

Group Rings of Infinite Groups

by Prof. Dr. Giles Gardam

notes by Stefan Albrecht

University Bonn – winter term 2023/24

Literature Passman: The algebraic structure of group rings

Contents

1	The Kaplansky Conjectures for Group Rings	2
1.1	The Unit Conjecture	3
1.2	Ordered Groups and related Properties	4
2	Hyperbolic Groups	7
3	Primality of group rings	9

1 The Kaplansky Conjectures for Group Rings

Definition 1.1. Let R be a ring and G be a group. The *group ring*

$$R[G] = \left\{ \sum_{i=1}^n r_{g_i} g_i \mid g_i \in G, r_{g_i} \in R \right\}$$

is the ring consisting of finite formal R -linear combinations of the group elements with multiplication

$$\left(\sum r_g g \right) \left(\sum s_h h \right) = \sum r_g s_h gh = \sum_k \left(\sum_{gh=k} r_g s_h \right) k.$$

In this course, we will (almost) always have $R = \mathbb{Z}$ or $R = K$ a field. In the latter case, $K[G]$ is often called the group algebra.

Example 1.2. For $G = \mathbb{Z} = \langle t \rangle$, then $R[G]$ is the ring of Laurent polynomials in t over R , usually denoted $R[t, t^{-1}]$.

Viewpoint of Noether: Representations of groups are modules over group rings.

Warning: $K[G]$ is a non-commutative ring unless G is abelian. It is (left-)Noetherian only in special settings and it is never semisimple for infinite G . (cf. Masuhke's theorem).

Although group rings tend to have bad ring-theoretic properties, they conjecturally have nice elementary properties. Note first that for $k \in K^\times$ and $g \in G$, the element $kg \in K[G]$ is a unit, such units are called *trivial*. A group is called *torsion free* if it has no nontrivial elements of finite order.

Conjecture 1.3 (Kaplansky). *Let K be a field and G be a torsion free group. Then $K[G]$*

- *has no nontrivial units,*
- *has no non-zero zero divisors,*
- *has no non-trivial idempotents.*

Furthermore, for any group G (possibly with torsion), $K[G]$ is directly finite (=von Neumann-finite =Dedekind-finite), i.e. if $\alpha\beta = 1$, then $\beta\alpha = 1$.

Remark 1.4. Torsion-freeness is essential. Assume $g \in G$ has order $n \geq 2$. Then $0 = (1 - g)(1 + g + \dots + g^{n-1})$

Remark 1.5. The unit conjecture is false, the others are open.

Remark 1.6. These conjectures are "local" in the sense that they only depend on the finitely generated subgroups of G .

Proposition 1.7. *For a given field K and a group G , we have*

$$\text{unit conj.} \implies \text{zero divisor-conj.} \implies \text{idempotent conj.} \implies \text{direct finite-conj.}$$

Proof. The last 2 implications are easy ring theoretic statements. The first implication requires the following theorem by Connell (which we will prove later): $K[G]$ is prime (meaning $AB = 0$ implies $A = 0$ or $B = 0$ for two-sided ideals $A, B \subseteq K[G]$) if and only if G has no non-trivial finite normal subgroups. Since G is torsion-free, $K[G]$ is prime. Now suppose $\alpha\beta = 0$ for $\alpha, \beta \neq 0$. Then there exists some $\gamma \in K[G]$ with $\beta\gamma\alpha \neq 0$: Otherwise $(K[G]\beta K[G]) \cdot (K[G]\alpha K[G]) = 0$. Now $(1 -$

$\beta\gamma\alpha)(1 + \beta\gamma\alpha) = 1$ and $1 + \beta\gamma\alpha$ is a non-trivial unit, since if it were trivial then $\beta\gamma\alpha = kg - 1$, but $0 = (\beta\gamma\alpha)^2 = k^2g^2 - 2kg + 1$, which is absurd unless $g = 1$, in which case $\beta\gamma\alpha = k - 1$ again squares to zero, hence $\beta\gamma\alpha = 0$. \square

Definition 1.8. A group G is residually finite if for all $1 \neq g \in G$ there exists a homomorphism $\varphi_g : G \rightarrow Q$, Q finite, such that $\varphi_g(g) \neq 1$.

We will see later that the direct finiteness conjecture is true for $K = \mathbb{C}$. For now, we prove

Proposition 1.9. *Let G be residually finite. Then $K[G]$ is directly finite.*

Proof. A group homomorphism $\varphi : G \rightarrow Q$ induces a ring homomorphism $K[G] \rightarrow K[Q]$. Thus $K[Q]$ is a $K[G]$ -module. Note that Q is a basis for the K -vector space $K[Q]$, so if Q is finite this is a finite dimensional representation of G on $V = K[Q]$.

Suppose $\alpha\beta = 1$ in $K[G]$. Let $A = \text{supp}(\alpha) := \{g \in G \mid (\alpha)_g \neq 0\}$, $B = \text{supp}(\beta)$. Let $C = BA$. By residual finiteness, there is a finite quotient $\varphi : G \rightarrow Q$ which is injective on C . Now the induced maps $\rho_\alpha, \rho_\beta \in \text{End}(V)$ satisfy $\rho_\alpha \circ \rho_\beta = \rho_{\alpha\beta} = \text{id}_V$ and thus – since V is finite-dimensional – we have $\rho_\beta \circ \rho_\alpha = \text{id}_V$ as well. Write $\beta_\alpha = \sum_{c \in C} (\beta\alpha)_c c$ and thus

$$\rho_{\beta\alpha}(1_Q) = \varphi(\beta\alpha) = \sum_{c \in C} (\beta\alpha)_c \varphi(c) = 1_Q$$

forces $(\beta\alpha)_c = 1$ if $c = 1$ and 0 else. \square

1.1 The Unit Conjecture

There is only one known way to probe the unit conjecture for a given group G : the unique product property.

Definition 1.10. A group G has the *unique product property* (UPP, "has unique products", "has UP") if for all non-empty finite subsets $A, B \subseteq G$ there exists some $g \in G$ s.t. $g = ab$ for a unique pair $(a, b) \in A \times B$.

Example 1.11. In $(\mathbb{Z}, +)$, given finite $A, B \subseteq \mathbb{Z}$, one can take $g = \max A + \max B$. Hence \mathbb{Z} has unique products.

Remark 1.12. A group with unique products is torsion-free: If $1 \neq H \leq G$, H finite, then take $A = B = H$. Each product now occurs exactly $|H|$ times.

Remark 1.13. It's difficult to produce torsion-free groups that don't have UP.

Proposition 1.14. *A group with UP satisfies the zero divisor conjecture for all fields K .*

Proof. Let $\alpha, \beta \in K[G]$ with $\alpha, \beta \neq 0$, and set $A = \text{supp}(\alpha)$, $B = \text{supp}(\beta)$. Write $\alpha = \sum_{a \in A} \lambda_a a$ and $\beta = \sum_{b \in B} \mu_b b$. Then if $g = a_0 b_0$, $a_0 \in A$, $b_0 \in B$ is a unique product for A, B , then we have

$$(\alpha\beta)_g = \sum_{ab=g} \lambda_a \mu_b = \lambda_{a_0} \mu_{b_0} \neq 0.$$

Hence $\alpha\beta \neq 0$ in $K[G]$. \square

For the unit conjecture, we need something that is a priori stronger.

Definition 1.15. A group G has the *two unique products property* if for all finite subsets $A, B \subseteq G$ with $|A| \cdot |B| \geq 2$, there exist $g_0 \neq g_1 \in G$, such that $g_0 = a_0 b_0$ and $g_1 = a_1 b_1$ for unique pairs $(a_0, b_0), (a_1, b_1) \in A \times B$.

Proposition 1.16 (Strognowski). *The two unique products property is equivalent to the unique product property.*

Proof. If G satisfies 2UPP, it clearly satisfies UPP (if $|A| = |B| = 1$, the product is clearly unique).

Conversely, assume that G has UP but that there exist finite sets $A, B \subseteq G$ with $|A||B| \geq 2$ with only 1 unique product. Without loss (by translating A on the left and B on the right), we may assume that $1 = 1 \cdot 1$ is the unique unique product. Now let $C = B^{-1}A$ and $D = BA^{-1}$. We claim that now there is unique product for C and D . Every element of CD can be written as $b_1^{-1}a_1b_2a_2^{-1}$ for some $a_i \in A, b_i \in B$. If $(a_1, b_2) \neq (1, 1)$ then by assumption there is another pair a'_1, b'_2 s.t. $a_1b_2 = a'_1b'_2$ and thus $b_1^{-1}a_1b_2a_2^{-1} = b_1^{-1}a'_1b'_2a_2^{-1}$ is not a unique product for CD . If, on the other hand, $(a_1, b_2) = (1, 1)$, then unless $(a_2, b_1) = (1, 1)$, we find a'_2, b'_1 such that

$$b_1^{-1}a_1b_2a_2^{-1} = b_1^{-1}a_2^{-1} = (a_2b_1)^{-1} = (a'_2b'_1)^{-1} = b'^{-1}_1a_1b_2a'^{-1}_2$$

is not a unique product. Finally, if $a_2 = b_1 = 1$, then our element of CD is $1 = 1 \cdot 1 = b^{-1}b = aa^{-1}$ for any $a \in A, b \in B$, and A or B has an element other than 1, which gives more than one factorisation. \square

Corollary 1.17. *A group with UP satisfies the unit conjecture.*

Proof. Exercise. \square

Most examples of groups with UP are left-orderable.

1.2 Ordered Groups and related Properties

Definition 1.18. A group G is *(left-)orderable* if it admits a total order \prec that is left-invariant, i.e. if $g \prec h$, then $kg \prec kh$ for all $g, h, k \in G$.

Remark 1.19. Being left- and right-orderable are equivalent (define $g \prec' h$ iff $g^{-1} \prec h^{-1}$) but admitting a bi-invariant total order is much stronger.

Proposition 1.20. *A left-orderable group G has unique products.*

Proof. Fix a left-order \prec . Given finite subsets $A, B \subseteq G$, we show that the maximum of AB is a unique product. Let $b_0 = \max B$. Then for all $a \in A, b \in B \setminus \{b_0\}$, we have $b \prec b_0$, so $ab \prec ab_0$. Thus the maximum of AB can only be written as ab_0 for some $a \in A$, and thus must be unique. \square

Remark 1.21. It is not necessarily true that $\max(AB) = \max A \cdot \max B$.

Definition 1.22. For a left-ordered group (G, \prec) , the set $\mathcal{P} = \{g \in G \mid 1 \prec g\}$ is called its *positive cone*.

The positive cone clearly satisfies $\mathcal{P}^2 \subseteq \mathcal{P}$ (i.e. it's a subsemigroup) and $G = \mathcal{P} \sqcup \{1\} \sqcup \mathcal{P}^{-1}$. The converse is also true:

Lemma 1.23. *Left-orders are equivalent to choices of $\mathcal{P} \subseteq G$ satisfying $\mathcal{P}^2 \subseteq \mathcal{P}$ and $G = \mathcal{P} \sqcup \{1\} \sqcup \mathcal{P}^{-1}$.*

Proof. Exercise. \square

Lemma 1.24. *A group G is left-orderable if and only if for all $g_1, \dots, g_n \in G \setminus \{1\}$, there exists a choice of signs $\varepsilon_1, \dots, \varepsilon_n \in \{1, -1\}$ such that $1 \notin S(g_1^{\varepsilon_1}, \dots, g_n^{\varepsilon_n})$ (the subsemigroup generated by $g_1^{\varepsilon_1}, \dots, g_n^{\varepsilon_n}$).*

Proof. If G is left-ordered, set $\varepsilon_i = 1$ iff $g_i \in \mathcal{P}$.

For the other implication, we use compactness (slogan: the inverse limit of non-empty finite sets is non-empty). Let $X = \{1, -1\}^{G \setminus \{1\}}$ be the set of functions $G \setminus \{1\} \rightarrow \{1, -1\}$, and let $A \subseteq X$ be the set of those functions that define a positive cone. This is equivalent to satisfying (simultaneously) the condition on choice of sign for all possible $g_1, \dots, g_n \in G \setminus \{1\}$ (for $n = 3$). That is, if we denote such functions $A_{\{g_1, \dots, g_n\}} \subseteq X$, then

$$A = \bigcap_{\substack{S \subseteq G \setminus \{1\} \\ S \text{ finite}}} A_S$$

But X is compact by Tychonoff and all the A_S are closed. Furthermore, all finite intersections of the A_S are non-empty by assumption. So $A \neq \emptyset$. \square

We apply the lemma to prove

Theorem 1.25 (Burns-Hale, 1972). *Let G be a group. If every non-trivial finitely generated subgroup of G has a non-trivial left-orderable quotient, then G is left-orderable.*

In particular, a locally indicable group (i.e. every nontrivial finitely generated subgroup surjects onto \mathbb{Z}) is left-orderable.

Corollary 1.26 (Higman, 1940). *Locally indicable groups satisfy the unit conjecture.* \square

Example 1.27 (of locally indicable groups). • Free groups (Niedsen-Schreier)

- Fundamental groups of closed surfaces of non-positive Euler characteristic
- Torsion-free nilpotent groups
- Torsion-free one-relator groups, i.e. groups of the form $\langle X \mid r \rangle$, $r \in F(X)$, where r is not a proper power in $F(X)$ (Brodski-Howie)

Proof. (of 2.16) Suppose G is not left-orderable and let n be minimal such that $\exists g_1, \dots, g_n \in G \setminus \{1\}$ such that $1 \in S(g_1^{\varepsilon_1}, \dots, g_n^{\varepsilon_n})$ for all choices of $\varepsilon_i \in \{-1, 1\}$. Let $H = \langle g_1, \dots, g_n \rangle \neq 1$, so by assumption H has a non-trivial left-orderable quotient $q : H \twoheadrightarrow Q$. By relabelling, assume $g_1, \dots, g_t \in \ker(q)$ and $g_{t+1}, \dots, g_n \notin \ker(q)$. As $t < n$, we can assign $\varepsilon_1, \dots, \varepsilon_t$ such that $1 \notin S(g_1^{\varepsilon_1}, \dots, g_t^{\varepsilon_t})$. and since Q is left-orderable, we can assign $\varepsilon_{t+1}, \dots, \varepsilon_n$ such that $1 \notin S(q(g_{t+1})^{\varepsilon_{t+1}}, \dots, q(g_n)^{\varepsilon_n})$. But this implies $1 \notin S(g_1^{\varepsilon_1}, \dots, g_n^{\varepsilon_n})$ as every product of these elements either only uses $g_1^{\varepsilon_1}, \dots, g_t^{\varepsilon_t}$, hence lies in $S(g_1^{\varepsilon_1}, \dots, g_t^{\varepsilon_t})$ or has image under q in $S(q(g_{t+1})^{\varepsilon_{t+1}}, \dots, q(g_n)^{\varepsilon_n})$. \square

Proposition 1.28. $\text{Homeo}^+(\mathbb{R})$ is left-orderable.

Proof. Let $\{x_0, x_1, \dots\} \subseteq \mathbb{R}$ be dense. Define the order \prec on $f \in \text{Homeo}^+(\mathbb{R})$ via the lexicographic order on $(f(x_0), f(x_1), \dots)$. The map $f \mapsto (f(x_0), f(x_1), \dots)$ is injective (because continuous functions are determined by their values on a dense set), so the order descends. \square

Proposition 1.29. *A countable group is left-orderable if and only if it is a subgroup of $\text{Homeo}^+(\mathbb{R})$.*

Proof. Exercise. □

Proposition 1.30. *Let G be a group. Suppose $N \trianglelefteq G$ such that N and G/N both have unique products. Then G has unique products.*

Proof. Let $A, B \subseteq G$ be non-empty finite subsets. Write $\varphi : G \rightarrow G/N$. Suppose $\varphi(a) \cdot \varphi(b)$ is a unique product in G/N , $a \in A$, $b \in B$. By replacing A with $a^{-1}A$ and B with Bb^{-1} , we may assume the unique product in G/N is $1 \cdot 1 = 1$. Thus $a, b \in N$. Hence the unique product of $A \cap N$ and $B \cap N$ is a unique product for A and B . □

Definition 1.31. Let $A \subseteq G$ be a finite subset. An element $a \in A$ is called *extremal* (for A) if for all $s \in G \setminus \{1\}$ we have $as \notin A$ or $as^{-1} \notin A$. G is called *diffuse* if every non-empty finite subset $A \subseteq G$ has at least one extremal point.

Remark 1.32. $a \in A$ is extremal iff $a^{-1}A \cap A^{-1}a = \{1\}$

Proposition 1.33. *For any group G we have the implications*

$$\text{left-orderable} \implies \text{diffuse} \implies \text{unique products}.$$

Proof. Suppose $(G, <)$ is a left-ordered group and let $\emptyset \neq A \subseteq G$ a finite subset. Then let $a = \max A$. For any $s \in G \setminus \{1\}$ either $s > 1$ or $s^{-1} > 1$, hence $as > a$ or $as^{-1} > a$, i.e. a is extremal.

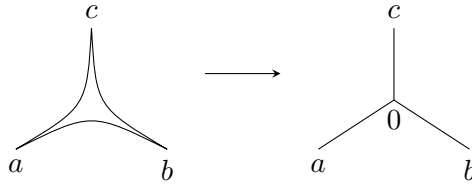
Suppose G is diffuse and let $A, B \subseteq G$ be non-empty finite subsets. Consider $C = AB$. Let $c = ab \in C$ be extremal. Suppose $c = a_1b_1$ with $b \neq b_1$. Then $c(b_1^{-1}b_2) = a_1b_2 \in C$ and $c(b_2^{-1}b_1) = a_2b_1 \in C$, in contradiction to extremity. □

Remark 1.34. Given a finite set $B \subseteq G$, we can easily decide if all $\emptyset \neq A \subseteq B$ have an extremal point, because if $a \in A_0 \subseteq A_1$ is extremal in A_1 , then it is also extremal in A_0 . Thus we can run a greedy algorithm, starting with $A = B$ and throwing out the extremal points at each step.

We can establish diffuseness geometrically, specifically for many hyperbolic groups.

2 Hyperbolic Groups

Geodesic triangles in the hyperbolic plane \mathbb{H}^2 resemble tripods.



Given three points in a metric space, they embed isometrically as the vertices of a unique tripod T_Δ . The length $d(0, a)$ must be $\frac{1}{2}(d(a, b) + d(a, c) - d(b, c)) =: (b \cdot c)_a$ which we call the Gromov product. Morally, this is the distance to the incircle. Let X be a geodesic¹ metric space. For a geodesic triangle $\Delta = \Delta(a, b, c)$, define $\mathcal{X}_\Delta : \Delta \rightarrow T_\Delta$ by mapping the geodesics isometrically. Δ is called δ -thin if $p, q \in \mathcal{X}_\Delta^{-1}(t)$, then $d_X(p, q) \leq \delta$ for all $t \in T_\Delta$.

Definition 2.1. X is called δ -hyperbolic if all geodesic triangles are δ -thin. X is called (Gromov) hyperbolic if it is δ -hyperbolic for some $\delta \geq 0$.

There are multiple equivalent definitions, e.g. slim triangles, but the constant δ needs to change.

Definition 2.2. A group G is called *hyperbolic* if it acts properly cocompactly by isometries on a proper hyperbolic space.

An action of a group G on a topological space X is *proper*, if for all compact $K \subseteq X$, the set $\{g \in G \mid gK \cap K \neq \emptyset\}$ is finite. It is *cocompact*, if there exists a compact $K \subseteq X$ such that $X = G \cdot K$. A metric space X is called *proper*, if $\bar{B}_r(x)$ is compact for all $x \in X, r \geq 0$.

Remark 2.3. For a proper metric space, an action $G \curvearrowright X$ is proper iff for all $x \in X, r \geq 0$, the set $\{g \in G : d(gx, x) \leq r\}$ is finite. The action is cocompact iff $X = G\bar{B}_r(x)$ for some $x \in X, r > 0$.

Example 2.4. A tree is 0-hyperbolic.

Corollary 2.5. $F_2 = \pi_1(S^1 \vee S^1)$ acts on the universal cover of $S^1 \vee S^1$, which is a locally finite graph. Hence F_2 is a hyperbolic group.

Lemma 2.6. Let $G \curvearrowright X$ be a proper cocompact isometric action on a proper metric space. Let $r > 0$. Then

$$\{g \in G \mid \exists x \in X : d(gx, x) \leq r\}$$

consists of finitely many conjugacy classes

Proof. By cocompactness, $X = G\bar{B}_{r_0}(x_0)$ for some $x_0 \in X, r_0 > 0$. Suppose $g \in G$ and $x \in X$ s.t. $d(gx, x) \leq r$. There exist $h \in G$ s.t. $x \in h\bar{B}_r(x_0)$, i.e. $d(x_0, h^{-1}x) \leq r_0$. Then

$$d(g^h h^{-1}x, h^{-1}x) = d(h^{-1}gx, h^{-1}x) = d(gx, x) \leq r.$$

Thus

$$d(g^h x_0, x_0) \leq d(g^h x_0, g^h h^{-1}x) + d(g^h h^{-1}x, h^{-1}x) + d(h^{-1}x, x_0) \leq 2r_0 + r.$$

By properness, there are only finitely many possibilities for g^h . □

An alternative definition for hyperbolic spaces is the four-point condition.

¹ $\forall x, y \in X \exists \text{geodesic } [x, y], \text{ i.e. an isometric embedding } i : [0, d(x, y)] \rightarrow X \text{ with } i(0) = x, i(d(x, y)) = y$

Definition 2.7. Let $\delta \geq 0$. A metric space X is (δ) -hyperbolic if $(xy)_w \geq \min\{(xz)_w, (yz)_w\} - \delta$ for all $x, y, z, w \in X$

Remark 2.8. This definition is arguably less intuitive, but it also works for non-geodesic metric spaces such as discrete spaces.

Proposition 2.9. Let X be a geodesic metric space. Then

- (i) X is (δ) -hyperbolic $\Rightarrow X$ is 4δ -hyperbolic.
- (ii) X is δ -hyperbolic $\Rightarrow X$ is (δ) -hyperbolic.

Proof. (i) Exercise.

(ii) Let $x, y, z, w \in X$. Pick $x' \in [w, x]$, $y' \in [w, y]$ and $z' \in [w, z]$ such that $d(w, x') = d(w, y') = d(w, z') = \min\{(x \cdot z)_w, (z \cdot y)_w\}$. By δ -thinness of $\Delta(w, x, z)$, we have $d(x', y') \leq \delta$. Similarly, $d(y', z') \leq \delta$, hence $d(x', z') \leq 2\delta$. Thus

$$d(x, y) \leq d(x, x') + 2\delta + d(y, y') = d(w, x) + d(w, y) + 2\delta - 2 \min\{(xz)_w, (yz)_w\},$$

which is equivalent to $(xy)_w \geq \min\{(xz)_w, (yz)_w\} - \delta$ □

The 4 point condition can also be phrased symmetrically: We have either $(xy)_w \geq (xz)_w - \delta$ or $(xy)_w \geq (yz)_w - \delta$, that is, $d(x, y) + d(z, w) \leq d(x, z) + d(y, w) + 2\delta$ or $d(x, y) + d(z, w) \leq d(x, w) + d(y, z) + 2\delta$, together

$$d(x, y) + d(w, z) \leq \max\{d(x, z) + d(y, w), d(x, w) + d(y, z)\} + 2\delta.$$

There are 3 ways to pair up $\{x, y, z, w\}$. Suppose $S \leq M \leq L$ are the corresponding sums of pair-distances. Then the above inequality is equivalent to $L \leq M + 2\delta$.

Theorem 2.10 (Delzant). Let X be a δ -hyperbolic geodesic metric space. Suppose $G \curvearrowright X$ by isometries s.t. for all $g \in G \setminus \{1\}$ and $x \in X$, we have $d(gx, x) > 3\delta$. Then G is diffuse.

Proof. We claim that for all $g \in G$, $1 \neq h \in G$ and $p \in X$ we have either $d(ghp, p) > d(gp, p)$ or $d(gh^{-1}p, p) > d(gp, p)$. Then we are done because for finite $A \subseteq G$ and any $p \in X$, an element $a \in A$ achieving $\max\{d(gp, p) \mid g \in A\}$ will be extremal.

Suppose that $d(gp, p) \geq d(ghp, p), d(gh^{-1}p, p)$ for some $g, h \in G, h \neq 1, p \in X$. Consider the symmetric 4-point condition for these four points as described above. The three possible distances are

$$\begin{aligned} d(gp, p) + d(ghp, gh^{-1}p) &= d(gp, p) + d(h^2p, p) \\ d(ghp, p) + d(gp, gh^{-1}p) &= d(ghp, p) + d(hp, p) \\ d(gh^{-1}p, p) + d(gp, ghp) &= d(gh^{-1}p, p) + d(hp, p) \end{aligned}$$

If we assume $d(h^2p, p) \geq d(hp, p)$, then the first of these three is the largest and thus by the 4-point condition $d(gp, p) + d(h^2p, p) \leq d(gh^{\pm 1}p, p) + d(hp, p) + 2\delta \leq d(gp, p) + d(hp, p) + 2\delta$. In either case, $d(h^2p, p) \leq d(hp, p) + 2\delta$. Thus $(hp, h^{-1}p)_p \geq \frac{1}{2}d(hp, p) - \delta$. If we let q be the midpoint of $[h^{-1}p, p]$, and let q', q'' on $[q, p]$ and $[hq, p]$ at distance δ from q , resp. hq . Then $d(q', q'') \leq \delta$ by δ -thinness of $\Delta(p, hp, h^{-1}p)$. (Pick the geodesic $[p, hp]$ so that it contains hq .) Together,

$$d(hq, q) \leq d(q, q') + d(q, q'') + d(q'', hq) \leq 3\delta,$$

in contradiction to the assumption $d(hq, q) > 3\delta$. □

Definition 2.11. Let X be a property of groups. Then G is *virtually* X if there exists a finite index subgroup $G_0 \leq G$ such that G_0 has X .

Corollary 2.12. *Let G be a residually finite hyperbolic group. Then G is virtually diffuse.*

Remark 2.13. It is a famous open problem whether every hyperbolic group is residually finite.

Proof. Let $G \curvearrowright X$ properly cocompactly by isometries on a proper δ -hyperbolic space. By Lemma 2.6, there exists $1 = g_0, \dots, g_n \in G$ s.t. for all $g \in G$, if there is $x \in X$ with $d(gx, x) \leq 3\delta$, then g is conjugate to some g_i . By residual finiteness, we can find $\varphi : G \rightarrow Q$ finite such that $\varphi(g_1), \dots, \varphi(g_n) \neq 1$. Then $G_0 = \ker(\varphi)$ satisfies the assumption of Delzant's theorem. \square

3 Primality of group rings

Our aim is to give a complete proof of the following, which was used to show that the unit conjecture for $K[G]$ implies the zero-divisor conjecture $K[G]$.

Theorem 3.1 (Connell). *$K[G]$ is prime if and only if G has no nontrivial finite normal subgroup.*

Recall that a ring R is prime if for all $0 \neq \alpha, \beta \in R$ there exists $\gamma \in R$ such that $\alpha\gamma\beta \neq 0$. (i.e. the zero ideal is a prime ideal in the sense of noncommutative ring theory.) For the proof, we need some more group ring basics, a fair bit of group theory and an ingenious trick of Passman.

Definition 3.2. Let $H \leq G$. Then there is a *projection* $\pi_H : K[G] \rightarrow K[H]$ defined by $\sum_{g \in G} a_g g \mapsto \sum_{g \in H} a_g g$.

Warning: This is never a ring homomorphism unless $G = H$. But we do have

Lemma 3.3. π_H is a homomorphism of $(K[H], K[H])$ -bimodules.

Proof. Exercise. \square

Corollary 3.4. *Let $H \leq G$. If $\alpha \in K[H]$ is a unit in $K[G]$, then it is a unit in $K[H]$.*

Proof. For $\beta \in K[G]$ with $\alpha\beta = \beta\alpha = 1$ we have $\alpha\pi_H(\beta) = \pi_H(\alpha\beta) = \pi_H(1) = 1 = \pi_H(\beta)\alpha$, so in fact $\alpha^{-1} = \beta = \pi_H(\beta) \in K[H]$. \square

Recall that a left transversal for $H \leq G$ is a set X containing exactly one representative x of each coset of H , so that $G = \bigsqcup_{x \in X} xH$

Lemma 3.5. *Let X be a left transversal for $H \leq G$. Then every element $\alpha \in K[G]$ can be written uniquely as a finite sum $\alpha = \sum_{x \in X} x\alpha_x$ with $\alpha_x \in H[X]$. In fact, $\alpha_x = \pi_H(x^{-1}\alpha)$. Thus $K[G]$ is a free right $K[H]$ -module with X as basis.* \square

Let $M_n(R)$ denote the ring of $n \times n$ -matrices over the ring R .

Lemma 3.6. *Let $[G : H] = n < \infty$. Then $K[G] \hookrightarrow M_n(K[H])$.*

Proof. Let $X = \{x_1, \dots, x_n\}$ be a left transversal for $H \leq G$. Then $V = K[G]$ is a free right $K[H]$ -module with basis X . It is also a left $K[G]$ -module and since left and right multiplication commute, $K[G]$ acts by $K[H]$ -linear transformations of $V \cong K[H]^n$. Since for each $\alpha \in K[G]$ and each index $1 \leq j \leq n$ we have $\alpha x_j = \sum_{i=1}^n x_i \pi_H(x_i^{-1} \alpha x_j)$, sending α to the matrix

$$\eta_X(\alpha) = (\pi_H(x_i^{-1} \alpha x_j))_{i,j=1,\dots,n}$$

defines an embedding (for choice of basis X). \square

Remark 3.7. If G is finite, $H = 1$, this is just the regular representation of G .

Example 3.8. Let $D_\infty = \langle r, t \mid r^2, t^r t \rangle = \mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ and take $X = \{1, r\}$ as transversal for $\langle t \rangle \cong \mathbb{Z}$ in D_∞ . Then we calculate $\alpha x_i = x_j \eta_X(\alpha)$ for $\alpha = r, t$. Since

$$r \cdot 1 = r \cdot 1, \quad r \cdot r = 1 \cdot 1, \quad t \cdot 1 = 1 \cdot t, \quad t \cdot r = r \cdot t^{-1},$$

the map $\eta_X : K[D_\infty] \rightarrow M_2(K[t, t^{-1}])$ is given by extending

$$r \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix}$$

Lemma 3.9 (Schur). *If $[G : Z(G)] < \infty$, then $|G'| < \infty$.*

Definition 3.10. Let $H \leq G$ and $[G : H] = n < \infty$. Pick a left transversal $\{x_1, \dots, x_n\}$ for H . For each $g \in G$ and $1 \leq j \leq n$ we have $gx_j = x_i h_j$ for some unique i and $h_j \in H$. The *transfer* is defined as the map $G/G' \rightarrow H/H'$ given by $gG' \mapsto h_1 h_2 \cdots h_n H'$.

Lemma 3.11. *The transfer is a group homomorphism and doesn't depend on the choice of transversal.*

Proof. Map $K[G] \rightarrow M_n(K[H])$ by lemma 3.6, $M_n(K[H]) \rightarrow M_n(K[H/H'])$ extending $H \rightarrow H/H'$ and $M_n(K[H/H']) \rightarrow H/H'$ by taking the determinant. For given g and $1 \leq j \leq n$, $gx_j = x_i h_j$, i.e. $h_j = x_i^{-1} g x_j$, so $\eta_X(g)_{ij} = h_j$ and $\eta_X(g)_{i'j} = 0$ for $i' \neq i$. Letting $\text{sgn}(g) \in \{\pm 1\}$ denote the sign of the permutation g induces on the set G/H , we have that the composition of our maps sends g to $\text{sgn}(g) h_1 h_2 \cdots h_n \in K[H/H']$. As $\text{sgn} : G \rightarrow \{\pm 1\}$ is a homomorphism, so is the map $G \rightarrow H/H' : g \mapsto h_1 \cdots h_n$. As the image is abelian, it factors through G/G' to define the transfer. It is independent of the choice of transversal X , since change of basis of $K[G]$ produces similar matrices. \square

Proof. (Schur) Let $Z = Z(G)$ and $[G : Z] = n$. Consider the transfer $G/G' \rightarrow Z/Z' = Z$. By centrality of Z , this is just $g \mapsto g^n$. Hence if $g \in G'$, then $g^n = 1$. If $\{x_1, \dots, x_n\}$ is a transversal, then every commutator is of the form $[x_i z_1, x_j z_2] = [x_i, x_j]$ and thus G' is finitely generated. Now $[G' : G' \cap Z] \leq n$, so $G' \cap Z$ is finitely generated, has finite exponent and is abelian, hence finite. Therefore G' is also finite. \square

Definition 3.12. The *FC-center* ("finite conjugacy") of a group G is $\Delta(G) = \{g \in G \mid |g^G| < \infty\}$, that is, the set of elements whose conjugacy class is finite. This is alternatively the set of elements whose centralizer $C_G(g)$ has finite index (by the orbit-stabilizer theorem for $G \curvearrowright G$ by conjugating). As $C_G(gh) \geq C_G(g) \cap C_G(h)$, we see that $\Delta(G)$ is in fact a (characteristic) subgroup of G . We call G an *FC-group* if $G = \Delta(G)$.

Lemma 3.13. *An FC-group is locally finite-by-(free abelian), i.e. all finitely generated subgroups are extensions of a finite by a free abelian group.*

Proof. Let $H = \langle h_1, \dots, h_n \rangle \leq G$, G an FC-group. Then $C_G(H) = \bigcap_{i=1}^n C_G(h_i)$ is finite index in G and thus $Z(H) = C_G(H) \cap H$ is finite index in H . Thus Schur's lemma applies and H' is finite. Now H/H' is a finitely generated abelian group, so of the form $T \oplus \mathbb{Z}^d$ with T finite. Thus the kernel of the torsion-free abelianization $H \rightarrow H/H' \rightarrow \mathbb{Z}^d$ is finite. \square