Sur Les Codes Indecomposables Abéliens

M. BOULAGOUAZ

Faculté des Sciences et Techniques
Fès, Maroc

Noncommutative Rings
and
their Applications
LENS, 29 June - 2 July 2009

REMARQUES

1. Il est nécessaire d'avoir des codes longs pour obtenir des codes ayant une distance minimale de Hamming importante.
(et donc un fort pouvoir de correction).
2. Théoriquement il est possible de construire des codes ayant une DHM élevée. Mais :
2.a- Sans structure particulière, il est presque impossible de décoder ces codes.
2.b- Cependant même avec des codes ayant une structure algébrique,dans les constructions classique,la complexité de décodage de tels codes devient prohibitive,
3. L'invention des **codes produits**, permet de contourner ce problème :
en utilisant des codes simples à faible pouvoir de correction mais dont le décodage est peu coûteux, il est possible de les assembler pour obtenir un code plus long dont le pouvoir de correction est imortant.

REMARQUES

1. Il est nécessaire d'avoir des codes longs pour obtenir des codes ayant une distance minimale de Hamming importante.
(et donc un fort pouvoir de correction).

2. Théoriquement il est possible de construire des codes ayant une DHM élevée. Mais :

2.a- Sans structure particulière, il est presque impossible de décoder ces codes.

2.b- Cependant même avec des codes ayant une structure algébrique,dans les constructions classique,la complexité de décodage de tels codes devient prohibitive,

3. L'invention des **codes produits**, permet de contourner ce problème :
en utilisant des codes simples à faible pouvoir de correction mais dont le décodage est peu coûteux, il est possible de les assembler pour obtenir un code plus long dont le pouvoir de correction est imortant.

REMARQUES

1. Il est nécessaire d'avoir des codes longs pour obtenir des codes ayant une distance minimale de Hamming importante.
(et donc un fort pouvoir de correction).
2. Théoriquement il est possible de construire des codes ayant une DHM élevée. Mais :
2.a- Sans structure particulière, il est presque impossible de décoder ces codes.
2.b- Cependant même avec des codes ayant une structure algébrique,dans les constructions classique,la complexité de décodage de tels codes devient prohibitive,
3. L'invention des **codes produits**, permet de contourner ce problème :
en utilisant des codes simples à faible pouvoir de correction mais dont le décodage est peu coûteux, il est possible de les assembler pour obtenir un code plus long dont le pouvoir de correction est imortant.

REMARQUES

1. Il est nécessaire d'avoir des codes longs pour obtenir des codes ayant une distance minimale de Hamming importante.
(et donc un fort pouvoir de correction).
2. Théoriquement il est possible de construire des codes ayant une DHM élevée. Mais :
2.a- Sans structure particulière, il est presque impossible de décoder ces codes.
2.b- Cependant même avec des codes ayant une structure algébrique,dans les constructions classique,la complexité de décodage de tels codes devient prohibitive,
3. L'invention des **codes produits**, permet de contourner ce problème :
en utilisant des codes simples à faible pouvoir de correction mais dont le décodage est peu coûteux, il est possible de les assembler pour obtenir un code plus long dont le pouvoir de correction est imortant.

REMARQUES

1. Il est nécessaire d'avoir des codes longs pour obtenir des codes ayant une distance minimale de Hamming importante.
(et donc un fort pouvoir de correction).
2. Théoriquement il est possible de construire des codes ayant une DHM élevée. Mais :
2.a- Sans structure particulière, il est presque impossible de décoder ces codes.
2.b- Cependant même avec des codes ayant une structure algébrique,dans les constructions classique,la complexité de décodage de tels codes devient prohibitive,
3. L'invention des **codes produits**, permet de contourner ce problème :
en utilisant des codes simples à faible pouvoir de correction mais dont le décodage est peu coûteux, il est possible de les assembler pour obtenir un code plus long dont le pouvoir de correction est imortant.

REMARQUES

1. Il est nécessaire d'avoir des codes longs pour obtenir des codes ayant une distance minimale de Hamming importante.
(et donc un fort pouvoir de correction).
2. Théoriquement il est possible de construire des codes ayant une DHM élevée. Mais :
2.a- Sans structure particulière, il est presque impossible de décoder ces codes.
2.b- Cependant même avec des codes ayant une structure algébrique,dans les constructions classique,la complexité de décodage de tels codes devient prohibitive,
3. L'invention des **codes produits**, permet de contourner ce problème :
en utilisant des codes simples à faible pouvoir de correction mais dont le décodage est peu coûteux, il est possible de les assembler pour obtenir un code plus long dont le pouvoir de correction est imortant.

REMARQUES

1. Il est nécessaire d'avoir des codes longs pour obtenir des codes ayant une distance minimale de Hamming importante.
(et donc un fort pouvoir de correction).
2. Théoriquement il est possible de construire des codes ayant une DHM élevée. Mais :
2.a- Sans structure particulière, il est presque impossible de décoder ces codes.
2.b- Cependant même avec des codes ayant une structure algébrique,dans les constructions classique,la complexité de décodage de tels codes devient prohibitive,
3. L'invention des **codes produits**, permet de contourner ce problème :
en utilisant des codes simples à faible pouvoir de correction mais dont le décodage est peu coûteux, il est possible de les assembler pour obtenir un code plus long dont le pouvoir de correction est imortant.

REMARQUES

1. Il est nécessaire d'avoir des codes longs pour obtenir des codes ayant une distance minimale de Hamming importante.
(et donc un fort pouvoir de correction).
2. Théoriquement il est possible de construire des codes ayant une DHM élevée. Mais :
2.a- Sans structure particulière, il est presque impossible de décoder ces codes.
2.b- Cependant même avec des codes ayant une structure algébrique,dans les constructions classique,la complexité de décodage de tels codes devient prohibitive,
3. L'invention des **codes produits**, permet de contourner ce problème :
en utilisant des codes simples à faible pouvoir de correction mais dont le décodage est peu coûteux, il est possible de les assembler pour obtenir un code plus long dont le pouvoir de correction est imortant.

REMARQUES

1. Il est nécessaire d'avoir des codes longs pour obtenir des codes ayant une distance minimale de Hamming importante.
(et donc un fort pouvoir de correction).
2. Théoriquement il est possible de construire des codes ayant une DHM élevée. Mais :
2.a- Sans structure particulière, il est presque impossible de décoder ces codes.
2.b- Cependant même avec des codes ayant une structure algébrique,dans les constructions classique,la complexité de décodage de tels codes devient prohibitive,
3. L'invention des **codes produits**, permet de contourner ce problème :
en utilisant des codes simples à faible pouvoir de correction mais dont le décodage est peu coûteux, il est possible de les assembler pour obtenir un code plus long dont le pouvoir de correction est imortant.

Codes produits

DEFINITION.1 : Soient C_1 et C_2 deux codes linéaires de longueurs respectives n_1 et n_2 et de dimension respectives k_1 et k_2. Le code produit $C = C_1 \otimes C_2$ est l'ensemble des matrices M de taille $n_1 \times n_2$ telles que :

1.Chaque ligne est un mot de code de C_1,

2.Chaque colonne est un mot de code de C_2.

Ce code est un code linéaire de longueur $n_1 \times n_2$, de dimension $k_1 \times k_2$ et de distance minimale $d_1 \times d_2$

Buts et hypothèses générales

Le but de cet exposé est de :

1. Introduire les codes indécomposables
2. Donner des ingrédients pour une généralisation d'un théorème de K.H. Zimmermann, Trasactions of information Theory, Vol. 37, en Nov 1991.

Théorème exprimant la distance minimale d'un code indécomposable abéilen M comme produit de la distance minimale d'un code abélien semisimple et de la distance minimale du module source de M.

Dans toute la suite :
- Les groupes considérés sont supposés finis.
- F est un corps de caractéristique $\neq 0$ et G un groupe multiplicatif.

Buts et hypothèses générales

Le but de cet exposé est de :

1. Introduire les codes indécomposables
2. Donner des ingrédients pour une généralisation d'un théorème de K.H. Zimmermann, Trasactions of information Theory, Vol. 37, en Nov 1991.

Théorème exprimant la distance minimale d'un code indécomposable abéilen M comme produit de la distance minimale d'un code abélien semisimple et de la distance minimale du module source de M.

Dans toute la suite :

- Les groupes considérés sont supposés finis.
- F est un corps de caractéristique $\neq 0$ et G un groupe multiplicatif.

Buts et hypothèses générales

Le but de cet exposé est de :

1. Introduire les codes indécomposables

2. Donner des ingrédients pour une généralisation d'un théorème de K.H. Zimmermann, Trasactions of information Theory, Vol. 37, en Nov 1991.

Théorème exprimant la distance minimale d'un code indécomposable abéilen M comme produit de la distance minimale d'un code abélien semisimple et de la distance minimale du module source de M.

Dans toute la suite :

- Les groupes considérés sont supposés finis.
- F est un corps de caractéristique $\neq 0$ et G un groupe multiplicatif.

Buts et hypothèses générales

Le but de cet exposé est de :

1. Introduire les codes indécomposables

2. Donner des ingrédients pour une généralisation d'un théorème de K.H. Zimmermann, Trasactions of information Theory, Vol. 37, en Nov 1991.

Théorème exprimant la distance minimale d'un code indécomposable abéilen M comme produit de la distance minimale d'un code abélien semisimple et de la distance minimale du module source de M.

Dans toute la suite :

- Les groupes considérés sont supposés finis.
- F est un corps de caractéristique $\neq 0$ et G un groupe multiplicatif.

Buts et hypothèses générales

Le but de cet exposé est de :
1. Introduire les codes indécomposables
2. Donner des ingrédients pour une généralisation d'un théorème de K.H. Zimmermann, Trasactions of information Theory, Vol. 37, en Nov 1991.
Théorème exprimant la distance minimale d'un code indécomposable abéilen M comme produit de la distance minimale d'un code abélien semisimple et de la distance minimale du module source de M.

Dans toute la suite :
- Les groupes considérés sont supposés finis.
- F est un corps de caractéristique $\neq 0$ et G un groupe multiplicatif.

Buts et hypothèses générales

Le but de cet exposé est de :
1. Introduire les codes indécomposables
2. Donner des ingrédients pour une généralisation d'un théorème de K.H. Zimmermann, Trasactions of information Theory, Vol. 37, en Nov 1991.
Théorème exprimant la distance minimale d'un code indécomposable abéilen M comme produit de la distance minimale d'un code abélien semisimple et de la distance minimale du module source de M.

Dans toute la suite :
- Les groupes considérés sont supposés finis.
- F est un corps de caractéristique $\neq 0$ et G un groupe multiplicatif.

Buts et hypothèses générales

Le but de cet exposé est de :
1. Introduire les codes indécomposables
2. Donner des ingrédients pour une généralisation d'un théorème de K.H. Zimmermann, Trasactions of information Theory, Vol. 37, en Nov 1991.
Théorème exprimant la distance minimale d'un code indécomposable abéilen M comme produit de la distance minimale d'un code abélien semisimple et de la distance minimale du module source de M.

Dans toute la suite :
- Les groupes considérés sont supposés finis.
- F est un corps de caractéristique $\neq 0$ et G un groupe multiplicatif.

Définitions

DEFINITION.2 :On appelle algèbre du groupe G sur le corps F, l'algèbre dont :

1. l'ensemble des éléments est celui de toutes les combinaisons linéaires des éléments de G à coefficients dans F : $\sum_{g\in G} k_g g$.
2. l'addition est définie par :

$$\sum_{g\in G} k_g g + \sum_{g\in G} l_g g = \sum_{g\in G}(k_g + l_g)g.$$

3. La multiplication :$(\sum_{u\in G} k_u u)(\sum_{v\in G} l_v v) = \sum_{g\in G}(\sum_{uv=g} k_u l_v)g$. 4. la multiplication par un scalaire : $k(\sum_{g\in G} l_g g) = \sum_{g\in G}(kl_g)g$.

NOTATIONS :

Cette F-algèbre est notée $F[G]$ et l'élément unité de $F[G]$ est $1 = 1_F 1_G$,où 1_F et 1_G sont les éléments unités respectives de F et de G.

Définitions

DEFINITION.2 :On appelle algèbre du groupe G sur le corps F, l'algèbre dont :
1. l'ensemble des éléments est celui de toutes les combinaisons linéaires des éléments de G à coefficients dans F : $\sum_{g\in G} k_g g$.
2. l'addition est définie par :

$$\sum_{g\in G} k_g g + \sum_{g\in G} l_g g = \sum_{g\in G}(k_g + l_g)g.$$

3. La multiplication :$(\sum_{u\in G} k_u u)(\sum_{v\in G} l_v v) = \sum_{g\in G}(\sum_{uv=g} k_u l_v)g$. 4. la multiplication par un scalaire : $k(\sum_{g\in G} l_g g) = \sum_{g\in G}(kl_g)g$.

NOTATIONS :
Cette F-algèbre est notée $F[G]$ et l'élément unité de $F[G]$ est $1 = 1_F 1_G$,où 1_F et 1_G sont les éléments unités respectives de F et de G.

Définitions

DEFINITION.2 :On appelle algèbre du groupe G sur le corps F, l'algèbre dont :

1. l'ensemble des éléments est celui de toutes les combinaisons linéaires des éléments de G à coefficients dans F : $\sum_{g\in G} k_g g$.
2. l'addition est définie par :

$$\sum_{g\in G} k_g g + \sum_{g\in G} l_g g = \sum_{g\in G}(k_g + l_g)g.$$

3. La multiplication :$(\sum_{u\in G} k_u u)(\sum_{v\in G} l_v v) = \sum_{g\in G}(\sum_{uv=g} k_u l_v)g$. 4. la multiplication par un scalaire : $k(\sum_{g\in G} l_g g) = \sum_{g\in G}(kl_g)g$.

NOTATIONS :

Cette F-algèbre est notée $F[G]$ et l'élément unité de $F[G]$ est $1 = 1_F 1_G$,où 1_F et 1_G sont les éléments unités respectives de F et de G.

Définitions

DEFINITION.2 :On appelle algèbre du groupe G sur le corps F, l'algèbre dont :

1. l'ensemble des éléments est celui de toutes les combinaisons linéaires des éléments de G à coefficients dans F : $\sum_{g\in G} k_g g$.

2. l'addition est définie par :

$$\sum_{g\in G} k_g g + \sum_{g\in G} l_g g = \sum_{g\in G}(k_g + l_g)g.$$

3. La multiplication :$(\sum_{u\in G} k_u u)(\sum_{v\in G} l_v v) = \sum_{g\in G}(\sum_{uv=g} k_u l_v)g$. 4. la multiplication par un scalaire : $k(\sum_{g\in G} l_g g) = \sum_{g\in G}(kl_g)g$.

NOTATIONS :

Cette F-algèbre est notée $F[G]$ et l'élément unité de $F[G]$ est $1 = 1_F 1_G$,où 1_F et 1_G sont les éléments unités respectives de F et de G.

Définitions

DEFINITION.2 :On appelle algèbre du groupe G sur le corps F, l'algèbre dont :

1. l'ensemble des éléments est celui de toutes les combinaisons linéaires des éléments de G à coefficients dans F : $\sum_{g\in G} k_g g$.

2. l'addition est définie par :

$$\sum_{g\in G} k_g g + \sum_{g\in G} l_g g = \sum_{g\in G}(k_g + l_g)g.$$

3. La multiplication :$(\sum_{u\in G} k_u u)(\sum_{v\in G} l_v v) = \sum_{g\in G}(\sum_{uv=g} k_u l_v)g$. 4. la multiplication par un scalaire : $k(\sum_{g\in G} l_g g) = \sum_{g\in G}(kl_g)g$.

NOTATIONS :

Cette F-algèbre est notée $F[G]$ et l'élément unité de $F[G]$ est $1 = 1_F 1_G$,où 1_F et 1_G sont les éléments unités respectives de F et de G.

Définitions

DEFINITION.2 :On appelle algèbre du groupe G sur le corps F, l'algèbre dont :

1. l'ensemble des éléments est celui de toutes les combinaisons linéaires des éléments de G à coefficients dans F : $\sum_{g\in G} k_g g$.
2. l'addition est définie par :

$$\sum_{g\in G} k_g g + \sum_{g\in G} l_g g = \sum_{g\in G}(k_g + l_g)g.$$

3. La multiplication :$(\sum_{u\in G} k_u u)(\sum_{v\in G} l_v v) = \sum_{g\in G}(\sum_{uv=g} k_u l_v)g$. 4. la multiplication par un scalaire : $k(\sum_{g\in G} l_g g) = \sum_{g\in G}(kl_g)g$.

NOTATIONS :

Cette F-algèbre est notée $F[G]$ et l'élément unité de $F[G]$ est $1 = 1_F 1_G$,où 1_F et 1_G sont les éléments unités respectives de F et de G.

Définitions

DEFINITION.2 :On appelle algèbre du groupe G sur le corps F, l'algèbre dont :

1. l'ensemble des éléments est celui de toutes les combinaisons linéaires des éléments de G à coefficients dans F : $\sum_{g\in G} k_g g$.
2. l'addition est définie par :

$$\sum_{g\in G} k_g g + \sum_{g\in G} l_g g = \sum_{g\in G}(k_g + l_g)g.$$

3. La multiplication :$(\sum_{u\in G} k_u u)(\sum_{v\in G} l_v v) = \sum_{g\in G}(\sum_{uv=g} k_u l_v)g$. 4. la multiplication par un scalaire : $k(\sum_{g\in G} l_g g) = \sum_{g\in G}(kl_g)g$.

NOTATIONS :

Cette F-algèbre est notée $F[G]$ et l'élément unité de $F[G]$ est $1 = 1_F 1_G$,où 1_F et 1_G sont les éléments unités respectives de F et de G.

Définitions

DEFINITION.2 :On appelle algèbre du groupe G sur le corps F, l'algèbre dont :

1. l'ensemble des éléments est celui de toutes les combinaisons linéaires des éléments de G à coefficients dans F : $\sum_{g\in G} k_g g$.
2. l'addition est définie par :

$$\sum_{g\in G} k_g g + \sum_{g\in G} l_g g = \sum_{g\in G}(k_g + l_g)g.$$

3. La multiplication :$(\sum_{u\in G} k_u u)(\sum_{v\in G} l_v v) = \sum_{g\in G}(\sum_{uv=g} k_u l_v)g$. 4. la multiplication par un scalaire : $k(\sum_{g\in G} l_g g) = \sum_{g\in G}(kl_g)g$.

NOTATIONS :

Cette F-algèbre est notée $F[G]$ et l'élément unité de $F[G]$ est $1 = 1_F 1_G$,où 1_F et 1_G sont les éléments unités respectives de F et de G.

Définitions

DEFINITION.2 :On appelle algèbre du groupe G sur le corps F, l'algèbre dont :

1. l'ensemble des éléments est celui de toutes les combinaisons linéaires des éléments de G à coefficients dans F : $\sum_{g\in G} k_g g$.
2. l'addition est définie par :

$$\sum_{g\in G} k_g g + \sum_{g\in G} l_g g = \sum_{g\in G}(k_g + l_g)g.$$

3. La multiplication :$(\sum_{u\in G} k_u u)(\sum_{v\in G} l_v v) = \sum_{g\in G}(\sum_{uv=g} k_u l_v)g$. 4. la multiplication par un scalaire : $k(\sum_{g\in G} l_g g) = \sum_{g\in G}(kl_g)g$.

NOTATIONS :

Cette F-algèbre est notée $F[G]$ et l'élément unité de $F[G]$ est $1 = 1_F 1_G$,où 1_F et 1_G sont les éléments unités respectives de F et de G.

Définitions

DEFINITION.2 :On appelle algèbre du groupe G sur le corps F, l'algèbre dont :

1. l'ensemble des éléments est celui de toutes les combinaisons linéaires des éléments de G à coefficients dans F : $\sum_{g\in G} k_g g$.
2. l'addition est définie par :

$$\sum_{g\in G} k_g g + \sum_{g\in G} l_g g = \sum_{g\in G}(k_g + l_g)g.$$

3. La multiplication :$(\sum_{u\in G} k_u u)(\sum_{v\in G} l_v v) = \sum_{g\in G}(\sum_{uv=g} k_u l_v)g$. 4. la multiplication par un scalaire : $k(\sum_{g\in G} l_g g) = \sum_{g\in G}(kl_g)g$.

NOTATIONS :

Cette F-algèbre est notée $F[G]$ et l'élément unité de $F[G]$ est $1 = 1_F 1_G$,où 1_F et 1_G sont les éléments unités respectives de F et de G.

Définitions

DEFINITION.2 :On appelle algèbre du groupe G sur le corps F, l'algèbre dont :

1. l'ensemble des éléments est celui de toutes les combinaisons linéaires des éléments de G à coefficients dans F : $\sum_{g\in G} k_g g$.
2. l'addition est définie par :

$$\sum_{g\in G} k_g g + \sum_{g\in G} l_g g = \sum_{g\in G}(k_g + l_g)g.$$

3. La multiplication :$(\sum_{u\in G} k_u u)(\sum_{v\in G} l_v v) = \sum_{g\in G}(\sum_{uv=g} k_u l_v)g$. 4. la multiplication par un scalaire : $k(\sum_{g\in G} l_g g) = \sum_{g\in G}(kl_g)g$.

NOTATIONS :

Cette F-algèbre est notée $F[G]$ et l'élément unité de $F[G]$ est $1 = 1_F 1_G$,où 1_F et 1_G sont les éléments unités respectives de F et de G.

Définitions

DEFINITION.2 :On appelle algèbre du groupe G sur le corps F, l'algèbre dont :

1. l'ensemble des éléments est celui de toutes les combinaisons linéaires des éléments de G à coefficients dans F : $\sum_{g\in G} k_g g$.
2. l'addition est définie par :

$$\sum_{g\in G} k_g g + \sum_{g\in G} l_g g = \sum_{g\in G}(k_g + l_g)g.$$

3. La multiplication :$(\sum_{u\in G} k_u u)(\sum_{v\in G} l_v v) = \sum_{g\in G}(\sum_{uv=g} k_u l_v)g$. 4. la multiplication par un scalaire : $k(\sum_{g\in G} l_g g) = \sum_{g\in G}(kl_g)g$.

NOTATIONS :

Cette F-algèbre est notée $F[G]$ et l'élément unité de $F[G]$ est $1 = 1_F 1_G$,où 1_F et 1_G sont les éléments unités respectives de F et de G.

Définitions

DEFINITION.2 :On appelle algèbre du groupe G sur le corps F, l'algèbre dont :

1. l'ensemble des éléments est celui de toutes les combinaisons linéaires des éléments de G à coefficients dans F : $\sum_{g\in G} k_g g$.
2. l'addition est définie par :

$$\sum_{g\in G} k_g g + \sum_{g\in G} l_g g = \sum_{g\in G}(k_g + l_g)g.$$

3. La multiplication :$(\sum_{u\in G} k_u u)(\sum_{v\in G} l_v v) = \sum_{g\in G}(\sum_{uv=g} k_u l_v)g$. 4. la multiplication par un scalaire : $k(\sum_{g\in G} l_g g) = \sum_{g\in G}(kl_g)g$.

NOTATIONS :

Cette F-algèbre est notée $F[G]$ et l'élément unité de $F[G]$ est $1 = 1_F 1_G$,où 1_F et 1_G sont les éléments unités respectives de F et de G.

Définitions

DEFINITION.2 :On appelle algèbre du groupe G sur le corps F, l'algèbre dont :

1. l'ensemble des éléments est celui de toutes les combinaisons linéaires des éléments de G à coefficients dans F : $\sum_{g\in G} k_g g$.
2. l'addition est définie par :

$$\sum_{g\in G} k_g g + \sum_{g\in G} l_g g = \sum_{g\in G}(k_g + l_g)g.$$

3. La multiplication :$(\sum_{u\in G} k_u u)(\sum_{v\in G} l_v v) = \sum_{g\in G}(\sum_{uv=g} k_u l_v)g$. 4. la multiplication par un scalaire : $k(\sum_{g\in G} l_g g) = \sum_{g\in G}(kl_g)g$.

NOTATIONS :

Cette F-algèbre est notée $F[G]$ et l'élément unité de $F[G]$ est $1 = 1_F 1_G$,où 1_F et 1_G sont les éléments unités respectives de F et de G.

Codes sur F[G]

DEFINITION.3 :
Soit G un groupe fini d'ordre n. Un idéal à droite M de l'algèbre du groupe $F[G]$ est appelé un code de longueur n sur F ou encore un $F[G]$-code de longueur n sur F.

DEFINITION.4 :
Un F[G]- code M est dit cyclique ou abélien si G est cyclique ou abélien.
Soit $a = \sum_{g \in G} a_g g \in FG$.
supp(a)=$\{g \in G \mid a_g \neq 0\}$ est appelé le support de a.
Le nombre $\mid supp(a) \mid$ est appelé le **poids de a**.
La distance minimale d'un F[G]- code M est donnée par :

$$dis(M) := min\{\mid supp(a) \mid \ tel\ que\ a \in M \setminus \{0\}\}.$$

Tous les F[G]-Modules considérés dans la suite seront supposés de dimension finie comme F-espace vectoriel.

Codes sur F[G]

DEFINITION.3 :

Soit G un groupe fini d'ordre n. Un idéal à droite M de l'algèbre du groupe $F[G]$ est appelé un code de longueur n sur F ou encore un $F[G]$-code de longueur n sur F.

DEFINITION.4 :

Un F[G]- code M est dit cyclique ou abélien si G est cyclique ou abélien.

Soit $a = \sum_{g \in G} a_g g \in FG$.

supp(a)=$\{g \in G \mid a_g \neq 0\}$ est appelé le support de a.

Le nombre $\mid supp(a) \mid$ est appelé le **poids de a**.

La distance minimale d'un F[G]- code M est donnée par :

$$dis(M) := min\{\mid supp(a) \mid \ tel\ que\ a \in M \setminus \{0\}\}.$$

Tous les F[G]-Modules considérés dans la suite seront supposés de dimension finie comme F-espace vectoriel.

Codes sur F[G]

DEFINITION.3 :
Soit G un groupe fini d'ordre n. Un idéal à droite M de l'algèbre du groupe $F[G]$ est appelé un code de longueur n sur F ou encore un $F[G]$-code de longueur n sur F.

DEFINITION.4 :
Un F[G]- code M est dit cyclique ou abélien si G est cyclique ou abélien.
Soit $a = \sum_{g \in G} a_g g \in FG$.
supp(a)=$\{g \in G \mid a_g \neq 0\}$ est appelé le support de a.
Le nombre $\mid supp(a) \mid$ est appelé le **poids de a**.
La distance minimale d'un F[G]- code M est donnée par :

$$dis(M) := min\{\mid supp(a) \mid \ tel\ que\ a \in M \setminus \{0\}\}.$$

Tous les F[G]-Modules considérés dans la suite seront supposés de dimension finie comme F-espace vectoriel.

Codes sur F[G]

DEFINITION.3 :
Soit G un groupe fini d'ordre n. Un idéal à droite M de l'algèbre du groupe $F[G]$ est appelé un code de longueur n sur F ou encore un $F[G]$-code de longueur n sur F.

DEFINITION.4 :
Un F[G]- code M est dit cyclique ou abélien si G est cyclique ou abélien.
Soit $a = \sum_{g \in G} a_g g \in FG$.
supp(a)=$\{g \in G \mid a_g \neq 0\}$ est appelé le support de a.
Le nombre $\mid supp(a) \mid$ est appelé le **poids de a**.
La distance minimale d'un F[G]- code M est donnée par :

$$dis(M) := min\{\mid supp(a) \mid \ tel\ que\ a \in M \setminus \{0\}\}.$$

Tous les F[G]-Modules considérés dans la suite seront supposés de dimension finie comme F-espace vectoriel.

Codes sur F[G]

DEFINITION.3 :
Soit G un groupe fini d'ordre n. Un idéal à droite M de l'algèbre du groupe $F[G]$ est appelé un code de longueur n sur F ou encore un $F[G]$-code de longueur n sur F.

DEFINITION.4 :
Un F[G]- code M est dit cyclique ou abélien si G est cyclique ou abélien.

Soit $a = \sum_{g \in G} a_g g \in FG$.
supp(a)=$\{g \in G \mid a_g \neq 0\}$ est appelé le support de a.
Le nombre $\mid supp(a) \mid$ est appelé le **poids de a**.
La distance minimale d'un F[G]- code M est donnée par :

$$dis(M) := min\{\mid supp(a) \mid \ tel\ que\ a \in M \setminus \{0\}\}.$$

Tous les F[G]-Modules considérés dans la suite seront supposés de dimension finie comme F-espace vectoriel.

Codes sur F[G]

DEFINITION.3 :
Soit G un groupe fini d'ordre n. Un idéal à droite M de l'algèbre du groupe $F[G]$ est appelé un code de longueur n sur F ou encore un $F[G]$-code de longueur n sur F.

DEFINITION.4 :
Un F[G]- code M est dit cyclique ou abélien si G est cyclique ou abélien.

Soit $a = \sum_{g \in G} a_g g \in FG$.

supp(a)=$\{g \in G \mid a_g \neq 0\}$ est appelé le support de a.

Le nombre $\mid supp(a) \mid$ est appelé le **poids de a**.

La distance minimale d'un F[G]- code M est donnée par :

$$dis(M) := min\{\mid supp(a) \mid \ tel\ que\ a \in M \setminus \{0\}\}.$$

Tous les F[G]-Modules considérés dans la suite seront supposés de dimension finie comme F-espace vectoriel.

Codes sur F[G]

DEFINITION.3 :
Soit G un groupe fini d'ordre n. Un idéal à droite M de l'algèbre du groupe $F[G]$ est appelé un code de longueur n sur F ou encore un $F[G]$-code de longueur n sur F.

DEFINITION.4 :
Un F[G]- code M est dit cyclique ou abélien si G est cyclique ou abélien.

Soit $a = \sum_{g \in G} a_g g \in FG$.

supp(a)=$\{g \in G \mid a_g \neq 0\}$ est appelé le support de a.

Le nombre $\mid supp(a) \mid$ est appelé le **poids de a**.

La distance minimale d'un F[G]- code M est donnée par :

$$dis(M) := min\{\mid supp(a) \mid \ tel\ que\ a \in M \setminus \{0\}\}.$$

Tous les F[G]-Modules considérés dans la suite seront supposés de dimension finie comme F-espace vectoriel.

Codes sur F[G]

DEFINITION.3 :
Soit G un groupe fini d'ordre n. Un idéal à droite M de l'algèbre du groupe $F[G]$ est appelé un code de longueur n sur F ou encore un $F[G]$-code de longueur n sur F.

DEFINITION.4 :
Un F[G]- code M est dit cyclique ou abélien si G est cyclique ou abélien.
Soit $a = \sum_{g \in G} a_g g \in FG$.
supp(a)=$\{g \in G \mid a_g \neq 0\}$ est appelé le support de a.
Le nombre $\mid supp(a) \mid$ est appelé le **poids de a**.
La distance minimale d'un F[G]- code M est donnée par :

$$dis(M) := min\{\mid supp(a) \mid \ tel\ que\ a \in M \setminus \{0\}\}.$$

Tous les F[G]-Modules considérés dans la suite seront supposés de dimension finie comme F-espace vectoriel.

Codes sur F[G]

DEFINITION.3 :
Soit G un groupe fini d'ordre n. Un idéal à droite M de l'algèbre du groupe $F[G]$ est appelé un code de longueur n sur F ou encore un $F[G]$-code de longueur n sur F.

DEFINITION.4 :
Un F[G]- code M est dit cyclique ou abélien si G est cyclique ou abélien.
Soit $a = \sum_{g \in G} a_g g \in FG$.
supp(a)=$\{g \in G \mid a_g \neq 0\}$ est appelé le support de a.
Le nombre $\mid supp(a) \mid$ est appelé le **poids de a**.
La distance minimale d'un F[G]- code M est donnée par :

$$dis(M) := min\{\mid supp(a) \mid \ tel\ que\ a \in M \setminus \{0\}\}.$$

Tous les F[G]-Modules considérés dans la suite seront supposés de dimension finie comme F-espace vectoriel.

Codes sur F[G]

DEFINITION.3 :
Soit G un groupe fini d'ordre n. Un idéal à droite M de l'algèbre du groupe $F[G]$ est appelé un code de longueur n sur F ou encore un $F[G]$-code de longueur n sur F.

DEFINITION.4 :
Un F[G]- code M est dit cyclique ou abélien si G est cyclique ou abélien.
Soit $a = \sum_{g \in G} a_g g \in FG$.
supp(a)=$\{g \in G \mid a_g \neq 0\}$ est appelé le support de a.
Le nombre $\mid supp(a) \mid$ est appelé le **poids de a**.
La distance minimale d'un F[G]- code M est donnée par :

$$dis(M) := min\{\mid supp(a) \mid \ tel\ que\ a \in M \setminus \{0\}\}.$$

Tous les F[G]-Modules considérés dans la suite seront supposés de dimension finie comme F-espace vectoriel.

Définitions

DEFINITION.5 :
Un F[G]-code M est dit indécomposable si M est un F[G]- module indécomposable.

PROPOSITION :
Tout indécomposable $F(G_1 \times G_2)$-code est de la forme $M_1 \otimes_F M_2$ où M_i est un $F[G_i]$-code indécomposable(i = 1,2).

PROPOSITION :
Tous les indécomposables $F(G_1 \times G_2)$-codes sont produit de codes.

DEFINITION.6 :
Soit M un F[G]-module à droite et H est un sous groupe de G.
M est dit relativement H-projective s'il existe un F[H]-module à droite N tel que M est un facteur directe du F[G]-module à droite $N^G = N \otimes_{F[H]} F[G]$.

Définitions

DEFINITION.5 :
Un F[G]-code M est dit indécomposable si M est un F[G]- module indécomposable.

PROPOSITION :
Tout indécomposable $F(G_1 \times G_2)$-code est de la forme $M_1 \otimes_F M_2$ où M_i est un $F[G_i]$-code indécomposable(i = 1,2).

PROPOSITION :
Tous les indécomposables $F(G_1 \times G_2)$-codes sont produit de codes.

DEFINITION.6 :
Soit M un F[G]-module à droite et H est un sous groupe de G.
M est dit relativement H-projective s'il existe un F[H]-module à droite N tel que M est un facteur directe du F[G]-module à droite $N^G = N \otimes_{F[H]} F[G]$.

Définitions

DEFINITION.5 :
Un F[G]-code M est dit indécomposable si M est un F[G]- module indécomposable.

PROPOSITION :
Tout indécomposable $F(G_1 \times G_2)$-code est de la forme $M_1 \otimes_F M_2$ où M_i est un $F[G_i]$-code indécomposable(i = 1,2).

PROPOSITION :
Tous les indécomposables $F(G_1 \times G_2)$-codes sont produit de codes.

DEFINITION.6 :
Soit M un F[G]-module à droite et H est un sous groupe de G.
M est dit relativement H-projective s'il existe un F[H]-module à droite N tel que M est un facteur directe du F[G]-module à droite $N^G = N \otimes_{F[H]} F[G]$.

Définitions

DEFINITION.5 :
Un F[G]-code M est dit indécomposable si M est un F[G]- module indécomposable.

PROPOSITION :
Tout indécomposable $F(G_1 \times G_2)$-code est de la forme $M_1 \otimes_F M_2$ où M_i est un $F[G_i]$-code indécomposable(i = 1,2).

PROPOSITION :
Tous les indécomposables $F(G_1 \times G_2)$-codes sont produit de codes.

DEFINITION.6 :
Soit M un F[G]-module à droite et H est un sous groupe de G.
M est dit relativement H-projective s'il existe un F[H]-module à droite N tel que M est un facteur directe du F[G]-module à droite $N^G = N \otimes_{F[H]} F[G]$.

Sommet et source

PROPOSITION :

Pour chaque indécomposable F[G]-module à droite il existe un p-sous groupe D de G tel que pour chaque sous groupe H de G on a :
M est relativement H-projective, si et seulement si D est un sous groupe de H (D est unique à une conjugaison G près).

DEFINITION.7 :

Pour chaque indécomposable F[G]-module à droite :
1. D est appelé le **sommet** de M.
2. l'indécomposable F[D]-module à droite N tel que M est un facteur direct de N^G est appelé le D-source de M,
Où D et N sont ceux donnés par la proposition ci-dessus.

Sommet et source

PROPOSITION :

Pour chaque indécomposable F[G]-module à droite il existe un p-sous groupe D de G tel que pour chaque sous groupe H de G on a :

M est relativement H-projective, si et seulement si D est un sous groupe de H (D est unique à une conjugaison G près).

DEFINITION.7 :

Pour chaque indécomposable F[G]-module à droite :

1. D est appelé le **sommet** de M.
2. l'indécomposable F[D]-module à droite N tel que M est un facteur direct de N^G est appelé le D-source de M,

Où D et N sont ceux donnés par la proposition ci-dessus.

Sommet et source

PROPOSITION :

Pour chaque indécomposable F[G]-module à droite il existe un p-sous groupe D de G tel que pour chaque sous groupe H de G on a :
M est relativement H-projective, si et seulement si D est un sous groupe de H (D est unique à une conjugaison G près).

DEFINITION.7 :

Pour chaque indécomposable F[G]-module à droite :

1. D est appelé le **sommet** de M.
2. l'indécomposable F[D]-module à droite N tel que M est un facteur direct de N^G est appelé le D-source de M,

Où D et N sont ceux donnés par la proposition ci-dessus.

Sommet et source

PROPOSITION :
Pour chaque indécomposable F[G]-module à droite il existe un p-sous groupe D de G tel que pour chaque sous groupe H de G on a :
M est relativement H-projective, si et seulement si D est un sous groupe de H (D est unique à une conjugaison G près).

DEFINITION.7 :
Pour chaque indécomposable F[G]-module à droite :
1. D est appelé le **sommet** de M.
2. l'indécomposable F[D]-module à droite N tel que M est un facteur direct de N^G est appelé le D-source de M,
Où D et N sont ceux donnés par la proposition ci-dessus.

Théorème de K.H. Zimmermann

THEOREME :

Soit G un groupe abélien fini avec H son p-sous groupe de Hall, et soit M un indécomposable F[V]-code avec sommet V et V-source N. Alors N peut être choisi comme un F[V]-code et il existe un élément idempotent primitif $e \in F[G]$ tel que : $dis(M) = dis(eF[H])dist(N)$.

Cas d'une algèbre de rand fini

PROPOSITION :

Tout idéal de $A_1 \otimes A_2$ qui est un $A_1 \otimes A_2$-module indécomposable est de la forme $M_1 \otimes_F M_2$ où M_i est un idéal indécomposable de A_i.

PROPOSITION :

Tous les idéaux indécomposables de $A_1 \otimes A_2$ sont des produits tensoriels d'idéaux.

Cas d'une algèbre de rand fini

PROPOSITION :

Tout idéal de $A_1 \otimes A_2$ qui est un $A_1 \otimes A_2$-module indécomposable est de la forme $M_1 \otimes_F M_2$ où M_i est un idéal indécomposable de A_i.

PROPOSITION :

Tous les idéaux indécomposables de $A_1 \otimes A_2$ sont des produits tensoriels d'idéaux.

Cas d'une algèbre de rand fini

PROPOSITION :

Tout idéal de $A_1 \otimes A_2$ qui est un $A_1 \otimes A_2$-module indécomposable est de la forme $M_1 \otimes_F M_2$ où M_i est un idéal indécomposable de A_i.

PROPOSITION :

Tous les idéaux indécomposables de $A_1 \otimes A_2$ sont des produits tensoriels d'idéaux.

MERCI POUR VOTRE PATIENCE