

Álgebra II Práctica (clase 17)

Guido Arnone

Universidad de Buenos Aires

23 de Junio de 2020

Para leer estas diapositivas se recomienda haber leído el apunte teórico hasta la Sección 3.11.

Módulos Simples y Semisimples

Recordemos que un A -módulo S se dice **simple** si tiene exactamente dos submódulos, el submódulo 0 y todo S .

Módulos Simples y Semisimples

Recordemos que un A -módulo S se dice **simple** si tiene exactamente dos submódulos, el submódulo 0 y todo S . Podemos caracterizar a todos los módulos simples conociendo la estructura de anillo de A ,

Proposición

Un A -módulo es S simple si y sólo si existe un ideal a izquierda maximal $\mathfrak{m}$ tal que $S \simeq A/\mathfrak{m}$.

Módulos Simples y Semisimples

Recordemos que un A -módulo S se dice **simple** si tiene exactamente dos submódulos, el submódulo 0 y todo S . Podemos caracterizar a todos los módulos simples conociendo la estructura de anillo de A ,

Proposición

Un A -módulo es S simple si y sólo si existe un ideal a izquierda maximal $\mathfrak{m}$ tal que $S \simeq A/\mathfrak{m}$.

En la clase pasada vimos como se relacionan los módulos simples entre sí:

Lema (Schur)

Si $f : S \rightarrow T$ es un morfismo A -lineal entre A -módulos simples, entonces f es o bien nulo o bien un isomorfismo. En particular, si S es simple entonces $\text{End}_A(S)$ es un anillo de división.

Módulos Simples y Semisimples (cont.)

Los módulos semisimples son, al menos intuitivamente, los que se pueden "armar a partir de módulos simples".

Módulos Simples y Semisimples (cont.)

Los módulos semisimples son, al menos intuitivamente, los que se pueden "armar a partir de módulos simples".

Decimos que un A -módulo es **semisimple** si existe una familia $(S_i)_{i \in I}$ de submódulos simples de M tal que $M = \bigoplus_{i \in I} S_i$. Se tiene la siguiente caracterización:

Proposición (3.10.2)

Sea M un A -módulo. Son equivalentes:

- i) Existe una familia $(S_i)_{i \in I}$ de submódulos simples de M tal que $M = \sum_{i \in I} S_i$.
- ii) Existe una familia $(S_j)_{j \in J}$ de submódulos simples de M tal que $M = \bigoplus_{j \in J} S_j$.
- iii) Para todo submódulo $N \subset M$ existe un submódulo $P \subset M$ tal que $N \oplus P = M$.

Más aún, el lema 3.10.1 nos dice que si se satisface (i) podemos tomar una subfamilia de $(S_i)_{i \in I}$ que satisfaga (ii).

Módulos Simples y Semisimples (cont.)

Con lo anterior podemos extender un resultado conocido de álgebra lineal a D -módulos con D un anillo de división:

Proposición

Sea D un anillo de división y M un D -módulo. Si $S = \{s_i\}_{i \in I} \subset M$ es un sistema de generadores de M , existe una base $B \subset S$ de M .

Módulos Simples y Semisimples (cont.)

Con lo anterior podemos extender un resultado conocido de álgebra lineal a D -módulos con D un anillo de división:

Proposición

Sea D un anillo de división y M un D -módulo. Si $S = \{s_i\}_{i \in I} \subset M$ es un sistema de generadores de M , existe una base $B \subset S$ de M .

Demostración.

Como S es un sistema de generadores de M , se tiene que $M = \sum_{i \in I} Ds_i$. Podemos suponer sin pérdida de generalidad que cada s_i es no nulo.

Módulos Simples y Semisimples (cont.)

Con lo anterior podemos extender un resultado conocido de álgebra lineal a D -módulos con D un anillo de división:

Proposición

Sea D un anillo de división y M un D -módulo. Si $S = \{s_i\}_{i \in I} \subset M$ es un sistema de generadores de M , existe una base $B \subset S$ de M .

Demostración.

Como S es un sistema de generadores de M , se tiene que $M = \sum_{i \in I} Ds_i$. Podemos suponer sin pérdida de generalidad que cada s_i es no nulo. En consecuencia cada epimorfismo $L_{s_i} : d \in D \mapsto d \cdot s_i \in Ds_i$ es no nulo y entonces $\ker L_{s_i} = 0$. En particular $Ds_i \simeq D$ es simple.

Módulos Simples y Semisimples (cont.)

Con lo anterior podemos extender un resultado conocido de álgebra lineal a D -módulos con D un anillo de división:

Proposición

Sea D un anillo de división y M un D -módulo. Si $S = \{s_i\}_{i \in I} \subset M$ es un sistema de generadores de M , existe una base $B \subset S$ de M .

Demostración.

Como S es un sistema de generadores de M , se tiene que $M = \sum_{i \in I} Ds_i$. Podemos suponer sin pérdida de generalidad que cada s_i es no nulo. En consecuencia cada epimorfismo $L_{s_i} : d \in D \mapsto d \cdot s_i \in Ds_i$ es no nulo y entonces $\ker L_{s_i} = 0$. En particular $Ds_i \simeq D$ es simple.

Por lo observado anteriormente existe entonces una subfamilia de $(Ds_j)_{j \in J}$ para cierto $J \subset I$ tal que $M = \bigoplus_{j \in J} Ds_j$. Basta tomar $B = \{s_j\}_{j \in J}$. $\square$

Módulos Simples y Semisimples (cont.)

Antes de seguir, observemos que lo anterior no es cierto en general.

Antes de seguir, observemos que lo anterior no es cierto en general.

Por ejemplo, si $A = \mathbb{Z}$ entonces $S = \{2, 3\}$ es un sistema de generadores que no es base, pues es linealmente dependiente, y ni $S' = \{2\}$ ni $S'' = \{3\}$ son bases de $\mathbb{Z}$ ya que no generan.

Módulos Simples y Semisimples (cont.)

Antes de seguir, observemos que lo anterior no es cierto en general.

Por ejemplo, si $A = \mathbb{Z}$ entonces $S = \{2, 3\}$ es un sistema de generadores que no es base, pues es linealmente dependiente, y ni $S' = \{2\}$ ni $S'' = \{3\}$ son bases de $\mathbb{Z}$ ya que no generan.

Como vimos, podemos caracterizar los A -módulos simples a partir de los ideales maximales de A . Siguiendo con esta idea, la semisimplicidad de los A -módulos nos da información sobre A .

Anillos Semisimples

Un anillo A se dice **semisimple** a izquierda (resp. a derecha) si es semisimple a izquierda (resp. a derecha) visto como A -módulo sobre sí mismo.

Anillos Semisimples

Un anillo A se dice **semisimple** a izquierda (resp. a derecha) si es semisimple a izquierda (resp. a derecha) visto como A -módulo sobre sí mismo.

La semisimplicidad de un anillo es una condición muy fuerte, como nos muestra el siguiente teorema:

Teorema (Artin-Wedderburn)

Sea A un anillo. Son equivalentes:

- i) A es semisimple a derecha.
- ii) todo A -módulo a derecha es semisimple.
- iii) todo A -módulo a derecha es proyectivo.
- iv) todo A -módulo a derecha es inyectivo.
- v) Toda sucesión exacta corta de A -módulos a derecha se parte.
- vi) Existen $r \in \mathbb{N}$, $n_1, \dots, n_r \in \mathbb{N}$ y anillos de división $D_1, \dots, D_r$ tales que $A \simeq M_{n_1}(D_1) \times \dots \times M_{n_r}(D_r)$.
- vii) A es semisimple a izquierda.

De (i) $\iff$ (vii) todas las otras condiciones también valen para módulos a izquierda.

Anillos Semisimples (cont.)

Si A es **conmutativo**, el ejercicio 21 de la práctica 5 nos dice que A es semisimple si y sólo si es isomorfo a un producto de cuerpos

$$A \simeq k_1 \times \cdots \times k_n.$$

Anillos Semisimples (cont.)

Si A es **conmutativo**, el ejercicio 21 de la práctica 5 nos dice que A es semisimple si y sólo si es isomorfo a un producto de cuerpos

$$A \simeq k_1 \times \cdots \times k_n.$$

Por la sección 3.7 del apunte teórico, esto nos dice que todo A -módulo M es isomorfo a $V_1 \oplus \cdots \oplus V_n$ con $V_i = e_i M$ un k_i -espacio vectorial y la acción de A es la acción de cada cuerpo coordenada a coordenada.

Además, si $M \simeq \bigoplus_{i \in [n]} V_i$, $N = \bigoplus_{i \in [n]} W_i$ y $f : M \rightarrow N$ es un morfismo A -lineal, se puede describir como $f_1 \oplus \cdots \oplus f_n$ con $f_i : V_i \rightarrow W_i$ una función k_i -lineal para cada i .

Es decir, si A es conmutativo y semisimple, entonces entender sus módulos se reduce a hacer álgebra lineal (aunque hay que conocer para esto a los cuerpos $k_1, \dots, k_n$).

Anillos Semisimples (cont.)

Por lo visto, si k es un cuerpo y $n \in \mathbb{N}$ el anillo $M_n(k)$ es semisimple: si N es un $M_n(k)$ -módulo, es isomorfo a una suma directa de $M_n(k)$ -módulos simples $(S_i)_{i \in I}$.

Anillos Semisimples (cont.)

Por lo visto, si k es un cuerpo y $n \in \mathbb{N}$ el anillo $M_n(k)$ es semisimple: si N es un $M_n(k)$ -módulo, es isomorfo a una suma directa de $M_n(k)$ -módulos simples $(S_i)_{i \in I}$.

Recordemos que los ideales a izquierda de $M_n(k)$ estaban caracterizados como

$$I_V = \{A \in M_n(k) : \text{las filas de } A \text{ están en } V\}$$

para cada subespacio $V \leq k^n$. En particular I_V es maximal si y sólo si V es un subespacio maximal de k^n , y esto equivale a que $\dim_k V = n - 1$.

Anillos Semisimples (cont.)

Por lo visto, si k es un cuerpo y $n \in \mathbb{N}$ el anillo $M_n(k)$ es semisimple: si N es un $M_n(k)$ -módulo, es isomorfo a una suma directa de $M_n(k)$ -módulos simples $(S_i)_{i \in I}$.

Recordemos que los ideales a izquierda de $M_n(k)$ estaban caracterizados como

$$I_V = \{A \in M_n(k) : \text{las filas de } A \text{ están en } V\}$$

para cada subespacio $V \leq k^n$. En particular I_V es maximal si y sólo si V es un subespacio maximal de k^n , y esto equivale a que $\dim_k V = n - 1$.

Tomando $w \in k^n$ tal que $V \oplus \langle w \rangle = k^n$ tenemos un morfismo $M_n(k)$ -lineal

$$\varphi : p \in k^n \mapsto \begin{pmatrix} p_1 w \\ \vdots \\ p_n w \end{pmatrix} \in M_n(k)$$

que nos dá un isomorfismo $k^n \xrightarrow{\varphi} M_n(k) \rightarrow M_n(k)/I_V$. Por lo tanto todo $M_n(k)$ -módulo simple es isomorfo a k^n .

Morfismos de k -álgebras $M_n(k) \rightarrow M_m(k)$

A partir de la semisimplicidad de los anillos de matrices sobre un cuerpo, vamos a resolver el siguiente ejercicio de la práctica:

Ejercicio (20, práctica 5)

Sea k un cuerpo y $f : M_n(k) \rightarrow M_m(k)$ un morfismo de k -álgebras. Probar que n divide a m .

Morfismos de k -álgebras $M_n(k) \rightarrow M_m(k)$

A partir de la semisimplicidad de los anillos de matrices sobre un cuerpo, vamos a resolver el siguiente ejercicio de la práctica:

Ejercicio (20, práctica 5)

Sea k un cuerpo y $f : M_n(k) \rightarrow M_m(k)$ un morfismo de k -álgebras. Probar que n divide a m .

Demostración.

Morfismos de k -álgebras $M_n(k) \rightarrow M_m(k)$

A partir de la semisimplicidad de los anillos de matrices sobre un cuerpo, vamos a resolver el siguiente ejercicio de la práctica:

Ejercicio (20, práctica 5)

Sea k un cuerpo y $f : M_n(k) \rightarrow M_m(k)$ un morfismo de k -álgebras. Probar que n divide a m .

Demostración.

Sabemos que k^m es un $M_m(k)$ -módulo.

Morfismos de k -álgebras $M_n(k) \rightarrow M_m(k)$

A partir de la semisimplicidad de los anillos de matrices sobre un cuerpo, vamos a resolver el siguiente ejercicio de la práctica:

Ejercicio (20, práctica 5)

Sea k un cuerpo y $f : M_n(k) \rightarrow M_m(k)$ un morfismo de k -álgebras. Probar que n divide a m .

Demostración.

Sabemos que k^m es un $M_m(k)$ -módulo. El morfismo f induce entonces una estructura de $M_n(k)$ -módulo en k^m via $A \cdot v := f(A)v$ y en particular es un k -espacio vectorial con su estructura usual $\lambda \cdot v = f(\lambda)v = \lambda v$.

Morfismos de k -álgebras $M_n(k) \rightarrow M_m(k)$

A partir de la semisimplicidad de los anillos de matrices sobre un cuerpo, vamos a resolver el siguiente ejercicio de la práctica:

Ejercicio (20, práctica 5)

Sea k un cuerpo y $f : M_n(k) \rightarrow M_m(k)$ un morfismo de k -álgebras. Probar que n divide a m .

Demostración.

Sabemos que k^m es un $M_m(k)$ -módulo. El morfismo f induce entonces una estructura de $M_n(k)$ -módulo en k^m via $A \cdot v := f(A)v$ y en particular es un k -espacio vectorial con su estructura usual $\lambda \cdot v = f(\lambda)v = \lambda v$. Como $M_n(k)$ es semisimple, debe existir un conjunto I tal que $k^m \simeq (k^n)^{(I)}$ como $M_n(k)$ -módulos y en particular como espacios vectoriales.

Morfismos de k -álgebras $M_n(k) \rightarrow M_m(k)$

A partir de la semisimplicidad de los anillos de matrices sobre un cuerpo, vamos a resolver el siguiente ejercicio de la práctica:

Ejercicio (20, práctica 5)

Sea k un cuerpo y $f : M_n(k) \rightarrow M_m(k)$ un morfismo de k -álgebras. Probar que n divide a m .

Demostración.

Sabemos que k^m es un $M_m(k)$ -módulo. El morfismo f induce entonces una estructura de $M_n(k)$ -módulo en k^m via $A \cdot v := f(A)v$ y en particular es un k -espacio vectorial con su estructura usual $\lambda \cdot v = f(\lambda)v = \lambda v$. Como $M_n(k)$ es semisimple, debe existir un conjunto I tal que $k^m \simeq (k^n)^{(I)}$ como $M_n(k)$ -módulos y en particular como espacios vectoriales. Por lo tanto el conjunto I debe ser finito y más aún tomando dimensión se tiene que $m = \dim_k k^m = \dim_k (k^n)^{(I)} = |I|n$, así que en efecto $n \mid m$. $\square$

Representaciones irreducibles y $k[G]$ -módulos simples

Fijemos un cuerpo k y consideremos la acción $C_2 \curvearrowright k^2$ por reflexión. Concretamente, si $C_2 = \langle g \mid g^2 = 1 \rangle$ entonces $g \cdot (x, y) = (y, x)$.

Representaciones irreducibles y $k[G]$ -módulos simples

Fijemos un cuerpo k y consideremos la acción $C_2 \curvearrowright k^2$ por reflexión. Concretamente, si $C_2 = \langle g \mid g^2 = 1 \rangle$ entonces $g \cdot (x, y) = (y, x)$. En k^2 la recta $L = \langle (1, 1) \rangle$ es invariante por reflexiones. ¿Habría otra?

Representaciones irreducibles y $k[G]$ -módulos simples

Fijemos un cuerpo k y consideremos la acción $C_2 \curvearrowright k^2$ por reflexión. Concretamente, si $C_2 = \langle g \mid g^2 = 1 \rangle$ entonces $g \cdot (x, y) = (y, x)$. En k^2 la recta $L = \langle (1, 1) \rangle$ es invariante por reflexiones. ¿Habrá otra?

Notar que en este caso, por dimensión, que exista otra recta invariante equivale a tener $L' \leq k^2$ tal que $k^2 = L \oplus L'$ y $C_2 \cdot L' \subset L'$.

Representaciones irreducibles y $k[G]$ -módulos simples

Fijemos un cuerpo k y consideremos la acción $C_2 \curvearrowright k^2$ por reflexión. Concretamente, si $C_2 = \langle g \mid g^2 = 1 \rangle$ entonces $g \cdot (x, y) = (y, x)$. En k^2 la recta $L = \langle (1, 1) \rangle$ es invariante por reflexiones. ¿Habrá otra?

Notar que en este caso, por dimensión, que exista otra recta invariante equivale a tener $L' \leq k^2$ tal que $k^2 = L \oplus L'$ y $C_2 \cdot L' \subset L'$. Podemos hacer la cuenta a mano: una tal recta L' está determinada por un generador (a, b) , y que sea invariante por la acción es lo mismo que $g \cdot (a, b) \in L'$, es decir, que exista $\lambda \in k$ tal que $(a, b) = \lambda(b, a)$.

Representaciones irreducibles y $k[G]$ -módulos simples

Fijemos un cuerpo k y consideremos la acción $C_2 \curvearrowright k^2$ por reflexión. Concretamente, si $C_2 = \langle g \mid g^2 = 1 \rangle$ entonces $g \cdot (x, y) = (y, x)$. En k^2 la recta $L = \langle (1, 1) \rangle$ es invariante por reflexiones. ¿Habrá otra?

Notar que en este caso, por dimensión, que exista otra recta invariante equivale a tener $L' \leq k^2$ tal que $k^2 = L \oplus L'$ y $C_2 \cdot L' \subset L'$. Podemos hacer la cuenta a mano: una tal recta L' está determinada por un generador (a, b) , y que sea invariante por la acción es lo mismo que $g \cdot (a, b) \in L'$, es decir, que exista $\lambda \in k$ tal que $(a, b) = \lambda(b, a)$.

Esto a su vez dice que $a = \lambda^2 a$ y, descartando el caso $a = 0$ se obtiene que $\lambda^2 = 1$. Por lo tanto

$$0 = \lambda^2 - 1 = (\lambda - 1)(\lambda + 1)$$

así que $\lambda = 1$ y $(a, b) = (a, a)$ o $\lambda = -1$ y $(a, b) = (a, -a)$.

Si queremos que L' sea distinta a $L = \langle (1, 1) \rangle$, la única opción posible es $L' = \langle (a, -a) \rangle = \langle (1, -1) \rangle$.

Representaciones irreducibles y $k[G]$ -módulos simples

Si queremos que L' sea distinta a $L = \langle (1, 1) \rangle$, la única opción posible es $L' = \langle (a, -a) \rangle = \langle (1, -1) \rangle$. Cuidado! Esta condición es necesaria, pero no suficiente! Existirá $L' \neq L$ como queremos si y sólo si $-1 \neq 1$ en k , es decir, si $2 \neq 0$.

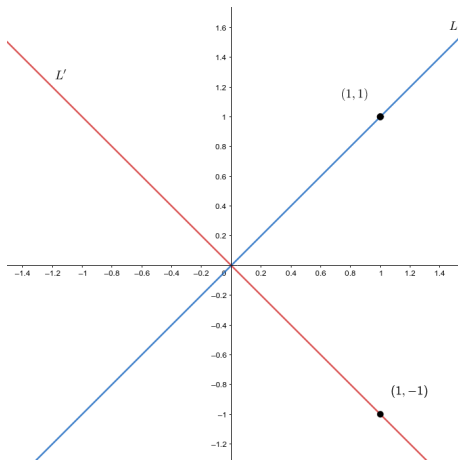
Representaciones irreducibles y $k[G]$ -módulos simples

Si queremos que L' sea distinta a $L = \langle (1, 1) \rangle$, la única opción posible es $L' = \langle (a, -a) \rangle = \langle (1, -1) \rangle$. Cuidado! Esta condición es necesaria, pero no suficiente! Existirá $L' \neq L$ como queremos si y sólo si $-1 \neq 1$ en k , es decir, si $2 \neq 0$.

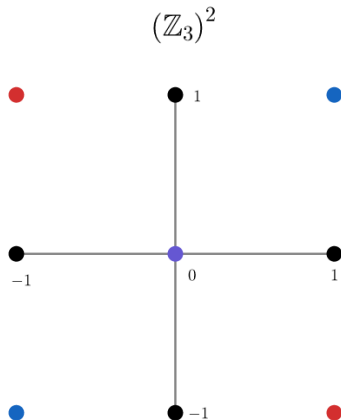
Por ejemplo, en $\mathbb{R}^2$ o $(\mathbb{Z}_3)^2$ esto es posible, pero no así en $(\mathbb{Z}_2)^2$ pues $L = \langle (1, 1) \rangle$ es la única recta invariante por reflexión.

Representaciones irreducibles y $k[G]$ -módulos simples (cont.)

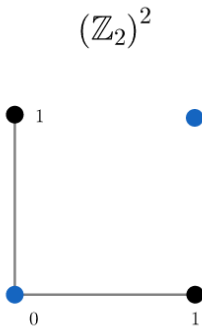
En $\mathbb{R}^2$:



Representaciones irreducibles y $k[G]$ -módulos simples (cont.)



Representaciones irreducibles y $k[G]$ -módulos simples (cont.)



Representaciones irreducibles y $k[G]$ -módulos simples (cont.)

El ejemplo anterior era una instancia de la siguiente situación: si tenemos un k -espacio vectorial V junto con una acción $G \curvearrowright V$ por automorfismos lineales, y un subespacio $S \leq V$ que es G -invariante, queremos saber cuando existirá $T \leq V$ G -invariante tal que $V = S \oplus T$.

Representaciones irreducibles y $k[G]$ -módulos simples (cont.)

El ejemplo anterior era una instancia de la siguiente situación: si tenemos un k -espacio vectorial V junto con una acción $G \curvearrowright V$ por automorfismos lineales, y un subespacio $S \leq V$ que es G -invariante, queremos saber cuando existirá $T \leq V$ G -invariante tal que $V = S \oplus T$.

Podemos responder esta pregunta a partir de la teoría de $k[G]$ -módulos.

Representaciones irreducibles y $k[G]$ -módulos simples (cont.)

Recordemos que si M es un $k[G]$ módulo, la multiplicación por elementos de k hace de éste un k -espacio vectorial, y la multiplicación por elementos de G nos da una acción $G \curvearrowright M$ que es k -lineal con respecto a la anterior estructura.

Representaciones irreducibles y $k[G]$ -módulos simples (cont.)

Recordemos que si M es un $k[G]$ módulo, la multiplicación por elementos de k hace de éste un k -espacio vectorial, y la multiplicación por elementos de G nos da una acción $G \curvearrowright M$ que es k -lineal con respecto a la anterior estructura.

Recíprocamente, si V es un k -espacio vectorial y $G \curvearrowright V$ una acción por automorfismos k -lineales, entonces V es un $k[G]$ -módulo vía

$$\left(\sum_{g \in G} \lambda_g g \right) \cdot v := \sum_{g \in G} \lambda_g (g \cdot v)$$

y estas construcciones son inversas.

Representaciones irreducibles y $k[G]$ -módulos simples (cont.)

Podemos pensar entonces directamente a un $k[G]$ -módulo como un k -espacio vectorial con una acción $G \curvearrowright V$ por automorfismos lineales.

En estos términos, un submódulo de V es un subespacio G -invariante.

Representaciones irreducibles y $k[G]$ -módulos simples (cont.)

Podemos pensar entonces directamente a un $k[G]$ -módulo como un k -espacio vectorial con una acción $G \curvearrowright V$ por automorfismos lineales.

En estos términos, un submódulo de V es un subespacio G -invariante.

Nuestro problema original se traduce en la siguiente pregunta: fijemos un $k[G]$ -módulo M . ¿Es cierto que para todo submódulo S de M existe un submódulo T tal que $M = S \oplus T$?

Representaciones irreducibles y $k[G]$ -módulos simples (cont.)

Podemos pensar entonces directamente a un $k[G]$ -módulo como un k -espacio vectorial con una acción $G \curvearrowright V$ por automorfismos lineales.

En estos términos, un submódulo de V es un subespacio G -invariante.

Nuestro problema original se traduce en la siguiente pregunta: fijemos un $k[G]$ -módulo M . ¿Es cierto que para todo submódulo S de M existe un submódulo T tal que $M = S \oplus T$?

Esto es equivalente a decidir si M es semisimple, así que esta propiedad vale para todo $k[G]$ -módulo si y sólo si $k[G]$ es semisimple.

Representaciones irreducibles y $k[G]$ -módulos simples (cont.)

En la sección 3.11 del apunte teórico vimos la siguiente caracterización:

Teorema (Maschke)

Sea k un cuerpo y G un grupo finito. Si $|G|$ es inversible en k , entonces $k[G]$ es semisimple.

Observamos que cuando $|G| = 0$ en k , el anillo $k[G]$ puede no ser semisimple: en el ejemplo con el que empezamos teníamos un $k[C_2]$ -submódulo propio S de k^2 , y queríamos encontrar T tal que $k^2 = S \oplus T$. Vimos que si $k = \mathbb{Z}_2$, no existía tal T , y la obstrucción era precisamente que $2 = 0$ en $\mathbb{Z}_2$.