,\phi}^2 = n_{\hat{A},\hat{\phi}}^2\), so \(|A||K_\phi| = |\hat{A}||K_{\hat{\phi}}|\), since \(|A| < |\hat{A}|\) we have that \(|K_{\hat{\phi}}| < |K_\phi| = p^k\). It follows that we can apply the induction hypothesis to \((\hat{A}, \hat{\phi})\) and there exists an abelian group \(B\) of order \(n := n_{\hat{A},\hat{\phi}}\) such that :

\[
(\hat{A}, \hat{\phi}) \leq B \times B^*
\]

Since \((A, \phi)\) is a submodule of \((\hat{A}, \hat{\phi})\), we finally have included the module \((A, \phi)\) in \(B \times B^*\) where \(|B| = n = n_{\hat{A},\hat{\phi}} = n_{A,\phi}\). It follows that \((A, \phi)\) is subsymplectic by definition. \(\square\)

4 Remarks

The proof is constructive. Indeed, it explicitely gives the construction (by induction) of a symplectic module \(B \times B^*\) containing \((A, \phi)\) with \(|B| = n_{A,\phi}\). Basically, in order to define an algorithm computing \(B\), one needs an
algorithm that, given \((A, \phi)\) computes its kernel and a ”diagonalization” of its associated symplectic module \((A/K, \overline{\phi})\).

Remark that, given \((A, \phi)\), an alternate module, there might exist \(B_1 \neq B_2\), both of cardinal \(n_{A, \phi}\) such that \((A, \phi)\) is included in \(B_i \times B_i^*\) for \(i = 1, 2\):

**Counter-example 2.** Let \(A\) be the abelian group \(\mathbb{Z}/2 \times \mathbb{Z}/4\) endowed with the trivial bilinear form. It follows that \(n_{A, \phi} = |A|\). Let \(B_1 := A\) and \(B_2 := \mathbb{Z}/8\). Then we have two inclusions:

\[
\iota_{A,1} : \begin{cases} 
A \to B_1 \times B_1^* \\
(u, v) \mapsto (u, v, (0, 0))
\end{cases}
\text{ and } \iota_{A,2} : \begin{cases} 
A \to B_2 \times B_2^* \\
(u, v) \mapsto (4u, 2v)
\end{cases}
\]

Those two inclusions are inclusions of submodules (when \(B_i \times B_i^*\) is endowed with its natural structure of symplectic form, defined in example 1). Furthermore, it is clear that they are extensions with constant Lagrangians. However \(B_1 \neq B_2\).

As we have stated in the introduction of this paper, the theorem will be used in another paper in order to give a classification of centralizer of irreducible subgroups of \(PSL(n, \mathbb{C})\). An interesting thing to have would be a classification of alternate modules.

Let \((A, \phi)\) be an alternate module, we say that \((A, \phi)\) is **indecomposable** if, whenever \((A, \phi)\) is the orthogonal sum of \((A_1, \phi_1)\) and \((A_2, \phi_2)\) then \((A_1, \phi_1)\) or \((A_2, \phi_2)\) is \((\{0\}, 0)\).

Since any alternate module is clearly the sum of indecomposable ones by induction, if we want to classify alternate modules, we only need to characterize indecomposable ones. This leads to the following question:

**Question.** Let \((A, \phi)\) be an indecomposable alternate module. Does it follow that \(rk(A) \leq 3\)? Does it follow that \(rk(A/K, \phi) \leq 2\)?

We computed many examples and this conjecture seems to be verified. However we still do not have a proof for it.
Acknowledgements

All computations performed on examples leading to this result have been performed using the GAP system [GAP].

I would like to thank my thesis advisor Olivier Guichard, whose suggestions have been very helpful. I would also like to thank Gaël Collinet who encouraged me to fully investigate this topic and Jean-Pierre Tignol for pointing out some helpful references. Finally, I would like to thank my fellow Ph.D student, Mohamad Maassarani for carefully listening to my proofs and his helpful comments.

References

[AT85] S.A. Amitsur, J.-P. Tignol. Kummer subfields of Malcev-Neumann division algebras. Israel Journal of mathematics, Vol. 50, Nos 1-2, 1985.

[AT86] S.A. Amitsur, J.-P. Tignol. Symplectic modules. Israel Journal of mathematics, Vol. 54, No 3, 1986.

[GAP] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.8.3; 2016, (http://www.gap-system.org).

[TW15] J.-P. Tignol, A. Wadsworth. Value Functions on Simple Algebras, and Associated Graded Rings. Springer Monographs in Mathematics, 2015.

[Wal64] C.T.C. Wall. Quadratic forms on finite groups, and related topics. Topology, Vol. 2:281-298, 1964.