Leandro Vendramin

Non-commutative algebra

Notes

Wednesday 16th February, 2022

Contents

List of topics

Lecture 1

§1. Group rings

Let K be a field and G be a group (written multiplicatively). Let $K[G]$ be the vector space with basis $\{g : g \in G\}$. Then $\dim K[G] < \infty$ if and only if G is finite. The vector space $K[G]$ is an algebra with multiplication

$$\left(\sum_{g\in G}\lambda_g g\right)\left(\sum_{h\in G}\mu_h h\right)=\sum_{g,h\in G}\lambda_g\mu_h(gh).$$

Exercise 1.1. Prove that $\mathbb{C}[\mathbb{Z}] \simeq \mathbb{C}[X, X^{-1}]$.

For $n \in \mathbb{Z}_{>1}$ let C_n be the cyclic group of order n.

Exercise 1.2. Let $n \in \mathbb{Z}_{>1}$. Prove that $\mathbb{C}[C_n] \simeq \mathbb{C}[X]/(X^n)$.

Exercise 1.3. Prove that if G and H are isomorphic groups, then $K[G] \simeq K[H]$.

In a similar way, if R is a ring (with 1) and G is a group, then one defines the group ring $R[G]$. More precisely, $R[G]$ is the set of linear combinations

$$\sum_{g\in G}\lambda_g g$$

where $\lambda_g \in R$ and $\lambda_g = 0$ for all but finitely many $g \in G$. One easily proves that $R[G]$ is a ring with addition

$$\left(\sum_{g\in G}\lambda_g g\right)+\left(\sum_{g\in G}\mu_g g\right)=\sum_{g\in G}(\lambda_g+\mu_g)(g)$$

and multiplication

$$\left(\sum_{g\in G}\lambda_g g\right)\left(\sum_{h\in G}\mu_h h\right)=\sum_{g,h\in G}\lambda_g\mu_h(gh).$$

Moreover, $R[G]$ is a left R-module with $\lambda(\sum_{g\in G}\lambda_g g)=\sum_{g\in G}(\lambda\lambda_g)g$.

Exercise 1.4. Let G be a group. Prove that if $\mathbb{Z}[G]\simeq\mathbb{Z}[H]$, then $R[G]\simeq R[H]$ for any commutative ring R.

question:IP *Question 1.1 (Isomorphism problem).* Let G and H be groups. Does $\mathbb{Z}[G]\simeq\mathbb{Z}[H]$ imply $G\simeq H$?

Despite the fact that there are several cases were the isomorphism problem has an affirmative answer (e.g. abelian groups, metabelian groups, nilpotent groups, nilpotent-by-abelian groups, simple groups, abelian-by-nilpotent groups), it is false in general. In 2001 Hertweck found a counterexample of order $2^{21}97^{28}$, see [3].

question:MIP *Question 1.2 (Modular isomorphism problem).* Let p be a prime number. Let G and H be finite p-groups and let K be a field of characteristic p. Does $K[G]\simeq K[H]$ imply $G\simeq H$?

Question 1.2 has an affirmative answer in several cases. However, it is not true in general. This question recently answered by García, Margolis and del Río. They found two non-isomorphic groups G and H both of order 512 such that $K[G]\simeq K[H]$ for all field K of characteristic two.

§2. Kapanskly's problems

Let G be a group and K be a field. If $x\in G$ is such that $x^n=1$, then, since

$$(1-x)(1+x+x^2+\cdots+x^{n-1})=0,$$

it follows that $K[G]$ has non-trivial zero divisors. What happens in the case where G is torsion-free?

example:k[Z] **Example 2.1.** Let $G=\langle x\rangle\simeq\mathbb{Z}$. Then $K[G]$ has no zero divisors. Let $\alpha,\beta\in K[G]\setminus\{0\}$ and write $\alpha=\sum_{i\leq n}a_ix^i$ with $a_n\neq 0$ and $\beta=\sum_{j\leq m}b_jx^j$ with $b_m\neq 0$. Since the coefficient of x^{n+m} of $\alpha\beta$ is non-zero, it follows that $\alpha\beta\neq 0$.

A similar problem concerns units of group algebras. A unit $u\in K[G]$ is said to be **trivial** if $u=\lambda g$ for some $\lambda\in K\setminus\{0\}$ and $g\in G$.

Exercise 2.2. Prove that units of $\mathbb{C}[C_2]$ are trivial.

Exercise 2.3. Prove that $\mathbb{C}[C_5]$ has non-trivial units.

We mention some intriguing problems, generally known as Kaplansky's problems.

prob:units

Open problem 2.1 (Units). Let G be a torsion-free group. Is it true that all units of $K[G]$ are trivial?

The unit problem is still open for fields of characteristic zero. However, it was recently solved by Gardam [2] in the case of K the field of two elements. We will present Gardam's theorem as a computer calculation. We will use GAP [1]. Let P be the group generated by

$$a = \begin{pmatrix} 1 & 0 & 0 & 1/2 \\ 0 & -1 & 0 & 1/2 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1/2 \\ 0 & 0 & -1 & 1/2 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

The group P appears in the literature with various names. For us P will be the Promislow group.

thm:Gardam

Theorem 2.4 (Gardam). *Let F be the field of two elements. For $x = a^2$, $y = b^2$ and $z = (ab)^2$ let*

$$p = (1+x)(1+y)(1+z^{-1}), \qquad q = x^{-1}y^{-1} + x + y^{-1}z + z,$$
$$r = 1 + x + y^{-1}z + xyz, \qquad s = 1 + (x + x^{-1} + y + y^{-1})z^{-1}.$$

Then $u = p + qa + rb + sab$ is a non-trivial unit in $F[P]$.

Proof. We claim that the inverse of u is the element $v = p_1 + q_1 a + r_1 b + s_1 ab$, where

$$p_1 = x^{-1}(a^{-1}pa), \qquad q_1 = -x^{-1}q, \qquad r_1 = -y^{-1}r, \qquad s_1 = z^{-1}(a^{-1}sa).$$

We only need to show that $uv = vu = 1$. We will perform this calculation with GAP. We first need to create the group $P = \langle a, b \rangle$.

```
gap> a := [[1,0,0,1/2],[0,-1,,0,1/2],[0,0,-1,0],[0,0,0,1]];;
gap> b := [[-1,0,0,0],[0,1,0,1/2],[0,0,-1,1/2],[0,0,0,1]];;
gap> P := Group([a,b]);
```

Now we create the group algebra $F[P]$ and the embedding $P \hookrightarrow F[P]$. The field F will be `GF(2)` and the embedding will be denoted by `f`.

```
gap> R := GroupRing(GF(2),P);;
gap> f := Embedding(P, R);;
```

We first need the elements x, y and z that were defined in the statement.

```
gap> x := Image(f, a^2);;
gap> y := Image(f, b^2);;
gap> z := Image(f, (a*b)^2);;
```

Now we define the elements p, q, r and s. Note that the identity of the group algebra `R` is `One(R)`.

```
gap> p := (One(R)+x)*(One(R)+y)*(One(R)+Inverse(z));;
gap> r := One(R)+x+Inverse(y)*z+x*y*z;;
gap> q := Inverse(x)*Inverse(y)+x+Inverse(y)*z+z;;
gap> s := One(R)+(x+Inverse(x)+y+Inverse(y))*Inverse(z);
```

Rather than trying to compute the inverse of u we will show that $uv = vu = 1$. For that purpose we need to define p_1, q_1, r_1 and s_1.

```
gap> p1 := Inverse(x)*p^Image(f, a);;
gap> q1 := -Inverse(x)*q;;
gap> r1 := -Inverse(y)*r;;
gap> s1 := Inverse(z)*s^Image(f, a);;
```

Now it is time to prove the theorem.

```
gap> u := p+q*a+r*b+s*a*b;;
gap> v := p1+q1*a+r1*b+s1*a*b;;
gap> IsOne(u*v);
true
gap> IsOne(v*u);
true
```

This completes the proof of the theorem. $\square$

Our proof of Theorem 2.4 is exactly as that of [2].

Exercise 2.5. Let p be a prime number and F_p be the field of size p. Use the technique for proving Gardam's theorem to prove Murray's theorem on the existence on non-trivial units in $F_p[P]$. Reference: arXiv:2106.02147.

A ring R is **reduced** if for all $r \in R$ such that $r^2 = 0$ one has $r = 0$.

prob:reducido **Open problem 2.2.** Let G be a torsion-free group. Is it true that $K[G]$ is reduced?

prob:dominio **Open problem 2.3 (Zero divisors).** Let G be a torsion-free group. Is it true that $K[G]$ is a domain?

prob:J **Open problem 2.4 (Semisimplicity).** Let G be a torsion-free group. It is true that $J(K[G]) = 0$ if G is non-trivial?

pro:idempotente **Open problem 2.5 (Idempotents).** Let G be a torsion-free group and $\alpha \in K[G]$ be an idempotent. Is it true that $\alpha \in \{0, 1\}$?

Exercise 2.6. Prove that if $K[G]$ has no zero-divisors and $\alpha \in K[G]$ is an idempotent, then $\alpha \in \{0, 1\}$.

Exercise 2.7. Prove that $K[\mathbb{Z}/4]$ contains non-trivial zero divisors and every idempotent of $K[\mathbb{Z}/4]$ is trivial.

The problems mentioned are all related. Our goal is the prove the following implications:

$$2.4 \Longleftarrow 2.1 \Longrightarrow 2.2 \Longleftrightarrow 2.3$$

We first prove that an affirmative solution to the Units Problem 2.1 yields a solution to Problem 2.2 about the reducibility of group algebras.

Theorem 2.8. *Let G be a non-trivial group. Assume that $K[G]$ has only trivial units. Then $K[G]$ is reduced.*

Proof. Let $\alpha \in K[G]$ be such that $\alpha^2 = 0$. We claim that $\alpha = 0$. Since $\alpha^2 = 0$,

$$(1-\alpha)(1+\alpha) = 1-\alpha^2 = 1,$$

it follows that $1-\alpha$ is a unit of $K[G]$. Since units of $K[G]$ are trivial, there exist $\lambda \in K \setminus \{0\}$ and $g \in G$ such that $1-\alpha = \lambda g$. If $g \neq 1$, then

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

a contradiction. Therefore $g = 1$ and hence $\alpha = 1-\lambda \in K$. Since K is a field, one concludes that $\alpha = 0$. □

We now prove that an affirmative solution to the Units Problem 2.1 also yields a solution to the Jacobson Semisimplicity Problem 2.4.

Theorem 2.9. *Let G be a non-trivial group. Assume that $K[G]$ has only trivial units. If $|K| > 2$ or $|G| > 2$, then $J(K[G]) = \{0\}$.*

Proof. Let $\alpha \in J(K[G])$. There exist $\lambda \in K \setminus \{0\}$ and $g \in G$ such that $1-\alpha = \lambda g$. Assume that $g \neq 1$. If $|K| \geq 3$, then there exist $\mu \in K \setminus \{0,1\}$ such that

$$1-\alpha\mu = 1-\mu+\lambda\mu g$$

is a non-trivial unit, a contradiction. If $|G| \geq 3$, there exists $h \in G \setminus \{1, g^{-1}\}$ such that $1-\alpha h = 1-h+\lambda gh$ is a non-trivial unit, a contradiction. Thus $g = 1$ and hence $\alpha = 1-\lambda \in K$. Therefore $1+\alpha h$ is a trivial unit for all $h \neq 1$ and hence $\alpha = 0$. □

Exercise 2.10. Prove that if $G = \langle g \rangle \simeq \mathbb{Z}/2$, then $J(\mathbb{F}_2[G]) = \{0, g-1\} \neq \{0\}$.

§3. Passman's theorem

Now we prove that an affirmative solution to the Units Problem (Open Problem 2.1) yields a solution to Open Problem 2.3 about zero divisors in group algebras. The proof is hard and requires some preliminaries. We first need to discuss a group theoretical tool known as the *transfer map*.

If H is a subgroup of G, a **transversal** of H in G is a complete set of coset representatives of G/H.

thm:transfer **Theorem 3.1.** *Let G be a group and H be a finite-index subgroup of G. The map*

$$\nu\colon G \to H/[H,H], \quad g \mapsto d(Rg,R),$$

does not depend on the transversal R of H in G and it is a group homomorphism.

To prove the theorem we first need a lemma.

lem:d **Lemma 3.2.** *Let G be a group and H be a subgroup of G of finite index. Let R and S be transversals of H in G and let $\alpha\colon H \to H/[H,H]$ be the canonical map. Then*

$$d(R,S) = \prod \alpha(rs^{-1}),$$

where the product is taken over all pairs $(r,s) \in R\times S$ such that $Hr = Hs$, is well-defined and satisfies the following properties:

1) $d(R,S)^{-1} = d(S,R)$.
2) $d(R,S)d(S,T) = d(R,T)$ *for all transversal T of H in G.*
3) $d(Rg,Sg) = d(R,S)$.
4) $d(Rg,R) = d(Sg,S)$.

Proof. The product that defines $d(R,S)$ is well-defined since $H/[H,H]$ is an abelian group. The first three claim are trivial. Let us prove 4). By 2),

$$d(Rg,Sg)d(Sg,S)d(S,R) = d(Rg,S)d(S,R) = d(Rg,R).$$

Since $H/[H,H]$ is abelian, 1) and 3) imply that

$$d(Rg,Sg)d(Sg,S)d(S,R) = d(R,S)d(S,R)d(Sg,S) = d(Sg,S). \qquad \square$$

We are know ready to prove the theorem:

Proof of Theorem 3.1. The lemma implies that the map does not depend on the transversal used. Moreover, ν is a group homomorphism, as

$$\nu(gh) = d(R(gh),R) = d(R(gh),Rh)d(Rh,R) = d(Rg,R)d(Rh,R) = \nu(g)\nu(h). \quad \square$$

The theorem justifies the following definition:

Definition 3.3. Let G be a group and H be a finite-index subgroup of G. The **transfer map** of G in H is the group homomorphism

$$\nu\colon G \to H/[H,H], \quad g \mapsto d(Rg,R),$$

of Theorem 3.1, where R is some transversal of H in G.

Veamos cómo calcular el morfismo de transferencia. Si H es un subgrupo de G de índice n, fijemos un transversal $T = \{x_1,\dots,x_n\}$. Para $g \in G$,

$$\nu(g) = \prod \alpha(xy^{-1}),$$

donde el producto se hace sobre los pares $(x,y) \in (Tg,T)$ tales que $Hx = Hy$ y $\alpha\colon H \to H/[H,H]$ es el morfismo canónico. Si escribimos $x = x_i g$ para algún $i \in \{1,\dots,n\}$, entonces $Hx_i g = Hx_{\sigma(i)}$ para alguna permutación $\sigma \in \mathbb{S}_n$. Luego

$$\nu(g) = \prod_{i=1}^{n} \alpha(x_i g x_{\sigma(i)}^{-1}).$$

lem:transfer **Lemma 3.4.** *Sean G un grupo y H un subgrupo de índice finito n y sea T un transversal de H en G. Para cada $g \in G$ existe k y existen enteros positivos $n_1,\dots,n_k$ tales que $n_1+\cdots+n_k = n$ y elementos $t_1,\dots,t_k \in T$ tales que*

$$\nu(g) = \prod_{i=1}^{k} \alpha(t_i g^{n_i} t_i^{-1}),$$

donde $\alpha\colon H \to H/[H,H]$ es el morfismo canónico.

Proof. Sabemos que existe una permutación $\sigma \in \mathbb{S}_n$ tal que

$$\nu(g) = \prod_{i=1}^{n} t_i g t_{\sigma(i)}^{-1}.$$

Si escribimos a σ como producto de k ciclos disjuntos $\sigma = \alpha_1 \cdots \alpha_k$, donde cada α_j es un ciclo de longitud n_j, entonces para cada ciclo de la forma $(i_1 \cdots i_{n_j})$ reordenamos el producto de forma tal que

$$\alpha(x_{i_1} g x_{i_2}^{-1})\alpha(x_{i_2} g x_{i_3}^{-1}) \cdots \alpha(x_{i_{n_j}} g x_{i_1}^{-1}) = \alpha(x_{i_1} g^{n_1} x_{i_1}^{-1}).$$

Luego existen $t_1,\dots,t_k \in T$ tales que $\nu(g) = \prod_{j=1}^{k} t_i g^{n_i} t_i^{-1}$. □

El morfismo de transferencia nos permite demostrar el siguiente lema:

lem:center **Lemma 3.5.** *Si G es un grupo tal que su centro $Z(G)$ tiene índice finito n, entonces $(gh)^n = g^n h^n$ para todo $g,h \in G$.*

Proof. Sea $g \in G$. Por el lema 3.4 sabemos que existen enteros positivos $n_1,\dots,n_k$ tales que $n_1+\cdots+n_k = n$ y elementos $t_1,\dots,t_k$ de un transversal de $Z(G)$ en G tales que

$$\nu(g) = \prod_{i=1}^{k} \alpha(t_i g^{n_1} t_i^{-1}),$$

donde $\alpha\colon G \to H/[H,H]$ es el morfismo canónico. Como $g^{n_i} \in Z(G)$ para todo $i \in \{1,\dots,k\}$ (pues $t_i g^{n_i} t_i^{-1} \in Z(G)$), se sigue que $\nu(g) = g^{n_1+\cdots+n_k} = g^n$. Como ν es un morfismo de grupos por el teorema 3.1, se concluye que

$$(gh)^n = \nu(gh) = \nu(g)\nu(h) = g^n h^n.$$

□

Dado un grupo G consideramos el subconjunto

$$\Delta(G) = \{g \in G : (G : C_G(g)) < \infty\}.$$

Exercise 3.6. Demuestre que $\Delta(\Delta(G)) = \Delta(G)$.

Lemma 3.7. *Si G es un grupo, entonces $\Delta(G)$ es un subgrupo característico de G.*

Proof. Primero veamos que $\Delta(G)$ es un subgrupo de G. Si $x, y \in \Delta(G)$ y $g \in G$, entonces $g(xy^{-1})g^{-1} = (gxg^{-1})(gyg^{-1})^{-1}$. Además $1 \in \Delta(G)$. Veamos ahora que $\Delta(G)$ es característico en G. Si $f \in \mathrm{Aut}(G)$ y $x \in G$, entonces, como $f(gxg^{-1}) = f(g)f(x)f(g)^{-1}$, se concluye que $f(x) \in \Delta(G)$. □

Exercise 3.8. Demuestre que si $G = \langle r, s : s^2 = 1, srs = r^{-1}\rangle$ es el grupo diedral infinito, entonces $\Delta(G) = \langle r\rangle$.

Exercise 3.9. Sean H y K subgrupos de G de índice finito. Demuestre que

$$(G : H \cap K) \leq (G : H)(G : K).$$

lem:FCabeliano

Lemma 3.10. *Si G es un grupo sin torsión tal que $\Delta(G) = G$, entonces G es abeliano.*

Proof. Sean $x, y \in G$ y sea $S = \langle x, y\rangle$. El grupo $Z(S) = C_S(x) \cap C_S(y)$ tiene índice finito, digamos n, en S. Como por el lema 3.5 la función $S \to Z(S)$, $s \mapsto s^n$, es un morfismo de grupos, se tiene que

$$[x, y]^n = (xyx^{-1}y^{-1})^n = x^n y^n x^{-n} y^{-n} = 1$$

pues $x^n \in Z(S)$. Como G es libre de torsión, $[x, y] = 1$. □

lem:Neumann

Lemma 3.11 (Neumann). *Sean $H_1, \dots, H_m$ subgrupos de G. Supongamos que existen finitos elementos $a_{ij} \in G$, $1 \leq i \leq m$, $1 \leq j \leq n$, tales que*

$$G = \bigcup_{i=1}^{m} \bigcup_{j=1}^{n} H_i a_{ij}.$$

Entonces algún H_i tiene índice finito en G.

Proof. Procederemos por inducción en m. El caso $m = 1$ es trivial. Supongamos entonces que $m \geq 2$. Si $(G : H_1) = \infty$, existe $b \in G$ tal que

$$Hb \cap \left(\bigcup_{j=1}^{n} H_1 a_{1j} \right) = \emptyset.$$

Como entonces $H_1 b \subseteq \bigcup_{i=2}^{m} \bigcup_{j=1}^{n} H_i a_{ij}$, se concluye que

$$H_1 a_{1k} \subseteq \bigcup_{i=2}^{m} \bigcup_{j=1}^{n} H a_{ij} b^{-1} a_{1k}.$$

Luego G puede cubrirse con finitas coclases de $H_2,\dots,H_m$ y por hipótesis inductiva alguno de estos H_j tiene índice finito en G. □

Veremos ahora un operador de proyección del álgebra de grupo. Si G es un grupo y H es un subgrupo de G, se define

$$\pi_H\colon K[G]\to K[H],\quad \pi_H\left(\sum_{g\in G}\lambda_g g\right)=\sum_{g\in H}\lambda_g g.$$

Exercise 3.12. Sea G un grupo y sea H un subgrupo de G. Demuestre que si $\alpha\in K[G]$, entonces π_H es un morfismo de $(K[H],K[H])$-bimódulos con las multiplicaciones a izquierda y a derecha, es decir:

$$\pi_H(\beta\alpha\gamma)=\beta\pi_H(\alpha)\gamma$$

para todo $\beta,\gamma\in K[H]$.

lem:escritura

Lemma 3.13. *Sea X un transversal a izquierda de H en G. Todo $\alpha\in K[G]$ se escribe unívocamente como*

$$\alpha=\sum_{x\in X}x\alpha_x,$$

donde $\alpha_x=\pi_H(x^{-1}\alpha)\in K[H]$.

Proof. Sea $\alpha\in K[G]$. Como $\operatorname{supp}\alpha$ es finito, $\operatorname{supp}\alpha$ está contenido en finitas coclases de H, digamos $x_1H,\dots,x_nH$, donde los x_j son elementos de X. Escribimos $\alpha=\alpha_1+\cdots+\alpha_n$, donde $\alpha_i=\sum_{g\in x_iH}\lambda_g g$. Si $g\in x_iH$, entonces $x_i^{-1}g\in H$ y luego podemos escribir

$$\alpha=\sum_{i=1}^{n}x_i(x_i^{-1}\alpha_i)=\sum_{x\in X}x\alpha_x$$

con $\alpha_x\in K[H]$ para todo $x\in X$. Para la unicidad observemos que para cada $x\in X$ gracias al ejercicio anterior se tiene

$$\pi_H(x^{-1}\alpha)=\pi_H\left(\sum_{y\in X}x^{-1}y\alpha_y\right)=\sum_{y\in X}\pi_H(x^{-1}y)\alpha_y=\alpha_x$$

pues

$$\pi_H(x^{-1}y)=\begin{cases}1 & \text{si } x=y,\\ 0 & \text{si } x\neq y.\end{cases}$$

□

lem:ideal_pi

Lemma 3.14. *Sea G un grupo y H un subgrupo de G. Si I es un ideal a izquierda no nulo de $K[G]$, entonces $\pi_H(I)\neq 0$.*

Proof. Sea X un transversal a izquierda de H en G y sea $\alpha\in I\setminus\{0\}$. Por el lema 3.13 podemos escribir $\alpha=\sum_{x\in X}x\alpha_x$ con $\alpha_x=\pi_H(x^{-1}\alpha)\in K[H]$ para todo $x\in X$. Como

$\alpha \neq 0$, existe $y \in X$ tal que $0 \neq \alpha_y = \pi_H(y^{-1}\alpha) \in \pi_H(I)$ ($y^{-1}\alpha \in I$ pues I es un ideal a izquierda). ☐

Antes de avanzar, veamos una aplicación del operador de proyección:

Proposition 3.15. *Sean G un grupo, H un subgrupo de G y $\alpha \in K[H]$. Valen las siguientes afirmaciones:*

1) *α es inversible en $K[H]$ si y sólo si α es inversible en $K[G]$.*
2) *α es un divisor de cero en $K[H]$ si y sólo si α es un divisor de cero en $K[G]$.*

Proof. Si α es inversible en $K[G]$, existe $\beta \in K[G]$ tal que $\alpha\beta = \beta\alpha = 1$. Al aplicar π_H y usar que π_H es un morfismo de $(K[H], K[H])$-bimódulos,

$$\alpha\pi_H(\beta) = \pi_H(\alpha\beta) = \pi_H(1) = 1 = \pi_H(1) = \pi_H(\beta\alpha) = \pi_H(\beta)\alpha.$$

Si $\alpha\beta = 0$ para algún $\beta \in K[G] \setminus \{0\}$, sea $g \in G$ tal que $1 \in \operatorname{supp}(\beta g)$. Como $\alpha(\beta g) = 0$,

$$0 = \pi_H(0) = \pi_H(\alpha(\beta g)) = \alpha\pi_H(\beta g),$$

donde $\pi_H(\beta g) \in K[H] \setminus \{0\}$ pues $1 \in \operatorname{supp}(\beta g)$. ☐

lem:Passman **Lemma 3.16 (Passman).** *Sea G un grupo y sean $\gamma_1, \gamma_2 \in K[G]$ con $\gamma_1 K[G]\gamma_2 = 0$. Entonces $\pi_{\Delta(G)}(\gamma_1)\pi_{\Delta(G)}(\gamma_2) = 0$.*

Proof. Basta ver que $\pi_{\Delta(G)}(\gamma_1)\gamma_2 = 0$ pues en este caso

$$0 = \pi_{\Delta(G)}(\pi_{\Delta(G)}(\gamma_1)\gamma_2) = \pi_\Delta(\gamma_1)\pi_{\Delta(G)}(\gamma_2).$$

Escribimos $\gamma_1 = \alpha_1 + \beta_1$, donde

$$\begin{aligned} \alpha_1 &= a_1u_1 + \cdots + a_ru_r, && u_1, \dots, u_r \in \Delta(G), \\ \beta_1 &= b_1v_1 + \cdots + b_sv_s, && v_1, \dots, v_s \notin \Delta(G), \\ \gamma_2 &= c_1w_1 + \cdots + c_tw_t, && w_1, \dots, w_t \in G. \end{aligned}$$

El subgrupo $C = \bigcap_{i=1}^r C_G(u_i)$ tiene índice finito en G. Supongamos que

$$0 \neq \pi_\Delta(\gamma_1)\gamma_2 = \alpha_1\gamma_2$$

y sea $g \in \operatorname{supp}(\alpha_1\gamma_2)$. Si v_i es conjugado de algún gw_j^{-1} en G, sea $g_{ij} \in G$ tal que $g_{ij}^{-1}v_ig_{ij} = gw_j^{-1}$. Si v_i y gw_j^{-1} no son conjugados tomamos $g_{ij} = 1$.

Para cada $x \in C$ se tiene $\alpha_1\gamma_2 = (x^{-1}\alpha_1x)\gamma_2$. Como además

$$x^{-1}\gamma_1x\gamma_2 \in x^{-1}\gamma_1K[G]\gamma_2 = 0,$$

tenemos

$$\begin{aligned} (a_1u_1 + \cdots + a_ru_r)\gamma_2 = \alpha_1\gamma_2 = x^{-1}\alpha_1x\gamma_2 &= -x^{-1}\beta_1x\gamma_2 \\ &= -x^{-1}(b_1v_1 + \cdots + b_sv_r)x(c_1w_1 + \cdots + c_tw_t). \end{aligned}$$

Como $g \in \operatorname{supp}(\alpha_1\gamma_2)$, existen i, j tales que $g = x^{-1}v_i x w_j$. Luego v_i y gw_j^{-1} son conjugados y entonces $x^{-1}v_i x = gw_j^{-1} = g_{ij}^{-1}v_i g_{ij}$, es decir $x \in C_G(v_i)g_{ij}$. Esto demuestra que

$$C \subseteq \bigcup_{i,j} C_G(v_i)g_{ij}$$

y como C tiene índice finito en G, esto implica que G puede cubrirse con finitas coclases de los $C_G(v_i)$. Pero como $v_i \notin \Delta(G)$, cada uno de los $C_G(v_i)$ tiene índice infinito en G, una contradicción al lema de Neumann. □

Theorem 3.17. *Sea G un grupo sin torsión. Si $K[G]$ es reducido, entonces $K[G]$ es un dominio.*

Proof. Supongamos que $K[G]$ no es un dominio y sean $\gamma_1, \gamma_2 \in K[G] \setminus \{0\}$ tales que $\gamma_2\gamma_1 = 0$. Si $\alpha \in K[G]$, entonces

$$(\gamma_1\alpha\gamma_2)^2 = \gamma_1\alpha\gamma_2\gamma_1\alpha\gamma_2 = 0$$

y luego $\gamma_1\alpha\gamma_2 = 0$ pues $K[G]$ es reducido. En particular, $\gamma_1 K[G]\gamma_2 = 0$. Sea I el ideal a izquierda de $K[G]$ generado por γ_2. Como $I \neq 0$, $\pi_{\Delta(G)}(I) \neq 0$ por el lema 3.14 y luego $\pi_{\Delta(G)}(\beta\gamma_2) \neq 0$ para algún $\beta \in K[G]$. Similarmente se demuestra que $\pi_{\Delta(G)}(\gamma_1\alpha) \neq 0$ para algún $\alpha \in K[G]$. Como

$$\gamma_1\alpha K[G]\beta\gamma_2 \subseteq \gamma_1 K[G]\gamma_2 = 0,$$

se tiene que $\pi_{\Delta(G)}(\gamma_1\alpha)\pi_{\Delta(G)}(\beta\gamma_2) = 0$ por el lema de Passman. Luego $K[\Delta(G)]$ tiene divisores de cero, una contradicción pues $\Delta(G)$ es un grupo abeliano. □

§4. Grupos (bi)ordenables

En esta sección estudiaremos algunas propiedades del grupo G motivadas por el análisis que se hizo en el ejemplo 2.1.

Definition 4.1. Un grupo G se dice **biordenable** si existe un orden total $<$ en G tal que $x < y$ implica que $xz < yz$ y $zx < zy$ para todo $x, y, z \in G$.

Example 4.2. El grupo $\mathbb{R}_{>0}$ de números reales positivos es biordenable.

Exercise 4.3. Sea G un grupo biordenable y sean $x, x', y, y' \in G$. Demuestre que si $x < y$ y $x' < y'$, entonces $xx' < yy'$.

Exercise 4.4. Sea G un grupo biordenable y sean $g, h \in G$. Demuestre que si $g^n = h^n$ para algún $n > 0$ entonces $g = h$.

Definition 4.5. Sea G un grupo biordenable. El cono positivo es el conjunto $P(G) = \{x \in G : 1 < x\}$.

lemma:biordenableP1

Lemma 4.6. *Sea G un grupo biordenable con cono positivo P. Entonces*

1) *P es cerrado para la multiplicación.*
2) *$G = P \cup P^{-1} \cup \{1\}$ (unión disjunta).*
3) *$xPx^{-1} = P$ para todo $x \in G$.*

Proof. Si $x, y \in P$ y $z \in G$, entonces, como $1 < x$ y además $1 < y$, se tiene que $1 < xy$. Luego $1 = z1z^{-1} < zxz^{-1}$. Queda demostrar entonces la segunda afirmación: Si $g \in G$, entonces $g = 1$ o $g > 1$ o $g < 1$. Como $g < 1$ y si sólo si $1 < g^{-1}$. ◻

lem:biordenableP2

Lemma 4.7. *Sea G un grupo y sea P un subconjunto de G cerrado para la multiplicación y tal que $G = P \cup P^{-1} \cup \{1\}$ (unión disjunta) y $xPx^{-1} = P$ para todo $x \in G$. Si definimos $x < y$ si y sólo si $yx^{-1} \in P$, entonces G resulta biordenable con cono positivo P.*

Proof. Sean $x, y \in G$. Como $yx^{-1} \in G$ y sabemos que $G = P \cup P^{-1} \cup \{1\}$ (unión disjunta), se tiene exactamente alguna de las siguientes tres posibilidades: $yx^{-1} \in P$, $xy^{-1} = (yx^{-1})^{-1} \in P$ o bien $yx^{-1} = 1$. Luego $x < y$, $y < x$ o bien $x = y$. Si $x < y$ y $z \in G$, entonces $zx < zy$ pues $(zy)(zx)^{-1} = z(yx^{-1})z^{-1} \in P$ ya que $zPz^{-1} = P$. Además $xz < yz$ pues $(yz)(xz)^{-1} = yx^{-1} \in P$. Para demostrar que que P es el cono positivo de este biorden en G basta observar que $x1^{-1} = x \in P$ si y sólo si $1 < x$. ◻

pro:BOsintorsion

Proposition 4.8. *Todo grupo biordenable es libre de torsión.*

Proof. Sea G un grupo biordenable y sea $g \in G \setminus \{1\}$. Si $g > 1$, entonces $1 < g < g^2 < \cdots$. Si $g < 1$, entonces $1 > g > g^2 > \cdots$. Luego $g^n \neq 1$ para todo $n \neq 0$. ◻

Example 4.9. El grupo $G = \langle x, y : yxy^{-1} = x^{-1} \rangle$ no es biordenable y es libre de torsión. Supongamos que G es biordenable y sea P su cono positivo. Si $x \in P$ entonces $yxy^{-1} = x^{-1} \in P$, una contradicción. Entonces $x^{-1} \in P$ y luego $x = y^{-1}x^{-1}y \in P$, una contradicción.

thm:BO

Theorem 4.10. *Sea G un grupo biordenable. Entonces $K[G]$ es un dominio tal que solamente tiene unidades triviales. Más aún, si G es no trivial, $J(K[G]) = 0$.*

Proof. Sean $\alpha, \beta \in K[G]$ tales que

$$\alpha = \sum_{i=1}^{m} a_i g_i, \qquad g_1 < g_2 < \cdots < g_m, \qquad a_i \neq 0 \qquad \forall i \in \{1, \dots, m\},$$
$$\beta = \sum_{j=1}^{n} b_j h_j, \qquad h_1 < h_2 < \cdots < h_n, \qquad b_j \neq 0 \qquad \forall j \in \{1, \dots, n\}.$$

Entonces
$$g_1 h_1 \leq g_i h_j \leq g_m h_n$$
para todo i, j. Además $g_1 h_1 = g_i h_j$ si y sólo si $i = j = 1$. El coeficiente de $g_1 h_1$ en $\alpha\beta$ es $a_1 b_1 \neq 0$ y en particular $\alpha\beta \neq 0$. Si $\alpha\beta = \beta\alpha = 1$, entonces el coefciente de $g_m h_n$ en $\alpha\beta$ es $a_m b_n$ y luego $m = n = 1$ y por lo tanto $\alpha = a_1 g_1$ y $\beta = b_1 h_1$ con $a_1 b_1 = b_1 a_1 = 1$ en K y $g_1 h_1 = 1$ en G. ◻

thm:Levi **Theorem 4.11 (Levi).** *Sea A un grupo abeliano. Entonces A es biordenable si y sólo si A es libre de torsión.*

Proof. Si A es biordenable, entonces A no tiene torsión por la proposición 4.8. Supongamos entonces que A es un grupo abeliano sin torsión y veamos que es biordenable. Sea $\mathcal{S}$ la clase de subconjuntos P de A tales que $0 \in P$, P es cerrado para la suma de A y cumplen con la siguiente propiedad: si $x \in P$ y $-x \in P$, entonces $x = 0$. Claramente $\mathcal{S}$ es no vacía pues $\{0\} \in \mathcal{S}$. Si ordenamos parcialmente a $\mathcal{S}$ con la inclusión, vemos que el elemento $\bigcup_{i \in I} P_i$ es una cota superior para la cadena $P_1 \subseteq P_2 \subseteq \cdots$ de $\mathcal{S}$. Por el lema de Zorn, $\mathcal{S}$ tiene un elemento maximal $P \in \mathcal{S}$.

Claim. Si $x \in A$ es tal que $kx \in P$ para algún $k > 0$, entonces $x \in P$.

Para demostrar la afirmación sea $Q = \{x \in A : kx \in P \text{ para algún } k > 0\}$. Veamos que $Q \in \mathcal{S}$. Trivialmente $0 \in Q$. Además Q es cerrado por la adición: si $k_1x_1 \in P$ y $k_2x_2 \in P$ entonces $k_1k_2(x_1 + x_2) \in P$. Sea $x \in A$ tal que $x \in Q$ y $-x \in Q$. Entonces $kx \in P$ y $l(-x) \in P$ para algún $l > 0$. Como entonces $klx \in P$ y $kl(-x) \in P$, se concluye que $klx = 0$, una contradicción pues A no tiene torsión. Luego $x \in Q \subseteq P$.

Claim. Si $x \in A$ es tal que $x \notin P$ entonces $-x \in P$.

Supongamos que $-x \notin P$ y sea $P_1 = \{y + nx : y \in P, n \geq 0\}$. Vamos a ver que $P_1 \in \mathcal{S}$. Claramente $0 \in P_1$ y P_1 es cerrado para la suma. Si $P_1 \notin S$ existe

$$0 \neq y_1 + n_1x = -(y_2 + n_2x),$$

donde $y_1, y_2 \in P$ y $n_1, n_2 \geq 0$. Entonces $y_1 + y_2 = -(n_1 + n_2)x$. Si $n_1 = n_2 = 0$, entonces $y_1 = -y_2 \in P$ y luego $y_1 = y_2 = 0$ y se concluye que $y_1 + n_1x = 0$, una contradicción. Si $n_1 + n_2 > 0$, entonces, como

$$(n_1 + n_2)(-x) = y_1 + y_2 \in P,$$

la primera afirmación que hicimos implica que $-x \in P$, una contradicción. Demostramos entonces que $P_1 \in \mathcal{S}$. Como $P \subseteq P_1$, la maximalidad de P implica que $x \in P = P_1$.

Gracias al lema 4.7 sabemos que el conjunto $P^* = P \setminus \{0\}$ que construimos es en realidad el cono positivo de un biorden en A. En efecto, P^* es cerrado para la suma pues si $x, y \in P^*$, entonces $x + y \in P$ y si $x + y = 0$ entonces, como $x = -y \in P$, se concluye que $x = y = 0$. Además $G = P^* \cup -P^* \cup \{0\}$ (unión disjunta) pues demostramos en la segunda afirmación que si $x \notin P^*$ entonces $-x \in P$. □

Corollary 4.12. *Sea A un grupo abeliano no trivial y sin torsión. Entonces $K[A]$ es un dominio tal que solamente tiene unidades triviales y $J(K[A]) = 0$.*

Proof. Es consecuencia del teorema de Levi y del teorema 4.10. □

Definition 4.13. Un grupo G se dice **ordenable a derecha** si existe un orden total $<$ en G tal que si $x < y$ entonces $xz < yz$ para todo $x, y, z \in G$.

Si G es un grupo ordenable a derecha, se define el cono positivo de G como el subconjunto $P(G) = \{x \in G : 1 < x\}$.

Exercise 4.14. Sea G un grupo ordenable a derecha con cono positivo P. Demuestre las siguientes afirmaciones:

1) P es cerrado por multiplicación.
2) $G = P \cup P^{-1} \cup \{1\}$ (unión disjunta).

Exercise 4.15. Sea G un grupo y sea P un subconjunto cerrado por multiplicación y tal que $G = P \cup P^{-1} \cup \{1\}$ (unión disjunta). Demuestre que si se define $x < y$ si y sólo si $yx^{-1} \in P$, entonces G es ordenable a derecha con cono positivo P.

Lemma 4.16. *Sea G un grupo y sea N un subgrupo normal de G. Si N y G/N son ordenables a derecha, entonces G también lo es.*

Proof. Como N y G/N son ordenables a derecha, existen los conos positivos $P(N)$ y $P(G/N)$. Sea $\pi \colon G \to G/N$ el morfismo canónico y sea

$$P(G) = \{x \in G : \pi(x) \in P(G/N) \text{ o bien } x \in N\}.$$

Dejamos como ejercicio demostrar que $P(G)$ es cerrado por la multiplicación y que $G = P(G) \cup P(G)^{-1} \cup \{1\}$ (unión disjunta). Luego G es ordenable a derecha. □

Para dar un criterio de ordenabilidad necesitamos un lema:

lemma:fg

Lemma 4.17. *Sea G un grupo finitamente generado y sea H un subgrupo de índice finito. Entonces H es finitamente generado.*

Proof. Supongamos que G está generado por $\{g_1, \dots, g_m\}$ y supongamos que para cada i existe k tal que $g_i^{-1} = g_k$. Sea $t_1, \dots, t_n$ un conjunto de representantes de G/H. Para $i \in \{1, \dots, n\}$, $j \in \{1, \dots, m\}$, escribimos

$$t_i g_j = h(i,j) t_{k(i,j)}.$$

Vamos a demostrar que H está generado por los $h(i,j)$. Sea $x \in H$. Escribamos

$$\begin{aligned} x &= g_{i_1} \cdots g_{i_s} \\ &= (t_1 g_{i_1}) g_{i_2} \cdots g_{i_s} \\ &= h(1,i_1) t_{k_1} g_{i_2} \cdots g_{i_s} \\ &= h(1,i_1) h(k_1,i_2) t_{k_2} g_{i_3} \cdots g_{i_s} \\ &= h(1,i_1) h(k_1,i_2) \cdots h(k_{s-1}, g_{i_s}) t_{k_s}, \end{aligned}$$

donde $k_1, \dots, k_{s-1} \in \{1, \dots, n\}$. Como $t_{k_s} \in H$, $t_{k_s} = t_1 \in H$ y luego $x \in H$. □

El siguiente teorema nos da un criterio de ordenabilidad a derecha:

Theorem 4.18. *Sea G un grupo libre de torsión y finitamente generado. Si A es un subgrupo normal abeliano tal que G/A es finito y cíclico, entonces G es ordenable a derecha.*

Proof. Primero observemos que si A es trivial, entonces G también es trivial. Supongamos entonces que $A \neq 1$. Como A tiene índice finito, es finitamente generado. Procederemos por inducción en la cantidad de generadores de A. Como G/A es cíclico, existe $x \in G$ tal que $G = \langle A, x\rangle$. Luego $[x, A] = \langle [x, a] : a \in A\rangle$ es un subgrupo normal de G tal que $A/C_A(x) \simeq [x, A]$ (pues $a \mapsto [x, a]$ es un morfismo de grupos $A \to A$ con imagen $[x, A]$ y núcleo $C_A(x)$). Si $\pi\colon G \to G/[x, A]$, entonces $G/[x, A] = \langle \pi(A), \pi(x)\rangle$ y luego $G/[x, A]$ es abeliano pues $[\pi(x), \pi(A)] = \pi[x, A] = 1$. Además $G/[x, A]$ es finitamente generado pues G es finitamente generado. Como $(G : A) = n$ y G no tiene torsión, $1 \neq x^n \in A$. Luego $x^n \in C_A(x)$ y entonces $1 \leq \operatorname{rank} C_A(x) < \operatorname{rank} A$ (si $\operatorname{rank} C_A(x) = \operatorname{rank} A$, entonces $[x, A]$ sería un subgrupo de torsión de A, una contradicción pues $x \notin A$). Luego

$$\operatorname{rank}[x, A] = \operatorname{rank}(A/C_A(x)) \leq \operatorname{rank} A - 1$$

y entonces $\operatorname{rank}(A/[x, A]) \geq 1$. Demostramos así que $A/[x, A]$ es infinito y luego $G/[x, A]$ es también infinito.

Como $G/[x, A]$ es un grupo abeliano finitamente generado e infinito, existe un un subgrupo normal H de G tal que $[x, A] \subseteq H$ y $G/H \simeq \mathbb{Z}$. El subgrupo $B = A \cap H$ es abeliano, normal en H y cumple que H/B es cíclico (pues puede identificarse con un subgrupo de G/A). Como $\operatorname{rank} B < \operatorname{rank} A$, la hipótesis inductiva implica que H es ordenable a derecha y luego G también es ordenable a derecha. □

Exercise 4.19 (Malcev–Neumann). Sea G un grupo ordenable a derecha. Demuestre que $K[G]$ no tiene divisores de cero ni unidades no triviales.

En 1973 Formanek demostró que la conjetura de los divisores de cero es verdadera para grupos super resolubles sin torsión. En 1976 Brown e independientemente Farkas y Snider demostraron que la conjetura es verdadera para grupos policíclicos-por-finitos sin torsión.

§5. Grupos con la propiedad del producto único

Sea G un grupo y sean $A, B \subseteq G$ subconjuntos no vacíos. Diremos que un elemento $g \in G$ es un producto único en AB si $g = ab = a_1b_1$ con $a, a_1 \in A$ y $b, b_1 \in B$ implica que $a = a_1$ y $b = b_1$.

Definition 5.1. Se dice que un grupo G tiene la **propiedad del producto único** si dados dos subconjuntos $A, B \subseteq G$ finitos y no vacíos existe al menos un producto único en AB.

Proposition 5.2. *Si un grupo G es ordenable a derecha, entonces G tiene la propiedad del producto único.*

Proof. Sean $A = \{a_1, \dots, a_n\} \subseteq G$ y $B \subseteq G$ ambos finitos y no vacíos. Supongamos que $a_1 < a_2 < \cdots < a_n$. Sea $c \in B$ tal que a_1c es el mínimo del conjunto $a_1B = \{a_1b :$

$b \in B\}$. Veamos que $a_1 c$ admite una única representación de la forma $\alpha\beta$ con $\alpha \in A$ y $\beta \in B$. Si $a_1 c = ab$, entonces, como $ab = a_1 c \leq a_1 b$, se tiene que $a \leq a_1$ y luego $a = a_1$ y $b = c$. □

Exercise 5.3. Demuestre que un grupo que satisface la propiedad del producto único es libre de torsión.

Definition 5.4. Se dice que un grupo G tiene la **propiedad del doble producto único** si dados dos subconjuntos $A, B \subseteq G$ finitos y no vacíos tales que $|A|+|B| > 2$ existen al menos dos productos únicos en AB.

theorem:Strojnowski

Theorem 5.5 (Strojnowski). *Sea G un grupo. Las siguientes afirmaciones son equivalentes:*

1) *G tiene la propiedad del doble producto único.*
2) *Para todo subconjunto $A \subseteq G$ finito y no vacío, existe al menos un producto único en $AA = \{a_1 a_2 : a_1, a_2 \in A\}$.*
3) *G tiene la propiedad del producto único.*

Proof. La implicación (1) $\implies$ (2) es trivial. Demostremos que vale (2) $\implies$ (3). Si G no tiene la propiedad del producto único, existen subconjuntos $A, B \subseteq G$ finitos y no vacíos tales que todo elemento de AB admite al menos dos representaciones. Sea $C = AB$. Todo $c \in C$ es de la forma $c = (a_1 b_1)(a_2 b_2)$ con $a_1, a_2 \in A$ y $b_1, b_2 \in B$. Como $a_2^{-1} b_1^{-1} \in AB$, existen $a_3 \in A \setminus \{a_2\}$ y $b_3 \in B \setminus \{b_1\}$ tales que $a_2^{-1} b_1^{-1} = a_3^{-1} b_3^{-1}$. Luego $b_1 a_2 = b_3 a_3$ y entonces

$$c = (a_1 b_1)(a_2 b_2) = (a_1 b_3)(a_3 b_2)$$

son dos representaciones distintas de c en AB. pues $a_2 \neq a_3$ y $b_1 \neq b_3$.

Demostremos ahora que (3) $\implies$ (1). Si G tiene la propiedad del producto único pero no tiene la propiedad del doble producto único, existen subconjuntos $A, B \subseteq G$ finitos y no vacíos con $|A|+|B| > 2$ tales que en AB existe un único elemento ab con una única representación en AB. Sean $C = a^{-1}A$ y $D = Bb^{-1}$. Entonces $1 \in C \cap D$ y el elemento neutro 1 admite una única representación en CD (pues si $1 = cd$ con $c = a^{-1}a_1 \neq 1$ y $d = b_1 b^{-1} \neq 1$, entonces $ab = a_1 b_1$ con $a \neq a_1$ y $b \neq b_1$). Sean $E = D^{-1}C$ y $F = DC^{-1}$. Todo elemento de EF se escribe como $(d_1^{-1}c_1)(d_2 c_2^{-1})$. Si $c_1 \neq 1$ o $d_2 \neq 1$ entonces $c_1 d_2 = c_3 d_3$ para algún $c_3 \in C \setminus \{c_1\}$ y algún $d_3 \in D \setminus \{d_2\}$. Entonces $(d_1^{-1}c_1)(d_2 c_2^{-1}) = (d_1^{-1}c_3)(d_3 c_2^{-1})$ son dos representaciones distintas para $(d_1^{-1}c_1)(d_2 c_2^{-1})$. Si $c_2 \neq 1$ o $d_1 \neq 1$ entonces $c_2 d_1 = c_4 d_4$ para algún $d_4 \in D \setminus \{d_1\}$ y algún $c_4 \in C \setminus \{c_2\}$ y entonces, como $d_1^{-1}c_2^{-1} = d_4^{-1}c_4^{-1}$, $(d_1^{-1}1)(1c_2^{-1}) = (d_4^{-1}1)(1c_4^{-1})$. Como $|C|+|D| > 2$, C o D contienen algún $c \neq 1$, y entonces $(1 \cdot 1)(1 \cdot 1) = (1 \cdot c)(1 \cdot c^{-1})$. Demostramos entonces que todo elemento de EF tiene al menos dos representaciones. □

Exercise 5.6. Demuestre que si G es un grupo que satisface la propiedad del producto único, entonces $K[G]$ tiene solamente unidades triviales.

En general es muy difícil verificar si un grupo posee la propiedad del producto único. Una propiedad similar es la de ser un grupo difuso. Si G es un grupo libre de torsión y $A \subseteq G$ es un subconjunto, diremos que A es antisimétrico si $A \cap A^{-1} \subseteq \{1\}$, donde $A^{-1} = \{a^{-1} : a \in A\}$. El conjunto de **elementos extremales** de A se define como $\Delta(A) = \{a \in A : Aa^{-1}$ es antisimétrico$\}$. Luego

$$a \in A \setminus \Delta(A) \iff \text{existe } g \in G \setminus \{1\} \text{ tal que } ga \in A \text{ y } g^{-1}a \in A.$$

Definition 5.7. Un grupo G se dice **difuso** si para todo subconjunto $A \subseteq G$ tal que $2 \leq |A| < \infty$ se tiene $|\Delta(A)| \geq 2$.

Lemma 5.8. *Si G es ordenable a derecha, entonces G es difuso.*

Proof. Supongamos que $A = \{a_1, \dots, a_n\}$ y $a_1 < a_2 < \cdots < a_n$. Vamos a demostrar que $\{a_1, a_n\} \subseteq \Delta(A)$. Si $a_1 \in A \setminus \Delta(A)$, existe $g \in G \setminus \{1\}$ tal que $ga_1 \in A$ y $g^{-1}a_1 \in A$. Esto implica que $a_1 \leq ga_1$ y $a_1 \leq g^{-1}a_1$, de donde se concluye que $1 \leq g$ y $1 \leq g^{-1}$, una contradicción. De la misma forma se demuestra que $a_n \in \Delta(A)$. □

lemma:difuso=>2up

Lemma 5.9. *Si G es difuso, entonces G tiene la propiedad del doble producto único.*

Proof. Supongamos que G no tiene la propiedad del doble producto único. Existen entonces subconjuntos finitos $A, B \subseteq G$ con $|A| + |B| > 2$ tales que $C = AB$ tiene a lo sumo un producto único. Luego $|C| \geq 2$. Como G es difuso, $|\Delta(C)| \geq 2$. Si $c \in \Delta(C)$, entonces c tiene una única expresión como $c = ab$ con $a \in A$ y $b \in B$ (de lo contrario, si $c = a_0b_0 = a_1b_1$ con $a_0 \neq a_1$ y $b_0 \neq b_1$. Si $g = a_0a_1^{-1}$, entonces $g \neq 1$, $gc = a_0a_1^{-1}a_1b_1 = a_0b_1 \in C$ y además $g^{-1}c = a_1a_0^{-1}a_0b_0 = a_1b_0 \in C$. Luego $c \notin \Delta(c)$, una contradicción. □

Open problem 5.1. Find a non-diffuse group with the unique product property.

§6. Connel's theorem

When $K[G]$ is prime? Connel's theorem gives a full answer to this natural question in the case where K is of characteristic zero.

If S is a finite subset of a group G, then we define $\widehat{S} = \sum_{x \in S} x$.

lemma:sumN

Lemma 6.1. *Let N be a finite normal subgroup of G. Then $\widehat{N} = \sum_{x \in N} x$ is central in $K[G]$ and $\widehat{N}(\widehat{N} - |N|1) = 0$.*

Proof. Assume that $N = \{n_1, \dots, n_k\}$. Let $g \in G$. Since $N \to N$, $n \mapsto gng^{-1}$, is bijective,

$$g\widehat{N}g^{-1} = g(n_1 + \cdots + n_k)g^{-1} = gn_1g^{-1} + \cdots + gn_kg^{-1} = \widehat{N}.$$

Since $nN = N$ if $n \in N$, it follows that $n\widehat{N} = \widehat{N}$. Thus $\widehat{N}\widehat{N} = \sum_{j=1}^{k} n_j\widehat{N} = |N|\widehat{N}$. □

Before proving Connel's theorem we need to prove two group theoretical results. The first one goes to Dietzman:

theorem:Dietzmann

Theorem 6.2 (Dietzmann). *Let G be a group and $X \subseteq G$ be a finite subset of G closed by conjugation. If there exists n such that $x^n = 1$ for all $x \in X$, then $\langle X \rangle$ is a finite subgroup of G.*

Proof. Let $S = \langle X \rangle$. Since $x^{-1} = x^{n-1}$, every element of S can be written as a finite product of elements of X. Fix $x \in X$. We claim that if $x \in X$ appears $k \geq 1$ times in the word s, then we can write s as a product of m elements of X, where the first k elements are equal to x. Suppose that

$$s = x_1 x_2 \cdots x_{t-1} x x_{t+1} \cdots x_m,$$

where $x_j \neq x$ for all $j \in \{1, \dots, t-1\}$. Then

$$s = x(x^{-1}x_1 x)(x^{-1}x_2 x) \cdots (x^{-1}x_{t-1}x)x_{t+1} \cdots x_m$$

is a product of m elements of X since X is closed under conjugation and the first element is x. The same argument implies that s can be written as

$$s = x^k y_{k+1} \cdots y_m,$$

where each y_j belongs to $X \setminus \{x\}$.

Let $s \in S$ and write s as a product of m elements of X, where m is minimal. We need to show that $m \leq (n-1)|X|$. If $m > (n-1)|X|$, then at least $x \in X$ appear n times in the representation of s. Without loss of generality, we write

$$s = x^n x_{n+1} \cdots x_m = x_{n+1} \cdots x_m,$$

a contradiction to the minimality of m. $\square$

The second result goes back to Schur:

thm:Schur

Theorem 6.3 (Schur). *Let G be a group. If $Z(G)$ has finite index in G, then $[G,G]$ is finite.*

Proof. Let $n = (G : Z(G))$ and X be the set of commutators of G. We claim that X is finite, in fact $|X| \leq n^2$. The map

$$\varphi\colon X \to G/Z(G) \times G/Z(G), \quad [x,y] \mapsto (xZ(G), yZ(G)),$$

is injective: if $(xZ(G), yZ(G)) = (uZ(G), vZ(G))$, then $u^{-1}x \in Z(G)$, $v^{-1}y \in Z(G)$. Thus

$$[u,v] = uvu^{-1}v^{-1} = uv(u^{-1}x)x^{-1}v^{-1} = xvx^{-1}(v^{-1}y)y^{-1} = xyx^{-1}y^{-1} = [x,y].$$

Moreover, X is closed under conjugation, as

$$g[x,y]g^{-1} = [gxg^{-1}, gyg^{-1}]$$

for all $g,x,y \in G$. Since $G \to Z(G)$, $g \mapsto g^n$ is a group homomorphism, Lemma 3.5 implies that $[x,y]^n = [x^n,y^n] = 1$ for all $[x,y] \in X$. The theorem follows from applying Dietzmann's theorem. □

Si G es un grupo, consideramos el subconjunto

$$\Delta^+(G) = \{x \in \Delta(G) : x \text{ tiene orden finito}\}.$$

lem:DcharG **Lemma 6.4.** *Si G es un grupo, entonces $\Delta^+(G)$ es un subgrupo característico de G.*

Proof. Claramente $1 \in \Delta^+(G)$. Sean $x,y \in \Delta^+(G)$ y sea H el subgrupo de G generado por el conjunto C formado por los finitos conjugados de x e y. Si $|x| = n$ y $|y| = m$, entonces $c^{nm} = 1$ para todo $c \in C$. Como C es finito y cerrado por conjugación, el teorema de Dietzmann implica que H es finito. Luego $H \subseteq \Delta^+(G)$ y en particular $xy^{-1} \in \Delta^+(G)$. Es evidente que $\Delta^+(G)$ es un subgrupo característico pues para todo $f \in \operatorname{Aut}(G)$ se tiene que $f(x) \in \Delta^+(G)$ si $x \in \Delta^+(G)$. □

La segunda aplicación del teorema de Dietzmann es el siguiente resultado:

lem:Connel **Lemma 6.5.** *Sea G un grupo y sea $x \in \Delta^+(G)$. Existe entonces un subgrupo finito H normal en G tal que $x \in H$.*

Dejamos la demostración como ejercicio ya que el muy similar a lo que hicimos en la demostración del lema 6.4.

thm:Connel **Theorem 6.6 (Connell).** *Supongamos que el cuerpo K es de característica cero. Sea G un grupo. Las siguientes afirmaciones son equivalentes:*

1) *$K[G]$ es primo.*
2) *$Z(K[G])$ es primo.*
3) *G no tiene subgrupos finitos normales no triviales.*
4) *$\Delta^+(G) = 1$.*

Proof. Demostremos que (1) $\implies$ (2). Como $Z(K[G])$ es un anillo conmutativo, probar que es primo es equivalente a probar que no existen divisores de cero no triviales. Sean $\alpha,\beta \in Z(K[G])$ tales que $\alpha\beta = 0$. Sean $A = \alpha K[G]$ y $B = \beta K[G]$. Como α y β son centrales, A y B son ideales de $K[G]$. Como $AB = 0$, entonces $A = \{0\}$ o $B = \{0\}$ pues $K[G]$ es primo. Luego $\alpha = 0$ o $\beta = 0$.

Demostremos ahora que (2) $\implies$ (3). Sea N un subgrupo normal finito. Por el lema 6.1, $\widehat{N} = \sum_{x \in N} x$ es central en $K[G]$ y $\widehat{N}(\widehat{N} - |N|1) = 0$. Como $\widehat{N} \neq 0$ (pues K tiene característica cero) y $Z(K[G])$ es un dominio, $\widehat{N} = |N|1$, es decir: $N = \{1\}$.

Demostremos que (3) $\implies$ (4). Sea $x \in \Delta^+(G)$. Por el lema 6.5 sabemos que existe un subgrupo finito H normal en G que contiene a x. Como por hipótesis H es trivial, se concluye que $x = 1$.

Finalmente demostramos que (4) $\implies$ (1). Sean A y B ideales de $K[G]$ tales que $AB = 0$. Supongamos que $B \neq 0$ y sea $\beta \in B \setminus \{0\}$. Si $\alpha \in A$, entonces, como

$\alpha K[G]\beta \subseteq \alpha B \subseteq AB = 0$, el lema 3.16 de Passman implica que $\pi_{\Delta(G)}(\alpha)\pi_{\Delta(G)}(\beta) = 0$. Como por hipótesis $\Delta^+(G)$ es trivial, sabemos que $\Delta(G)$ es libre de torsión y luego $\Delta(G)$ es abeliano por el lema 3.10. Esto nos dice que $K[\Delta(G)]$ no tiene divisores de cero y luego $\alpha = 0$. Demostramos entonces que $B \neq 0$ implica que $A = 0$. □

Theorem 6.7 (Connel). *Sea K un cuerpo de característica cero y sea G un grupo. Entonces $K[G]$ es artiniano a izquierda si y sólo si G es finito.*

Proof. Si G es finito, $K[G]$ es un álgebra de dimensión finita y luego es artiniano a izquierda. Supongamos entonces que $K[G]$ es artiniano a izquierda.

Primero observemos que si $K[G]$ es un álgebra prima, entonces por el teorema de Wedderburn $K[G]$ es simple y luego G es el grupo trivial (pues si G no es trivial, $K[G]$ no es simple ya que el ideal de aumentación es un ideal no nulo de $K[G]$).

Como $K[G]$ es artiniano a izquierda, es noetheriano a izquierda por Hopkins–Levitzky y entonces, $K[G]$ admite una serie de composición por el teorema **??**. Para demostrar el teorema procederemos por inducción en la longitud de la serie de composición de $K[G]$. Si la longitud es uno, $\{0\}$ es el único ideal de $K[G]$ y luego $K[G]$ es prima y el resultado está demostrado. Si suponemos que el resultado vale para longitud n y además $K[G]$ no es prima, entonces, por el teorema de Connel, G posee un subgrupo normal H finito y no trivial. Al considerar el morfismo canónico $K[G] \to K[G/H]$ vemos que $K[G/H]$ es artiniano a izquierda y tiene longitud $< n$. Por hipótesis inductiva, G/H es un grupo finito y luego, como H también es finito, G es finito. □

References

1. The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.11.1*, 2021.
2. G. Gardam. A counterexample to the unit conjecture for group rings. *Ann. of Math. (2)*, 194(3):967–979, 2021.
3. M. Hertweck. A counterexample to the isomorphism problem for integral group rings. *Ann. of Math. (2)*, 154(1):115–138, 2001.

Index