Group rings of infinite groups

Giles Gardam

University of Bonn
Email address: lastname@math.uni-bonn.de

The students of my lecture course in winter semester 2023/2024 provided much valuable feedback and I thank them for this. In particular, Guglielmo Cametti fixed multiple typos.
If you see an error in this manuscript, please send me a pull request at
`https://github.com/gilesgardam/lectures` (or, failing that, an email).

Contents

Preface

This lecture course covers various topics around group rings of infinite groups. We are motivated by geometric group theory but do not assume familiarity with it. Most of the course will treat the Kaplansky conjectures.

The main reference text is Passman's book [**Pas85**] but we often deviate from it, either to cut a quicker path to the specific applications we are interested in or because of developments since its publication. Some topics will use recent research articles.

CHAPTER 1

The Kaplansky conjectures

1.1. Introduction

Definition 1.1. Let R be a ring and G be a group. The *group ring* $R[G]$ consists of finite formal R-linear sums

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

with multiplication

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

In this course, we'll almost always have $R = \mathbb{Z}$ or $R = K$ a field; in the latter case, one often calls $K[G]$ the *group algebra*.

From now on:
G will always be a group,
K will always be a field, and
R will always be a ring.

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

A viewpoint due to Noether: Representations of G on K-vector spaces are $K[G]$-modules.

Warning 1.3. $K[G]$ is non-commutative unless G is abelian. It is (left) Noetherian only in special settings and it is never semisimple for infinite G (cf. Maschke's theorem).

Although group rings tend to have bad ring theoretic properties, they conjecturally have nice elementary properties. Note first that for $k \in K \setminus \{0\}$ and $g \in G$, the element $kg \in K[G]$ is a unit (with $(k \cdot g)^{-1} = k^{-1} \cdot g^{-1}$); such units are called *trivial*. A group is called *torsion-free* if it has no non-trivial finite order elements. For example, fundamental groups of aspherical manifolds are torsion-free.

Definition 1.4. Let $\mathcal{P}$ be a property of groups. A group G is *virtually* $\mathcal{P}$ if it has a finite-index subgroup G_0 with $\mathcal{P}$.

As another example, a finitely generated subgroup of $\mathrm{GL}_n(\mathbb{C})$ is virtually torsion-free (Selberg).

Conjecture 1.5 (The Kaplansky conjectures)**.** If G is torsion-free, then $K[G]$ has

- no non-trivial units: $\alpha\beta = \beta\alpha = 1 \implies \alpha = kg$ for some $k \in K^\times, g \in G$
- no non-zero zero divisors: $\alpha\beta = 0 \implies \alpha = 0$ or $\beta = 0$, and

- no non-trivial idempotents: $\alpha^2 = \alpha \implies \alpha = 0$ or $\alpha = 1$.

For *any* G (possibly with torsion), $K[G]$ is

- directly finite: $\alpha\beta = 1 \implies \beta\alpha = 1$.

These are the unit conjecture, zero divisor conjecture, idempotent conjecture and direct finiteness conjectures respectively. (Direct finiteness is also called *Dedekind finiteness* or *von Neumann finiteness.*)

Remark 1.6. The unit conjecture is false; the others are open.

Remark 1.7. Torsion-freeness is essential. For example, if $g \in G$ has order $n \geq 2$ then $(1-g)(1+g+\cdots+g^{n-1}) = 1-g^n = 0$.

Remark 1.8. These conjectures are "local" in the sense that they only depend on the finitely generated subgroups of G.

Proposition 1.9. For a given torsion-free group G and field K, we have

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

Proof. The 3 weaker conjectures are ring theoretic statements and their implications are easy ring theoretic observations: if $\alpha\beta = 1$ and $\beta\alpha \neq 1$ then $(\beta\alpha)^2 = \beta(\alpha\beta)\alpha = \beta\alpha$ is a non-trivial idempotent. If $\alpha^2 = \alpha$ is a non-trivial idempotent, then $\alpha^2 - \alpha = \alpha(\alpha - 1) = 0$ with both factors non-zero.

The unit conjecture is a "group ring theoretic" statement and the proof of the implication requires the following (which we'll prove later using group theory):

Theorem 1.10 (Connell). *$K[G]$ is prime if and only if G has no non-trivial finite normal subgroup.*

A non-commutative ring R is called *prime* if the zero ideal is not a product of two non-zero ideals. This is equivalent to saying that for all $0 \neq \alpha, \beta \in R$ there exists $\gamma \in R$ with $\alpha\gamma\beta \neq 0$.

Since G is torsion-free, $K[G]$ is prime. Suppose that $\alpha\beta = 0$ for $\alpha, \beta \neq 0$. Then there exists $\gamma \in K[G]$ with $\beta\gamma\alpha \neq 0$. Now

$$(1+\beta\gamma\alpha)(1-\beta\gamma\alpha) = 1 - \beta\gamma(\alpha\beta)\gamma\alpha = 1.$$

Thus $1+\beta\gamma\alpha$ is a non-trivial unit, since if it were trivial then $\beta\gamma\alpha = kg - 1$ which implies $k^2g^2 - 2kg + 1 = 0$ which is absurd unless $g = 1$, which then forces $\beta\gamma\alpha \in K$ so $\beta\gamma\alpha = 0$ since it is nilpotent. □

Definition 1.11. A group G is *residually finite* if for all $1 \neq g \in G$ there exists a homomorphism $\phi_g \colon G \to Q$ to a finite group such that $\phi_g(g) \neq 1$.

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

Proposition 1.12. Let G be residually finite. Then $K[G]$ is directly finite.

Notation 1.13. For $\alpha \in K[G]$ and $g \in G$, let $(\alpha)_g \in K$ denote the coefficient of g in α. Then $\alpha = \sum_{g\in G}(\alpha)_g \cdot g$ and $(\alpha)_g = 0$ for all but finitely many elements of G.

Definition 1.14. An element $\alpha \in K[G]$ has *support*

$$\operatorname{supp}(\alpha) = \{g \in G \mid (\alpha)_g \neq 0\}.$$

Proof. Suppose $\alpha, \beta \in K[G]$ with $\alpha\beta = 1$. A group homomorphism $\phi\colon G \to Q$ induces a ring homomorphism $K[G] \to K[Q]$. 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 $V = K[Q]$.

Let $A = \operatorname{supp}(\alpha)$, $B = \operatorname{supp}(\beta)$. Let $C = BA = \{ba \mid a \in A, b \in B\}$. By residual finiteness, there is a finite quotient $\phi\colon G \twoheadrightarrow Q$ which is injective on C: take the product of homomorphisms ϕ_g given by the definition over all $g \in C^{-1}C \setminus \{1\}$ (and let Q be the image of this product homomorphism).

Now the induced maps $\rho_\alpha, \rho_\beta \in \operatorname{End}(V)$ satisfy $\rho_\alpha \circ \rho_\beta = \mathrm{id}_V$ and thus – since $V = K[Q]$ is finite dimensional – we have $\rho_\beta \circ \rho_\alpha = \mathrm{id}_V$.

But we can write $\beta\alpha = \sum_{c\in C} (\beta\alpha)_c \cdot c$ and thus

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

forces (since all $\phi(c)$ are distinct!)

$$(\beta\alpha)_c = \begin{cases} 1 & c = 1 \\ 0 & \text{else} \end{cases}$$

that is, $\beta\alpha = 1$. □

1.2. Proving the unit conjecture

There is only one way known to prove the unit conjecture: the unique product property.

Definition 1.15. A group G has the *unique product property* (or "has unique products", or "has UP") if for all non-empty finite subsets $A, B \subseteq G$ there exists $g \in G$ such that $g = ab$ for a unique pair $(a, b) \in A \times B$.

Example 1.16. In $(\mathbb{Z}, +)$ the "product" $\max(A) + \max(B)$ is unique.

Remark 1.17. A group with UP is torsion-free: if $1 \neq H \leq G$ is a finite subgroup, set $A = B = H$. Each product occurs exactly $|H|$ times.

Proposition 1.18. A group G with UP satisfies the zero divisor conjecture.

Proof. Let $\alpha, \beta \in K[G]$ with $\alpha, \beta \neq 0$ and set $A = \operatorname{supp}(\alpha), B = \operatorname{supp}(\beta)$. Write

$$\alpha = \sum_{a\in A} \lambda_a \cdot a$$
$$\beta = \sum_{b\in B} \mu_b \cdot b.$$

Then if $g_0 = a_0 b_0$ is a unique product for (A, B) we have

$$(\alpha\beta)_{g_0} = \sum_{gh=g_0} \lambda_g \mu_h = \lambda_{a_0}\mu_{b_0} \neq 0$$

and thus $\alpha\beta \neq 0$. □

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

Definition 1.19. A group G has the *two unique products property* if for all finite subsets $A, B \subseteq G$ with $|A||B| \geq 2$, there exist elements $g_0 \neq g_1$ of G such that $g_0 = a_0 b_0$ for a unique pair $(a_0, b_0) \in A \times B$ and $g_1 = a_1 b_1$ for a unique pair $(a_1, b_1) \in A \times B$.

Proposition 1.20 (Strojnowski)**.** The two unique product property is equivalent to the unique product property.

Proof. TUP $\implies$ UP is immediate (TUP doesn't apply if $|A| = |B| = 1$, but if $|A| = 1$ or $|B| = 1$, then all products are unique!)

Suppose now G has UP but that finite sets $A, B \subseteq G$ with $|A||B| \geq 2$ have only 1 unique product. Without loss of generality, by translating A on the left and B on the right, we can assume that $1 = 1 \cdot 1$ is the unique unique product.

Now let $C = B^{-1}A$, $D = BA^{-1}$. We claim that $C \cdot D$ has no unique product, giving the desired contradiction. Every element of CD can be written as $b_1^{-1} a_1 b_2 a_2^{-1}$ for some $a_1, a_2 \in A$, $b_1, b_2 \in B$.

If $(a_1, b_2) \neq (1, 1)$, then by assumption there is another pair (a_1', b_2') with $a_1' b_2' = a_1 b_2$ and thus

$$(b_1^{-1} a_1) \cdot (b_2 a_2^{-1}) = (b_1^{-1} a_1') \cdot (b_2' a_2^{-1})$$

is *not* a unique product for (C, D).

If $(a_1, b_2) = (1, 1)$, then unless $(a_2, b_1) = (1, 1)$ we can write

$$b_1^{-1} \cdot a_2^{-1} = (a_2 b_1)^{-1} = (a_2' b_1')^{-1} = (b_1')^{-1} (a_2')^{-1}$$

with $a_2 \neq a_2'$ (and $b_1 \neq b_1'$). Finally, if $(a_1, b_2) = (1, 1)$ and $(a_2, b_1) = (1, 1)$, then our element of CD is $1 = 1 \cdot 1 = b^{-1} \cdot b = a \cdot a^{-1}$ for any $a \in A$ or $b \in B$. □

Corollary 1.21. *A group with UP satisfies the unit conjecture.*

Proof. Exercise. □

Most examples of groups with UP are orderable groups.

Definition 1.22. A group G is *left-orderable* if it admits a total order $<$ that is left-invariant, that is, $g < h$ implies $kg < kh$ for all $g, h, k \in G$.

Remark 1.23. Being left-orderable and right-orderable are equivalent, but admitting a bi-invariant total order is much stronger!

Proposition 1.24. A left-orderable group has UP.

Proof. We show that the maximum of AB is a unique product. Let $b_0 = \max B$. Then for all $a \in A$ and $b \in B \setminus \{b_0\}$ we have $b < b_0 \implies ab < ab_0$. Thus the maximum of AB can only be written as $a \cdot b_0$ and this expression must be unique (as $a_i \neq a_j \implies a_i b_0 \neq a_j b_0$). □

Remark 1.25. It is *not* necessarily true that $\max(AB) = \max(A)\max(B)$!

Definition 1.26. For a left-ordered group $(G, <)$, the set

$$\mathcal{P} = \{g \in G \mid 1 < g\}$$

is called its *positive cone*.

The positive cone satisfies

(1) $\mathcal{P}^2 \subseteq \mathcal{P}$ (that is, it is a subsemigroup)

(2) $G = \mathcal{P} \sqcup \{1\} \sqcup \mathcal{P}^{-1}$.

Lemma 1.27. *Left-orderings are equivalent to choice of $\mathcal{P} \subset G$ satisfying (1) and (2).*

Proof. Exercise (hint: $x < y \Leftrightarrow 1 < x^{-1}y$). □

Lemma 1.28. *A group G is left-orderable if and only if for all $g_1, \ldots, g_n \in G \setminus \{1\}$ there exists a choice of signs $\epsilon_1, \ldots, \epsilon_n \in \{1, -1\}$ such that*

$$1 \notin S(g_1^{\epsilon_1}, \ldots, g_n^{\epsilon_n}),$$

the subsemigroup generated by $g_1^{\epsilon_1}, \ldots, g_n^{\epsilon_n}$.

Proof. $\Rightarrow$ set $\epsilon_i = 1$ if $g_i \in \mathcal{P}$ (that is, $1 < g_i$) else -1.

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

$$A = \bigcap_{\text{finite } S \subset G \setminus \{1\}} A_S.$$

But X is compact by Tychonoff and the A_S are closed (only depend on the restriction to $S \to \{1, -1\}$) and have all finite intersections non-empty by assumption. Thus $A \neq \emptyset$. □

We will apply the lemma to prove the following:

Theorem 1.29 (Burns–Hale). *If every finitely generated non-trivial subgroup of G has a non-trivial left-orderable quotient, then G is left-orderable.*

Definition 1.30. Let $\mathcal{P}$ be a property of groups. A group G is *locally* $\mathcal{P}$ if every finitely generated subgroup of G has $\mathcal{P}$.

We call a group *indicable* if it either maps onto $\mathbb{Z}$ or is trivial. So the Burns–Hale theorem says in particular that a *locally indicable* group is left-orderable.

Corollary 1.31 (Higman, 1940)**.** *Locally indicable groups satisfy the conjectures on units and zero divisors.*

Proof. Locally indicable $\implies$ left-orderable $\implies$ UP. □

Example 1.32. The following groups are locally indicable:

- free groups (subgroups of free groups are free by Nielsen–Schreier)
- fundamental groups of surfaces of non-positive Euler characteristic
- torsion-free nilpotent groups
- torsion-free one-relator groups i.e. groups of the form $\langle X \,|\, r \rangle$ where $r \in F(X)$ is not a proper power (Brodskii, Howie)

Proof of Burns–Hale theorem. Suppose G is not left-orderable and let n be minimal such that there exist $g_1, \ldots, g_n \in G \setminus \{1\}$ with $1 \in S(g_1^{\epsilon_1}, \ldots, g_n^{\epsilon_n})$ for all choices of ϵ_i. Let $H = \langle g_1, \ldots, g_n \rangle \leq G$. By assumption, H has a non-trivial left-orderable quotient $q \colon H \twoheadrightarrow Q$. By relabelling, assume $g_1, \ldots, g_t \in \ker(q)$ and $g_{t+1}, \ldots, g_n \notin \ker(q)$. As $t < n$, we can assign $\epsilon_1, \ldots, \epsilon_t$ such that

$$1 \notin S(g_1^{\epsilon_1}, \ldots, g_t^{\epsilon_t}),$$

and since Q is left-orderable we can assign $\epsilon_{t+1}, \dots, \epsilon_n$ such that

$$1 \notin S(q(g_{t+1})^{\epsilon_{t+1}}, \dots, q(g_n)^{\epsilon_n}).$$

But this implies that

$$1 \notin S(g_1^{\epsilon_1}, \dots, g_n^{\epsilon_n})$$

as every non-empty product of those elements *either* only uses $g_1, \dots, g_t$ so lies in $S(g_1^{\epsilon_1}, \dots, g_t^{\epsilon_t})$ *or* has image under q in $S(q(g_{t+1})^{\epsilon_{t+1}}, \dots, q(g_n)^{\epsilon_n})$. □

The dynamical point of view.

Proposition 1.33. The group $\mathrm{Homeo}^+(\mathbb{R})$ of orientation-preserving (i.e. increasing) homeomorphisms of the real line is left-orderable.

Proof. Let $\{x_0, x_1, x_2, \dots\} \subset \mathbb{R}$ be dense (e.g. enumerate $\mathbb{Q}$). Then we define $f < g$ for $f \neq g \in \mathrm{Homeo}^+(\mathbb{R})$ by

$$f < g \Leftrightarrow f(x_i) < g(x_i) \text{ for the minimal } i \in \mathbb{N} \text{ s.t. } f(x_i) \neq g(x_i).$$

(Such an i exists as continuous functions to Hausdorff spaces are determined by their values on dense subsets.) Left-invariance is immediate as elements of $\mathrm{Homeo}^+(\mathbb{R})$ are strictly monotone (and we take $\mathrm{Homeo}^+(\mathbb{R})$ to act on $\mathbb{R}$ on the left!). Let $f, g, h \in \mathrm{Homeo}^+(\mathbb{R})$ with $f < g$ and $g < h$ and let $i \in \mathbb{N}$ be the minimal index such that $f(x_i) \neq g(x_i)$ or $g(x_i) \neq h(x_i)$. Then $f(x_i) \leq g(x_i)$ and $g(x_i) \leq h(x_i)$ with at least one inequality being strict, so $f(x_i) < h(x_i)$. Moreover, for $j < i$ we have $f(x_j) = g(x_j) = h(x_j)$, so $f < h$. □

In fact:

Proposition 1.34. A countable group is left-orderable if and only if it is a subgroup of $\mathrm{Homeo}^+(\mathbb{R})$.

Proof. Exercise. □

Proposition 1.35. Suppose that $N \lhd G$ such that N and G/N both have UP. Then G has UP.

Proof. Let $A, B \subset G$ be finite non-empty subsets and write $\phi \colon G \twoheadrightarrow G/N$. Suppose $\phi(a_1) \cdot \phi(b_1)$ is a unique product for $\phi(A) := \{\phi(a) \mid a \in A\}$ and $\phi(B)$ in G/N. By replacing A with $a_1^{-1}A$ and B with Bb_1^{-1}, we can assume without loss of generality that $\phi(a_1) = \phi(b_1) = 1$. Thus for $a \in A$ and $b \in B$ we have

$$ab \in N \Leftrightarrow \phi(ab) = 1 \Leftrightarrow \phi(a) = 1 \text{ and } \phi(b) = 1 \Leftrightarrow a \in N \text{ and } b \in N$$

Hence the unique product of the non-empty finite sets $A \cap N$ and $B \cap N$ in the UP group N is a unique product for A and B. □

Diffuse groups. We now meet the weakest property known to imply UP.

Definition 1.36. Let $A \subset G$ be a finite subset. An element $a \in A$ is called *extremal* if for all $1 \neq s \in G$, either $as \notin A$ or $as^{-1} \notin A$ (or both). A group is called *diffuse* if every non-empty finite subset contains an extremal element.

Remark 1.37. $a \in A$ is extremal if and only if $a^{-1}A \cap A^{-1}a = \{1\}$.

Remark 1.38. This notion has been called "weakly diffuse" with diffuse reserved for the *a priori* stronger property that any $A \subset G$ with $2 \leq |A| < \infty$ has at least 2 extremal points, but they turn out to be equivalent.

Proposition 1.39. For any group we have the implications

$$\text{left-orderable} \implies \text{diffuse} \implies \text{UP}.$$

Proof. Suppose $(G,<)$ is left-ordered. Let $A \subset G$ be an arbitrary non-empty finite subset and let $a = \max A$. For any $1 \neq s \in G$ either $1 < s$ or $1 < s^{-1}$, which implies either $a < as$ or $a < as^{-1}$. Thus a is extremal. Hence G is diffuse.

Suppose G is diffuse and let $A, B \subset G$ be non-empty finite subsets. Consider $C = AB$. Let $c \in C$ be an extremal point and pick some $a_1 \in A, b_1 \in B$ such that $c = a_1 b_1$. We claim that this is a unique product. Suppose for the sake of contradiction that $c = a_2 b_2$ with $b_1 \neq b_2$ (and $a_2 \in A$, $b_2 \in B$). Then

$$c \cdot (b_2^{-1} b_1) = a_2 b_2 \cdot (b_2^{-1} b_1) = a_2 b_1 \in C$$
$$c \cdot (b_2^{-1} b_1)^{-1} = a_1 b_1 \cdot (b_1^{-1} b_2) = a_1 b_2 \in C$$

contradicting diffuseness. □

Remark 1.40. Given finite $B \subset G$ we can easily decide if all non-empty $A \subseteq B$ have an extremal point because if $a \in A_0 \subseteq A_1$ and a 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 all extremal points at each step (checking extremality in finitely many steps via Remark 1.37), seeing if we terminate with $A = \emptyset$ or with a non-empty set A that falsifies diffuseness.

Exercise 1.2.1. Show that the following classes of groups are closed under taking extensions:

- locally indicable groups
- left-orderable groups
- diffuse groups

1.3. Hyperbolic groups

Geodesics in the hyperbolic plane resemble tripods.

Given 3 points a, b, c in a metric space, they map isometrically to the vertices $\overline{a}, \overline{b}, \overline{c}$ of a unique tripod with central vertex $\overline{o}$.

The length $d(\overline{o}, \overline{a})$ 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, it measures “distance to the incircle”.

Let X be a geodesic metric space, i.e. a metric space such that for all $x, y \in X$ there is an isometric embedding $p\colon [0, d(x,y)] \to X$ of an interval (standard metric on $\mathbb{R}$) such that $p(0) = x$ and $p(d(x,y)) = y$. We denote the image of such a geodesic p from x to y by $[x,y]$. For a geodesic triangle $\Delta = \Delta(a,b,c)$, define

$$\chi_\Delta\colon \Delta \to T_\Delta$$

by mapping the three geodesics isometrically to the comparison tripod T_Δ. For $\delta \geq 0$, Δ is called *δ-thin* if $p, q \in \chi_\Delta^{-1}(t)$ implies $d(p,q) \leq \delta$ for all $t \in T_\Delta$.

Definition 1.41. Let $\delta \geq 0$. A geodesic metric space X is called *δ-hyperbolic* if every geodesic triangle is δ-thin. X is called *(Gromov) hyperbolic* if it is δ-hyperbolic for some $\delta \geq 0$.

Example 1.42. A tree is 0-hyperbolic.

Warning 1.43. There are multiple equivalent definitions of hyperbolicity, but the constant δ will need to change in general.

Definition 1.44. A group G is called *hyperbolic* if it acts properly cocompactly by isometries on a proper geodesic hyperbolic space.

Example 1.45.

- A free group acting a tree (deck transformations on universal cover of rose graph).
- The fundamental group of a closed hyperbolic surface acting on the hyperbolic plane.

Definition 1.46. An action $G \curvearrowright X$ by homeomorphisms of a topological space is called *proper* if for all compact $K \subseteq X$, the set $\{g \in G \,|\, gK \cap K \neq \emptyset\}$ is finite. It is called *cocompact* if there exists compact $K \subseteq X$ such that $X = G \cdot K$.

Definition 1.47. A metric space X is called *proper* if for all $x \in X$ and for all $r \geq 0$, the closed ball $\overline{B}(x,r) := \{y \in X \,|\, d(x,y) \leq r\}$ is compact.

Remark 1.48. For a proper metric space X, an action $G \curvearrowright X$ by isometries is proper if and only if for all $x \in X$ and $r \geq 0$, the set $\{g \in G \,|\, d(g \cdot x, x) \leq r\}$ is finite and it is cocompact if and only if for all $x \in X$ there exists $r \geq 0$ such that $X = G \cdot \overline{B}(x,r)$.

Lemma 1.49. *Let $G \curvearrowright X$ be a proper cocompact action by isometries on a proper metric space. Let $R \geq 0$. Then*

$$S_R = \{g \in G \,|\, \exists\, x \in X \text{ s.t. } d(g \cdot x, x) \leq R\}$$

consists of finitely many conjugacy classes.

Proof. Pick some basepoint $x_0 \in X$. By cocompactness, there exists $r_0 \geq 0$ such that $X = G \cdot \overline{B}(x_0, r_0)$. Suppose $g \in G$ and $x \in X$ with $d(g \cdot x, x) \leq R$. Since $X = G \cdot \overline{B}(x_0, r_0)$, there exists $h \in G$ such that $x_1 := h^{-1} \cdot x \in \overline{B}(x_0, r_0)$. Then

$$d(g^h \cdot x_1, x_1) = d(h^{-1}gh \cdot (h^{-1} \cdot x), h^{-1} \cdot x) = d(h^{-1}gx, h^{-1}x) = d(g \cdot x, x) \leq R$$

and thus

$$d(g^h \cdot x_0, x_0) \leq d(g^h \cdot x_0, g^h \cdot x_1) + d(g^h \cdot x_1, x_1) + d(x_1, x_0) \leq 2r_0 + R$$

so by properness there are only finitely many possibilities for g^h. Thus the elements of S_R are contained in finitely many conjugacy classes. Since $d(g^h \cdot (h^{-1} \cdot x), h^{-1} \cdot x) = d(g \cdot x, x)$ for all $g, h \in G$ and $x \in X$, we note that S_R will be a union of conjugacy classes.

□

Definition 1.50 (4-point condition)**.** Let $\delta \geq 0$. A metric space X is (δ)-hyperbolic if

$$(*) \qquad (x \cdot y)_w \geq \min\{(x \cdot z)_w, (y \cdot z)_w\} - \delta$$

for all $w, x, y, z \in X$.

Remark 1.51. This definition is arguably less intuitive, but it also works for non-geodesic metric spaces e.g. discrete metric spaces.

Proposition 1.52. Let X be a geodesic metric space. Then

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

Proof. (i) is left as an exercise.

Hint: Suppose that $p \in [x,y]$ and $q \in [x,z]$ with $d(x,p) = d(x,q) \leq (y \cdot z)_x$. Prove the required inequality $d(p,q) \leq 4\delta$ by bounding $(p \cdot q)_x$ from below by first proving the general fact that, for all $a, b, c, d, w \in X$, we have

$$(a \cdot d)_w \geq \min\{(a \cdot b)_w, (b \cdot c)_w, (c \cdot d)_w\} - 2\delta.$$

(ii) Pick x' on a geodesic $[w,x]$, y' on $[w,y]$ and z' on $[w,z]$ such that

$$d(w,x') = d(w,y') = d(w,z') = \min\{(x \cdot z)_w, (y \cdot z)_w\}.$$

By δ-thinness of $\Delta(w,x,z)$ we have $d(x',z') \leq \delta$ and similarly $d(z',y') \leq \delta$ so that $d(x',y') \leq 2\delta$. Thus

$$d(x,y) \leq d(x,x') + 2\delta + d(y,y')$$

but by construction

$$\begin{aligned} d(x,x') &= d(w,x) - \min\{(x \cdot z)_w, (y \cdot z)_w\} \\ d(y,y') &= d(w,y) - \min\{(x \cdot z)_w, (y \cdot z)_w\} \end{aligned}$$

so that

$$d(x,y) \leq d(w,x) + d(w,y) - 2\min\{(x \cdot z)_w, (y \cdot z)_w\} + 2\delta$$

which says precisely that

$$(x \cdot y)_w \geq \min\{(x \cdot z)_w, (y \cdot z)_w\} - \delta.$$

□

Let's repackage the 4-point condition to be symmetric: we have that

$$(x \cdot y)_w \geq (x \cdot z)_w - \delta \tag{1.1}$$

$$\text{or} \qquad (x \cdot y)_w \geq (y \cdot z)_w - \delta \tag{1.2}$$

(or both). Inequality (1.1) says

$$\begin{aligned} & d(w,x) + d(w,y) - d(x,y) \geq d(w,x) + d(w,z) - d(x,z) - 2\delta \\ \Leftrightarrow \qquad & d(w,z) + d(x,y) \leq d(w,y) + d(x,z) + 2\delta. \end{aligned}$$

So similarly rewriting (1.2) and combining the two possibilities, we see that the 4-point condition $(*)$ is equivalent to

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

There are 3 ways to partition $\{w,x,y,z\}$ into 2 pairs, all of which occur in the previous equation. Suppose $S \leq M \leq L$ are the corresponding sums of opposite edge lengths. Then $(*)$ is equivalent (considering permutations of the 4 points) to the assertion $L \leq M + 2\delta$.

Theorem 1.53 (Delzant). *Let X be a δ-hyperbolic geodesic metric space (in the sense of thin triangles) and suppose that $G \curvearrowright X$ by isometries such that for all $1 \neq g \in G$ and for all $x \in X$, we have*

$$d(x, g \cdot x) > 3\delta.$$

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

$$\begin{aligned} & d(gh \cdot p, p) > d(g \cdot p, p) \\ \text{or} \qquad & d(gh^{-1} \cdot p, p) > d(g \cdot p, p). \end{aligned}$$

Then we are done because for finite $A \subseteq G$ and any $p \in X$, an element $a \in A$ achieving $\max_{a \in A} d(a \cdot p, p)$ will be extremal.

Suppose for the sake of contradiction that

$$d(g \cdot p, p) \geq d(gh \cdot p, p), d(gh^{-1} \cdot p, p). \tag{1.3}$$

Consider the symmetric 4-point condition ($\diamond$) on $p, g \cdot p, gh \cdot p, gh^{-1} \cdot p$. (Note that X is assumed δ-hyperbolic and is thus (δ)-hyperbolic by Proposition 1.52.) The three possible sums are (since $G \curvearrowright X$ by isometries):

$$\begin{aligned} d(g \cdot p, p) + d(gh^{-1} \cdot p, gh \cdot p) &= d(g \cdot p, p) + d(h^2 \cdot p, p) \\ d(gh \cdot p, p) + d(g \cdot p, gh^{-1} \cdot p) &= d(gh \cdot p, p) + d(h \cdot p, p) \\ d(gh^{-1} \cdot p, p) + d(g \cdot p, gh \cdot p) &= d(gh^{-1} \cdot p, p) + d(h \cdot p, p). \end{aligned}$$

If we assume $d(h^2 \cdot p, p) \geq d(h \cdot p, p)$, then together with (1.3) this implies that the first term is the largest and thus the 4-point condition says

$$\begin{aligned} d(g \cdot p, p) + d(h^2 \cdot p, p) &\leq d(gh^{\pm 1} \cdot p, p) + d(h \cdot p, p) + 2\delta \\ &\leq d(g \cdot p, p) + d(h \cdot p, p) + 2\delta. \end{aligned}$$

So in either case, we have $d(h^2 \cdot p, p) \leq d(h \cdot p, p) + 2\delta$. Thus

$$(h \cdot p, h^{-1} \cdot p)_p \geq \frac{1}{2} d(h \cdot p, p) - \delta.$$

Take any geodesic $[p, h^{-1} \cdot p]$ and translate it by h to get a preferred geodesic $[h \cdot p, p]$. If we let q be the midpoint of $[p, h^{-1} \cdot p]$ and then let q', q'' lie on $[q, p]$ respectively $[h \cdot q, p] \subset [h \cdot p, p]$ at distance δ from q respectively $h \cdot q$, we have $d(q', q'') \leq \delta$ by δ-thinness of $\Delta(h^{-1} \cdot p, p, h \cdot p)$. But now

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

a contradiction.

□

Corollary 1.54. *Let G be a residually finite hyperbolic group. Then G is virtually diffuse.*

Remark 1.55. It is a famous open problem whether all hyperbolic groups are residually finite.

Proof. Let $G \curvearrowright X$ properly cocompactly by isometries, where X is a proper geodesic δ-hyperbolic metric space. By Lemma 1.49 there exist $1 = g_0, g_1, \ldots, g_n \in G$ such that for all $g \in G$, if there exists $x \in X$ with $d(g \cdot x, x) \leq 3\delta$ then $g \sim g_i$ for some i. By residual finiteness we can find $\phi\colon G \twoheadrightarrow Q$, Q finite, such that $\phi(g_1), \ldots, \phi(g_n) \neq 1$. Then $G_0 = \ker(\phi)$ satisfies the assumptions of Delzant's theorem 1.53. □

We note one consequence of this corollary of general interest (i.e. beyond studying group rings).

Corollary 1.56. *A residually finite hyperbolic group is virtually torsion-free.*

EXERCISE 1.3.1. Verify Remark 1.48 (translating between topological and metric conditions).

1.4. 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 for $K[G]$.

THEOREM 1.57 (Connell). *$K[G]$ is prime if and only if G has no non-trivial finite normal subgroup.*

Recall that a ring R is *prime* if for all $\alpha, \beta \in R \setminus \{0\}$ there exists $\gamma \in R$ such that $\alpha\gamma\beta \neq 0$ (that is, the zero ideal is a prime ideal in the sense of non-commutative ring theory).

To get there we need some group ring basics, a fair bit of group theory and an ingenious trick of Passman.

Definition 1.58. Let $H \leq G$. Then the projection $\pi_H \colon K[G] \to K[H]$ is defined by

$$\pi_H(\sum_{g\in G} a_g g) = \sum_{g\in H} a_g g.$$

Warning: this is never a ring homomorphism for $H \lneq G$! But we do have:

Lemma 1.59. *π_H is a homomorphism of $(K[H], K[H])$-bimodules.*

PROOF. Exercise. □

Corollary 1.60. *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

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

so in fact $\alpha^{-1} = \beta = \pi_H(\beta) \in K[H]$. □

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

Lemma 1.61. *Let X be a left transversal for H in 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 $\alpha_x \in K[H]$. In fact, $\alpha_x = \pi_H(x^{-1}\alpha)$. Thus $K[G]$ is a free right $K[H]$-module with X as a basis.

PROOF. Exercise. □

Recall that $M_n(R)$ denotes the ring of $n \times n$ matrices over a ring R.

Lemma 1.62. *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 in 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 j we have

$$\alpha x_j = \sum_{i=1}^{n} x_i \pi_H(x_i^{-1} \alpha x_j),$$

sending the element α to the matrix

$$\eta_X(\alpha) := \left(\pi_H(x_i^{-1} \alpha x_j)\right)_{ij}$$

defines the embedding (for choice of basis X).

□

Remark 1.63. If G is finite and $H = 1$ then this is just the regular representation.

Example 1.64. Let $D_\infty = \langle\, r, t \,|\, r^2 = 1, t^r = t^{-1} \,\rangle = \mathbb{Z} \rtimes \mathbb{Z}/2$ and take $X = \{1, r\}$ as the obvious left transversal for $\langle t \rangle = \mathbb{Z}$. Then since $r \cdot 1 = r, r \cdot r = 1 \cdot 1, t \cdot 1 = 1 \cdot t, t \cdot r = r \cdot t^{-1}$, we have $K[D_\infty] \to M_2(K[t, t^{-1}])$ given by extending

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

The first bit of group theory is:

Lemma 1.65 (Schur)**.** *If $[G : Z(G)] < \infty$ then $|G'|$ is finite.*

Definition 1.66. Let $H \leq G$ with $[G : H] = n < \infty$. Pick a left transversal $\{x_1, \dots, x_n\}$ for H. For each $g \in G$ and $1 \leq j \leq n$, we have $g x_j = x_i h_j$ for some unique $h_j \in H$. The *transfer* is defined as the map $G/G' \to H/H'$ given by

$$g \mapsto h_1 \dots h_n H'.$$

Lemma 1.67. *The transfer is a group homomorphism and does not depend on the choice of transversal.*

Proof. Map $K[G] \to M_n(K[H])$ via lemma 1.62, $M_n(K[H]) \to M_n(K[H/H'])$ by extending $K[H] \to K[H/H']$, and $M_n(K[H/H']) \to K[H/H']$ via the determinant. For given $g \in G$ and $1 \leq j \leq n$, with $g x_j = x_i h_j \Leftrightarrow h_j = x_i^{-1} g x_j$, the j-th column of $\eta_X(g)$ contains h_j in row i, otherwise zeroes. Letting $\operatorname{sgn}(g)$ denote the sign of the permutation g induces on the set G/H, we have that the composition $G \to K[H/H']$ so defined maps

$$g \mapsto \operatorname{sgn}(g) h_1 \dots h_n \in K[H/H']$$

where the image is moreover a trivial unit. The group of trivial units is $K^\times \times H/H'$ so we can project onto the second factor to obtain our map

$$G \to H/H' \colon g \mapsto h_1 \dots h_n.$$

As the image is abelian, it factors through G/G' to define the transfer. It is independent of the choice of transversal since change of basis of $K[G]$ produces similar matrices in $M_n(K[H])$, whose images in $M_n(K[H/H'])$ will have the same determinant.

□

Proof of Schur's lemma. Let $Z = Z(G)$. Consider the transfer map $G/G' \to Z/Z' = Z$. By centrality of Z, for $g \in Z$ this is simply $g \mapsto g^n$ (in fact, one can show this for all $g \in G$). Thus $g \in G' \cap Z$ implies $g^n = 1$. If $x_1, \dots, x_n$ is a transversal, then every commutator is of the form $[x_i z_1, x_j z_2] = [x_i, x_j]$ (for some $z_1, z_2 \in Z$) and thus G' is finitely generated. Now $[G' : G' \cap Z] \leq n$ so $G' \cap Z$ is finitely generated, finite exponent and abelian, thus finite. Thus G' is finite. □

Definition 1.68. The *FC-centre* of a group G is

$$\Delta(G) = \{g \in G : |g^G| < \infty\},$$

the set of elements whose conjugacy class is finite.

This is alternatively the set of elements g whose centralizer $C_G(g)$ is finite index (by orbit-stabilizer theorem for $G \curvearrowright G$). As $C_G(gh) \geq C_G(g) \cap C_G(h)$ and $[G : C_G(g) \cap C_G(h)] \leq [G : C_G(g)][G : C_G(h)]$ for all $g, h \in G$, we see that $\Delta(G)$ is a (characteristic) subgroup of G.

We call G an *FC-group* if $G = \Delta(G)$. Note that $\Delta(\Delta(G)) = \Delta(G)$, i.e. the FC-centre is an FC-group.

Lemma 1.69. *An FC-group is locally finite-by-(free abelian).*

Proof. Let $H = \langle h_1, \dots, h_n \rangle \leq G$. Then $C_G(H) = \cap_{i=1}^n C_G(h_i)$ is finite index in G and thus $Z(H) = C_G(H) \cap H$ is finite index in H. Thus Schur's lemma implies that H' is finite. Now H/H' is a finitely generated abelian group so it has the form $T \oplus \mathbb{Z}^d$ where T is finite. Thus the kernel of the composition $H \to \mathbb{Z}^d$ is finite. □

Remark 1.70. The torsion elements of an abelian group form a characteristic subgroup, so any group (finitely generated or not) has a well-defined torsion-free abelianization.

Corollary 1.71. *A torsion-free virtually cyclic is cyclic.*

Proof. Let G be torsion-free and virtually cyclic with $G_0 = \langle t \rangle$ a finite index subgroup. (If G_0 is finite, then G is finite and thus trivial.) We claim that G is an FC-group. For any $1 \neq g \in G$ there exists $n \geq 1$ such that $g^n \in G_0$, i.e. $g^n = t^m$ for some $m \in \mathbb{Z}$. By torsion-freeness $m \neq 0$ and thus $C_G(g)$ contains $\langle t^m \rangle$ which is finite index in G_0 and thus in G.

A virtually finitely generated group is finitely generated so lemma 1.69 applies. Now we are done by the classification of finitely generated abelian groups. □

Remark 1.72. A torsion-free virtually abelian group need not be abelian, e.g. the fundamental group $\mathbb{Z} \rtimes \mathbb{Z}$ of the Klein bottle.

We now have the tools to prove the following result on the torsion of $\Delta(G)$,

$$\Delta^+(G) := \{g \in \Delta(G) : \operatorname{ord}(g) < \infty\}.$$

Lemma 1.73 (B.H. Neumann)**.** *$\Delta^+(G)$ is a characteristic subgroup of G and $\Delta(G)/\Delta^+(G)$ is torsion-free abelian.*

Proof. If $g, h \in \Delta^+(G)$ then the generators of $H = \langle g, h \rangle$ are both in the kernel of its torsion-free abelianization, so H is finite. Thus $\Delta^+(G)$ is a subgroup, which is clearly characteristic.

Since $\Delta^+(G)$ contains *precisely* the torsion elements of $\Delta(G)$, the quotient $\Delta(G)/\Delta^+(G)$ is torsion-free. For any $H = \langle g, h \rangle \leq \Delta(G)$, we have that H' is finite by lemma 1.69 and thus $H' \leq \Delta^+(G)$, so $\Delta(G)/\Delta^+(G)$ is abelian. □

Lemma 1.74. *If $x_1, \ldots, x_n \in \Delta^+(G)$ then the normal closure $N = \langle\langle x_1, \ldots, x_n \rangle\rangle_G$ is finite.*

Proof. N is generated by the finitely many conjugates in G of the x_i, which are all in the kernel of the torsion-free abelianization of N, so we are done by lemma 1.69. □

Lemma 1.75 (B.H. Neumann)**.** *Let G be a group and $H_1, \ldots, H_n \leq G$. Suppose there exist finitely many (left) cosets $g_{ij}H_i$ such that*

$$G = \bigcup_{i,j} g_{ij}H_i.$$

Then some $[G : H_i] < \infty$.

Proof. We proceed by induction on n. The base case $n = 1$ is clear. Suppose $n \geq 2$. If all (left) cosets of H_n occur, then $[G : H_n] < \infty$. If not, then let gH_n be such that $gH_n \neq g_{nj}H_n$ for all j, which gives $gH_n \cap g_{nj}H_n = \emptyset$ for all j. Thus

$$gH_n \subseteq \bigcup_{i \leq n-1, k} g_{ik}H_i.$$

Now replace each $g_{nj}H_n$ with $\left\{g_{nj}g^{-1}g_{ik}H_i \,\middle|\, i \leq n-1\right\}$ to write G as a finite union of cosets of $H_1, \ldots, H_{n-1}$. □

This result is similarly true for right cosets.

The final ingredient is:

Theorem 1.76 (Passman). *Suppose that $\alpha, \beta \in K[G]$ such that $\alpha\gamma\beta = 0$ for all $\gamma \in K[G]$. Then $\pi_{\Delta(G)}(\alpha)\pi_{\Delta(G)}(\beta) = 0$.*

Proof of Connell's Theorem. If $H \lhd G$ is finite then let $\alpha = \sum_{h \in H} h \in K[G]$. Note that $\alpha \in Z(K[G])$ and $\alpha^2 = |H|\alpha$. Thus $\alpha\gamma(\alpha - |H|) = 0$ for all $\gamma \in K[G]$, so $K[G]$ is not prime.

If G has no non-trivial finite normal subgroup, then by lemma 1.74 we have $\Delta^+(G) = 1$ and thus by Neumann's lemma 1.73 $\Delta(G)$ is torsion-free abelian. Suppose that $0 \neq \alpha, \beta \in K[G]$ with $\alpha\gamma\beta = 0$ for all $\gamma \in K[G]$. By choosing some $g \in \operatorname{supp}(\alpha), h \in \operatorname{supp}(\beta)$ and replacing α with $g^{-1}\alpha$ and β with βh^{-1}, we can assume without loss of generality that $1 \in \operatorname{supp}(\alpha)$ and $1 \in \operatorname{supp}(\beta)$. Thus $\pi_{\Delta(G)}(\alpha), \pi_{\Delta(G)}(\beta) \neq 0$ but by Passman's theorem their product is zero. This is impossible as $\Delta(G)$ is torsion-free abelian so $K[\Delta(G)]$ satisfies the zero divisor conjecture. □

Proof of Passman's Theorem. Let $\Delta = \Delta(G)$. It suffices to prove that $\pi_\Delta(\alpha)\beta = 0$ since then

$$0 = \pi_\Delta\left(\pi_\Delta(\alpha)\beta\right) = \pi_\Delta(\alpha)\pi_\Delta(\beta)$$

(as π_Δ is a homomorphism of $K[\Delta]$-bimodules, lemma 1.59).

Write $\alpha = \alpha_0 + \alpha_1$ where $\alpha_0 = \pi_\Delta(\alpha)$. Suppose for the sake of contradiction that $\alpha_0\beta \neq 0$ and fix some $g_0 \in \operatorname{supp}(\alpha_0\beta)$. The assumption on α and β is equivalent to saying

$$x^{-1}(\alpha_0 + \alpha_1)x\beta = 0$$

for all $x \in G$. If $x \in C_G(\operatorname{supp}(\alpha_0))$ then this simplifies to

$$x^{-1}\alpha_1 x\beta = -\alpha_0\beta$$

so that $g_0 \in \operatorname{supp}(x^{-1}\alpha_1 x\beta)$. Let

$$\operatorname{supp}(\alpha_1) = \{v_1, \dots, v_m\}$$
$$\operatorname{supp}(\beta) = \{w_1, \dots, w_n\}$$

So if $x \in C_G(\operatorname{supp}(\alpha_0))$ there exist $1 \le i \le m, 1 \le j \le n$ such that

$$x^{-1}v_i x w_j = g_0.$$

If g_{ij} is some solution in x to $v_i^x = g_0 w_j^{-1}$, then the set of solutions is precisely the coset $C_G(v_i)g_{ij}$.

Now the definition of Δ guarantees that

$$C := C_G(\operatorname{supp}(\alpha_0)) = \bigcap_{g \in \operatorname{supp}(\alpha_0)} C_G(g)$$

is finite index in G whereas for $v_i \in \operatorname{supp}(\alpha_1)$ we have $[G : C_G(v_i)] = \infty$ which implies $[C : C \cap C_G(v_i)] = \infty$ too. If every $x \in C$ lies in some $C_G(v_i)g_{ij}$, then C can be written as a finite union of cosets of infinite index subgroups, contradicting Neumann's lemma 1.75.

□

Exercise 1.4.1. Let

$$T(G) = \{g \in G \mid \operatorname{ord}(g) < \infty\}$$

denote the set of torsion of the group G.

(1) Show that if G/N is torsion-free then $T(G) \subseteq N$.
(2) Show that if $T(G)$ is a subgroup of G, then $G/T(G)$ is torsion-free.
(3) Show that if $T(G)$ is finite, then it is indeed a subgroup. (Hint: consider the FC-centre $\Delta(G)$.)

Exercise 1.4.2. Suppose that $g, h, x_0 \in G$ satisfy $g^{x_0} = h$. Show that

$$\{x \in G \mid g^x = h\} = C_G(g)x_0.$$

Exercise 1.4.3. Let $[G : G_0] < \infty$. Prove or disprove: If G_0 is an FC-group, then G is an FC-group.

Exercise 1.4.4. Consider the group ring $\mathbb{F}_2[\mathbb{Z}/3]$.

(1) Does is contain zero-divisors?
(2) Does is contain non-trivial units?
(3) Does this contradict anything we proved?

1.5. Traces

(This section of the lectures follows [**Pas85**, Chapter 2] very closely.)

Suppose $|G| = n < \infty$. Then $V = K[G]$ gives a finite dimensional representation of G, namely the regular representation. Fix as a basis G which gives $\rho \colon K[G] \to M_n(K)$. As $G \curvearrowright G$ freely, we know that each $\rho(g)$ for $g \ne 1$ is a permutation matrix with zeroes on the diagonal, and of course $\rho(1) = I_n$. Thus

$$\operatorname{tr}(\rho(\sum_{g \in G} a_g \cdot g)) = \sum_{g \in G} a_g \cdot \operatorname{tr}(\rho(g)) = |G| \cdot a_1$$

i.e. the trace of $\rho(\alpha)$, $\alpha \in K[G]$, is just a fixed multiple of the coefficient $a_1 = (\alpha)_1$ of the identity. This motivates defining

Definition 1.77. The *trace* on $K[G]$ is

$$\begin{aligned}\operatorname{tr}\colon K[G] &\to K\\ \alpha &\mapsto (\alpha)_1.\end{aligned}$$

Lemma 1.78. $\operatorname{tr}\colon K[G]\to K$ *is K-linear and* $\operatorname{tr}(\alpha\beta)=\operatorname{tr}(\beta\alpha)$ *for all* $\alpha,\beta\in K[G]$.

Note that $\operatorname{tr}(\alpha\beta)=\operatorname{tr}(\beta\alpha)$ is called the *trace identity.*

Proof. Linearity is clear. If

$$\begin{aligned}\alpha &= \sum_g a_g\cdot g\\ \beta &= \sum_g b_g\cdot g\end{aligned}$$

then

$$\operatorname{tr}(\alpha\beta)=\sum_{gh=1} a_g\cdot b_h=\sum_{hg=1} b_h\cdot a_g=\operatorname{tr}(\beta\alpha).$$

□

Definition 1.79. An element $\alpha\in K[G]$ is called *algebraic* if there is some non-zero polynomial $p(x)\in K[x]$ such that $p(\alpha)=0$.

Example 1.80.
- α is called *nilpotent* if $\alpha^m=0$ for some $m\in\mathbb{Z}^+$
- idempotent elements are algebraic (with $p(x)=x^2-x$)

For these algebraic elements, trace is worth studying.

Lemma 1.81. *Let* $|G|=n<\infty$ *and suppose that* $\operatorname{char}(K)\nmid n$.

(i) *If α is nilpotent, then* $\operatorname{tr}(\alpha)=0$.
(ii) *If e is an idempotent, then* $\operatorname{tr}(e)=\dim(e\cdot K[G])/n\in\{0,\frac{1}{n},\frac{2}{n},\dots,1\}$.

Proof. Consider $V=K[G]$. We will use $\operatorname{tr}(\alpha)=\frac{1}{|G|}\operatorname{tr}(\rho(\alpha))$.

(i) Pick a basis of V that is compatible with the chain of subspaces $V\supseteq\alpha V\supseteq\alpha^2V\cdots\supseteq\alpha^mV=\{0\}$. (We want $v_1,\dots,v_k$ to be a basis of α^iV for all i, where $k=k(i)=\dim(\alpha^iV)$.) Then the matrix for α with respect to this basis is strict upper triangular. Thus $\operatorname{tr}(\rho(\alpha))=0$ and hence $\operatorname{tr}(\alpha)=0$.

(ii) Suppose $e^2=e$. Then $V=eV\oplus(1-e)V$ (for $v\in V$, we have $v=ev+(1-e)v$ so that eV and $(1-e)V$ together span, whereas if $ev=(1-e)v'$ then $ev=e^2v=e(1-e)v'=(e-e^2)v'=0$.) Then e acts as the identity on eV and is zero on $(1-e)V$ and hence $\operatorname{tr}(\rho(e))=\dim(eV)$. □

Remark 1.82. If e is an idempotent, then so is $1-e$. If $|G|=n<\infty$ then $\frac{1}{n}\sum_g g$ is an idempotent.

We will work towards proving the following general result on traces:

Theorem 1.83 (Kaplansky). *If $e\in\mathbb{C}[G]$ is a non-trivial idempotent, then* $\operatorname{tr}(e)\in(0,1)$.

Corollary 1.84. $\mathbb{C}[G]$ *is directly finite.*

Proof. If $\alpha\beta=1$ then $(\beta\alpha)^2=\beta(\alpha\beta)\alpha=\beta\alpha$ is an idempotent, but $\operatorname{tr}(\beta\alpha)=\operatorname{tr}(\alpha\beta)=1$ so $\beta\alpha$ must be the trivial idempotent 1. □

Definition 1.85. The *prime subfield* of a field K is the smallest subfield of K.

If $\operatorname{char}(K) = p > 0$, the prime subfield is $\mathbb{F}_p$. If $\operatorname{char}(K) = 0$, it is $\mathbb{Q}$.

In particular, Lemma 1.81 (ii) shows that if e is an idempotent then $\operatorname{tr}(e)$ is in the prime subfield. This algebraic property is also true for infinite G, as we'll see later in Theorem 1.120. Also if $\operatorname{char}(K) = 0$ then $0 \leq \operatorname{tr}(e) \leq 1$ and this analytic property is true in general by Theorem 1.83.

For infinite G we no longer have a finite dimensional representation at hand, so we need to be able to get at $\operatorname{tr}(e)$ internally to $\mathbb{C}[G]$.

Definition 1.86. For $\alpha = \sum_g a_g \cdot g, \beta = \sum_g b_g \cdot g \in \mathbb{C}[G]$, we define the inner product

$$\langle \alpha,\, \beta \rangle = \sum_g a_g \overline{b_g}$$

which induces the norm

$$\|\alpha\| = \sqrt{\langle \alpha,\, \alpha \rangle}.$$

We also define an absolute value

$$|\alpha| = \sum_g |a_g|.$$

Finally, we define conjugation via

$$\overline{\alpha} = \sum_g \overline{a_g} g^{-1}.$$

Lemma 1.87. *$(\mathbb{C}[G], \langle \cdot,\, \cdot \rangle)$ is an inner product space and $\langle \alpha,\, \beta \rangle = \operatorname{tr}(\alpha\overline{\beta})$. Furthermore $\alpha \mapsto \overline{\alpha}$ is a ring anti-automorphism of $\mathbb{C}[G]$ and for all $\alpha, \beta, \gamma \in \mathbb{C}[G]$ we have*

$$\langle \alpha,\, \beta\gamma \rangle = \langle \alpha\overline{\gamma},\, \beta \rangle = \langle \overline{\beta}\alpha,\, \gamma \rangle.$$

Thus conjugation is the adjoint with respect to left and right multiplication.

Proof. This is the standard inner product on $V = \mathbb{C}[G]$ with respect to the basis G. Note that

$$\operatorname{tr}(\alpha\overline{\beta}) = (\alpha\overline{\beta})_1 = \sum_{gh=1} (\alpha)_g (\overline{\beta})_h = \sum_g a_g \overline{b_g} = \langle \alpha,\, \beta \rangle.$$

Since $(g \cdot h)^{-1} = h^{-1} \cdot g^{-1}$, it is clear that $\overline{\alpha\beta} = \overline{\beta}\,\overline{\alpha}$. Likewise it is clear that $\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}$ and $\overline{\overline{\alpha}} = \alpha$. For all $\alpha, \beta, \gamma \in \mathbb{C}[G]$ we have

$$\langle \alpha,\, \beta\gamma \rangle = \operatorname{tr}(\alpha \cdot \overline{\beta\gamma}) = \operatorname{tr}(\alpha\overline{\gamma}\overline{\beta}) = \langle \alpha\overline{\gamma},\, \beta \rangle$$

and

$$\langle \alpha,\, \beta\gamma \rangle = \operatorname{tr}(\alpha\overline{\gamma}\overline{\beta}) = \operatorname{tr}(\overline{\beta}\alpha\overline{\gamma}) = \langle \overline{\beta}\alpha,\, \gamma \rangle.$$

□

Now, as a warm up to the general result, we can give a different proof of:

Lemma 1.88. *Let G be finite. If $e \in \mathbb{C}[G]$ is an idempotent, then* $\operatorname{tr}(e) \geq 0$.

Proof. Let $I = e\mathbb{C}[G] = \{e\alpha \mid \alpha \in \mathbb{C}[G]\}$ be the right ideal of $\mathbb{C}[G]$ generated by e. Let $I^\perp$ be its orthogonal complement. Since $\mathbb{C}[G]$ is finite dimensional, $\mathbb{C}[G] = I \oplus I^\perp$ is a direct sum decomposition. We note that $I^\perp$ is also a right ideal: if $\alpha \in I$, $\beta \in I^\perp$ and $\gamma \in \mathbb{C}[G]$, then

$$\langle \alpha,\, \beta\gamma \rangle = \langle \alpha\overline{\gamma},\, \beta \rangle = 0$$

as $\alpha\overline{\gamma} \in I$.

Now let $1 = f + f^\perp$ with $f \in I, f^\perp \in I^\perp$. As $f^\perp = 1 - f$ we see that $f^\perp f = ff^\perp$, but $f^\perp f \in I^\perp$ and $ff^\perp \in I$, so in fact $ff^\perp = 0$, so that $f^2 = f(1 - f^\perp) = f$ and similarly $(f^\perp)^2 = f^\perp$.

For any $\alpha \in \mathbb{C}[G]$ we have $\alpha = f\alpha + f^\perp\alpha$ with $f\alpha \in I$ and $f^\perp\alpha \in I^\perp$. Thus if $\alpha \in I$, then $f\alpha = \alpha$, so we have $f\mathbb{C}[G] \supseteq I$. But $f\mathbb{C}[G] \subseteq I$ since $f \in I$ and I is a right ideal, thus $f\mathbb{C}[G] = I$ and similarly $f^\perp\mathbb{C}[G] = I^\perp$.

As f is orthogonal to $f^\perp\mathbb{C}[G] = I^\perp$, for all $\alpha \in \mathbb{C}[G]$ we have

$$0 = \langle f,\, f^\perp\alpha \rangle = \langle f,\, (1-f)\alpha \rangle = \langle \overline{(1-f)}f,\, \alpha \rangle.$$

Letting $\alpha = \overline{(1-f)}f$ we see that $(1 - \overline{f})f = 0$, that is $\overline{f}f = f$. Hence $\overline{f} = \overline{\overline{f}f} = \overline{f}f = f$ so f is a self-adjoint idempotent, i.e. what we call a *projection.* Since $e, f \in I$ and both act as the identity on I, we have $e = fe$ and $f = ef$. Thus

$$\operatorname{tr}(e) = \operatorname{tr}(fe) = \operatorname{tr}(ef) = \operatorname{tr}(f).$$

But

$$\operatorname{tr}(f) = \operatorname{tr}(f\overline{f}) = \langle f,\, f \rangle = \|f\|^2 \geq 0.$$

□

For infinite G, $\mathbb{C}[G]$ will not have such direct sum decompositions, or in other words, such an f need not exist. One approach is to embed $\mathbb{C}[G]$ in either the reduced group C^*-algebra of G or the von Neumann algebra of G. An alternative approach introduced by Passman, which we follow, is to take better and better approximations f_n of such an element f without ever leaving $\mathbb{C}[G]$.

We can characterize f as follows. For $\alpha \in I$ we consider the distance from α to 1. By definition

$$d(\alpha, 1)^2 = \|\alpha - 1\|^2 = \langle \alpha - 1,\, \alpha - 1 \rangle = \langle \alpha - f - f^\perp,\, \alpha - f - f^\perp \rangle = \|\alpha - f\|^2 + \left\|f^\perp\right\|^2$$

as $\alpha - f \in I$ implies that $\langle \alpha - f,\, f^\perp \rangle = 0$. Thus $d(\alpha, 1) \geq \left\|f^\perp\right\|$ with equality if and only if $\alpha = f$, so f is the unique element of I that is closest to 1.

Let G be arbitrary. If L is a $\mathbb{C}$-subspace of $\mathbb{C}[G]$, we define

$$d(L, \gamma) = \inf_{\alpha \in L} \|\alpha - \gamma\|.$$

For $I = e\mathbb{C}[G]$, since $\mathbb{C}[G]$ is not complete we cannot expect that this infimum is achieved. But we can approach it. Recall that $\langle \beta,\, f - 1 \rangle = 0$ for all $\beta \in I$. We will take f_n such that $\|f_n - 1\| \to d(I, 1)$ as $n \to \infty$. The following generalization of the Cauchy–Schwarz inequality lets us see that then also $\langle \beta,\, f_n - 1 \rangle \to 0$ as $n \to \infty$.

Lemma 1.89. *Let $(V, \langle\cdot,\, \cdot\rangle)$ be an inner product space, $L \subseteq V$ a subspace and $\alpha, \beta \in L$. Then*

$$|\langle \beta,\, \alpha - \gamma \rangle|^2 \leq \|\beta\|^2 \left(\|\alpha - \gamma\|^2 - d(L, \gamma)^2\right).$$

So if $\alpha \in L$ is close to realizing $d(L, \gamma)$, then $\alpha - \gamma$ is almost orthogonal to L.

Proof. The lemma is trivial for $\beta = 0$ so suppose $\beta \neq 0$ and set $k = \langle \alpha - \gamma,\, \beta\rangle / \|\beta\|^2$. Then $\alpha - k\beta \in L$ so that

$$\|\alpha - k\beta - \gamma\|^2 \geq d(L,\gamma)^2.$$

Then

$$\begin{aligned}\|\alpha - \gamma\|^2 - d(L,\gamma)^2 &\geq \|\alpha-\gamma\|^2 - \|\alpha - k\beta - \gamma\|^2\\ &= \langle \alpha-\gamma,\, \alpha-\gamma\rangle - \langle \alpha - k\beta - \gamma,\, \alpha - k\beta-\gamma\rangle\\ &= k\langle\beta,\, \alpha-\gamma\rangle + \overline{k}\langle \alpha-\gamma,\, \beta\rangle - k\overline{k}\langle\beta,\,\beta\rangle\\ &= \langle\beta,\,\alpha-\gamma\rangle\overline{\langle\beta,\,\alpha-\gamma\rangle}/\|\beta\|^2\\ &= |\langle\beta,\,\alpha-\gamma\rangle|^2/\|\beta\|^2.\end{aligned}$$

□

Exercise 1.5.1. Let $G = S_3 = D_6$ generated by $r = (123)$ and $s = (12)$. We can present G as $\langle\, r, s \,|\, r^3, s^2, r^s = r^{-1}\,\rangle$. Let $\omega \in \mathbb{C}$ be a primitive cube root of 1. Consider the elements

$$\begin{aligned}f_1 &= 1 + r + r^{-1}\\ f_\omega &= 1 + \omega r + \omega^{-1} r^{-1}\\ f_{\omega^{-1}} &= 1 + \omega^{-1} r + \omega r^{-1}\end{aligned}$$

of $\mathbb{C}[G]$ and let

$$e = \frac{1}{6} f_\omega (1+s).$$

(1) Verify that $\frac{1}{3}f_1, \frac{1}{3}f_\omega, \frac{1}{3}f_{\omega^{-1}}$ are all self-adjoint idempotents.
(2) Show that $f_1 + f_\omega + f_\omega^{-1} = 3$.
(3) Show that $f_\omega f_1 = 0$.
(4) Show that $(1+s)f_\omega = f_\omega + f_{\omega^{-1}} s$.
(5) Show that e is an idempotent. (Hint: apply the previous three calculations!)
(6) Check that e is not self-adjoint and verify moreover that $\langle e, 1-e\rangle \neq 0$.

We will use a few basic identities.

Lemma 1.90. (i) $\|\alpha+\beta\| \leq \|\alpha\| + \|\beta\|$, $|\alpha+\beta| \leq |\alpha| + |\beta|$.
(ii) $|\operatorname{tr}\alpha| \leq \|\alpha\|$, $\langle\alpha,\, 1\rangle = \operatorname{tr}\alpha$.
(iii) $\|\alpha\beta\| \leq \|\alpha\|\cdot|\beta|$, $|\alpha\beta| \leq |\alpha|\cdot|\beta|$.

Proof. (i) is standard (or an exercise using Cauchy–Schwarz) and (ii) is immediate. For (iii), let $g \in G$. Then clearly $\|\alpha g\| = \|\alpha\|$ as both are $\sum_h |(\alpha)_h|^2$. Seen differently, g is an isometry since $\overline{g} = g^{-1}$:

$$\|\alpha g\|^2 = \langle \alpha g,\, \alpha g\rangle = \langle \alpha g\overline{g},\, \alpha\rangle = \|\alpha\|^2.$$

Thus

$$\|\alpha\beta\| = \left\|\sum_g \alpha\cdot(\beta)_g g\right\| \leq \sum_g \|\alpha\cdot(\beta)_g g\| = \sum_g \|\alpha\|\cdot|\beta_g| = \|\alpha\|\,|\beta|.$$

and similarly $|\alpha g| = |\alpha|$ so that $|\alpha\beta| \leq |\alpha||\beta|$. □

Proof of Theorem 1.83. Let $e \neq 0$ be an idempotent in $\mathbb{C}[G]$ and let $I = e\mathbb{C}[G]$. We will prove that $\operatorname{tr}(e) > 0$ and in fact $\operatorname{tr} e \geq \|e\|^2 / |e|^2$. Then we are done since if e is a non-trivial idempotent, then so is $1 - e$, and $\operatorname{tr}(1-e) = 1 - \operatorname{tr}(e) > 0$ so that $\operatorname{tr}(e) < 1$.

Let $d = d(I, 1)$ and choose $f_n \in I$ with

$$\|f_n - 1\|^2 < d^2 + \frac{1}{n^4}.$$

Then the lemma ensures

$$|\langle \beta,\, f_n - 1\rangle| < \|\beta\| \frac{1}{n^2}$$

for all $\beta \in I$. Since $f_n \in I$ we have $ef_n = f_n$ and thus

$$\operatorname{tr}(f_n e) = \operatorname{tr}(ef_n) = \operatorname{tr}(f_n).$$

Now

$$|\operatorname{tr} f_n e - \operatorname{tr} e| = |\operatorname{tr}(f_n e - e)| \leq \|f_n e - e\|$$

and

$$\begin{aligned} \|f_n e - e\|^2 &= \langle (f_n - 1)e,\, (f_n - 1)e\rangle \\ &= \langle (f_n - 1)e\bar{e},\, f_n - 1\rangle \\ &\leq \|(f_n - 1)e\bar{e}\| \frac{1}{n^2} \\ &\leq \|f_n - 1\|\, |e\bar{e}| \frac{1}{n^2} \\ &\leq \frac{(d+1)|e\bar{e}|}{n^2} \end{aligned}$$

(where we used that $(f_n - 1)e \in I$ as $f_n, e \in I$.) Thus $|\operatorname{tr} f_n - \operatorname{tr} e| \to 0$ as $n \to \infty$.

But

$$\|f_n\|^2 - \operatorname{tr} f_n = \langle f_n,\, f_n\rangle - \langle f_n,\, 1\rangle = \langle f_n,\, f_n - 1\rangle$$

so that

$$\left| \|f_n\|^2 - \operatorname{tr} f_n \right| \leq \|f_n\| \frac{1}{n^2} \leq \frac{d+2}{n^2} \to 0$$

as $n \to \infty$. Thus $\left| \|f_n\|^2 - \operatorname{tr} e \right| \to 0$ as $n \to \infty$ so

$$\operatorname{tr} e = \lim_{n \to \infty} \|f_n\|^2 \geq 0.$$

Finally, we have

$$\|e\| \leq \|e - f_n e\| + \|f_n e\| \leq \|e - f_n e\| + \|f_n\|\, |e|$$

where $\|e - f_n e\| = O(\frac{1}{n})$, so taking limits we have $\|e\| \leq \sqrt{\operatorname{tr} e}|e|$ and thus

$$\operatorname{tr} e \geq \|e\|^2 / |e|^2 > 0$$

□

We show later that in fact $\operatorname{tr} e \in \mathbb{Q} \cap [0,1]$ but we already have:

Corollary 1.91. *If $\operatorname{char}(K) = 0$ and $e \in K[G]$ is a non-trivial idempotent, then $\operatorname{tr}(e)$ is a totally real algebraic number all of whose algebraic conjugates lie in $(0,1)$.*

Proof. Let $F = \mathbb{Q}((e)_g : g \in \operatorname{supp}(e))$. Then $e \in F[G]$ and F is embeddable in $\mathbb{C}$, so viewing e as an element of $\mathbb{C}[G]$ we have $\operatorname{tr}(e) \in (0,1)$. Any field automorphism of $\mathbb{C}$ induces an automorphism of $\mathbb{C}[G]$ and thus $\sigma(\operatorname{tr}(e)) \in (0,1)$. If $\operatorname{tr}(e)$ transcendental, there would exist σ violating this. □

Places. We shifted from an arbitrary characteristic 0 field to $\mathbb{C}$ via a common subfield. Another way to shift fields is homomorphisms – of rings, not fields!

Recall: an ideal M of a (unital) commutative ring R is called maximal if and only if R/M is a field. We frequently use the homomorphism $R[G] \to (R/M)[G]$.

Definition 1.92. A subring R of a field is called a *valuation ring* if for all $x \in K$, either $x \in R$ or $x^{-1} \in R$ (or both).

Example 1.93.
- $R = K$
- $\mathbb{Z}_p \subset \mathbb{Q}_p$
- $K[[X]] \subset K((X))$

Lemma 1.94. *Let $R \subset K$ be a valuation ring. If M denotes the set of non-units of R, then M is the unique maximal ideal of R.*

Proof. Let $x, y \in R$. If xy is a unit, so are x and y (as R is commutative!). Thus M is closed under multiplication by R. Let $x, y \in M$ and consider $x - y \in R$. Then since R is a valuation ring, either $x^{-1}y \in R$ or $y^{-1}x \in R$. Since $x - y = x(1 - x^{-1}y) = y(y^{-1}x - 1)$, we see in either case that $x - y \in M$. Thus M is an ideal. Any proper ideal of R consists of non-units, so M is indeed maximal. □

A valuation ring R has a homomorphism onto the field $F = R/M$. We extend this to K by defining

$$\phi_R \colon K \to F \cup \{\infty\}$$
$$x \mapsto \begin{cases} x + M & \text{if } x \in R \\ \infty & \text{if } x \notin R \end{cases}$$

Definition 1.95. Let K and F be fields. A map $\phi \colon K \to F \cup \{\infty\}$ is called a *place* if $R := \phi^{-1}(F)$ is a subring of K with ϕ_R a homomorphism $R \to F$ and $\phi(x) = \infty$ if and only if x is nonzero and $\phi(x^{-1}) = 0$.

Lemma 1.96. *Let K be a field.*

(i) *If R is a valuation ring in K, then ϕ_R is a place.*

(ii) *If $\phi \colon K \to F \cup \{\infty\}$ is a place, then $R = \phi^{-1}(F)$ is a valuation ring in K with maximal ideal $M = \phi^{-1}(0)$.*

Proof. (i) If $x \notin R$ then $x^{-1} \in R$ and moreover $x^{-1} \in M$ (since $(x^{-1})^{-1} \notin R$). Also $x^{-1} \in M$ implies $x \notin R$. That is, ϕ_R satisfies $\phi(x) = \infty \Leftrightarrow \phi(x^{-1}) = 0$.

(ii) R is by definition a subring. If $x \notin R$ then $\phi(x) = \infty$ so $\phi(x^{-1}) = 0$ and $x^{-1} \in R$, so R is a valuation ring. Since $\phi(x) = 0 \Leftrightarrow x^{-1} \notin R$, we see that M is the set of non-units of R. □

So there is essentially a one-to-one correspondence between places and valuation rings (up to picking $F \cong R/M$).

Theorem 1.97 (Extension theorem for places). *Let K be a field, S a subring of K and $\sigma \colon S \to F$ a homomorphism to the algebraically closed field F. Then there exists a place $\phi_R \colon K \to F \cup \{\infty\}$ such that $R \supseteq S$ and $\phi_R|_S = \sigma$.*

Example 1.98. $K = \mathbb{C}$, $S = \mathbb{Z}$ and $F = \overline{\mathbb{F}}_p$.

Proof. Consider the set of all pairs (R, ϕ) such that $S \subseteq R \subseteq K$ and $\phi \colon R \to F$ is a homomorphism that extends σ. This is a poset under

$$(R_1, \phi_1) \leq (R_2, \phi_2) :\Leftrightarrow R_1 \subseteq R_2, \phi_2 \text{ extends } \phi_1.$$

This poset is non-empty, as it contains (S, σ), and chains are bounded, so by Zorn's lemma there is a maximal pair (R, ϕ). We will show that R is a valuation ring. Let $M = \ker(\phi)$.

Claim. M is the unique maximal ideal of R.

We show that $s \in R \setminus M$ implies $s^{-1} \in R$, so M contains all the non-units. Let

$$R' = \{r/s \mid r \in R, s \in R \setminus M\} \subseteq K$$

and define

$$\begin{aligned} \phi' \colon R' &\to F \\ r/s &\mapsto \phi(r)/\phi(s). \end{aligned}$$

We can check that ϕ' is a homomorphism extending ϕ, so by maximality we have $R' = R$, so $s^{-1} \in R$ for all $s \in R \setminus M$ in particular. Thus M is the unique maximal ideal of R and $\phi(R) \cong R/M$ is a field.

Claim. If $x \in K \setminus R$ then $1 \in M[x]$.

Consider the polynomial ring $R[t]$ and let

$$I = \{f \in R[t] \mid f(x) = 0\},$$

the kernel of the evaluation homomorphism $R[t] \to R[x]$, so $R[x] = R[t]/I$. Now ϕ extends to $\tilde{\phi} \colon R[t] \to \phi(R)[t]$ and so $\tilde{\phi}(I)$ is an ideal of $\phi(R)[t]$, which we will show is the whole ring. If that were not the case, then since $\phi(R)$ is a field, $\phi(R)[t]$ is a PID and there would exist a non-constant polynomial $h \in \phi(R)[t]$ such that $\tilde{\phi}(I) = (h)$. Since $\phi(R) \subseteq F$ and F is algebraically closed, we then have $y \in F$ such that $h(y) = 0$. Then the composition

$$R[t] \xrightarrow{\tilde{\phi}} \phi(R)[t] \xrightarrow{\text{ev}} F$$

has I in its kernel. This factors through $R[t]/I = R[x] \supsetneq R$, contradicting maximality of (R, ϕ). Thus $\tilde{\phi}(I) = \phi(R)[t]$ so $1 \in \tilde{\phi}(I)$ so picking some $f \in I$ such that $\tilde{\phi}(f) = 1$ we have $1 = f(t) + g(t)$, $g \in \ker(\tilde{\phi})$. But $\ker(\tilde{\phi}) = M[t]$ and $f(x) = 0$ so setting $t = x$ gives $1 = g(x) \in M[x]$.

We can now show R is a valuation ring. Suppose for the sake of contradiction that $x, x^{-1} \in K \setminus R$. Then we can find polynomials $g, h \in M[t]$ such that $1 = g(x) = h(x^{-1})$. Choose them to have minimal possible degree and suppose without loss of generality that $n = \deg(h) \leq \deg(g)$.

Now $1 = \sum_{i=0}^{n} a_i x^{-i}$ with $a_i \in M$. Then

$$(1 - a_0)x^n = \sum_{i=1}^{n} a_i x^{n-i} = \sum_{i=0}^{n-1} a_{n-i} x^i$$

and since $1 - a_0 \notin M$ it is invertible in R so we write

$$x^n = \sum_{i=0}^{n-1} \frac{a_{n-1}}{1 - a_0} x^i.$$

But we can substitute this into g to eliminate all terms of degree $\geq n$, a contradiction.

Thus R is a valuation ring, whose unique maximal ideal is $M = \ker(\phi)$. Thus $\phi_R \colon K \to F \cup \{\infty\}$ is a place. □

What is the "valuation"?

Definition 1.99. A *valuation* on a field K is a surjection $v\colon K \to vK \cup \{\infty\}$, where vK is an ordered abelian group (the *value group*) such that for all $x, y \in K$

- $v(x) = \infty \iff x = 0$,
- $v(xy) = v(x) + v(y)$, and
- $v(x + y) \geq \min\{v(x), v(y)\}$.

(Here we define $a + \infty = \infty$ for $a \in vK \cup \{\infty\}$ and $a < \infty$ for $a \in vK$.)

Example 1.100.

- p-adic valuation $\mathbb{Q}_p \to \mathbb{Z}$ ($\sum_{i=k}^{\infty} a_i p^i$ with $a_k \neq 0$ is mapped to k)
- $K((t)) \to \mathbb{Z}$: $\sum_{i=k}^{\infty} a_i t^i \mapsto k$.

Valuations v and w are equivalent if there is an order-preserving $\phi\colon vK \overset{\cong}{\to} wK$ such that $w = \phi \circ v$.

Proposition 1.101. *Equivalence classes of valuations on K are in one-to-one correspondence with valuation rings in K.*

Proof. Given $v\colon K \to vK \cup \{\infty\}$, $R_v = \{x \in K \mid v(x) \geq 0\}$ is a valuation ring: closure under addition and multiplication is immediate and $x \notin R_v$ implies $v(x) < 0$ which implies $v(x^{-1}) > 0$ so that $x^{-1} \in R_v$. Note that its group of units is $R_v^\times = \{x \in K \mid v(x) = 0\}$ and the maximal ideal is $M_v = \{x \in K \mid v(x) > 0\}$.

If $R \subseteq K$ is a valuation ring, then $\Gamma = K^\times / R^\times$ is an abelian group and it is ordered with positive cone $\{xR^\times \mid x \in M\}$. Since M is an ideal of R, $x \in M$ implies $xR^\times \subseteq M$ so there is no dependence on the choice of coset representative. If $x, y \in M \setminus \{0\}$ then $xy \in M \setminus \{0\}$ so we have a subsemigroup and $x \notin R \Leftrightarrow x^{-1} \in M$ so we indeed partition. □

Corollary 1.102. *Let p be a prime. Suppose $\mathbb{C}[G]$ contains non-zero zero divisors. Then $\mathbb{F}_{p^n}[G]$ contains zero divisors for some n.*

Proof. There is a homomorphism $\mathbb{Z} \to \overline{\mathbb{F}}_p$ so by the extension theorem for places there is a place $\phi\colon \mathbb{C} \to \overline{\mathbb{F}}_p \cup \{\infty\}$. Suppose $0 \neq \alpha, \beta \in \mathbb{C}[G]$ with $\alpha\beta = 0$. Consider $\{(\alpha)_g \mid g \in \operatorname{supp}(\alpha)\}$. This finite set contains some minimal $\lambda = (\alpha)_{g_0}$ under the corresponding valuation v so that $v((\alpha)_g) \geq v(\lambda)$ for $g \in \operatorname{supp}(\alpha)$ and hence $v(\lambda^{-1}(\alpha)_g) \geq 0$. That is, $\lambda^{-1}\alpha \in R[G]$ where $R \subset \mathbb{C}$ is the corresponding valuation ring $R = \phi^{-1}(\overline{\mathbb{F}}_p)$. Similarly some $\mu^{-1}\beta \in R[G]$ where $\mu = (\beta)_{h_0}$. Now $\overline{\alpha} = \phi(\lambda^{-1}\alpha)$, $\overline{\beta} = \phi(\mu^{-1}\beta) \in \overline{\mathbb{F}}_p[G]$ satisfy

$$\overline{\alpha}\overline{\beta} = \phi(\lambda^{-1}\mu^{-1}\alpha\beta) = \phi(0) = 0$$

but have support containing g_0, h_0 respectively. Since $\overline{\mathbb{F}}_p = \lim_{n\to\infty} \mathbb{F}_{p^n}$, the result follows. □

Lemma 1.103. *Let $S \subseteq K$ be a subring of a field and let $x_1, \ldots x_n$ be finitely many elements of K. Then there exists an element $s_0 \in S \setminus \{0\}$ such that if $\sigma\colon S \to F$ is a homomorphism to an algebraically closed field F with $\sigma(s_0) \neq 0$, then σ extends to a place $\phi_R\colon K \to F \cup \{\infty\}$ with $R \supseteq S[x_1, \ldots, x_n]$.*

Proof. TODO break up into exercises. □

Corollary 1.104. *Let $\operatorname{char}(K) = 0$ and let $x_1, \ldots, x_n \in K^\times$. Then for infinitely many primes p there exists a place $\phi_R\colon K \to \overline{\mathbb{F}}_p \cup \{\infty\}$ with $\phi_R(x_i) \neq 0$ or ∞ for all i.*

Proof. Take $S = \mathbb{Z}$ in Lemma 1.103 and take the finite set

$$\{x_1, \dots, x_n, x_1^{-1}, \dots, x_n^{-1}\}.$$

Then $s_0 \in \mathbb{Z}$ has only finitely many prime factors. For all other primes p, $\sigma\colon \mathbb{Z} \to \overline{\mathbb{F}}_p$ satisfies $\sigma(s_0) \neq 0$ and so extends to a place ϕ_R with $x_i, x_i^{-1} \in R$ which gives $\phi_R(x_i) \neq 0$ or ∞. □

Corollary 1.105. *If $\mathbb{C}[G]$ has a non-trivial unit, then for all but finitely many primes p there exists n such that $\mathbb{F}_{p^n}[G]$ has a non-trivial unit.*

Proof. Exercise. □

The augmentation map

$$\epsilon\colon R[G] \to R$$

restricts to a map $(R[G])^\times \to R^\times$. The kernel is $V(R[G])$, the group of *normalized* units. Since

$$1 \to V(R[G]) \to (R[G])^\times \to R^\times \to 1$$

is split such that $R^\times$ is central (assuming R to be commutative), then in fact $R[G] \cong R^\times \times V(R[G])$. The unit conjecture states that for torsion-free G, the natural injection $G \hookrightarrow V(K[G])$ is surjective.

We can strengthen the link between the unit conjecture and the zero divisor conjecture as follows.

Proposition 1.106. Let $\operatorname{char}(K) > 0$ and let G be torsion-free. Then $V(K[G])$ is torsion-free if and only if $K[G]$ has no zero divisors.

Proof. Let $\operatorname{char}(K) = p$. Suppose $0 \neq \alpha, \beta \in K[G]$ with $\alpha\beta = 0$. By primality of $K[G]$, we can assume without loss of generality that $\alpha = \beta$, that is, that $\alpha^2 = 0$ (by replacing α with some non-zero product $\beta\gamma\alpha$). Now

$$(1+\alpha)^p = 1 + p\alpha + \binom{p}{2}\alpha^2 + \cdots + \alpha^p = 1 + \alpha^p = 1.$$

Note that $\alpha^2 = 0$ implies $\epsilon(\alpha)^2 = 0 \in K$ so that $\epsilon(\alpha) = 0$. As $\alpha \neq 0$, we have that $1 + \alpha \in V(K[G])$ is non-trivial torsion.

Now suppose $1 \neq \alpha \in V(K[G])$ with $\alpha^n = 1$, for some $n \geq 2$. Then $(1-\alpha)(1 + \alpha + \cdots + \alpha^{n-1}) = 0$. The first factor is non-zero by assumption on α. The second factor has augmentation n, which is non-zero provided that $p \nmid n$. If $p \mid n$ then supposing (without loss of generality) that $\operatorname{ord}(\alpha) = n$, we have $\alpha^{n/p} \neq 1$ and thus

$$0 = 1 - \alpha^n = (1 - \alpha^{n/p})^p$$

so $K[G]$ has zero divisors. □

Corollary 1.107. *G satisfies the zero divisor conjecture for all fields K if and only if $V(K[G])$ is torsion-free for all fields K.*

Proof. We've already seen in Corollary 1.102 that G satisfies the zero divisor conjecture in characteristic 0 if it does in characteristic $p > 0$. If $V(K[G])$ has torsion for $\operatorname{char}(K) = 0$, the proof of Proposition 1.106 gives zero divisors in $K[G]$. □

Remark 1.108. The "detour" via positive characteristic is necessary – we cannot strengthen Corollary 1.107 to say for all K that $K[G]$ is a domain precisely when $V(K[G])$ is torsion-free (at least, not with our current knowledge). In particular, we don't know if $\mathbb{Z}[G]$ can have zero divisors for torsion-free G, but it is a theorem of Sehgal that $V(\mathbb{Z}[G])$ is torsion-free (in fact, $V(\mathcal{O}[G])$, where $\mathcal{O}$ is the ring of algebraic integers).

1.5.1. The power map.

Let $\mathrm{char}(K) = p > 0$. In a non-commutative K-algebra, we do not necessarily have $(\alpha+\beta)^p = \alpha^p + \beta^p$, but we will establish what one might call "Frobenius under the trace".

Definition 1.109. Let A be a K-algebra. The *commutator subspace* $[A, A]$ is the subspace spanned by $[\alpha, \beta] := \alpha\beta - \beta\alpha$ for $\alpha, \beta \in A$.

Lemma 1.110. *Let A be an algebra over a field K, with* $\mathrm{char}(K) = p > 0$. *If $\alpha_1, \dots, \alpha_m \in A$ and $q = p^n$, then*

$$(\alpha_1 + \alpha_2 + \cdots + \alpha_m)^q = \alpha_1^q + \cdots + \alpha_m^q \mod [A, A].$$

Proof. The difference $\beta := (\alpha_1 + \cdots + \alpha_m)^q - (\alpha_1^q + \cdots + \alpha_m^q)$ is a sum of expressions $\alpha_{i_1}\alpha_{i_2}\dots\alpha_{i_q}$ where not all indices are the same. Modulo $[A, A]$, cyclic permutation does not change such expressions. Note that $\mathbb{Z}/q\mathbb{Z}$ acts on the $m^q - m$ summands of β by cyclic permutation and all orbits have size greater than 1 and hence divisible by p. Thus $\beta \in [A, A]$. □

For $g \in G$ we write $[g]$ for its conjugacy class

$$[g] = [g]_\sim = g^G \in G/\sim.$$

Definition 1.111. For $g \in G$, let

$$\begin{aligned} \tau_{[g]} \colon K[G] &\to K \\ \alpha &\mapsto \sum_{h \in [g]} (\alpha)_h \end{aligned}$$

denote the sum of coefficients over the conjugacy class of g.

This is a K-linear map. "The" trace is $\mathrm{tr} = \tau_{[1]}$.

Lemma 1.112. *Let $\alpha \in K[G]$. Then $\alpha \in [K[G], K[G]]$ if and only if $\tau_{[g]}(\alpha) = 0$ for all $g \in G$. Moreover, a K-linear map $\tau \colon K[G] \to K$ annihilates $[K[G], K[G]]$ if and only if it is constant on conjugacy classes.*

Proof. Exercise. □

In particular, the trace identity

$$\tau_{[g]}(\alpha\beta) = \tau_{[g]}(\beta\alpha)$$

holds for all $g \in G$ and $\alpha, \beta \in K[G]$.

Definition 1.113. We call $g \in G$ a p-element if its order is p^n, $n \geq 1$. For $\alpha \in K[G]$, define

$$p\text{-supp}(\alpha) = \{g \in \mathrm{supp}(\alpha) \mid g \text{ is a } p\text{-element}\}.$$

Lemma 1.114. *Let $\alpha = \sum_g a_g \cdot g \in K[G]$ be nilpotent.*

(i) *If* $\mathrm{char}(K) = p > 0$ *then*

$$\mathrm{tr}(\alpha) + \sum_{g \in p\text{-}supp(\alpha)} a_g = 0.$$

In particular, either $\mathrm{tr}(\alpha) = 0$ *or* p*-supp*$(\alpha) \neq \emptyset$.

(ii) *If* $\mathrm{char}(K) = 0$ *then* $\mathrm{tr}(\alpha) = 0$.

Proof. (i) We choose $q = p^n$ large enough so that $\alpha^q = 0$ and $g^q = 1$ for all $g \in p\text{-supp}(\alpha)$. Thus

$$0 = \alpha^q = \sum_{g \in G} a_g^q g^q \mod [K[G], K[G]]$$

and taking traces gives

$$0 = \sum_{g^q=1} a_g^q = (\sum_{g^q=1} a_g)^q$$

and since $\{g \in \mathrm{supp}(\alpha) \mid g^q = 1\} = \{1\} \sqcup p\text{-supp}(\alpha)$, we have

$$\mathrm{tr}(\alpha) + \sum_{g \in p\text{-supp}(\alpha)} a_g = \sum_{g^q=1} a_g = 0.$$

(ii) By Corollary 1.104, for infinitely many primes p there exists a place $\phi_R \colon K \to \overline{\mathbb{F}}_p \cup \{\infty\}$ with $\phi_R(a_g) \neq 0, \infty$ for all $g \in \mathrm{supp}(\alpha)$. Thus $\alpha \in R[G]$ and its image $\tilde{\alpha}$ in $(R/M)[G] \subseteq \overline{\mathbb{F}}_p[G]$ is nilpotent. If $\mathrm{tr}(\alpha) \neq 0$, then $\mathrm{tr}(\tilde{\alpha}) = \phi_R(a_1) \neq 0$ and by (i) $p\text{-supp}(\alpha) \neq \emptyset$. But this cannot be true for infinitely many primes. □

Using this we can show some more trace functions vanish on nilpotents. We define a preorder on G by setting

$$x < y :\Leftrightarrow \langle\!\langle x \rangle\!\rangle_G \subseteq \langle\!\langle y \rangle\!\rangle_G .$$

That is, $<$ is reflexive and transitive, but not antisymmetric. It induces a partial order on $\approx$-equivalence classes, where we say

$$x \approx y :\Leftrightarrow (x < y \text{ and } y < x) \Leftrightarrow \langle\!\langle x \rangle\!\rangle_G = \langle\!\langle y \rangle\!\rangle_G .$$

Remark 1.115. This is a coarser equivalence relation than conjugacy. We always have $x \approx x^{-1}$. Magnus proved that if $x, y \in F_n$ with $x \approx y$, then $x \sim y$ or $x \sim y^{-1}$. In general this is far from true, e.g. a simple group G has two $\approx$-classes: $\{1\}$ and $G \setminus \{1\}$.

If $S = [g]_\approx \in G/\approx$, we define

$$\tau_S \colon K[G] \to K \colon \alpha \mapsto \sum_{g \in S} (\alpha)_g.$$

Remark 1.116. If we pick a transversal X for $[g]_\approx/\sim$, then $\tau_S = \sum_{x \in X} \tau_{[x]}$.

Proposition 1.117. If $\mathrm{char}(K) = 0$ and $\alpha \in K[G]$ is nilpotent, then $\tau_S(\alpha) = 0$ for each $S \in G/\approx$.

Proof. We "induct" over the finite poset of $\approx$-classes S that intersect $\mathrm{supp}(\alpha)$. Pick a maximal such S for which we haven't proved $\tau_S(\alpha) = 0$. Let $x \in S$. Then $y \in \langle\!\langle x \rangle\!\rangle_G$ if and only if $[y]_\approx = T \leq S$. The image of α in $K[G/\langle\!\langle x \rangle\!\rangle_G]$ is nilpotent and has trace

$$0 = \sum_{y \in \langle\!\langle x \rangle\!\rangle_G} (\alpha)_y = \sum_{T \leq S} \tau_T(\alpha).$$

As $\tau_T(\alpha) = 0$ for $T \lneq S$, we are done. □

We will need the following black box from number theory and a corollary of it. (The black box is a consequence of the Frobenius density theorem.)

Proposition 1.118. Let $f \in \mathbb{Z}[t]$ be a monic irreducible polynomial with $\deg f > 1$. Then there exist infinitely many primes p such that $f \bmod p \in (\mathbb{Z}/p\mathbb{Z})[t]$ does not have all its roots in $\mathbb{Z}/p\mathbb{Z}$.

Corollary 1.119. *Let* $\operatorname{char}(K) = 0$ *and* $x_0, x_1, \ldots, x_n \in K$ *with* $x_0 \notin \mathbb{Q}$. *Then for infinitely many primes* p, *there exists a place* $\phi_R \colon K \to \overline{\mathbb{F}}_p \cup \{\infty\}$ *with* $\phi_R(x_i) \neq 0$ *for all* i *and* $\phi_R(x_0) \notin \mathbb{F}_p$.

THEOREM 1.120 (Zalesskii). *Let* $e \in K[G]$ *be an idempotent. Then* $\operatorname{tr}(e)$ *is in the prime subfield of* K.

PROOF. Let $e = \sum_g a_g g$ and suppose first that $\operatorname{char}(K) = p > 0$. Let $S = \{1\} \cup p\text{-supp}(e)$. We can find n_0 such that $g^{p^n} = 1$ for all $g \in S$ and $n \geq n_0$. Moreover, $S = \left\{ g \in \operatorname{supp}(e) \,\middle|\, g^{p^n} = 1 \right\}$ for all $n \geq n_0$. By "Frobenius under the trace" (i.e. Lemma 1.110 plus Lemma 1.112) we have for $q = p^n, n \geq n_0$

$$\operatorname{tr}(e^q) = \sum_{g \in S} a_g^q = (\sum_{g \in S} a_g)^q$$

so now $e = e^2$ implies $e = e^{p^{n_0}} = e^{p^{n_0+1}}$ and thus

$$\operatorname{tr}(e) = \left(\sum_{g \in S} a_g \right)^{p^{n_0}} = \left(\sum_{g \in S} a_g \right)^{p^{n_0+1}}$$

so that $\operatorname{tr}(e)$ is a root of the polynomial $x^p - x$, which has all its roots in $\mathbb{F}_p$.

Now suppose $\operatorname{char}(K) = 0$ and suppose for the sake of contradiction that $\operatorname{tr}(e) \notin \mathbb{Q}$. By Corollary 1.119 there exists a prime p (in fact, infinitely many) and a place $\phi_R \colon K \to \overline{\mathbb{F}}_p \cup \{\infty\}$ such that $\phi_R(a_g) \neq \infty$ for all $g \in \operatorname{supp}(e)$ and $\phi_R(a_1) = \phi_R(\operatorname{tr}(e)) \notin \mathbb{F}_p$. But then $e \in R[G]$ and its image $\tilde{e} \in (R/M)[G] \subseteq \overline{\mathbb{F}}_p[G]$ is an idempotent and has trace $\operatorname{tr}(\tilde{e}) = \phi_R(\operatorname{tr}(e)) \notin \mathbb{F}_p$, contradicting the characteristic p case. □

Our results on traces of nilpotents and idempotents admit a nice generalization, which we state but will not prove.

THEOREM 1.121. *Let* α *be an algebraic element of* $K[G]$ *with minimal polynomial* $f(t) \in K[t]$. *Let* $\lambda_1, \ldots, \lambda_n$ *be the distinct roots of* f *in some algebraic closure of* K.

(i) *If* $\operatorname{char}(K) = 0$ *then there exist rational numbers* $r_1, \ldots, r_n$ *satisfying* $0 < r_i$ *and* $\sum_{i=1}^n r_i = 1$ *such that*

$$\operatorname{tr}(\alpha) = \sum_{i=1}^{n} r_i \lambda_i.$$

(ii) *If* $\operatorname{char}(K) = p > 0$ *and either* G *has no* p*-elements or* $f(t)$ *has no repeated roots, then there exist* $r_1, \ldots, r_n \in \mathbb{F}_p$ *with* $\sum_{i=1}^n r_i = 1$ *such that*

$$\operatorname{tr}(\alpha) = \sum_{i=1}^{n} r_i \lambda_i.$$

Theorem 1.122 (Formanek). *Let G be a torsion-free group. Let*

$$N_G = \left\{ p \,\middle|\, p \text{ is prime and there exist } g \in G \setminus \{1\}, n \in \mathbb{Z}^+ \text{ s.t. } g \sim g^{p^n} \right\}$$

(this is the set of primes that are in a sense "bad" for G). Suppose $e \in K[G]$ is an idempotent.

(i) *If* $\operatorname{char}(K) = p > 0$ *and $p \notin N_G$, then* $\operatorname{tr}(e) = 0$ *or* 1.

(ii) *If* $\operatorname{char}(K) = 0$ *and $p \notin N_G$ for infinitely many primes p, then $e = 0$ or 1.*

Remark 1.123. When Formanek proved this theorem in 1973, the condition $|N_G| < \infty$ may have appeared somewhat esoteric. Since then, geometric group theory has brought many groups into focus where this holds (often $N_G = \emptyset$).

Example 1.124. $|N_G| < \infty$ for torsion-free G if G is

- a finitely generated subgroup of $\mathrm{GL}_n F$, F any field (Bass)
- hyperbolic
- CAT(0)
- a subgroup of $\mathrm{Out}(F_n)$ or the mapping class group $\mathrm{Mod}(\Sigma)$ of a surface

Corollary 1.125. *All those groups satisfy the idempotent conjecture in characteristic* 0.

Remark 1.126. Osin proved that every countable torsion-free group embeds into a torsion-free group G with exactly 2 conjugacy classes. Then N_G contains all primes!

Proof of Formanek's Theorem 1.122. (i) Let $e = \sum_g a_g g \in K[G]$, $\operatorname{char}(K) = p > 0$, $p \notin N_G$. Let $h \in G \setminus \{1\}$. We wish to compute

$$\tau_{[h]}(e) = \sum_{g \sim h} a_g.$$

For any $g \in G \setminus \{1\}$, there is at most one $n \in \mathbb{Z}^+$ such that $g^{p^n} \sim h$, as otherwise $g^{p^{n+i}} \sim g^{p^n}$ with $i \geq 1$ and then $(g^{p^n})^{p^i} \sim g^{p^n}$, contradicting $p \notin N_G$. Since $\operatorname{supp}(e)$ is finite, there exists $q = p^n$ such that $g^q \not\sim h$ for all $g \in \operatorname{supp}(e)$. Now Frobenius under the trace gives us, since $e = e^q$, that

$$\tau_{[h]}(e) = \tau_{[h]}(e^q) = \sum_{\substack{g \in \operatorname{supp}(e) \\ g^q \sim h}} a_g^q = \sum_{g \in \emptyset} a_g^q = 0$$

for all $h \neq 1$. Now the augmentation $\epsilon(e) = 0$ or 1 in K, since it is an idempotent. But

$$\epsilon(e) = \sum_{[g] \in \operatorname{supp}(e)/\sim} \tau_{[g]}(e) = \tau_{[1]}(e) = \operatorname{tr}(e)$$

so that $\operatorname{tr}(e) = 0$ or 1.

(ii) Now $\operatorname{char}(K) = 0$. Suppose for the sake of contradiction that $e \neq 0$ or 1, so that by Kaplansky's Theorem 1.83 we have $a_1 = \operatorname{tr}(e) \neq 0$ or 1. Then set $b = a_1(1 - a_1) \neq 0$. By Corollary 1.104, for all but finitely many primes p, there is a place $\phi_R \colon K \to \overline{\mathbb{F}}_p \cup \{\infty\}$ with all $\phi_R(a_g) \neq \infty$ and $\phi_R(b) \neq 0$ (or ∞).

Thus $e \in R[G]$ has image $\tilde{e} \in (R/M)[G] \subseteq \overline{\mathbb{F}}_p[G]$ with trace $\phi_R(a_1) \neq 0$ or 1 (since $\phi_R(a_1)(1 - \phi_R(a_1)) = \phi_R(b) \neq 0$). For infinitely many of these p we will also have $p \notin N_G$, which contradicts the $\operatorname{char}(K) = p$ case. □

1.6. The unit conjecture counterexample

Rips and Segev (1987) gave the first example of a torsion-free group without unique products, using small cancellation theory ($|A| = 4$ and B is huge). Promislow showed shortly thereafter (1988) that the crystallographic group

$$P = \langle\, a, b \,|\, b^{-1}a^2b = a^{-2}, a^{-1}b^2a = b^{-2} \,\rangle$$

does not have unique products, with $A = B$, $|A| = 14$. In 2021, it was shown that $K[P]$ is a counterexample to the unit conjecture whenever char $K > 0$ (Gardam, Murray).

Let $D_\infty = \langle\, r, t \,|\, r^2 = 1, t^r = t^{-1} \,\rangle$ denote the infinite dihedral group. It naturally acts on $\mathbb{R}$ (isometrically) via $t \cdot x = x + 1$ and $r \cdot x = -x$ ("translate" and "rotate").

Lemma 1.127.

$$\begin{aligned} \phi\colon P &\to D_\infty \times D_\infty \times D_\infty \\ a &\mapsto (t, tr, r) \\ b &\mapsto (r, t, tr) \end{aligned}$$

is an injective group homomorphism.

Remark 1.128. The stabilizer of $K^n \times \{1\}$ in $GL(K^n \oplus K)$ is $\mathrm{Aff}(K^n)$. This lets us rephrase the above embedding as the faithful representation

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

Proof of Lemma 1.127. Note that $\phi(a^2) = (t^2, 1, 1)$ so that $\phi(b^{-1}a^2b) = (r^{-1}t^2r, 1, 1) = (t^{-2}, 1, 1) = \phi(a^{-2})$. Similarly $\phi(a^{-1}b^2a) = \phi(b^{-2})$, so this is a well-defined group homomorphism.

Since $(a^2)^b = a^{-2}$, we have $b \in N_P(\langle a^2 \rangle)$, thus $\langle a^2 \rangle \lhd P$ and likewise $\langle b^2 \rangle \lhd P$. As $(a^2)^{b^2} = (a^{-2})^b = a^2$, we see that $\mathbb{Z}^2 \cong \langle a^2, b^2 \rangle \lhd P$. The relations of P are a consequence (in general) of $a^2 = 1$ and $b^2 = 1$ respectively, so $P/\langle a^2, b^2 \rangle \cong \langle\, a, b \,|\, a^2, b^2 \,\rangle \cong D_\infty$. The abelianization of D_∞ is $\mathbb{Z}/2 \oplus \mathbb{Z}/2$ with $[D_\infty, D_\infty] = \langle abab \rangle \cong \mathbb{Z}$ (exercise!). Let $x = a^2, y = b^2, z = (ab)^2$. Now $x^z = (a^2)^{abab} = (a^2)^{bab} = (a^{-2})^{ab} = (a^{-2})^b = a^2 = x$ and similarly $y^z = y$. Thus $\langle x, y, z \rangle \cong \mathbb{Z}^3$ is a normal subgroup of P with quotient $\mathbb{Z}/2 \oplus \mathbb{Z}/2$.

Since $\phi(x) = (t^2, 1, 1)$, $\phi(y) = (1, t^2, 1)$ and $\phi(ab) = (tr, trt, rtr) = (tr, r, t^{-1})$ which implies $\phi(z) = (1, 1, t^{-2})$, we see that ϕ is injective on $\langle x, y, z \rangle$. We project $D_\infty \times D_\infty \times D_\infty$ onto the first two factors and then maps to $\mathbb{Z}/2 \oplus \mathbb{Z}/2$ by quotienting out the corresponding $\langle t \rangle$. This gives a map $q \circ \phi\colon P \twoheadrightarrow \mathbb{Z}/2 \oplus \mathbb{Z}/2$ which has $\langle x, y, z \rangle$ in the kernel. Since $P/\langle x, y, z \rangle \cong \mathbb{Z}/2 \oplus \mathbb{Z}/2$, we see $\ker(q \circ phi) = \langle x, y, z \rangle$ and thus $g \notin \langle x, y, z \rangle$ implies $\phi(g) \neq 1$. So ϕ is injective. □

Exercise 1.6.1. Show that $\langle\, r, t \,|\, r^2, t^r = t^{-1} \,\rangle \cong \langle\, a, b \,|\, a^2, b^2 \,\rangle$ and that the latter has derived subgroup $\langle abab \rangle \cong \mathbb{Z}$.

Exercise 1.6.2. Show that if G does not have the unique product property then there is a finite subset $A \subset G$ such that $A \cdot A$ does not have a unique product. Deduce that if G does not have the unique product property, then there are arbitrarily large sets A that witness this.

Having identified the abstract finitely presented group P with a subgroup of $D_\infty \times D_\infty \times D_\infty$ in Lemma 1.127, we can prove:

Corollary 1.129. *P is torsion-free.*

Proof. The abelianization of D_∞ is $\mathbb{Z}/2 \oplus \mathbb{Z}/2$ and an element is non-trivial torsion if and only if it has image $(0, \bar{r})$ or $(\bar{t}, \bar{r})$. Thus the abelianization of D_∞^3 is an elementary abelian 2-group (isomorphic to $(\mathbb{Z}/2)^6$) and the image of P is an order 4 subgroup of $(D_\infty^3)^{\mathrm{ab}}$, comprising

$$\begin{aligned} \overline{\phi(1)} &= ((0,0),(0,0),(0,0)) \\ \overline{\phi(a)} &= ((\bar{t},0),(\bar{t},\bar{r}),(0,\bar{r})) \\ \overline{\phi(b)} &= ((0,\bar{r}),(\bar{t},0),(\bar{t},\bar{r})) \\ \overline{\phi(ab)} &= ((\bar{t},\bar{r}),(0,\bar{r}),(\bar{t},0)). \end{aligned}$$

Thus every element of P is either in the torsion-free subgroup $\langle x, y, z\rangle \cong \mathbb{Z}^3$ or has infinite order in precisely one of the three D_∞ factors. Thus P is torsion-free. □

Alternative proof of Corollary 1.129. (This abstract proof, that does not require identifying P with a subgroup of $D_\infty \times D_\infty \times D_\infty$, is not examinable.) We rewrite

$$\begin{aligned} P &= \langle\, x, b, y, a \,|\, x^b = x^{-1}, y^a = y^{-1}, x = a^2, b^2 = y \,\rangle \\ &= \langle\, x, b \,|\, x^b = x^{-1} \,\rangle \underset{\substack{x=a^2 \\ b^2=y}}{*} \langle\, y, a \,|\, y^a = y^{-1} \,\rangle \end{aligned}$$

and since $\langle x, b^2\rangle \cong \langle a^2, y\rangle \cong \mathbb{Z}^2$ this exhibits P as the free product with amalgamation over $\mathbb{Z}^2$ of two Klein bottle groups. A standard fact of Bass–Serre theory is that free product with amalgamation preserves torsion-freeness. □

Recall that bi-orderable $\implies$ locally indicable $\implies$ left-orderable $\implies$ diffuse $\implies$ unique products $\implies$ unit conjecture. Each successive property is weaker and indeed more difficult to falsify for P.

Definition 1.130. A group G is *bi-orderable* if it admits a total order $<$ that is bi-invariant, that is, $g < h$ implies $kg < kh$ and $gk < hk$ for all $g, h, k \in G$.

P is not bi-orderable: a^2 is non-trivial and conjugate to a^{-2}

P is not locally indicable: we compute $P^{\mathrm{ab}} \cong \mathbb{Z}^2/\langle(4,0),(0,4)\rangle \cong \mathbb{Z}/4 \oplus \mathbb{Z}/4$ so P itself does not surject onto $\mathbb{Z}$.

P is not left-orderable: note that $\sigma_a \colon P \to P \colon a \mapsto a^{-1}, b \mapsto b$ is an automorphism, as

$$\sigma_a(b^{-1}a^2ba^2) = b^{-1}a^{-2}ba^{-2} \sim a^{-2}b^{-1}a^{-2}b = (b^{-1}a^2ba^2)^{-1}$$

and

$$\sigma_a(a^{-1}b^2ab^2) = ab^2a^{-1}b^2 \sim a^{-1}b^2ab^2$$

so it is a well-defined group homomorphism $P \to P$, which is an involution so in particular an automorphism. (Similarly $\sigma_b \colon P \to P \colon a \mapsto a, b \mapsto b^{-1}$ is an automorphism.) Suppose $<$ is a left-order on P. We can now suppose without loss of generality that $a > 1$ and $b > 1$. But $a^{-1}b \neq 1$ and if $a^{-1}b > 1$ we have

$$1 = a^{-1}b^2ab^2 = (a^{-1}b) \cdot b \cdot a \cdot b^2 > 1$$

and if $a^{-1}b < 1$ we have $b^{-1}a > 1$ and thus

$$1 = b^{-1}a^2ba^2 = (b^{-1}a) \cdot a \cdot b \cdot a^2 > 1$$

giving a contradiction in either case.

Bowditch gave an elegant proof that P is not diffuse (after this was already known via failure of unique products). We exploit some 3-fold symmetry that is not immediately clear from the 2-generator presentation. Recall

$$\phi(ab) = (tr, r, t^{-1})$$

and thus

$$\phi(b^{-1}a^{-1}) = (tr, r, t)$$

and hence cycling the factors of D_∞^3 cycles through a, b, $c := b^{-1}a^{-1}$. (In a sense, this is "all" the 3-fold symmetry of P, as $|\mathrm{Out}(P)| = 2^5 \cdot 3$.)

As we are acting on the left, it is more convenient to phrase diffuseness in terms of extremal points $a \in A$ such that $sa \notin A$ or $s^{-1}a \notin A$ for all $s \in G \setminus \{1\}$. It is also convenient to replace the finite set $A \subset G$ with a finite set $A \subset X$, where $G \curvearrowright X$ simply transitively. In this case, $X = \{(x, y, z) \in \mathbb{Z}^3 \,|\, x + y + z = 1 \mod 2\}$.

For the set A we take 6 elements:

$$A = \{(\pm 1, 0, 0), (0, \pm 1, 0), (0, 0, \pm 1)\}.$$

The isometry $\phi(a)$ is a glide reflection about $y = \frac{1}{2}, z = 0$. Since for example

$$a\colon (-1, 0, 0) \mapsto (0, 1, 0) \mapsto (1, 0, 0)$$

we see that $(0, 1, 0)$ is *not* extremal. As $b^{-2} \cdot (0, 1, 0) = (0, -1, 0)$ and $(b^{-2}a)^2 = a^2$ we also have

$$b^{-2}a\colon (-1, 0, 0) \mapsto (0, -1, 0) \mapsto (1, 0, 0)$$

so that also $(0, -1, 0)$ is *not* extremal. By symmetry the same is true for the other 4 points, completing the proof that P is not diffuse.

We name the sets that witness the failure of diffuseness:

Definition 1.131. A finite subset $A \subset G$ is called a *ravel* if it contains no extremal points, i.e. for all $a \in A$ there exists $1 \neq s \in G$ such that $sa, s^{-1}a \in A$.

We have a translational degree of freedom: if A is a ravel then so is Ag for any $g \in G$. Similarly, turning the failure of diffuseness for $P \curvearrowright \mathbb{R}^3$ into a ravel $A \subset P$ requires a choice of basepoint. Let's pick $p = (0, 1, 0)$. Recall

$$\begin{aligned} a&\colon (-1, 0, 0) \mapsto (0, 1, 0) \mapsto (1, 0, 0) \\ b&\colon (0, -1, 0) \mapsto (0, 0, 1) \mapsto (0, 1, 0) \\ c&\colon (0, 0, -1) \mapsto (1, 0, 0) \mapsto (0, 0, 1) \end{aligned}$$

so we compute labels for our six points as

$$\begin{aligned} a^{-1} \cdot p &= (-1, 0, 0) & a \cdot p &= (1, 0, 0) \\ b^{-2} \cdot p &= (0, -1, 0) & p &= (0, 1, 0) \\ c^{-1}a \cdot p &= (0, 0, -1) & b^{-1} \cdot p &= (0, 0, 1). \end{aligned}$$

This gives the ravel $A = \{g_1, \ldots, g_6\}$ with

$$g_1 = a^{-1}, g_2 = a, g_3 = b^{-2}, g_4 = 1, g_5 = c^{-1}a, g_6 = b^{-1}.$$

The failure to have extremal points is verified by

$$\begin{aligned} a\colon g_1 &\mapsto g_4 \mapsto g_2 \\ b^{-2}a\colon g_1 &\mapsto g_3 \mapsto g_2 \\ b\colon g_3 &\mapsto g_6 \mapsto g_4 \\ c^{-2}b\colon g_3 &\mapsto g_5 \mapsto g_4 \\ c\colon g_5 &\mapsto g_2 \mapsto g_6 \\ a^{-2}c\colon g_5 &\mapsto g_1 \mapsto g_6. \end{aligned}$$

A natural question is: what is encoded by this combinatorial data? The data is: each element of A has a corresponding pair of elements it lies between e.g. $g_4 \rightsquigarrow \{g_1, g_2\}$. The existence of $s \in G$ (in this case: $s = a$) such that $g_1 = s^{-1}g_4, g_2 = sg_4$ is equivalent to $g_4 g_1^{-1} g_4 g_2^{-1} = 1$.

(Note: in general, there could be multiple $s \neq 1$ such that $s^{-1}a, sa \in A$, beyond having a given $s^{\pm 1}$. We assume a choice has been made for simplicity.)

Given this data as $f\colon \{1, \ldots, n\} \to \binom{\{1,\ldots,n\}}{2}$, where $i \notin f(i)$, we add for notational convenience an arbitrary order on the pairs, writing $f(i) = \{s(i), t(i)\}$, and then we can define a group

$$G_f = \langle\, g_1, \ldots, g_n \mid g_i g_{s(i)}^{-1} g_i g_{t(i)}^{-1}, i = 1, \ldots, n \,\rangle.$$

In our case, this is

$$G = \left\langle g_1, \ldots, g_6 \,\middle|\, \begin{smallmatrix} g_1 g_5^{-1} g_1 g_6^{-1},\, g_2 g_5^{-1} g_2 g_6^{-1},\, g_3 g_1^{-1} g_3 g_2^{-1}, \\ g_4 g_1^{-1} g_4 g_2^{-1},\, g_5 g_3^{-1} g_5 g_4^{-1},\, g_6 g_3^{-1} g_6 g_4^{-1} \end{smallmatrix} \right\rangle.$$

By construction, $G \twoheadrightarrow \langle A \rangle = P$.

Lemma 1.132. *$G_f \cong H_f * \mathbb{Z}$ for some group H_f.*

The free factor of $\mathbb{Z}$ corresponds to our translational degree of freedom. Note that H_f is *a priori* "well-defined": $H * \mathbb{Z} \cong K * \mathbb{Z} \implies H \cong K$ by Grushko's theorem.

Proof. We choose a "basepoint" g_j and change to the basis $h_1, \ldots, h_j, g_j, h_{j+1}, \ldots, h_n$ of the free group $F(g_1, \ldots, g_n)$, where we set $h_i = g_i g_j^{-1}$ for $i = 1, \ldots, n$. (NB: $h_j = 1$!) Thus $g_i = h_i g_j$. Note that

$$g_i g_{s(i)}^{-1} g_i g_{t(i)}^{-1} = h_i g_j (h_{s(i)} g_j)^{-1} h_i g_j (h_{t(i)} g_j)^{-1} = h_i h_{s(i)}^{-1} h_i h_{t(i)}^{-1}$$

is a word in the free group $F(h_1, \ldots, \widehat{h_j}, \ldots, h_n)$ of rank $n - 1$ and so substituting gives

$$G_f = \langle\, h_1, \ldots, h_{j-1}, h_{j+1}, \ldots, h_n \mid h_i h_{s(i)}^{-1} h_i h_{t(i)}^{-1} \,\rangle * \langle\, g_j \mid \,\rangle$$

which completes the proof as $\langle\, g_j \mid \,\rangle \cong \mathbb{Z}$. □

Remark 1.133. As $g_i g_k^{-1} = (g_i g_j^{-1})(g_k g_j^{-1})^{-1} = h_i h_k^{-1}$, we see that

$$H_f = \langle \{ g_i g_k^{-1} \,|\, i, k \in \{1, \ldots, n\} \} \rangle$$

which is independent of the choice of j.

Lemma 1.134. *For Bowditch's 6-element ravel function f, we have $H_f \cong P$.*

In other words, one could say P is the universal group supporting this ravel.

PROOF. We "cheat" by keeping in mind that we have a homomorphism $G_f \twoheadrightarrow P$ which sends $g_2 \mapsto a, g_4 \mapsto 1, g_6 \mapsto b^{-1}$. So g_4 is a convenient choice of basepoint (but any choice works!).

We have

$$H_f = \left\langle h_1, h_2, h_3, h_5, h_6 \,\middle|\, \begin{array}{c} h_1h_5^{-1}h_1h_6^{-1}, \underline{h_2h_5^{-1}h_2h_6^{-1}}, h_3h_1^{-1}h_3h_2^{-1}, \\ \underline{h_1^{-1}h_2^{-1}}, h_5h_3^{-1}h_5, \underline{h_6h_3^{-1}h_6} \end{array} \right\rangle$$

where the underlined relations will be used to eliminate variables h_5, h_1 and h_3 respectively. We rename h_2 to be a and h_6 to be b^{-1}, then use

$$h_5 = aba, \quad h_1 = a^{-1}, \quad h_3 = b^{-2}$$

to write

$$\begin{aligned} H_f &\cong \langle\, a, b \,|\, a^{-1}(aba)^{-1}a^{-1}(b^{-1})^{-1},\ b^{-2}ab^{-2}a^{-1},\ (aba)b^2(aba) \,\rangle \\ &\cong \langle\, a, b \,|\, a^{-2}b^{-1}a^{-2}b,\ b^{-2}ab^{-2}a^{-1},\ (aba)^2b^2 \,\rangle \\ &\cong \langle\, a, b \,|\, b^{-1}a^2b = a^2,\ a^{-1}b^2a = b^2,\ (aba)^2b^2 \,\rangle \end{aligned}$$

but in P we have

$$(aba)^2 = a(ba^2)ba = a(a^{-2}b)ba = a^{-1}b^2a = b^{-2}$$

so the final relator is redundant and indeed $H_f \cong P$. □

The ravel function f clearly has symmetries, i.e. permutations $\sigma \in \mathrm{Sym}(n)$ such that $f(\sigma(i)) = \{\sigma(s(i)), \sigma(t(i))\}$ for all i. Specifically, its automorphism group is isomorphic to the wreath product $\mathbb{Z}/2 \wr \mathbb{Z}/3$, generated by (1 2) and (1 3 5)(2 4 6). Such an automorphism induces an automorphism

$$\sigma \colon G_f \to G_f \colon g_i \mapsto g_{\sigma(i)}$$

since it (and its inverse) preserve the relations. Moreover, as $H_f = \langle g_ig_k^{-1} \rangle$ and σ simply permutes the elements of the set $\left\{g_ig_k^{-1} \,\middle|\, i,k \in \{1,\ldots,n\}\right\}$, this restricts to an automorphism of H_f.

EXERCISE 1.6.3. Compute the automorphisms of P induced by the generating symmetries (1 2) and (1 3 5)(2 4 6) of the automorphism group of Bowditch's ravel.

We now turn to:

THEOREM 1.135 (Promislow). *P is not a UP group.*

The duplex is of the form (S, S) where $|S| = 14$.

The combinatorial data of a duplex with $|A| = m$, $|B| = n$ is a partition of (or equivalent relation on) $\{1,\ldots,m\} \times \{1,\ldots,n\}$ into sets of size at least 2. Similarly to with ravels, this also defines a finitely presented group: if (i,j) and (k,l) are in the same set of the partition then we have a relation $a_ib_j = a_kb_l$.

This group similarly has an obvious free factor, this time a free factor of $F_2 = \mathbb{Z} * \mathbb{Z}$ (corresponding to left translation on A and right translation on B). The data for Promislow's duplex has no non-trivial symmetry in $\mathrm{Sym}(14) \times \mathrm{Sym}(14)$ – but it does in $(\mathrm{Sym}(14) \times \mathrm{Sym}(14)) \rtimes \mathbb{Z}/2$ where we allow swapping the sets A and B. Such a twist is *not* an automorphism of the corresponding universal group as $a_ib_j = a_kb_l$ is *not* equivalent to $b_ja_i = b_ja_k$. We only get an automorphism after inversion. In other words: there exists $\phi \in \mathrm{Aut}(P)$ such that $S = \phi(S)^{-1}$.

Remark 1.136. Our presentation of Promislow's example differs from his. He uses a different embedding $P \hookrightarrow D_\infty^3$ and exploits symmetry on a "piecewise" basis i.e. coset by coset. Both expositions really boil down to P being virtually abelian.

For notational brevity, we follow Promislow's example and write n for $t^n \in D_\infty$ and $n*$ for $t^n r \in D_\infty$.

Let

$$\begin{aligned} E_0 &= \{(0,0,-2),(0,0,2)\} \\ E_1 &= \{(-1,1*,2*),(-1,-1*,0*),(-1,1*,0*) \\ &\qquad (1,1*,-2*),(1,-1*,0*),(1,1*,0*)\} \\ E_2 &= \{(2*,-1,1*),(0*,-1,1*),(0*,-1,-1*) \\ &\qquad (2*,1,-1*),(0*,1,-1*),(0*,1,1*)\} \end{aligned}$$

THEOREM 1.137 (Promislow). *Let $S = E_0 \cup E_1 \cup E_2$. Then $S \cdot S$ has no unique product.*

The automorphism ϕ is conjugation by $(1,1,r) \in D_\infty^3$ i.e. by $(0,0,0*)$ in Promislow's shorthand.

Lemma 1.138. *Let ϕ be conjugation by $(0,0,0*)$ and let S be as Theorem 1.137. Then $\phi(S) = S^{-1}$.* □

Remark 1.139. Let $A = \langle x,y,z\rangle \lhd P$. Then $E_0 \subset A$, $E_1 \subset aA$, $E_2 \subset bA$.

Note that $\phi(c) = (tr,r,t)^{(1,1,r)} = (tr,r,t^{-1}) = c^{-1}$ and that $\phi\colon x \mapsto x, y \mapsto y, z \mapsto z^{-1}$.

Why is Lemma 1.138 helpful? We'll see in Corollary 1.142. Let's keep in mind:

Lemma 1.140. *The map $G \to G\colon g \mapsto g^{-1}$ is an automorphism if and only if G is abelian.*

PROOF. Since it is a bijection, it is an automorphism if and only if for all $g,h \in G$ we have $(gh)^{-1} = g^{-1}h^{-1}$ which is equivalent to $gh = hg$. □

Lemma 1.141. *If $A \lhd G$ is an abelian normal subgroup and $\phi \in \mathrm{Aut}(G)$, $g \in G$ are such that $\phi(g) = g^{-1}$ and $\phi(a)^g = a^{-1}$ for all $a \in A$, then $\phi(h) = h^{-1}$ for all $h \in gA$.*

PROOF. There exists $a \in A$ such that $h = ga$ and so

$$\phi(h) = \phi(ga) = \phi(g)\phi(a) = g^{-1}\phi(a)gg^{-1} = a^{-1}g^{-1} = h^{-1}.$$

□

Corollary 1.142 (to Lemma 1.138)**.** $E_1 \cdot E_2 = E_2 \cdot E_1$.

PROOF. We note that Lemma 1.141 is satisfies for $G = P$, $A = \langle x,y,z\rangle$, $g = c$ and the aforementioned ϕ. So if $u \in E_1$, $v \in E_2$, then $uv \in cA$ and $\phi(uv) = v^{-1}u^{-1}$ so that $uv = \phi(v)^{-1}\phi(u)^{-1} \in E_2 \cdot E_1$ as $E_2 = \phi(E_2)^{-1}$ and $E_1 = \phi(E_1)^{-1}$. □

We also have $E_0 \cdot E_1 = E_1 \cdot E_0$ and $E_0 \cdot E_2 = E_2 \cdot E_0$ (for similar but not identical reasons), so the tedious part is verifying that every element of A in $S \cdot S$ occurs at least twice, which we skip.

The known non-trivial units of torsion-free groups exhibit symmetry.

Definition 1.143. Let $\theta \in \mathrm{Aut}(K[G])$. We call a unit $\alpha \in K[G]$ *θ-unitary* if $\alpha^{-1} = \theta(\alpha)^*$.

If $K[G]$ has non-trivial units, then $\mathrm{Aut}(K[G])$ is big and mysterious – including conjugation by all units. We'll consider the subgroup of automorphisms that preserve the subgroup $K^\times \times G$ of trivial units.

Let G and H be arbitrary groups. We have $\mathrm{Aut}(G) \times \mathrm{Aut}(H) \hookrightarrow \mathrm{Aut}(G \times H)$ in the obvious way, but $\mathrm{Aut}(G \times H)$ can be much bigger. Consider for example $G = H = \mathbb{Z}$: we're comparing $\left\{\left(\begin{smallmatrix} \pm 1 & \\ & \pm 1 \end{smallmatrix}\right)\right\}$ with $\mathrm{GL}_2(\mathbb{Z})$.

In our case, the full automorphism group fairly manageable.

Proposition 1.144. Suppose G is centreless and H is abelian. Then

$$\mathrm{Aut}(G \times H) \cong (\mathrm{Aut}(G) \times \mathrm{Aut}(H)) \ltimes \mathrm{Hom}(G, H).$$

Remark 1.145. We need H abelian to have a *group* $\mathrm{Hom}(G, H)$. For arbitrary G and H, there is a subgroup of $\mathrm{Aut}(G \times H)$ consisting of those automorphisms

$$\left\{ \begin{pmatrix} \theta_G & \chi_H \\ \chi_G & \theta_H \end{pmatrix} \in \mathrm{Aut}(G \times H) \;\middle|\; \substack{\theta_G \in \mathrm{Aut}(G),\ \theta_H \in \mathrm{Aut}(H), \\ \chi_G \in \mathrm{Hom}(G, Z(H)),\ \chi_H \in \mathrm{Hom}(H, Z(G))} \right\}.$$

Note that for some choice of $\theta_G, \theta_H, \chi_G, \chi_H$ we get a homomorphism that is *not* an automorphism (e.g. $\left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right) \in \mathrm{End}(\mathbb{Z} \times \mathbb{Z})$.)

PROOF. Let $\theta \in \mathrm{Aut}(G \times H)$ and let i_G, i_H, ϕ_G, ϕ_H be the natural inclusions and projections

$$G \overset{i_G}{\hookrightarrow} G \times H \overset{\phi_G}{\twoheadrightarrow} G$$

$$H \overset{i_H}{\hookrightarrow} G \times H \overset{\phi_H}{\twoheadrightarrow} H.$$

Since $1 \times H$ is central in $G \times H$, so is $\theta(1 \times H)$ and thus $(\pi_G \circ \theta)(1 \times H) = 1$ as G is centreless. Thus

$$(\pi_G \circ \theta)(g, h) = (\pi_G \circ \theta)(g, 1) \cdot (\pi_G \circ \theta)(1, h) = (\pi_G \circ \theta)(g, 1)$$

is independent of h so we have a well-defined homomorphism

$$\mathrm{Aut}(G \times H) \to \mathrm{Aut}(G) \colon \psi \mapsto \pi_G \circ \psi \circ i_G.$$

Since $\theta(1 \times H) \leq 1 \times H$ we similarly get a homomorphism

$$\mathrm{Aut}(G \times H) \to \mathrm{Aut}(H) \colon \psi \mapsto \pi_H \circ \psi \circ i_H.$$

Let $\theta_G = \pi_G \, \theta \, i_G \in \mathrm{Aut}(G)$, $\theta_H = \pi_H \, \theta \, i_H \in \mathrm{Aut}(H)$, and let $\chi = \theta_H^{-1} \, \pi_H \, \theta \, i_G \in \mathrm{Hom}(G, H)$ (where the final θ_H^{-1} is introduced for convenience, as will become apparent soon). Since $\pi_G \, \theta \, i_H = 1$, we have for all $g \in G, h \in H$ that

$$\begin{aligned} \theta(g, h) &= \theta(g, 1) \cdot \theta(1, h) \\ &= (\theta_G(g), \theta_H \chi(g)) \cdot (1, \theta_H(h)) \\ &= (\theta_G(g), \theta_H(\chi(g) h)). \end{aligned}$$

Now if $\theta' \in \mathrm{Aut}(G \times H)$ with $\theta'_G, \theta'_H, \chi'$ defined similarly, we compute

$$\begin{aligned}(\theta'\theta)(g,h) &= (\theta'_G(\theta_G(g)), \theta'_H\left(\chi'(\theta_G(g))\theta_H(\chi(g)h)\right)) \\ &= (\theta'_G\theta_G(g), \theta'_H\theta_H\left(\theta_H^{-1}\chi'\theta_G(g)\chi(g)h\right)) \\ &= (\theta'_G\theta_G(g), \theta'_H\theta_H\left((\chi'^{(\theta_G,\theta_H)}\chi)(g)h\right))\end{aligned}$$

where we define the action

$$\chi'^{(\theta_G,\theta_H)} = \theta_H^{-1}\chi'\theta_G.$$

Thus we have an isomorphism

$$\mathrm{Aut}(G \times H) \xrightarrow{\cong} (\mathrm{Aut}(G) \times \mathrm{Aut}(H)) \ltimes \mathrm{Hom}(G, H).$$

□

Corollary 1.146. *The trivial-unit-preserving ring automorphisms of $K[P]$ are the maps of the form*

$$\sum a_g \cdot g \mapsto \sum \tau(\chi(g)a_g) \cdot \phi(g)$$

for $\phi \in \mathrm{Aut}(P)$, $\tau \in \mathrm{Aut}(K)$, $\chi \in \mathrm{Hom}(P, K^\times)$.

Proof. First note that these are automorphisms of the group of trivial units that extend to automorphisms of $K[P]$. P is centreless as every $g \in P$ has $g^2 \in A = \langle x, y, z\rangle$, a normal $\mathbb{Z}^3$ subgroup on which the generators a, b acts as $\begin{pmatrix} 1 & & \\ & -1 & \\ & & -1 \end{pmatrix}$ and $\begin{pmatrix} -1 & & \\ & 1 & \\ & & -1 \end{pmatrix}$ respectively. The group of trivial units is isomorphic to $P \times K^\times$, with $K^\times$ abelian, so Proposition 1.144 applies. Note that $K^\times$ has many more automorphisms as a group than we get by restricting field automorphisms, but a ring automorphism of $K[P]$ that preserves $K^\times$ thus preserves K, on which it acts as a ring (equivalently, field) automorphism. □

Remark 1.147. A character $\chi \in \mathrm{Hom}(P, K^\times)$ is the same thing as a 1-dimensional representation $P \to \mathrm{GL}_1(K)$. A representation of P is a $K[P]$-module. If we twist this module by precomposing with the automorphism of $K[P]$ associated to χ, this has the effect of tensoring with the 1-dimensional representation. One could call such χ a "gauge automorphism".

Theorem 1.148 ([**Gar21**]). *There exists $\alpha \in (\mathbb{F}_2[P])^\times$ with $|\mathrm{supp}(\alpha)| = 21$.*

That is, the Kaplansky unit conjecture is false.

Corollary 1.149 ([**Gar21**]). *$(\mathbb{F}_2[P])^\times$ contains free subgroups and is not finitely generated.*

The construction of a non-trivial unit over $\mathbb{F}_2$ was generalized by Murray [**Mur21**] to a unit $\alpha_d \in \mathbb{F}_d[P]$ for arbitrary prime d, with $|\mathrm{supp}\,\alpha_d| \to \infty$ as $d \to \infty$.

The unit α exhibits symmetry that was expressed in [**Gar21**] in terms of cosets of $N = \langle x, y, z\rangle$. This was explained coherently by Bartholdi, who observed

Theorem 1.150 ([**Bar23**]). *There exist non-trivial automorphisms $\theta_0, \theta_1 \in \mathrm{Aut}(K[P])$ such that $\theta_0(\alpha_d) = \alpha_d$ and $\theta_1(\alpha_d)^* = \alpha_d^{-1}$.*

That is, the units are θ_1-unitary.

Remark 1.151. It is unclear whether allowing the field automorphism is helpful.

Remark 1.152. If $\alpha \in K[G]$ is θ-unitary, then $\alpha\theta(\alpha)^* = 1$ gives $\theta(\alpha)\theta^2(\alpha)^* = 1$ and thus $(\theta^2(\alpha)^*)^*\theta(\alpha)^* = 1^* = 1$ so that $\theta^2(\alpha)\theta(\alpha)^* = 1$ and by uniqueness of inverses $\theta^2(\alpha) = \alpha$. Thus θ acts as a permutation on $\operatorname{supp}(\alpha)$ and will induce a finite order automorphism of $\langle \operatorname{supp}(\alpha)\rangle$ (which is typically all of G). In Bartholdi's theorem, $\theta_1^2 = 1$ but in general θ^2 can be non-trivial!

Bartholdi's explanation of the units first requires translation, i.e. multiplication of units by group elements (specifically $\alpha \mapsto \alpha b^{-1}a^{-1}$). We can simplify his explanation further if we apply a further group automorphism (namely $a \mapsto a, b \mapsto a^{-2}b$) which has the effect of conjugating θ_0, θ_1 in $\operatorname{Aut}(K[P])$. Then we arrive at:

Proposition 1.153. Let $\chi\colon P \to K^\times : a \mapsto -1, b \mapsto -1$. Then we can take

$$\theta_0 = (\phi_0, 1), \theta_1 = (\phi_1, \chi) \in \operatorname{Aut}(P) \ltimes \operatorname{Hom}(P, K^\times)$$

where

$$\begin{aligned}\phi_0 &\colon a \mapsto a^{-1}, b \mapsto b^{-1}\\ \phi_1 &\colon a \mapsto a, b \mapsto b^{-1}\end{aligned}$$

in Theorem 1.150.

As observed in [**Gar21**, Lemma 1] in very different terms, this gives "2 out of 4 cosets" for free.

Lemma 1.154 ("2 out of 4 cosets")**.** *If $\alpha \in K[P]$ satisfies $\phi_0(\alpha) = \alpha$, then*

$$(\alpha \cdot \theta_1(\alpha)^*)_g = 0$$

for all $g \in Na, Nb$, where $\mathbb{Z}^3 \cong N = \langle x, y, z\rangle \lhd P$.

Proof. Let $\alpha = \sum a_g \cdot g$, so $\theta_1(\alpha)^* = \sum \chi(g)a_g \cdot \phi_1(g)^{-1}$. Let $k \in Nb$. Then

$$(\alpha \cdot \theta_1(\alpha)^*)\, k = \sum_{\substack{g,h \text{ s.t.}\\ g\phi_1(h)^{-1} = k}} a_g \chi(h) a_h.$$

But $\phi_1(k) = k^{-1}$, so $g\phi_1(h)^{-1} = k$ implies $\phi_1(g)\phi_1^2(h)^{-1} = \phi_1(k) = k^{-1}$ and so $h\phi_1(g) = k$ too. Since $g\phi_1(h) \in Nb$ and ϕ_1 acts trivially on P/N, $gh \in Nb$ and in particular $g \neq h$. As $P/N \cong \mathbb{Z}/2 \oplus \mathbb{Z}/2$, we also have $gh^{-1} \in Nb$, so now

$$\begin{aligned}(\alpha \cdot \theta_1(\alpha)^*)_k &= \sum_{\substack{\{g,h\} \text{ s.t.}\\ g\phi_1(h)^{-1} = k}} a_g a_h (\chi(g) + \chi(h))\\ &= \sum a_g a_h \chi(h^{-1})(\chi(gh^{-1}) + 1)\\ &= 0\end{aligned}$$

as $gh^{-1} \in Nb$ implies $\chi(gh^{-1}) = \chi(b) = -1$.

Since $\theta_0(\alpha) = \alpha$, we have for $k \in Na$ that

$$(\alpha \cdot \theta_1(\alpha)^*)_k = (\alpha \cdot (\theta_1\theta_0(\alpha))^*)_k = 0$$

similarly as $\phi_1\phi_0 \colon a \mapsto a^{-1}, b \mapsto b$. □

Remark 1.155. The first non-trivial unit in $\mathbb{F}_2[P]$ was found by reformulating the quadratic system of equations one has for given finite candidate support sets (on 147 elements) as a problem in boolean satisfiability (a.k.a. SAT). Note that $2^{147} \sim 10^{44}$! SAT is the original NP-complete problem. It is the problem of deciding, given a propositional (so quantifier-free) Boolean formula, whether it can be made true (*satisfied*) for some assignment of its variables to `false` and `true`. Generally, the input is assumed to be in conjunctive normal form, something like

$$(\neg x \vee \neg y \vee \neg z) \wedge (\neg x \vee y \vee z) \wedge (x \vee \neg y \vee z) \wedge (x \vee y \vee \neg z)$$

which asserts that $x + y + z = 0$ in $\mathbb{F}_2$ (making the natural identification of `false` with 0 and `true` with 1).

1.7. Units of the infinite dihedral group

We won't prove Corollary 1.149 as it is mostly a computation using (variants on) the unit from Theorem 1.148. It does however have one essential ingredient that is of independent interest: the computation of the entire group of units of $\mathbb{F}_2[D_\infty]$, due to Mirowicz [**Mir91**]. A map $P \to D_\infty$ induces a map $(\mathbb{F}_2[P])^\times \to (\mathbb{F}_2[D_\infty])^\times$ and understanding $(\mathbb{F}_2[D_\infty])^\times$ completely (in particular, knowing its abelianization) allows us to deduce that $(\mathbb{F}_2[P])^\times$ is not finitely generated without even knowing all the units of $\mathbb{F}_2[P]$ (or whether they surject onto the units of $\mathbb{F}_2[D_\infty]$, for that matter).

Characterizing units in $\mathbb{F}_2[D_\infty]$. Recall that $D_\infty = \langle\, t, r \mid r^2 = 1, t^r = t^{-1}\,\rangle$ and $\langle t\rangle \cong \mathbb{Z}$ is an index 2 subgroup. By the standard trick 1.62, we can embed $\mathbb{F}_2[D_\infty] \hookrightarrow M_2(\mathbb{F}_2[\mathbb{Z}])$. Every $\alpha \in \mathbb{F}_2[D_\infty]$ is uniquely expressible as $a + br$ for $a, b \in \mathbb{F}_2[\mathbb{Z}]$. Let $*\colon \mathbb{F}_2[\mathbb{Z}] \to \mathbb{F}_2[\mathbb{Z}]$ denote the involution induced by the action of r: $t^* = t^{-1}$. Then the embedding is

$$a + br \mapsto \begin{pmatrix} a & b \\ b^* & a^* \end{pmatrix}.$$

Since we now are working with matrices over a commutative ring, we can check invertibility by whether or not the determinant is a unit. Since $\mathbb{F}_2[\mathbb{Z}]$ has no non-trivial units, this means the determinant must be some $t^k \in \mathbb{Z}$. However, the inverse matrix

$$t^{-k}\begin{pmatrix} a^* & b \\ b^* & a \end{pmatrix}$$

will be in the image of $\mathbb{F}_2[D_\infty]$ if and only if $k = 0$. Thus:

Lemma 1.156. *The element $\alpha = a + br \in \mathbb{F}_2[D_\infty]$ is a unit if and only if* $\det\alpha = aa^* - bb^* = 1$. □

Example 1.157. The embedding sends

$$t^{-1} + t + (1 + t + t^2)r \mapsto \begin{pmatrix} t^{-1} + t & 1 + t + t^2 \\ 1 + t^{-1} + t^{-2} & t + t^{-1} \end{pmatrix}$$

which has determinant

$$(t^{-1} + t)^2 - (1 + t + t^2)(t^{-2} + t^{-1} + 1) = t^{-2} + 2 + t^2 + t^{-2} + 2t^{-1} + 3 + 2t + t^2 = 1$$

so it is a unit. For general invertible 2×2 matrices over commutative rings,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

so since we're in characteristic 2 with $a = d$ and $\det = 1$, we see that this units is its own inverse.

For $a \in \mathbb{F}_2[\mathbb{Z}]$ define

$$\begin{aligned}\max a &:= \max \operatorname{supp} a\\ \min a &:= \min \operatorname{supp} a\\ \deg a &:= \max a - \min a = \max aa^*\end{aligned}$$

(with $\max(0) = -\infty, \min(0) = \infty, \deg(0) = -\infty$). The trivial units are precisely those $a + br$ for which one of a and b is 0 and the other has degree 0 (that is, is some t^k). If one of a and b is 0, this is moreover the only way to satisfy $\det \alpha = 1$. So every non-trivial unit has $a \neq 0$ and $b \neq 0$. Suppose $a + br$ is a non-trivial unit. If $\deg a = 0$, then $aa^* = t^0 = 1$ so we get $bb^* = 0$ which forces $b = 0$, contradicting non-triviality. Thus our non-trivial unit $a + br$ has

$$\deg(\alpha) := \deg a = \max aa^* = \max bb^* = \deg b \geq 1.$$

We define the degree of a trivial unit (where $\{\deg(a), \deg(b)\} = \{-\infty, 0\}$) to be 0.

Generators for a group of non-trivial units. We now introduce our generators for $(\mathbb{F}_2[D_\infty])^\times$. For $i \in \mathbb{N}^+$ and $j \in \mathbb{Z}$ define

$$\begin{aligned}n_{ij} &:= t^{-i} + t^i + t^j(t^{-i} + t^i)r\\ e_{ij} &:= t^{-i} + 1 + t^i + t^j(t^{-i} + t^i)r = 1 + n_{ij}.\end{aligned}$$

In general $(a + br)^2 = a^2 + bb^* + (ab + ba^*)r$, so when $a^* = a$ this cancels to $a^2 + bb^*$. So $(1 + t^j r)^2 = 1 + t^j t^{-j} = 0$. Note that $(t^{-i} + t^i)^* = t^{-i} + t^i$, so that $[1 + t^j r, t^{-i} + t^i] = 0$. Thus

$$\begin{aligned}n_{ij} n_{i'j} &= (t^{-i} + t^i)(1 + t^j r)(t^{-i'} + t^{i'})(1 + t^j r)\\ &= (t^{-i} + t^i)(t^{-i'} + t^{i'})(1 + t^j r)^2\\ &= 0.\end{aligned}$$

In particular, $n_{ij}^2 = 0$ so that $e_{ij}^2 = 1$.

Infinite elementary abelian 2-groups. Let us define subgroups (for $j \in \mathbb{Z}$)

$$\begin{aligned}U_j &:= \langle e_{ij} \colon i \in \mathbb{N}^+ \rangle\\ U &:= \langle U_j \colon j \in \mathbb{Z} \rangle.\end{aligned}$$

As $n_{ij} n_{i'j} = 0$, we have that

$$\begin{aligned}\bigoplus_{i \in \mathbb{N}^+} \mathbb{Z}/2 &\to U_j\\ \sum_{i \in I} 1_i &\mapsto 1 + \sum_{i \in I} n_{ij}\end{aligned}$$

is an isomorphism, as

$$(1 + \sum_{i \in I} n_{ij})(1 + \sum_{i' \in I'} n_{i'j}) = 1 + \sum_{i \in I} n_{ij} + \sum_{i' \in I'} n_{i'j} + 0.$$

The free product. Our next claim is that the natural map

$$\bigstar_{j\in\mathbb{Z}} U_j \to U$$

is an isomorphism.

We reformulate Mirowicz's argument as ping pong. The ping pong lemma is the standard way to prove that a group is a free product. We recall a statement of it here but will not prove it.

Lemma 1.158 (Ping pong lemma). *Let G act on a set X and let $G_i \leq G$ be subgroups, $i \in I$, at least one of which contains more than 2 elements, and let $X_i \subset X$ be disjoint subsets. Suppose that for all distinct $i, j \in I$ and all $g \in G \setminus \{1\}$ we have $g \cdot X_j \subseteq X_i$. Then $G = *_{i\in I} G_i$.*

Remark 1.159. The condition that some G_i has more than 2 elements is necessary: consider $G = G_1 \times G_2$ where both G_1 and G_2 are order 2 and act non-trivially (in the only way possible) on $X = \{1, 2\}$ with $X_1 = \{1\}, X_2 = \{2\}$.

Example 1.160. The standard example of an application of the ping pong lemma is to show that

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}$$

generate a free subgroup of $\mathrm{SL}_2(\mathbb{R})$ whenever $x \geq 2$. Here $G \curvearrowright \mathbb{R}^2$ in the natural way, G_1, G_2 are the respective cyclic subgroups and

$$X_1 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 \,\middle|\, |x| > |y| \right\}, \quad X_2 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 \,\middle|\, |y| > |x| \right\}.$$

Lemma 1.161. *Let $X = U$ and define disjoint X_j, $j \in \mathbb{Z}$, by*

$$X_j = \{ar + b \in X : \min(a) + j = \min(b)\}.$$

Then the action of U (with subgroups U_j, $j \in \mathbb{Z}$) on X by right multiplication satisfies the assumptions of the ping pong lemma, so $U = *_{j\in\mathbb{Z}} U_j$. Moreover $U = \{1\} \sqcup \bigsqcup_{j\in\mathbb{Z}} X_j$ so that all $g \in U \setminus \{1\}$ are non-trivial units.

Proof. Let $a + br \in X_i$, $i \neq j$, so that $\min(b) - \min(a) \neq j$ (and both $\min(a), \min(b)$ are finite). Consider $g \in U_j \setminus \{1\}$. We are required to prove that

$$(c + dr) := (a + br)g$$

lies in X_j.

From the proof that $U_j \cong \oplus_{\mathbb{N}^+} \mathbb{Z}/2$ and the definition of n_{ij} we see that $g = 1 + p(1 + t^j r)$ for some non-zero $p \in \mathbb{F}_2[\mathbb{Z}]$ with $p = p^* = \sum_{i\in I}(t^{-i} + t^i)$. Set $n = \max p > 0$ (so we can write $p = t^{-n} + \cdots + t^n$). Thus

$$c = a(1 + p) + b(pt^{-j})$$

and since $\min(a(1 + p)) = \min(a) - n$ and $\min(b(pt^{-j})) = \min(b) - n - j$, which are distinct by assumption (that $a + br \notin X_j$), we have

$$\min(c) = \min(\min(a), \min(b) - j) - n.$$

Likewise

$$d = apt^j + b(1 + p)$$

so that

$$\min(d) = \min(\min(a) - n + j, \min(b) - n)$$

and hence $\min(c) + j = \min(d)$ so that $c + dr \in X_j$.

Finally, note that if $g_j \in U_j \setminus \{1\}$ then $1 \cdot g_j \in X_j$ so by writing any non-trivial element of U in normal form $g_{j_1} g_{j_2} \dots g_{j_k}$ we see it lies in X_{j_k} and thus is of the form $a + br$ where both $a \neq 0$ and $b \neq 0$. □

The semidirect product decomposition. We abuse notation slightly and write D_∞ for the subgroup of trivial units. We claim that $\langle U, D_\infty \rangle$ is naturally a semidirect product $U \rtimes D_\infty$. Since we proved above that $U \cap D_\infty = 1$, it only remains to show that the generators t and r of D_∞ normalize U.

$$\begin{aligned} t^{-1} e_{i,j} t &= t^{-i} + 1 + t^i + t^{j-1}(t^{-i} + t^i) r t \\ &= t^{-i} + 1 + t^i + t^{j-2}(t^{-i} + t^i) r \\ &= e_{i,j-2} \\ r^{-1} e_{i,j} r &= t^i + 1 + t^{-i} + t^{-j}(t^i + t^{-i}) r \\ &= e_{i,-j} \end{aligned}$$

So D_∞ simply permutes the free factors U_j $(j \in \mathbb{Z})$ of U according to a natural action of D_∞ on $\mathbb{Z}$ with two orbits, namely evens and odds. (This action is generated by reflection in 0 and 1. Another natural choice of action of D_∞ on $\mathbb{Z}$ would be generated by reflection in 0 and $\frac{1}{2}$ and thus have only one orbit.) In other words, we have what has been referred to in the literature as a graph wreath product

$$(\oplus_{\mathbb{N}^+} \mathbb{Z}/2) \wr D_\infty$$

where $\mathbb{Z}$ is a discrete graph, hence the "graph product" is just a free product.

Proving all units are accounted for.

Lemma 1.162. *Let $\alpha \in (\mathbb{F}_2[D_\infty])^\times$ be non-trivial. Then there exist $i \in \mathbb{N}^+, j \in \mathbb{Z}$ such that*

$$\deg(\alpha e_{ij}) < \deg(\alpha).$$

This immediately implies that $(\mathbb{F}_2[D_\infty])^\times = \langle U, D_\infty \rangle = U \rtimes D_\infty$.

Proof. Let $\alpha = a + br$. As one might guess after studying the proof of Lemma 1.161, we set $j := \min(b) - \min(a)$.

For $c + dr := (a + br) e_{ij}$ we have

$$c = a + (t^{-i} + t^i)(a + t^{-j} b).$$

Our choice of j ensures cancellation at both ends (min and max) in computing $a + t^{-j} b$. We now choose our i to be the minimal amount we move inside after such cancellation, so that when we extend by i in both directions (by multiplying by $t^{-i} + t^i$) we get something that will again cancel with a. That is, we set

$$i := \min\left(\min(a + t^{-j} b) - \min(a), \max(a) - \max(a + t^{-j} b)\right).$$

Then

$$\begin{aligned} \min\left((t^{-i} + t^i)(a + t^{-j} b)\right) &\geq \min(a) \\ \max\left((t^{-i} + t^i)(a + t^{-j} b)\right) &\leq \max(a) \end{aligned}$$

with at least one being an equality, and thus $\min(c) \geq \min(a)$ and $\max(c) \leq \max(a)$ with at least one inequality being strict, so $\deg(c) < \deg(a)$ as claimed. (NB: it is possible that $\deg(c) = 0$ or $c = 0$, in which case we know that $(a + br) e_{ij}$ is a trivial unit.) □

1.8. The unit conjecture is not a ring theoretic statement

We now make precise (in a way) the observation that the unit conjecture is a "group ring theoretic" statement and not simply a ring theoretic statement about a group ring, as the other 3 Kaplansky conjectures are.

If the trivial units were a definable subset of the ring $K[G]$ (in the sense of model theory) then they would necessarily be invariant under all ring automorphisms, including conjugation by non-trivial units (if any exist). This cannot be the case for non-exotic groups, at least. Let's introduce the exotic groups in question.

Definition 1.163. A group V is called an *Adian extension* if it is finitely generated and torsion-free and $V/Z(V)$ is an infinite group of finite exponent.

This means there exists a positive integer n such that $g^n = 1$ for all $g \in V/Z(V)$.

Remark 1.164. The famous Burnside problem (1902) asks whether a finitely generated group of finite exponent must be finite. Novikov–Adian (1968) gave the first counterexample. Adian (1971) went one step further and constructed the first Adian extension. A group containing an Adian extension can certainly be considered "exotic".

Example 1.165. There are no solvable infinite "Burnside groups": we can prove by induction on the derived length that a finitely generated solvable group G of finite exponent is finite. Indeed, the base case of derived length 0 is the trivial group. For the inductive step, note that the abelianization of G is finite (e.g. by the classification of finitely generated abelian groups, or argue directly) and the derived subgroup, being finite index in a finitely generated group, is itself finitely generated. Since solvability passes to quotients, this immediately implies that there are no solvable Adian extensions. In particular, the following proposition applies whenever G is solvable.

Proposition 1.166. Let G be torsion-free. Suppose that no subgroup of G is an Adian extension. Let $T \leq (K[G])^\times$ denote the subgroup of trivial units. Then T is self-normalizing i.e. $N_{(K[G])^\times}(T) = T$.

In other words, if u is *any* non-trivial unit then $T^u \neq T$. (To show T is not a definable subset of $K[G]$ we only need one such u.)

Proof of Proposition 1.166. Suppose for the sake of contradiction that u is a non-trivial unit of $K[G]$ with $T^u = T$. Let $S = \operatorname{supp}(u)$. Since tu will also normalize T for any $t \in T$, we can assume without loss of generality that $1 \in S$. Let $n = |S|!$.

Let $g \in G$ be a trivial unit. Let $h := u^{-1}gu \in T$. Considering the augmentation map, we see that $h \in G$. We change perspective and write the previous equation as $g^{-1}uh = u$. The map $G \to G\colon x \mapsto g^{-1}xh$ permutes the elements of S and thus $x \mapsto g^{-n}xh^n$ fixes S pointwise. As $1 \in S$, this means that $g^n = h^n$ and the aforementioned map is actually the inner automorphism $x \mapsto g^{-n}xg^n$, so $g^n \in C_G(V)$ where $V = \langle S \rangle$. This holds in particular for $g \in V$ so that the finitely generated group V has the property that $V/Z(V)$ has exponent (dividing) n. By assumption V cannot be an Adian extension, so $V/Z(V)$ is finite. By Schur's Lemma 1.65, this implies V' is finite and hence trivial by torsion-freeness. Thus V is a torsion-free abelian group supporting the non-trivial unit u, a contradiction. □

1.9. Bi-orderable groups

We will prove that if G is bi-orderable, then $K[G]$ embeds into a skew field. This is much stronger than satisfying the zero divisor conjecture.

Lemma 1.167. *$\mathcal{P} \subset G$ is the positive cone of a bi-ordering if and only if*

(1) $\mathcal{P}^2 \subseteq \mathcal{P}$ *(that is, it is a subsemigroup)*
(2) $G = \mathcal{P} \sqcup \{1\} \sqcup \mathcal{P}^{-1}$.
(3) $\mathcal{P}^g = \mathcal{P}$ *for all* $g \in G$ *(that is, it is a normal subset)*

Proof. Exercise. □

Example 1.168. Torsion-free abelian groups are left-orderable (assuming the axiom of choice) and thus bi-orderable.

Example 1.169. Free groups are bi-orderable.

We will not prove this but it follows from F_n being residually torsion-free nilpotent.

Lemma 1.170. *A bi-orderable group has unique roots. That is, if $n \in \mathbb{Z}^+$ and $g, h \in G$ such that $g^n = h^n$, then $g = h$.*

Proof. If $g \neq h$ then without loss of generality $g < h$ and thus

$$g^n = g^{n-1}g < g^{n-1}h < g^{n-2}h^2 < \cdots < h^n.$$

□

Example 1.171. We can present the fundamental group $\mathbb{Z} \rtimes \mathbb{Z}$ of the Klein bottle as $\langle\, a, b \mid a^2 = b^2 \,\rangle$ which clearly fails to have unique roots.

Proposition 1.172. Torsion-free nilpotent groups are bi-orderable.

Example 1.173.

$$\left\{ \begin{pmatrix} 1 & x & z \\ & 1 & y \\ & & 1 \end{pmatrix} \middle| \, x, y, z \in \mathbb{Z} \right\}$$

is the (integral) Heisenberg group. It is the free 2-generated class-2 nilpotent group.

Lemma 1.174. *Suppose $N \lhd G$ such that N and G/N are bi-orderable, where N admits a bi-ordering whose positive cone is a normal subset of G. Then G is bi-orderable.*

Proof. Exercise. □

Lemma 1.174 lets us prove inductively that torsion-free nilpotent groups are bi-orderable: if G is class-c nilpotent then $G/Z(G)$ is class-$(c-1)$ nilpotent. We just need to ensure $G/Z(G)$ is also torsion-free, that is, that for $n \in \mathbb{Z}^+$ and $g \in G$ we have

$$([g^n, h] = 1 \quad \forall h \in G) \implies ([g, h] = 1 \quad \forall h \in G).$$

It suffices to show for all $n \in \mathbb{Z}^+$ and $g, h \in G$ that

$$g^n = (h^{-1}gh)^n \implies g = h^{-1}gh.$$

In other words, the whole question of bi-orderability for torsion-free nilpotent groups boils down to uniqueness of roots!

Lemma 1.175. *Suppose $Z(G)$ is torsion-free. Then $Z(G/Z(G))$ is torsion-free.*

PROOF. Suppose $\overline{g} \in Z(G/Z(G))$ satisfies $\overline{g}^n = 1$ for some $n \in \mathbb{Z}^+$. That is, for $g \in G$ with $\overline{g} = gZ(G)$ we have $g^n \in Z(G)$ and $[g,h] \in Z(G)$ for all $h \in G$. The identity $[xy,z] = [x,z]^y[y,z]$ implies the identity

$$[x^n,y] = [x,y]^{x^{n-1}}[x,y]^{x^{n-2}} \dots [x,y]^x[x,y].$$

In our case, for arbitrary $h \in G$ we have $[g,h] \in Z(G)$ and thus $[g^n,h] = [g,h]^n$. But $g^n \in Z(G)$ so $[g^n,h] = 1$ and $[g,h] \in Z(G)$ which is torsion-free. Thus $[g,h] = 1$. As h was arbitrary, this means $g \in Z(G)$, that is, $\overline{g} = 1$. □

Corollary 1.176. *Let G be torsion-free nilpotent. Then $G/Z(G)$ is also torsion-free.*

Remark 1.177. We see that for nilpotent G, if $Z(G)$ is torsion-free then G is torsion-free.

PROOF OF COROLLARY 1.176. The upper central series is

$$1 = Z_0 \lhd Z_1 \lhd \dots \lhd Z_c = G$$

(where G is class-c nilpotent) defined by $Z_{i+1}/Z_i = Z(G/Z_i)$. Repeated application of Lemma 1.175 (to $G, G/Z_1, G/Z_2, \dots$) shows that all quotients Z_{i+1}/Z_i are torsion-free. As extensions of torsion-free groups are torsion-free, the result follows. □

PROOF OF PROPOSITION 1.172. Induct on nilpotency class, noting that a central subset is normal (so that Lemma 1.174 applies) and torsion-free abelian groups are bi-orderable. □

Bi-orderability is the strongest property we've seen that implies the Kaplansky conjectures:

Proposition 1.178. Bi-orderable groups are locally indicable.

We will prove Proposition 1.178 mostly in exercises. As bi-orderability passes to subgroups, it is equivalent to showing that a finitely generated bi-orderable group has infinite abelianization.

Definition 1.179. Let G be an ordered group. A subgroup $H < G$ is called *convex* if for $a, b \in H$ and $g \in G$ we have $a < g < h$ implies $g \in H$.

Definition 1.180. Let G be an ordered group. Then G is called *Archimedean* if for all $g, h > 1$ there exists $n \in \mathbb{Z}^+$ such that $g^n > h$.

Proposition 1.181. Let G be an Archimedean bi-ordered group. Then G is abelian.

Remark 1.182. In fact, an Archimedean left-ordered group is automatically bi-ordered and moreover isomorphic to a subgroup of $\mathbb{R}$ (a theorem of Hölder).

PROOF. Note that if $g, t > 1$ then there exists $n \in \mathbb{N}$ such that $t^n \leq g < t^{n+1}$. Suppose G has a least positive element t. Then $t^n \leq g < t^{n+1}$ implies $1 \leq t^{-n}g < t$ so that $t^{-n}g = 1$, that is, any positive element is a power of t, so $G = \langle t \rangle \cong \mathbb{Z}$ is abelian. So we now assume there is no least positive element.

Let $x, y \in G$. We will show $[x,y] = 1$. We can assume without loss of generality that $x > 1$ and $y > 1$ and since $[y,x] = [x,y]^{-1}$ we can also assume $[x,y] \geq 1$. Given any $t > 1$ we find integers m, n such that $t^m \leq x < t^{m+1}$ and $t^n \leq y < t^{n+1}$ and thus $x^{-1} \leq t^{-m}$ and $y^{-1} \leq t^{-n}$ so that $[x,y] < t^{-m}t^{-n}t^{m+1}t^{n+1} = t^2$. We now just need to show that if $g > 1$ then there exists $t > 1$ such that $t^2 \leq g$ as this will force $[x, y] = 1$.

Let $g > 1$ and take some $1 < s < g$. If $s^2 \leq g$ then we take $t = s$. Otherwise $s < g < s^2$ and $g < s^2$ implies $(s^{-1}g)^2 = s^{-1} \cdot g \cdot (s^{-1}g) < s^{-1} \cdot s^2 \cdot (s^{-1}g) = g$ whereas $s < g$ implies $1 < s^{-1}g$ so that $t = s^{-1}g$ works. □

Exercise 1.9.1. In this exercise we prove Proposition 1.178. Let G be a bi-ordered group.

(1) Let $g_0 > 1$. Show that
$$N_{g_0} := \{g \in G \,|\, g^n < g_0 \quad \forall n \in \mathbb{Z}\}$$
is a subgroup of G.
(2) Suppose $G = \langle S \rangle$ and $g_0 = \max(S^{\pm 1})$. (Note that if S is infinite, the maximum may not exist.) Show that $N_{g_0} \lhd G$. (Hint: let $g \in N_{g_0}$ and write arbitrary $h \in G$ as a product of $|h|$ elements of $S^{\pm 1}$. Then show $g_0 < (hg_0h^{-1})^{2|h|+1}$ so that $g^{n(2|h|+1)} < g_0$ implies $(h^{-1}gh)^n < g_0$.)
(3) Show that N_{g_0} is convex.
(4) Show that there is a natural bi-ordering on the quotient of a bi-ordered group by a convex normal subgroup.
(5) Show that the bi-ordering on G/N_{g_0} thus constructed is Archimedean.
(6) Conclude that a finitely generated bi-orderable group has infinite abelianization.

A stronger conjecture than the zero divisor conjecture is:

Conjecture 1.183. Let K be a field a G be a torsion-free group. Then $K[G]$ embeds into a skew field (a.k.a. division ring).

Suppose $K[G]$ satisfies the zero divisor conjecture. We could attain a skew field by localization provided $K[G]$ satisfies the Ore condition: for all $a, b \in K[G]$ with $b \neq 0$ there exist $x, y \neq 0$ such that $xa = yb$. However, we'll see later that this holds if and only if G is amenable!

As a motivating example, an alternative way to embed $K[\mathbb{Z}]$ into a field is to take the formal Laurent series. Then supports can be infinite but are sufficiently well controlled that multiplication can be defined. This generalizes to:

Theorem 1.184 (Malcev, Neumann). *Let G be a bi-ordered group. Let D denote the formal sums $\sum_{g \in G} a_g \cdot g$, where $a_g \in K$, with well-ordered support. Then D is a skew field containing $K[G]$.*

Definition 1.185. A set X is *well-ordered* if every non-empty subset of X contains a least element.

Every subset of a well-ordered set is well-ordered.

Lemma 1.186. *Let G be a bi-ordered group, $g \in G$ and $A, B \subseteq G$ well-ordered subsets. Then*

(i) *$S = \{(a, b) \in A \times B \,|\, ab = g\}$ is finite.*
(ii) *$A \cup B$ and AB are well-ordered.*

Proof. (i) If S were infinite, we could construct an infinite ascending sequence in the projection $S_A = \pi_A(S) \subseteq A$ by defining $a_0 = \min(S_A)$ and $a_{i+1} =$

$\min\{a \in S_A \mid a > a_i\}$. Then $b_i := a_i^{-1}g$ defines an infinite descending sequence in B, a contradiction.

(i) If $\emptyset \neq S \subseteq A \cup B$ then $\min(S) = \min(\min(S \cap A), \min(S \cap B))$.

If AB is not well-ordered, then we can construct an infinite descending sequence $a_1b_1 > a_2b_2 > \dots$ with $a_i \in A, b_i \in B$. Since A is well-ordered we can construct an infinite non-decreasing subsequence (a_{n_j}) by setting n_0 such that $a_{n_0} = \min\{a_i\}$ and then setting n_{j+1} such that $a_{n_{j+1}} = \min\{a_i \mid i > n_j\}$. Then (b_{n_j}) is strictly decreasing, a contradiction. □

Proof of Theorem 1.184. We define addition and multiplication on D in the same way as for $K[G]$. Multiplication is well-defined by Lemma 1.186 part (i). Moreover, the resulting formal sums have well-ordered support by part (ii). This makes D into a ring - the ring axioms hold for the same reasons as in $K[G]$.

We only need to check that non-zero elements are invertible. If $\beta \neq 0$ then letting $x = \min(\operatorname{supp}(\beta))$, we have $x^{-1}\operatorname{supp}(\beta) \subseteq \{1\} \cup \mathcal{P}$, where $\mathcal{P}$ is the positive cone of G, so we can write $\beta = (\beta)_x x(1-\alpha)$ where $A = \operatorname{supp}(\alpha) \subseteq \mathcal{P}$. As $(\beta)_x x$ is invertible, we just have to show that such $1-\alpha$ is invertible. The obvious expression to try is $1 + \alpha + \alpha^2 + \dots$. We need to show that this is well-defined and has well-ordered support.

Proposition 1.187. Let G be a bi-ordered group with positive cone $\mathcal{P}$ and suppose $A \subseteq \mathcal{P}$ is well-ordered. Then $\tilde{A} = S(A) = \cup_{n=1}^{\infty} A^n$, the subsemigroup generated by A, is also well-ordered.

We finish the proof of Theorem 1.184 assuming Proposition 1.187. The proposition has as a corollary that each g only occurs in finitely many A^n, in other words,

$$\limsup_{n\to\infty} A^n := \bigcap_{n=1}^{\infty} \bigcup_{j \geq n} A^j = \emptyset.$$

Indeed, suppose the limsup is non-empty. Being a subset of $\tilde{A}$ it is well-ordered so we let g be its least element. Then $g \in A^{n_j}$ for some $n_1 < n_2 < \dots$ and we write $g = a_j b_j$ where $a_j \in A$ and $b_j \in A^{n_j - 1} \subset \tilde{A}$. By Lemma 1.186 (i) there are only finite many different pairs (a_j, b_j) so some $b_j = a_j^{-1}g < g$ occurs infinitely many times, contradicting the minimality of g. Thus each $g \in G$ is in the support of only finitely many α^n and we can define $\gamma = 1 + \alpha + \alpha^2 + \dots \in D$, since $\tilde{A}$ is well-ordered. Clearly $((1-\alpha)\gamma)_1 = 1$ whereas general

$$((1-\alpha)\gamma)_g = \sum_{ab=g} (1-\alpha)_a (\gamma)_b$$

can only involve finitely many $b \in \tilde{A}$ (Lemma 1.186 (i)). Call them $b_1, \dots, b_k$ and choose N such that $g, b_1, \dots, b_k \notin A^n$ for all $n > N$ so that we have

$$\begin{aligned}((1-\alpha)\gamma)_g &= \sum_{ab=g} (1-\alpha)_a(\gamma)_b \\ &= \sum_{ab=g} (1-\alpha)_a(1+\alpha+\cdots+\alpha^N)_b \\ &= ((1-\alpha)(1+\alpha+\cdots+\alpha^N))_g \\ &= (1)_g - (\alpha^{N+1})_g \\ &= 0.\end{aligned}$$

Thus $(1-\alpha)\gamma = 1$ and similarly $\gamma(1-\alpha) = 1$. □

Proof of Proposition 1.187. We wish to do proof by induction. We need to control how elements "grow" (in the ordering) when we take products of $a_i \in A$. We do this by breaking $\tilde{A}$ up into manageable pieces.

The smallest convex subgroup containing $x \in G$ is

$$c(x) := \left\{ g \in G \,\middle|\, x^{-i} \le g \le x^i \text{ for some } i \in \mathbb{Z} \right\}.$$

We note that $1 \le x \le y$ implies $c(x) \le c(y)$. Define an equivalence relation $\sim$ on A by $x \sim y$ if $c(x) = c(y)$. In other words, $x \sim y$ if there exist $m, n \in \mathbb{Z}^+$ such that $x \le y^m$ and $y \le x^n$. (This is called Archimedean equivalence.)

As A is well-ordered, we can define a transversal W for $A/\!\sim$ by taking the smallest element of each equivalence class. Note that W is also well-ordered. Equip $W \times \mathbb{N}^+$ with the lexicographic order, a well-ordering.

Define $f\colon \tilde{A} \to W \times \mathbb{N}^+$ by sending x to (w, r) where $x \sim w$ (which is possible, even though W is a transversal for $A/\!\sim$ and not $\tilde{A}/\!\sim$, as $a_1 \dots a_k \sim \max\{a_i\}$ for a product of $a_i \in A$) and r is minimal such that $x \le w^r$.

Then one checks that f is order-preserving. It is convenient to extend $W \times \mathbb{N}^+$ by adding a smallest element $(1, 0)$. Let $X = W \times \mathbb{N}^+ \cup \{(1,0)\}$ and (by slight abuse of notation) also write $f\colon \tilde{A} \cup \{1\} \to X$ for the order-preserving extension.

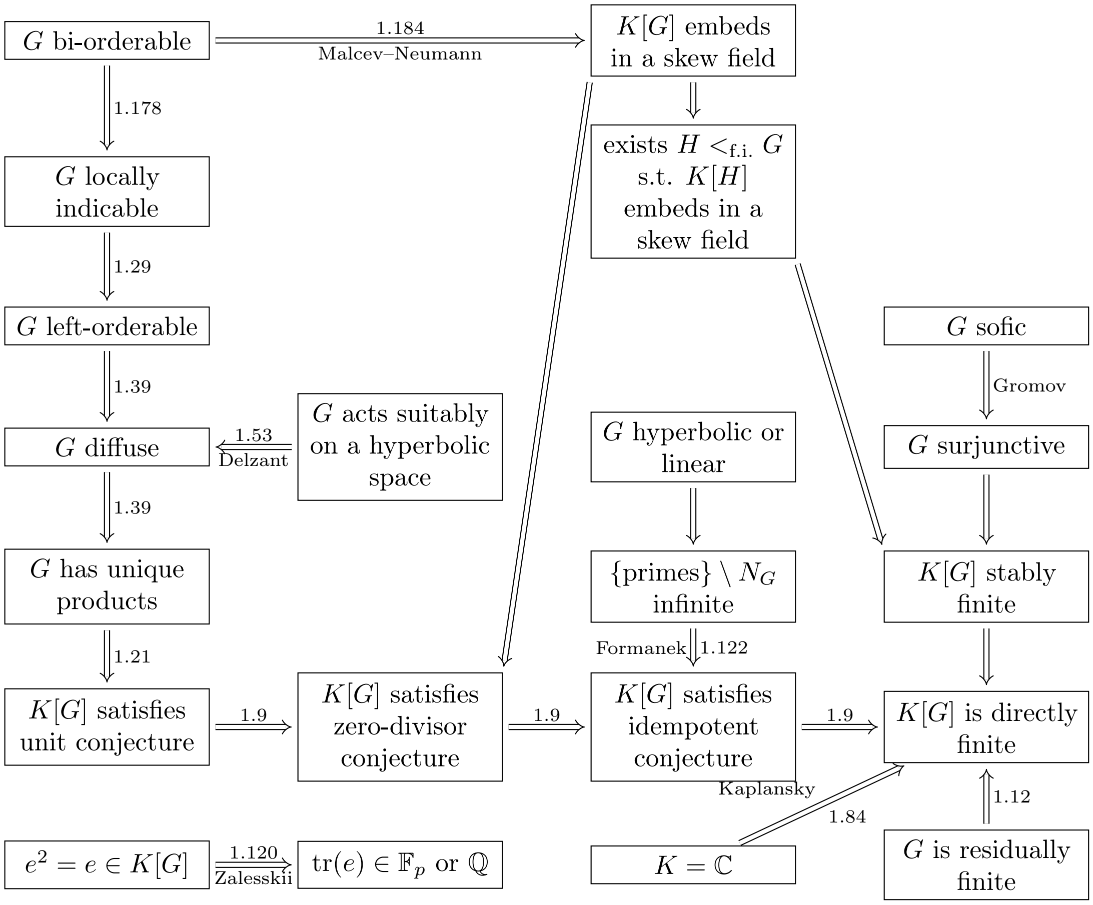
Claim. If $x \in \tilde{A}$ we can write $x = x_0 a x_1$ for some $a \in A$ and $x_0, x_1 \in \tilde{A} \cup \{1\}$ such that $f(x_0), f(x_1) < f(x)$.

The proof of the claim is left as an exercise, with the hint that we write $x = a_1 a_2 \dots a_k$ for $a_i \in A$ and let $a = \max\{a_i\}$.

Since f is order-preserving and X is well-ordered, $\tilde{A} \cup \{1\}$ will be well-ordered if and only if every $f^{-1}((w, r))$ is well-ordered. We prove this by transfinite induction on X. The base case is $f^{-1}((1,0)) = \{1\}$, so trivial. The inductive step follows from the claim: if $S = f^{-1}(\{(w', r') \in X \mid (w', r') < (w, r)\})$ then $f^{-1}((w, r)) \subseteq SAS$, which is well-ordered by Lemma 1.186 (ii). □

APPENDIX A

Overview of results in the course


G bi-orderable
1.184
Malcev–Neumann
$K[G]$ embeds in a skew field
1.178
exists $H <_{\text{f.i.}} G$ s.t. $K[H]$ embeds in a skew field
G locally indicable
1.29
G left-orderable
G sofic
1.39
Gromov
G diffuse
1.53
Delzant
G acts suitably on a hyperbolic space
G hyperbolic or linear
G surjunctive
1.39
G has unique products
$\{\text{primes}\} \setminus N_G$ infinite
$K[G]$ stably finite
1.21
Formanek
1.122
$K[G]$ satisfies unit conjecture
1.9
$K[G]$ satisfies zero-divisor conjecture
1.9
$K[G]$ satisfies idempotent conjecture
1.9
$K[G]$ is directly finite
Kaplansky
1.84
1.12
$e^2 = e \in K[G]$
1.120
Zalesskii
$\text{tr}(e) \in \mathbb{F}_p$ or $\mathbb{Q}$
$K = \mathbb{C}$
G is residually finite

APPENDIX B

Lectures in winter semester 2023/2024

(1) 2023-10-10: The Kaplansky conjectures and their implications, residually finite groups are directly finitely.

(2) 2023-10-12: Unique product property, left orderability, statement of Burns–Hale, corollary 1.31.

(3) 2023-10-17: Proof of Burns–Hale theorem, dynamical point of view, diffuse groups.

(4) 2023-10-19: Hyperbolic groups, Delzant's theorem.

(5) 2023-10-24: Primality of group rings (Connell's theorem) up to the proof of lemma 1.69.

(6) 2023-10-26: Rest of proof of Connell's theorem.

(7) 2023-10-31: Exercises (on torsion, FC-groups, $\mathbb{F}_2[\mathbb{Z}/3]$), trace map, traces of idempotents and nilpotents for finite G.

(8) 2023-11-02: Inner product on $\mathbb{C}[G]$, alternative proof for trace of complex idempotents for finite G, start of proof for arbitrary G (Kaplansky's theorem) with generalized Cauchy–Schwarz.

(9) 2023-11-07: Rest of approximation-based proof of Kaplansky's theorem on complex idempotents, generalization to arbitrary characteristic zero fields, direct finiteness of $K[G]$ when $\mathrm{char}(K) = 0$, places and valuation rings.

(10) 2023-11-09: Extension theorem for places, valuations, zero divisors over $\mathbb{C}$ give zero divisors over $\mathbb{F}_{p^n}$ for some n, lemma on test elements for places with finitely many elements guaranteed to be in valuation ring.

(11) 2023-11-14: The zero divisor conjecture is equivalent to the group of normalized units always being torsion-free, the power map, trace-like functions, traces of nilpotents, "normal closure traces" of nilpotents.

(12) 2023-11-16: Zalesskii's theorem that the trace of an idempotent is in the prime subfield (using number theoretic black box to get required places to deduce characteristic 0 case from characteristic p case), Formanek's theorem on idempotents, corollaries of Formanek's theorem.

(13) 2023-11-21: Big picture overview of results in the course, the Hantzsche–Wendt group P as an abstract finitely presented group and as a subgroup of $D_\infty \times D_\infty \times D_\infty$.

(14) 2023-11-23: Two proofs that P is torsion-free, P is none of the following: bi-orderable, locally indicable, left-orderable, diffuse.

(15) 2023-11-28: Ravels and corresponding universal groups (with and without free factor of $\mathbb{Z}$), Bowditch's ravel defines P, symmetries of the ravel give group automorphisms.

(16) 2023-11-30: Duplexes, the symmetry of Promislow's duplex and its utility in verifying the failure of the unique product property.

(17) 2023-12-05: Automorphism group of the direct product of a centreless and an abelian group, trivial-unit-preserving group ring automorphisms, twisted-unitary and symmetric units.

(18) 2023-12-07: The "2 out of 4 cosets" lemma for units of $K[P]$, reformulation in Boolean satisfiability, start of Mirowicz's computation of $(\mathbb{F}_2[D_\infty])^\times$ (embedding in matrix ring and determinant condition)

(19) 2023-12-12: Ping pong lemma, subgroup of units of the form $*_{\mathbb{Z}} \oplus_{\mathbb{N}} \mathbb{Z}/2$.

(20) 2023-12-14: End of computation of $(\mathbb{F}_2[D_\infty])^\times$ (semi-direct product structure and proof that we found all units), the subgroup of trivial units is self-normalizing under mild assumptions.

(21) 2023-12-19: Bi-orderability, torsion-free nilpotent groups are bi-orderable, bi-orderable groups are locally indicable.

(22) 2023-12-21: Malcev–Neumann theorem embedding $K[G]$ in a skew field for bi-orderable G.

(23) 2024-01-09: Stable finiteness of $K[G]$ from direct finiteness of $K[G \times H]$ with H finite, amenability and soficity, cellular automata.

(24) 2024-01-11: Surjunctive groups are directly finite, amenability is detected by the Ore condition (Bartholdi–Kielak).

(25) 2024-01-16: Semisimplicity.

(26) 2024-01-18: Property (T) (cancelled due to snow).

(27) 2024-01-23: Revision and Q&A.

(28) 2024-01-25: Revision and Q&A.

(29) 2024-01-30: Live coding demo (using SAT for left-orderability and the unique product property).

(30) 2024-02-01: Guest lecture by Grigori Avramidi on conjectures around 2-complexes.

Bibliography

[Bar23] Laurent Bartholdi. On Gardam's and Murray's units in group rings. *Algebra Discrete Math.*, 35(1):22–29, 2023.

[Gar21] Giles Gardam. A counterexample to the unit conjecture for group rings. *Ann. of Math. (2)*, 194(3):967–979, 2021.

[Mir91] Maciej Mirowicz. Units in group rings of the infinite dihedral group. *Canad. Math. Bull.*, 34(1):83–89, 1991.

[Mur21] Alan G. Murray. More counterexamples to the unit conjecture for group rings. 2021. arXiv preprint arXiv:2106.02147.

[Pas85] Donald S. Passman. *The algebraic structure of group rings*. Robert E. Krieger Publishing Co., Inc., Melbourne, FL, 1985. Reprint of the 1977 original.